Network and Complex Systems
ISSN 2224-610X (Paper) ISSN 2225-0603 (Online)
Vol 2, No.2, 2012

A New Scheme for Secured on Demand Routing

Vijay Kumar[1*] Ashwani Kush [2]

1. Department of Computer Science,Guru Nanak Khalsa College Karnal – India vk.gnkc@gmail.com
2. Department of Computer Science University College, Kurukshetra University, Kurukshetra, India

Abstract

A Mobile Adhoc Network (MANET) is characterized by mobile nodes, multihop wireless connectivity, Non infrastructural environment and dynamic topology. A recent trend in Ad Hoc network routing is the reactive on-demand philosophy where routes are established only when required. Stable Routing, Security and Power efficiency are the major concerns in this field. This paper is an effort to achieve security solutions to achieve more reliable routing. The ad hoc environment is accessible to both legitimate network users and malicious attackers. The proposed scheme is intended to incorporate security aspect on existing protocol AODV. The study will help in making protocol more robust against attacks to achieve stable routing in routing protocols.

Keywords: Ad hoc Networks, Modified AODV, AODV, Performance evaluation.

1. Introduction

The wireless network can be classified into two types: (Kush A.2009, Kush et al.2009) Infrastructured and Non-Infrastructural. In Infrastructured wireless networks, the mobile node can move while communicating, the base stations are fixed and as the node goes out of the range of a base station, it gets into the range of another base station. In non Infrastructural or Ad Hoc wireless network, the mobile node can move while communicating, there are no fixed base stations and all the nodes in the network act as routers. The mobile nodes in the Ad Hoc network dynamically establish routing among themselves to form their own network 'on the fly'. A Mobile Ad Hoc Network is a collection of wireless mobile nodes forming a temporary/ short lived network without any fixed infrastructure where all nodes are free to move about arbitrarily and where all the nodes configure themselves. In this network, each node acts both as a router and as a host & even the topology of network may also change rapidly. Some of the challenges in this network include:(Kush A. 2009)Unicast/Multicast routing, Dynamic network topology, Network overhead, Scalability, QoS, Stable routing, Secure routing and Power aware routing. In this paper, a particularly challenging attack to defend against *wormhole* attack, and present a new, general mechanism for detecting and thus defending against wormhole attacks has been discussed. In this attack, an attacker records a packet, or individual bits from a packet, at one location in the network, tunnels the packet to another location, and replays it there. Rest of the apepr is organzed as: In section 2 problem statement is discussed, section 3 explains working of wormhole attack in AODV, section 4 is about proposed algorithm and its analysis and Conclusion have been made in section 6.

2. Problem Statement

The dynamics of Mobile Ad hoc Networks pose a problem in finding stable multi-hop routes for communication between a source and a destination. Since the nodes in mobile ad hoc network can move randomly, the topology may change arbitrarily and frequently at unpredictable times. So it is very difficult to find and maintain an optimal route. Basically, the routing algorithm must react quickly to topological changes. Most of the existing protocols maintain single routing path and rediscover the new path whenever a link fails. Popular ad hoc routing protocol normally uses the minimum number of hop routes or shortest routes for sending information. These routes tend to contain long-range links, therefore routes frequently fail and are not reliable. Stable routing makes the protocol robust and ready to use and is most important for transfer of packets.

2.1 Security Requirements

There have been numerous published reports and papers describing attacks on wireless networks that expose organizations to security risks such as attacks on confidentiality, integrity, non repudiation and network availability. There are several proposals to solve these issues but they target specific threats separately. Therefore, there is a requirement to have an efficient security system which takes care of all aspects of security.

Security Threats: (Bouam S.et al. 2003, Ghazizadeh S.et al 2002) Network security attacks are typically divided into passive & active attacks as summarized in table 1.

Passive Attack: An attack in which an unauthorized party gains access to an asset and does not modify its content. Passive attacks can be either eavesdropping or traffic analysis (sometimes called traffic flow analysis). These two passive attacks are described as;

- *Eavesdropping:* The attacker monitors transmissions for message content. An example of this attack is a person listening into the transmissions on a network topology between two workstations or tuning into transmissions between a wireless handset and a base station.
- *Traffic analysis:* The attacker, in a more subtle way, gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties.

