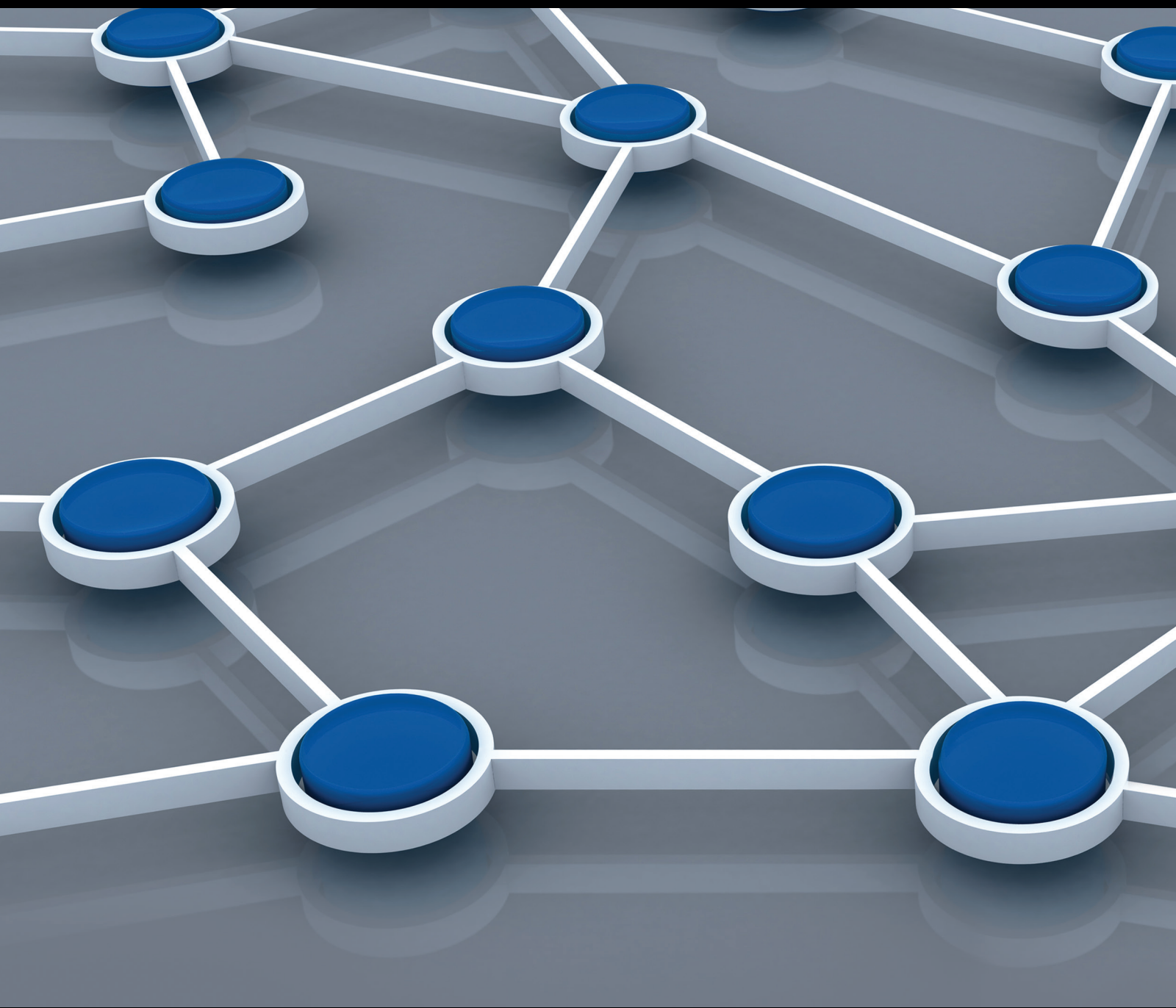
International Journal of Distributed Sensor Networks

Advances in Vehicular Ad Hoc Networking and Applications

Guest Editors: Liusheng Huang, Chunming Qiao, Limin Sun, Shukui Zhang, and Xu Li



Advances in Vehicular Ad Hoc Networking and Applications

International Journal of Distributed Sensor Networks

Advances in Vehicular Ad Hoc Networking and Applications

Guest Editors: Liusheng Huang, Chunming Qiao, Limin Sun, Shukui Zhang, and Xu Li

Editorial Board

Contents

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2014, Article ID 906084, 17 pages
http://dx.doi.org/10.1155/2014/906084

Research Article

Non-GPS Data Dissemination for VANET

Kulit Na Nakorn and Kultida Rojviboonchai

Department of Computer Engineering, Faculty of Engineering, Chulalongkorn University, Bangkok 10400, Thailand

Correspondence should be addressed to Kultida Rojviboonchai; kultida.r@chula.ac.th

Received 12 April 2013; Revised 27 October 2013; Accepted 12 November 2013; Published 29 January 2014

Academic Editor: Xu Li

Fast, reliable, and efficient data dissemination in VANET is a key of success for intelligent transportation system. This requires a broadcasting protocol which has efficient forwarder nodes and an efficient broadcasting mechanism. In this paper, we propose a self-decision algorithm that allows a node to know that it belongs to a member of connected dominating set or not. The algorithm is a combination of density based algorithm and topology based algorithm, called "DTA." The algorithm does not require any geographical knowledge. Therefore, it can avoid violating a privacy issue. Moreover, the algorithm can resist inaccurate data than position-base algorithms that need high frequent beaconing for accurate data. The simulation results show that our algorithm provides the highest coverage results compared to existing solutions. We also propose a new broadcasting protocol, called "NoG." NoG consists of a broadcasting mechanism, a waiting timeout mechanism, and a beaconing mechanism. The proposed protocol operates without any geographical knowledge and provides reliable and efficient data dissemination. The performance is evaluated with a realistic network simulator (NS-3). Simulation results show that NoG with DTA outperforms other existing protocols in terms of reliability and data dissemination speed.

1. Introduction

Vehicular ad hoc network (VANET) is one of mobile ad hoc networks (MANET). Vehicles in the network are equipped with wireless communication devices. Therefore, they can directly communicate to each other without infrastructure and without centralized control. The data can be quickly delivered to applications. This can support some applications of intelligent transportation system (ITS) such as driver assistant or safety transport applications. These applications need a fast and reliable solution for data dissemination to provide accurate and reliable services [1]. So the efficient data dissemination is one of the key successes for such applications. To achieve this, the unique characteristic of vehicle environment should be considered. Vehicle's movement changes frequently and rapidly. The speed of vehicles also affects wireless signal that leads to high intermittent connectivity occurrences between vehicles. Moreover, vehicles may be very densely packed in urban areas but are very sparse on highway roads or in rural areas.

A traditional approach for data dissemination or broadcasting for wireless ad hoc networks is simple flooding. Simple flooding does not require any information from environment or nodes. A packet is rebroadcasted once by every received node. This approach can provide very high data dissemination speed. However, simple flooding may cause the contention and collision [2] due to its redundant transmission in dense areas and it may cause useless broadcasting as there is no neighbor to receive data in sparse area [3]. Epidemic protocol [4] was proposed to improve the performance in sparse areas by using store and forward technique. So upon receiving of a broadcasting packet, nodes will store the packet and forward it later when nodes meet a new neighbor. Then this technique has been employed to most of broadcasting protocols in VANET because it can handle the intermittent connectivity issue. As a result, reliability or delivery ratio is increased.

In VANET, several reliable broadcasting protocols have been proposed. We can categorize these reliable broadcasting protocols into 2 groups by their main algorithm. In the first group, the protocols make their decision based on node position such as EAEP [5], APBSM [6], POCA [7], and DV-Cast [8]. These protocols prefer nodes at the edge of broadcasting circular to rebroadcast the packets. All of

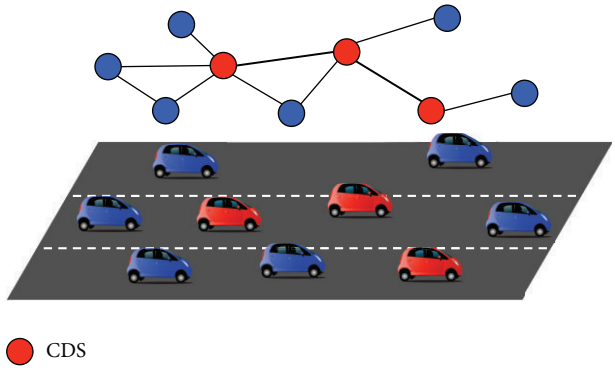


Figure 1: An example of connected dominating set (CDS).

protocols in this group rely on geographical knowledge. They use position or direction of nodes to make decision. In the second group, the protocols make their decision based on node's properties such as DECA [9]. The properties of nodes that are used in these protocols are number of one-hop neighbors (density) or relation between nodes and their neighbors (topology). So these protocols do not require any geographical information to make decision.

However, every algorithm in every protocol has the same goal. The goal is to minimize the number of rebroadcast nodes that can cover all of their neighbors in each group. This can minimize number of retransmissions for delivering a packet to most of nodes in networks. This problem can be solved by minimum connected dominating set (CDS). This algorithm can construct graph and select the minimum number of nodes to cover 100% of their neighbor nodes in each group as shown in Figure 1, but the algorithm requires global knowledge and the CDS computation is an NP-complete problem [10]. Therefore, an approximation algorithm is a practical solution that can construct CDS. Some previous works have been proposed for general mobile ad hoc networks such as [11–14]. These algorithms are self-decision algorithm. This means each node will decide by itself whether it is in CDS or not. Most of them make decision based on topology properties. However, these algorithms have high complexities and they are not specifically designed for vehicular environment.

In this paper, we focus on a nongeographical knowledge based CDS forming algorithms. These methods can avoid privacy issue that most of users are concerned with. Moreover, the nongeographical knowledge based algorithms can resist inaccurate data than position-base algorithms that need high frequent beaconing for accurate position data. We propose a hybrid algorithm, that is, a combination of density based algorithm and topology based algorithm (DTA). DTA has advantage points from both density based algorithm and topology based algorithm. The density based algorithm is a simple algorithm that works well in simple connection scenarios. On the other hand, a topology based algorithm is a complex algorithm that efficiently works in complex connection scenarios. So DTA is an appropriate algorithm for vehicular environment that has such a dynamic topology. We evaluate our algorithm by simulations. The evaluation is focused on coverage results and the ratio between CDS members to total nodes. DTA can provide the highest coverage results than other algorithms.

We also propose a nongeographical broadcasting protocol (NoG). It is designed to provide the fast, reliable, and efficient data dissemination in VANET. The broadcasting protocol consists of a broadcasting mechanism, a waiting timeout mechanism, and a beaconing mechanism. NoG is implemented with our proposed DTA algorithm in NS-3. The simulation results show that NoG with DTA outperforms other previous protocols in terms of reliability and data dissemination speed. NoG also operates well with other algorithms.

The rest of this paper is organized as follows. In Section 2, the related works are discussed. Section 3 describes the overview and details of density and topology based CDS forming algorithm (DTA). Section 4 describes the overview and details of nongeographical Broadcasting Protocol (NoG). The performance evaluation is reported in Section 5. Finally, this paper is concluded in Section 6.

2. Related Work

We discuss more details on the previously mentioned protocols in Section 2.1 and the nongeographical knowledge algorithm is discussed in Section 2.2.

2.1. Broadcasting Protocol in VANET. Simple flooding is a traditional approach for broadcasting. It provides very high data dissemination speed, but all nodes will participate in rebroadcasting packets. This causes the broadcast storm problem due to redundant retransmissions. Epidemic protocol [4] is the most simple store and forward protocol. It can handle an intermittent connectivity in VANET, but all nodes still rebroadcast packets the same as simple flooding. So the broadcast storm problem is still found in epidemic protocol.

There are many previous broadcasting protocols for VANET that we have found in the works of the literature. These protocols use store and forward technique to handle intermittent connectivity that frequently occurs in vehicular environment. All protocols reduce the number of redundant retransmissions by self-decision algorithm. We can categorize these protocols into two groups based on their self-decision algorithm. The first group makes a decision based on position of node. These protocols prefer nodes at the edge of broadcasting circular to rebroadcast the packets. All of protocols in this group rely on geographical knowledge (GPS). The protocols use position or direction of nodes to make decision. This can cause privacy issue [15–17] because nodes need to broadcast their location to the others to exchange the geographical knowledge. A malicious node can track the past and current positions of these nodes. The treats that are from position tracking are discussed in [18]. The protocols in this group include PGB [19], POCA [7], EAEP [5], POCA [7], DV-Cast [8], and APBSM [6].

PGB [20] (preferred group broadcast) is a broadcasting mechanism in CAR protocol. When nodes receive a packet, they calculate the waiting timeout. A node with the shortest

timeout will rebroadcast the packet. Nodes at the edge of broadcasting circular have shorter waiting timeout than nodes that are closer to the source. However, PGB is used for routing information broadcasting, so it does not concern about a reliability issue.

EAEP [5] (edge-aware epidemic protocol) uses both the waiting timeout and probabilistic function. The waiting timeout is calculated by distance between nodes and source nodes. While the waiting timeout does not expire, nodes will count number of redundant retransmissions. The number of redundant retransmissions is used to calculate rebroadcast probabilistic value. Nodes at the edge of broadcasting circular have higher probability value than other nodes.

POCA [7] (position-aware broadcasting protocol) uses the geographical knowledge to select the next rebroadcast node. A node, that is, the furthest node to source node, will be selected by source node. The source node piggybacks the selected node's identifier to the broadcasting packet. The selected node will immediately rebroadcast once it receives the packet. This mechanism avoids the delay from waiting timeout.

DV-Cast [8] (distributed vehicular broadcast protocol) uses the broadcast suppression mechanism. A node, that is, the furthest node to source node, has the shortest waiting timeout, but if a node meets another node in the same direction of broadcasting packets, it will immediately rebroadcast the packets. This is because a node in the same direction of packets can help source node to forward the packets while it is running.

APBSM [6] (acknowledged parameterless broadcasting in static to highly mobile wireless ad hoc) is an extended version of PBSM. Nodes in APBSM use position of their neighbors to construct CDS. The CDS is calculated by Stojmenovic's algorithm [14], which is a combination of self-decision CDS forming from Wu and Li's algorithm and rebroadcast node elimination in scalable broadcast algorithm (SBA). Both of Wu and Li's algorithm and SBA will be discussed later in Section 2.2. Stojmenovic's algorithm uses geographical knowledge to select CDS members. In the case that a node is a CDS member, it will set shorter waiting timeout than other nodes. While timeout does not expire, the algorithm uses the rebroadcast node elimination the same as in SBA.

The other group of protocols makes a decision by node properties. The decision relies on comparison of node properties, so the protocols in this group can avoid using the geographical knowledge. These protocols use the density information (number of 1-hop neighbors) or the topology information, such as a list of 2-hop neighbors and relationship between neighbor nodes. The interesting protocol in this group is DECA [9].

DECA [9] (density-aware broadcasting protocol) relies on only the density information. A source node makes a decision by selecting its neighbor with the highest number of 1-hop neighbor nodes. Upon receiving the packet, the selected node will immediately rebroadcast it to avoid delay from waiting timeout. DECA also uses an adaptive beaconing mechanism to reduce overhead in dense areas.

However, most of nongeographical knowledge protocols are designed for general mobile ad hoc networks. But the CDS forming algorithms for these protocols are interesting because they can operate without any geographical knowledge.

2.2. Nongeographical Knowledge CDS Forming Algorithm. These CDS forming algorithms efficiently select CDS members and they also eliminate unnecessary retransmissions without any geographical knowledge.

Wu and Li's algorithm [11] proposed a self-decision algorithm to determine nodes in CDS, called gateway node. To be a CDS member, a node has to pass all three conditions. The first condition is an intermediate node condition. A node has to have at least two neighbors that are not directly connected to each other. The second condition is an intergateway node condition. A node has to have at least one neighbor, that is, not covered by its other neighbors. Let N_A be a set of node A's neighbors and N_{NB} a set of neighbor nodes of A's neighbors. If $N_A \subseteq N_{\mathrm{NB}}$, node A will be eliminated from CDS because all of A's neighbors can be covered by its other neighbors. The final condition is a gateway condition. A gateway node has at least a neighbor, that is, not covered by a pair of gateway node's neighbors and these two neighbors also are neighbors of each other. For example, let node A be a node that considers its gateway condition. A needs to have at least a neighbor (D), that is, not covered by a pair of A's connected neighbors (B and C). If A is a gateway node, the neighbor (D) is not covered by B or C. Therefore, N_A is not a neighbor of B or C. Let N_A be a set of node A's neighbors, N_B a set of node B's neighbors, and N_C a set of node C's neighbors. B and C are neighbors of node A. If $\{B, C\} \in N_A$, $\{C\} \in N_B$, $\{B\} \in N_C$ and $N_A \subseteq N_B \cup N_C$, node A will be eliminated from CDS. Therefore, nodes in CDS are only the necessary nodes for covering the other nodes in the group.

LENWB [12] (lightweight and efficient network-wide broadcast) uses a set of 1-hop neighbors to eliminate unnecessary rebroadcast nodes. When nodes receive a packet, they will estimate the neighbor list of source node by number of their 1-hop neighbors. If a source node has higher number of 1-hop neighbors than the received nodes, this means that the source node may cover all neighbors of received nodes so the received nodes will not rebroadcast the packets. Otherwise the received nodes will randomly set backoff delay and rebroadcast the packet. If nodes have the same number of 1-hop neighbors, the algorithm will compare with values of node identifiers.

