Volume 6, Issue 7, July 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

New Scheme for Improving Security of TCP Connections in MANET

Dr. Sima

Department of Computer Science & Applications, DAV College for Girls Yamunanagar,
Haryana, India

***Abstract**—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

I. 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.

II. ALGORITHM DESCRIPTION

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 and removes 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.

III. 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.

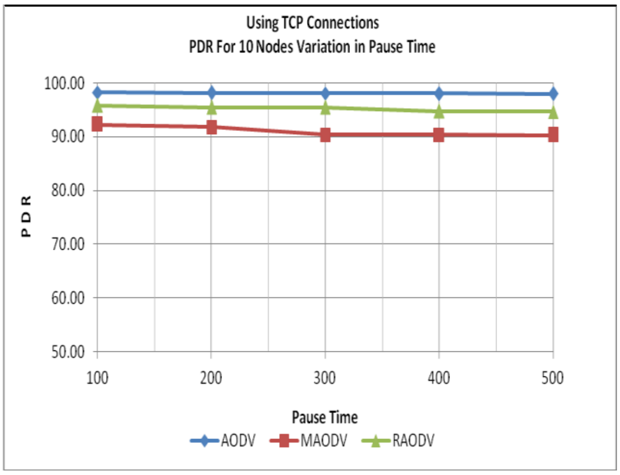
The simulations have been performed using Network Simulator (NS-2.34) [6]. The traffic sources are CBR (continuous bit–rate). The source-destination pairs are spread randomly over the network. Operating System used is Fedora Linux 12. The results have been derived by writing TCL scripts and generating 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 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.

IV. PERFORMANCE EVALUATION

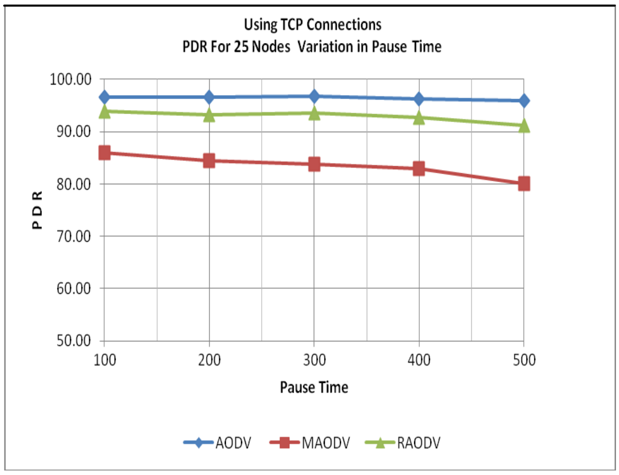
Various quantitative metrics used for evaluating the performance of routing protocols in ad-hoc networks are [5]: Packet Delivery Ratio, End to end delay and throughput. Transmission Control Protocol is the most commonly used protocol on the internet. TCP is a heavyweight protocol it takes more time for setup, in spite of it, it is preferred because it is

(I) Packet delivery ratio:

