Passive Duplicate Address Detection in DYMO Routing Protocol for MANETS

M Sivakumar
Dept of Electrical & Electronics Engineering
Gnanamani College of Technology
Namakkal, India

C J Jickson
Dept of Electrical & Electronics Engineering
Gnanamani College of Technology
Namakkal, India

R M S Parvathi
Dept of Computer Science Engineering
Sengunthar College of Engineering
Thiruchengode, India

ABSTRACT

MANET (Mobile Ad Hoc Networks) is a wireless network in which all movable nodes can communicate with each other without depend on a fixed infrastructure. Here packet forwarding and routing is achieved by intermediate nodes. In reactive protocols, a routing path is acquired on-demand when a source desires to send data packets to destination. In order to send and receive packets between two nodes, they should have their unique address in the network. Since IP is also used in MANETs, a unique IP address should be assigned to each node. Therefore, IP address auto-configuration schemes have been developed to remove the overhead of manual configuration. Mobility is one of the reasons for partitioning of the network. When a node having unique IP address in one partition, moves into another partition, there may arise a chance of duplication of the IP address. Since, IP address has to be unique, address conflicts need to be detected through a DAD (Duplicate Address Detection) procedure. This paper mainly focused on passive DAD schemes such as LOC-SD-INT (Location Source Destination with Intermediate nodes) over DYMO routing protocol. In this paper improved accuracy of detecting address conflicts, improved detection success ratio and reduced detection delay to detect address conflicts has been achieved. Through extensive simulations using the ns-2 simulator, PDAD schemes verified and better results are achieved when compared to the PACMAN scheme. By using PDAD schemes better throughput can be obtained and hence quality of service improved. In this paper, PDAD schemes achieved better detection efficiency compared to PACMAN schemes. The performance evaluations and results are analyzed and verified by using NS 2 (Network Simulator 2) simulator and compared with the results of existing method PACMAN (Passive Auto Configuration for Mobile Ad Hoc Networks).

Keywords: MANET, DAD, DYMO, PACMAN

1. INTRODUCTION

A mobile Ad Hoc Network (MANET) is an autonomous network that consists of mobile nodes that communicate with each other over wireless links. This type of networks is suited for use in situations where a fixed infrastructure is not available. A few examples include: rescue operations, temporary head quarters, etc. Absence of fixed infrastructure poses several types of challenges for this type of networking. Among these challenges is routing. Mobile ad hoc networks are basically characterized by dynamic topology, energy contrast, limited bandwidth, limited physical security, Infrastructure less, terminals limitation. In Mobile Ad hoc Networks, routing is needed to find the path between source and the destination and to forward the packets appropriately. In routing, the responsibilities of a routing protocol include exchanging the route information, finding a feasible path to a destination based on the criteria such as hop length, and utilizing minimum bandwidth. Routing in mobile ad hoc network remains a problem given the limited wireless bandwidth and user mobility and insufficient scalability.

Routing protocols are divided into two types, they are Proactive routing (Table-Driven), Reactive routing (On Demand). In proactive routing protocols, routing information to reach all the other nodes in a network is always maintained in the format of the routing table at every node.

Reactive routing protocol discovers a route only when actual data transmission takes place. When a node wants to send information to another node in a network, a source node initiates a route discovery process. Once a route is discovered, it is maintained in the temporary cache at a source node unless it expires or some event occurs (e.g., a link failure) that requires another route discovery to start over again. Reactive protocols require less routing information at each node compared to proactive protocols, as there is no need to obtain and maintain the routing information for all the nodes in a network.

In a MANET, node mobility can cause the network to be partitioned into several sub-networks. In partitioned networks, new joining nodes have their unique addresses independent of other partitioned networks. In other words, same addresses can exist between partitioned networks. Therefore, when several partitioned networks or independent networks merge into one network, potential address conflicts must be resolved. In order to send and receive packets between two nodes, they should have their unique addresses in the network. Since IP (Internet Protocol) is also used in MANETs, a unique IP address should be assigned

to each node. Therefore, IP address auto-configuration schemes have been developed to remove the overhead of manual configuration. In particular, the IETF Autoconf working group has been created to address this issue. Since the address has to be unique, address conflicts need to be detected through a DAD (Duplicate Address Detection) procedure. There are two types of DAD schemes they are PACMAN and PDAD. Three existing DAD (called PACMAN) schemes that operate over on-demand routing protocols: RREP-Without-RREQ (RwR), RREQ-Never-Sent (RNS), and 2RREPs-on- RREQ (2RoR). In this paper PDAD schemes, to detect address conflicts of source nodes, implement Location-S scheme, to detect address conflicts of destination nodes, PDAD implement Location-D scheme..