SBA [13] (scalable broadcast algorithm) has the similar elimination algorithm as found in LENWB. Upon receiving the broadcasting packet, nodes calculate the waiting timeout. While the waiting timeout does not expire, nodes will remove the rebroadcast nodes' neighbors from their neighbor list. If the neighbor list does not empty after waiting timeout, they will immediately rebroadcast the packet.

These algorithms are based on topology properties. They use 1-hop neighbor list or 2-hop neighbor list to select the CDS members. The advantage is that these algorithms do not require any geographical knowledge, but they are designed

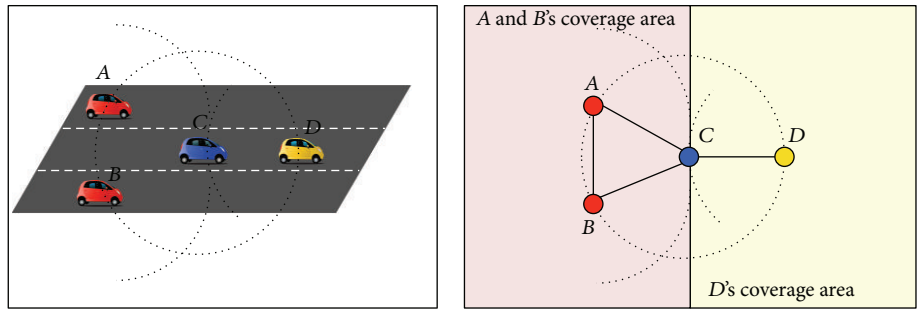


Figure 2: An example of gateway condition.

for general mobile ad hoc networks that may not be efficient in vehicular environment.

3. New Density and Topology Based CDS Forming Algorithm

Section 3.1 presents the motivation and the new density and topology based algorithm overview. Section 3.2 describes the details of the proposed algorithm.

3.1. Motivation and Overview. The unique characteristic of vehicular environment is the speed of nodes. Node's movement changes frequently and rapidly. So beacon messages have to be frequently broadcasted to provide the accurate geographical knowledge to position based protocols. This can cause the broadcast storm problem from beacon transmission. The information from equipment like GPS device also does not provide accurate data due to GPS drift. Moreover, broadcasting location data that can be tracked by unknown people may be concerned as privacy violation [15–17]. Therefore, we propose a new algorithm for CDS forming that does not require any geographical knowledge. It uses only density information (number of 1-hop neighbors) and 2-hop neighbor list that can be exchanged by beacon message.

Another interesting characteristic of vehicle environment is that vehicles always form groups. The vehicle environment is a nonuniform distribution and the topologies are mixed with very dynamic density environment; for example, the density is very sparse in highway scenarios, but nodes are very densely packed at the middle of intersection in urban areas. The algorithms need to be adaptable to each environment. So the algorithm should consider a node with the highest number of 1-hop neighbors to rebroadcast a packet because it can maximize a number of received nodes while minimizing a number of rebroadcast nodes. This algorithm works well for all sizes of group in every scenario. Therefore, DTA uses the number of 1-hop neighbors as a primary condition for algorithm. A node with the highest number of 1-hop neighbors is a CDS member.

However, only nodes with the highest density cannot cover all nodes in high density and complex scenarios, so DTA uses a topology based decision to increase the coverage results. In the case that nodes do not satisfy the density condition, they will use a topology based condition for their decision. Our topology based decision is a simplified version of Wu and Li's algorithm. DTA employs only the gateway condition, that is, the most important condition especially on vehicular environment because the vehicular environment (a road) consists of narrow and long distance topology. The standard width of a road in US is 3.4 meters in each lane [18], but the maximum transmission range of 802.11p is up to 1000 meters [20]. Therefore, the width of the road is much less than the width of transmission range. For example, a pair of connected neighbors (A and B) can cover the red area behind node C as shown in Figure 2. If node D does not exist in this scenario, C will be at the edge of the group, so C is unnecessary to rebroadcast the message. Otherwise, if D exists, C is a connector between A, B (red area) and D (yellow area). In this case, C is considered as a gateway node because C has a neighbor (D), that is, not covered by a pair of C's connected neighbors (A and B). This scenario shows that the gateway condition is an important condition for CDS member selection.

3.2. Algorithm Detail. Upon receiving of a new beacon, a node always updates its CDS state. There are two conditions for checking CDS state. First, a node has to check a density based condition. If a node has the highest number of neighbors compared to its neighbors, it will be a CDS member. The other nodes that do not have the highest density will use a topology based condition. If they complete the condition, they will be CDS members. Otherwise they are not the CDS members. The procedure of DTA can be described as shown in Procedure 1.

4. New Nongeographical Knowledge Broadcasting Protocol for VANET

Nongeographical Knowledge Broadcasting Protocol (NoG) consists of three main modules: (1) broadcast mechanism that uses our DTA for CDS forming, (2) waiting timeout mechanism that is used for collision avoidance, and (3) beacon mechanism that helps nodes to exchange their local information and it helps nodes to detect the missing packet. Section 4.1 describes the protocol mechanism overview

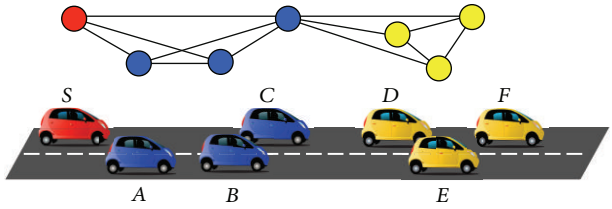


Figure 3: A normal broadcasting scenario.

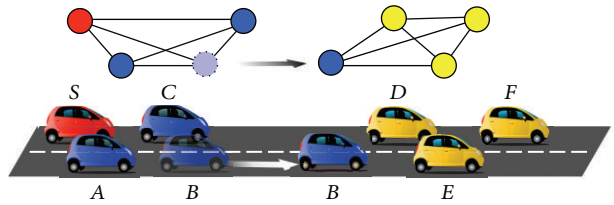


Figure 4: An intermittent connectivity scenario.

and Section 4.2 explains the details of each module in our protocol.

4.1. Protocol Overview. Our proposed broadcasting protocol is a store and forward protocol with adaptive beacon intervals. A node uses beacon to exchange its information between its neighbors. The beacon includes a number of 1-hop neighbors, a 1-hop neighbor list, and a received packet identifier list. A node in protocol makes a decision by itself from this information whether to be a CDS member or not. If it is a CDS member, upon receiving the broadcasting packet, it randomly sets very short backoff delay (<10 ms.). After the delay expires, it immediately rebroadcasts the packet. The nodes that are not CDS members set their waiting timeout with longer period than CDS members. While waiting timeout does not expire, they are listening to rebroadcasting from the other nodes. If they hear any rebroadcasting of the same packet in their waiting list, they will remove this packet from their waiting list to avoid redundant retransmissions.

For intermittent connectivity scenarios, NoG can detect a missing packet via an acknowledgement from the beacon. If there are some missing packets, a node will set their waiting timeout. If other nodes do not rebroadcast the packet before its waiting timeout expires, it will retransmit this packet to its neighbors.

Let us show the examples of protocol behaviors in a normal broadcasting scenario and in an intermittent connectivity scenario.

Figure 3 shows a normal broadcasting scenario. S is a source node. Let C be a node that has the highest local density, so C will be a CDS member. When S broadcasts a packet, A, B, and C receive the broadcasting packet. A and B calculate their waiting timeout and wait for rebroadcasting from CDS members. C, that is, a CDS member, will randomly set very short backoff delay before it rebroadcasts the packet. In the case that C correctly rebroadcasts the packet, A and B will cancel their waiting timeout to avoid redundant retransmissions. On the other hand, if C does not rebroadcast the packet, one of A and B that has the shortest waiting timeout will rebroadcast the packet. Let B have the shortest waiting timeout, so B rebroadcasts the packet instead of C. A will cancel its waiting timeout not causing redundant retransmission. This mechanism will occur until all nodes in the group receive the packet or until the packet is expired.

In another case, there is an intermittent connectivity scenario. A node needs to retransmit the packet between groups of nodes. The scenario is illustrated in Figure 4. Nodes A, B, and C already received the broadcasting packet from S. When B overtakes other vehicles, it leaves from the old group and joins a new group. Nodes in a new group are D, E, and F. They never receive the broadcasting packet from S. B can detect the missing packet via acknowledgement from D, E, and F's beacon. B will set its waiting timeout and it will rebroadcast the packet to other nodes. When D, E, and F receive the packet, then they act as the normal broadcasting scenario. The members of CDS almost immediately rebroadcast the packet and others set the longer waiting timeout than CDS members. The mechanism occurs until all of nodes receive the packet or until the packet is expired.

4.2. Protocol Detail. Each node in NoG has two lists: *neighbor list* and *broadcast list*. *Neighbor List* maintains identifiers of all 1-hop neighbors and their neighbor information (a number of 1-hop neighbors and a 1-hop neighbor identifier list). When nodes receive a new beacon, they will update their *Neighbor List* and they also update their CDS state. The neighbor entry will be removed if nodes do not receive an updated beacon from their neighbors within the next beacon intervals so nodes can avoid using stale information from the neighbors that currently stay out of their transmission range. *Broadcast List* maintains the identifiers of broadcasting packets and their waiting timeouts. *Broadcast List* is a list of packets that are waiting to be rebroadcasted. An entry of *Broadcast List* will be removed by two events. The first one is that nodes rebroadcast the packet when waiting timeout expires. The other one is when nodes receive the redundant retransmission from their neighbors. The entry will be removed although the waiting timeout still does not expire. Pseudocode 1 describes the pseudocode of the protocol. The details of main modules are explained as shown in Pseudocode 1.

4.2.1. Waiting Timeout Mechanism. Waiting timeout is a solution to avoid broadcasting collision in distributed system. Nodes will randomly set their waiting timeout as backoff delay for rebroadcasting. There are two events that use waiting timeout. The first event is when nodes receive the broadcasting packet, but they are not members of CDS. They will add the packet to *Broadcast List* and set waiting timeout. These nodes have to listen to the rebroadcasting by their neighbors that are CDS members. If waiting timeout is expired and no CDS members rebroadcast the packet, a node with the shortest waiting timeout will rebroadcast the packet. The second event is when nodes detect the missing packet from their neighbors. They add the packet to *Broadcast List* and set waiting timeout the same as the first case. As a result,

```
Procedure cds-state(a);
cds(a) = true;
//density based condition
for each neighbor b of a do{
    if noNeighbor(b) > noNeighbor (a) then
        cds(a) = false;
}
//topology based condition
if cds(a) = false then{
    cds(a) = true;
    for each neighbor b of a do{
        for each neighbor c of a, b ≠ c do{
            if b and c are neighbor to each other then
                cover =true;
                for each neighbor d of a, d ≠ b, d ≠ c do{
                    if d is not neighbor of b and c then
                        cover = false;
                }
                if cover = true then cds(a) = false;
}}}
```

Procedure 1: DTA procedure.

```
Initialize (node a)
P: received packets buffer, N: neighbor list
B: broadcast list

Event receiving a broadcasting packet p
If {p} ∉ P then{
    add p to P;
    if cds(a) = true then
        rebroadcast p with randomly delay (<10 ms.);
    else
        add p and waiting timeout to B;
}else{
    remove p and cancel waiting timeout from B;
}

Event receiving a beacon from neighbor n
if {n} ∉ N then{
    add n and beacon expire time to N;
}else{
   update n and beacon expire time to N;
}
//update CDS state of node a
cds-state(a);
for each packet p in P
    if id(p) does not contain in list of pkt. of n then
        add p and waiting timeout to B;
missPacket = false;
for each packet identifier id(q) in list of pkt. of n
    if id(q) does not contain in P then
        missPacket = true;
if (missPacket) then
    if a never send beacon within this interval then
        send beacon(a);
```

Pseudocode 1: NoG pseudocode.

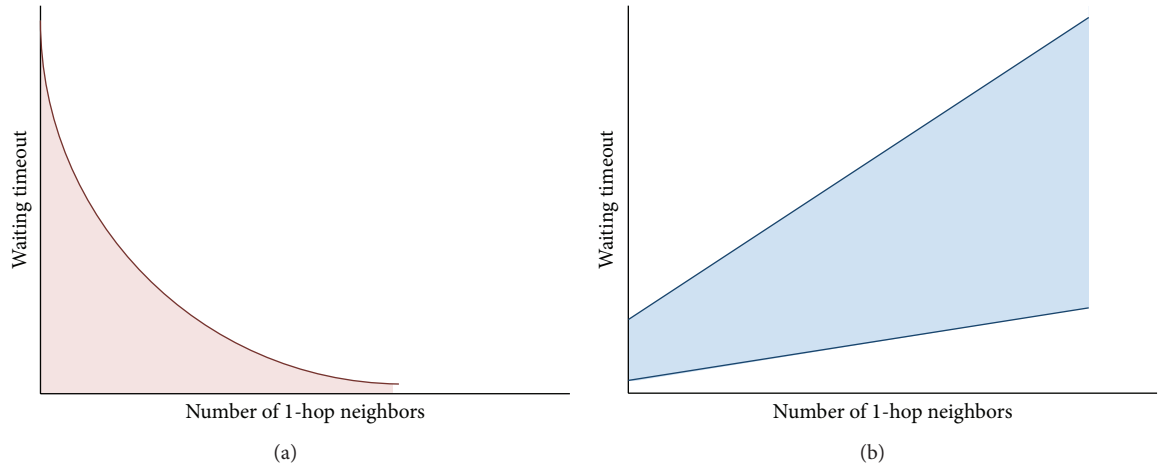


Figure 5: Waiting timeout function. (a) Reversed function. (b) Directed function.

a node with the shortest waiting timeout will rebroadcast the missing packet to its neighbors. These two events are explained in Pseudocode 1.

The disadvantage of waiting timeout is that it increases delay to overall system. Most of previous works calculate their waiting timeout as a reversed function to number of 1-hop neighbors. The purpose is to maximize number of received nodes in each retransmission by a node with the highest number of 1-hop neighbors, but this leads to a contention problem. It also increases extremely high redundant retransmissions in high density scenarios. The reason is that when nodes are in the dense areas, the reverse function calculates very short range of delay. For this reason, most of nodes in the same area will have the same waiting timeout. Then they simultaneously rebroadcast the packet causing collision. In order to prevent such situation, protocols should use the number of 1-hop neighbors to be directed variation of waiting timeout function. As reported in [21], the directed function can prevent collision in extremely high density scenarios. This new waiting timeout also increases the data dissemination speed in sparse areas. Since the directed function provides much shorter waiting timeout period than the inversed function in sparse area, the data dissemination speed can be increased.

The waiting timeout can be calculated by (1). τ represents the network delay since a packet is sent by source until it is delivered to receivers. n is a number of 1-hop neighbors. β is a constant value used for expanding the range between minimum waiting timeout and maximum waiting timeout. The best β value can significantly reduce collision occurrences in dense areas while increasing only a little delay. The minimum term of waiting timeout represents the possibility delay from a beacon queuing in MAC layer. So the minimum term will be equal to total delay of all neighbors' beacon sending time. The maximum term of waiting timeout consists of two terms. The first term, 2τ, is equal to two times of network delay. This is because in the case that nodes have one neighbor, they have possibility to wait for one beacon from the neighbor and another network delay from rebroadcasting. The second term, $n\beta\tau$, is the possibility delay from a beacon queuing in MAC layer, that is, multiplied by the expanding value (β). β is used for expanding the range between minimum term and maximum term. The configuration of β is discussed in Section 5.2. The waiting timeout value can be illustrated in Figure 5

$$W(n) = \text{Random}\left[n\tau, (2 + n\beta)\tau\right]. \quad (1)$$

4.2.2. Beacon Mechanism

(a) Beacon Structure. Nodes in NoG use beacon messages for discovering 1-hop neighbors and exchanging their local information. The beacon message header consists of a source identifier, a number of 1-hop neighbors, a list of 1-hop neighbor identifiers, and a list of received packets that still do not expire. The list of received packet contains an identifier of source and an identifier of the packet. This list is used for missing message detection. The beacon size will be at least 5 bytes in case there is no 1-hop neighbor and received packet. The beacon size will increase 4 bytes for each 1-hop neighbor and 5 bytes for each received packet. In order to reduce the number of beacons, nodes piggyback the beacon header with the broadcasting packet when they have a packet to rebroadcast, as shown in Figure 6. Then the next beacon will be postponed until the next beacon interval.

(b) Beacon Interval Calculation. The accuracy of 1-hop neighbors' position depends on the frequency rate of beacon. In fact, this can cause a broadcast storm problem in dense areas. In this paper, the nongeographical knowledge algorithms are focused. These algorithms do not require very high accurate data from beacon information. Moreover, density of vehicles has related to speed of vehicles [22], so the vehicles in dense area are moving slower than the vehicles in sparse area. Consequently, a short beacon interval is needed in sparse areas, but it is unnecessary in dense areas. NoG uses an adaptive beacon interval algorithm to appropriately calculate the beacon interval in each density environment.