Table 1: Passive vs. active attacks

Passive attacks: Eavesdropping, traffic analysis
Active attacks: Masquerading/Spoofing, Replaying, Message modification, DoS

Active Attack: (Inkinen Kai 2004, Wenjia Li et al. 2008) An attack whereby an unauthorized party makes modifications to a message, data stream, or file. It is possible to detect this type of attack but it may not be preventable. Active attacks may take the form of one of four types masquerading, replay, message modification, and Denial-of-Service (DoS). These attacks are summarized as:

- Masquerading: The attacker impersonates an authorized user and thereby gains certain unauthorized privileges. A spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.
- Replay: The attacker monitors transmissions and retransmits messages as the legitimate user.
- Message modification: The attacker alters a legitimate message by deleting, adding to, changing, or reordering it.
- Denial-of-Service: The attacker prevents or prohibits the normal use or management of communications facilities.

The consequences of these attacks include, but are not limited to, loss of proprietary information, legal and recovery costs, tarnished image, and loss of network service. Due to the dynamically changing topology and infrastructure less, decentralized characteristics, security is hard to achieve in mobile ad hoc networks. Hence, security mechanisms have to be a built-in feature for all sorts of ad hoc network based applications.

3. Working of Wormhole Attack in AODV

In this study wormhole attack is considered (Lazos L. et al.2005, Khalil I. et al. 2005, Chiu H.S. et al. 2006). Wormhole attack is not that difficult to set up, but still can be immensely harmful for a MANET. Moreover, finding better techniques for detection of wormhole attacks and securing AODV against them

still remains a big challenge in Mobile Ad-hoc Networks. Working of AODV in the presence of wormhole attack is described using Figure1.

In Figure 1 during path discovery process, sender "S" broadcasts RREQ to a destination node D. Thus nodes 24, 1, 2 and 3 neighbours of S, receive RREQ and forward RREQ to their neighbours. Now the malicious node M1 that receives RREQ forwarded by 25 records and tunnels the RREQ via the high-speed wormhole link to its partner M2. Malicious node M2 forwards RREQ to its neighbour 10, 9 and 26. Finally 26 forwards it to 27 and it will forward it to destination D. Thus, RREQ is forwarded via S-24-25-26-27-D. On the other hand, other RREQ packet is also forwarded through the path S-4-13-22-14-15-16-17-18-19-20-21-27-D. However, as M1 and M2 are connected via a high speed bus, RREQ from S-24-25-26-27-D reaches first to D. The wormhole attack exits in the route selected in AODV according to shortest path S-24-25-26-27-D. After getting the route requests to destination from the sender destination it will unicast a route reply packet to source "S" using shortest path. Source will select the shortest path as best route from source to destination for transmitting the data and other routes will be discarded. In above example destination "D" ignores the RREQ that reaches later and chooses D-27-26-25-24-S to unicast an RREP packet to the source node S. As a result, S chooses S-24-25-26-27-D route to send data that indeed passes through malicious M1 and M2 nodes that are very well placed in comparison to other nodes in the network.

4. Proposed Algorithm

The following assumptions are taken in order to design the proposed algorithm.

1. A node interacts with its 1-hop neighbours directly and with other nodes via intermediate nodes using multi-hop packet forwarding.
2. Every node has a unique id in the network, which is assigned to a new node collaboratively by existing nodes.
3. The network is considered to be layered.
4. Source and Destination node will not be wormhole node.

Steps of Modi_AODV Algorithm

1. *Source node sends route request*
2. *Intermediate node forward request*
3. *If intermediate node is wormhole it tunnels the packet to next end*
4. *If packet reaches destination it send reply to source*
5. *If wormhole receive reply then it tunnels to another wormhole end*
6. *Reply reaches source node and start transmitting data packet through shortest path*
7. *Then source node send path message to all intermediate node upto destination*
8. *Intermediate node receive path message and select 2nd hop path node as target node*
9. *It sends route message to one hop neighbour alongwith other nodes in path*
10. *One hop neighbour receive route message and find alternate path to target node*
11. *If hop count of alternate path > hop count threshold*
12. *Then previous hop node of target is detected as wormhole node*
13. *Else no wormhole present.*

The working of routing largely depends upon successful transmission of packets to the destination. This requires proper selection of Routing path and algorithm. AODV and Modified AODV have been used in this paper for routing solutions. All the simulations have been performed using Network Simulator Ns-2.32 on the platform Fedora 13. The traffic sources are CBR (continuous bit–rate). The source-destination pairs are spread randomly over the network. The mobility model uses 'random waypoint model' in area 1000m x 750m with 25, 50, 75 and 100 nodes. During the simulation, each node starts its journey from a random spot to a random chosen destination. Once the destination is reached, the node takes a rest period of time in second and another random destination is chosen after that pause time. This process repeats throughout the simulation, causing continuous changes in the topology of the underlying network. Different network scenario for different number of nodes and different node transmission range are generated.