2. RELATED WORK

The Dynamic MANET On-demand routing protocol (DYMO) is a newly protocol currently defined in an IETF Internet-Draft. DYMO is a successor of the AODV routing protocol and is the current engineering focus for reactive routing in the IETF MANET working group. It operates similarly to AODV, but rather simplifies it, while retaining the basic mode of operation. AODV with Path Accumulation (AODV-PA) proposed by Gwalani et al. extends AODV with the source route path accumulation feature of DSR. Using AODV as a basis, DYMO combines the ideas originated in AODV-PA and AODVjr.

Route discovery is the process of creating a route to a destination when a node needs a route to it. When a node S wishes to communicate with a node D, it initiates a Route Request (RREQ) message. The RREQ message and the Route Reply (RREP) message are collectively known as Routing Messages (RM). Because they are used for distribute routing information. The sequence number maintained by the node is incremented before it is added to the RREQ.

In the RREQ message, the node includes its own address and its sequence number, which is incremented before it is added to the RREQ. Since replies are sent on the reverse path, DYMO does not support asymmetric links. The packet processing done by nodes forwarding the RREP is identical to the processing that nodes forwarding an RREQ perform, i.e., the information found in the RREP can be used to create forward routes to nodes that have added their address block to the RREP.

Three existing DAD (called PACMAN) schemes that operate over on-demand routing protocols: DAD-RREP-Without-RREQ (RwR), DAD-RREQ-Never-Sent (RNS), and DAD-2RREPs-on-RREQ (2RoR).

1) RwR scheme: During route discovery, the source node floods an RREQ packet to discover a route towards a destination node, and it then receives an RREP packet from the destination node. However, if the source node receives an RREP packet destined to itself (although it has never sent an RREQ packet), this means that the same address that the source node uses definitely exists in the network (see Figure 1a). Therefore, the source node will invoke an address conflict resolution process.

2) RNS scheme: If a node has never sent an RREQ packet, but it receives an RREQ whose source address is the same address that it is using, this indicates an address conflicts (see Figure 1 b). Therefore, the node will invoke an address conflict resolution process.

3) 2RoR scheme: This scheme assumes that a destination node should reply only once with an RREP packet. If a source node receives more than one RREP packet from the same destination node, this means that there exist duplicate addresses (see Figure 1c). Therefore, the source node will invoke an address resolution process. Figure 2 shows PACMAN schemes flow diagram. In that all three schemes are explained. Both RwR and RNS schemes can be applied to on-demand routing protocols such as AODV and DYMO protocols. However, they still have to resolve a situation in which multiple nodes with the same address want to obtain paths towards their destination nodes and will flood their RREQ packets simultaneously. In addition, to detect address conflicts, each node should store RREQ packets (which was sent from itself) and compare the received RREQ whenever receiving new RREQ packets from other intermediate notes,

