Int. J. Advanced Networking and Applications
Volume: 03, Issue: 02, Pages:1135-1139 (2011)

Role of ANN in Secured Wireless Multicast Routing during Dynamic Channel Allocation for User Demanded Packet Optimality

Dr. B.S. Pradeep
Professor, Department of CSE, RRCE, Bangalore, India
Email: pradeepbs78@yahoo.com

S. Soumya
Karnataka State Open University, Mysore, Karnataka, India
Email: soumyaswarna@yahoo.co.in

ABSTRACT

The application of Artificial Neural Network (ANN's to mobile Ad Hock Network) for multicasting where the problem is to find an efficient route to transmit packets over many nodes in the network. For multicasting in MANETS which address the security and Quality of service (Q.O.S.) issues on the utility database makes this area highly suitable for ANN implementation. ANN is able to learn the relationship among past, current, and future route discoveries of the different nodes in the mobility range. A wide variety of different ANN has been used for route discoveries in the few years resulting in a noticeable number of publications on the subject. This paper proposes effective and novel application of Artificial Neural Network to Secure Multicasting in MANET's with Supporting Nodes has gained a lot of attention for secure routing using an ANN model. The methodology considers selection of input Variables for the ANN, determination of the optimum number of neurons for the hidden Layer selection of Multicasting with supporting nodes routing function. The proposed ANN model uses the feed forward network using back propagation algorithms.

Keywords : Mobile ad hoc network, artificial neural network, multi casting, multicast tree.

Date of Submission: December 04, 2010 Revised: June 30, 2011 Date of Acceptance: July 27, 2011

1. Introduction

MANET (Mobile Ad Hoc Network) is an autonomous collection of mobile hosts that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, network topology may change rapidly and unpredictably over time. The ad hoc wireless networks are generally decentralized, where all network activity including discovering the Topology and delivering messages must be executed by nodes themselves, i.e., routing functionality will be incorporated into mobile nodes. In some cases routing is done by a cluster head for all the mobile hosts of the cluster which it represents.

In this paper we proposed secure route in MANET's having support nodes. Support nodes are the special nodes which are deployed in the network for the sole purpose of helping regular nodes in routing. The support nodes are always connected and sweep across the network in snake like fashion. All nodes advertise their links periodically. When a node has a packet to send, it checks its two-hop neighborhood to find it satisfies the bandwidth and reliability requirements, it encrypts the packet with the secret key that it shares with the support node and sends the packet to the destination node in the neighborhood of any support node in the support structure. After success, it sends the packet by encrypting it with the secret key of the destination node. The destination generates an acknowledgment for received packet and sends it to the source through the Support structure.

2. Neural Network

In this section deals a short introduction to neural networks. Artificial neural networks are mathematical tools originally inspired by the way the human brain processes information. Their basic unit is the artificial neuron, schematically represented below in Fig.2.1.

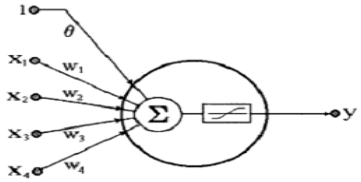

Fig 2.1: Artificial Neuron

The neuron receives (numerical) information through a number of input nodes (four, in this example), processes it internally, and puts out a response. The processing is usually done in two stages: first, the input values are linearly combined, and then the result is used as the argument of a non linear activation function. The combination uses the weights W_i attributed to each connection, and a constant bias term θ, represented in the figure by the weight of a connection with a fixed input equal to 1.The activation function must be a non decreasing and differentiable function; the most common choices are either the identity function ($y = x$) or bounded sigmoid (s-shaped) functions, as the logistic one ($y = 1 / (1 + e^{-x})$).

The neurons are organized in a way that defines the network architecture. The one we shall be most concerned with in this paper is the multiplayer perception (MLP) type, in which the neurons are organized in layers. The neurons in each layer may share the same inputs, but are not connected to each other. If the architecture is feed-forward, the outputs of one layer are used as the inputs to the following layer. The layers between the input nodes and the output layer are called the hidden layers.