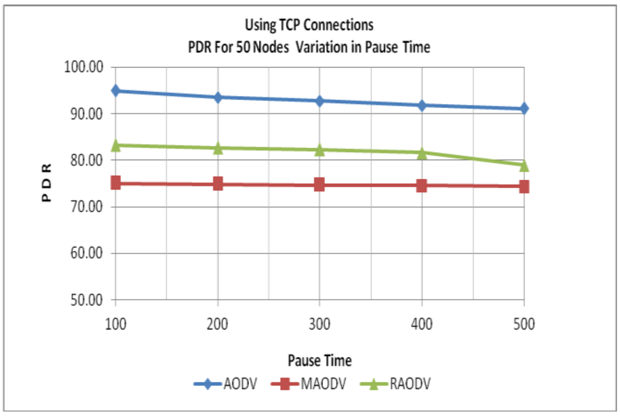
In Graph 1 TCP connections are used. In this simulation area chosen is 650 meter x 650 meter and number of nodes are 10. The number of sources connected via TCP connections are 5. Performance metric has been evaluated for AODV protocol, MAODV protocol and RAODV protocol using pause time as a parameter. Pause time selected from 100s to 500s and speed remains constant i.e. 5 meter/s. Where pause time 100 means maximum movement of nodes and 500 means least movement of nodes. The PDR values computed using received and dropped packets range from 98% to 97 % in AODV protocol. In MAODV some packets are dropped and range decreases approx to 90 %. RAODV improves PDR and touches 95% at start and 94 % in the end. In MAODV two malicious nodes have been introduced and this causes fall of packets. RAODV improves PDR by detecting and removing the malicious nodes. Graph 2 shows Packet Delivery Ratio for 25 nodes by using TCP connections. For simulation of 25 nodes 850m x 850m area is used. Pause time varies from 100 to 500s. Speed remains constant i.e. 3meter/s. For performing simulation, 8 connections are established among different moving nodes. The PDR values computed using received and dropped packets, range from 96% to 95 % in AODV. In MAODV four malicious nodes are introduced and this causes fall of packets. When simulation starts malicious nodes drops some packets and its PDR dropped and range from 83% to 75% and that’s why the performance of MAODV is low as compared to AODV performance. Proposed RAODV detects and removes these malicious nodes and improves the performance of MAODV and takes it from 83 % to 93 % in the start and 75% to 91 % in the end. When TCP connections are used, senders slow down or even stop their transmissions if it does not receive the acknowledgment from the destination. The performance comparison of AODV , MAODV and proposed RAODV has been shown in Graph 3 for measuring the PDR of 50 nodes. 1Km x 1Km area is used for performing the simulation. Speed remains constant i.e. 5 meter/s and pause time varies from 100s to 500s. Total 14 connections have been established among different moving nodes by using TCP traffic pattern. The PDR values computed using received and dropped packets, range from 95% to 91 % in AODV. In MAODV six malicious nodes have been introduced and this causes fall of packets. When simulation starts malicious nodes drops some packets and its PDR dropped and ranged from 75% to 74% and that’s why the performance of MAODV is low in comparison to AODV performance. Proposed RAODV detects and removes these malicious nodes and improves PDR. In RAODV the PDR range started from a peak of 83 % at start and then to 78 % in the end. Graph 4 shows Packet Delivery Ratio for 75 nodes vs pause time. In this Graph it can be seen very clearly as number of nodes increases the performance of all the protocols decreases. It has been analyzed from Graph 4 that PDR of proposed RAODV obtained by using UDP traffic is much better then the Packet Delivery Ratio of proposed RAODV obtained by TCP traffic. In other words it can be concluded that proposed protocol performs much better for UDP traffic than TCP traffic.