Performance Metric: There are number of qualitative and quantitative metrics that can be used to compare reactive routing protocols. Most of the existing routing protocols ensure the qualitative metrics. Therefore we have used the following metrics. These performance metrics determines the completeness and correctness of the routing protocol. Performance metrics used here are: *Packet Delivery Ratio, Throughput and Average end to end delay*.

In Figure 2 the End to End Delay Ratio is compared in AODV and Modified AODV protocol using number of mobile nodes as a parameter. This performance metric has been evaluated using 25, 50, 75 and 100 mobile nodes. The results shows that the End to End Delay Ratio is though increasing with the increase in number of nodes in AODV but still the performance of Modified AODV is excellent than AODV in all cases. Figure 3 shows the performance of throughput is compared for AODV and modified AODV by increasing the number of nodes. The results show that modified AODV gives stable good throughput in all cases but in the case of AODV's throughput fluctuate and is low with the number of nodes 50. In Figure 4 packet delivery ratio has been evaluated for AODV and modified AODV protocols using 25, 50, 75 and 100 nodes. The PDR is very good of modified AODV in the comparison of AODV in all the situations. The result of modified AODV is slightly less with the high mobile nodes i.e. 100.

In Figure 5 and Figure 6 control packets are displayed. In any wireless network if control packets are high the overhead will be high. In above mentioned both figures modified AODV have more routing overhead compared to AODV. Routing overhead increases when the number of nodes increases in the scenario.

6. Conclusion

This paper has proposed an effective mechanism for AODV called modified AODV to detect and react to wormhole attacks and enhance the stability for MANETs. In all the comparisons shows that the results of modified AODV is much better and stable in the comparison of AODV. In AODV there are more fluctuations in the case of end to end delay ratio, PDR and throughput. But in the case of routing overhead its high compare to AODV.

Finally, stability is getting the cost in the shape of routing overhead. In next paper trying to detect and remove wormhole attack from the MAENT.

References

Bouam S. and J. B. Othman (2003), "Data Security in Ad hoc Networks using MultiPath Routing", in *Proc. of the 14th IEEE PIMRC*, pp. 1331-1335, Sept. 7-10, 2003.

Chiu H.S. and K.S. Lui,(2006), "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks", *In Proc. International Symposium on Wireless Pervasive Computing*, Phuket, Thailand.

D.B.J., Yih-Chun Hu, Adrian Perrig, (2002), "Ariadne: A secure on-demand routing protocol for ad-hoc networks", *Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002)*.

Ghazizadeh S., O. Ilghami, E. Sirin, and F. Yaman, (2002), "Security-Aware Adaptive Dynamic Source Routing Protocol", *In Proc. of 27th Conference on Local Computer Networks*, pp. 751-760, Nov. 6-8.

Hu Y.C., A. Perrig, and D.B. Johnson,(2006), "Wormhole Attacks in Wireless Networks", *In IEEE JSAC*, Vol. 24, No. 2, pp. 370-380.

Inkinen Kai (2004), "New Secure Routing in Ad Hoc Networks: Study and Evaluation of Proposed Schemes", Helsinki University of Technology T-110.551, *Seminar on Internetworking*, Sjökulla.

Khalil I., S. Bagchi, and N.B. Shroff,(2005), "LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks", *In Proc. International Conference on Dependable System and Networks (DSN)*, Yokohama, Japan.

Kush A. (2009) "Security Aspects in AD hoc Routing", *Computer Society of India Communications*, Vol. no 32 Issue 11, pp. 29-33.

Kush A. (2009), "Security and Reputation Schemes in Ad-Hoc Networks Routing", *International Journal of Information Technology and Knowledge Management*, Volume 2, No. 1, pp. 185-189.

