The Impact of Packet Drop Attack and Solution on Overall Performance of AODV in Mobile Ad–hoc Networks

Ashok M. Kanthe, Dina Simunic, Ramjee Prasad

Abstract*— Mobile ad-hoc network has features like self organization, adaptation in changing environment, nodes in ad hoc network works as router for routing packets. Each nodes have limited resources like bandwidth, battery power and storage capacity. MANETs are vulnerable to Denial of Service (DoS) attacks like black hole attack, gray hole attack and packet drop attack. Packet drop attack is a kind of denial of service (DoS) attack in mobile ad hoc networks. Due to the bandwidth and memory buffer limitation, queue manager of some nodes by default may drop some packets. So differentiating between normal node to attacker node is critical one. In this paper, it is proposed the reputation and trust based mechanism against packet drop attack and improves the network performance interms of throughput, packet drop rate, packet delivery ratio, normalized routing overhead and end-to-end delay.

Index Terms*— AODV, mobile ad-hoc networks, protocol, packet drop attack, Security.

I. INTRODUCTION

Mobile ad hoc networks are self creating, self administering and self organizing for wireless communication.Each node having features like autonomous, limited battery power, dynamic topology and distributed multihop environment. Nodes to share or exchange the information between devices, they are interconnected to each other using some protocols working at different layers (E.g. Network layer, Transport layer). The medium of communication or channels may be unsecure and the transmitted data over the channel can fall into malicious activity. Wireless networks are less secure than wired network. They are created temporary as per requirement or application. Devices itself acts as router in MANET. Any device can join or leave network at any instance. Hence malicious devices can join the network at any time without any detection. Packets passing through malicious device can be captured.

Manuscript Received on December, 2012.

Ashok M. Kanthe, working Sinhagad Institute of Technology,Lonavala,Maharashtra.Currently he is pursuing his Ph.D.in Wireless Communication at University of Zagreb, Croatia, Faculty of Electrical Engineering and Computing in Zagreb.

Prof. Dr. Dina Simunic is a full professor at University of Zagreb, Faculty of Electrical Engineering and Computing in Zagreb.

Prof. Dr. Ramjee Prasad is the Director of the Center for TeleInfrastruktur (CTIF) and Professor Chair of Wireless Information Multimedia Communication at Aalborg University (AAU), Denmark.

Protocol design on all layers of the protocol stack is a technological challenge. At the network layer, each node should cooperate to calculate the paths. For routing packets in ad hoc networks, various routing algorithms or protocols are implemented like AODV, DSR. It is possible and feasible to detect malicious activity at routing level i.e. at network layer. The applications of MANET are, network established for emergency services, commercial and civilian environments, home and enterprise networking, education etc [1][2].

Ad hoc network are established in the absence of interconnection backbone. They are easily deployable and most users are migrating to mobile devices. Most of the research is going in the field of security. There are various types of attacks such as eavesdropping, wormhole attack, misdirection, flooding attack, packet drop attack, black hole attack, gray hole attack.

This paper presents the solution to packet drop attack and improves the performance of the network. The paper is organized like as follows section II discusses about related work on routing protocol security, section III discusses about AODV protocol, section IV discusses about packet drop attack, section V proposed mechanism against packet drop attack, section VI simulation and finally section VII concludes the paper and future work.

II. RELATED WORK

Sanzagiri [3] proposed Authenticated Routing for Ad-hoc Networks (ARAN) which is based on AODV protocol. It uses authentication and trusted certificate which is known to all legal nodes in MANET. Route discovery and route reply must sign for every node. It requires more time, size of the routing messages are increases for every hop and higher cost due to asymmetric cryptography.

Buchheger [4] proposed the CONFIDENT protocol which is a solution to identify misbehaving nodes in the MANET. This protocol is consisting the components which are 1) the monitor 2) the reputation system 3) the path manager and 4) trust manager. Here protocol uses global reputation value and alarm message to punish misbehaving node. This protocol is applicable for low mobility. This protocol is suitable only for small networks and not efficient for large networks. Each node is maintaining a large table for reputation. This protocol is having the overhearing problem.

Kejun Liu [5] proposed the two acknowledgement schemes for routing misbehavior and recovering their

effects. The received data packets are acknowledged in two acknowledgement schemes. Two packets have a route of two hops which is reverse direction of the data traffic. This paper is focusing on misbehaving links instead of nodes. This solution solved the overhearing problem. It is flexible to control overhead. This scheme is not suitable to other types of routing schemes and open networks.

Zhang [6] introduced RADAR a new solution for anomaly detection in wireless mesh networks. In this system reputation approach is used to observe the each node's behaviour. It generates the trust values of each node. Overhearing problem is solved in this technique.

Neelavathy [7] introduced a Novel Reputation Based Mechanism to Detect the Misbehaving nodes (NRMDM).It uses local reputation value. Each node maintains the reputation value of its k-hop neighbourhood.Reputation value is exchanged between the k-hop neighbourhoods. Objective of this paper is proposing a solution which monitors, detect and exclude the malicious node. This solution is not suitable for multiple routing for secure data transmission.

