PROTOCOL FOR IMPROVING PACKET DELIVERY RATIO IN MANET

S.Vasudevi[1], D.Mary Ponrani[2]

[1]Final year PG Student, [2]Assistant Professor, Department of Computer Science Engineering,
Dr.Sivanthi Aditanar College of Engineering, Tiruchendur, (India)

ABSTRACT

Mobile Ad Hoc Network (MANET) is regarded as a collection of mobile nodes in which communication among those nodes are done without need of any established infrastructure. In MANET, high mobility of nodes causes frequent topology changes and recurrent link failures. The failure of the link will deny the transmission of packets through the existing path that contains the lost link. This leads to rediscovery of new route by forwarding RREQ packet. As the link failures gets increased, number of RREQ packet in the network also gets raised, that result in increased routing overhead which further affects the packet delivery ratio. So it is essential to reduce the overhead of route discovery in designing routing protocols for MANET. In this paper, new routing protocol based on neighbour details and probabilistic knowledge for improving the packet delivery ratio is proposed. Through this protocol packet delivery ratio gets increased by reducing the routing overhead. The confidentiality and integrity of the data packets also needs to be ensured to avoid unauthenticated access.

Index Terms: MANET, Routing Protocols, Routing Overhead, Packet Delivery Ratio, Cryptography Algorithms.

I. INTRODUCTION

In Ad hocZ networks, nodes should be able to move freely and the information should be routed through new paths after old path selected have been broken, the network should also be able to handled clustering. MANETs consists of fixed or mobile nodes which are associated without the help of fixed infrastructure or central administration.

In MANETs, link breakage and extinction of end-to-end route occurs due to the topology variation and its prediction is done by means of routing protocols like AODV and DSR. Both conventional on demand routing protocols [2] [4] uses flooding to discover a route to a particular destination. Through flooding, the source node broadcast a Route Request (RREQ) packet to its 1 hop neighbours, and this neighbours can retransmit the packet to its neighbors.This redundant retransmission causes the broadcast storm problem [1], which leads to contention and enormous number of packet collisions.Some of the Optimization methods [1] to reduce this storm problem are “area-based methods ,probability-based methods, flooding, neighbor-knowledge methods ”.To contract the Broadcast storm problem occurred in MANET, Probabilistic Scheme, Counter based Scheme and Distance based Schemes are used [1]. In Probabilistic Scheme, based on the computed probability value, RREQ is forwarded. Smaller Probability value will result in reduced Storm effect. In Counter based Scheme, Expected Additional Coverage (EAC) is used for taking forwarding decisions. In Distance based scheme, relative distance between nodes are used to adjust the packet retransmission.

Route discovery is optimized in the absence of previous knowledge by using the tree based routing protocol named "OTRP " [3] . Broadcast redundancy gets reduced by using Scalable broadcast algorithm[8], thus reduces overhead of routing.

Probability and Neighbor knowledge methods are combined and routing protocols that use these methods (both probabilistic and neighbor knowledge) are derived [9]. This protocol (DPR) can solve the problem in FPR, but not works well in case of increased heterogeneity in network. NCPR [10] solves the problem of DPR and it reduces the routing overhead problem and thus it provides better Packet delivery ratio. In NCPR, additional coverage ratio and connectivity factors are used to determine the rebroadcast probability. As NCPR provides better result than its predecessors like AODV, OTRP, FPR and DPR, it is used for routing the data in MANET.

By means of NCPR, problems in normal flooding are discarded. i.e., Broadcast storm problem that causes serious contention and collision is avoided. As a result, overhead occurs during route discovery in MANET is reduced, this automatically leads to increased Packet delivery ratio. Additional protection in Packet delivery is obtained by using effective security mechanisms like Symmetric cryptographic techniques for encrypting and decrypting the data packets.

II. RELATED WORK

Routing is defined as the process of finding path from a source to every destination in the network. Three main requirements for designing ad hoc network routing protocols are Adaptiveness, Resilience to loss and low overhead. Major classifications of Ad hoc routing protocols are Reactive(On- demand), Proactive(Table-driven) and hybrid routing protocols. In this classification, Reactive routing protocols also called as On demand routing protocols can disseminate route discovery packets only if data packets are needs to be sent from source node to destination node. The reference papers [1] and [2] describes the conventional On demand routing protocols AODV and DSR respectively. C. Perkins, E. Belding-Royer, and S. Das [1] proposed the working of AODV protocol. This routing protocol is intended for use by mobile nodes in an ad hoc network and it offers quick adaptation to dynamic link conditions. This protocol gives reasonable result, but routing overhead and hello packet overhead gets raised if mobility gets increased. It also affects packet delivery ratio if mobility gets increased. D. Johnson, Y. Hu and D. Maltz [2] proposed Dynamic Source Routing protocol (DSR) for efficient routing in MANET. The source node places a "source route" in the header of the packet, When it sends a new packet to some destination node. This "source route" gives the sequence of hops that the packet needs to follow on its way to the destination. By using this protocol, Stale cache may impact the Performance of network.