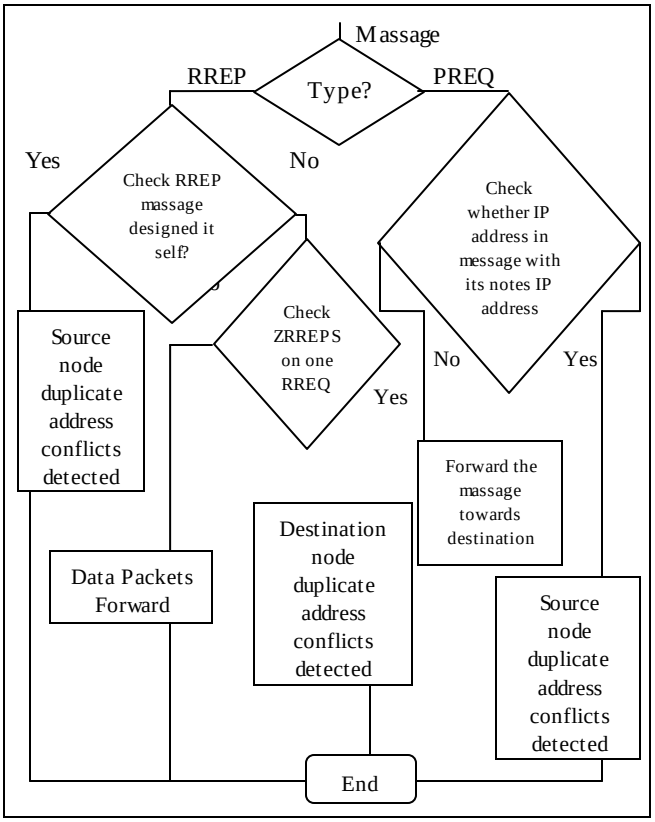

Figure 1. Passive Auto Configuration for MANETS

i.e. different paths. When the destination node receives the first RREQ packet from a source node, it will reply to the source node with an RREP packet. Meanwhile, if an RREQ packet which traversed a better route is received, the node will send a new RREP packet back to the source node. The criteria to determine better routes are based on power saving, route stability, and others. Therefore, the destination node can reply with multiple RREP packets back to the source. However, 2RoR relies on the strong assumption that a single destination node only replies once to a specific RREQ.

Hence, the scheme cannot be applied to the route discovery protocol that attempts to obtain the best route according to route selection criteria. In summary, the 2RoR scheme cannot differentiate between the case in which a single destination node replies with multiple RREP packets for providing the best route and the case in which other nodes that use the same destination addresses reply with their RREP packets. Drawbacks of PACMAN scheme are It requires more than one RTT(round trip time), It detects source and destination node duplicate address conflicts only, False detections are more, RREQ's and RREP's should be stored itself.

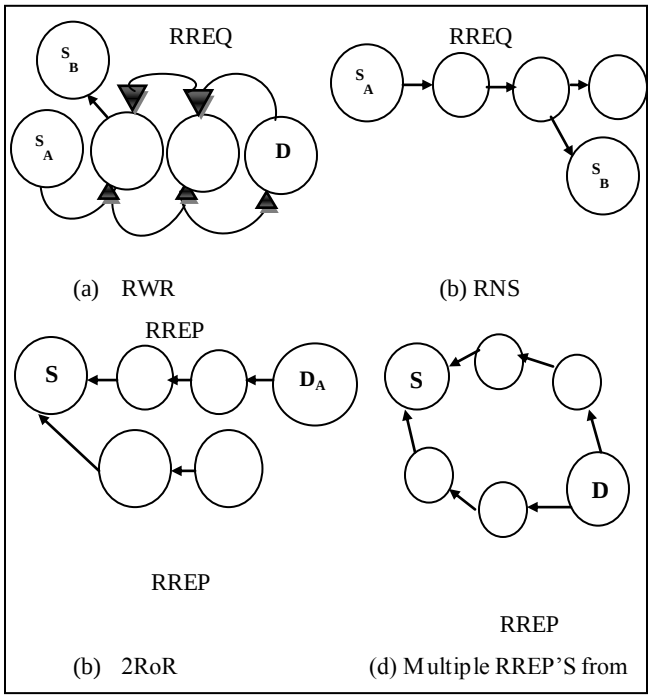

Figure 2. Flow diagram of PACMAN schemes

3. PDAD SCHEMES

Passive Duplicate Address Detection Schemes: PDAD schemes have three main goals: (a) improving the accuracy of detecting address conflicts, (b) improving the detection success ratio, and (c) reducing the time taken to detect these conflicts. To detect address conflicts of source nodes, implement Location-S scheme. To detect address conflicts of destination nodes, PDAD implement Location-D scheme.