III. AODV Protocol

AODV is a reactive routing protocol in which routes are created only when they are needed [8] [9]. Hence AODV discovers the route from source to destination only on demand rather than table driven approach. It is not maintaining any partial network copy. It does not make sense to maintain due to mobility. AODV protocol has different processes like route discovery, route table management, route maintenance and local connectivity management. In route discovery process source node communicate to the destination node through intermediate nodes (routing nodes) if there is no direct connection between source and destination. Each node maintains routing table, having fields are destination (IP address or node ID), next hop (neighbour selected ID), number of hops (total hops to reach packet to destination), destination sequence number (highest sequence number),active neighbours in this route and expiration time for this route entry (time out or time to live for entry in table).

If there is no routing information available in the routing table of source node, route discovery starts by broadcasting route request (RREQ) packet to all the neighbouring nodes within range of source node/IN nodes, RREQ goes on propagating through intermediate nodes until valid path is not found. RREQ contains the fields are source IP addresses, source sequence number, broadcast identity, destination address, destination sequence number and hop count.

Sequence numbers ensure the freshness of routes and guarantee the loop-free routing. Sequence numbers are always incremented. They are incremented only when RREP packet is received and RREQ packet is sent.

The reverse path sets up when RREP packet is sent. Replying node (IN) generates the route reply (RREP) and sends it to source/intermediate (route requesting) node. Source may receive multiple RREP. But the valid, fresh and shortest is selected. Forward path is the reverse of reverse path setup .Actual data is routed through forward path. RREP packet fields are source address, destination address, destination sequence number, hop count and Life time.

In path maintenance, continuously hello messages are used to ensure that neighbours links are available hence it is local link management. Hello message does not change sequence numbers. If in the route intermediate node detects link failure the it generates RRER message and send it to source node hence source node , restarts route discovery process and finds the route.

IV. Packet Drop Attack

Black hole attack is kind of DoS attack where black hole node can attract all packets by pretending shortest route to the destination [10] [11]. It drops all traffic destined for that node when traffic is received by it. The effect of this attack completely degrades the performance of the network because the destination node never receives any information from the source. In packet drop attack nodes drop the packets, but it is not attracting the neighbouring nodes to drop the packets. Figure 1 shows the packet drop attack.

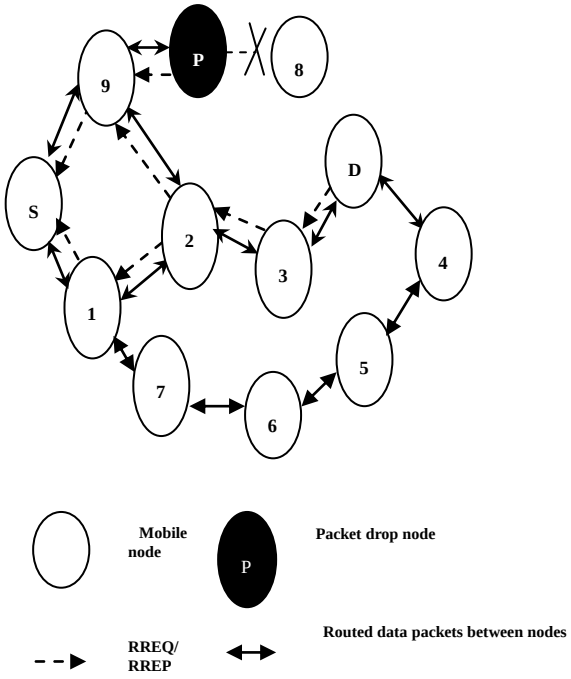

Figure 1: Packet drop attack

Packet drop Attack is Minor Attack

1. Packet droppers are the malicious node which do not forward the packet (or route the packet through it) they just drop the packets routing through them.
2. Packet drop attack is a less destructive in network compared to black hole attack and gray hole attack. In black hole attack, black holes intentionally attract the packets towards it and drop them to degrade overall performance of network. But packet dropping holes, drops only packets passing or routing through them. Packet drop attack is DoS attack whose intention is not to degrade the overall performance of network but its purpose may be.

a) To save battery power this is consumed in routing.
b) To introduce denial of service for specific nodes or specific routes.
c) To sniff a packet by eaves dropping.

Figure 2 and figure 3 shows packet drop rate vs. simulation time and packet delivery ratio vs. simulation time respectively. It shows the comparison of packet drop attack,

black hole attack and gray hole attack. Packet drop rate is less in packet drop attack as compared to black hole attack and gray hole attack. This is happen due to properties of packet drop attack. Simulation parameters are wireless channel, Omni antenna which propagates radio waves in all possible directions, two ray ground which is propagation model used (full duplex ,waves are propagated using ground reflection for far distances), link layer, packet size 512 bytes/packet, pause time 50 sec., speed 50 m/s, number of malicious node 1(packet drop attack) and protocol AODV.