S.Y. Ni, Y.C. Tseng, Y.S. Chen, and J.P. Sheu [4] identify Broadcast Storm problem and propose several schemes to reduce redundant rebroadcasts and differentiate the timing of rebroadcasts to solve this problem. According to ref paper [4], To solve this storm problem, probabilistic scheme, distance-based scheme, counter based scheme and cluster based schemes are used. In Probabilistic Scheme , authors of ref paper [5] described that rebroadcast is done by tossing a die .i.e. based on the computed probability value, packet gets forwarded. If computed probability value is equal to 1, it is similar to flooding. In Counter-Based Scheme[4] and [5], based on the counter threshold value, rebroadcast is done. Expected Additional Coverage (EAC) is used to control the unnecessary rebroadcast of RREQ. When EAC of host rebroadcast becomes too low, retransmission is prevented.

W. Peng and X. Lu [8] propose the Scalable Broadcasting Algorithm (SBA) for reducing broadcast redundancy in MANET. By means of this algorithm, unnecessary broadcasts are avoided by using the information regarding duplicate broadcasting and local topology, thus network bandwidth and energy gets saved. The idea of SBA is "if all neighbours of the particular node have been covered by previous RREQ , then that node need not rebroadcast the received RREQ.

H. AlAamri, M.Abolhasan, and T.Wysocki proposed OTRP in which Tree-based Optimized Flooding (TOF) algorithm is used to improve the scalability in ad hoc network eventhough previous knowledge to the destination is not available.

FPR is the basic probabilistic route discovery method discussed in [9]. It makes use of fixed probability value, without considering network density. In FPR, source can initially send RREQ with probability "P=1" i.e.,(initially sending nodes can broadcast the packet with simple flooding). Any inner node that receives that RREQ, rebroadcast it to its neighbours with probability "P<1". The probability value used here during rebroadcast is same for all nodes and it does not varied regarding the local topology characteristics, so it result in unfair distribution of probability "P". To solve this unfair distribution of "P" in FPR, forwarding probability needs to be computed based on random distribution of mobile nodes and regions of varying degrees of node density.

J.D. Abdulai, M. Ould-Khaoua, L.M. Mackenzie, and A. Mohammed [9] propose a generic probabilistic method for reducing the storm problem. This method will reduce the overhead associated with the dissemination of RREQs. This method also solves the unfair probability distribution problem occurred in FPR. In Dynamic Probabilistic route discovery (DPR), dynamic forwarding probability values are computed by considering local density of forwarding node and set of covered neighbours of forwarding node. Local density is estimated by finding density of region in network using local neighbourhood information of that region. A node is located in dense region if its number of neighbours are greater than average number of neighbours in network.

III. PROTOCOL DESCRIPTION

In this section, the protocol used for reducing the routing overhead is discussed. Neighbor Coverage based Probabilistic Routing protocol (NCPR) from ref paper [10] is considered for effective routing and increased packet delivery ratio. NCPR algorithm makes use of additional coverage ratio and connectivity factor to calculate the rebroadcast probability. Also symmetric cryptographic mechanisms are added to ensure secure routing.

3.1 Computation of Neighbors set that are Uncovered

When the source node broadcast the RREQ packet to its neighbours, those neighbour nodes can perform the uncovered neighbour computation to calculate the set of its neighbours. Those set of neighbours fails to receive the RREQ flooded from the source and so called as uncovered neighbours. Thus for each neighbour of source, uncovered neighbours are determined and RREQ is forwarded only to those uncovered neighbours.

Initial Uncovered neighbour computation is done using the below formula :

$$\mathrm{UCN}(n_a) = \mathrm{N}(n_a) - [\, \mathrm{N}(n_a) \cap \mathrm{N}(\mathrm{src}) \,] - \{\mathrm{src}\} \qquad (1)$$

Where UCN(n_a) denotes uncovered neighbours of node n_a. n_a is one of the neighbour node of source node. src denotes the source which broadcast the RREQ packet. N(n_a) represents the neighbours of node n_a and N(src) denotes the neighbours of source node.

