INTERNATIONAL JOURNAL OF ENHANCED RESEARCH IN MANAGEMENT & COMPUTER APPLICATIONS
VOL. 2 ISSUE 2, FEB.-2013 ISSN NO: 2319-7471

A New Solution for Security in MANET with the RAODV protocol

Najiya Sultana[1], S. S. Sarangdevot[2]
[1]Research Scholar, [2]Dean, Dept. of CS & IT
JRN Rajasthan Vidyapeeth University, Udaipur, India
saara.sultan@gmail.com

Abstract: Mobile Ad-hoc Networks are unplanned, self-organizing networks composed of mobile nodes that utilize mesh networking principles for interconnectivity. Routing in ad hoc networks is a very challenging issue due to nodes mobility, dynamic topology, frequent link breakage, limitation of nodes memory, battery, bandwidth, and processing power and lack of central point like base stations or servers. 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, Mobile Network Protocols.

1. INTRODUCTION

MANET technologies allow a force of mobile nodes to more easily share data and attain greater situational awareness than a non-networked force. Mobile ad hoc network has to face many challenges and issues. Routing in these networks is highly complex due to moving nodes and hence many protocols have been developed. Many small (in size only) computers operate for hours with battery power users are free to move about at their convenience without being constrained by wires. People have mobile computers for sharing information between the computers but now such sharing is made difficult by the need for users to perform administrative tasks and set up static, bidirectional links between their computers. 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] and TORA [18] which assume perfectly cooperative network. AODV is an adhoc routing protocol. [4]. AODV routing protocol [2, 3, and 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 SCHEME

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

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.

Algorithm Section: 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 node id 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. 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:

Packet Delivery Ratio

It is defined as the ratio of data packets received at the destination over the data packets sent by the source.
Packet Delivery Fraction = Total Data Packets received / Total Data Packets send X 100

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

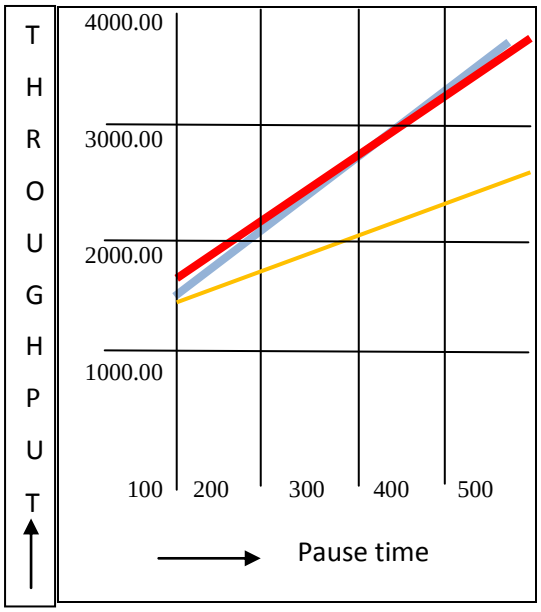
Average end to end data delay

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.

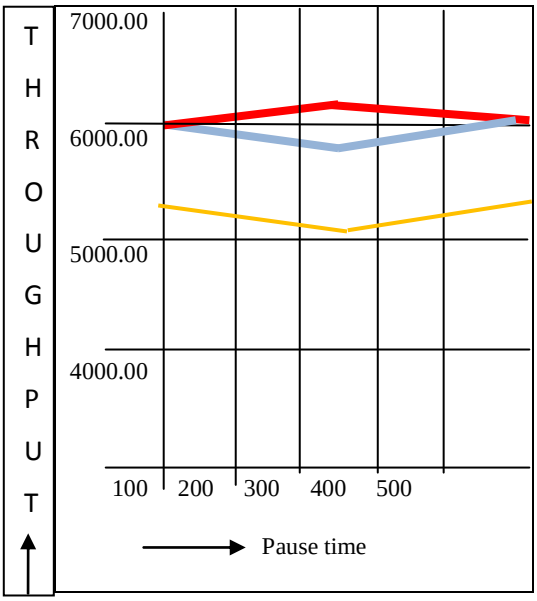
Packet Delivery Fraction = Time received — Time Send / Total Data Packets received Throughput:

Graph 1-3 shows Throughput using 10, 25, 50 nodes. Performances for 10 nodes are shown in Graph-1. It shows that RAODV performs very well. Performance for 25 nodes has been shown in Graph-2. Still the difference is too less. But the performance of RAODV is much better than MAODV. Graph-3 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.