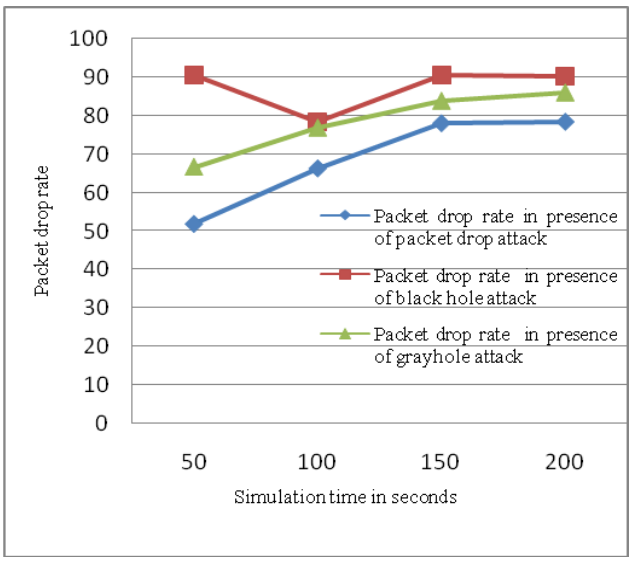

Figure 2. Packet drop rate vs. simulation time

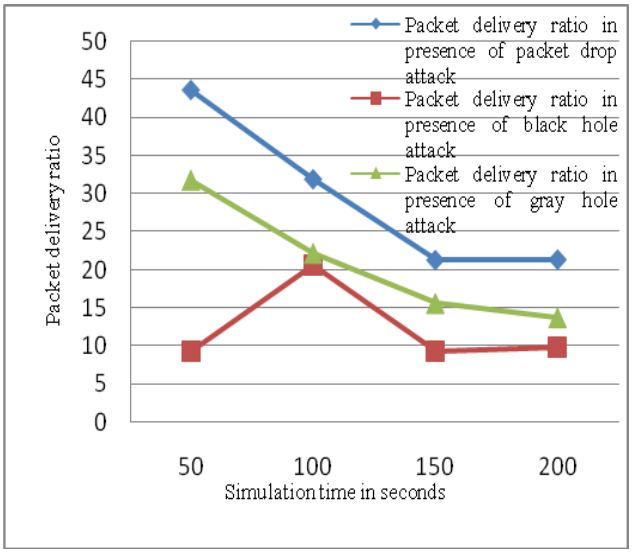

Figure 3.Packet delivery ratio vs. simulation time

V. Mechanism of Packet Drop Attack in Mobile Ad-hoc Networks

Proposed algorithm is to detect packet drop attack and improve the performance of the network. The concepts used in the proposed scheme.

A) Trust List: It is a list maintained on each and every node locally. The nodes which have passed the analysis are entered in the trust list. So in future if the reply comes from these trusted nodes the analysis overhead is skipped.

B) Direct Reputation: This mechanism proposed a direct reputation approach in which it is fetching the information like total sent packet by replying nodes and total dropped packets by replying node.

Description of the proposed work is

1. In this approach, introduced the trusted list instead black list. As the packet drop is minor attack as proved, to reduce re-analysis overhead analyzed node is added to trusted list. So it is skip that node's analysis in future. Hence it is reduce the calculation/analysis or detection overhead for already analyzed trusted list to some extent.
2. Trusted list is local to every node maintained as data structure in local RAM/buffer.
3. Direct reputation method using two counters are used. Total forwarded packets and total dropped packets of the replying nodes.
4. Flag named as reliable flag is setted (1) and resetted (0) as per conditions used in algorithm.
5. Reputation, reliable flag and presence/absence of route entry are the parameters used in algorithm to discard the packet from replying node.

A. Algorithm for detection against packet drop attack

Step 1. Start (for each node which receive RREP)
Step 2. Check if the replying node entry is present in routing table
rt = rtable.rt_lookup (rp→rp_dst)
if yes goto step 10
no goto step 3
Step 3. Check if replying node entry is present in trust list
If yes goto step 10
No goto step 4
Step 4. Reset the reliable flag
reliable = 0
Step 5. Check if replying node is final destination node
If yes do not add node to trust list and goto step 10
No goto step 10
Step 6. Check the DRI table that whether it had sent packet or related packet through replying node.
If yes set reliable =1
Step 7. Check if node has not routed packets through replying node but had received a packet from replying node.
If yes reset reliable = 0
Step 8. If (reliable == 0) and total number of forward packets of replying node are less
than total packets send.
Yes discard packet
goto step 11
No goto step 9
Step 9. Add the replying node into trust list
Step 10. Execute rest part of recvreply function
Step 11. Stop