This computation takes the difference of neighbours of node n_a and common neighbours of both n_a and src.

3.2 Rebroadcast Delay and UCN adjustments

After the initial uncovered neighbour computation, rebroadcast of RREQ is delayed for some time interval. This delay value is called Rebroadcast delay and is used to calculate the rebroadcast order.

According to [10] , Rebroadcast delay is computed using below formula :

$$\mathrm{RBD}(n_a) = \mathrm{MaxDelay} \times \left(1 - \frac{|\mathrm{N(src)} \cap \mathrm{N}(n_a)\ |}{|\mathrm{N(src)}|}\right) \tag{2}$$

Where RBD(n_a) denotes rebroadcast delay of node n_a. A small constant delay is used as MaxDelay. To determine the number of elements in the set, the symbol | . | is used.

Based on that rebroadcast delay value, the node can set its timer. By means of this delay time, efficient transmission order is determined.

During this delay time, if any redundant RREQ packet is received in $n_a$from its neighbour n_b , then the node n_a further adjust its neighbour list in UCN set as :

$$\mathrm{UCN}(n_a) = \mathrm{UCN}(n_a) - [\mathrm{UCN}(n_a) \cap \mathrm{N}(n_b)\ ] \tag{3}$$

The duplicate RREQ packet received from the node n_b is discarded after this adjustment. The node can gain its final UCN set when this delay timer gets expired.

3.3 Rebroadcast Probability Computation

Rebroadcast probability is determined by means of using additional coverage ratio and connectivity factor.

Additional coverage ratio is the ratio of uncovered neighbours of node n_a to neighbours of the node n_a. It is computed as :

$$\mathrm{ACR}(n_a) = \frac{|\mathrm{UCN}\ (n_a)|}{|\mathrm{N}(n_a)|} \tag{4}$$

Connectivity factor is obtained by dividing connectivity metric by total number of neighbours of node n_a. Connectivity metric is indicated by 5.1774 log(n), where n is the number of nodes in the MANET. The formula for Connectivity factor is given as below :

$$\mathrm{CF} = \frac{5.1774\ \log(\mathrm{n})}{|\mathrm{N}(n_a)|} \tag{5}$$

Rebroadcast probability is determined by taking the product of connectivity factor and additional coverage ratio . Then based on that rebroadcast probability, the node n_a can rebroadcast the RREQ to its uncovered neighbours.

3.4 Incorporating Security Mechanisms

Maintaining security while routing is a significant issue in MANET [6],[7]. Data messages and routing or control messages are the two types of messages utilized in MANET. Control messages are used for the establishment of new route and maintaining the already identified route. During the broadcast of the routing messages like RREQ, RREP and RERR, the intermediate nodes may process these messages. This makes maintaining the security in routing messages a exigent task than securing data messages. In this paper, the data packets are secured using symmetric key algorithm to ensure confidentiality and identity. Here AES is used for encryption purposes .

AES stands for Advanced Encryption standard and is based on Rijndael cipher. It uses three different key lengths like 128, 192 and 256 bits. Symmetric cipher algorithm stores the compressed form of encrypted data resulted in small size database. It provides faster encryption and decryption as well as confidentiality.

3.5 Algorithm Flow

The flow of the NCPR algorithm is given below :

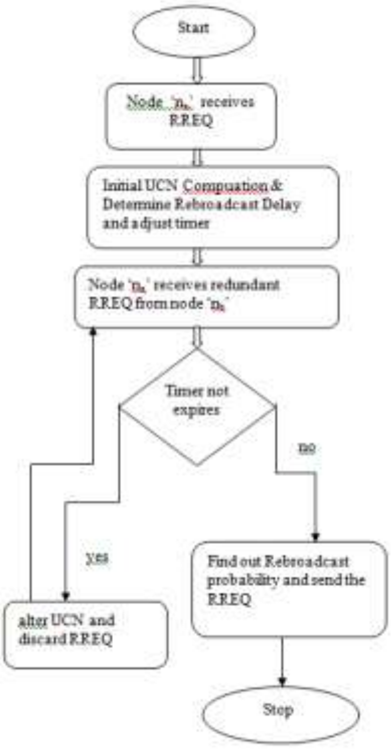
Start
Node 'n$_s$' receives RREQ
Initial UCN Computation & Determine Rebroadcast Delay and adjust timer
Node 'n$_s$' receives redundant RREQ from node 'n$_j$'
Timer not expires
no
yes
Find out Rebroadcast probability and send the RREQ
alter UCN and discard RREQ
Stop

Fig. 1 Flow of Algorithm

3.6 Implementation of NCPR

According to [10], the source code of AODV in NS-2 is modified to implement NCPR. By means of using this protocol, hello packet overhead and overhead occurred due to the neighbor list in RREQ are reduced.

