New Scheme for Secured Routing in MANET

Sima [1] and Ashwani Kush[2]

[1]Department of Computer Engineering, Karnal institute of Tech & Mgt., Karnal
simasingh.2009@gmail.com
[2] Department of Computer Science, University College, Kurukshetra Univ. Kurukshetra
akush20.@gmail.com

ABSTRACT

Mobile ad hoc network (MANET) is an autonomous system of mobile nodes. Each node operates not only as an end system, but also as a router to forward packets. The nodes are free to move about and organize themselves into a network. These cause extra challenges on security. In this paper, evaluation of prominent on-demand routing protocol i.e. AODV,MAODV,RAODV has been done by varying the network size. An effort has been carried out to do the performance evaluation of these protocols using random way point model. The simulator used is NS 2.34. The performance of either protocol has been studied by using a self created network scenario with respect to pause time.

KEYWORDS

AODV, MAODV,RAODV,Evaluation, MobileNetwork Protocols, Wireless Network, Mobile Network, Virus, Worms &Trojon

1. INTRODUCTION

A Mobile ad hoc network is a group of wireless mobile computers (or nodes); in which nodes collaborate by forwarding packets for each other to allow them to communicate outside range of direct wireless transmission. Ad hoc networks require no centralized administration or fixed network infrastructure such as base stations or access points, and can be quickly and inexpensively set up as needed [7]. MANET is a kind of wireless ad-hoc network and it is a self-configuring network of mobile routers (and associated hosts) connected by wireless links – the union of which forms an arbitrary topology. The routers, the participating nodes act as router, are free to move randomly and manage themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet [1].

Mobile ad hoc networks present different threats due to their very different properties. These properties open up very different security risks from conventional wired networks, and each of them affects how security is provided and maintained. [13]In mobile ad hoc networks (MANETs), routing is a primary issue attracting large amounts of attention[14,15]. Early research efforts have yielded many well-known routing protocols such as AODV[16], DSR[8], TORA[18] which assume perfectly cooperative network.

AODV is an adhoc routing protocol. [4]. AODV routing protocol [2, 3, 11] is collectively based on DSDV [9] and DSR [8, 10]. AODV uses route expiry, dropping some packets when a route expires and a new route must be found [12].

2. PROPOSED PLAN

A New protocol has been proposed titled RAODV modifying MAODV [17] Protocol. In RAODV protocol malicious nodes are detected . Then using NS-2 simulator a comparative study of three protocols AODV , MAODV & RAODV has been carried out for 10, 25 and 50 nodes . The simulation has been performed using TCL scripts. The simulation results have been obtained with the help of three metrics as Packet delivery ratio, End To End Delay and Throughput. The results of AODV, MAODV & RAODV are represented in the form of Graph. Using these graphs AODV, MAODV & RAODV performance comparison have been made. To carry out the analysis a malicious node has been introduced in the script. This node when comes in direct communication contact with the routing nodes, results in hacker attack. This causes fall of packets. This performance has been studied using extensive simulations with varying scripts. The proposed scheme takes care of this node and the authors remove this node and generate a new path. This new path will be secured and will result in stable and secured routing.

3. ALGORITHM DESCRIPTION

In proposed algorithm there are three parts as Route Request, Route Reply & Data Transmission. Route request phase is started using Source and Destination nodes. At the time of route request it uses malicious and non malicious nodes. Nodes are verified one by one as ; if node status is True then this node enters in to the Non_Malicious array & if node status is False then this node enters in to the Malicious_array.

In Route reply it starts from 1 to TN(Total no of nodes). If status of node = TRUE All the possible routes will be searched by RREP. Then available route will be selected by the RREP broadcasting. It Repeat procedure until it reaches source node. Source node will select the path for data transmission based on the shortest path algorithm. In Data Transmission it starts from initial to final node, .if node id between S (Source Node) & D (Destination Node) then it set status of this node = TRUE otherwise it set status of this node = FALSE.