Lazos L., R. Poovendan, C. Meadows, P. Syverson, and L.W. Chang,(2005), "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach", *In Proc. IEEE Wireless Communications & Netwoking Conference (IEEE WCNC)*, New Orleans, USA.

Qian ., N. Song, and X. Li (2005), "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks through Statistical Analysis of Multi-path", *In Proc. IEEE Wireless Communications & Netwoking Conference (IEEE WCNC)*, New Orleans, USA.

Wenjia Li, Anupam Joshi, (2008), "Security Issues in Mobile Ad Hoc Networks- A Survey", *Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County*, http://www.cs.umbc.edu/~wenjia1/ 699_report.pdf.

Author 1: Mr. Vijay is research scholar at Graphic Era University Dehradun - India and is working as assistant professor at Guru Nanak Khalsa College Karnal – India. He has 8 research papers to his credit. His area of interest is security and stability in Mobile ad-hoc networks.

Author 2: Dr. Ashwani Kush is working as Associate professor and head at university college, computer department, Kurukshetra university kurukshera India. He earned PhD in association with IIT Kanpur and KUK India on Ad hoc networks and has teaching experience of 20 years. Dr kush is member of IEEE, ACM, IAENG, IACSIT, CSI India and many other professional organizations. He has chaired sessions at Singapore, USA, India and Canada. He has more than 80 research papers to his credit. His areas of interest are Wireless networks, security, power awareness in Manet and e-goverance. He can be reached at akush@kuk.ac.in