The hello packet overhead is reduced by restricting the use of periodical hello mechanism. Instead of hello packets, RREQ and RERR control packets are used. The mechanism specified in [11] helps for hello packet overhead reduction. According to that paper [11] , the node can send hello packet only if the elapsed time of RREQ is greater than hello interval value.

In RREQ packet, the neighbor list overhead is reduced by monitoring the changes of the node's neighbor table. RREQ header of the existing AODV is modified by inserting a fixed field that represents the size of neighbor list in RREQ and dynamic neighbor list.

As the implementation of NCPR gets succeeded, the next step is to apply the AES algorithm for secure data transfer in MANET.

IV. SIMULATION RESULTS

The routing protocol discussed in this paper is used for improving the packet delivery ratio in mobile ad hoc network. By this protocol, reduced routing overhead is achieved in MANET and hence improved packet delivery ratio is obtained. Then by using AES, secure data gets transferred in the overhead less network.

For simulate this protocol in ns2, the following simulation parameters are used.

TABLE 1 Simulation Parameters

Simulation Parameter	**Value**
Simulator	NS-2 (v2.30)
Size of topology	1100m x 1100m
Number of nodes	50,100 or 150
Transmission range	250m
Interface Queue length	50
Bandwidth	2 Mbps
Type of Traffic	CBR
Number of CBR connections	10 or 12
Size of packet	512 bytes
Packet Rate	4 packets/sec
Pause Time	0sec
Minimum Speed	1 m/sec
Maximum Speed	5 m/sec
Simulation time	150 sec

The implemented secure routing protocol is evaluated by means of checking the following performance metrics :

- **Routing Overhead :** the total number of control (RREQ) packets transmitted in MANET during the simulation time.
- **End-to-end delay :** It is also called average delay. It is the average time difference between the sent time of CBR data packet by the source node and the successful reception time by the destination node.
- **Throughput :** It is the total number of CBR data packets received (bytes) at destinations in one second.
- **MAC Collision rate :** The total number of packets dropped as a result of collisions happened at the MAC layer.
- **Packet delivery ratio :** The ratio of the number of data packets successfully arrived in the CBR destinations to the number of data packets generated by the CBR sources.

First, number of nodes needed and number of CBR connections needed are selected. The nodes may be 50,100 or 150.and CBR connection may be 10 or 12. After that, run the corresponding nam window. Initially nodes are in one position. After simulation time starts running, nodes started to move here and there. Then CBR connections are started between source 15 and destination 17. so node 15 starts broadcasted RREQ to reach node 17.

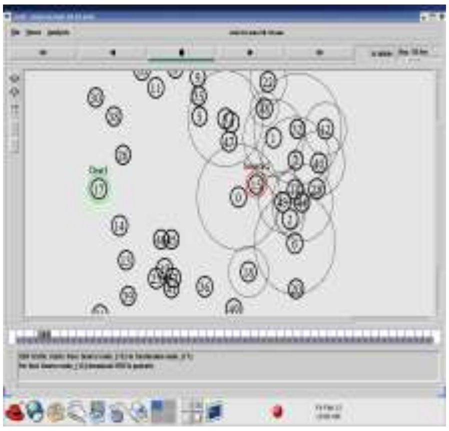

Fig. 2 Source Broadcast The RREQ

The RREQ gets broadcasted until it reaches the destination node 17.

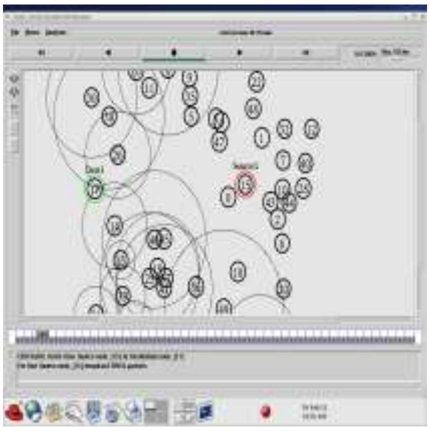

Fig. 3 RREQ reaches the destination

The broadcasted RREQ reaches the destination 17 and then RREP is unicasted from 17 to 15.After RREP reaches the source, data packet starts moving from 15 to 17

.