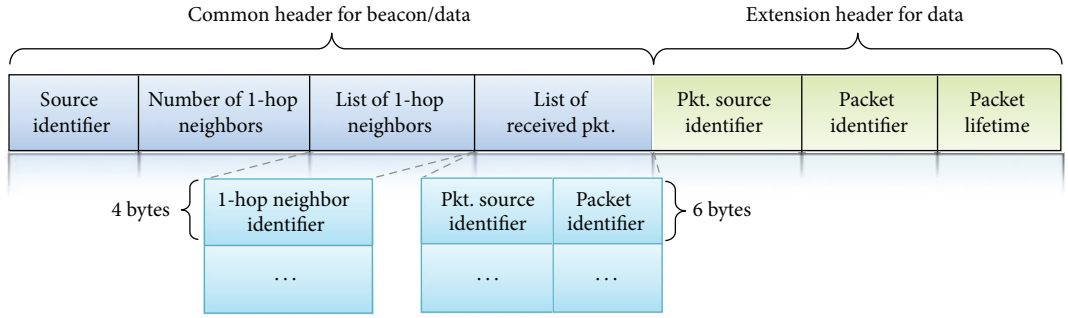


Figure 6: Beacon structure.

The algorithm linearly increases the beacon interval based on network density, called Linear Adaptive Interval or LIA [23]. The algorithm can reduce beacon overhead without decreasing the protocol performance.

As mentioned, the beacon interval is linear increased depending on the network density. The network density (netDensity) is calculated by a number of 1-hop neighbors (n) and a number of broadcasting packets (p) that do not expire. This can be represented by (2). The beacon interval (beaconInv) calculation is represented by (3). minInv is a minimum beacon interval. c is a constant value. maxInv is the longest interval that does not affect the performance of protocol. The parameter setting of beacon interval calculation is explained in Section 5.2:

$$\text{netDensity} = n + p, \tag{2}$$

$$\text{beaconInv} = \min\left[\text{minInv} + \left(c \times \text{netDensity}\right), \text{maxInv}\right]. \tag{3}$$

(c) Missing Packet Mechanism. In VANET, an intermittent connection always occurs. In order to provide reliable broadcasting, protocols need an ability to detect missing packets. The packets can be lost due to channel error. The missing packet mechanism has two parts for its operation. The first part is that a node checks for neighbor's missing packets from incoming beacon. A node can check the missing packets by the list of received packets in the beacon. If a node detects that its neighbor has the missing packets, it will set waiting timeout and add the missing packets to *Broadcast List*. Another part is that a node checks whether there are any packets that it never receives from the incoming beacon. If it finds that it has the missing packets, it will immediately broadcast a beacon to let its neighbors know and detect its missing packets. However, this mechanism can flood many beacons to the networks, so the beaconing for missing packets will be restricted to broadcast only once within a beacon interval. This means that a node cannot rebroadcast its beacon until the next beacon schedule.

5. Performance Evaluation

5.1. Performance Evaluation of CDS Forming Algorithm

5.1.1. Simulation Setup. In order to evaluate performance of our algorithm, we implement a Java simulator. The simulator uses mobility traces from NS-2 [24]. The trace is generated via simulation of urban mobility (SUMO) [25]. The vehicle traces obtained from SUMO are in XML format. They are converted to NS-2 traces format by traffic simulation environment (TraNS) [26]. There are two traffic scenarios: (1) a highway scenario is a straight 4-kilometer road with two lanes per direction; (2) an urban scenario is 2×2 kilometers Manhattan grid. Nodes are equipped with 250 meters transmission range wireless device.

The simulator samples groups of nodes every 10 seconds and then it analyses the CDS forming algorithm in terms of a coverage result and a ratio of CDS members to total nodes in groups. There are more than 2000 groups of nodes that are sampled. No real broadcasting is employed in this simulation. The real broadcasting performance evaluation is done

Table 1: Parameters setting.

Simulation setup	
Message lifetime	10 seconds
Number of broadcast sources	5
Size of broadcast packet	512 bytes
Simulation time	200 seconds
Number of simulation runs	20
Max. vehicle speed (km/h)	50, 80
Vehicle density (veh/km)	2, 6, 10, 20, 30, 40, 60, 80
DECA	
Beacon interval	LIA 1.5–7 seconds $c = 0.2$
Beacon size	5 bytes + 5 bytes for each pkt.
APBSM	
Beacon interval	Constant 1 seconds
Beacon size	21 bytes + 5 bytes for each pkt.
NoG	
Beacon interval	LIA 1.5–7 seconds $c = 0.2$
Beacon size	5 bytes + 4 bytes for each 1-hop neighbor + 5 bytes for each pkt.

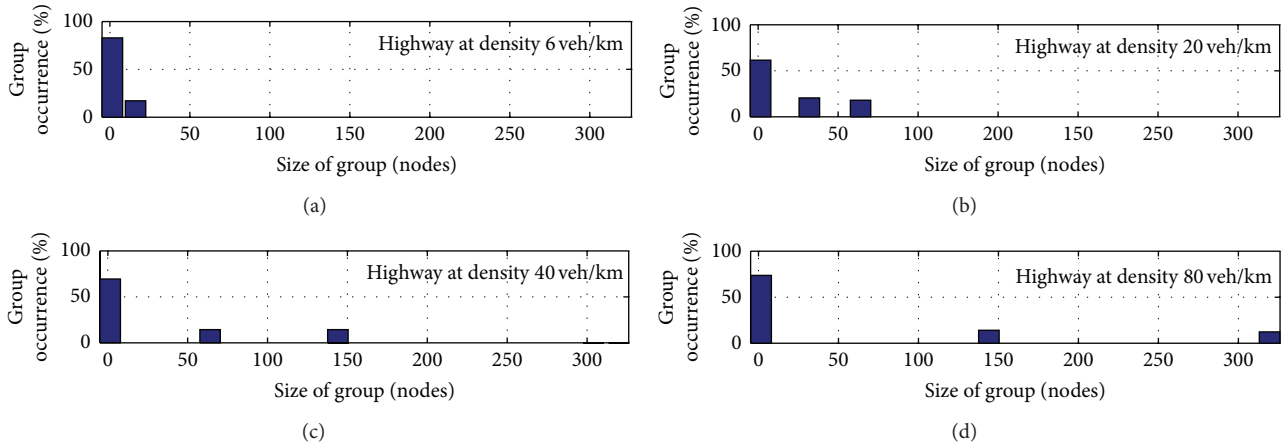


Figure 7: Occurrence of each size of group in highway scenarios.

on well-known network simulator 3 (NS-3) [27] in Section 5.2. The other parameters setting are shown in Table 2.

We have implemented all of following CDS forming algorithm in the simulator.

(i) *Density based (DEN)*: only nodes with the highest number of 1-hop neighbors are members of CDS. This algorithm represents the density based algorithm.

(ii) *Density and topology based with internode condition (DEN+IN)*: members of CDS consist of nodes with the highest number of 1-hop neighbors and nodes that can pass the intermediate condition of Wu and Li's algorithm.

(iii) *Density and topology based with intergateway condition (DEN+IG)*: members of CDS consist of nodes with the highest number of 1-hop neighbors and nodes that can pass the intergateway condition of Wu and Li's algorithm.

(iv) *DTA*: the algorithm that we proposed. DTA is a density and topology based with gateway condition (DEN+G). Members of CDS consist of nodes with the highest number of 1-hop neighbors and nodes that can pass the gateway condition of Wu and Li's algorithm.

(v) *Wu and Li's algorithm (WLA)*: members of CDS are nodes that can complete all of three conditions of Wu and Li's Algorithm. This represents the most efficient topology based algorithm in our literature review.

5.1.2. Metrics. There two metrics considered. All simulation results are averaged from 100 of runs with 95% confidence interval. A group of nodes, that is, a complete graph connection, is not included in the results. The reason is that nodes can directly communicate to each other in this type of group. Note that an overhead result from exchanged beacon is not considered in this evaluation. However, the overhead results are discussed in Section 5.2.

(i) *Coverage node* is measured as a percentage of the number of nodes that are covered by members of CDS to total nodes in the group.

(ii) *Ratio of CDS members* is measured as a ratio of the number of nodes that are members of CDS to a number of total nodes in the group.

5.1.3. Simulation Results. Figures 7 and 8 show the occurrences of node groups in each size for highway scenarios and those for urban scenarios, respectively. For highway scenarios, vehicles are uniformly distributed although vehicles are randomly released and vehicles have the different maximum speed. This is because the highway scenario is a simple straight road with nonstructure the same as the realistic long distance highway road. On the other hand, vehicles are nonuniform distributed in urban scenarios. There are many several sizes of group in each scenario. Therefore, both scenarios and mobility traces can represent the realistic environment of vehicles in both highway areas and urban areas.

Coverage Results. All coverage results in both highway scenarios and urban scenarios are shown in Figure 9.

DEN that considers only the number of 1-hop neighbors provides well coverage results on low density scenarios. The coverage results decrease in high density scenarios because there are more nodes and more complex connections in dense scenarios than in sparse scenarios. The reason is that the number of members in CDS from DEN is not enough to cover all nodes in the groups.

On the other hand, WLA, that is, Wu and Li's algorithm that forms CDS by using topology information, does not operate well in sparse scenarios because the algorithm prunes too much nodes so it decreases a number of covered nodes in sparse scenarios. The advantage of Wu and Li's algorithm is it can construct the efficient members of CDS that can cover all nodes in groups in dense scenarios. WLA works well with complex connections in high density scenarios. These scenarios are similar to general mobile ad hoc scenarios

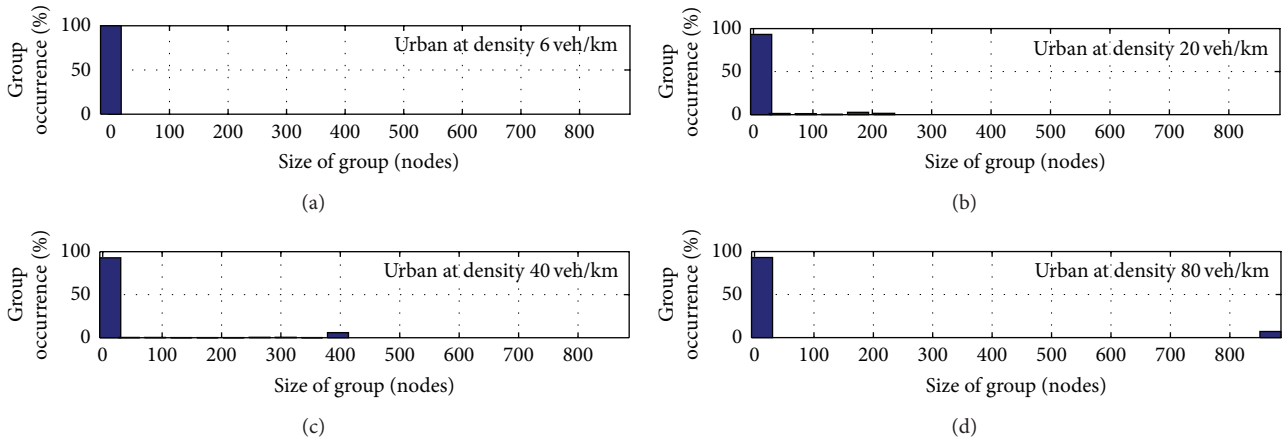


Figure 8: Occurrence of each size of group in urban scenarios.

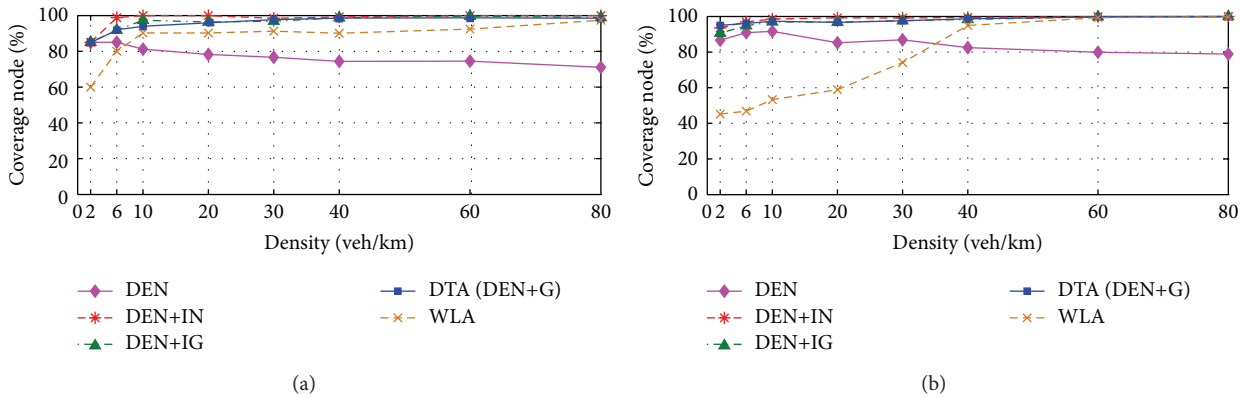


Figure 9: Coverage result. (a) Highway scenarios. (b) Urban scenarios.

that the algorithm is designed for. Therefore, we combine the advantages from both density based algorithm and topology based algorithm. We use the density based algorithm that can provide high coverage results in low density scenarios with a simple concept. Then we combine it with topology based algorithm that provides the efficient CDS members that can cover all nodes in groups in dense scenarios.

The combination algorithms are DEN + IN, DEN + IG, and DTA (DEN + G). These algorithms are a combination of density based algorithm and topology based algorithm. All of them provide the highest coverage results in the simulation. The algorithms can construct CDS members with almost 100% coverage results.

Ratio of CDS Member. The results are shown in Figure 10. The ratio results represent the efficiency of algorithm. A number of CDS members should be as low as possible, while the CDS members can cover all nodes in the group.

DEN has the least ratio results because it considers only nodes with the highest number of 1-hop neighbors. The number of CDS members converges to about 0.07 of total nodes.

WLA is the second least ratio results. It provides almost constant ratio results in every density scenario. The algorithm is very efficient, but this leads to low coverage results in sparse areas. There are many small groups of vehicles in the sparse scenarios and the distance between nodes is longer than in dense scenarios, so the ratio of CDS members should be higher.

DEN+IN has extremely high ratio results. The results are almost 1. This means that the internode condition of Wu and Li's algorithm cannot efficiently prune nodes in vehicular environment. As a result, almost all nodes in the scenarios are CDS members.

DEN+IG also provides the efficient CDS members. It has very low ratio results, but the ratio results are higher than DTA. This is because the gateway condition can significantly prune more the unnecessary nodes than the intergateway condition as described in Section 3.1.

DTA is the most efficient algorithm because it can provide very low ratio of CDS members to total nodes. The ratio results converge to about 0.2 of total nodes. In low density scenarios, DTA has the high ratio results which are close to the results from DEN. DTA also has the ratio results that almost are the same as the results from WLA in high density. The reason is that DTA has the advantages from both density based algorithm and topology based algorithm so DTA will appropriately keep a number of CDS members depending

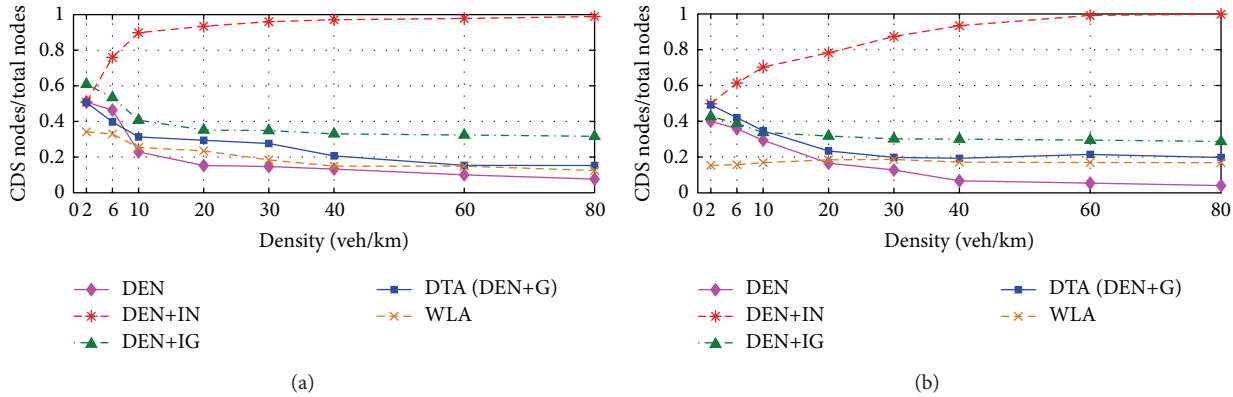


Figure 10: Ratio of CDS members. (a) Highway scenarios. (b) Urban scenarios.

Table 2: Simulation setting.

Simulation time	200 seconds
Number of simulation runs	100
Maximum vehicle speed (km/h)	50, 80
Vehicle density (veh/km)	2, 6, 10, 20, 30, 40, 60, 80

on scenarios. This can maximize the coverage results while minimizing a number of CDS members.

5.2. Performance Evaluation of Broadcasting Protocol

5.2.1. Simulation Setup. All broadcasting protocols evaluated their performance with the same road scenarios and vehicle mobility traces the same as in Section 5.1.1.