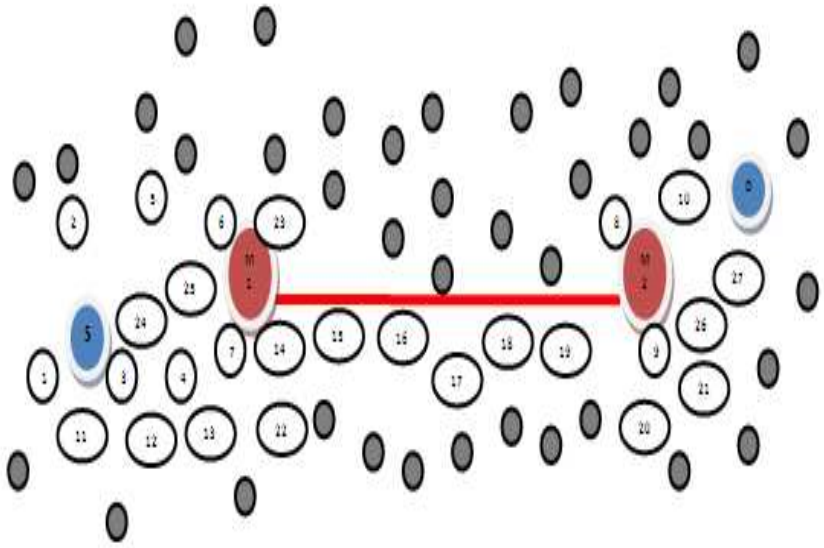

Figure1. Wormhole attack in AODV

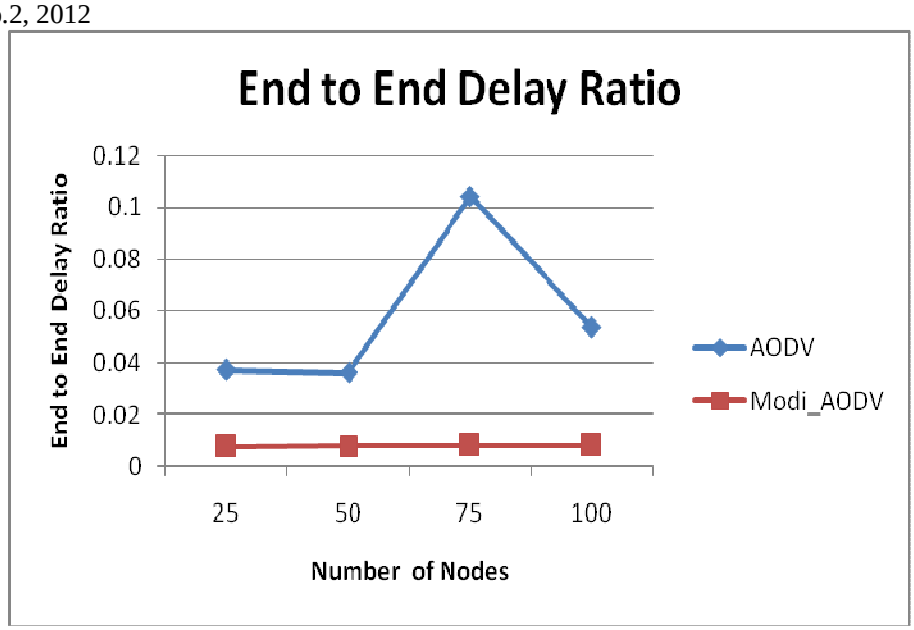

Figure 2: End to End Delay Ratio versus no. of nodes

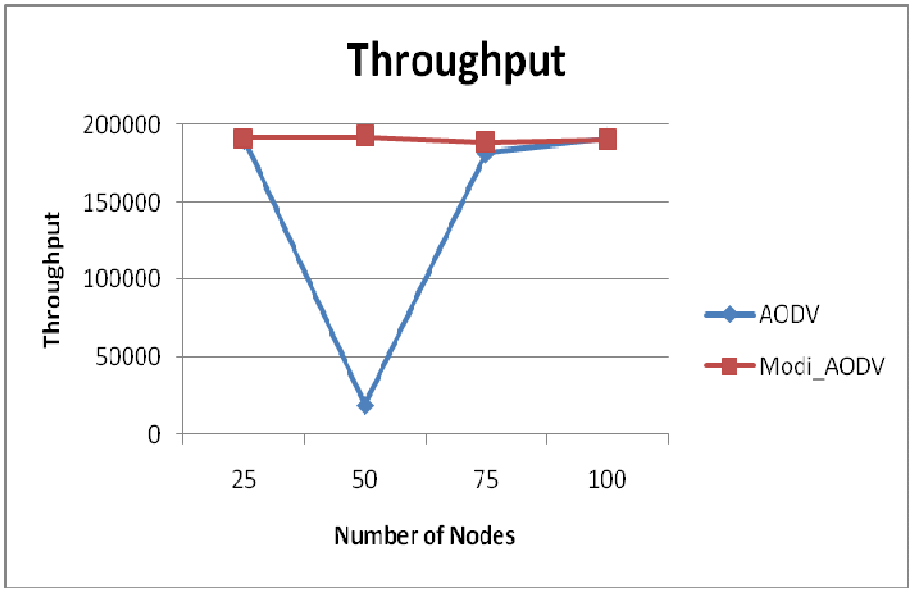

Figure 3: Throughput versus no. of packets per second

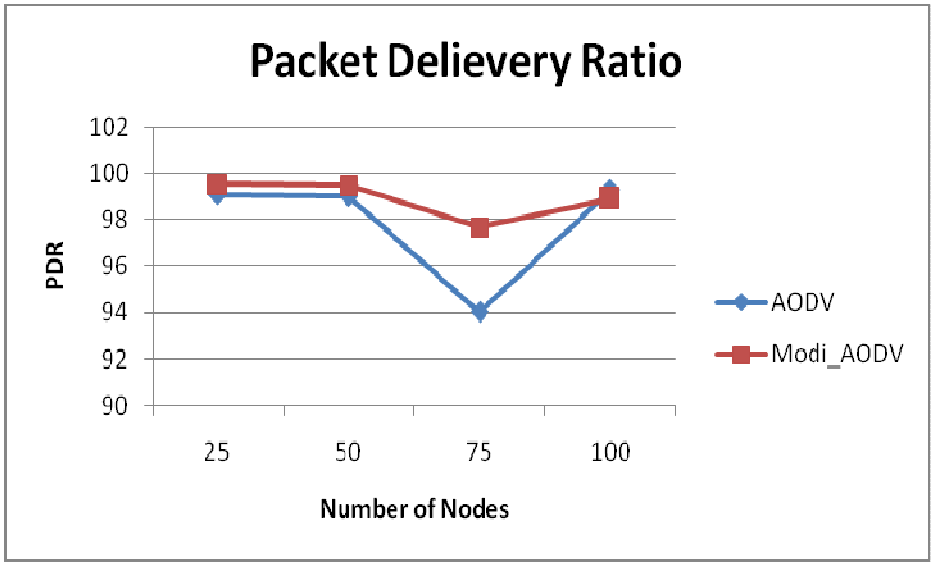

