Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Performance Comparison of on Demand Routing Protocols under Black Hole for MANET

Akshayadevi Arivazhagan
Master of Technology
Department of ECE
Periyar Maniammai University
Thanjavur, Tamilnadu, India

K. Thamizhmaran
Assistant Professor/ECE
Dept.of Electrical Engineering
Annamalai University
Chidambaram, Tamilnadu, India

N. Thamilselvi
Assistant Professor
Department of ECE
Periyar Maniammai University
Thanjavur, Tamilnadu, India

Abstract: ***MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network in contrast to a mesh network has a central controller. The solutions may not always be sufficient, as ad-hoc networks have their own vulnerabilities that cannot be addressed by these solutions. In the network, some malicious nodes pretend to be intermediate nodes of a route to some given destinations, drop any packet that subsequently goes through it, is one of the major types of attack. We propose a analysis method to detect malicious nodes in MANETs. The mechanism is cooperative hence the protocol work cooperatively together so that they can analyze, detect malicious nodes in a reliable manner. We verify our method by running simulations with mobile nodes using Ad-hoc on-demand Distance Vector (AODV) routing comparison with Dynamic Source Routing (DSR). It is observed that the malicious node detection rate is very good; the overhead detection rate is low, packet delivery ratio is little bit high and also the response time is observed when there is a change of mobility speed.***

Keywords: MANET, Black hole, AODV, DSR

I. INTRODUCTION

A mobile ad hoc network (MANET) is a self configuring network of mobile nodes. It lacks any fixed infrastructure like access points or base stations. It lacks centralized administration and is connected by wireless links or cables [4]. Wireless ad hoc network can be build up where there is no support of wireless access or wired backbone is not feasible. Black hole problem in MANETS is a serious security problem to be solved. In this problem, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept [11]. In flooding based protocol, if the malicious reply reaches the requesting node before the reply from the actual node, a forged route has been created. This malicious node then can choose whether to drop the packets to perform a denial-of-service attack or to use its place on the route as the first step in a man-in-the-middle attack [5]. Hence the performance compares the increase in malicious nodes.

II. ATTACK

The threats on a MANET can be from the unauthorized nodes those are outside the network or from the nodes inside the network. Threats from the nodes outside of the network are likely to be more easily detected than the internal nodes of the network [10]. Threats on the MANET can be broadly divided into 2 categories such as (i) external threats and (ii) internal threats.

A. Black Hole Attack

A node which is a black hole has two properties – it participates in the route discovery process and the second property is that, it sometimes does not forward the data packet towards the destination [3].

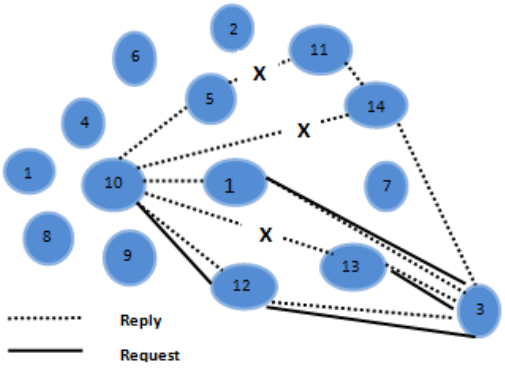

Fig.1. Black hole attack

When the data packets are forwarded to the destination these selfish nodes simply do not forward the data packets towards the destination. Hence, these nodes act as a black hole which causes data packet dropping. Here the Black-Hole node separates the network into two parts [3]. Few strategies to mitigate the problem: (i) collecting multiple RREP messages (from more than two nodes) and thus hoping multiple redundant paths to the destination node and then buffering the packets until a safe route is found. (ii) Maintaining a table in each node with previous sequence number in increasing order.

The sender node broadcasts RREQ to its neighbors and once this RREQ reaches the destination, it replies with a RREP with last packet sequence number. If the intermediate node finds that RREP contains a wrong sequence number, it understands that somewhere something went wrong [11].