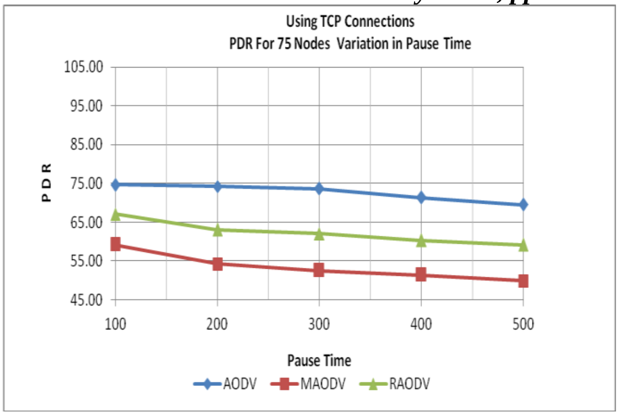
Graph 1



Graph 2



Graph 3

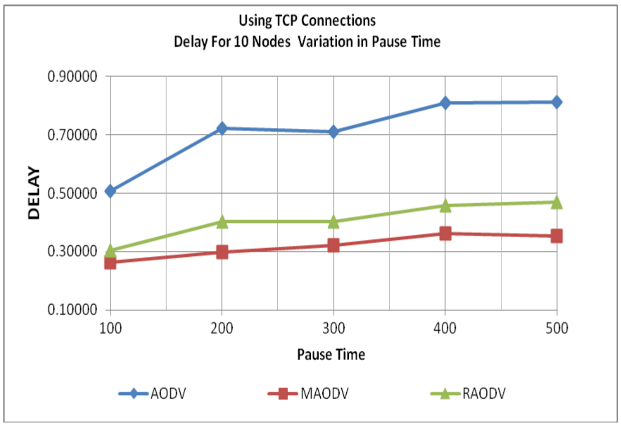


Graph 4

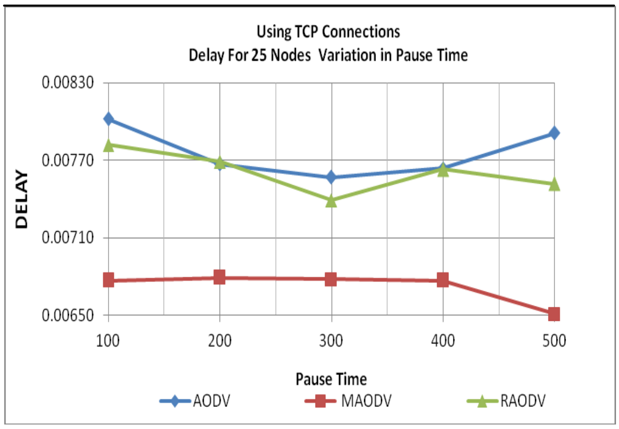
(II) End to end delay:

The behavior of different protocols with 10 nodes having TCP connections has been shown in Graph 5 and Graph 6. Area selected is 650 meter x 650 meter. Total 5 connections has been established among different moving nodes. In Graph 5 AODV starts with a high Delay and it increases as pause time increases. In this Graph MAODV Delay is less in comparison to other protocols. The reason beind this is that more packets are dropped in MAODV and they have not been counted in calculations. RAODV performance is better in comparison to AODV performance in this Graph. RAODV performance is close to MAODV performance. The reason is that number of nodes are only 10, so number of malicious nodes are also less, RAODV dectes and removes all malicious nodes earlier. This is the reason that RAODV performance is close to MAODV performance. Graph 6 shows Delay for 25 nodes varying in pause time and varying in speed respectively by using TCP connections. Area selected is 850 meter x 850 meter. Total 9 connections has been established among different movindg nodes.In Graph 7 AODV and RAODV Delay is very close. At the pause time of 200s AODV Delay and RAODV Delay is approximately same. This Graph shows as pause time between 100 to 300s AODV and RAODV Delay decreases. After 300s AODV Delay starts increaseing. RAODV Delay increases after 300s but after 400s RAODV Delay starts decreasing.

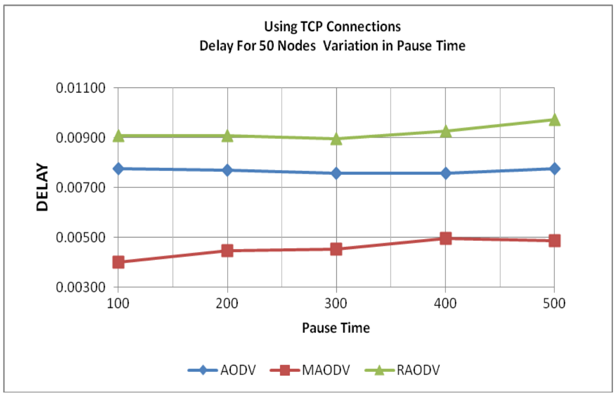
MAODV Delay is very low in this Graph and as pause time increases its Delay decreases. The reason is not because of better performance but it is due to the fact that more packets are dropped and they have not been counted in calculations. Graph 7 and Graph 8 shows End to End Delay for 75 nodes with respect to pause time and speed respectively. It has been found that MAODV has minimum Delay in both the Graphs. MAODV performance is very



