Detection of Duplicate Address in Mobile Adhoc Networks for On Demand Routing Protocols

P. Nagesh[1], G. Ramesh[2], P.V.Gopikrishna Rao[3] V. S. Sivakumar[4]

[1]Network Engineer Ailwireict P V T L T D Bangalore,
[2]Assistant Professes or Dept. Of Eie, Rg Mcet, Nandyal, A. P, India
[3]Associate Profess or Dept. Of Eie, Rg Mcet, Nandyal, A. P, India
[4]Assistant Profess or Dept. Of Eie, Rg Mcet, Nandyal, A. P, India

ABSTRACT: *MANET is a wireless network in which all nomadic nodes can communicate with each other without relying on a fixed infrastructure. By using the intermediate nodes we will achieve the forwarding and routing of the packet. The necessity of developing the IP addresses auto configuration schemes is because of to send and receive the packets between two nodes with the same IP (unique addresses). In order to assign the unique IP addresses to each node, when one node from one partition moves in to another partition the chance of duplication of IP addresses. For implementing, since IP is also used in MANETS. The addresses detection schemes have been developed to remove the over head manual configuration. This project mainly focuses on passive DAD schemes over on- demand ad hoc routing protocols. The ultimate goal of this project is to improve accuracy of detecting address conflicts and improve detection success ratio.*

Key words: *Mobile Adhoc Networks (MANETS), on demand routing protocols, Duplicate Address Detection.*

I. INTRODUCTION

Recently, research interest in MANETs (Mobile Ad Hoc Networks) has increased because of the proliferation of small, inexpensive, portable, mobile personal computing devices. A MANET is a group of mobile, wireless nodes which cooperatively and spontaneously form a network independent of any fixed infrastructure or centralized administration. Since packet forwarding and routing are achieved via intermediate nodes, the MANET working group of IETF has standardized AODV (Ad hoc On- Demand Distance Vector Routing), DSR (Dynamic Source Routing) and OLSR (Optimized Link State Routing) as its reactive and proactive routing protocols, respectively. Nowadays, DYMO and OLSRv2 have been standardized as working group drafts. In proactive protocols, routing information to all possible destinations in the network is maintained by each node so that a packet can be transmitted over an already- existing routing path. In reactive protocols, a routing path is acquired on-demand when a source desires to send packets to a destination. In addition, a hybrid routing protocol like ZRP (Zone Routing Protocol) has been proposed in order to support a large-scale MANET.

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 info.

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. Since the address has to be unique, address conflicts need to be detected through a DAD (Duplicate Address Detection) procedure.

II. RELATED WORK AND MOTIVATION

Three previously proposed PDAD (called PACMAN) schemes that operate over on-demand routing protocols are de- scribed in this section: PDAD-RREP-Without-RREQ (RwR), PDAD-RREQ-Never-Sent (RNS), and PDAD-2RREPs-on- RREQ (2RoR).

2.1 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.

2.2 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 Both RWR and RNS schemes can be applied to on-demand routing protocols such as AODV and DYMO protocols. How- ever, 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 nodes. In particular, the 2RoR scheme has a serious drawback. Since an RREQ packet is flooded into the network, the destination node will receive multiple RREQ packets each of which traverses different intermediate nodes, 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 (this is beyond the scope of our paper). Therefore, the destination node can reply with multiple RREP packets back to the source.

III. OUR PROPOS ED SCHEMES

Our 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, we propose: (a) Location-S scheme and (b) Neighbor- S scheme. To detect address conflicts of destination nodes, we propose: (a) Sequence-D scheme, (b) Location-D scheme, and (c) Neighbor-D scheme. These schemes will be elaborated below.

3.1 Schemes to detect address conflicts of source nodes

We propose two schemes that can detect address conflicts when receiving RREQ packets from multiple nodes using the same address. In our schemes, an RREQ packet contains location or neighbor information that can be used to detect address conflict of source nodes.

3.1.1 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.1

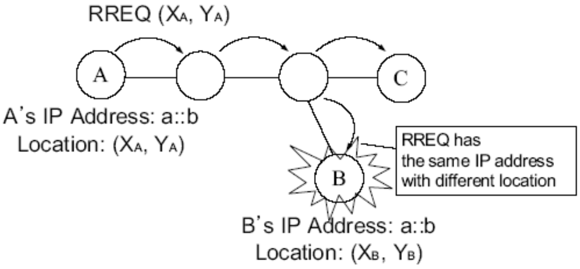


Figure1: Example of Location-S scheme

To obtain the location information of a node, various existing wireless localization schemes can be employed, such as GPS, TOA, TDOA, etc. However, they all have some location errors due to inaccuracy of their localization schemes. Hence, nodes within an error tolerance range may obtain information on the time when nodes acquire their addresses is included into RREQ packets, in addition to location.

