International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 4 Issue 3 September 2013

A NOVEL SCHEME FOR SECURING MANETAGAINST MALICIOUS ATTACK

SIMA
Department of Computer Engineering, Karnal Institute of Tech. &Mgt,
Kunjpura, Karnal(Haryana), India

ASHWANI KUSH
Department of Computer Science, University College,
Kurukshetra University Kurukshetra, India

Mobile ad hoc networks have different properties as compare to traditional networks. These cause extra challenges and difficulties on security for ad hoc networks. In this paper, a new scheme to tackle security concerns in MANET has been suggested and it has been evaluated using metrics. Based on the performance evaluation, recommendations have been made about the significance of the protocol under various circumstances .The scheme has been compared with other existing schemes. The proposed scheme has been incorporated on ADOV as a case study.

Keywords: AODV; MAODV; RAODV; Evaluation; Mobile Network Protocols; Wireless Network.

1. Introduction

A wireless ad hoc network is a decentralized wireless network [18]. The network is ad hoc because without centralized administration or fixed infrastructure nodes can communicate. The network topology may vary rapidly and unpredictably, because of the mobility of nodes. These characteristic makes wireless ad hoc networks suitable for a variety of applications [7, 1]. Wireless ad hoc networks can be further classified based on their applications as:

- Mobile ad hoc networks (MANETs)
- Wireless mesh networks
- Wireless sensor networks.

For basic network functions like packet forwarding and routing, security is an essential component. These functions can be easily affected if countermeasures are not embedded at the early stages of their design. In mobile ad hoc networks (MANETs), secure routing is a primary issue [14, 15]. In this paper, an attempt has been made to provide secure routing for MANET. Early research efforts are based on many well-known routing protocols such as AODV [16, 4, 12], DSR [8], and TORA [13]. AODV routing protocol [2, 3, 11] is collectively based on DSDV [9] and DSR [8, 10]. Rest of the paper has been organized as follows. Section 2 contains description of proposed algorithm. Simulation Environment is given in Section 3 followed by description of performance comparison in Section 4. The paper concludes with Section 5.

2. Algorithm Description

ISSN (Online) : 2229-6166

Volume 4 Issue 3 September 2013

A New routing protocol has been proposed titled (Reverse Ad-hoc On demand Distance Vector) RAODV modifying (Malicious Ad-hoc On Demand Distance Vector) MAODV [17]. In MAODV protocol malicious nodes enters at random locations. RAODV detects these malicious nodes andremoves them. In the proposed scheme there are three phases as Route Request, Route Reply and Data Transmission.

Route request is almost same as that of AODV. It starts with request to search shortest path. Two arrays are used in this phase, first for malicious nodes and second for non malicious nodes. At the time of route request nodes are verified one by one for checking nodes status. If node status is „TRUE‟ then this node enters in to the Non_Malicious array and if node status is „FALSE‟ then this node enters in to the Malicious_array.

In Route Reply phase it checks the status of nodes whether they belongs to malicious or non malicious array. All the possible routes will be searched by RREP from non malicious array. Then available route will be selected by the RREP for broadcasting. It repeats procedure until it reaches to source node. Source node will select the path for data transmission based on the shortest path algorithm.

Data Transmission starts from source to destination node.

It is expected that RAODV will increase packet delivery ratio as compared to MAODV. Though the performance may be still poor as compared to (Ad-hoc On Demand Distance Vector) AODV. The reason to this is attributed to functioning of RAODV because RAODV detect and removes malicious nodes one by one.

3. Simulation Environment

A comparative study of three protocols AODV, MODV and RAODV have been carried out for 10, 25, 50 and 100 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. Results are represented in the form of Graphs. Using these Graphs performance comparisons have been made. To carry out the analysis malicious nodes have been introduced in the script. When these nodes used as routers for data transmission it results in hacker attack. This causes fall of packets. The proposed scheme takes care of these nodes and removes these nodes and generates a new path. This new path will be secured and will result in stable and secured routing.