There are 5 source nodes in each simulation. After the simulation has run for 100 seconds, source nodes randomly start to broadcast their packet every 10 seconds until simulation ends at 200 seconds. The last packet will be expired at 200 seconds of simulation. All protocols use IEEE802.11b with contention for MAC. We cannot use IEEE802.11p [22] because it is under development phase in NS-3. All nodes are equipped with a wireless module with Rayleigh fading. The transmission success rate is 80% at distance 250 meters. Unless stated otherwise, parameters setting for simulations is configured as indicated in Table 1.

We have implemented all of the following protocols in the well-known network simulator NS-3.16 [27]. All of previous works are configured following their publications.

(i) *DECA [9]*: DECA represents a protocol that uses only density information to select the next rebroadcast node. It provides very high data dissemination speed by avoiding waiting timeout.

(ii) *APBSM [6]*: APBSM represents a protocol that uses both density and geographical knowledge to construct members of CDS by extending Wu and Li's algorithm.

(iii) *NoG+DEN*: our proposed protocol with the simplest algorithm: This algorithm uses only density information to construct CDS members. It represents a density based protocol.

(iv) *NoG+WLA*: our proposed protocol with the original Wu and Li's CDS forming algorithm: it represents a topology based protocol.

(v) *NoG+DTA*: our proposed protocol with our proposed algorithm: DTA is a combination of density and topology based algorithm for constructing CDS members.

5.2.2. Parameter Setting in NoG. The parameter setting for waiting timeout as mentioned in Section 4.2.1 and the parameter setting for beacon interval as mentioned in Section 4.2.2 are discussed. These parameter settings are used in our simulation.

Waiting Timeout. As mentioned in Section 4.2, the efficient β value can significantly reduce collision occurrences in dense areas while increasing only a little delay. In order to select the β, we performed a simulation. The simulation setup is the same setup as in Section 5.2. (Table 1). The highway scenario is used in this simulation. We evaluated the performance of NoG using the directed function with varied β (1–5). From the results, 3 is the best value that provides low overhead and it introduces the lowest additional delay. According to (1) in Section 4.2.1, the maximum waiting timeout depends on β value.

Beacon Interval. The efficient beacon interval should help the protocol to provide the fastest data dissemination speed, while it increases the least additional overhead to each network density. In order to select the efficient beacon interval, we performed a simulation. We used the highway scenario in this simulation. The beacon interval is varied from 0.1 to 9 seconds in different density scenarios (2–80 veh/km). The other parameters such as communication setup and packet setup are set the same as those in Section 5.2 (Table 1). From simulation results, we observed that 1.5 seconds are the beacon interval that provides the fastest data dissemination

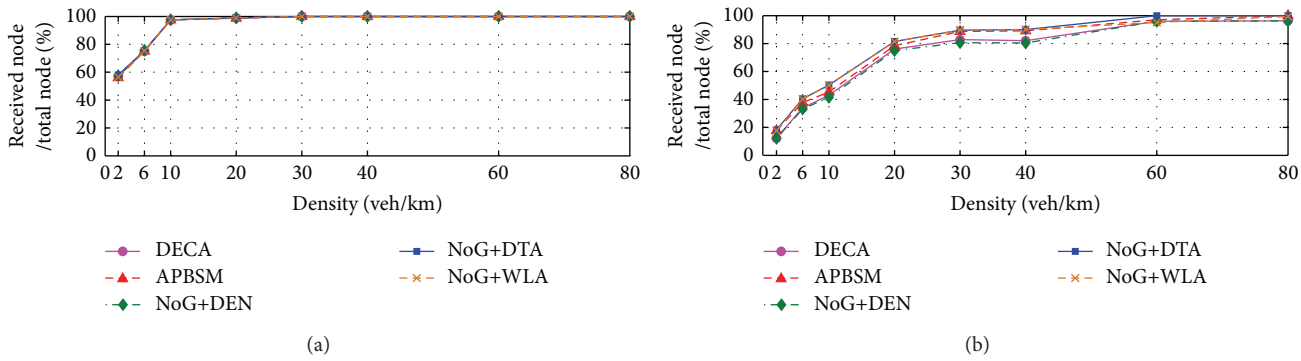


Figure 11: Reliability results. (a) Highway scenarios. (b) Urban scenarios.

speed with the lowest overhead in low density scenarios and 7 seconds are the longest beacon interval that provides the fastest data dissemination speed with the lowest overhead in dense scenarios. Therefore, the suitable beacon interval for NoG is between 1.5 seconds and 7 seconds. According to (3) in Section 4.2.2, (c) is equal to 0.2, minInv is 1.5, and maxInv is 7.

5.2.3. Metrics. Five metrics are considered. All simulation results are averaged from 20 of runs with 95% confidence interval.

(i) *Reliability* is measured as a percentage of nodes that received the packets at the end of simulation.

(ii) *Retransmission overhead* is measured from bandwidth consumption, that is, from packet retransmission.

(iii) *Beacon overhead* is measured from bandwidth consumption that is from beacon transmission.

(iv) *Source of retransmission* is measured as percentages of three sources of packet retransmission that consist of retransmission by CDS members, retransmission by waiting timeout mechanism, and retransmission by neighbor's missing packet mechanism.

(v) *Speed of data dissemination* is measured as (4), where r_i represent number of nodes that received the packet for the first time at the time i and n is total number of vehicles in the scenario:

$$y(t)\,\frac{\sum_{i=0}^{t} r_i}{n} \times 100. \tag{4}$$

5.2.4. Simulation Results

Reliability. The reliability results in highway scenarios are shown in Figure 11(a). All protocols provide the same reliability in every scenario because these protocols are well designed to operate in vehicular environment. All of them employ store and forward technique that can handle the intermittent connectivity. The difference of CDS forming algorithm does not affect the reliability due to simple scenarios.

On the other hand, the difference of algorithms affects reliability results in urban scenarios as shown in Figure 11(b). NoG+DTA provides the highest reliability results in every scenario because the rebroadcast nodes are efficiently selected to cover all of nodes in the scenarios. NoG+WLA that operates well in urban scenarios provides reliability slightly less than NoG+DTA. This is because the coverage ability of WLA is less than DTA as mentioned in Section 5.1. APBSM that uses the extended version of WLA provides reliability less than NoG with the original WLA about 1–5%. The reason is from its broadcasting mechanism and its waiting timeout mechanism. A node in APBSM has to wait for waiting timeout expiration before each rebroadcasting. Moreover, when a node detects the missing message from its neighbors, it has to wait for more than one beacon interval before each retransmission. This reduces the opportunity to increase the reliability. DECA and NoG + DEN have the lowest reliability result due to its only density based algorithm that does not perform well in high density and complex scenarios.

Retransmission Overhead. The retransmission overhead results are illustrated in Figure 12.

For highway scenarios, all of protocols have the same retransmission overhead except APBSM. This is because APBSM uses the inversed function to calculate their waiting timeout, so the redundant retransmissions increase in dense area. Although DECA also uses the inversed function, it avoids using waiting timeout by selecting the next rebroadcast node from source. All of algorithms on NoG protocol can efficiently operate in every highway scenario.

For urban scenarios, APBSM still has the highest retransmission overhead due to its waiting timeout calculation. Although its CDS algorithm is extended from Wu and Li's algorithm, but Wu and Li's can work better on NoG (NoG+WLA). NoG+WLA can decrease up to 35% of redundant retransmission from APBSM. For density based algorithm, DECA and NoG+DEN have the same retransmission overhead, but the results are worse than NoG+WLA and NoG+DTA by about 23%. The reason is that density based algorithm cannot work well on complex scenarios. NoG+DTA has the most efficient operation. NoG+DTA can provide the lowest overhead in every urban scenario. DTA has the advantage from density based algorithm and topology based algorithm so it is only a protocol that has the least

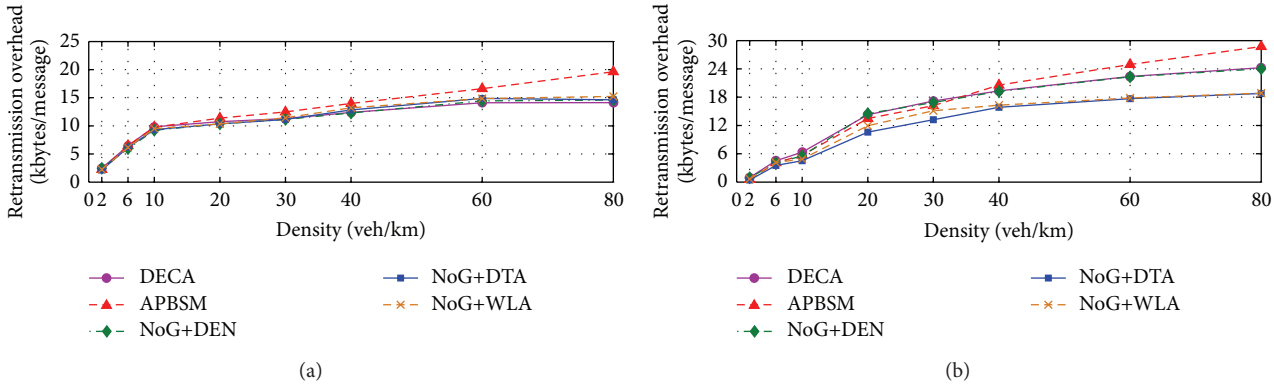


Figure 12: Retransmission overhead results. (a) Highway scenarios. (b) Urban scenarios.

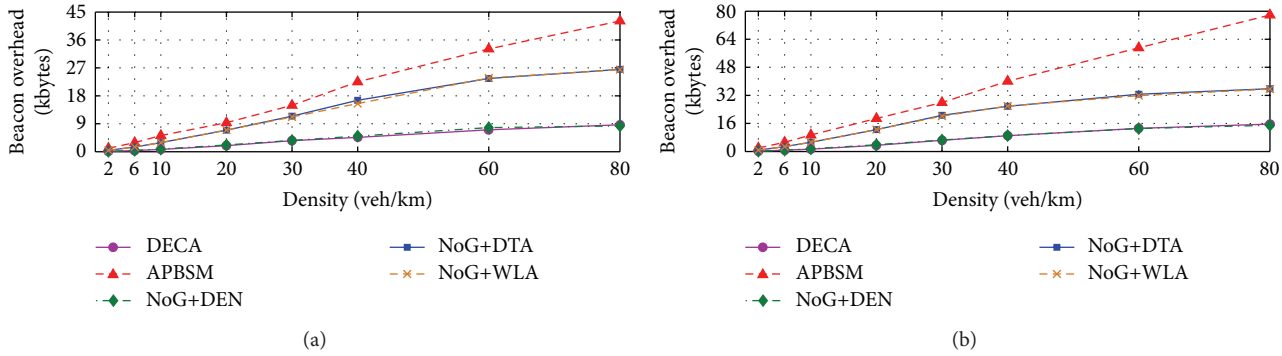


Figure 13: Beacon overhead results. (a) Highway scenarios. (b) Urban scenarios.

number of retransmissions in normal density scenarios that consist of many sizes of groups of vehicles.

Beacon Overhead. The beacon overhead results are illustrated in Figure 13.

For highway scenarios, DECA and NoG+DEN have the lowest beacon overhead results in the simulation. The overhead of DECA and NoG+DEN is very low because DECA and NoG+DEN use only density information so they require only a number of 1-hop neighbors. For NoG+DTA and NoG+WLA, their beacon messages need to contain 1-hop neighbor list. For APBSM, its beacon needs to contain position knowledge of neighbors and it has to use the constant beacon interval for accurate neighbors' position. So APBSM has the highest overhead results.

For urban scenarios, all of results are in the same trend with highway scenarios. APBSM has the highest overhead due to its constant beacon interval. DECA and NoG+DEN have the lowest beacon overhead. NoG+WLA and NoG+DTA have 55% more beacon overhead than density based algorithm. However, the difference of overhead results between density based algorithm and topology based algorithm in urban scenarios is less than the difference of results in highway scenarios. This is because the average beacon sizes in urban scenarios are larger than highway scenarios. Note that the protocol has to maintain 2-hop neighbor list for topology based algorithm. The size of beacon depends on the size of scenario. The adaptive beacon interval significantly reduces overhead in the following case. When a node is in the dense area, the size of beacon is larger, while the beacon interval is also longer, so the large beacon will be reduced.

Source of Retransmission. The source of retransmission represents the efficiency of protocols and algorithms. The protocols and algorithms that have the higher retransmissions from their preferred nodes are better because these nodes are working as designed. This affects the performance in terms of data dissemination speed. The reason is that the preferred nodes can immediately rebroadcast or have the shorter waiting timeout than other nodes. The preferred node of DECA is selected by source node and the preferred node of APBSM, NoG+DEN, NoG+DTA, and NoG+WLA is a CDS member.

The results are shown in Figure 14. For density based algorithms, DECA and NoG+DEN have the best results in highway scenarios because the algorithms can operate well in simple scenarios. Both of the protocols have very close percentages of preferred node retransmissions, but DECA has better results than NoG+DEN in highway scenarios. The reason is that DECA selects the next rebroadcast node from source's perspective. The selected node is a node with the highest density of source's neighbors, so a number of selected nodes are higher than a number of CDS members from NoG+DEN. However, in urban scenarios, a number of

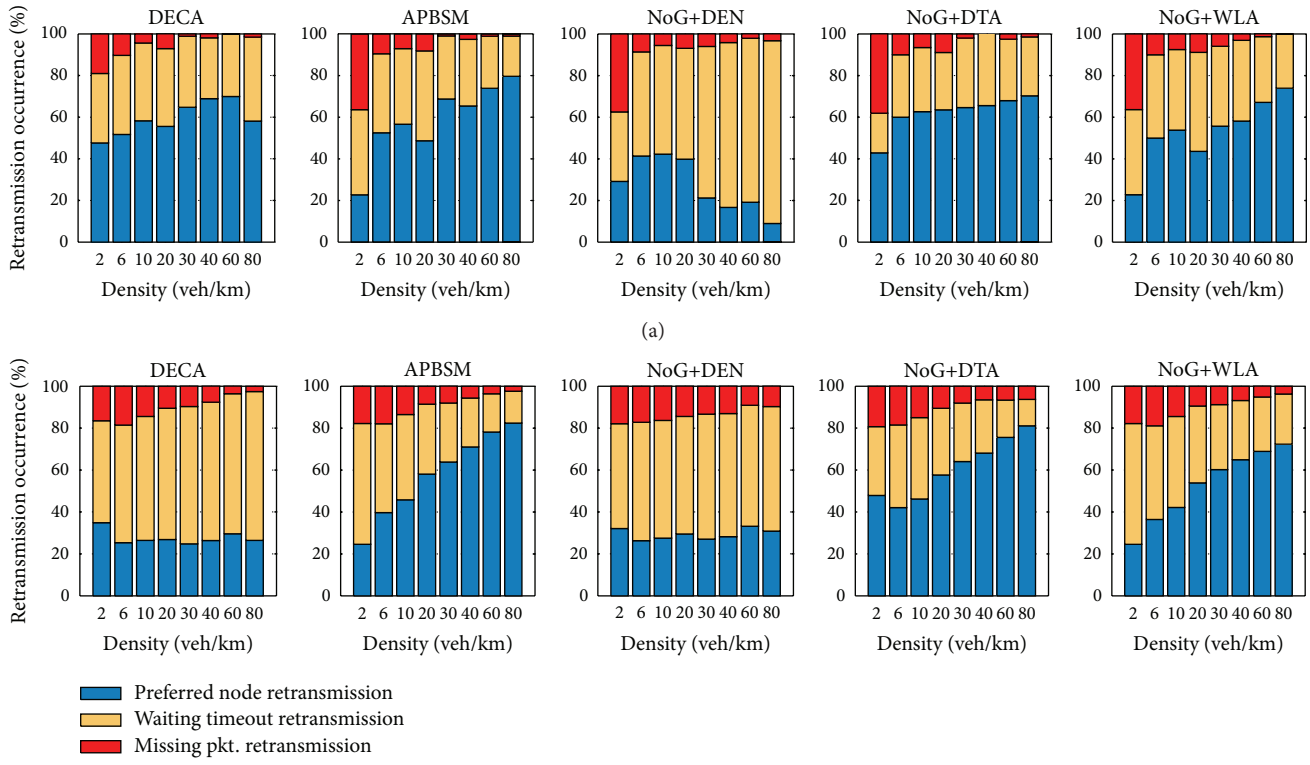


Figure 14: Source of retransmission. (a) Highway scenarios. (b) Urban scenarios.