3.1.2. Using neighbor information PDAD of Source Node with Neighbor Knowledge (Neighbor-S) scheme

In Neighbor- S scheme, instead of using location information, a list of neighbor nodes is used. A list of neighboring nodes is noted and recorded when the node's IP address is configured. Since nodes with many neighbors produce a large-sized packet, a subset of neighboring nodes (neighbor_list) is utilized to detect the address duplication. To choose the k number of nodes among neighboring nodes, various algorithms can be used: random selection, a sorting of the address list and a selection of the first *k* addresses. As the *k* value increases, the protocol overhead (i.e. the size of RREQ/RREP packets) also increases. However, this overhead can be reduced by taking advantage of packet compression techniques. When an RREQ packet is transmitted, the neighbor subset is included in the RREQ packet. When a source node recognizes the difference between the information of neighbor nodes in the received RREQ packet and its recorded list, it can therefore detect the address conflict.

However, consider an example shown in Figure 2. If nodes S_A and S_B, which have the same address, flood their RREQ packets toward node D using N_A and N_B as their neighboring nodes, duplicate addresses cannot be detected at D. In this case, one possible approach is using "hello" exchange. N_A and N_B will therefore detect the usage of duplicate addresses and invoke an address conflict resolution in case that S_A and S_B are using different MAC addresses. However, we cannot tell whether MAC address is unique in the network due to several reasons Some manufacturers sell network adapters with non-registered MAC addresses; MAC addresses may get corrupted during the manufacturing process, or most network adapters allow users to change the MAC address to an arbitrary value.

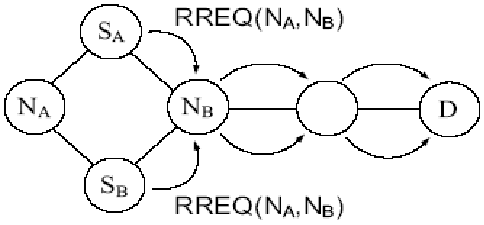


Figure2: Neighbor-S Scheme.

3.2 Schemes to detect address conflicts of destination

In this section, we propose three schemes to detect address conflicts of destination nodes more accurately. They are: (a) Sequence-D scheme, (b) Location-D scheme, and (c) Neighbor-D scheme. These schemes 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.

3.2.1 Using sequence number - PDAD of Destination Node with SEQ (Sequence-D) scheme

Sequence-D scheme requires an incremental sequence number to be included in each PREP packet transmitted by a destination node Sequence number is denoted by DAD-sequence to differentiate between it and the sequence number used by routing protocols such as AODV and DYMO in order to perform route discovery or maintenance. The latter is denoted by Routing-Sequence in this paper.) An additional new DAD-sequence field is needed to perform the DAD functionality in our scheme. Whenever the destination node replies with a new RREP packet because it has received an RREQ packet which traversed a better route, the DAD-sequence number increases and is put into the RREP packet. Therefore, when a source node receives more than one RREP packet with the same DAD-sequence number and the same destination address, the source node can detect the presence of address conflict. Since an RREQ packet contains an Routing-sequence number generated by a source node, the sequence number of RREP packets is reset when a new RREQ Packet with higher Routing-sequence number arrives at the destination. From Figure 4, a source node S can discover that destination nodes D_A and D_B are using the same IP address through The DAD-sequence number included in RREP packets (see sequence numbers in parenthesis in the figure). Node S floods

An RREQ packet with an Routing-sequence number into the Network in order to find a path towards its destination. Nodes D_A and D_B reply with RREP (1, 2, 3) and RREP (1, 2) packets. This is because each destination has received different RREQ packets which traversed better route than the previous RREQ packets. Thus, whenever D_A and D_B reply with a new RREP packet, an incremental DAD-sequence number is put into the RREP packets (i.e. from RREP(1) to RREP(3)). Hence, when the node S receives RREP packets with the same DAD sequence number, it can detect an address conflict.