3.1 Using location information - PDAD of Source Node with Location Information (Location-S) scheme:

In order to differentiate between RREQ packets which contain the same source address but are issued from different nodes, Location-S scheme includes location information (*longitude, latitude, altitude*) into RREQ packets. The location obtained when a node configures its IP address is recorded and utilized to detect address conflicts. Thereafter, when an RREQ packet is flooded from a source node, the source node includes its recorded location in the RREQ packet. When a source node receives an RREQ packet with the same source IP address but with different location information from its own recorded location, this means that an address conflict exists (see figure 3). To obtain the location information of a node, various existing wireless localization schemes can be employed. However, they all have some location errors due to inaccuracy of their localization schemes. Hence, nodes within an error tolerance range may obtain the same location. To address this inaccuracy problem, the information on the time when nodes acquire their addresses is included into RREQ packets add to location.

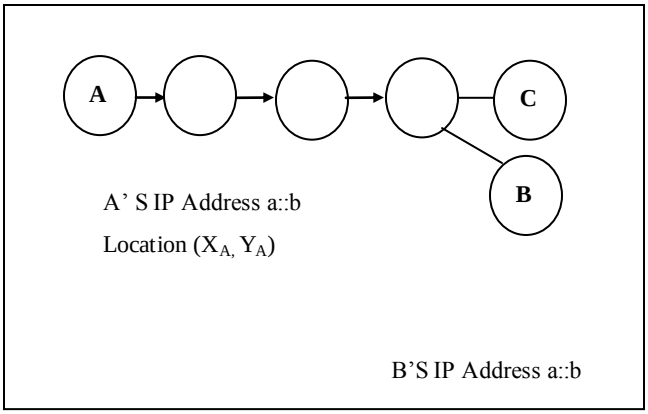

Figure 3. Location-S scheme

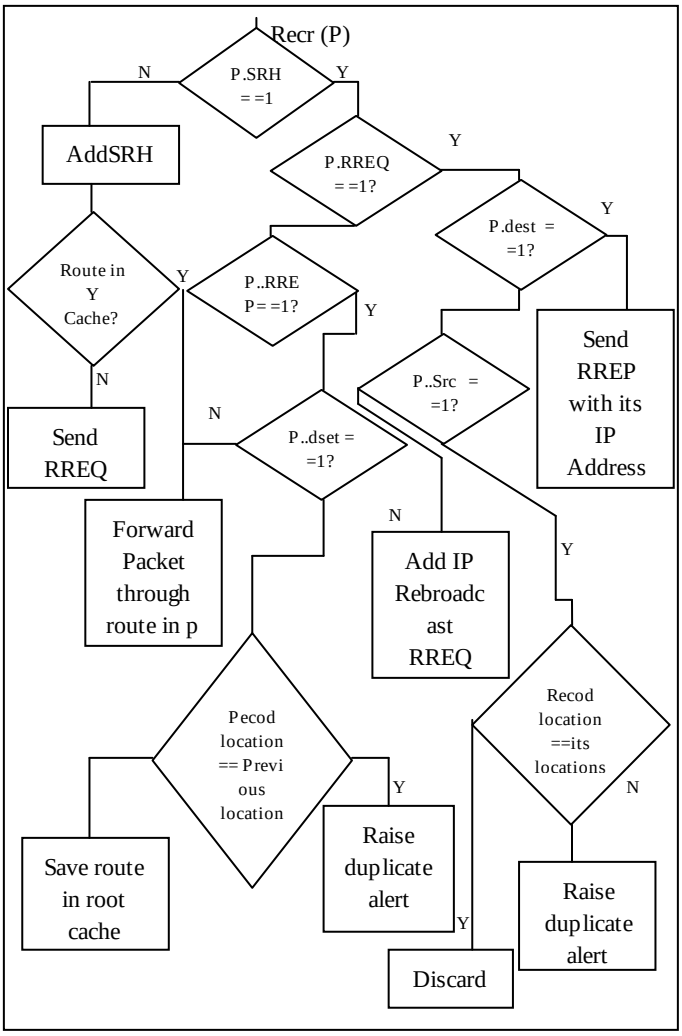

Figure 4. Data Flow Diagram for PDAD schemes

3.2 Using location information - PDAD of Destination Node with Location Information (Location-D) scheme:

This scheme can address the following two scenarios:

(a) A single destination node sent multiple RREP packets to the source node, and

(b) Multiple nodes using the same address sending their RREP packets to the source Node.