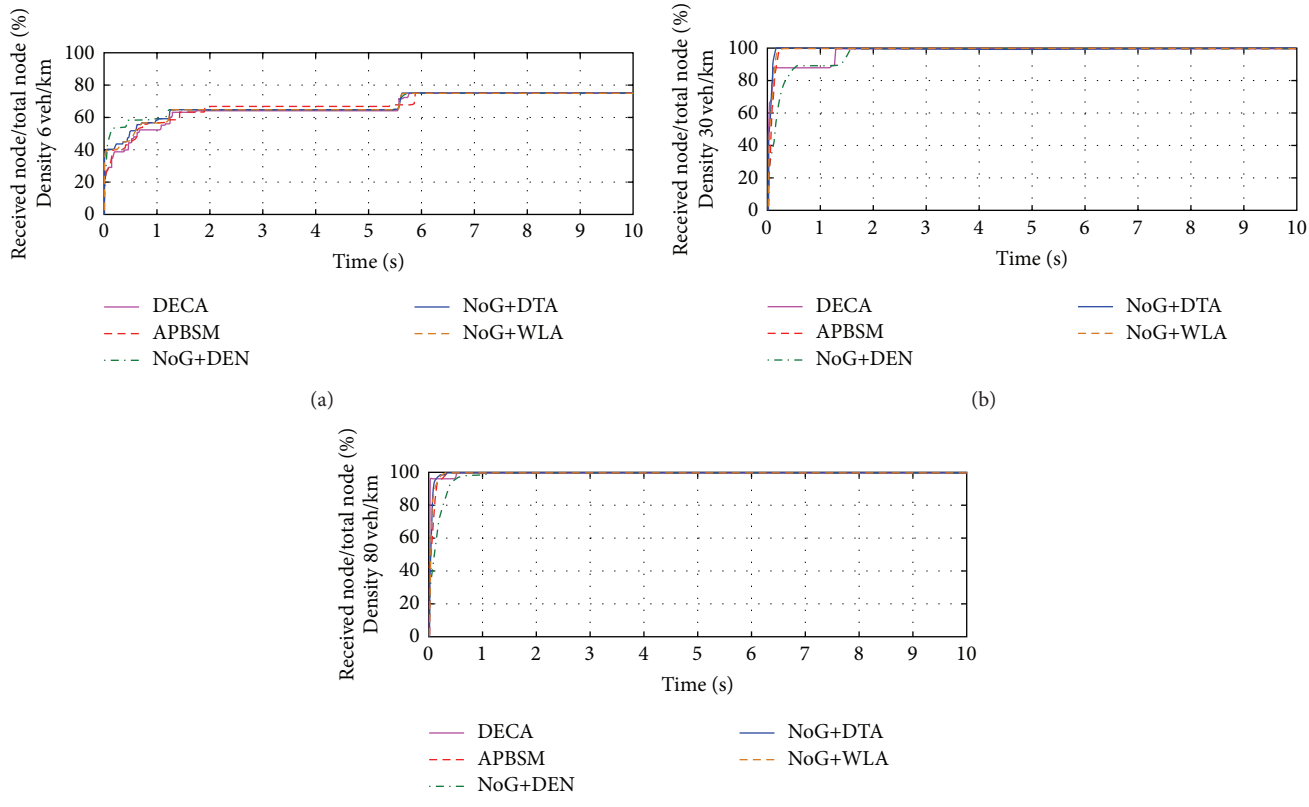


Figure 15: Speed of data dissemination in highway scenarios at 6 veh/km (a), 30 veh/km (b), and 80 veh/km (c).

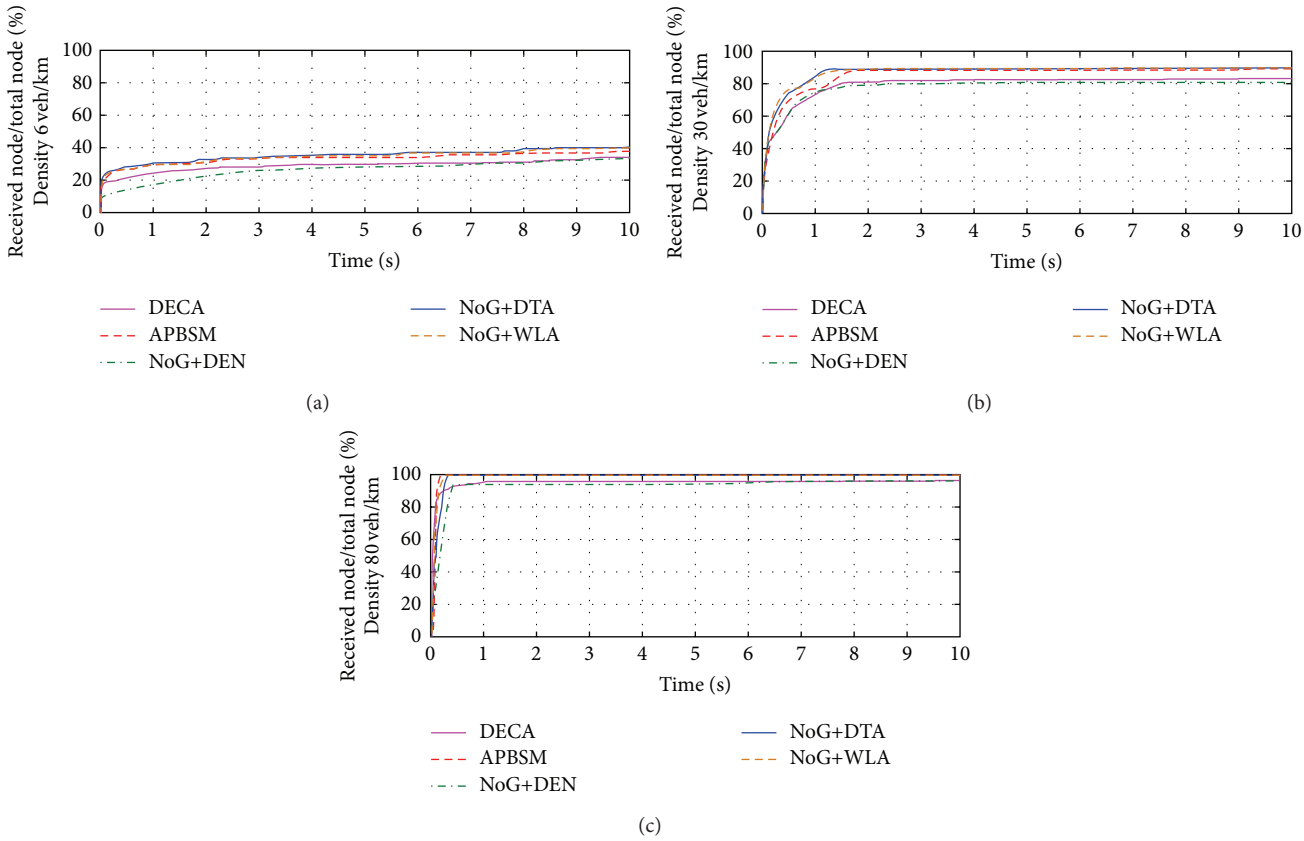


Figure 16: Speed of data disseminatrion in urban scenarios at 6 veh/km (a), 30 veh/km (b), and 80 veh/km (c).

rebroadcast nodes from both algorithms are not enough to cover all nodes in scenarios.

For topology based algorithms, the results of APBSM and NoG+WLA are the same trend with coverage results in Section 5.1. The topology based algorithm is appropriate to complex scenarios, so in higher density these algorithms have higher percentages of preferred node rebroadcasting.

NoG+DTA has the highest percentage of preferred nodes retransmission in every scenario because NOG+DTA is the combination of density-based algorithm that works well in simple scenarios and topology-based algorithm that works well in complex scenarios.

Speed of Data Dissemination. The speed of data dissemination results in the highway scenarios and the urban scenarios are, respectively, shown in Figures 15 and 16. The results at density 6 veh/km represent sparse scenarios (2–10 veh/km). The results at density 30 veh/km represent normal density scenarios (20–40 veh/km) and the results at density 80 veh/km represent high density scenarios.

For highway scenarios, NoG+DEN is the fastest protocol in low density scenarios, but it is the slowest one in high density scenarios due to its density based algorithm. Nodes in DECA have the results the same as NoG+DEN. NoG+DTA is the fastest protocol from simulation results. APBSM and NoG+WLA are slightly slower than NoG+DTA for all scenarios, but the difference is less than 0.1 milliseconds.

For urban scenarios, DECA and NoG+DEN are slower than topology based algorithm due to complexity of connection. APBSM is a bit slower than NoG+DTA and NoG+WLA in sparse areas and medium density areas. The reason is that rebroadcast nodes in APBSM have to wait for waiting timeout before each rebroadcasting. On the other hand, APBSM provides the fastest data dissemination in high density scenarios due to a lot of redundant retransmissions discussed in retransmission overhead results. NoG+DTA and NoG+WLA provide almost the same speed of data dissemination.

6. Conclusion

In this paper, we propose an approximation algorithm for constructing CDS members. It is a density and topology based algorithm, called DTA. DTA combines the advantages from density based algorithm and topology based algorithm. The density based algorithm can construct the efficient CDS members in simple connections or low density scenario. On the other hand, the topology-based algorithm can construct the efficient CDS members in complex connections or high density scenario. The simulation results show that DTA outperforms other algorithms in terms of coverage results and ratio of CDS members to total nodes. DTA has the coverage results better than other previous algorithms' results up to 50%. We also proposed a nongeographical

knowledge broadcasting protocol, called NoG. The protocol consists of a broadcast mechanism, a waiting timeout mechanism, and a beacon mechanism. It is designed to operate with high data dissemination speed and consume the least network resource as possible. The simulation results show that NoG provides the fastest data dissemination speed and the highest reliability. Currently, the beacon size of NoG depends on the size of 2-hop neighbor list which can be significantly increased in dense area. Most of broadcasting protocols in VANET uses beacon with variable size. Therefore, our future work is to reduce the beacon overhead by using fixed size beacon. The solution may be applied to other broadcasting protocols in VANET.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This research was supported in part by the TRF (Thailand Research Fund) (MRG5380164), the Ratchadaphiseksomphot Endowment Fund, and H.M. the King's 72nd Birthday Scholarship, Chulalongkorn University, Bangkok, Thailand.

References

[1] M. L. Sichitiu and M. Kihl, "Inter-vehicle communication systems: a survey," *IEEE Communication Survey and Tutorial*, vol. 10, no. 2, pp. 88–105, 2008.

[2] V. Naumov, R. Baumann, and T. Gross, "An evaluation of inter-vehicle ad hoc networks based on realistic vehicular traces," in *Proceedings of the 7th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '06)*, Florence, Italy, May 2006.

[3] N. Wisitpongphan, F. Bai, P. Mudalige, and O. K. Tonguz, "On the routing problem in disconnected vehicular ad hoc networks," in *Proceedings of the 26th Annual IEEE Conference on Computer Communications (INFOCOMM '07)*, Anchorage, Alaska, USA, May 2007.

[4] A. Vahdat and D. Becker, "Epidemic routing for partially connected ad hoc networks," Tech. Rep. CS-200006, Duke University, 2000.

[5] M. Nekovee and B. B. Bogason, "Reliable and efficient information dissemination in intermittent connected vehicular ad hoc networks," in *Proceedings of the 65th IEEE Vehicular Technology Conference (VTS '07)*, pp. 2486–2490, Dublin, Ireland, April 2007.

[6] F. J. Ros, P. M. Ruiz, and I. Stojmenovic, "Acknowledgment-based broadcast protocol for reliable and efficient data dissemination in vehicular ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 11, no. 1, pp. 33–46, 2012.

[7] K. N. Nakorn and K. Rojviboonchai, "POCA : position-aware reliable broadcasting in VANET," in *Proceedings of the 2nd Asia-Pacific Conference of Information Processing (APCIP '10)*, Nanchang, China, September 2010.

[8] O. K. Tonguz, N. Wisitpongphan, and F. Bai, "DV-CAST: a distributed vehicular broadcast protocol for vehicular ad hoc networks," *IEEE Wireless Communications*, vol. 17, no. 2, pp. 47–57, 2010.

[9] N. N. Nakorn and K. Rojviboonchai, "DECA: density-aware reliable broadcasting protocol on vehicular ad-hoc networks," in *Proceedings of the 7th IEEE International Conference on Electrical Engineering/Electronics Computer Telecommunications and Information Technolog (ECTI-CON '10)*, Chaing Mai, Thailand, May 2010.

[10] A. Qayyum, L. Viennot, and A. Laouiti, "Multipoint relaying: an efficient technique for flooding in mobile wireless networks," Tech. Rep. RR-3898, INRIA, 2000.

[11] J. Wu and H. Li, "On calculating connected dominating set for efficient routing in ad hoc wireless networks," in *Proceedings of the 3rd International Workshop Discrete Algorithms and Methods for Mobile Computing amd Communication (DIALM '09)*, pp. 7–14, August 1999.

[12] J. Sucec and I. Marsic, "An efficient distributed network-wide broadcast algorithm for mobile ad hoc networks," Tech. Rep. 248, CAIP, Rutgers University, 2000.

[13] W. Peng and X. Lu, "On the reduction of broadcast redundancy in mobile ad hoc networks," in *Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '00)*, pp. 129–130, 2000.

[14] I. Stojmenovic, M. Seddigh, and J. Zunic, "Dominating sets and neighbor elimination-based broadcasting algorithms in wireless networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 13, no. 1, pp. 14–25, 2002.

[15] F. Dötzer, "Privacy issues in vehicular ad hoc networks," in *Proceedings of the Workshop on Privacy Enhancing Technologies (PET '05)*, 2005.

[16] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," *ACM Journal of Computer Security*, vol. 15, no. 1, 2007.

[17] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Proceedings of the Workshop on Hot Topics in Networks (HOTNETS '05)*, 2005.

[18] "The 13 Controlling Criteria," in *Mitigation Strategies for Design Exceptions*, chapter 3, US Department of Transportation Federal Highway Administration, Washington, DC, USA, 2007.

[19] V. Naumov and T. Gross, "Connectivity-aware routing (CAR) in vehicular ad-hoc networks," in *Proceedings of the 26th Annual IEEE Conference on Computer Communications (INFOCOMM '07)*, Anchorage, Alaska, USA, May 2007.

[20] IEEE, "Part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications amendment 6: wireless access in vehicular environments," in *Proceedings of the IEEE Standard for Information Technology Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks Specific Requirements*, New York, NY, USA, July 2010.

[21] K. Na Nakorn and K. Rojviboonchai, "DECA-bewa: density-aware reliable broadcasting protocol in VANETs," in *Proceedings of the The Institute of Electronics, Information and Communication Engineers Transactions on Communications (IEICE '13)*, vol. 96, May 2013.

[22] M. Artimy, "Local density estimation and dynamic transmission-range assignment in vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 8, no. 3, pp. 400–412, 2007.

[23] N. N. Nakorn and K. Rojviboonchai, "Efficient beacon solution for wireless ad-hoc network," in *Proceedings of the 7th International Joint Conference on Computer Science and Software Engineering (JCSSE '10)*, Bangkok, Thailand, May 2010.

[24] "The Network Simulator (NS-2)," http://www.isi.edu/nsnam/ns/.

[25] Simulation of Urban Mobility (SUMO), http://sumo.sourceforge.net/.

[26] "Traffic and Network Simulation Environment (TraNS)," http://trans.epfl.ch/.

[27] "The Network Simulator (NS-3)," http://www.nsnam.com/.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2014, Article ID 838391, 14 pages
http://dx.doi.org/10.1155/2014/838391

Research Article

A Game Theory-Based Analysis of Data Privacy in Vehicular Sensor Networks

Yunhua He,[1] Limin Sun,[1,2] Weidong Yang,[2,3] and Hong Li[2]

[1] *School of Computer Science, Xidian University, Xi'an, China*
[2] *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Science, Beijing, China*
[3] *College of Information Science and Engineering, Henan University of Technology, Zhengzhou, China*

Correspondence should be addressed to Limin Sun; sunlimin@iie.ac.cn

Received 12 April 2013; Accepted 28 October 2013; Published 20 January 2014

Academic Editor: Liusheng Huang

Mobile traces, collected by vehicular sensor networks (VSNs), facilitate various business applications and services. However, the traces can be used to trace and identify drivers or passengers, which raise significant privacy concerns. Existing privacy protecting techniques may not be suitable, due to their inadequate considerations for the data accuracy requirements of different applications and the adversary's knowledge and strategies. In this paper, we analyze data privacy issues in VSNs with a game theoretic model, where a defender uses the privacy protecting techniques against the attack strategies implemented by an adversary. We study both the passive and active attack scenarios, and in each scenario we consider the effect of different data accuracy requirements on the performance of defense measures. Through the analysis results on real-world traffic data, we show that more inserted bogus traces or deleted recorded samples show a better performance when the cost of defense measures is small, whereas doing nothing becomes the best strategy when the cost of defense measures is very large. In addition, we present the optimal defense strategy that provides the defender with the maximum utility when the adversary implements the optimal attack strategy.

1. Introduction

With the advances and wide adoption of wireless communication technologies, vehicles are now often equipped with wireless devices that allow them to communicate with each other (V2V) as well as with roadside infrastructures (V2I). The V2V and V2I communications make driving more safe and improve a driver's driving experiences. Such communication networks are called Vehicular Ad Hoc Networks (VANETs). However, with the increasing needs for sensing and data acquisition in cities, VANETs have turned into Vehicular Sensor Networks (VSNs) [1]. VSNs exploit vehicles and passengers to capture the occurrence of events, such as traffic volume, road surface condition, chemical, and radiation. The location traces in the traffic-related data create various fresh new business applications and services, such as map drawing [2], traffic prediction [3], city planning, and mobile network analysis [4].

However, the places in these location traces that a driver or passenger has visited may reveal his/her sensitive information, such as traffic law violations, political affiliations, and medical conditions [5, 6]. Although the information about vehicular mobility traces are often collected in an anonymous way, an adversary can reidentify the true owner of a trace. Because the location information of drivers and passengers can be openly observed in public places, and also can be disclosed voluntarily or inadvertently by themselves, such as a casual conversation, or published media such as news articles or web blogs [4]. The adversary who has partial knowledge of the whereabouts of drivers or passengers (which are called victims), can infer the traces' true owners with high probability by using vehicular mobility constraints and spatiotemporal correlation [4, 7].