B. Flowchart for proposed Approach:

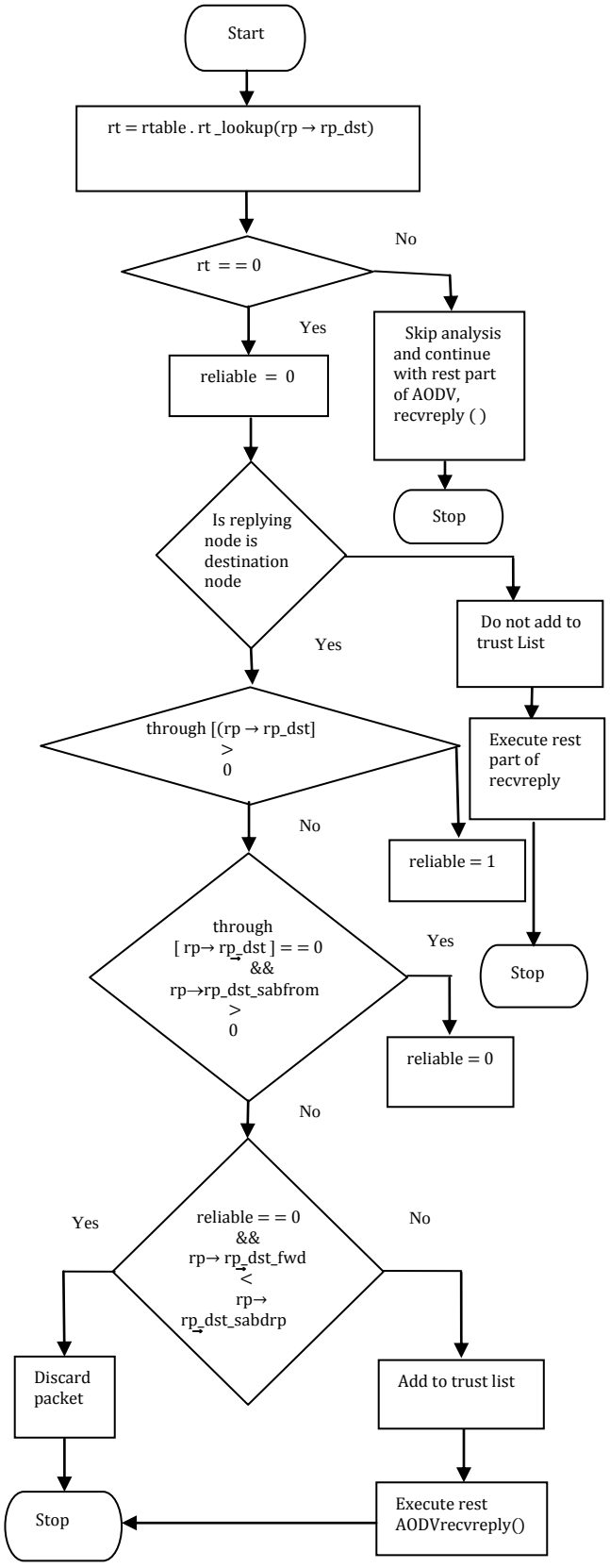

Figure 4.Flowchart for packet drop attack

VI. Experimental Setup

It is used simulation NS-2.35[12] having the simulation parameters shown in table I

A. Simulation environment

TABLE I. SIMULATION PARAMETERS

Parameter	Used in Simulation
Simulator	NS-2.35
DoS attack	Packet drop attack
Channel type	Channel/Wireless channel
Antenna type	Antenna/Omni Antenna
Radio propagation model	Propagation/Two Ray Ground
Link layer type	LL
Interface queue type	Queue/ Drop Tail / Pri Queue
Mac type	Mac/802_11
Protocols studied	AODV
Simulation time	100 sec.
Pause time	10-100 sec.
Simulation area	1500*1500
Trace format	New wireless format
Node movement model	Random waypoint
Traffic type	CBR(UDP)
CBR rate	50 Kbps
Data payload	512 Bytes/packet
Number of nodes	60
Sources	45
Number of Malicious Nodes	1
Speed	50 m/sec.

B. Metrics

The metrics used to evaluate the performance of the mobile ad hoc networks are given.

Throughput: It is defined as the amount of data transferred over the period of time expressed in kilobits per second (kbps).

Packet Drop Rate: It is the ratio of the data lost at destinations to those generated by the CBR sources. The packets are dropped when it is not able to find the valid route to deliver the packets.

Packet Delivery Ratio: It is the ratio of data delivered to the destination to the data sent out by source.

Normalized Routing Overhead: It is the ratio of routing transmissions to the data transmissions in the simulations. The routing transmissions are RREQ, RREP, RERR etc.

End to End Delay: The time taken for a packet to transmit across a network from source to destination .It includes all types of delays e.g. buffering route discovery, retransmission delays at MAC, queing at interface queue etc.

C. Results

Performance of the AODV protocol is measured by varying the parameters in simulation like mobility, number of sources and number of mobile nodes.

All the results are dependent on current position of nodes i.e. simulation scenario and may vary on next simulation because the packet drop attack is minor attack.