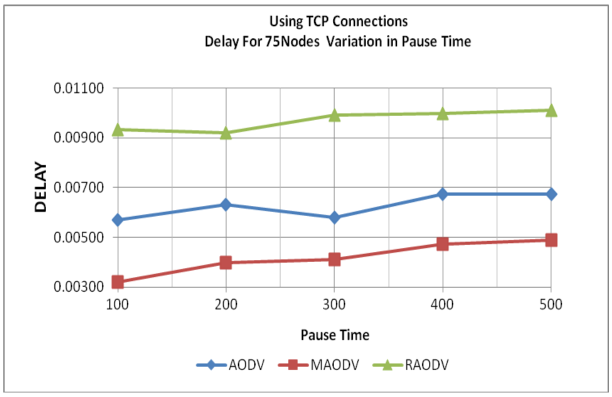
Graph 5



Graph 6



Graph 7



Graph 8

good at lower speed. AODV also performs well in both the Graphs. AODV has high Delay at higher speed. RAODV has higher Delay as compared to other counterparts. RAODV spends more time in selection of routes and this leads in higher Delay than others. This is due to calculation required for stable route based on security. RAODV has high Delay and MAODV has low Delay it doesn't mean that MAODV is better than RAODV. Proposed RAODV Delay is highest but it provide a stable and secure route, though MAODV Delay is lowest but MAODV is not secure.

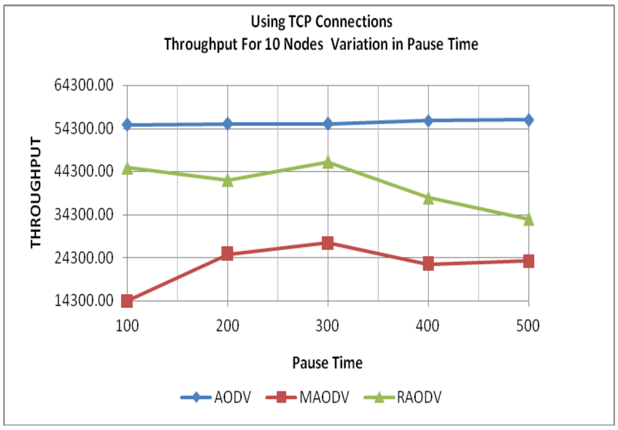
III) Throughput:

Figure 9 shows the Throughput performance for 10 nodes based on MANET's regular operation under collaborative malicious node attack and after detection and removal of malicious nodes. In Graph 9 AODV gives a high Throughput but as malicious nodes enters it starts drop the packets and MAODV Throughput goes down. As RAODV removes the malicious nodes its PDR improves. Same trend has been observed in case of 25 nodes.

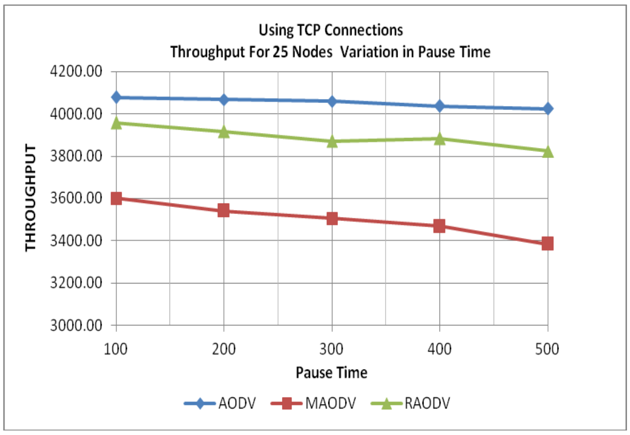
In Graph 10 AODV starts with a high Throughput in comparison to other protocol Throughput. Malicious nodes drop some packets and due to malicious nodes MAODV starts with a low Throughput and it decreases as pause time increases. RAODV provides a stable and secure path and improves the Throughput.