In addition, consider the occurrence of packet losses. In a case where RREP only is lost, Sequence-D scheme can detect the address conflict successfully by receiving both RREP (1) and RREP packets from each destination node,D_A and D_B . In the other case where RREP (1) of D_A reach node S successfully, node S will fail to detect the address conflict. In Sequence-D scheme, such simultaneous packet losses can cause the source node to miss detecting the address conflict. However, this problem can be resolved by our other DAD schemes, such as Location-D and Sequence-D schemes.

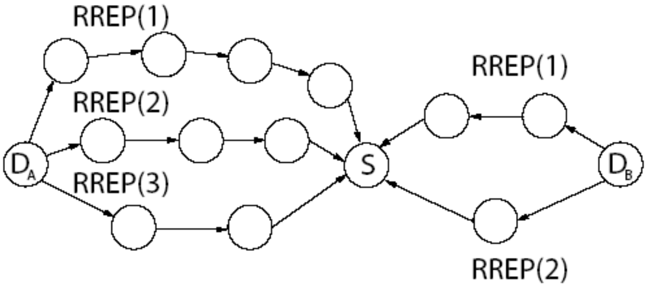


Figure3: Example of Sequence-D scheme.

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

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 (see Figure 4). 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.

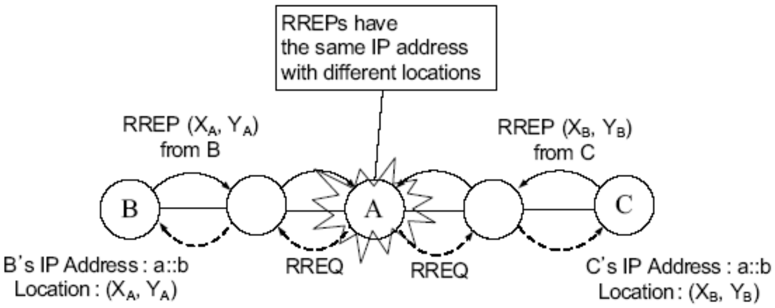


Figure4: Example of Location-D scheme.

3.2.3 Using neighbor information - PDAD of Destination Node with Neighbor Knowledge (Neighbor-D) scheme

Similar to the Neighbor-S scheme, the subset of neighbor nodes (neighbor_list) obtained when a node configures its IP ad- dress is captured and recorded. Then, it is utilized to detect the address duplication. When a destination node replies with an RREP packet, a subset of neighbor nodes of the destination node (neighbor_list) is included in the RREP packet. When a source node receives more than one RREP packet with different neighbor lists, it will determine the existence of duplicate addresses for destination nodes. addresses due to the same reason mentioned in Section III-A2. Such a collision might occur only if nodes with the same IP address have chosen the same subset of neighbor list (albeit low). If they are one-hop reachable, the collision can be easily addressed by the Neighbor Discovery (ND) protocol. For example, if nodes D_A and D_B are one- hop reachable, after assigning IP address to nodes D_A , it can detect address conflict using existing ND protocols which exchange Neighbor Request and Reply. Otherwise, using a combination of passive DAD scheme is recommended, such as Location-S and Neighbor-S, Sequence-D and Neighbor-D. In our Location-S/D and Neighbor-S/D schemes, we use extra control information (location and/or neighbor list) to achieve 100% detection accuracy. These extra bytes of control information did not incur large overhead. 16 bytes are needed in length. Hence 16 byte location information is needed, also the compression techniques can be used where there are more neighbours.

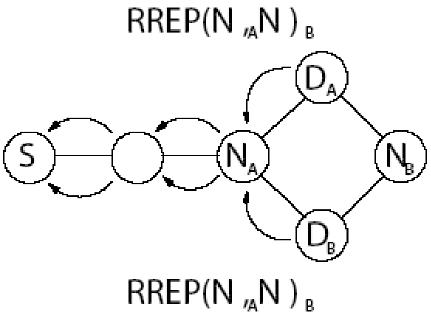


Figure5: The same neighbor list in the Neighbor- D scheme.

3.3 Participation of intermediate nodes

To detect address conflicts, Location-S, Location-D and Neighbor-S, Neighbor-D schemes 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*) or their captured neighboring nodes' addresses (*neighbor__list*) 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, the_location or source_node, neighbor_list. Also, the table entry will be deleted after a timeout (i.e. soft-state scheme). Therefore, when an intermediate node receives RREQ or RREP packets from a source or a destination node using the same address, the location or neighbors 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. Reducing the overhead of flooding is an important and challenging issue [11] [12]. Since this paper focuses primarily on the detection of address conflicts, conflict resolution is beyond the scope of our paper.