Similar to the Location-S scheme, in order to differentiate between RREP packets (which contain the same source address, but are issued from other nodes), Location-D scheme includes location information (*longitude, latitude, altitude*) into RREP packets. The location obtained when a node configures its IP address is recorded and utilized to detect address conflicts.

When sending an RREP packet, a destination node includes its recorded location. When a source node receives more than one RREP packet with different location, it will conclude the existence of duplicate addresses for destination nodes. The flow diagram of PDAD schemes is given in figure 4. How the receiving packet is processed can be understand easily.

3.3 Participation of intermediate nodes (LOC-SD-INT):

To detect address conflicts, Location-S, Location-D need some delay with more than one RTT (Round Trip Time) between source and destination nodes. This is because source and destination nodes only can detect address conflicts after exchanging RREQ and RREP packets.

This delay, however, can be reduced through the participation of intermediate nodes. When source and destination nodes send RREQ and RREP packets respectively, their recorded location (*longitude, latitude, altitude*) will be put into the RREQ and RREP packets. Each intermediate node receiving the RREQ or RREP packets will create a table entry with source node, destination node locations also.

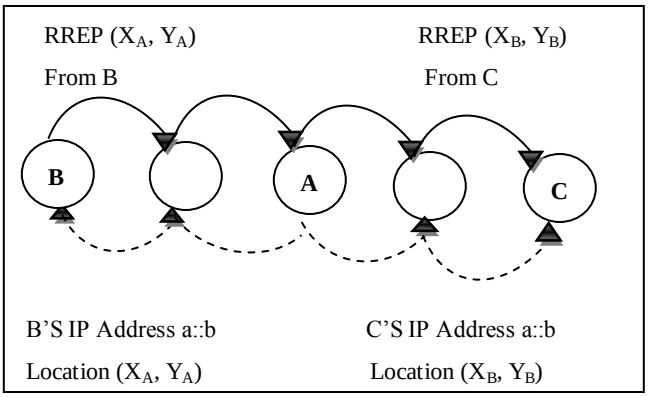

Figure 5. Location-D scheme

The table entry will be deleted after a timeout. Therefore, when an intermediate node receives RREQ or RREP packets from a source or a destination node using the same address, the location in the RREQ or RREP packets will be compared with those in the table entry. If a difference is detected, then an address conflict has occurred. Multiple intermediate nodes can detect an address conflict for a source or destination address at almost the same time. Hence, they will try to notify all nodes in the network of the address conflict. Consider a case where duplicate addresses exist in the network. Since a routing protocol cannot find any appropriate path towards nodes with duplicate addresses, any communication trial with these nodes will fail. To prevent these problems, a node which detects any address conflict should announce the detection to all nodes in the network, by utilizing an efficient flooding technique.

4. ANALYSIS

To evaluate performance, in this paper implemented our passive DAD schemes and an existing scheme (called PACMAN) in ns-2 simulator. The DYMO protocol was used as our underlying routing protocol because the IETF MANET working group has been trying to standardize it. Moreover, DYMO supports the "Generalized MANET Packet/Message Format", so that additional information (location, neighbor list, etc) can be easily added into the packet header through its TLV (type, length, value) block.

4.1 Simulation Environment

This paper extended the DYMO protocol to support our passive DAD schemes. Detailed simulation parameters are described in Table I. Initially, n% (from 5% to 20%) of network nodes are assigned duplicate addresses which are randomly selected among addresses which have been already assigned to the other nodes.

Table 1. Simulation parameters

Parameter Types	Value
Routing protocol	DYMO protocol
Number of nodes	8,10,12,16,20
Percentage of Duplicate Address	25%,50%
Simulation area	1000x1000 m^2
Simulation duration	50 seconds
Mac protocol	IEEE 802.11b
Topologies	Random

Passive DAD schemes can detect address conflicts in the network only when nodes with duplicate addresses receive an RREQ or RREP packet. Hence, we scheduled each node in the network to execute a route discovery during the simulation time to all nodes except itself. This makes each node send RREQ packets from 1 to 5 times every second.

