Overhead Reduction for Duplicate Address Detection in VANET

Kuan-Lan Tseng
Department of Computer Science
National Taichung University of Education
Taichung, Taiwan
balance10629@gmail.com

Tsan-Pin Wang
Department of Computer Science
National Taichung University of Education
Taichung, Taiwan
tpwang@mail.ntcu.edu.tw

Abstract—In VANET, nodes move at high speed and change connecting network frequently. As a consequence, IP duplication may occur and packets would not be sent to the correct destination. This paper aims at reducing the size of location information in duplicate address detection (DAD) scheme. We propose a grid-based duplicate address detection (GDAD) scheme and separate network into several grids, where the location information in the packet is replaced with the grid number. In addition, we model and calculate the probability of occurrence of IP duplication. Finally, we simulate and estimate the probability of IP duplication.

Keywords—vehicular ad hoc networks (VANET), duplicate address detection (DAD), IP auto-configuration

I. INTRODUCTION

With the development of services and applications in vehicular ad hoc networks (VANET), the number of nodes and packets increase dramatically. There are various types of applications in VANET, such as real-time traffic information, entertainment and road safety. With the uniqueness of IP, node can forward the packets with each other successfully. This is especially significant for the services transmitting emergency information. Therefore, confirming the uniqueness of IP in wireless networks is an important issue to investigate.

Passive duplicate address detection [1] is one of the methods to find IP conflict in the network. In PDAD, node attaches information, such as location, neighbor list, and other specific keys, in a packet. Source and destination nodes detect IP duplication after they receive packets. Detecting IP conflict during packet routing can reduce the transmitting overhead and prevent the broadcast storm. The following are two PDAD approaches previously proposed.

In [1], Okada et al. proposed partial-key DAD to reduce the key size of Weak DAD. The basic idea is that the original key is separated into several partial keys, and only one of them is added in a packet. The authors use the sequence number in the control message and the number of partial keys to choose the partial key. Each node maintains a key table to record IPs and the partial keys when receiving packets form other nodes. The more partial keys stored in the key table, the more accurate the DAD. Basically, this manner can reduce the overhead when transmitting the packet. However, this partial key is not long enough to guarantee the uniqueness of IP address.

In [2], Kim et al. attached location or neighbor information in packets. The IP conflict was detected when node receives the packet containing the information which had been already assigned. Besides, nodes will maintain a data structure (table entry) recording the IP and location or neighbor information in the received packet. The IP duplication is detected by not only source and destination nodes but also by intermediate nodes. These approaches not only reduce the detection delay but also improve the accuracy of DAD. However, the overhead of location information would be large. According to the definition of GPS in NMEA (National Marine Electronics Association), both of the longitude and latitude are presented in (dmm.mmmm) format. There are at least 16 bits GPS information attached in a packet.

In this paper, we propose a grid-based duplicate address detection (GDAD) scheme to reduce the size of location information in a packet. Nodes use the grid length, central location of grid and its GPS location to generate grid number and attaches to packets. The idea of grid number is similar to hash function. We transfer the GPS location into the grid number in partition phase. The size of grid number is much smaller than GPS location. When both the grid number and the IP address are conflict at the same time, we may not confirm the duplicated address at a packet. Therefore, we also propose a grid re-partition mechanism to solve this problem. Besides, the length of grid number is relative to the number of network partitions. The more partitions the longer grid number we generate. The longer grid number we generate, the fewer detections we may perform.

The reminder of this paper are organized as follows. Section 2 introduces our grid-based DAD scheme in detail. Section 3 shows the simulation results. Section 4 concludes this paper.

II. GRID-BASED DUPLICATE ADDRESS DETECTION

We separate the network according to the concept of quadtree. The root of a quadtree represents the whole network. In each separation, a grid is separated into four small grids just like each parent node has four child nodes in a quadtree. Fig.1 illustrates the grids in a quadtree and network. Each grid has a
unique grid number, which is represented in binary format. In the initial phase, we separate the network into $4^n$ grids and the length of grid number is $2n$, $n \geq 1$. The value of $n$ represents the execution time of partition and depends on the size of the network. We adopt AODV routing protocol to transmit packets in the network. Besides, our GDAD also allows intermediate nodes joining DAD phase.

![Grids in structure of quadtree](image1)

(a) Grids in structure of quadtree.  
(b) Grids in network

![Network partition](image2)

Fig. 1. Example of nodes in a quadtree.

A. Initial Network Partition

Before transmitting packets, the grid number should be generated first. We assume that nodes additionally maintain an information table containing the grid length, the central location, and the grid number, as shown in TABLE I. The partition includes the following three steps. In Step 1, a node divides the grid length by two. In Step 2, node use mathematical formulae in TABLE II to generate the central location. In Step 3, a node compares the central location and GPS location to obtain 2-bit new grid number, as shown in TABLE III. It is important that this 2-bit grid number will be attached to the original grid number. That is, after a partition, the length of grid number will be increased by two bits. It is necessary that nodes will update the information table after the execution of each step.