3.4. Consideration of Accuracy and Resolution

As mentioned before in Section III-A1 and Section III-B2, Location-S and Location-D schemes utilize location information using wireless localization schemes such as GPS, DOA and TDOA. However, these localization schemes have location errors due to their inaccuracy. In particular, these errors cause different nodes to obtain the same location information. Nodes with different IP addresses do not create any problems in the network, even if they have the same location information. However, nodes with the same IP address and the same location information can cause a problem which cannot be detected by our DAD schemes.

To address this inaccuracy problem in localization schemes, we additionally utilize the time information and the Neighbor Discovery (ND) protocol [14] with a positioning service. Since the basic Location-S and Location-D schemes utilize (longitude, latitude, altitude), the basic schemes can be extended to include the information on the time when each node was configured with its address (in addition to the location information), so that (longitude, latitude, altitude, configured time) is recorded and utilized to execute a DAD. From the difference of the time information, our scheme can detect address conflicts even if nodes have the same IP address and the same location information. If different nodes are configured with the same IP address at the same location and at the same time, they can detect the address conflict with the ND protocol.

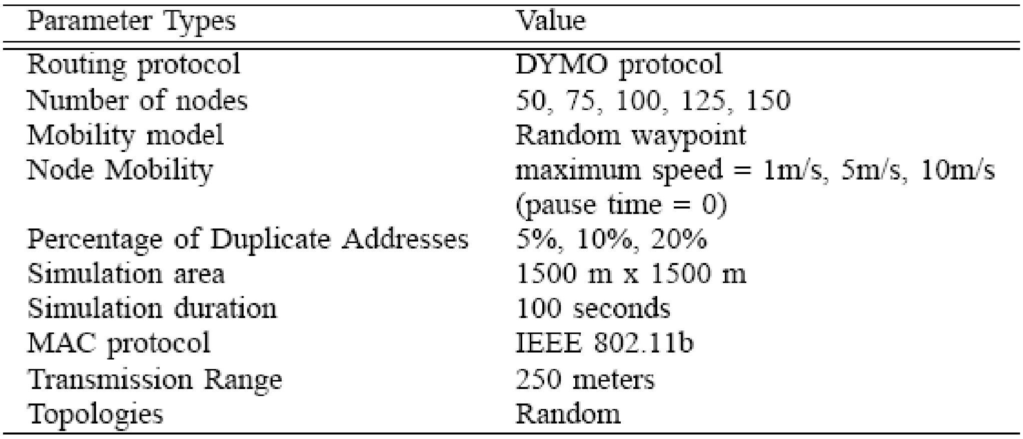
Other information such as a random number might be considered as a means of DAD. For example, techniques using random number generation or hash functions might be applied to our DAD schemes for the secondary identifier such as location and neighbor information. However, these functions still have a probability of collisions even if it is very low. In addition, a similar protocol overhead to ours can occur because including the information into RREQ/RREP packets is required. Moreover, since the hash and the random functions cannot guarantee the uniqueness, it is undesirable to use them for passive DAD schemes

IV. PERFORMANCE EVALUATION

4.1 Simulation Environment

To evaluate performance, we 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” (called pack- etBB) [15], so that additional information (location, neighbor list, etc) can be easily added into the packet header through its TLV (type, length, value) block. We extended the DYMO protocol to support our passive DAD schemes. Detailed sim- ulation 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. 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. All simulation results were plotted with an average of 20 runs.



Parameter Types	Value
Routing protocol	DYMO protocol
Number of nodes	50, 75, 100, 125, 150
Mobility model	Random waypoint
Node Mobility	maximum speed = 1m/s, 5m/s, 10m/s (pause time = 0)
Percentage of Duplicate Addresses	5%, 10%, 20%
Simulation area	1500 m x 1500 m
Simulation duration	100 seconds
MAC protocol	IEEE 802.11b
Transmission Range	250 meters
Topologies	Random

Table 1: Simulation parameters

Our proposed PDAD schemes are performed by source node, destination node, or intermediate nodes. Although each of them can be performed independently, better detection success ratio can be expected by combining these schemes. In our simulations, location based schemes (e.g., Location- S, Location-D, intermediate DAD with location information schemes) were tested, because they have lower routing pro- tocol overhead and less limitations to be applied than other schemes using neighbor or sequence information. The schemes using neighbor list require RREQ/RREP packets to carry the list of neighbor nodes, which needs bigger packet size. In addition, the sequence based schemes can be applied to the detection of address conflicts for destination nodes only. Hence, we investigated performance through two kind of combinations: (a) LOC-SD (Location-S and Location-D without participation of intermediate nodes) and (b) LOC-SD-INT (Location- S and Location-D with intermediate nodes’ participation). Both location and neighbor information based schemes exhibit almost similar performance. The only difference lies in the information type, i.e. location versus neighbors’ list. Hence, we only performed simulations on the location based schemes.