4.2 Evaluation Of DAD Schemes

Important parameters related to PDAD schemes include

4.2.1 Detection success ratio

Figure 6 shows the detection success ratio versus the number of nodes. Initially, 25% of network nodes were assigned duplicate addresses. As the number of nodes increases, better detection success ratio is achieved. This is because a larger number of nodes results in better connectivity with other nodes.

Especially, we observe a significant improvement in detection success ratio (Figure 6) when the number of nodes was increased from 16 to 20. The average detection success ratio of LOC-SD and LOC-SD- INT increases from 72% to 85% and from 90% to 98%,respectively. When the number of node is more than 25 nodes, both schemes achieve over 90% of detection success ratio, regardless of node mobility. When comparing LOC-SD with LOC-SD-INT, LOC-SD-INT performs better than LOC-SD under the same simulation parameters, such as the number of node and node mobility. In case of LOC-SD, the DAD can occur only when the source and destination exchange the RREQ/RREP packets. However, in LOC-SD-INT, an address conflict can be detected via intermediate nodes.

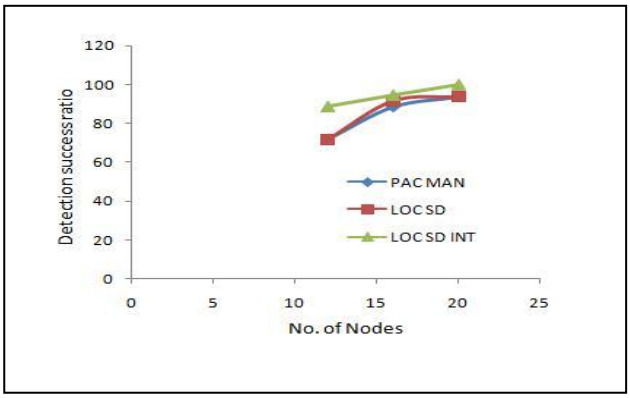

Figure 6. Detection success ratio

4.2.2 Detection Delay

Figure 7 shows the detection delay under varying number of nodes. The detection delay depends on the RTT (Round Trip Time) between source and destination nodes. From Figure 7, when the number of nodes in the network increases, the detection delay also increases.

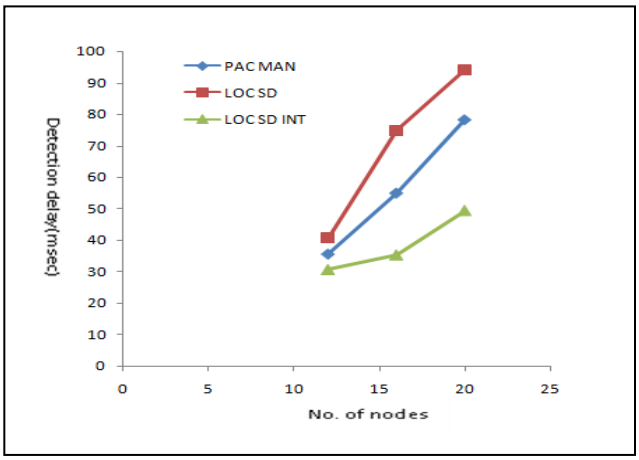

Figure 7. Detection delay

As the number of node increases (from 12 to 16 nodes), the average detection delays of LOC-SD and LOC-SD-INT increase steadily from 41 ms to 75 ms, and from 31 ms to 36 ms, respectively. In other words, LOC-SD-INT achieves shorter delay than LOC-SD. This is because a larger number of nodes create a longer hop path, and hence the RTT is also increased. However, for LOC-SD-INT, since an address conflict can be detected by intermediate nodes, LOC-SD-INT has better detection delay than LOC-SD.

4.2.3 Detection Accuracy

In the PACMAN scheme, a duplicate address can be misdetected. As mentioned in Section II, when multiple nodes invoke route discovery simultaneously, senders of a route request cannot detect the address conflict using RNS, because they can detect the conflict when receiving an RREQ without sending any RREQ. In addition, when a destination node replies with multiple RREPs, 2RoR can misdetect the address conflict. They are called RNS-false and 2RoR-false, respectively. In PDAD schemes detection accuracy is improved because location information is included in both RREQ and RREP packets.