The simulations have been performed using Network Simulator (NS-2.34) [6]. The traffic sources are CBR (continuous bit–rate). The source-destination pairs are spread randomly over the network. Operating System used is Fedora Linux 12. The results have been derived by writing TCL scripts and generating corresponding Trace and NAM files. The mobility model used is random waypoint model. The configuration area is 650 meter x 650 meter for 10 nodes and the packet size is 512 bytes. For 25

ISSN (Online) : 2229-6166

Volume 4 Issue 3 September 2013

nodes the area becomes 850 meter x 850 meter. For 50 nodes the configuration area increases up to 1 Km x 1 Km and this area increases 3 Km x 3 Km for 100 nodes. Packets start their journey from a random location to a random destination. Same scenario has been used for performance evaluation of all three protocols.

4. Performance Evaluation

Various quantitative metrics used for evaluating the performance of routing protocols in ad-hoc networks are [5]: Packet Delivery Ratio, End to end delay and throughput.

(I) Packet delivery ratio:

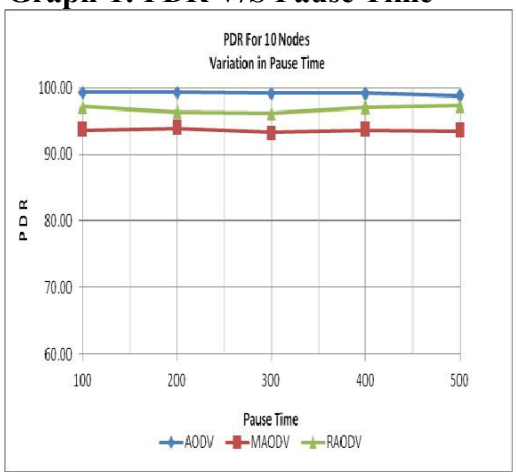
Graph 1-4 shows Packet Delivery Ratio for 10, 25, 50 and 100 nodes respectively. Gain in PDR in terms of percentage is approximately 4% for 10 nodes in the proposed scheme as compared to MAODV which has been shown in Graph 1. PDR Gain percentage approximately increases 6 to 10% for 25 nodes shown in Graph 2. Graph 3 shows gain in PDR as 8% for 50 nodes and gain in PDR is approximate 7% for 100 nodes shown in Graph 4. As the pause time increases the performance of RAODV decreases. But still the performance of RAODV is much better then MAODV. Less PDR is observed in the case of 50 &100 nodes. The reason is that only trusted packets are delivered. The fall in PDR is at the cost of security and which can be tolerable. It shows that as the numbers of nodes are increasing hacker affect also increases.

International Journal of Computing and Business Research (IJCBR)