4.2 Evaluation of proposed passive DAD schemes

Important metrics related to passive DAD schemes include: (a) protocol overhead and complexity, (b) detection success ratio, and (c) detection delay. The detection success ratio and detection delay are defined as the ratio of the number of detected nodes to the number of nodes with duplicate addresses, and the time taken to detect address conflicts, respectively. We evaluated the performance with respect to three factors: the number of total nodes in the network (from 50 to 150 nodes), node mobility (from 1m/s to 10m/s) and participation of intermediate node.

4.2.1 Protocol Overhead and Complexity

Compared with ac- tive DAD schemes in terms of overhead, active DAD schemes require a large amount of address allocation time and control overhead For example, RADA and MANET conf which are representative active DAD schemes, need several seconds to complete assigning a unique address to a joining node because control messages for DAD procedures should be flooded into the network. Whenever new nodes come and network merges occur, explicit DAD procedures should be per- formed. This produces much control overhead for exchanging control messages. On the other hand, passive DAD schemes do not re- quire such an explicit DAD procedure while assigning IP addresses to nodes. Hence, the delay and control overhead can be reduced. However, passive DAD schemes have their computational and storage overheads while performing route maintenance procedure, unlike active DAD schemes

In addition, our proposed PDAD schemes require localization and time synchronization schemes. If MANET nodes are equipped with a localization device such as GPS, the location and synchronization capability can be easily provided without any protocol overhead. Alternatively, our schemes can employ various localization schemes such as DOA and TDOA which do not need a special device for localization and are widely used in MANET protocols. As for the time synchronization issue, since the IEEE 802.11 standard [19] provides a time synchronization mechanism for ad hoc mode operation, our proposed scheme can also utilize such synchronization service without additional overhead.

4.2.2 Detection Success Ratio

Figure 7 shows the detection success ratio versus the number of nodes. Initially, 5% 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 7) when the number of nodes was increased from 50 to 125. The average detection success ratio of LOC-SD and LOC- SD-INT increases from 25% to 92% and from 51% to 93%, respectively. When the number of node is more than 125 nodes, both schemes achieve over 90% of detection success ratio, regardless of node mobility. With the same number of nodes and with mobility, higher mobility yields higher detection success ratio. For LOC-SD-INT, when node mobility is increased from 1m/s to 10m/s, the detection success ratio increases by 9% on the average. For the case of 50 nodes, the detection success ratio increases by 31% on the average. This is because higher mobility creates more opportunities to successfully exchange RREQ/RREP packets with other nodes. 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.

4.2.3 Detection Delay

Figure 8 shows the detection delay under varying number of nodes. The detection delay depends on the RTT (Round Trip Time) between source and desti- nation nodes. From Figure 8, when the number of nodes in the network increases, the detection delay also increases. As the number of node increases (from 50 to 150 nodes), the average detection delays of LOC-SD and LOC-SD-INT increase steadily from 47 ms to 93 ms, and from 36 ms to 81ms, respectively. In other words, LOC-SD-INT achieves 19% shorter delay than LOC-SD, on average. 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.

4.2.4 Contribution of DAD

Next, we investigated the extent of each passive DAD scheme’s contribution to detecting address conflicts. Table II shows the simulation results for 125 nodes. Location-S and Location-D schemes contribute to
95.4% and 4.6% of the detection, respectively Location-D does not contribute to the detection remarkably due to the characteristics inherent from most on-demand routing protocols such as AODV and DYMO. Consider the case where multiple destination nodes with the same addresses replied with their RREP packets to an RREQ packet. While intermediate nodes are forwarding the RREP packets, some RREP packets may be discarded due to the following reasons: networks (e.g., from 50 to 100 nodes) with 1 m/s mobility, we observe a low detection success ratio, as compared to other cases. In sparse networks, we achieve 54% of detection success ratio on average. However, in other cases, 91% of detection success ratio is observed. This is because a sparse network causes network partitions or route disconnections between the source and destination nodes to occur frequently. Hence, some duplicated addresses can not be detected since packet transmissions between conflicting nodes may not be performed successfully. For LOC-SD-INT, duplicate address can be detected by intermediate nodes. This explains why LOC-SD-INT has 12% higher detection success ratio than others in sparse networks,