To reduce spatiotemporal correlation, some frequently proposed privacy protecting techniques suggest reducing

the resolution of the recorded data [8, 9] or introducing noise in the data [10–12]. However, these techniques may not be suitable for privacy preserving in VSNs due to their inadequate consideration for the adversary's knowledge and its attack strategies. On the other hand, these techniques can not meet the different data accuracy requirements of different applications and services [13]. To address these challenges, we must first analyze the effect of the knowledge and attack strategies and the different accuracy requirements on the performance of defense strategies.

In this paper, we use a game-theoretic model to study the effect of the adversary's knowledge and strategies and the data accuracy requirements on the performance of defense measures. More specifically, we first present location privacy issues in VSNs, including the ability and goal of the adversary and defender. Then, we define a game theoretic model the attack and defense game which models the strategy selection decision behavior of the adversary and defender. In this game, the adversary implements its attack strategies in both the passive and active attack scenarios; the defender uses the frequently proposed privacy protecting approaches to increase the hardness of the adversary to reidentify the victims. Finally, through analysis results on real-world traffic data, we show that attack strategies in different scenarios show different performance. More inserted bogus traces or deleted recorded samples show a better performance when the cost of defense measures is small, whereas doing nothing becomes the best strategy when the cost of defense measures is very large. We also present the optimal defense strategy for each attack strategy. The main contributions of this paper are as follows.

(i) We define an attack and defense game model to capture the strategy selection decision behavior of the adversary and defender, and we show the effectiveness of defense strategies.

(ii) We establish the attack and defense game based on real world traffic data. In particular, for different attack scenarios, we study both the complete information game (the defender knows the adversary's knowledge on whereabouts of victims) and the incomplete information game (the defender does not know the adversary's knowledge).

(iii) Through the Nash equilibriums in these games, we show that the defender can balance the data accuracy and victims' location privacy to obtain the maximum utility when an adversary implements the optimal attack strategy.

The rest of the paper is organized as follows. In Section 2, we discuss related work. Section 3 presents the network model of VSNs and the location privacy issues in VSNs including the ability and goal of the adversary and defender. In Section 4, we define the attack and defense game model and present the attack in different scenarios and defense strategies. In Section 5, we present our main analysis results in the complete and incomplete information game for different attack strategies. We conclude the paper in Section 6.

2. Related Work

Several recent studies [4, 7] have analyzed the privacy risk of mobile traces and found that omitting identifiers from mobile traces does not guarantee anonymity due to the spatio-temporal correlation. Ma et al. [4] show that an adversary who have a relatively small amount of drivers' location snapshots, could infer the true owners of anonymous traces with high probability. Montjoye et al. [7] study fifteen months of human mobility data for one and a half million individuals and find that four spatio temporal points are enough to uniquely identify 95% of the individuals. Therefore, there is an raising need for stronger privacy protection mechanisms.

In general, the existing solutions can be divided into two categories: reducing the resolution of the recorded data [8, 14] and introducing noise in the data. Hoh et al. [8] propose a disclosure control algorithm called uncertainty-aware path cloaking algorithm that selectively reveals GPS samples to limit the maximum time-to-confusion for all vehicles. Nergiz et al. [14] adopt the notion of k-anonymity to trajectories. They find a representative trajectory in k trajectories so that every trajectory is indistinguishable from other $k - 1$ trajectories.

These approaches of introducing noise have also been extensively studied in [10, 12]. Lu et al. [10] create a mix area in social spots to achieve the provable location privacy in VANETs. Huang et al. [12] proposed a solution called silent period to provide user with location privacy preserving in wireless networks. However, these techniques may be not suitable for privacy preserving in VSNs for two reasons. First, these techniques rarely consider the effect of the adversary's knowledge and its attack strategies on the performance of defense strategies. Second, they cannot meet the different data accuracy requirements of different applications and services [13]. These issues are what we want to address in this paper.

Game theory provides the many needed mathematical frameworks for analysis, modeling, and decision processes for network security and privacy issues [15–17], so we adopt game theory to study the data privacy issues in VSNs. There are many works on using game theory in security aspects of VANETs. Raya et al. [18] model the revocation problem using a finite dynamic game with mobile nodes as players, who can detect misbehavior with a certain probability. Reidt et al. [19] design a distributed detection error tolerant revocation scheme called karmic-suicide by using a game theoretic approach. In [20], zerosum game, fuzzy game and fictitious play are applied to model the interaction of the attacker and defender. In [10], the authors use game theoretic techniques to prove the feasibility of their pseudonym changing strategy. Freudiger et al. [21] analyze the noncooperative behavior of mobile nodes by using a game theoretic model, where each player aims at maximizing its location privacy at a minimum cost. In this paper, we study a new aspect of privacy by evaluating the effect of the knowledge and attack strategies and the different accuracy requirements on the performance of defense strategies.

Table 1: List of symbols.

Symbol	Definition
L_i	Trace of user i
Tr	Set of anonymous traces
R	Side information
t_k	Time instances
τ_k	Sampled times
$u_i(s_i, s_{-i})$	Payoff function
s_i	Pure-strategy of user i
s_{-i}	Pure-strategy of other users besides i
θ_i	Type of user
$f(\theta_i)$	Probability density function of type
α, β	System parameters

3. Preliminaries

In this section, we explain our network model, as well as our assumptions and the location privacy issues in VSNs. We conclude by sketching the problem this work aims at solving. In Table 1, we summarize the notations introduced throughout this paper.

3.1. Network Model. In VSNs, vehicles and passengers act as sensors to capture the occurrence of events, such as traffic accidents, traffic distribution, and road weather information [22]. VSNs can perceive the traffic distribution in a city with efficiency and high accuracy, and thus they have been envisioned to have a great potential to revolutionize human's driving experiences and metropolitan-area traffic flow control. Figure 1 illustrates the network model of VSNs. Vehicles use Dedicated Short Range Communication (DSRC) [23] technology to transmit the traffic related information, that is, ⟨*time, position*⟩ pairs, to Roadside Unit (RSU) via single-hop or multihop communications. Then, RSUs upload the information to a traffic control center through wired networks, so the center can predict the traffic distribution with very low cost and high accuracy.

We assumed that a set of traces, each of which recording intermittently the time and corresponding location of a mobile node, are used by various applications, such as traffic prediction, city planning, and mobile network evaluation. These traces are anonymous in that the true identity of a vehicle has been replaced by a random identifier, but one same true identity is always mapped to a same identifier. In the following, we will elaborate the privacy threat on these anonymous traces.

3.2. Threat Model. An adversary tries to identify the complete path histories of one or more victims (drivers or passengers) from the anonymous traces. We assume that the adversary can collect certain side information about one or more victims. Each piece of side information gives the location of a victim at a time instant, although the information may not be exact. In practice, the side information may be obtained through the following means. First, nodes are open to observations in public spaces. Hence, the adversary may obtain

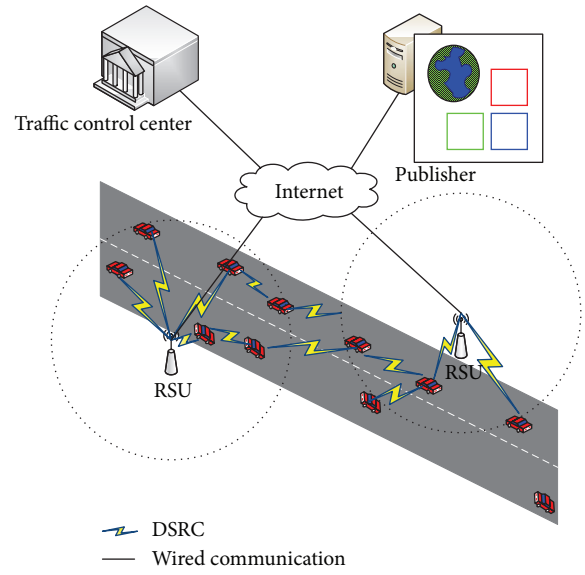


Figure 1: Network model of VSN.

the side information directly through meeting the victim by chance or engineered encounters. This case is called an active attack scenario. Second, nodes may disclose information on their whereabouts either voluntarily or inadvertently [11], which is called passive attack scenario. For example, a casual conversation between Alice and Bob may involve where Alice was around 8 am, or it may involve another person's location.

We set the trace of node i to be L_i, the set of all nodes' traces is $\mathrm{Tr} = \{L_i\}$, the side information R of a victim as a map, $R : \{t_k\} \rightarrow \Theta$, where t_k is the time instant at which some side information about the victim's locations is revealed, and Θ is the set of all cell location IDs. Then, the ability of the adversary to reveal the victim's trace can be given in the form of conditional entropy as follows:

$$H\left(L_T \mid R\right) = -\sum_{i=1}^{|\mathrm{Tr}|} \sum_{k} \Pr\left(L_i, R\left(t_k\right)\right) \log_2 \Pr\left(L_i \mid R\left(t_k\right)\right), \tag{1}$$

where $\Pr(L_i \mid R(t_k))$ is the conditional probability that the victim's trace L_i corresponds to the side information $R(t_k)$ known by the attacker, and $\Pr(L_i, R(t_k))$ is the joint probability of the trace L_i and the side information $R(t_k)$.

The ability of the attacker is determined by side information $R(t_k)$ and conditional entropy $H(L_T \mid R(t_k))$ because $H(L_T \mid R) = \sum_k \Pr(R(t_k)) H(L_T \mid R(t_k))$. When $\Pr(R(t_k))$ is fixed, the smaller the entropy $H(L_T \mid R(t_k))$, the smaller the conditional entropy $H(L_T \mid R)$, the stronger the attack power. When $H(L_T \mid R) = 0$, the victim's trace can be uniquely determined.

3.3. Defense Measures. A defender tries to protect the privacy of victims, which is defined by the uncertainty of a node's trace. The trace uncertainty is referred to as the entropy of the probability distribution of a node's trace [9, 12]. Let $p_i = \Pr(L_T = L_i)$, $\forall L_i \in \mathrm{Tr}$, denotes the probability that L_i

corresponds to the victim's trace L_T, so the entropy of the probability distribution of L_T can be defined as

$$H(L_T) = -\sum_{i=1}^{|\mathrm{Tr}|} p_i \log_2 p_i. \quad (2)$$

The larger the entropy $H(L_T)$ is, the more uncertainty the victim's trace L_T is. The smaller the entropy $H(L_T)$, the less uncertainty the victim's trace L_T, when $H(L_T) = 0$, the victim's trace can be uniquely determined.

Defense objectives for protecting trace privacy can be measured by k-anonymity. An anonymity set is denoted as V_A that includes the nodes with their traces indistinguishable from that of the victim T. The k-anonymity model for privacy protection as used in [24] essentially refers to an anonymity set V_A with a minimum size k, where the victim is guaranteed to be not distinguishable from at least $k-1$ nodes with respect to information related to the victim (such as location information). However, not all the nodes in the anonymity set are equally likely to be the victim since an adversary may be able to obtain side information on the nodes.

We use entropy to improve this model here. Let the defender want to provide an anonymity set with a minimum size k; then, the entropy of the distribution of the anonymity set is given by $H(V_A) = -\sum_k (1/k)\log_2(1/k) = \log_2 k$. Hence, the mechanisms for trace privacy protection should meet as follows:

$$H(L_T \mid \Omega) \geq H(V_A), \quad (3)$$

where Ω is the side information that the defender believes the attacker has known, and $H(L_T \mid \Omega)$ is the uncertainty of the victim's trace in the case of Ω.

Since privacy is a context-specific property and is socially and/or culturally defined [6, 25], the trace privacy needs of individual users may vary, and further different users may require different k-anonymity entropy $H(V_A)$. But here, we only consider the average of k-anonymity entropy for all users.

3.4. Problem Statement. Given the attacker's strategies and the defender's strategies, the problem is to find the relationship between the attack strategies and the performance of defense strategies, and the relationship between the data accuracy requirements and the performance of defense strategies. Then, based on these anlysis results, we find the optimal defense strategies for different attack scenarios.

In order to address these problems, we must consider (i) how to model the strategy selection decision behavior of the adversary and defender, and (ii) that the defender may not know the adversary's knowledge.

4. Attack and Defense Game

In this section, we introduce the attack and defense game model to capture the strategy selection decision behavior of the adversary and defender. We first define the game model and the concept of Nash Equilibrium (NE) throughout the paper, and then we present different attack strategies and defense strategies.

4.1. Game Model. The game G is defined as a triplet (P, S, U), where P is the set of players, S is the set of strategies, and U is the set of payoff functions [26].

Players. The set of players $P = \{P_i \mid 0 < i \leq I\}$, here $I = 2$, corresponds to the adversary and defender. There are two types of adversaries: Global Passive Adversary (GPA) and Local Active Adversary (LAA) [4].

Strategy. The set of strategies in the games is $S = \{S_i \mid 0 < i \leq I\}$, where S_1, S_2 are the set of strategies of the adversary and defender, respectively. We will describe them in detail in Sections 4.3 and 4.4.

Payoff Function. When the defender knows the side information that the adversary has collected, we use complete information games. In a complete information game, the payoff function of the adversary is $u_1(s_1, s_2) = H(L_T \mid R) - \gamma_1$, and the payoff function of the defender is $u_2(s_1, s_2) = H(L_T \mid \Omega) - \gamma_2$, where γ_1, γ_2 are the cost of attack and defense, respectively. In order to maximize attack power, γ_1 is set to 0. The defense cost γ_2 includes both the cost of implementing defensive strategies and the damage to data accuracy.

Typically, the defender does not know all the side information that the adversary has collected. Hence, we consider the suggestions proposed by Harsanyi [27]. We introduce a new player named Nature, which assigns a type θ to the adversary according to a prior distribution p. θ can be considered as the side information that the adversary has collected. Then, the payoff functions are expressed as $u_i(s_1, s_2(\theta))$.

4.2. Equilibrium Concepts. In complete information games, Nash equilibrium (NE) can be defined as follows.

Definition 1. A strategy profile $s^* = (s_i^*, s_{-i}^*)$ is a Nash equilibrium if, for each player i,

$$u_i(s_i^*, s_{-i}^*) \geq u_i(s_i, s_{-i}^*), \quad \forall s_i \in S_i. \quad (4)$$

In other words, in a NE, none of the players can unilaterally change his strategy to increase his payoff. A player can also play each of his pure strategies with some probability using mixed strategies. A mixed strategy σ_i of player i is a probability distribution defined over the pure strategies s_i.

In incomplete information games, we adopt the concept of Bayesian Nash equilibrium [21].

Definition 2. A strategy profile $s^* = (s_i^*(\theta_i), s_{-i}^*(\theta_{-i}))$ is a pure-strategy Bayesian Nash equilibrium (BNE) if, for each player i,

$$s^* \in \arg\max_{s_i \in S_i} \sum_{\theta_{-i}} p(\theta_{-i}) \cdot u_i(s_i, s_{-i}^*(\theta_{-i})), \quad \forall \theta_i, \quad (5)$$

where θ_{-i} is the type of player i's opponents, and $p(\theta_i)$ is the prior distribution of θ_i.

4.3. Attack Strategies

4.3.1. Attack Scenarios. According to the two types of adversaries, an attack can be classified as two scenarios: passive attack and active attack.

Scenario A: Passive Attack. In this setting, the adversary is given the complete (anonymized) traces. The adversary's goal is, given some pieces of side information about a victim, to identify in some optimal fashion the complete path history of the chosen victim. The key assumptions are (i) the adversary is passive that it does not actively go out to seek encounters with potential victims and (ii) the side information given to the adversary contains noise. If sampled times $\{\tau_k\}$, at which the actual node locations are published, are equally spaced, and $\{t_k\}$ is the time instants at which some side information about the victim's locations are revealed, passive attack can be divided into the two following attacks.

Attack 1 (A1). The side information references time instants that coincide with sampled times in the trace only, we have $\{t_k \mid k = 1, 2, \ldots\} \subset \{\tau_k \mid k = 1, 2, \ldots\}$.

Attack 2 (A2). The side information references time instants between two consecutive sampled times in the set of traces, we have $\{t_k \mid k = 1, 2, \ldots\} \not\subset \{\tau_k \mid k = 1, 2, \ldots\}$, and for each t_k, there exists $\widetilde{k}$ such that,

$$t_k = \lambda_k \tau_{\widetilde{k}} + (1 - \lambda_k)\, \tau_{\widetilde{k}+1}, \quad 0 \le \lambda_k < 1. \tag{6}$$

A2 is the more general attack. To some extent, A1 can be considered as a special case of A2, that is, for each k, $\lambda_k = 0$. We assume that the adversary will attempt to use all known information in its inference strategy, by employing some form of Bayesian inference. In applying the Bayesian inference, the adversary can make use of some general knowledge, including constraints on nodal movements imposed by geography of the roads, and general movement preferences of the nodes.

Scenario B: Active Attack. The adversary is active in this scenario that it obtains side information about victims by encountering the victims. The adversary can obtain traces in a real time and gradual fashion, that is, as time progresses, the adversary is provided with the trace information together with the information acquired up to the real time instants. The goal here is to identify as many traces as possible. If L_M is the trace of the adversary M, active attack can be divided into the following attacks.