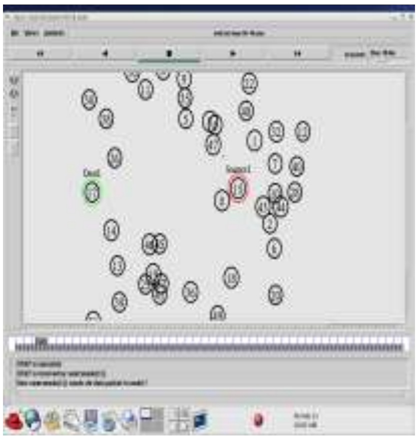

Fig. 4 Source 15 sends CBR packet to 17

Because of the mobility of nodes, the existing link in discovered route gets broken, resulted in dropping of packets and so new route discovery is started.

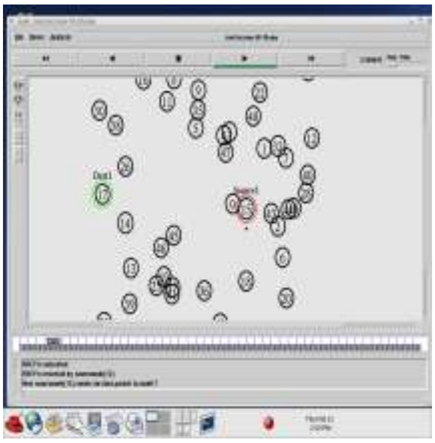

Fig. 5 Packet dropping

Thus in above Fig .5 packet gets dropped, so 15 sends RREQ to discover a new route.

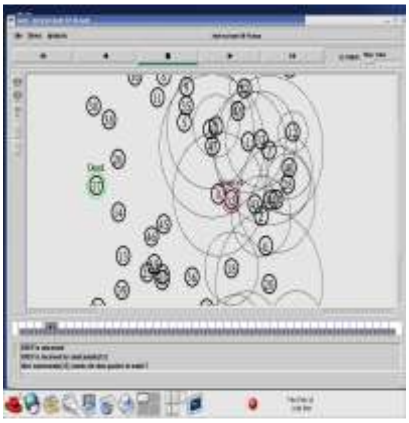

Fig. 6 Rediscovery of new route

Similarly other 9 different pairs of source and destination communicated through CBR traffic. As nodes are mobile, its neighbours can change from time to time. So, neighbors of each nodes are computed and it gets stored in one trace file named nodeneighbor.tr. This information is used for delay and probability calculation. Then additional nodes to be covered by rebroadcast are identified. Connectivity factor of each node are determined and based on that rebroadcast probability is found.

Using this probability, the packet gets forwarded. The packet delivery ratio obtained as a result of varying number of CBR connections are given as follows .

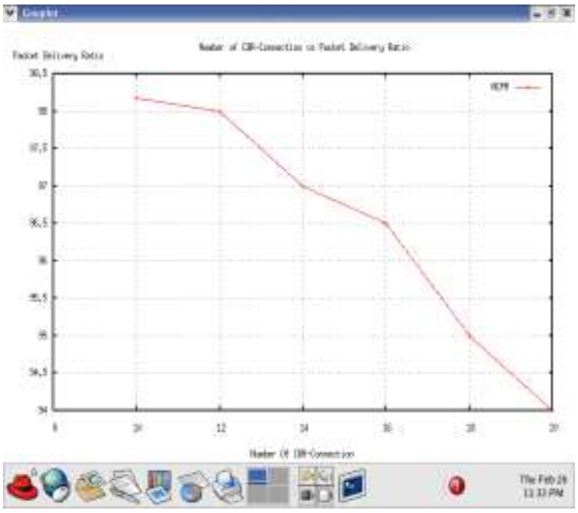

Fig. 6 PDR With Varied CBR Connections

If number of CBR connections gets increases, Packet delivery ratio gradually decreases. But PDR obtained using this protocol is better compared to conventional on-demand routing protocols. Also by using AES, confidentiality and integrity of the data packets are preserved.