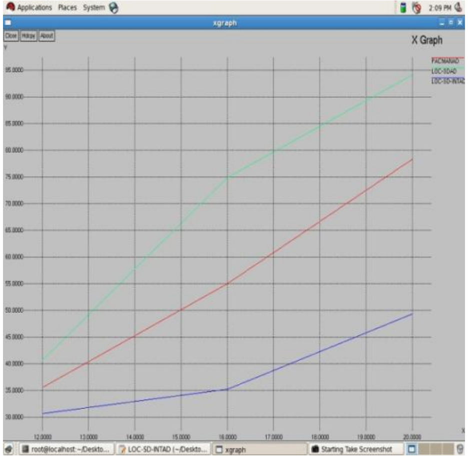


Figure6: average detection delay

In a case where intermediate nodes receive a new RREP packet with the same destination address after they already forwarded an RREP packet, if a Routing-sequence number included in the new RREP packet is less than the Routing-sequence number included in the previously forwarded RREP packet, intermediate nodes discard the new RREP packet according to the DYMO protocol. Thus, the contribution of Location-D is not so high. This is also applied to Neighbor-D. Although Location-D scheme has a relatively low contribution to the detection of duplicated address, it is still needed to improve detection success ratio without any missed detections.

Our scheme using Location-S/Location-D with the par- ticipation of intermediate nodes shows the most significant contribution of 76.7% (see Table II-b). However, the contri- butions of source and destination nodes are 21.7% and 1.7%, respectively (23% in total). This clearly shows the significance of using intermediate nodes for DAD.

4.3 Comparison with an existing passive DAD scheme

We evaluated the performance using three metrics: (a) de- tection success ratio, (b) detection delay and (c) the detection accuracy. From Figure 8 we investigate detection success ra- tio according to node mobility (from 1 to 10m/s). As mobility increases, better detection success ratio is achieved, because more opportunities exist for nodes to exchange RREQ/RREP packets with other nodes. Both LOC-SD and PACMAN can detect address conflicts when the source or destination node receives an RREQ or RREP packet successfully. As a result, they show fairly similar detection success ratio. LOC-SD aims at improving the detection accuracy, not the detection success ratio. Rather than improving the ratio, LOC-SD achieves better detection accuracy, as compared to the PACMAN scheme. nodes' DAD service, it can improve the performance of both the detection success ratio and the detection delay. Figure 8 show the detection success ratio at 1m/s node mobility with various percentage of duplicate addresses (from 5% to 20%). For all the percentages of duplicate addresses, similar results are observed. Hence, the percentage of duplicate addresses does not affect the performance of detection ratio.

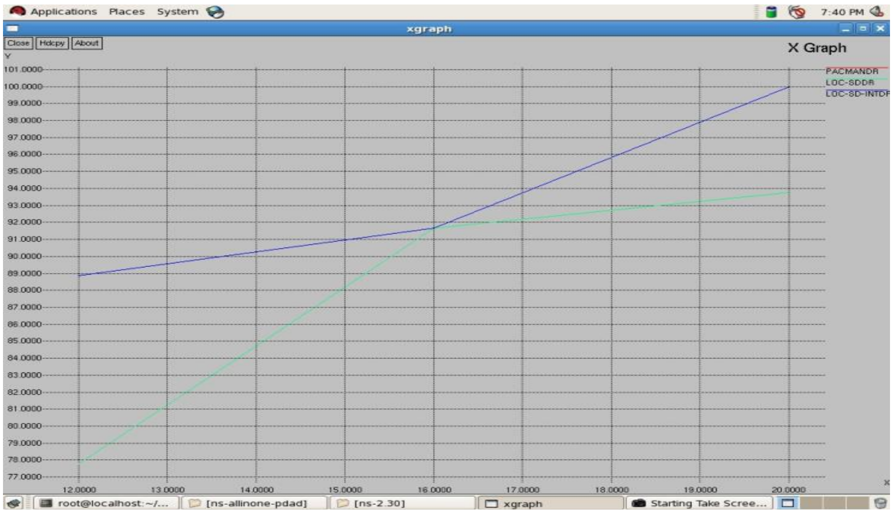


Figure 7 detection success ratio

4.3.1 Comparison of the Detection Delay

The detection delay was measured according to the number of total nodes, node mobility (1m/s, 5m/s and 10m/s) and percentage of duplicate addresses (5%, 10% and 20%). Regardless of node mobility, as the number of nodes increases, the detection delay become no longer. As shown in Figure 8, when increasing the number of nodes, we observe that the detection delay also increases from 52ms to 104ms in PACMAN and increases from 52ms to 100ms in LOC-