Attack 1 (B1). The adversary stays at one fixed location, that is, for any j and k, $L_M(\tau_j) = L_M(\tau_k)$.

Attack 2 (B2). The adversary moves to maximize the amount of useful side information, that is, there exists at least one pair of i and j such that $L_M(\tau_j) \neq L_M(\tau_k)$.

We assume that after encountering a victim, the adversary will not attempt to follow the victim. Because the objective of the adversary is to identify as many trace identities as possible.

4.3.2. Strategies for A1 and A2. As noted before, the side information often contains noise. The adversary thus needs to perform Bayesian inference or use the maximum likelihood estimator to make the best guess. The goal is, given R, to find the L_i that gives the best match. The formulation of such a procedure is described below. Given $R = \{R(t_k) \mid k = 1, 2, \ldots\}$, compute

$$\begin{aligned}\Pr(L_i \mid R) &= \frac{\Pr(L_i, R(t_k))}{\Pr(R(t_k))} \\ &= \frac{\Pr(R(t_k) \mid L_i)\Pr(L_i)}{\sum_{j=1}^{N} \Pr(R(t_k) \mid L_j)\Pr(L_j)}, \quad k = 1, 2, \ldots.\end{aligned} \tag{7}$$

The goal of the maximum likelihood estimator is to find i which maximizes the expression (7). Note that the denominator is a constant. In addition, without any knowledge about how the victim is chosen, we set the priori distribution of the victim to be uniform: as follows, $P(L_i) = 1/N$, $i = 1, 2, \ldots, N$. Hence the solution of the maximum likelihood estimator is given by

$$\max_{i=1,2,\ldots,N} \Pr(R(t_k) \mid L_i), \quad k = 1, 2, \ldots. \tag{8}$$

For A1 and A2, the expression (8) can be given in the following form.

Scenario A1. If the noise in the side information Z_k is independent and identically distributed, and obey some given distribution $\Pr_Z$, the expression (8) can be written as

$$\Pr(R(t_k) \mid L_i) = \prod_k \Pr_Z(R(t_k) - L_i(t_k)), \tag{9}$$

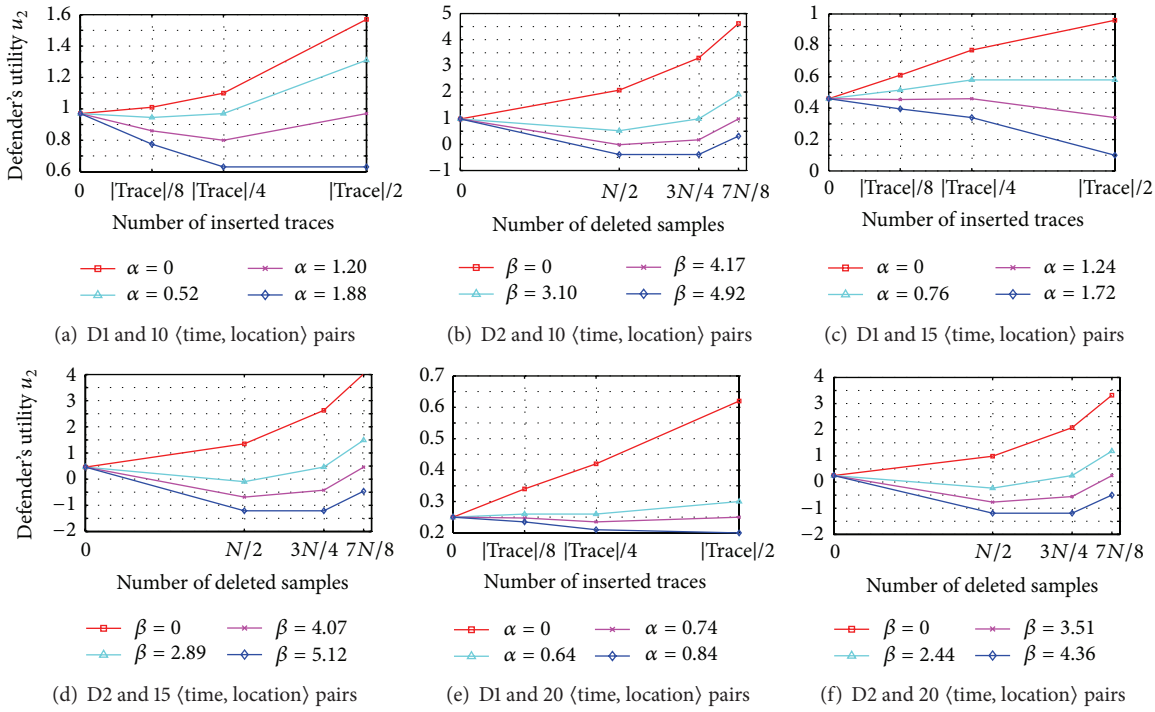
where $R(t_k) - L_i(t_k) = Z_k$, this location difference is computed using the Cartesian distance between the two cells [4].

Scenario A2. If node mobility obeys the Markov model, (8) can be given by

$$\begin{aligned}&\Pr(R(t_k) \mid L_i) \\ &\quad = \Pr(R(t_k) \mid L_i(\{\tau_k \mid k = 1, 2 \ldots\})) \\ &\quad = \frac{\prod_k [\Pr(L_i(\tau_{\widetilde{k}+1}) \mid R(t_k)) \times \Pr(R(t_k) \mid L_i(\tau_{\widetilde{k}}))]}{\prod_k \Pr(L_i(\tau_{\widetilde{k}+1}) \mid L(\tau_{\widetilde{k}}))},\end{aligned} \tag{10}$$

where $t_k = \lambda_k \tau_{\widetilde{k}} + (1 - \lambda_k)\tau_{\widetilde{k}+1}$, and when λ_k is a constant, the Markov process of node mobility is steady.

The expression (9) can be greatly simplified if the noise Z_k obeys specific forms, such as normal distribution or uniform distribution. Therefore, the adversary can use some heuristic approaches [4] to identify the victim's trace. In the following we consider four strategies used by the adversary



(a) D1 and 10 ⟨time, location⟩ pairs (b) D2 and 10 ⟨time, location⟩ pairs (c) D1 and 15 ⟨time, location⟩ pairs

(d) D2 and 15 ⟨time, location⟩ pairs (e) D1 and 20 ⟨time, location⟩ pairs (f) D2 and 20 ⟨time, location⟩ pairs

FIGURE 2: Optimal defense strategies at different values of α, β.

to identify the victim's trace from the published trace set. We first describe them for scenario A1 as follows.

(i) Maximum likelihood estimation approach (MLE). This is the same as formulation (9), that is, the similarity value of trace i is given by

$$\prod_k \Pr_Z \left(R\left(t_k\right) - L_i\left(t_k\right)\right), \tag{11}$$

where the trace with the maximum similarity value is declared to be the victim's.

(ii) Minimum square approach (MSQ). When the Z_k's takes normal distribution $N(0, \sigma^2)$, that is, $\Pr(R(t_k) \mid L_i) = C \exp\{-(\sum_k |R(t_k) - L_i(t_k)|^2)/(2\sigma^2)\}$, $k = 1, 2, \ldots$, for some constant C. Hence, the maximum likelihood estimator is essentially the same as the following minimum square approach:

$$\min_i \sum_k \left|R\left(t_k\right) - L_i\left(t_k\right)\right|^2, \tag{12}$$

where the trace with the least similarity value is declared to be the victim's.

(iii) Basic approach (BAS). The adversary assumes that the noise is zero-mean and has a specific standard deviation (σ), but makes no assumption about its exact distribution. The adversary then computes the similarity value of trace i with the side information as follows:

$$\sum_{k=1}^{M} I_{2\sigma}\left(L_i\left(t_k\right), R\left(t_k\right)\right), \tag{13}$$

where $I_{2\sigma}(x, y) = 1$ if $|x - y| \le 2\sigma$ and 0 otherwise. Hence, the adversary accepts a trace as a potential candidate if the trace owner appears in a radius of $2\times\sigma$ of the revealed location. The trace with the maximum similarity value is declared to be the victim's.

(iv) Weighted exponential approach (EXP). In this approach, which is proposed and analyzed in [11], the adversary does not know the type of noise or its magnitude. Similar to BAS, the adversary maximizes the similarity value of trace i as follows:

$$\sum_{k=1}^{M} \frac{1}{w\left(R\left(t_k\right)\right)} \exp\left\{-\frac{1}{C}\left|L_i\left(t_k\right) - R\left(t_k\right)\right|\right\}, \tag{14}$$

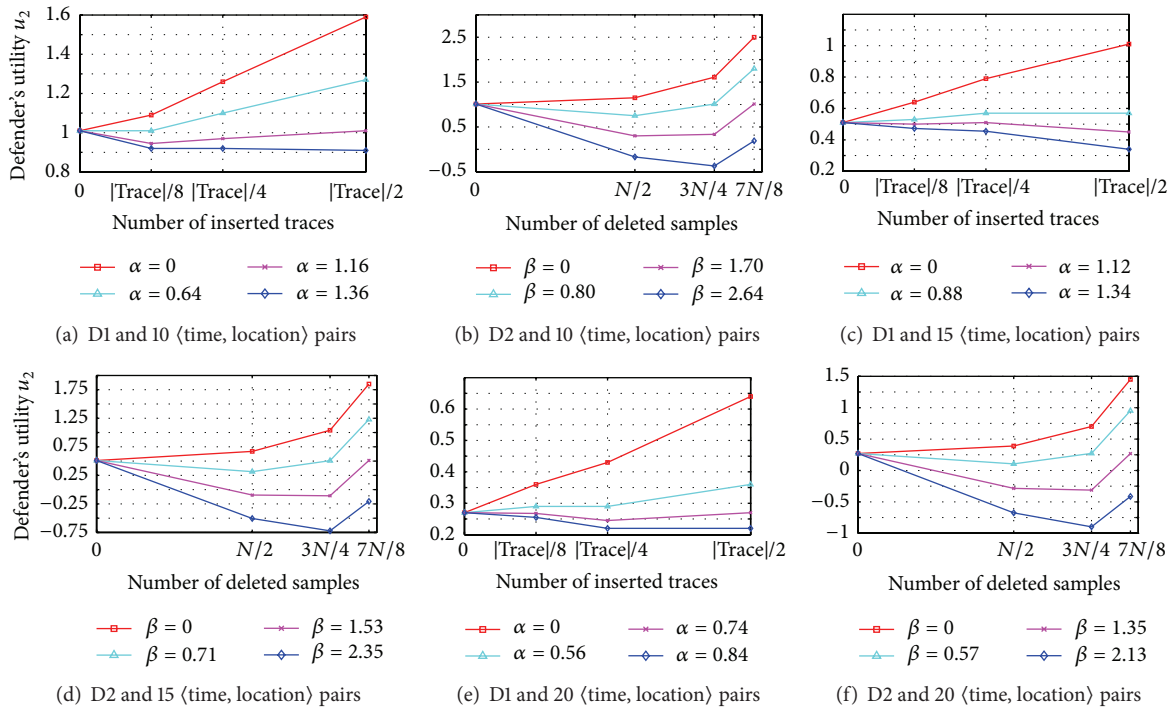
where $w(R(t_k))$ is some weight assigned to the revealed cell $R(t_k)$ and C is a constant.

The above formula can be easily modified for scenario A2. For convenience, the probability that the vehicle is on the cell l at time t_k for trace j is defined as the function $P_j : \Theta \times \{t_k \mid k = 1, 2, \ldots\} \to R_+$ as follows:

$$P_j\left(l, t_k\right) = \frac{\Pr\left(L_j\left(\tau_{\tilde{k}+1}\right) \mid R\left(t_k\right)\right) \times \Pr\left(R\left(t_k\right) \mid L_j\left(\tau_{\tilde{k}}\right)\right)}{\Pr\left(L_j\left(\tau_{\tilde{k}+1}\right) \mid L_j\left(\tau_{\tilde{k}}\right)\right)}, \tag{15}$$

where $l = \lambda_k L_j(\tau_{\tilde{k}}) + (1 - \lambda_k) L_j(\tau_{\tilde{k}+1})$, $\tau_{\tilde{k}} < t_k < \tau_{\tilde{k}+1}$. Then we have

$$\text{MLE}_2 \quad \prod_k \left(\sum_{l \in \Theta} P_j\left(l, t_k\right) \Pr_Z\left(R\left(t_k\right) - l\right)\right), \tag{16}$$



(a) D1 and 10 ⟨time, location⟩ pairs (b) D2 and 10 ⟨time, location⟩ pairs (c) D1 and 15 ⟨time, location⟩ pairs

(d) D2 and 15 ⟨time, location⟩ pairs (e) D1 and 20 ⟨time, location⟩ pairs (f) D2 and 20 ⟨time, location⟩ pairs

FIGURE 3: Optimal defense strategies at different values of α, β.

MSQ_2

$$\sum_k \left(\sum_{l \in \Theta} P_j(l, t_k) \left| R(t_k) - l \right|^2 \right), \tag{17}$$

BAS_2

$$\sum_k \left(\sum_{l \in \Theta} P_j(l, t_k) \times I_{2\sigma}(l, R(t_k)) \right), \tag{18}$$

EXP_2

$$\sum_k \left(\sum_{l \in \Theta} \frac{P_j(l, t_k)}{w(R(t_k))} \exp\left\{ -\frac{1}{C} \left| l - R(t_k) \right| \right\} \right). \tag{19}$$

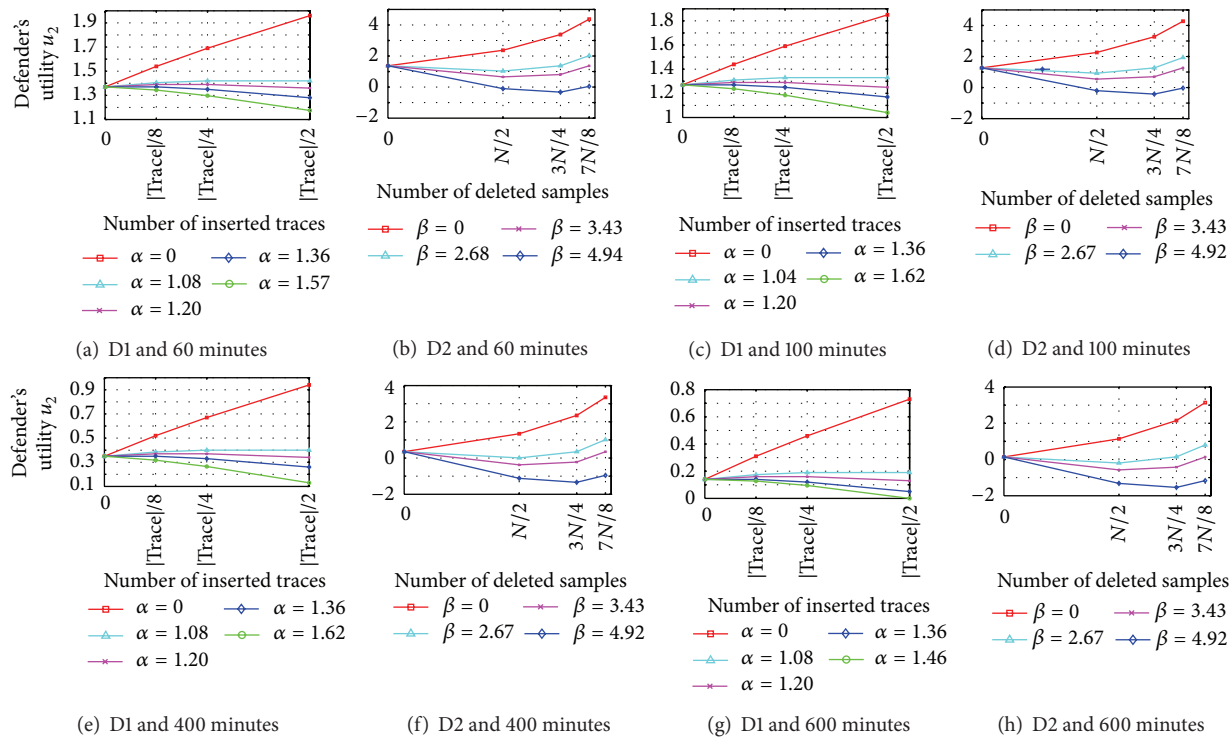
The four strategies have the same computational complexity, which is linear in the number of pieces of side information and the number of nodes. Notice that we assume attack strategies that only collect the side information about one victim. However, the strategies can be easily extended to the case in which the adversary collects the side information about several victims. In particular, the MLE approach can be used directly without modification, while a properly picked threshold can be used for the other attack strategies to remove traces from consideration if their similarity to the victim's trace is lower than the threshold.

4.3.3. Strategies for B1 and B2. In the active attack scenario, the adversary observes the participants directly. The published traces are revealed in a real-time and synchronized way with respect to the information collected by the adversary. As there is no noise when additional information is acquired, the adversary does not need to use any inference strategy. Based on the idea of excluding the unmatched traces [4], attack algorithm can be described as follows.