Graph -1 Throughput for 10 nodes variation in pause time
(AODV, MAODV, RAODV)



Graph-2



Graph-3

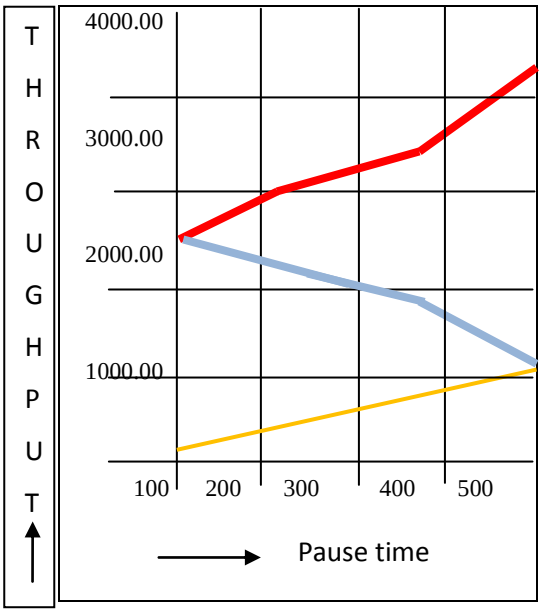


Figure 1: Spam traffic sample

5. CONCLUSIONS

The true challenges and the potential for the biggest risks to achieving the required MANET capabilities lie in the networking technologies. This approach can be utilized for the environment with less scalability and mobility. We think that it is a way to discover good operational values using other metrics such as control overhead, routing overhead with different mobility patterns.

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 shows 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.

REFERENCES

[1]. E. Royer and C. K. Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks", in IEEE Personal Communications, April 1999, pp.46–55.
[2]. E. Royer, Charles E. Perkins, "Evolution and future directions of the ad hoc on-demand distance- vector.
[3]. S. Corson, J. Macker., "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", IETF RFC2501, 1999.
[4]. 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).
[5]. Perkins, C., Royer, E.B., Das, S., "Adhoc On-Demand Distance Vector (AODV). Routing IETF Internet Draft (2003).
[6]. 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.
[7]. 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).
[8]. NS-2 Network simulator, http://www.isi.edu/nsnam/ns.
[9]. 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.
[10]. 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.
[11]. 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.
[12]. 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.
[13]. 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..
[14]. Samir R. Das, Robert Castaneda and Jiangtao Yan, "Simulationbased performance evaluation of routing protocols for mobile ad hoc networks".

VOL. 2 ISSUE 2, FEB.-2013 ISSN NO: 2319-7471

[15]. http://www.ids.nic.in/tnl_jces_Jun_2011/PDF.
[16]. 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.
[17]. He XU, Suo-ping WANG, Ru-chuan WANG, "A Novel RFID Reader System Framework based on Peer-to-Peer Network", "International Journal of Advancements in Computing Technology (IJACT)", AICIT, vol.3, no.3, pp.104-110, 2011.
[18]. C. E. Perkins and E. M. Royer, "Ad hoc On-Demand Distance Vector Routing", In Proceedings of IEEE WMCSA, pp. 90-100, 1999.
[19]. 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.
[20]. Vincent D. Park and M.Scott Corson, "A highly adaptive distributed routing algorithm for mobile wireless networks", In Proceedings of INFOCOM 1997, 1997.