A. Algorithm Section 1 : Route Request Section

Step 1: Activate and Initialize the following variables

: hackers // Count Number of hackers.
: id //identification number for nodes
: hack_Node hackerNode[TN];
: Non_MaliciousNode[TN];
: TN // Total Nodes;

Step 2: At the time of Route Request verify Node Status
// Checking one by one node status
//=TRUE/FALSE with help of loop

Step 3: Initalize loop for detecting hacker Nodes
: Set i= 1; i<=TN; i++;
: if nodeST== “FALSE”
hacker++;
:hack_Node[i]=Node;
:else if nodeST== “TRUE”;
: Non_MaliciousNode[i]=Node;

B. Algorithm Section 2 : Route Replyt Section

Step 1: Destination Node rebroadcast the RREP like the RREQ

Step 2: Step 3: Initalize loop for Route Reply
(a) Set i= 1; i<=TN; i++;

(b) if NodeST=Non_MaliciousNode[i] .
All the possible routes will be searched by RREP.
(c) Then available route will be selected by the RREP broadcasting.
(d) Repeat steps c and d until it reaches to source node.

Step 3: Source node will select the path for data transmission based on the shortest path.

C. Algorithm Section 3 : Data Packet Transmission.

Step1: Set ST of each Node //STATUS
(a) Set S=SI //SI = Source ID
(b) Set D=DI //DI = Destination ID

Step 2: After receiving an overhearing message. node will compare the data packet send by it. with the identification value.
: For(i =1; i<=TN; i++)
: If (nodeID>= S && nodeID<=D)
nodeST[i]= "TRUE"

Step 3: if any node does not receives overhearing message or nodeid does not match then successor node is declared as malicious node by setting its
nodeST = "FALSE"

Step 4: After detecting malicious node an error message will be generate by the node and send it to the source node. Source node will declare it as a malicious node by making its ST = "FALSE" in the routing table and the present route will be deactivated.

4. SIMULATION ENVIRONMENT

The simulations were performed using Network Simulator 2 (Ns-2.34) [6], particularly popular in the ad hoc networking community. The source-destination pairs are spread randomly over the network .installed in Fedora Linux 12. The results have been derived by writing a tcl script and generating corresponding trace and nam files. TCP agents have been used to analyze the traffic. The mobility model used is random waypoint model in a square area. The area configurations used are 650 meter x 650 meter for 10 nodes, 750 meter x 750 meter for 35 and 1000 meter x 1000 meter for 50 nodes. The packet size is 512 bytes. The packets start from a random location with a random speed. Same scenario has been used for performance evaluation of all AODV, MAODV and RAODV protocols. Simulation parameters are shown in

Table-1: Simulation Parameters

Parameter	**Value**
Number of nodes	10,25,50
Pause Time	500,400,300,200,100
Environment Size	650*650,750*750 1000*1000
Traffic pattern	CBR (Constant Bit Rate)
Packet Size	512 bytes
Queue Length	50
Simulator	ns-2.34
Antenna Type	Omni directional

5. PERFORMANCE EVALUTION

RFC 2501 describes a number of quantitative metrics that can be used for evaluating the performance of a routing protocol for mobile wireless ad-hoc networks. Some of these quantitative metrics [5] are defined as follow:

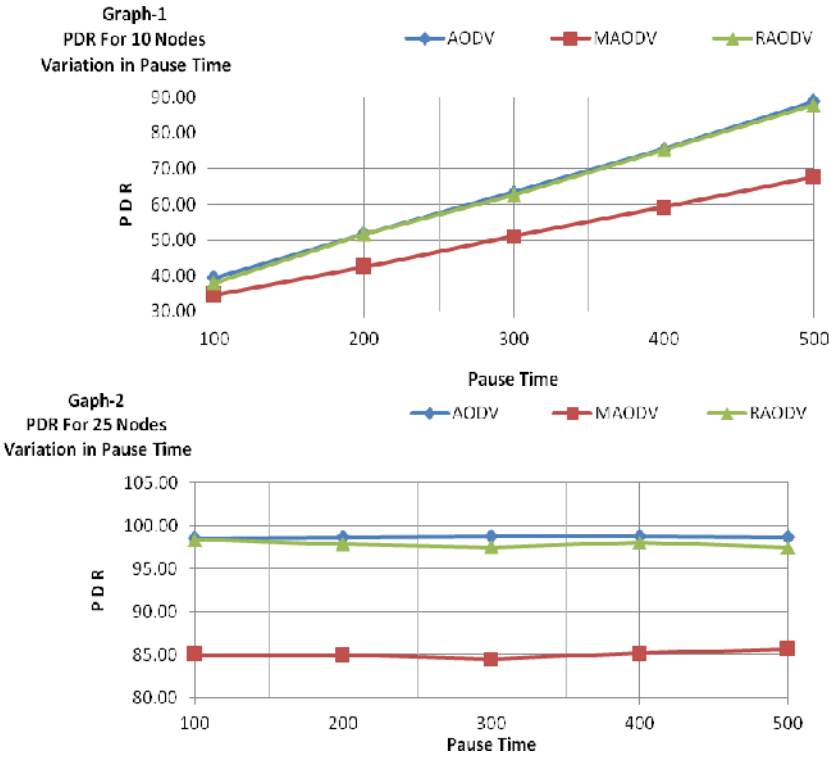
A. Packet Delivery Ratio:

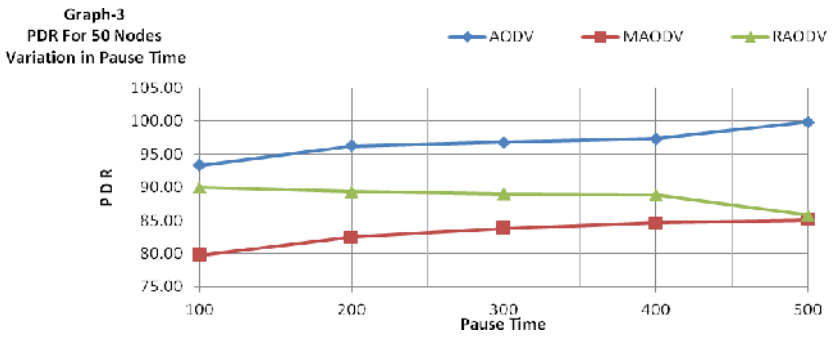
It is defined as the ratio of data packets received at the destination over the data packets sent by the source.

$$\text{Packet Delivery Fraction} = \frac{\textit{Total Data Packets received}}{\textit{Total Data Packets Sent}} \text{X100}$$

The performance of the protocols decreases as the pause time decreases & the performance of the protocols increases as the pause time increases.

Graph 1-3 shows PDR for 10,25,50 nodes. Performance for 10 nodes are shown in Graph-1. It shows that RAODV performs very well. But the difference in the performance of AODV & RAODV is too less because the no. of nodes are very less and also the no of hackers are less. Performance for 25 nodes have been shown in Graph-2. As predicted the PDR in case of malicious attacks decreases. As the pause time increases the performance of RAODV decreases. But still the performance of RAODV is much better then MAODV. Graph-3 shows the performance for 50 nodes but the performance difference of RAODV and MAODV is high as compare to Graph-2 . It shows that as the no of nodes are increasing hacker affect also increases.