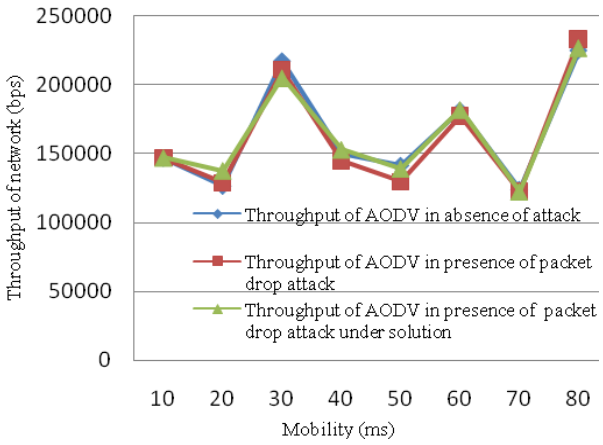

Figure 5. Throughput vs. mobility

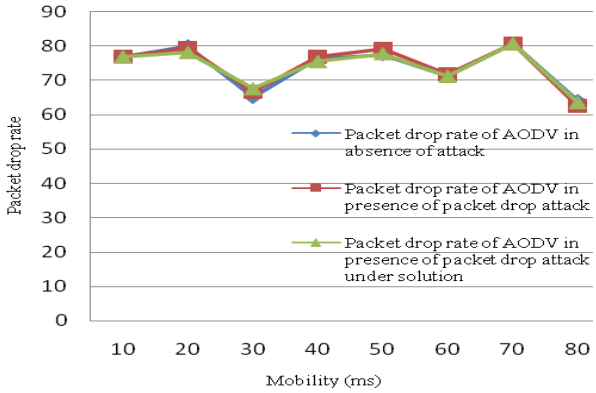

Figure 6. Packet drop rate vs. mobility

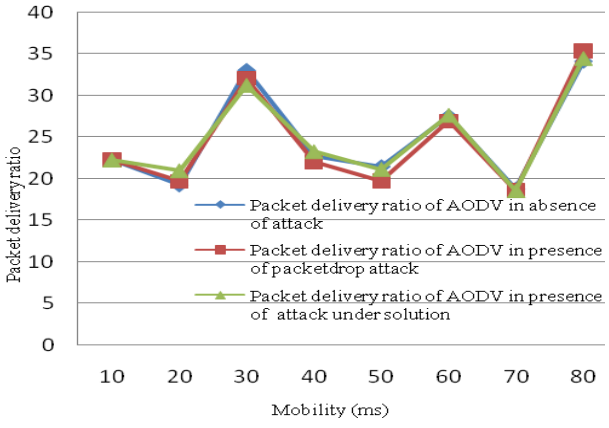

Figure 7. Packet delivery ratio vs. mobility

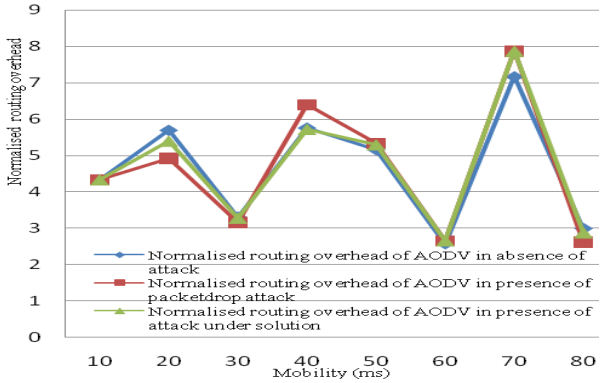

Figure 8. Normalized routing overhead vs. mobility

Figure 5, figure 6,figure 7 and figure 8 shows the graph throughput, packet drop rate, packet delivery ratio and normalized routing overhead vs. mobility.