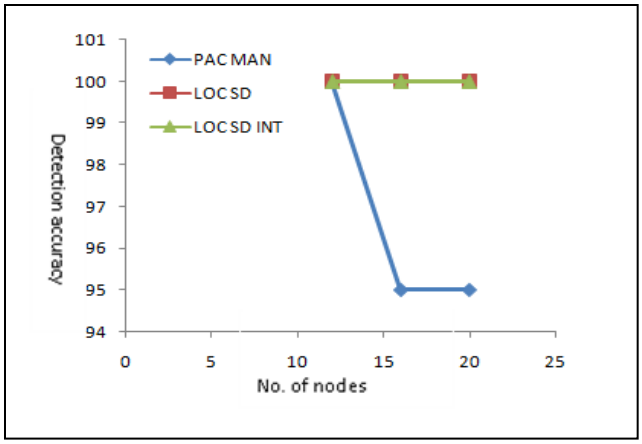

Figure 8. Detection accuracy

5. CONCLUSION

In this paper, several Passive Duplicate Address Detection schemes are presented. These schemes detect address conflicts quickly and accurately during route discovery and maintenance over DYMO routing protocol. The schemes utilize location of nodes. This information is included into routing control packets such as RREQ and RREP packets in order to detect the duplicate address of source and destination nodes.

Three main goals: (a) improving the accuracy of detecting address conflicts, (b) improving the detection success ratio, and (c) reducing the time taken to detect these conflicts are achieved. In addition, improved the detection success ratio and reduced the detection delay obtained by allowing intermediate nodes to participate in detecting address conflicts.

Through extensive simulations using the ns-2 simulator, verified that PDAD schemes and achieved better results when compared to the PACMAN scheme. By using PDAD schemes better throughput is obtained quality of service is improved. In this paper, PDAD schemes achieved better detection efficiency compared to PACMAN schemes. It is observed as the number of nodes increases avg. detection delay is increased. Because every node checks its IP address and location information with its recorded routing table information. However Passive Duplicate Address Detection schemes takes less time to detect duplicate addressed nodes because intermediate nodes are participated in detection process.

6. REFERENCES

[1] Dongkyun Kim, Hong-Jong Jeong, C.K.Toh, and Sutaek oh "Passive Duplicate Address Detection Schemes for On-demand Routing Protocols in Mobile Ad Hoc Networks" IEEE Transactions on Vehicular Technology,(To appear in 2009)

[2] Internet Engineering Task Force, "MANET working group charter,"

http://www.ietf.org/html.charters/manet-charter.html

[3] I. Chakeres and C. Perkins, "Dynamic MANET and (DYMO) Routing," IETF Internet-Draft, draft-ietf-.manet-dymo-16.txt, December 2008.

[4] Z. Haas, "A New Routing Protocol for the reconfigurable reconfigurable Wireless Networks " IEEE International Conference on Universal Personal Communications,October 1997.

[5] Internet Engineering Task Force, "Autoconf working group charter,"

http://www.ietf.org/html.charters/autoconf-charter.html

[6] S. Mesargi and R. Prakash, "MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network,"in Proc. of IEEE INFOCOM 2002, New York, USA, June 2002.

[7] N.H. Vaidya, "Weak Duplicate Address Detection in Mobile Ad Hoc Networks," in Proc. of MOBIHOC 2002, Lausanne, Switzerlan, June 2002.

[8] K. Weniger, "PACMAN: Passive Autoconfiguration for Mobile Ad Hoc Networks," IEEE Journal of Selected Areas in Communications Vol.23, No.3,March 2005.

[9] A. El-Rabbany, "Introduction to GPS: The Global Positioning System, Second Edition," Artech House publishers.

[10] N. Choi, C.K. Toh, Y. Seok, D. Kim, and Y. Choi "Random and Linear Address Allocation for Mobile Ad Hoc Networks," in Proc. of IEEEWCNC 2005, New Orleans, USA, March 2005.