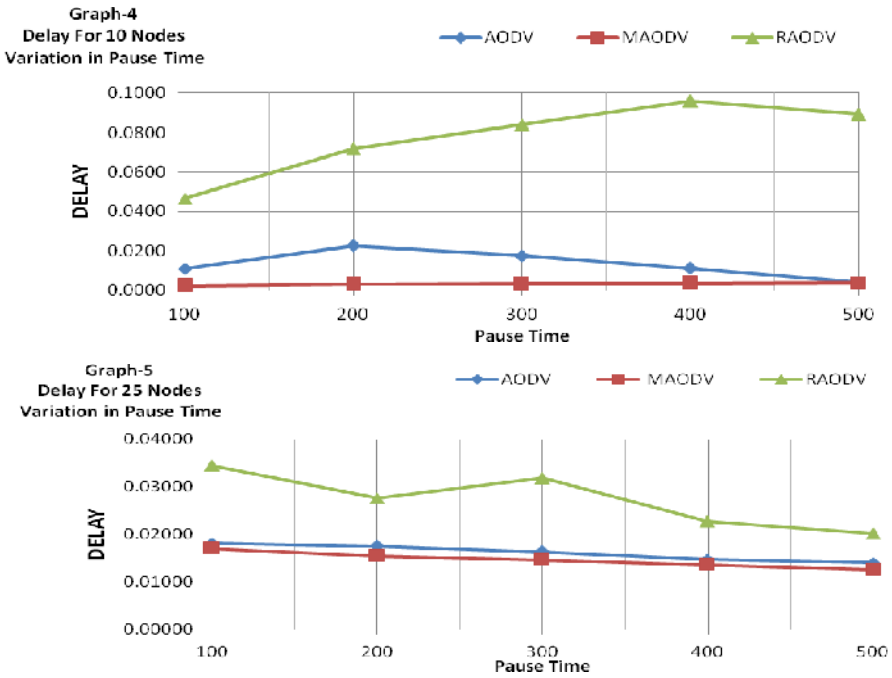


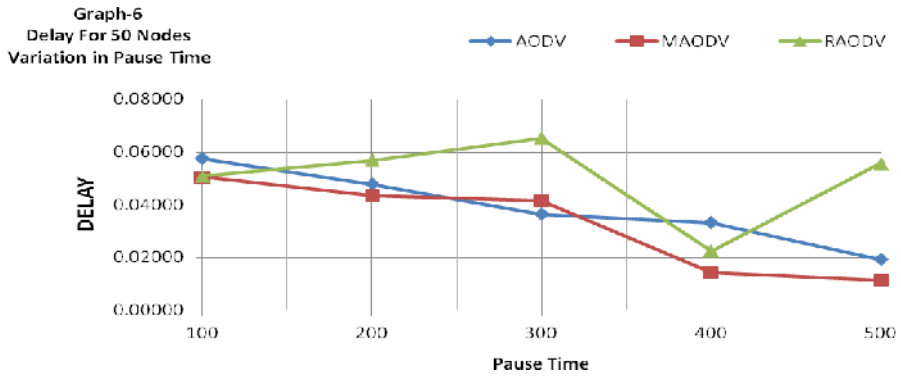
B. Average end to end data delay:

This is the average time involved in delivery of data packets from the source node to the destination node. To compute the average end-to-end delay, add every delay for each successful data packet delivery and divide that sum by the number of successfully received data packets.

$$\text{Packet Delivery Fraction} = \frac{\textit{Time Received} - \textit{Time Sent}}{\textit{Total Data Packets Received}}$$

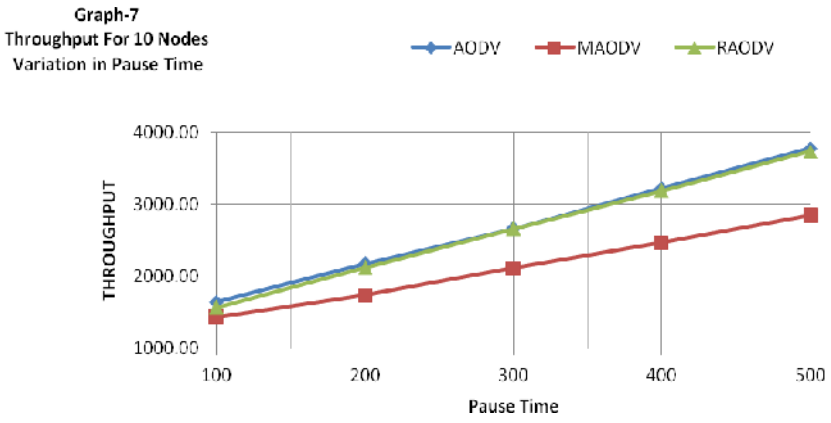
It can be seen that increasing in pause time results various changes in behavior of AODV ,MAODV & RAODV for end-to end delay . Graph 4-6 shows End To End Delay using 10,25,50 nodes. Performance of 10 nodes have been shown in Graph-4. It shows that the difference collapses as the pause time increasing same result for 25 nodes in Graph-5. But Graph-6 shows as no of nodes increases RAODV performances decreases.