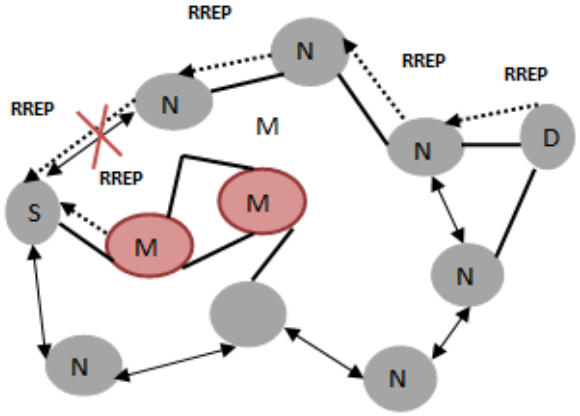

Fig.2. Co-Operative Black hole Attack

III. PROPOSED SOLUTION

To detect the malicious node we have proposed two methods which use a reactive routing protocol known as Ad hoc On-demand Distance Vector (AODV) and DSR routing for analysis of the effect of the black hole attack when the destination sequence number is changed via simulation [8]. M1HNs after receiving the Further Detection message broadcast a RREQ message by setting destination address to source nodes address [7]. If it receives a RREP message from the malicious node, it sends a Test packet (TP) to the source node via malicious node, and at the same time it sends a Acknowledgment Packet (AP) to source node(SN) though some other route.

Step 1. SN broadcast RREQ along with the Dst_Seq
Step 2. For each IN receives the RREQ check
Step 3. For each node IN receives RREP Check
Step 4. After receiving the NM, SN broadcast a Further Detection message to all M1HNs
Step 5. For each M1HN receive further detection message
Step 6. SN waits for „wt" time
Step 7. If all the flags are „N",
Step 8. End

IV. 4. ILLUSTRATION

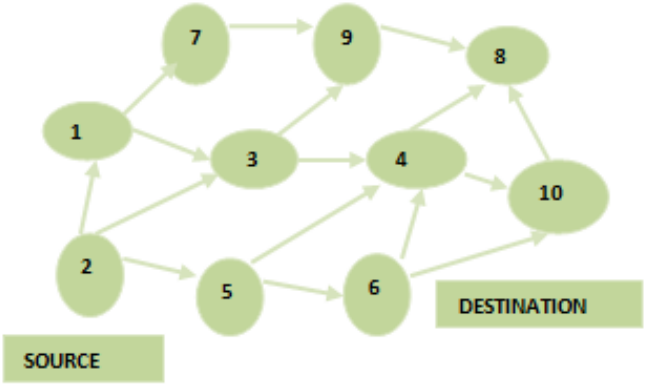

Fig.3. A MANET of 10 nodes

As in Fig 3, source is node 1 and the destination is node 10.If we consider node 6, first it will find out the nodes which are within its radio range and store in its N-List. According to Fig.1 neighbor list of node 6 are 3, 4, 5, 8 and9.Then node 6 sends the RREQ to all its neighbor nodes Each neighbor node that receives the broadcast checks the destination to see if it is the intended recipient [5]. If yes it sends a RREP message back to the node 6. RREP message contains the current sequence number of the destination node. At the same time node 3, 4, 5, 8, 9 maintain the sequence number in the SnT and sequence numbers are generated randomly [12]

Table 3.1 Sequence Table(SnT)

Node ID	Dst_Seq
3	10
4	7
5	8
8	6
9	5

When an intermediate node receives a RREP checks if the difference between the Dst_Seq present in the RREP message and the sequence no present in its table is greater than some predefined threshold value. If so then the intermediate node stops forwarding the message and mark the node as M or malicious in the status table(ST) and send a notification message(NM) to source node along with the malicious nodes id and neighbor list of the malicious node.

A. AODV

AODV, like all reactive protocols, is that topology information is only transmitted by nodes on-demand.

RREQ - A route request message is transmitted by a node requiring a route to a node. As an optimization AODV uses an expanding ring technique when flooding these messages. Every RREQ carries a time to live (TTL) value that states for how many hops this message should be forwarded.

RREP - A route reply message is unicasted back to the originator of a RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address.

RERR - Nodes monitor the link status of next hops in active routes. When a link breakage in an active route is detected, a RERR message is used to notify other nodes of the loss of the link.

B. DSR

A source routing protocol must solve two challenges, which DSR terms Route Discovery and Route Maintenance. Route Discovery is the mechanism whereby a node S wishing to send a packet to a destination D obtains a source route to D[2]. When Route Maintenance indicates a source route is broken, S can attempt to use any other route it happens to know to D, or can invoke Route Discovery again to find a new route. The basic mechanism of forwarding Route Requests forwards the Request if the node (1) is not the target of the Request and (2) is not already listed. Also, the Time-to-Live field in the IP header of the packet carrying the Route Request may be used to limit the scope over which the Request will propagate.