Fig.2.2 shows an example of a network with four input nodes, two layers (one of which is hidden), and two output neurons. The parameters of this network are the weight matrix W_{3x4} (containing the weights $W_{i,j}$ that connect the neuron i to input j), the weight matrix U_{2x3}, and the bias vector θ_{5x1}(the bias connections have not been represented in the figure). If logistic functions are used for the activation of the hidden layer, and linear functions used for the output layer, this network is equivalent to the model which shows how complex and flexible even a small network can be?

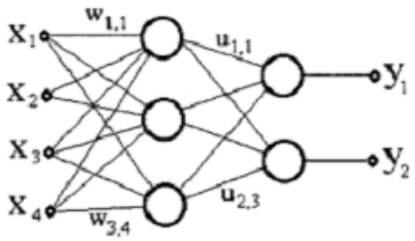

Fig 2.2: A two layer feed forward neural network

$$y_k = \sum_{j=1}^{3} \left(u_{kj} \cdot \frac{1}{1+\exp\left(-\sum_{i=1}^{4} w_{ji} x_i + \theta_j \right)} \right) + \theta_k \qquad \text{---Formula- (1)}$$

The estimation of the parameters is called the "training" of the network, and is done by the minimization of a loss function (usually a quadratic function of the output error).Many optimization methods have been adapted for this task. The first training algorithm to be devised was the back-propagation one, which uses a steepest-descent technique based on the computation of the gradient of the loss function with respect to the network parameters (that is the reason why the activation functions must be differentiable). Many other training algorithms, though, are now available, in load forecasting applications; this basic form of multiplayer feed-forward architecture shown above is still the most popular. Nevertheless, there are a large number of other designs, which might be suitable for other applications.

Artificial NNs have been developed and extensively applied since the mid-1980. There are many reports of successful applications particularly in pattern recognition and classification and in nonlinear control problems, where they may have some advantages over the traditional techniques. Since quantitative forecasting is based on extracting patterns from observed past events and extrapolating them into the future, one should expect NNs to be good candidates for this task. In fact, NNs are very well suited for it, for at least two reasons. First, it has been formally demonstrated that NNs are able to approximate numerically any continuous function to the desired accuracy [5].In this sense, NNs may be seen as multivariate, nonlinear and nonparametric methods, and they should be expected to model complex nonlinear relationships much better than the traditional linear models. Secondly, NNs are data-driven methods, in the sense that it is not necessary for the researcher to postulate tentative models and then estimate their parameters. Given a sample of input and output vectors, the NNs are able to automatically map the relationship between them; they "learn" this relationship, and store this learning into their parameters. As these two characteristics suggest, NNs should prove to be particularly useful when one has a large amount of data, but little a priori knowledge about the laws that govern the system that generated the data.

3. Proposed Approach

This work presents a detailed methodology for developing a neural network model for Secure Multicasting Routing with supporting nodes. There are some properties, which are considered important:-The model should be automatic and able to adapt quickly to changes in the routing behavior. The model is intended for use in many different cases. This means that generality is desired. The model should be reliable. Even under exceptional circumstances must not give rise to unreasonable errors. The model should be easily attachable to Multicast tree creation, deletion, Loop free Routing. The proposed ANN model uses the Feed-forward network using Back propagation algorithm.

Volume: 03, Issue: 02, Pages:1135-1139 (2011)

Multicast Tree Creation

A node (source) which wants to communicate with the other nodes (destinations) in the multicast groups, checks the routing table for a route towards the destination group. If the route is not found, it initiates the route tree creation by sending the MULTICASTROUTE_REQUEST packet to the neighbors. The source generates a MULTICASTROUTE_REQUEST packet, encrypts it with the common shared key and sends it to the neighboring nodes one by one. (Because all nodes know the shared key, intermediate nodes can decrypt the packet and process it and rebroadcast it after encrypting it again.).Each intermediate node decrypts the packet and stores the last hop routing entry if the sequence number is greater than the last entry. It checks if it has any multicast route to the destination group. If it has then it can send a MULTICASTROUTE_REPLY

Multicast Tree Destruction

When a multicast group is no longer required, the root of the multicast tree sends out of MULTICASTROUTE_DESTROY [packet to all the nodes in the group after which all nodes remove the entry for this multicast group from the multicast table and destroy all the keys used to transmit the data.