SD. However, the intervention of intermediate nodes enables the DAD to be completed before the RTT elapses. As node mobility increases, the overall detection delay decreases. This is because nodes moving at higher speeds tend to create longer hop paths among nodes. As shown in Figures 10a to 10c, when node mobility increases from 1m/s to 10m/s, the average detection delay of LOC-SD-INT decreases from 60ms to 52ms

Figures 10c show simulation results with 10m/s node mobility and various percentages of duplicate addresses (from 5% to 20%). As the percentage of duplicated addresses increases, detection delay decreases, especially when the number of nodes in the network increases.

4.3.2 Comparison of the Detection Accuracy

In the PAC-MAN scheme, a duplicate address can be misdirected. 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 this paper.

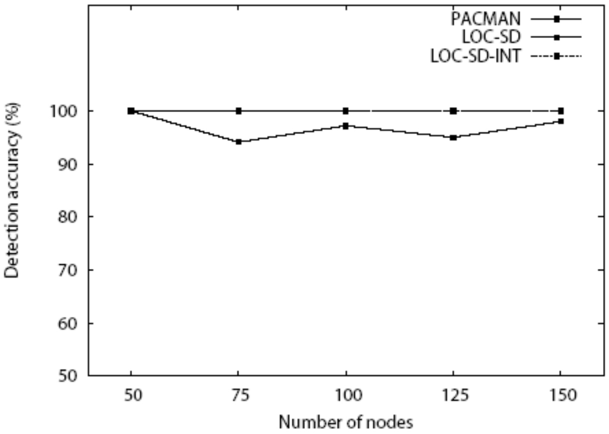


Figure 8: Detection of accuracy of various schemes

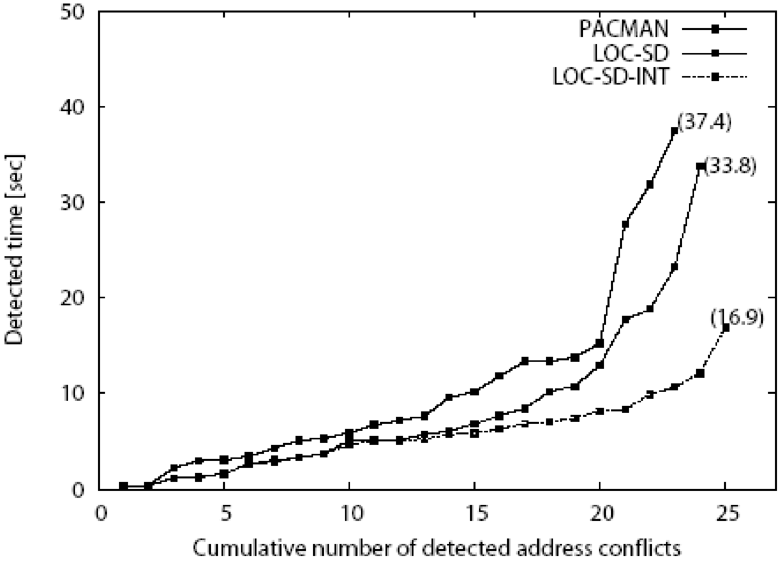


Figure 9: Tracing the DAD execution time of various schemes

We investigated the detection accuracy by measuring the frequency of mis-detections with 10% of duplicate addresses and 5 m/s mobility. Here, the detection accuracy represents the ratio of the number of actual duplicate addresses de- tected to the number of false detections (i.e. RNS-false and 2RoR-false). From Figure 11, we observe that the PACMAN scheme has lower detection accuracy than our schemes (i.e. maximum difference of 7%). There exists none of such RNS- false and 2RoR-false cases through Location-S and Location- D. In addition, our scheme using Sequence-D, Neighbor-S, and Neighbor-D can avoid the occurrence of RNS-false and 2RoR-false successfully. As a result, the PACMAN scheme suffers from poor network resources efficiency caused by these misdetections.