V. CONCLUSION

In this paper, the routing protocol that reduces overhead problem occurred during route discovery in MANET for improving the packet delivery ratio is discussed. By using this protocol, broadcast storm problem that causes the serious contention, collision and redundant rebroadcast in the network is resolved, thus reduces the routing overhead and ensures high packet delivery. Also the symmetric cipher algorithm AES is applied to ensure secure packet delivery. Using this AES algorithm, the data packets flows from source to destination are encrypted, thus confidentiality and integrity is guaranteed. QOS consideration of this protocol will be left for future enhancement. For improving the QOS of NCPR in MANET, the uncovered neighbours having higher signal strength should be selected and RREQ packet is forwarded only to those nodes.

REFERENCES

[1] “AdHoc On-Demand Distance Vector(Proactive routing) Routing” S. Das, E. Belding-Royer, C. Perkins , in RFC 3561, 2003.

[2] “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks for IPversion 4”, Y. Hu, D. Maltz & D. Johnson in IETF RFC 4728, 2007, vol. 15, pp. 153-181,2009.

[3] “On Optimising Route Discovery in Absence of Previous Route Information in MANET(OTRP)” T. Wysocki,, M. Abolhasan and H. AlAamri in 2009,VTC in IEEE.

[4] "The Broadcast Storm Problem in a Mobile AdHoc Network", Y. Ni, Sheu.J.P, Chen, in IEEE/ACM MobiCom,1999.

[5] "Probabilistic Counter-Based Route Discovery for Mobile Ad Hoc Networks", Mackenzie, A. Mohammed, Perkin, and J.D.Abdulai, in Proceedings. Int'l Conf. Wireless Comm. And Mobile Computing: Connecting the World Wirelessly (IWCMC '09), pp. 1335-1339, 2009.

[6] " Comparison of Broadcasting Techniques for Mobile Ad hoc Networks", B. Williams and T. Camp , in Proceedings. ACM MobiHoc, pp. 194-205,2002.

[7] "Improving Probabilistic Route Discovery in Mobile Ad Hoc Networks", Mackenzie ,J.D. Abdulai, and M. Ould-Khaoua,in Proceedings IEEE Conf. Local Computer Networks, pp. 739-746, (2007).

[8] "On the Reduction of Broadcast Redundancy in Mobile Ad Hoc Networks", X. Lu and Peng.w in Proceedings, ACM MobiHoc, pp. 129-130, 2000.

[9] "Neighbour Coverage: A Dynamic Probabilistic Route Discovery for Mobile Ad Hoc Networks",L.M. Mackenzie, J.D. Abdulai, M. Ould-Khaoua, and A. Mohammed, in Proceedings. Int'l Symp.Performance Evaluation of Computer and Telecomm. Systems (SPECTS '08), pp. 165-17,2008.

[10] "A Neighbor Coverage-Based Probabilistic Rebroadcast for Reducing Routing Overhead in Mobile Ad Hoc Networks", Sung Xin , Jing Xia, En Bo Wang and Dan Keun, in proceedings IEEE(2013) .

[11]"An Estimated Distance Based Routing Protocol for Mobile Adhoc Networks", Sung, Wang, X.M .Zhang., in proceedings. IEEE Trans. Vehicular Technology, no. 7, pp. 3473-3484, Sept.2011.

[12]"Performance Evaluation of Symmetric Encryption Algorithm in MANET and LAN", Md.MohirHossain and M.A.Matin, in Proceedings. IEEE Technical postgraduates International conferernce,2000.

[13]"A survey of security issues in mobile ad hoc and sensor networks", Badache.N, Khelladi.L, D.Djenouri, in Proceedings. IEEE Communications Surveys and Tutorials Journal, pp 2-29, (December 2005).

[14] "Routing security in wireless ad hoc networks", W., Agrawal, H.,Li. Deng, In Proceedings IEEE Communications Magazine 40.pp . 70-75, (October 2002).

AUTHORS

S.Vasudevi received B.E. (CSE) degree in 2013 from Anna University and pursuing M.E (CSE) in Dr.Sivanthi Aditanar College of Engineering, Tiruchendur. Her area of interest is Networking. She is affiliated to student member in Computer Society of India (CSI).

D.Mary Ponrani received B.E. (CSE) degree and M.E. (CSE) degree from Anna University. She is the Assistant Professor of Computer science and engineering department in Dr.Sivanthi Aditanar College of Engineering,Tiruchendur. Her Area of interest is networking.