4. Analytical Model

Let 'n' is the number of nodes in the network, D be the average number of neighbors of a node and P_s be the probability of the neighboring node fulfilling reliability, bandwidth and congestion requirements.

The probability that a node has a neighbor is approximately.

$$P_n = \pi r^2 l^2 \quad \text{…Formula -(2)}$$

Where l^2 is the total area of simulation and r is the radio range.

The number of neighbors D, of each node can be approximated as

$$D = P_n.n = \pi r^2 n L^2 \quad \text{…Formula -(3)}$$

The probability P_s is given by

$$P_s = P_r.P_b.P_c \quad \text{…Formula -(4)}$$

R_{total} indicates total number of route requests generated for creating one multicast group tree.

4.1 Secure Multicasting in MANETs (With support nodes)

In this method we assume that the network has special kinds of nodes called "support nodes". A mobile node is said to be a support node if its primary responsibility is routing. A mobile node which is not a support node is called a regular node. We assume that all the support nodes are always connected and they have snake-like mobility pattern. Since the support nodes are always connected, the task of message relay and message exchange policies are simplified. The regular nodes periodically send out HELLO packets advertising their neighbors.

4.2 Registration

All the nodes which want to be part of a multicast group send a Registration Request to the support nodes. The support nodes add these nodes in the list of multicast group and then send out a Registration Request to the particular node. This confirmation also has the secret key that is to be used for forwarding the packets for this group.

4.3 Data Transfer

A node which has to send data to a multicast group listens to the HELLO packets of its neighbors and checks if there exists any support node in its 2 hop neighborhood. When there is a support node available in its 2 hoop neighborhood, it forwards packets to the support node using the multicast group id as the destination address.

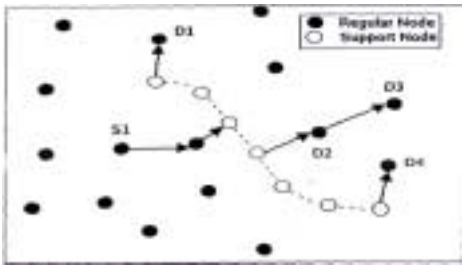

Figure 4.1: Example Multicast Delivery using Support nodes

When a support node receives a packet from regular node, it first decrypts the packet using the secret key used for the particular multicast group. It then checks the destination address. If the destination address is multicast group address registered to it, it notifies all support nodes that it has a packet for multicast group. Each of the support nodes which knows its 2 hop neighborhood checks if it can reach any node in this multicast group and whenever any node is available, it delivers the packet by fetching it from the other support nodes. All support nodes keep synchronized information about the nodes, which have been delivered a particular packet. When a particular packet is delivered to all the nodes in the multicast group, it is deleted from the buffer of the support nodes. An example of multicast data delivery is given in Figure 4.1.

4.4 Deregistration

If a node wants to leave a group, it sends a deregistration request to the support nodes. The support nodes generate a new secret key for the multicast group and distribute it to the remaining nodes in the group. All further packets will have to be encrypted using this new key. This way a node which has left the group will not be able to read the group data.