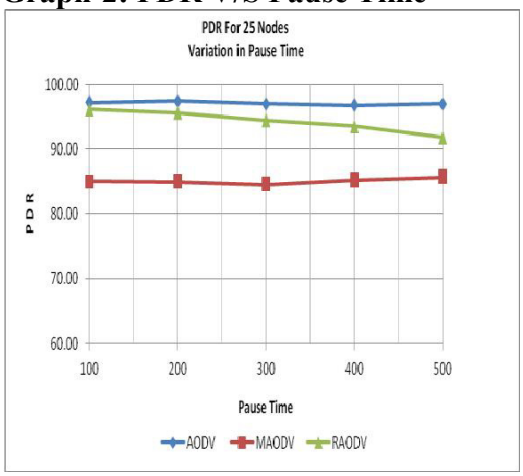
ISSN (Online) : 2229-6166

Volume 4 Issue 3 September 2013

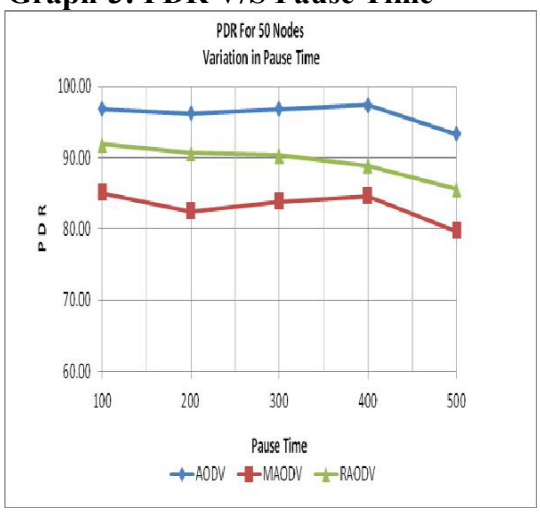
Graph-1: PDR V/S Pause Time



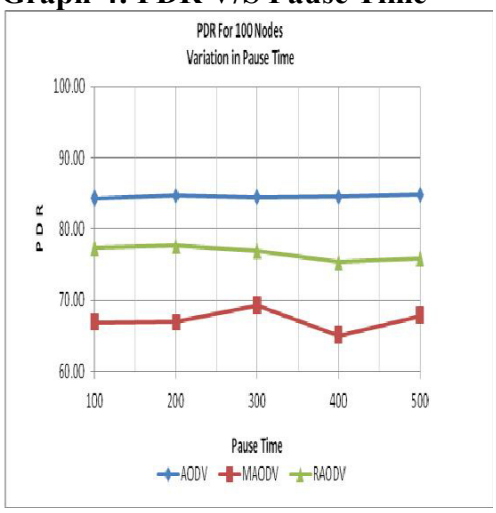
Graph-2: PDR V/S Pause Time



Graph-3: PDR V/S Pause Time



Graph-4: PDR V/S Pause Time

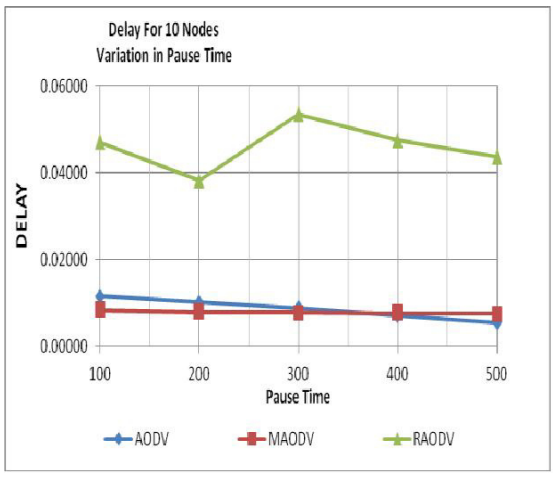


(II) End to end delay:

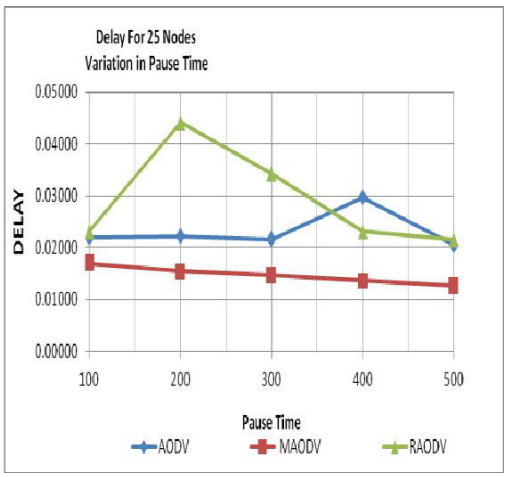
Average end-to-end delay is the delay calculated by the successfully delivered packets in reaching their destinations. This metric is used for comparing protocols and denotes how efficient the given routing protocol is. It can be seen that increasing in pause time results various changes in behaviour of AODV, MAODV and RAODV for this delay. Graph 5-8 represents the end to end delay for 10, 25, 50 and 100 nodes with respect to pause time. More end to end delay is observed in case of RAODV as compared to MAODV. This delay is because of more calculations involved

in initial route selection and route table updation. New scheme gives more stable and secured routes and it does cause more delays.