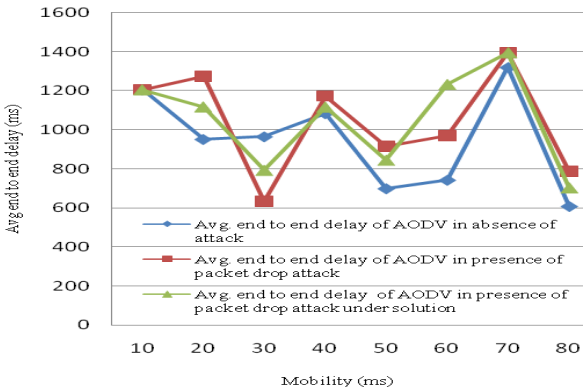

Figure 9. Average end-to-end delay vs. mobility

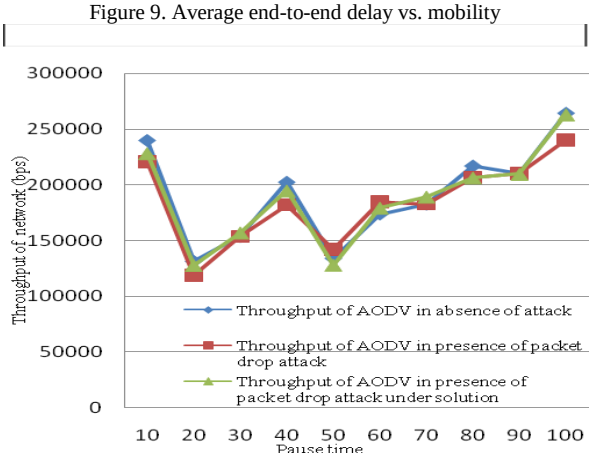

Figure 10. Throughput vs. pause time

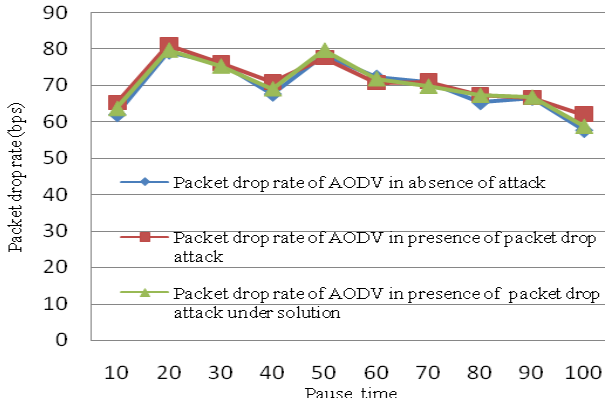

Figure 11.Packet drop rate vs. pause time

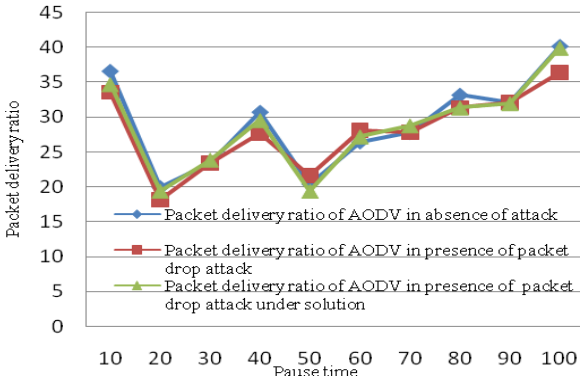

Figure 12.Packet delivery ratio vs.pause time

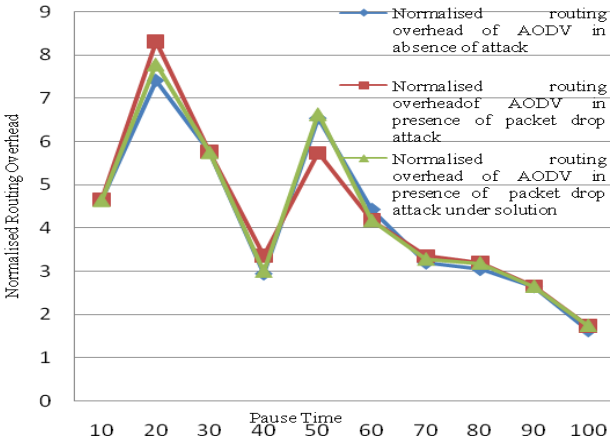

Figure 13. Normalised routing overhead vs. pause time

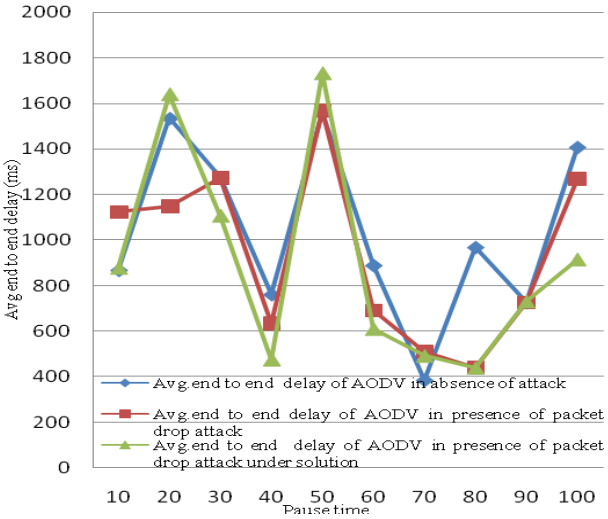

Figure 14.Avg.end-to-end delay vs.pause time

D. *Result Analysis*

It is observed that the difference between the result obtained for network in the presence of attack and in absence of attack is slightly difference.

Result difference analysis

A. Scenario 1

Consider S sends RREQ to neighbour to P and 5 ,both nodes sends RREP within time stamp. If 5 have less hops than P then source (S) selects 5 as a next hop node. Here P is not participating in route discovery. Here result will be very close to normal result even in presence of packet dropper. As no packets will be dropped by P.

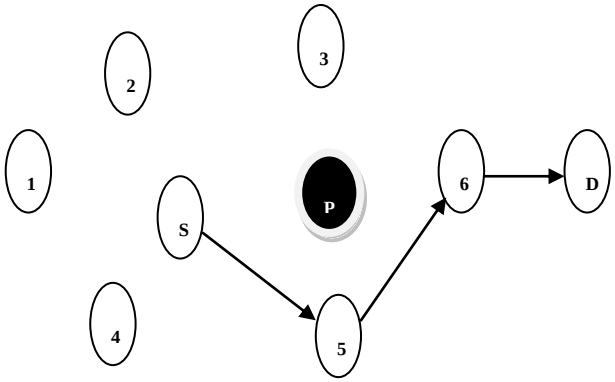

Figure 15. Packet dropper not taking part in route.