4.3.3 Tracing the DAD Execution Time

We traced the DAD execution time of each duplicate address over simulation time (100 seconds) with 125 nodes and 5 m/s mobility(see Figure 12). Initially, 25 nodes were assigned duplicate addresses. From Figure 12, LOC-SD-INT detects the occurrences of address duplication most quickly and completes all detections at 17s. LOC-SD and PACMAN finish their detections at 34s and 37s, respectively. LOC-SD-INT progresses steadily while detecting all duplicated addresses. PACMAN takes about 15s to detect 20 duplicate addresses. After 15s, PACMAN spends about 20s in detecting three more duplicate addresses. This is because the passive DAD schemes can accomplish the DAD while performing route discovery and maintenance. Thus, if a DAD fails after the exchange of RREQ and RREP packets, the address conflict cannot be detected until a new route discovery from the node is invoked. In this simulation, PACMAN misses several chances to detect address conflicts between 0s and 15s, and it fails to detect five duplicate addresses. In real networks, this is a serious problem that allows duplicate addresses to remain undetected longer and can disrupt data traffic between nodes.

V. CONCLUSIONS

In this paper, In this dissertation, several passive DAD (Duplicate Address Detection) schemes used to quickly and accurately detect address conflicts during route discovery and maintenance over MANET on-demand routing protocols. The main goals which are improved in this project: The accuracy of detecting addresses conflicts, The detection success ratio, and Reduced the time taken to detect these conflicts. By using the simulations (extensive) the ns-2 simulator, PDAD schemes can achieve 100% accurate detection of duplicate addresses with higher detection success ratio when compared to the PACMAN scheme. PDAD schemes utilize sequence number, location of nodes, or a list of neighboring nodes. These information is included into routing control packets (such as RREQ and RREP packets) in order to help detect the duplicate address of source and destination nodes. In addition, the detection success ratio is improved and reduced the detection delay by allowing intermediate nodes to participate in detecting address conflicts.

REFERENCES

[1] Internet Engineering Task Force, “MANET working group charter,”
[2] Dongkyun Kim, Hong-Jong Jeong, C. K. Toh and Sutaek Oh, “Passive Duplicate Address Detection Schemes for on demand Routing Protocols”, IEEE Transaction on vehicular technology,2009
[3] D. Johnson, Y. Hu and D. Maltz, “The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4,” RFC 4728
[4] I. Chakeres and C. Perkins, “Dynamic MANET On-demand (DYMO) Routing,” IETF Internet-Draft, draft-ietf-manet-dymo-16.txt, December2008.
[5] T. Clausen and P. Jacquet, “The Optimized Link-State Routing Protocol (OLSR),” RFC 3626, IETF, October 2003.
[6] Z. Haas, “A New Routing Protocol for the Reconfigurable Wireless Networks” IEEE International Conference on Universal Personal Communications,
[7] Internet Engineering Task Force, “AUTOCONF working group charter,”
[8] S. Mesargi and R. Prakash, “MANETconf: Configuration of Hosts ina Mobile Ad Hoc Network, in Proc. of IEEE INFOCOM 2002, NewYork, USA, June 2002.
[9] N.H. Vaidya, “Weak Duplicate Address Detection in Mobile Ad Hoc Networks,” in Proc. of MOBIHOC 2002, Lausanne, Switzerlan, June2002.
[10] K. Weniger, “PACMAN: Passive Auto configuration for Mobile Ad Hoc Networks,” IEEE Journal of Selected Areas in Communications Vol.23, No.3, March 2005.
[11] J. Wu and F. Dai, “Efficient Broadcasting with Guaranteed Coverage in Mobile Ad Hoc Networks,” IEEE Transactions on Mobile Computing, Vol.4, No.3, May/June 2005.
[12] M. Heissenbuettel, T. Braun, M. Waelchli and T. Bernoulli, “Optimized Stateless Broadcasting in Wireless Multi-hop Networks,” n Proc. ofINFOCOM 2006, Barcelona, Spain, April 2006.
[13] A. El-Rabbany, “Introduction to GPS: The Global PositioningSystem, Second Edition,” Artech House Publishers.
[14] T. Narten, E. Nordmark and W. Simpson, “Neighbor Discovery for IPVersion 6 (IPv6),” RFC 2461, IETF, December 1998.
[15] T. Clausen, C. Dearlove, J. Dean and C. Adjih, “Generalized MobileAd Hoc Network (MANET) Packet/Message Format,” RF 5444, IETF,February 2009.