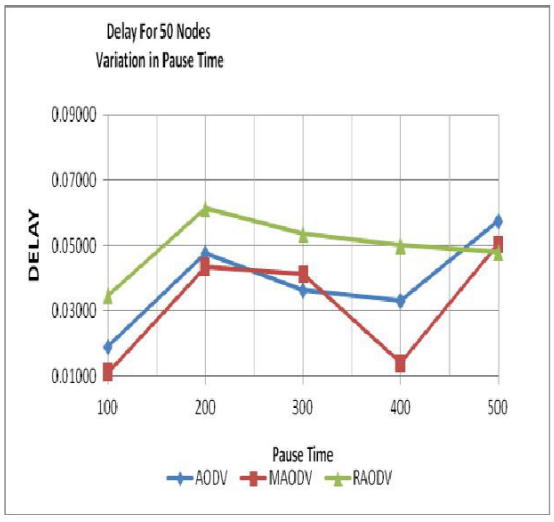
Graph-5: End to End Delay V/S Pause Time



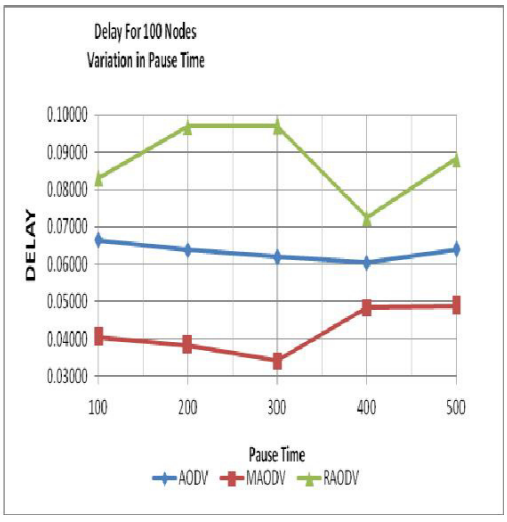
Graph-6: End to End Delay V/S Pause Time



Graph-7: End to End Delay V/S Pause Time



Graph-8: End to End Delay V/S Pause Time



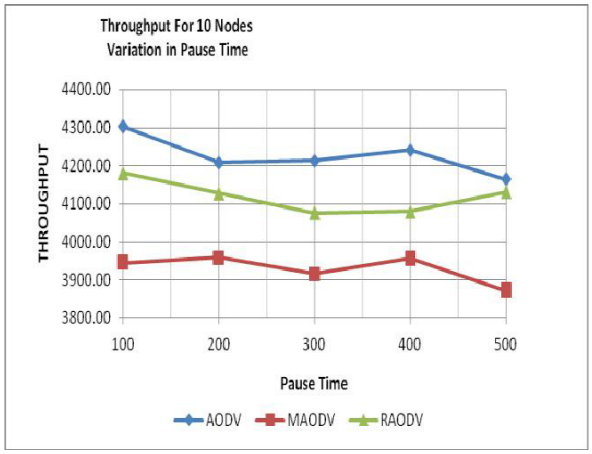
(III) Throughput:

Throughput (packets) shows numbers of packets in each time interval. Graph 9-12 shows Throughput using 10, 25, 50 and 100 nodes. Performances for 10 nodes are shown in Graph-9. It shows that RAODV performs very well as number of nodes are few the proposed scheme can easily detects malicious nodes. RAODV performance decreases in Graph 11 and 12 as compared to Graph 9 and 10 because RAODV detects and removes malicious nodes one by one.