4.5 Modeling

The number of transmissions required to send a packet from source to the multicast group can be modeled as follows:

The support structure is either one hop away or two hops away from source and destination. So the expected number of transmissions up to support structure can be give as

$$T_n = (1.P_n + 2.(1 - P_n)).M_s \quad \text{…Formula -(5)}$$

Where P_s is the probability that a support node is in one hop neighborhood and $1 - P_n$ is the probability that support node is in two hop neighborhood. P_n is taken to be 0.5.and M_s is the number of nodes in the multicast group. The number of transmissions required along the support structure can be written as

$$T_s = 2.P_s^2.\ (i\ (n - i)).M_s \quad \text{…Formula -(6)}$$

Where, P_s is the probability that the packet comes into/goes out of a support structure at a particular node and n is the number of support nodes. P_s is considered uniform, i.e. there is equal chance of reaching to any node of the support structure.

So $P_s = 1/n$.

The total number of transmissions for a packet is

$$P_s = 2T_n + T_s \quad \text{…Formula -(7)}$$

4.6 Simulation Environment

The simulation of the designed routing protocols was carried out in a multi-threaded simulator. In the simulation model, the area considered for simulation is 800 meters (m) by 800 meters with a set of nodes placed randomly with uniform distribution. The total number nodes (i.e. network density) are varied from 50 to 200 for different simulations. The broadcast range is 150m and the channel capacity is 1 Mbps. The communication medium is broadcast and all the nodes are assumed to have bi-directional connectivity. The simulation is carried out for different number of source nodes in the given area. Since no link layer details are modeled, a link layer event is generated automatically whenever a link fails or reappears.

Multiple runs are conducted for proposed routing scheme with different values of seeds to accommodate diverse network conditions and topologies. The final results are averaged over these runs.

The mobility of the mobile nodes in the simulation is modeled using the Random Waypoint Model which includes pause times between changes in it can be described as follows:

- A node selects a random point to move to in the area of simulation.
- The node randomly takes speeds up to 2 m/s and moves to the selected point.
- When it reaches the selected point, the node stops for some time and again starts the mobility.

4.7 Clusters

For simulating the cluster based routing protocols, clusters are formed and cluster heads are elected using the Lowest-ID. All nodes in the cluster are one hop away from the cluster head so that the cluster head knows all the members of the cluster. The nodes which are members of more than one cluster act as gateways between these clusters.

The Lowest-ID algorithm proceeds as follows and results in the formation of clusters which are at most two hops in diameter:

1. Each node is given a distinct ID and it periodically broadcasts the list of its neighbors (including itself).
2. A node which only hears the nodes with ID higher than itself is a cluster head.
3. The Lowest-ID node that a node hears is its cluster head, unless the Lowest-ID specifically gives up its role as a cluster head (deferring to a yet lower ID node)
4. A node which can hear two or more letterheads is a gateway; otherwise, a node is an ordinary node.

4.8 Multicast Group Membership

Multicast group members are randomly chosen from the available set of nodes based on the seed value. For algorithms which do not have explicit messages to join or leave the group, the members join the group at the beginning of the simulation. Sources are also randomly generated from the nodes in the network. The sources and group members are selected independently from the set of network nodes. Thus, there are no restrictions on the choice of the sources and the members. Experiments are conducted for a single multicast group.

4.9 Secure Multicasting (With support nodes)

For secure multicast with support nodes, the graphs of average delay versus number of support nodes (Formula -(5)) as well as average number of hops required versus number of support nodes is given in Formula -(6). It can be seen that the average delivery time decreases as the number of support nodes increase. His is because as the support nodes increase, more number of destinations is reachable in lesser time; also the number of hops increases because the packets travel through more number of nodes in the support structure. The total number of transmissions required for each multicast packet is given in Formula -(7). This graph shows the number of transmissions as given in analysis of Section As can be seen from the graph, the number of hops required to transmit a multicast data packet increases linearly with the number of support nodes because the packets pass through more number of support nodes.