Figure 4: Packet Delivery Ratio versus no. of packets per second

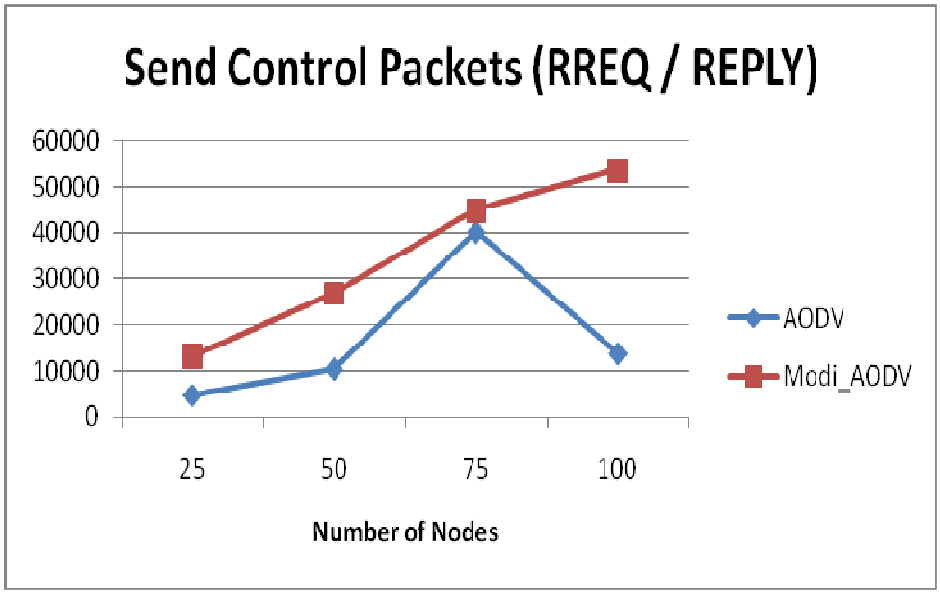

Figure 5: Send Control Packets (RREQ/ REPLY) versus no. of nodes

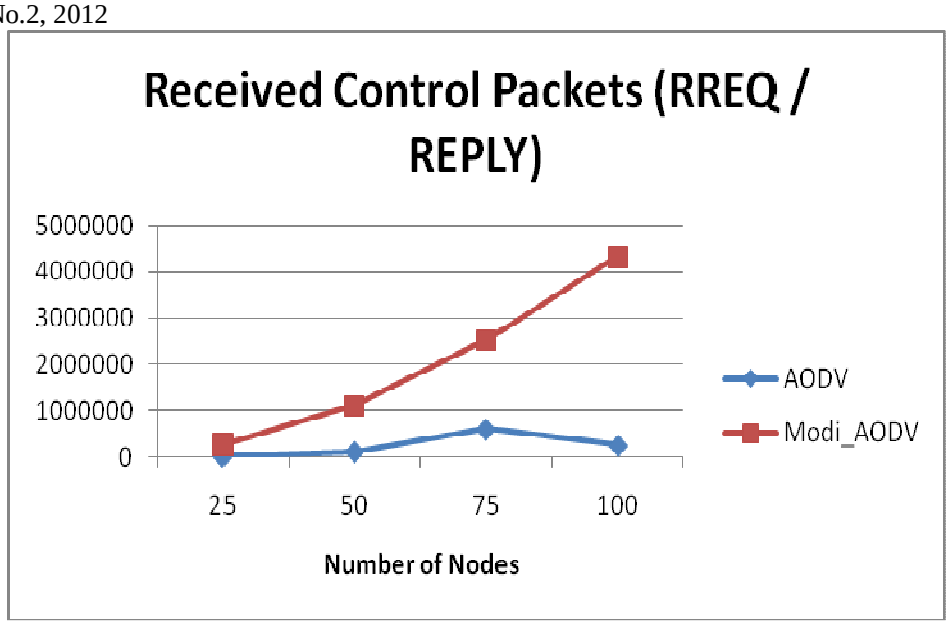

Figure 6: Received Control Packets (RREQ/ REPLY) versus no. of nodes