![Network partition](image3)

Fig. 2. Example of network partition and the information table of node A.

B. Packet Transmitting and Duplicate Address Detection

After partition, nodes transmit packets containing IP and the grid number. The nodes in the routing path will participate in DAD procedure during packet routing. Fig. 3 describes an example of DAD phase. Fig. 3(a) illustrates the routing path when the source (node C) transmits a packet to the destination (node E). There are three cases in DAD procedure.

1) IP conflict does not detected: Nodes do not receive packets with the same IP address. That is, the IP conflict is not detected. In Fig. 3(a), node C transmits a packet to node E. All of the nodes in the routing path maintain different IP addresses, the IP conflict does not occur.

2) IP conflict occurs: If nodes receive packets containing the same IP and different grid number, the IP conflict is detected. As shown in Fig. 3(b), we assume nodes A and C have the same IP address, $IP_A$. When the packet from node C is transmitted to node A, node A will detect the duplicate address.

3) Both of IP and grid number conflict: The node (discoverer) receives packets containing the same IP and the same grid number. In this situation, the discoverer can not confirm the IP duplication using the received packets. Therefore, it will perform the grid re-partition mechanism. In grid re-partition mechanism, the nodes containing the duplicate IP address execute network partition to generate a

### TABLE I. INFORMATION TABLE

<table>
<thead>
<tr>
<th>Grid Length</th>
<th>Central Location</th>
<th>Grid Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>$L$, $L \leq 1$</td>
<td>$(X,Y)$, $X$, $Y \leq 1$</td>
<td>$2n$ bits binary string, where $n &gt; 0$</td>
</tr>
</tbody>
</table>

### TABLE II. NODES GENERATE NEW CENTRAL LOCATION ACCORDING TO THE GRID NUMBER IN PREVIOUS PARTITION

<table>
<thead>
<tr>
<th>Original Grid Number in TABLE I</th>
<th>New Central Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>$(X-L,Y+L)$</td>
</tr>
<tr>
<td>01</td>
<td>$(X+L,Y+L)$</td>
</tr>
<tr>
<td>10</td>
<td>$(X-L,Y-L)$</td>
</tr>
<tr>
<td>11</td>
<td>$(X+L,Y-L)$</td>
</tr>
</tbody>
</table>

### TABLE III. NODES COMPARE GPS LOCATION: $(X_n,Y_n)$, AND CENTRAL LOCATION: $(X,Y)$ TO GENERATE NEW 2-BIT GRID NUMBER.

<table>
<thead>
<tr>
<th>Location Information</th>
<th>First Bit</th>
<th>Second Bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X_n \leq X$</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>$X_n &gt; X$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>$Y_n \leq Y$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>$Y_n &gt; Y$</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
tentative grid number and forward to the discoverer. The discoverer checks the grid duplication. The grid re-partition will be performed in a recursive way until the IP duplication is confirmed or detected. When the IP conflict is detected, nodes will generate a new IP address. The tentative information will be discarded. Therefore, the grid re-partition mechanism will not change the value in the information table. In Fig. 3(c), we assume that node B and node D have the same IP address, IP_B. When nodes B and D send packets to node E, node E detects both IP and grid number are conflict. Node E notifies nodes B and D to perform the grid re-partition mechanism. Fig. 3(d) shows that node B and node D generate different tentative grid number after executing grid re-partition. Consequently, node E detects the duplicate address.

Fig. 3. Example of DAD phase.

III. EVALUATION

In this section, we use the concept of combination to evaluate the probability of occurrence of IP conflict. Besides, in GDAD, the GPS information is replaced with grid number. To obtain the improvement ratio, we calculate the packet size which contains GPS information and grid number respectively.

A. Probability of Occurrence of IP Conflict

The probability of occurrence of IP conflict is defined as the ratio of the number of combination with IP duplication to the number of combination when assigning the IP to the nodes.

\[
P = \frac{\binom{IP + \text{Node} - 1}{\text{Node}} - \binom{IP}{\text{Node}}}{\binom{IP + \text{Node} - 1}{\text{Node}}}\]  

(1)

Fig. 4 shows the probability of occurrence of IP conflict with various numbers of nodes. It shows that when there are 100 nodes, the probability of IP conflict is almost 100%. This value emphasizes that the situation of IP duplication is inevitable in the network.

Fig. 4. Probability of occurrence of IP conflict with various numbers of nodes

B. Packet Size

We evaluate the packet size of GDAD containing the grid number and GPS information separately in the AODV packets. The GPS information in our evaluation only includes longitude, latitude and two directions, which are 18 bits in total. The location information in GDAD are 2 bits, 4 bits and 6 bits, which represent the network implements 1, 2 and 3 partitions.

Fig. 5 illustrates the route request (RREQ) message format in AODV. The packet size is 192 bits. The evaluation results are shown in TABLE IV. Another packet format is route reply (RREP) message format and the packet size is 160 bits, as shown in Fig. 6. The evaluation results are shown in TABLE V.