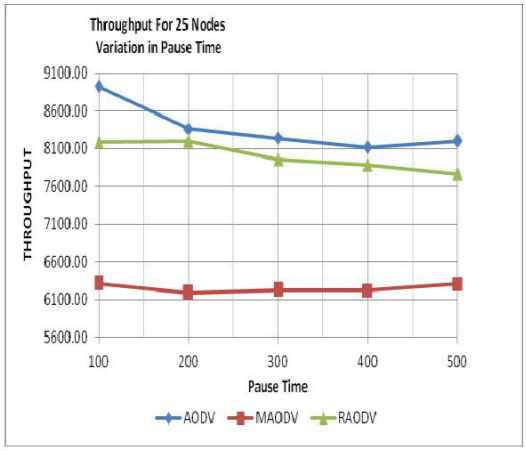
ISSN (Online) : 2229-6166

Volume 4 Issue 3 September 2013

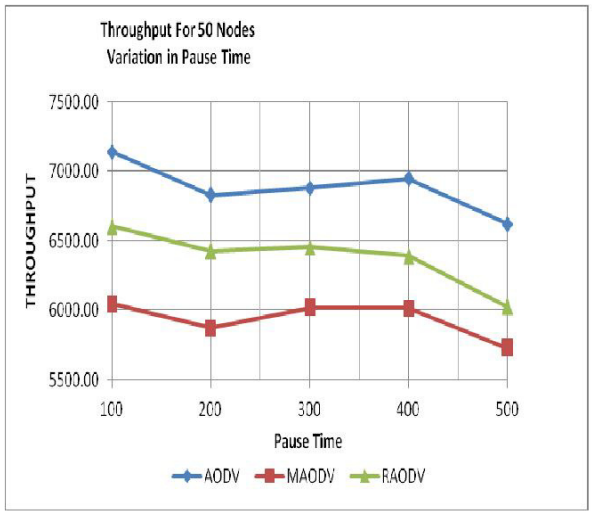
Graph-9: Throughput V/S Pause Time



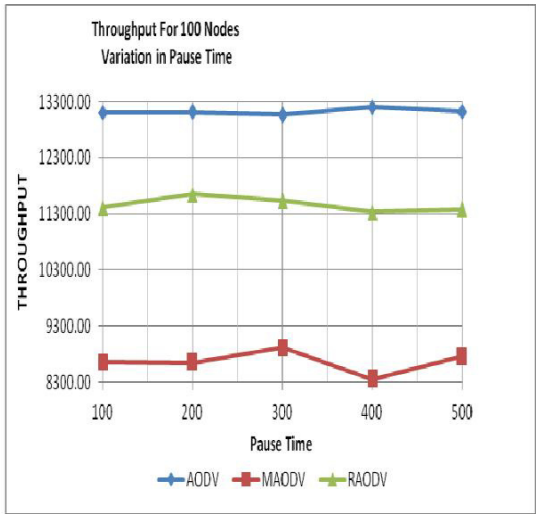
Graph-10: Throughput V/S Pause Time



Graph-11: Throughput V/S Pause Time



Graph-12: Throughput V/S Pause Time



5. Conclusion

In this paper, performance evaluation of RAODV has been carried out using various metrics and results have been compared with existing schemes like AODV and MAODV. The general observation from various simulations shows that the proposed scheme performs better for achieving security. In case of 10 nodes it detects almost all hackers as numbers of hackers are very less. As the number of nodes increases number of hackers also increases but RAODV protocol perform very well. It provides better security as compared to other protocols like MAODV. This study can be enhanced for

150 to 200 nodes. This will provide real life situations and provide a robust and effective solution for security.

References

[1] "Wireless Network Industry Report". http://www.wireless-nets.com/ resources /downloads/wireless_industry_report_2007. html

[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 andNetworks (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] Ram Ramanathan and Jason Redi "A brief overview of ad hoc networks:challenges and directions" www.ir.bbn.com/~ramanath/pdf/commmag-manets.pdf

[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-ector. 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] Vincent D. Park and M.Scott Corson. A highly adaptive distributed routing algorithm for mobile wireless networks. In Proceedings of INFOCOM 1997, 1997

[14] Seyed Mehdi Moosavi, MarjanKuchaki 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-Demand Distance 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] www.wikipedia.org.