V. RESULTS AND DISCUSSION

We conducted our experiments using NS-2 version 2.34, a scalable simulation environment for network systems. The routing protocol we use is AODV. Our simulated network consists of 100 mobile nodes placed randomly within a 1000 m x 1000 m area. All nodes have the same transmission range of 250 meters. The channel capacity is 2 Mbps. The random waypoint model was used in the simulation runs. In this model, a node selects a destination randomly within the roaming area and moves towards that destination at a predefined speed 10, 20, 30, 40 and 50m/s [8]. Once the node arrives at the destination, it pauses at the current position for 10 seconds. The node then selects another destination randomly and moves towards it, pausing there for 10seconds, and so on.

Each simulation executed for 70 seconds of simulation time. The traffic used is UDP/CBR traffic between random node pairs. The size of data payload is 512 bytes. Multiple runs with different seed numbers were conducted for each scenario and measurements were averaged over those runs. In our experiment we have assumed 5 percent of the number of nodes as malicious i.e. 3 nodes are malicious for 50 nodes, 5 nodes are malicious for 100 nodes and 7 nodes are malicious for 150 nodes. We study the detecting technique of the packet delivery ratio, overhead and response time for 50 node network, 100 node network and 150 node network. We run the simulation 5 times and all the data are plotted using MATLAB, averaged from the 5 runs.

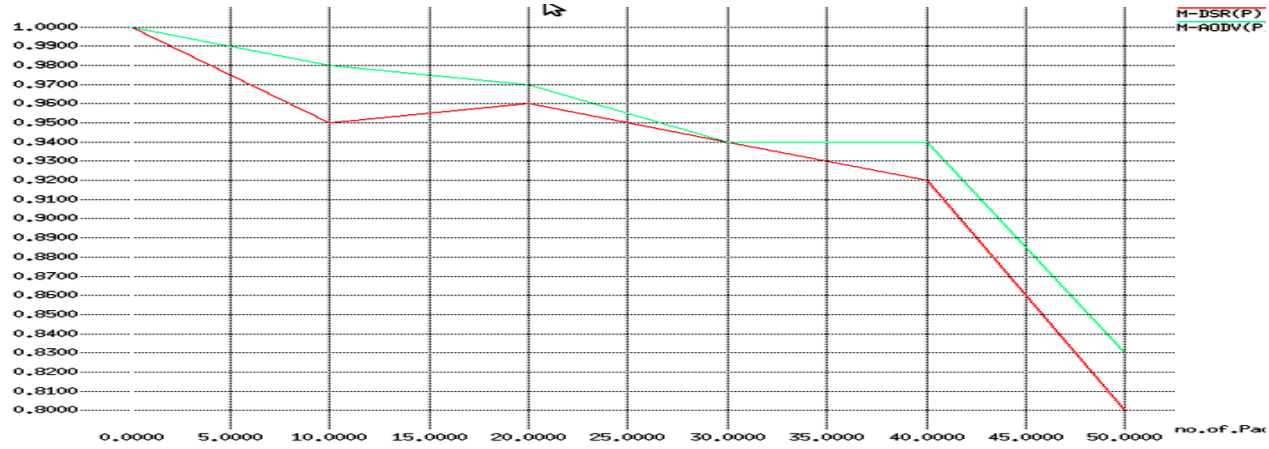

Fig.4 Comparison of Packet delivery ratio

The Fig 4 shows the packet delivery ratio for the network having 50 nodes, network having 100 nodes, network having 150 nodes respectively. The packet delivery ratio is shown as a function of mobility speed. As the number of nodes increases and malicious node increases, the packet delivery ratio decreases with the varying of mobility speed.