B.Scenario 2

Here if P has less number of hops source (S) selects P as next hop node. Here P is in the path of S, S sent packets to P. P does not forward/route packets to node 6,it drops the packet of S destined for D. Hence, the result will have difference. As there will be slight packet drop rate, less throughput etc in results.

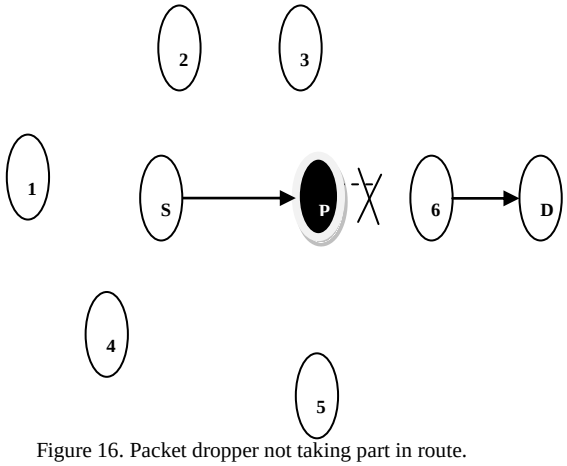

Figure 16. Packet dropper not taking part in route.

Reverse results are observed in some scenario.

1. In the proposed algorithm (node analysis is performed when RREP packet is received).We can say that it is analysis overhead.
2. Analysis is carried out by each and every node which receives RREP packet.
3. Expected results will be obtained in scenario 2/case II
4. But reverse result will be obtained in case I,as the packet dropper is not participated in route discovery but each and every node has done analysis. As discussed earlier, packet drop attack does not affect much the network performance .Hence reverse result can be easily observed.

VII. Conclusion and Future Work

In modified protocol,proposed approach uses providing security in AODV against packet drop attack. There is slightly difference between the performance of the network against packet drop attack for single attacker and solution. As the future scope of this work is to find cooperative environment to protect from packet drop attackers and increase the number of attackers. This algorithm has some limitation.It is executed on every route reply received.When absence of packet dropper in route discovery path,this makes unnecessary calculation increasing processing time unexpected result in some scenario.Hence using strawman approach and algorithmics,proposed algorithm can be made efficient.

Acknowledgment

We would like to thanks Erasmus Mundus ‘Mobility for Life’ under the Erausmus Mundus External Cooperation Window Lot 11 for supporting the research work. Erausmus Mundus is a cooperation and mobility programme in the field of higher education, the promotion of the European Union as a centre of excellance in learning around the world and the promotion of intercultural understanding through cooperation with the third countries in the field of higher education.

REFERENCES

[1] C.K.Toh, "Ad hoc Mobile Wireless Networks:Protocols and Systems",Prentice Hall ,December 03,2001

[2] Jeroen Hoebeke,Ingrid Moerman,Bart Dhoedt,Piet Demeester, "An Overview of Mobile Ad Hoc Networks:Applications and Challenges"Journal of the communication networks,July 2004.

[3] K.Sanzagiri,B.Dahill,B.N.Levine,C.Shields,E.M.Belding-Royer, "A Secure Routing Protocol for Ad hoc Networks"Proceeding of the 10th IEEE International Conference on Network Protocols (ICNP), November 2002.

[4] S.Buchegger and J.Y.Le Boudec,"Performance Analysis of the CONFIDENT Protocol",In Proc. 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing (MOBIHOC '02),Lausanne,Switzerland ,Tech.Rep.DSC/2001/001,June 2002.

[5] Kejun Liu , Jing Deng,Promod K,Varsheney,KashyapBalkrishnan, "An Acknowledgement-Based Approch for the detection of Routing misbehavior in MANETs" IEEE Transactions on Mobile Computing,pp. 448-502,vol.6,NO.5,May 2007.

[6] Z.H.Zhang,F.Nait-abdesselam,P.H.Ho and X.Lin, "RADAR:A ReputAtion –based scheme for Detecting Anomalous nodes in wireless networking Conference (WCNC 2008),Las Vegas,USA,March 2008.

[7] S.Neelavathy Pari,D Sridharan, "Mitigating Routing Misbehaviour in Self Organizing Mobile Ad hoc Network using K-neighbourhood Local Reputation System" IEEE-International Conference on Recent Trends Information Technology,ICRTIT ,Chennai,June 3-5,2011.

[8] C.Perkins, E.B.Royer,S.Das, "Ad hoc On Demand Distance Vector(AODV) Routing ,Internet Draft, " RFC 3561,IETF Network Working Group,July 2003.

[9] C.Perkins,E.B. Royer, S.Das, "Ad hoc On-Demand Distance Vector Routing," Proceeding of the 2nd IEEE Workshops on Mobile Computing System and Applications (WMCSA),pp.90-100,1999.

[10] Ashok M.Kanthe,Dina Simunic,Marijan Djurek, "Denial of Service (DoS) Attacks in Green Mobile Ad-hoc Networks",MIPRO 2012,IEEE Conference,Proceedings of the 35th International Convention,ISBN:978-1-4673-2511-6,May 21-25,2012,Opatija,Croatia.