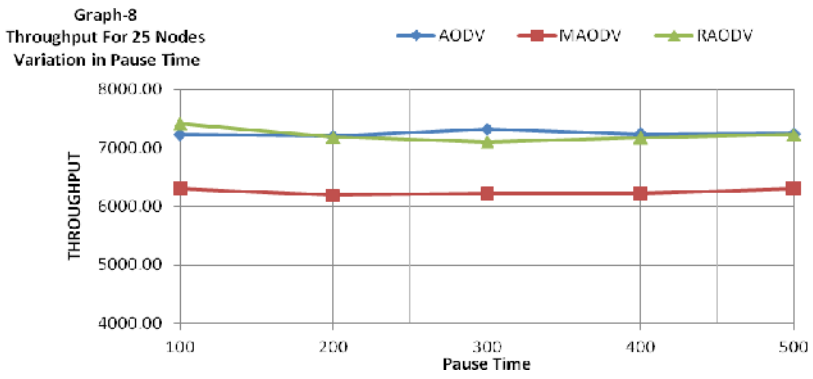




C. Throughput:

Graph 7-9 shows Throughput using 10, 25, 50 nodes. Performances for 10 nodes are shown in Graph-7. It shows that RAODV performs very well. Performance for 25 nodes has been shown in Graph-8. Still the difference is too less. But the performance of RAODV is much better then MAODV. Graph-9 shows the performance of 50 nodes but the performance difference of RAODV and MAODV is high as compare to Graph-8. It shows that as the no of nodes are increasing hacker affect also increases.





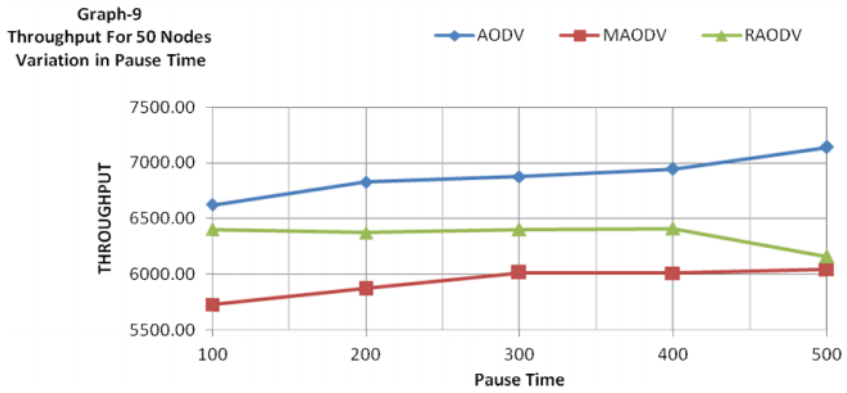


Figure 1. Spam traffic sample

6. CONCLUSIONS

In this paper, performance evaluation of AODV,MAODV & RAODV have been carried out using various metrics The results have been analyzed using a random way point self created network scenario. The general observation from various simulations show that the RAODV protocol performs better. In case of 10 nodes it detect almost all hackers as no of hackers are very less. As the no of nodes increases no of hackers also increases but RAODV protocol perform very well. It provides better security compared to other protocols like AODV. The proposed RAODV provides better security to data packets for sparse and significant security for denser medium. This study can be enhanced for 75 & 100 nodes. This will provide real life situations and provide a robust and effective solution for security. format.

REFERENCES

[1] S. Corson, J. Macker. Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. IETF RFC2501, 1999.

[2] Kush, A., Taneja, S.: A Survey of Routing Protocols in Mobile Adhoc Networks International Journal of Innovation, Management and Technology 1(3), 279–285 (2010)

[3] Perkins, C., Royer, E.B., Das, S.: Adhoc On-Demand Distance Vector (AODV). Routing IETF Internet Draft (2003)

[4] S.R. Das, R. Castaneda, J. Yan, and R. Sengupta. Comparative performance evaluation of. protocols for mobile, ad hoc networks. In 7th Int. Conf. on Computer Communications and Networks (IC3N), pages 153–161, October 1998.