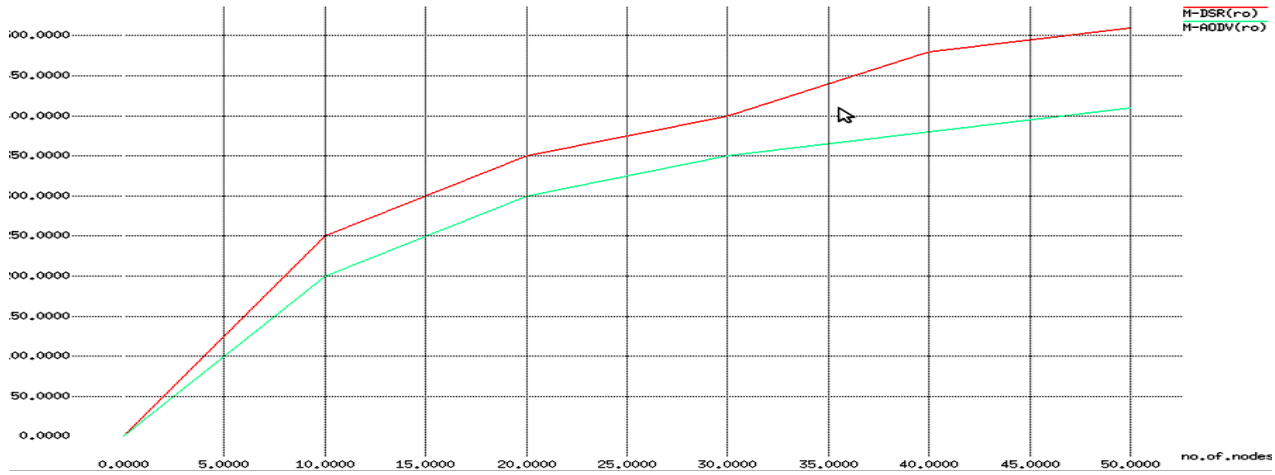

Fig.5 Comparison of Overhead

The Fig 5 shows the overhead for the network having 50 nodes, network having 100 nodes, network having 150 nodes respectively. The overhead is shown as a function of mobility speed. As the number of nodes increases and malicious node increases, the overhead increases with the varying of mobility speed.

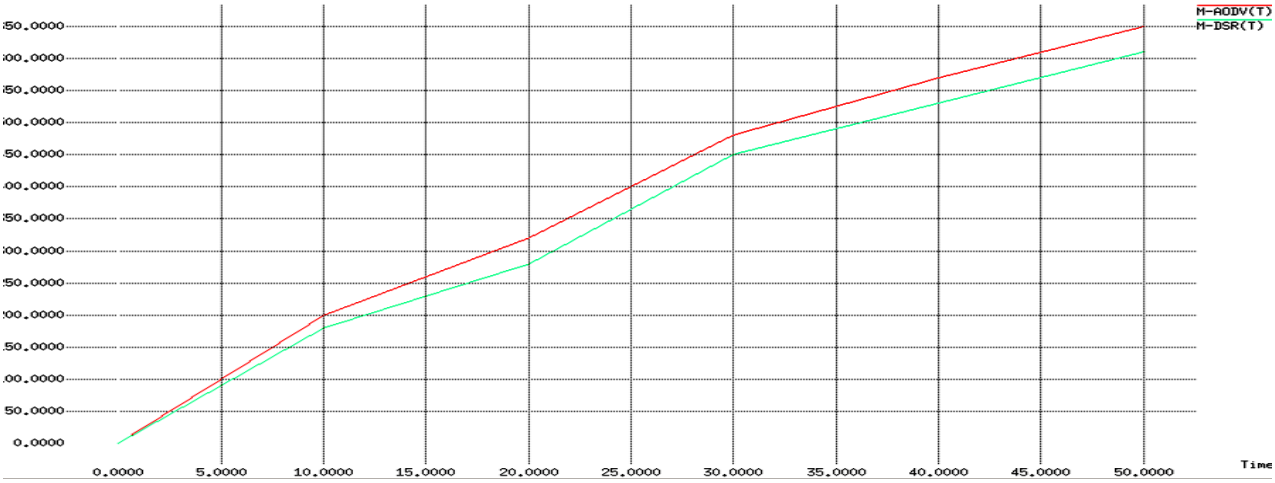

Fig.6 Comparison of Throughput

The Fig 6 shows the response time for the network having 50 nodes, network having 100 nodes, network having 150 nodes respectively. The response time is shown as a function of mobility speed. In our experiment we have taken the random way point model which changes the position of the node arbitrarily. So the response time changes arbitrarily when the number of nodes increases and malicious node increases.