5. Conclusion

As the importance of mobile ad hock networks is growing and their usage is increasing in sensitive applications like uninterrupted power supply and in military, the issues of security have become important. The routing in MANET'S which is already complex due to the multi hop nature of the ad hoc networks faces a lot of problem in terms of security. In this paper we have identified security issues affecting the routing in mobile ad hoc Networks and have proposed routing schemes. For multicasting the multicast group has a separate cryptographic key which is updated if any of the group members leaves the group. The analysis and simulation of the proposed schemes stated that the methods find secure loop tree path. The methods which use the support nodes have minimum delay when there is more number of nodes. Have minimum delay when there is more number of nodes because more number of source and destination and or destinations is reachable. When the number of support nodes is less, the delay incurred depends on the speed of the support structure. With supporting nodes using back propagation method by ANN's applies for solution.

References

[1]. Akio Koyama, Toshiki Nishie,Junpei Arai, Leonard Barilla, AGA-Based Q.O.S.multicast routing Algorithm for large-scale network. International Journal of high-Performance computing and Networking.V.5n.5/6,p381-387,May2005.

[2]. A.T.Haghighat.K.Falz.M.DehgahseA, Mowhari,y. Ghahrumani, Multicasting Routing with multiple constraints in high-speed networks based generic Proceeding of the 15th International conference in Computer communication,p181-192,August1214,Mumbai,Maharastra,India.

[3]. Chon gun Kim, Lemuroid Talipov, and Byounghulahn," AReverse AODV Routing Protocol in Ad Hoc Mobile Network", LNCS 4097. PP 522-531, 2006.

[4]. Gars F .A. and Schmidhuber J, "LSTM recurrent networks learn simple context free and context sensitive languages", Transaction on Neural network, IEEE, 12(6) 1333- 1340, 2001.

[5]. Hearth K.U. and Hashimoto sh, "Automated trend diagnosis using neural networks", 0-7803-6583-IEEE, 1186-1191, 2000.

[6]. J Tang, B Chuang and F Wu, " Link stability-based Routing Protocol for Mobile Ad Hoc Network", 2006 IEEE Conference on systems Man, and Cybernetics October 8-11, 2006, Taipei, Taiwan.

[7]. Jin-Ku Jeong, Sung-Ok Kim, Chihwa Song, Multicast Routing Algorithm based on extended simulated annealing algorithm", proceeding of 7th WSEAS International Conference on Mathematical Methods and computational Techniques on electrical engineering p, 129-133, October 27-29, 2005, Sofia, Bulgaria

[8]. Pallapa Venkataram, Sudip Ghosal, B.P. Vijay kumar, Neural Network based Optimal Routing Algorithm for communication Neural Networks, v.15.n.10.1.1289-1298, December 2002.

[9]. Pradeep.B.S, Soumya.S. Dynamic channel allocation for user demanded packet optimality- Focus on network initialization procedure-Int. J. Advanced Networking and Applications, Volume: 01, Issue: 03, Pages: 181-187 (2009).

[10]. Pradeep.B.S, Soumya.S- A New Approach for Load Balancing and QOS in on demand protocols – In the MANET's Perspective- Int. J. Advanced Networking and Applications, Volume: 01, Issue: 04, Pages: 275-281(Feb 2010).

[11]. S-J Lee and M. Gerla, "Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Network," Proc ICC 2001, vol 10. pp. 3201-3205, June 2001.

[12]. Y Kim, J Jung's. Lee and Skim," a Belt-Zone Method for decreasing control messages in Ad Hoc networks ". LNCS 3982, PP 64-72, 2006.

[13]. Zhi Li and YU-twang Kwak."A new Multipath Routing Approach to Enhancing TCP security in Ad Hoc Wireless Network" in Proc ICPPW ,2005.

Authors Biography

Dr. B.S. Pradeep B.E(CSE)., MTech (Networking)., Ph.D(CSE). He is working as Professor in CSE dept. of RRCE, Bangalore , Karnataka. 10+ years experienced in teaching. His areas of interest are networking, mobile computing, Computer organization, system software.

Mrs. Soumya.S. M.CA., She is pursuing her IV sem MTech in Information Technology at KSOU, Mysore, Karnataka. 3+ years experienced in teaching. Her areas of interest are networking, Computer graphics.