Fig. 5. Route request (RREQ) message format

<table>
<thead>
<tr>
<th>Packet Size with GPS Information</th>
<th>Packet Size in GDAD</th>
<th>Reduction Bits</th>
<th>Percentage of Reduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>192+18=210</td>
<td>192+2=194</td>
<td>210-194=16</td>
<td>7.6%</td>
</tr>
<tr>
<td>192+18=210</td>
<td>192+4=196</td>
<td>210-196=14</td>
<td>6.6%</td>
</tr>
<tr>
<td>192+18=210</td>
<td>192+6=198</td>
<td>210-198=12</td>
<td>5.7%</td>
</tr>
</tbody>
</table>

Table IV. Packet Size of RREQ Message Format (BITS)

Fig. 6. Route Reply (RREP) message format
As shown in TABLE IV and TABLE V, the reduction percentage in RREQ and RREP message format ranges from 5.7% to 8.9%. Another method to reduce more packet size is attaching the grid number in reserved field. For example, the reserved field in RREP message format is 8 bits. The network can execute at most 4 network partitions, and contains $4^4$ grids. This is large enough to confirm the IP duplication in the DAD procedure.

### IV. SIMULATION RESULTS

In this section, we simulate grid-based duplicate address detection in C program. We generate random number to assign IP and grid number for each node. The range of random value is from 0 to 32767. The number of IP addresses is 1000. We estimate the probability of the Case 2 and Case 3 in DAD phase in different scenarios. To obtain simulation results, we perform simulation of each scenario for 1000 times. The detail simulation parameters are shown in TABLE VI.

<table>
<thead>
<tr>
<th>Parameter Types</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Programming Language</td>
<td>C</td>
</tr>
<tr>
<td>Number of experiments</td>
<td>1000</td>
</tr>
<tr>
<td>Number of IP addresses</td>
<td>1000</td>
</tr>
<tr>
<td>Number of nodes</td>
<td>100, 200, 300, 400, 500</td>
</tr>
<tr>
<td>Number of grids</td>
<td>4, 16, 64</td>
</tr>
<tr>
<td>Topologies</td>
<td>Random</td>
</tr>
</tbody>
</table>

### A. Probability of IP Duplication

Fig. 7 illustrates the probability of Case 2 and Case 3 with respect to the numbers of nodes. The probability of Case 2 and Case 3 rises when the number of nodes increases. This is because the high density of node increases the chance of nodes sharing the same IP address. Furthermore, the probability of nodes assigned different grid numbers is much higher than the probability of nodes sharing the same grid number. As shown in Fig. 7, the probability of Case 3 is low, as compared with the probability of Case 2.

![Fig. 7. Probability of Case 2 and Case 3 with various number of nodes.](image)

Fig. 8 shows the probability of Case 2, Case 3 and IP conflict (Case 2+ Case 3) with various numbers of grids. The probabilities of IP conflict are nearly 0.005 with different numbers of grids. As the number of grids increases, the probability of Case 2 increases; however, the probability of Case 3 decreases. The probability of Case 3 is almost 0 when the number of 64 grids is assumed. It is obvious that the area of grid affects the probability of IP conflict. When the area of grid decreases, the number of nodes locating in the same grid decreases. The results indicate that partitioning network into large number of grids can reduce the number of implementing grid re-partition procedure.

![Fig. 8. Probability of case 2 and case 3 with different number of grids.](image)

Fig. 9 illustrates the probability of Case 2 and Case 3 with various numbers of grids and several numbers of nodes. In Fig. 9(a), the probability of Case 2 rises when the number of grids increases. When the number of grids changes from 16 to 64, the probability of Case 2 increases only slightly. The possible reason is that the density of nodes is not high enough to reveal the advantage of network partition. In other words, the performance of GDAD is flat in the sparse network. Fig. 9(b) depicts that the probability of Case 3 reduces by approximate 4 times when the number of nodes rises from 4 to 16, 16 to 64. The reason is that, in GDAD, the number of grids increases by 4 times after executing a network partition. As a result, the number of grids can be assigned rises by 4 times.

![Fig. 9. Probability of IP conflict with various numbers of grids and nodes.](image)
V. CONCLUSIONS

IP duplicate address detection is essential due to high mobility of vehicles in wireless vehicular networks. In this paper, we propose a grid-based scheme to reduce the overhead attached in packets for duplicate address detection. We attach only the grid number in the packet instead of all GPS information. The proposed grid re-partition procedure can deal with the nodes maintaining the same IP address and the same grid number. Finally, the simulation results show that the probability of IP conflict depends on the number of grids. The more grids, the few grid re-partition will be executed. Besides, according to the performance results, the packet size in GDAD is smaller than the one with all GPS information.

ACKNOWLEDGMENT

This work was supported in part by the Science Council under grant No. NSC 102-2221-E-142-006-, Taiwan.

REFERENCES