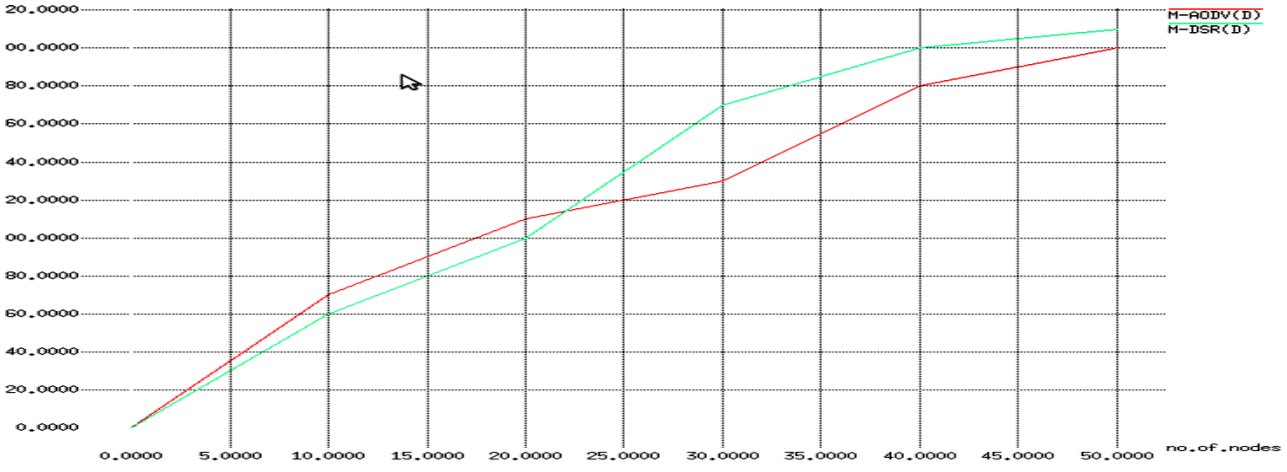

Fig.7 Comparison of Packet Drop

Fig 7 shows the packet drop ratio in two different scenarios i.e. for proposed model and the existing model TCLS. As the mobility speed increases, the packet drop ratio increases in both the cases. But from the graph it is cleared that the packet drop ratio for the mobility speed 10, 20, 30 m/s of the proposed model is improved as compared to TCLS whereas for the mobility speed 40 and 50 m/s, it is decreasing as compared to the existing one.

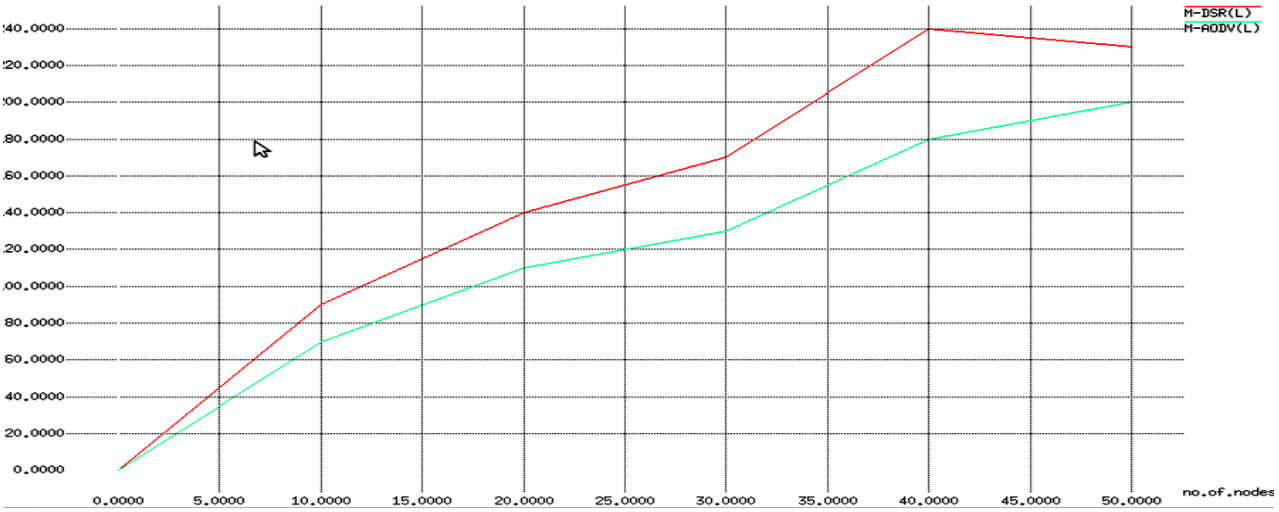

Fig.8 Comparison of End-To-End Delay

As the mobility speed increases, the end-to-end delay decreases in case of AODV. From the graph it is cleared that the delay of the proposed model is improved as compared to DSR.

VI. CONCLUSION AND FURTURE WORK

Black hole attack is one of the most important security problems in MANET. The black hole attack causes dropping of data packets by malicious nodes in the path source to destination. In this paper, we have analyzed the black hole attack and detected the malicious nodes. This paper is proposed to minimize the number of data packet dropping. Also it reduces false detection rate. This is a reliable algorithm since all mobile nodes cooperate together to analyze and detect possible multiple black hole nodes. The proposed scheme in this thesis work has been implemented to minimize the number of data packet dropping in the network and improves the efficiency of the network. In future work is to implement the hybrid network with minimum and higher throughput.