[5] Kioumourtzis, G.: Simulation and Evaluation of Routing Protocols for Mobile Adhoc Networks. Thesis, Master of Science in Systems Engineering and Master of Science in Computer Science, Naval Postgraduate School, Monterey, California (2005)

[6] NS-2 Network simulator http://www.isi.edu/nsnam/ns.

[7] Geetha Jayakumar and Gopinath Ganapathy, —Performance Comparison of Mobile Ad-hoc Network Routing Protocol‖, International Journal of Computer Science and Network Security (IJCSNS), VOL.7 No.11, pp. 77-84 November 2007.

[8] D. B. Johnson and D. A. Maltz, “Dynamic Source Routing in Ad-Hoc Ad hoc Networks," Mobile Computing, ed. T. Imielinski and H. Korth, Kluwer Academic Publishers, 1996, pp. 153-181

[9] C. E. Perkins and P. Bhagwat, “Highly Dynamic Destination-Sequenced Distance-Vector. Routing (DSDV) for Mobile Computers,” SIGCOMM, London, UK, August 1994, pp. 234-244.

[10] E. M. Royer and C. Toh, “A Review of Current Routing Protocols for Ad Hoc Mobile. Wireless Networks,” IEEE Personal Communications, pp. 46–55, April 1999.

[11] C. Perkins, Ad hoc On demand Distance Vector (AODV) routing, IETF Internet draft (1997), http://www.ietf.org/internet-drafts/draftietf-manet-aodv-00.txt..

[12] Samir R. Das, Robert Castaneda and Jiangtao Yan, "Simulationbased performance evaluation of routing protocols for mobile ad hoc networks".
[13] http://www.ids.nic.in/tnl_jces_Jun_2011/PDF.
[14] Seyed Mehdi Moosavi, Marjan Kuchaki Rafsanjani, "An Algorithm for Cluster Maintenance Based on Membership Degree of Nodes for MANETs", "International Journal of Advancements in Computing Technology (IJACT)",AICIT, vol.3, no.4, pp.73-78, 2011.
[15] He XU, Suo-ping WANG, Ru-chuan WANG, "A Novel RFID Reader System Framework basedon Peer-to-Peer Network", "International Journal of Advancements in Computing Technology (IJACT)",AICIT, vol.3, no.3, pp.104-110, 2011.
[16] C. E. Perkins and E. M. Royer, "Ad hoc On-DemandDistance Vector Routing", In Proceedings of IEEE WMCSA, pp. 90-100, 1999.
[17] Sima ,A. Kush, "Malicious Node Detection in MANET" in Computer Engineering and Intelligent Systems ISSN 2222-1719 Vol 2, No.4,pp. 6-13, 2011
[18] Vincent D. Park and M.Scott Corson. A highly adaptive distributed routing algorithm for mobile wireless networks. In Proceedings of INFOCOM 1997, 1997

Authors

Sima is working as a Head and Assistant Professor in Department of Computer Science & Engineering, Karnal institute of Tech. & Mgt Kunjpura, Karnal. She is M.Tech from Ch. Devilal University Sirsa, Master of Science (Computer Science) from Mahrishi Dayanand University Rohtak. She has got published Six papers in National/International Conferences/Seminars. Her research interests are in Mobile Ad hoc Networks. Ms. Sima is currently carrying out PhD research work in association with Kurukshetra University.

Dr Ashwani Kush is a member of IAENG. He is working as Head and Associate Professor in Department of Computer Science & Applications, University College, Kurukshetra University, Kurukshetra. He has done PhD in computer science in association with Indian Institute of Technology, Kanpur, India and Kurukshetra University, Kurukshetra, India. He is professional Member of ACM, IEEE, SCRA, CSI INDIA and IACSIT Singapore. He has more than 60 research papers to his credit in various International/National Journals and Conferences. His 15 books has been published in computer science for undergraduate and school students. His research interests are in Mobile Ad hoc Networks, E-Governance and Security. Dr. Kush has chaired many sessions in International Conferences in USA and Singapore. He is member of Syllabus Committee, Time table and Quiz Contests of Kurukshetra University, Kurukshetra, India.