Throughput calculated for 50 nodes with 18 TCP connections have been shown in Graph 11 and Throughput calculated for 75 nodes with 23 TCP connections have been shown in Graph 12. It can be seen from all the Graphs that malicious nodes highly affect the performance of AODV and this causes fall of packets. AODV gives a high Throughput but as malicious nodes enters it starts dropping the packets and MAODV Throughput goes down. Then RAODV comes it detects and removes these malicious nodes as it removes MAODV deficiency and demerit in terms of removal of malicious nodes and thus supports the proposed plan. It can be seen that proposed RAODV Throughput improves a lot as compared to MAODV Throughput after the removal of malicious nodes.

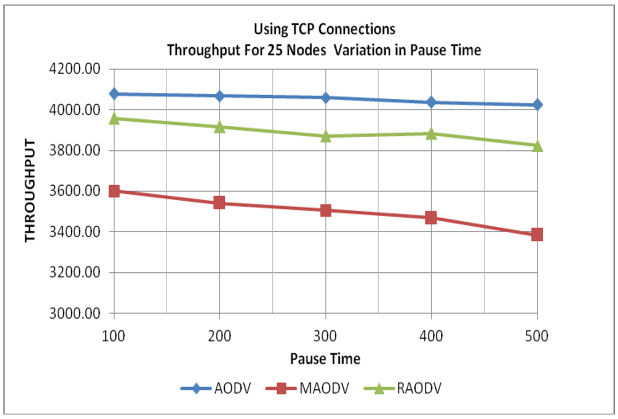
In general TCP results are poor as compared to UDP results because TCP source retransmits data. With increased mobility source may distribute several identical packets to different intermediate nodes, because of route changes. Retransmission thus makes a virtual multipath transmission. One of the packets reaches the destination, and the one which reaches the destination first is accepted. Thus, somehow, the mobility by cooperating with TCP, unwitting causes more reliable transmission. This does not apply to non TCP tests, because they have no chance of retransmitting data packets.



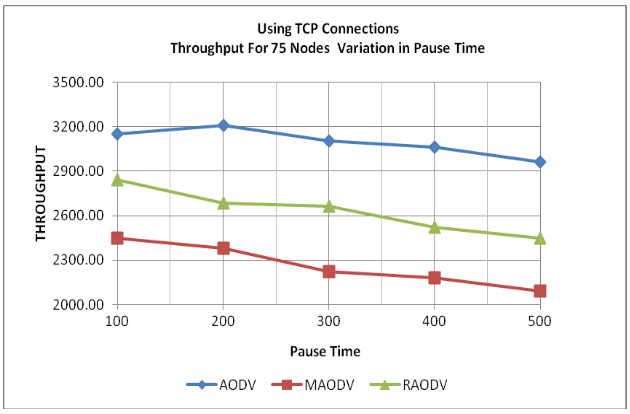
Graph 9



Graph 10



Graph 11



Graph 12

V. CONCLUSION

This paper presents a detailed comparative analysis of three MANET protocols i.e. AODV (Ad-hoc On-Demand Distance Vector), MAODV (Malicious Ad-hoc On-Demand Distance Vector), and proposed new scheme RAODV (Reverse Adhoc On-Demand Distance Vector) under TCP (Transmission Control Protocol). All the performances have been compared with the help of Packet Delivery Ratio, End to End Delay and Throughput. The discussion has been made to identify the merits and demerits of the proposed protocol. From the observations and results obtained from various simulations it can be concluded that modified scheme introduced here is effective for all cases. It identifies the attacker and keeps them away from the route for further communication. The proposed protocol was designed to provide better security with good PDR and high Throughput. Various Graphs show that proposed RAODV provides a stable and secure communication with a better performance. This study can be enhanced for150 to 200 nodes. This will provide real life situations and provide a robust and effective solution for security.

ACKNOWLEDGMENT

I would like to express my gratitude towards my husband and my son for the encouragement which help me in completion of this paper. I would like to express my special gratitude and thanks to my guide Dr. Ashwani Kush for imparting his knowledge and expertise in this study.

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.