REFERENCE

[1] Suman Deswal and Sukhbir Singh," Implementation of Routing Security Aspects in AODV", International Journal of Computer Theory and Engineering. Vol. 2, No.1, February, 2010.

[2] Jongoh Choi, Si-Ho Cha, GunWoo Park, and JooSeok Song."Malicious Nodes Detection in AODV-Based Mobile Ad-Hoc Networks" GESTS Int‟l Trans.Computer Science and Engr., Vol.18, No.1 49, Oct.2005.

[3] Payal N Raj, Prashant B.Swadas, "DPRAODV: A Dynamic Learning System against Black hole Attack in AODV Based MANET", IJCSI International Journal of Computer Science Issues, Vol. 2, 2009.

[4] Akanksha Saini, Harish Kumar," Comparison between Various Blackhole Detection Techniques in MANET", NCCI 2010 –National Conference on Computational Instrumentation CSIO Chandigarh, INDIA,19-20 March 2010.

[5] K.Thamizhmaran,R.Santosh Kumar Mahto,V.Sanjesh Kumar Tripathi,"Performance analysis of secure routing Protocols in MANET"Vol. 1 Issue 9, pp 651-654, Nov 2012.

[6] N Bhalaji, Sinchan banerjee, A.Shanmugam, "A Novel Routing Technique against Packet Dropping Attack in Ad-hoc Networks", Journal of Computer Science 4 (7): 538-544, 2008.

[7] Ganesh Reddy, P.M. Khilar."Secure Routing in MANET", International Journal of Data Warehousing, Vol.2 No.1, Jun-2010, pp.53-62.

[8] S Rangrajan, et. al., "A Distributed System level Diagnosis Algorithm for Arbitrary Network Topologies, IEEE Trans. on comp. Vol 44, No. 2, February 1995,pp.312-334.

[9] Sunil kumar Senapati, Pabitra Mohan Khilar, "Securing FSR against data dropping by malicious nodes", International Journal of Computer Applications in Engineering, Technology and Sciences (IJ-CA-ETS), ISSN: 0974-3596, April‟09-September‟09.

[10] A Rajaram, Dr.S.Palaniswami." Detecting Malicious node in MANET Using Trust Based Cross-Layer Security Protocol" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1.(2), 2010.

[11] Aishwarya Sagar Anand Ukey, Meenu Chawla," Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET", IJCSI International Journal of Computer Science Issues, Vol.7, Issue 4, No. 1, July 2010.

[12] A. Patwardhan, J. Parker, A. Joshi, A. Karygiannis and M. Iorga. "Secure Routing and Intrusion Detection in Ad-Hoc Networks". Third IEEE International Conference on Pervasive Computing and Communications 2005.

[13] Karygiannis, A. and Antonakakis: A Mobile Ad Hoc Network Test Bed. 1st Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing in conjunction with the IEEE International Conference in Pervasive Services 2005, July 14, 2005.

Biography

AkshayaDevi Arivazhagan has Doing Master of technology, Dept of Electronics and Communication Engineering, Periyar Maniammai University, vallam, Thanjavur, Tamilnadu, India. Her interested area includes Mobile Communication and networking , Digital Signal Processing.

Prof. K. Thamizhmaran has received his B.E and M.E degree from Annamalai University, Chidambaram, Tamilnadu, India in the year of 2008 and 2012. He is currently pursuing his Ph.D in Annamalai University At Present working as an Assistant Professor in ECE / Department of Electrical Engg, FEAT, Annamalai University, Annamalai Nagar, Chidambaram, Tamilnadu., India. His Research interested includes Ad hoc Networks. He has published more that 10 technical papers at various National / International Conference and Journals. He is a life member of IAENG, IACSIT.

Prof. Thamil Selvi Nambiappan received her B.E degree in Electronics and Engineering from Regional Engineering College Tiruchirappalli, India in 1994. She completed her M.E in Computer and Communication from Periyar Maniammai College of Technology for Women affiliated to Anna University, Chennai in 2004. She is currently pursuing her PhD degree at the Periyar Maniammai University, Thanjavur, India. Her research interests include antenna design in ultra wideband frequency, mm and sub-mm microwave frequencies using metamaterials.