[11] Ashok M.Kanthe,Dina Simunic,Ramjee Prasad , "A Mechanism for Gray Hole Attack in Mobile Ad-hoc Networks" International Journal of Computer Applications (0975-8887),Volume 53-No.16, September 2012.

[12] The network simulator-ns 2.35 http://www.isi.edu/nsnam/ns

Ashok M.Kanthe graduated Computer Science and Engineering at S.G.G.S.College of Engineering and Technology, Nanded, Dr.B.A.Marathwada University, Aurangabad in 1997,Maharashtra. He received Master Degree in Computer Engineering from Dr.Babasaheb Ambedkar Technological University, Lonere, Maharashtra. Currently he is pursuing his Ph.D.in Wireless Communication at University of Zagreb, Croatia, Faculty of Electrical Engineering and Computing in Zagreb. His research focus on mobile ad-hoc network security, protocol implementation. He published 4 scientific papers in journals and conference proceedings.

Dina Simunic is a full professor at University of Zagreb, Faculty of Electrical Engineering and Computing in Zagreb. She graduated in 1995 from University of Technology in Graz, Austria. In 1997 she was a visiting professor in "In Wandel & Goltermann Research Laboratory" in Germany, as well as in "Motorola Inc", Florida Corporate Electromagnetic Laboratory, USA, where she worked on measurement techniques, later on applied in IEEE standard. In 2003,she was a collaborator of USA FDA on scientific project of medical Interference. Dr.Simunic is a IEEE Transactions on Microwave Theory and Techniques and on Biomedical Engineering and Bioelectromagnetics, journal JOSE and a reviewer of many papers on various scientific conferences (e.g.IEEE on Electromagnetic Compatibility).She was a reviewer of Belgian and Dutch Government scientific projects,of the EU FP programs,as well as of COST_ICT and COST_TDP actions. She was acting as a main organizer of the database in the World Health Organization,for the service of International EMF Project from 2000 to 2009.From 1997 to 2000 she acted as a vice-chair of cost 244: "Biomedical Effects of Electromagnetic Fields". From 2001 to 2004, she served as vice-chair of Croatian Council of Telecommunications. In 2006, she is elected the first time and re-confirmed in 2010 as a vice-chair of Cost Domain Committee on Information and Communication Technologies (ICT).She is one of the proposer as well as a member of cost Transdomain committee. She is organizer of many workshops, symposia and round tables, as well as of special sessions (e.g., on telemedicine and intelligent transport systems during Wireless Vitae, Alborg, Denmark in 2009).She has held numerous invited Lecturers, among others at ETH Zurich, Switzerland in 1996 and US Air France, Brooks, as well as her student text for wireless communication, entitled: "Microwave Communications Basics". She is co-editor of the book "Towards Green ICT" ,published in 2010.She is also editor-in-chief of " Journal of Green Engineering" Her research work comprises electromagnetic fields dosimetry, wireless communications theory and its various applications (e.g.in intelligent transport system, body area networks, crisis management, security, green communications).She serves as a chair of the "Standards in Telecommunications" at Croatian standardization Institute.She serves as a member of Core group of Erausmus Mundus "Mobility for Life"

Prof. Dr. Ramjee Prasad is the Director of the Center for TeleInfrastruktur (CTIF) and Professor Chair of Wireless Information Multimedia Communication at Aalborg University (AAU), Denmark. Heisa Fellow of the Institute of Electrical and Electronic Engineers (IEEE), USA, the Institution of Electronics and Telecommunications Engineers(IETE), India; the Institution of Engineering and Technology (IET),UK; and a member of the Netherlands Electronics and Radio Society(NERG), and the Danish Engineering Society(IDA).He is recipient of several international academic, industrial and governmental awards of which the most recent is the Ridder in the Order of Dannebrog (2010), a distinguishment awarded by the Queen of Denmark.

Ramjee Prasad is the Founding Chairman of the Global ICT Standardisation Forum for India(GISFI: www.gisfi.org) established in 2009.GISFI has the purpose of increasing the collaboration between Indian, Japanese, European, North-American, Chinese, Korean and other worldwide standardization activities in the area of Information and Communication Technology (ICT) and related application areas. He is also the Founding Chairman of the HERMES Partnership (www.hermes-europe.net) a network of leading independent European research centres established in1997.

Ramjee Prasad is the founding editor-in-chief of the Springer International Journalon Wireless Personal Communications. He is member of the editorial board of several other renowned international journals and is the series editor of the Artech House Universal Personal Communications Series. Ramjee Prasad is a member of the Steering, Advisory, and Technical Program committees of many renowned annual international conferences,e.g.,Wireless Personal Multimedia Communications Symposium (WPMC);Wireless VITAE, etc. He has published more than 25 books, 750 plus journals and conferences publications, more than 15 patents, a sizeable amount of graduated PhD students (over 60) and an even larger number of graduated M.Sc. students (over 200). Several of his students are today worldwide telecommunication leaders themselves.