Illustrated in Algorithm 1, the attack algorithm takes as input the traces that are published progressively. The algorithm first assumes that all the traces are candidate traces for each victim. A trace is said to be a candidate trace of a victim if it appears at the same set of times and locations as when/where the adversary meets the victim. As time evolves, the adversary removes candidate traces which do not agree with the observed information about each victim from the set for that victim. When a victim's trace is identified, the identified trace is removed from the candidate set of other victims. Notice that the adversary may not identify a participant at times they meet each other, but the identification can occur at a later time when all but one candidate traces are identified and removed. Hence, the adversary identifies a participant more efficiently when it tries to identify as many participants as possible.

In the scenario B1, r is fixed, because the adversary always stays at one position. While r changes as the adversary moves in the scenario B2. B2 has experimentally a better performance than B1. The reason is because mobile nodes typically obtain more side information than stationary nodes.

4.4. Defense Strategies. There are two types of defense strategies: anonymous and cloaking techniques. Anonymous techniques which hide the true identities of users can be implemented by several ways. For example, one user uses



(a) D1 and 60 minutes (b) D2 and 60 minutes (c) D1 and 100 minutes (d) D2 and 100 minutes

(e) D1 and 400 minutes (f) D2 and 400 minutes (g) D1 and 600 minutes (h) D2 and 600 minutes

Figure 4: Optimal defense strategies at different values of α, β for different preformed time.

Input: $\{L_i \mid i = 1, 2, \ldots, |\mathrm{Tr}|\}$
Output: Identified traces
(1) **for** $m = 0$ to $|\mathrm{Tr}|$ **do**
(2) Candidate$_m$ $= \{L_i \mid i = 1, 2, \ldots, |\mathrm{Tr}|\}$;
(3) **end for**
(4) **while** s_k not ended **do**
(5) for each node i met at τ_k and $j \in$ Candidate$_i$
(6) **if** met node i at location r at τ_k and $L_j(\tau_k)! = r$ **then**
(7) remove trace j from Candidate$_i$;
(8) **if** |Candidate$_i$| $= 1$ **then**
(9) L_j in Candidate$_i$ is the identified trace and remove it from other candidate set;
(10) **end if**
(11) $k++$;
(12) **end if**
(13) **end while**

Algorithm 1: Attack algorithm for B1 and B2.

one or more pseudonyms [28–31], or a group of users share the same ID [32]. However, the true identity of each vehicle is only replaced by a random identifier in VSNs, so we will not discuss the anonymous techniques. Cloaking techniques, such as introducing noise data or reducing the recorded data, also can be used to protect users' privacy. But using cloaking techniques will impact on the truth of the published information, so we should balance the users' privacy and the data accuracy required by different applications.

In VSNs, the defender's (i.e., the traffic control center or other authorities) objective is to increase the hardness for the adversary to identify a trace in the anonymous published traces. The defender can insert some bogus traces or delete the recorded data at some sampled times to achieve its objective. If $\{\tau_1, \tau_2, \ldots, \tau_k, \ldots\}$ is the set of the sampled times in the set of the published traces Tr, the defense strategies can be expressed as follows.

Defense 1 (D1). m bogus traces are inserted into Tr to form a new set of trace Tr$'$, such that Tr$' \supset$ Tr and $|\mathrm{Tr}'| = |\mathrm{Tr}| + m$.

Defense 2 (D2). n sampled times are deleted in $\{\tau_1, \tau_2, \ldots, \tau_k, \ldots\}$ to form a new sequence $\{\tau_1', \tau_2', \ldots, \tau_k', \ldots\}$, such that $\{\tau_1, \tau_2, \ldots, \tau_k, \ldots\} \supset \{\tau_1', \tau_2', \ldots, \tau_k', \ldots\}$.

Theorem 3. *D1 can provide nodes with a higher trace privacy level.*

Proof. Before the execution of D1, the trace privacy levels of nodes meet as follows:

$$H(L_T) = -\sum_{i=1}^{|\mathrm{Tr}|} p_i \log_2 p_i$$

$$\leq \sum_{i=1}^{|\mathrm{Tr}|} \frac{1}{|\mathrm{Tr}|} \log_2 |\mathrm{Tr}|$$

$$= \log_2 |\mathrm{Tr}|. \tag{20}$$

After the execution of D1, the trace privacy levels of nodes meet as follows:

$$\begin{aligned} H(L_T) &= -\sum_{i=1}^{|\mathrm{Tr}'|} p_i \log_2 p_i \\ &\le \sum_{i=1}^{|\mathrm{Tr}'|} \frac{1}{|\mathrm{Tr}'|} \log_2 |\mathrm{Tr}'| \\ &= \log_2 |\mathrm{Tr}'| \\ &= \log_2 |\mathrm{Tr} + m| . \end{aligned} \tag{21}$$

Since $\log_2|\mathrm{Tr}+m| > \log_2|\mathrm{Tr}|$, D1 provides nodes with a higher trace privacy level. □

Lemma 4. *If f is a concave function and X is a random variable,*

$$Ef(X) \le f(EX). \tag{22}$$

Proof. For a two-mass-point distribution, the inequality becomes

$$p_1 f(x_1) + p_2 f(x_2) \le f(p_1 x_1 + p_2 x_2), \tag{23}$$

which follows directly from the definition of concave functions. Suppose that the lemma is true for distributions with $k-1$ mass points. Then, writing $p_i' = p_i/(1-p_k)$, $i = 1, 2, \ldots, k-1$, we have

$$\begin{aligned} \sum_{i=1}^{k} p_i f(x_i) &= p_k f(x_k) + (1-p_k) \sum_{i=1}^{k-1} p_i' f(x_i) \\ &\le p_k f(x_k) + (1-p_k) f\left(\sum_{i=1}^{k-1} p_i' x_i \right) \\ &\le f\left(p_k x_k + (1-p_k) \sum_{i=1}^{k-1} p_i' x_i \right) \\ &= f\left(\sum_{i=1}^{k} p_i x_i \right), \end{aligned} \tag{24}$$

where the first inequality follows from the induction hypothesis and the second follows from the definition of concavity. □

Theorem 5. *If the probability density function of l is concave over the interval $[R(t_k)-\varepsilon, R(t_k)+\varepsilon]$, D2 reduces the probability that the victim's trace is identified by the adversary.*

Proof. Let $\tau_{\tilde{k}}$ be the deleted sampled time. When there exists t_k such that $\tau_{\tilde{k}} = t_k$, A1 turns into A2. Since the probability density function of l is concave over $[R(t_k)-\varepsilon, R(t_k)+\varepsilon]$, $\Pr_Z(R(t_k)-l)$ is concave over $[R(t_k)-\varepsilon, R(t_k)+\varepsilon]$. Then, we have

$$\begin{aligned} \Pr(R(t_k) \mid L_i) &= \prod_k \Pr_Z(R(t_k) - L_i(t_k)) \\ &\ge \prod_k \left(\sum_{l\in\Theta} P_i(l, t_k) \Pr_Z(R(t_k) - l) \right) \\ &= \prod_k \left(\frac{\Pr(L_i(\tau_{\tilde{k}+1}) \mid R(t_k)) \Pr(R(t_k) \mid)}{\Pr(L_i(\tau_{\tilde{k}+1}) \mid L_i(\tau_{\tilde{k}-1}))} \right) \\ &= \Pr\left(R(t_k) \mid L_i\left(\left\{\tau_k' \mid k = 1, 2, \ldots\right\}\right)\right) \\ &= \Pr\left(R(t_k) \mid L_i'\right). \end{aligned} \tag{25}$$

When there is no such t_k, the adversary is always in A2. Then, we have

$$\begin{aligned} \Pr(R(t_k) \mid L_i) &= \Pr(R(t_k) \mid L_i(\{\tau_1, \tau_2, \ldots, \tau_k, \ldots\})) \\ &\ge \Pr\left(R(t_k) \mid L_i\left(\left\{\tau_1', \tau_2', \ldots, \tau_k', \ldots\right\}\right)\right) \\ &= \Pr\left(R(t_k) \mid L_i'\right), \end{aligned} \tag{26}$$

where $\{\tau_1, \tau_2, \ldots, \tau_k, \ldots\} \supset \{\tau_1', \tau_2', \ldots, \tau_k', \ldots\}$.

So, in both cases, the probability that the victim's trace is identified by the adversary will be reduced. □

Notice that it is reasonable to assume that the probability density function of l is concave over the interval $[R(t_k) - \varepsilon, R(t_k) + \varepsilon]$, because the collected side information $R(t_k)$ about l appears more frequently in the vicinity of l.

However, these defense strategies will bring some loss in data accuracy. The more the inserted bogus traces and the deleted sampled times, the more unreal the data. Hence, we assume that the defense cost γ is proportional to the inserted bogus traces and the deleted sampled times. We take into account the application requirements involved in the defense cost in a parameter γ. Then for A1, γ can be expressed as,

$$\gamma = \alpha \frac{m}{|\mathrm{Trace}|}, \tag{27}$$

where α is a system parameter that indicates the requirement of an application, |Trace| is the number of all the traces, m is the number of the inserted bogus traces.

Similarly to A1, γ for A2 can be expressed as:

$$\gamma = \beta \frac{n}{N}, \tag{28}$$

where β is a system parameter, N is the number of all the sampled times, and n is the number of the deleted sampled times in the N sampled times.

5. Analysis of Attack and Defense Game

In this section, we study both the passive and active attack scenarios. In the passive attack scenarios (A1 and A2),

Table 2: Complete information game for A1.

(a) The defender chooses D1

	$m = 0$	$m = \|\text{Trace}\|/8$	$m = \|\text{Trace}\|/4$	$m = \|\text{Trace}\|/2$
MLE	$0.35, 0.35$	$0.41, 0.41 - \gamma^1$	$0.56, 0.56 - \gamma^2$	$0.77, 0.77 - \gamma^3$
MSQ	$0.34, 0.34$	$0.40, 0.40 - \gamma^1$	$0.54, 0.54 - \gamma^2$	$0.76, 0.76 - \gamma^3$
BAS	$1.30, 1.30$	$1.49, 1.49 - \gamma^1$	$1.69, 1.69 - \gamma^2$	$2.06, 2.06 - \gamma^3$
EXP	$0.67, 0.67$	$0.77, 0.77 - \gamma^1$	$0.92, 0.92 - \gamma^2$	$1.18, 1.18 - \gamma^3$

(b) The defender chooses D2

	$n = 0$	$n = N/2$	$n = 3N/4$	$n = 7N/8$
MLE	$0.35, 0.35$	$1.13, 1.13 - \gamma^4$	$2.31, 2.31 - \gamma^5$	$3.75, 3.75 - \gamma^6$
MSQ	$0.34, 0.34$	$1.12, 1.12 - \gamma^4$	$2.30, 2.30 - \gamma^5$	$3.74, 3.74 - \gamma^6$
BAS	$1.30, 1.30$	$2.69, 2.69 - \gamma^4$	$4.47, 4.47 - \gamma^5$	$5.64, 5.64 - \gamma^6$
EXP	$0.67, 0.67$	$1.56, 1.56 - \gamma^4$	$2.72, 2.72 - \gamma^5$	$4.06, 4.06 - \gamma^6$

we consider games of complete and incomplete information. As the adversary can obtain the victims' positions accurately in the active attack scenarios (B1 and B2), the defender does not need to infer the side information the adversary obtained. Therefore, we only establish the complete information game in scenario B1 and B2.

The traffic data used in the experiments contains mobility traces of taxis in Beijing, China. It contains GPS coordinates of approximately 28,000 taxis collected in a month in Beijing [33]. The location updates are quite fine-grained the average time interval between two consecutive location updates is less than 30 sec. In the experiments, the adversary tries to identify the trace of one participant (randomly picked from all the participants) by gathering side information. The noisy randomly sampled ⟨*time, location*⟩ pairs from the trace are revealed to the adversary as side information, which the adversary utilizes to identify the complete movement history of the victim from the anonymous traces. The defender inserts some bogus traces (D1) or deletes the recorded data at some sampled times (D2) against the attack strategies implemented by the adversary.

5.1. Games for Scenario A1. The adversary has four attack strategies: MLE, MSQ, BAS, and EXP. The defender has two defense strategies: D1, and D2. In strategy D1, we set $m = 0, |\text{Trace}|/8, |\text{Trace}|/4, |\text{Trace}|/2$, where $|\text{Trace}|$ is the total number of the published traces. In strategy D2, we set $n = 0, N/2, 3N/4, 7N/8$, where N is the total number of the sampled times.

5.1.1. Analysis of Complete Information Game. Strategic form for complete information game in A1 is depicted as matrices, as in Table 2. Each player chooses a strategy simultaneously, and has common knowledge about the side information. We assumed that the side information contains 18 pairs of ⟨*time, location*⟩. In particular, since the adversary is still in scenario A1 when the defender uses strategy D2, the side information which is not at sampled times is not involved in calculating the payoff.

Table 3: Incomplete information game for Al.

(a) D1 and 10 ⟨time, location⟩ pairs

	$m = 0$	$m = \|\text{Trace}\|/8$	$m = \|\text{Trace}\|/4$	$m = \|\text{Trace}\|/2$
MLE	$0.99, 0.99$	$1.04, 1.04 - \gamma^1$	$1.12, 1.12 - \gamma^2$	$1.59, 1.59 - \gamma^3$
MSQ	$0.97, 0.97$	$1.01, 1.01 - \gamma^1$	$1.10, 1.10 - \gamma^2$	$1.57, 1.57 - \gamma^3$
BAS	$2.47, 2.47$	$2.59, 2.59 - \gamma^1$	$2.79, 2.79 - \gamma^2$	$3.47, 3.47 - \gamma^3$
EXP	$1.43, 1.43$	$1.51, 1.51 - \gamma^1$	$1.60, 1.60 - \gamma^2$	$2.05, 2.05 - \gamma^3$

(b) D2 and 10 ⟨time, location⟩ pairs

	$n = 0$	$n = N/2$	$n = 3N/4$	$n = 7N/8$
MLE	$0.99, 0.99$	$2.08, 2.08 - \gamma^4$	$3.32, 3.32 - \gamma^5$	$4.64, 4.64 - \gamma^6$
MSQ	$0.97, 0.97$	$2.07, 2.07 - \gamma^4$	$3.30, 3.30 - \gamma^5$	$4.62, 4.62 - \gamma^6$
BAS	$2.47, 2.47$	$4.05, 4.05 - \gamma^4$	$5.64, 5.64 - \gamma^5$	$6.64, 6.64 - \gamma^6$
EXP	$1.43, 1.43$	$2.51, 2.51 - \gamma^4$	$3.74, 3.74 - \gamma^5$	$4.92, 4.92 - \gamma^6$

(c) D1 and 15 ⟨time, location⟩ pairs

	$m = 0$	$m = \|\text{Trace}\|/8$	$m = \|\text{Trace}\|/4$	$m = \|\text{Trace}\|/2$
MLE	$0.47, 0.47$	$0.62, 0.62 - \gamma^1$	$0.79, 0.79 - \gamma^2$	$0.99, 0.99 - \gamma^3$
MSQ	$0.46, 0.46$	$0.61, 0.61 - \gamma^1$	$0.77, 0.77 - \gamma^2$	$0.96, 0.96 - \gamma^3$
BAS	$1.60, 1.60$	$1.83, 1.83 - \gamma^1$	$2.06, 2.06 - \gamma^2$	$2.47, 2.47 - \gamma^3$
EXP	$0.83, 0.83$	$1.03, 1.03 - \gamma^1$	$1.18, 1.18 - \gamma^2$	$1.43, 1.43 - \gamma^3$

(d) D2 and 15 ⟨time, location⟩ pairs

	$n = 0$	$n = N/2$	$n = 3N/4$	$n = 7N/8$
MLE	$0.47, 0.47$	$1.36, 1.36 - \gamma^4$	$2.64, 2.64 - \gamma^5$	$4.03, 4.03 - \gamma^6$
MSQ	$0.46, 0.46$	$1.35, 1.35 - \gamma^4$	$2.63, 2.63 - \gamma^5$	$4.02, 4.02 - \gamma^6$
BAS	$1.60, 1.60$	$3.05, 3.05 - \gamma^4$	$4.92, 4.92 - \gamma^5$	$6.27, 6.27 - \gamma^6$
EXP	$0.83, 0.83$	$1.86, 1.86 - \gamma^4$	$3.06, 3.06 - \gamma^5$	$4.27, 4.27 - \gamma^6$

(e) D1 and 20 ⟨time, location⟩ pairs

	$m = 0$	$m = \|\text{Trace}\|/8$	$m = \|\text{Trace}\|/4$	$m = \|\text{Trace}\|/2$
MLE	$0.26, 0.26$	$0.36, 0.36 - \gamma^1$	$0.44, 0.44 - \gamma^2$	$0.63, 0.63 - \gamma^3$
MSQ	$0.25, 0.25$	$0.34, 0.34 - \gamma^1$	$0.42, 0.42 - \gamma^2$	$0.62, 0.62 - \gamma^3$
BAS	$1.12, 1.12$	$1.32, 1.32 - \gamma^1$	$1.45, 1.45 - \gamma^2$	$1.84, 1.84 - \gamma^3$
EXP	$0.57, 0.57$	$0.67, 0.67 - \gamma^1$	$0.78, 0.78 - \gamma^2$	$1.04, 1.04 - \gamma^3$

(f) D2 and 20 ⟨time, location⟩ pairs

	$n = 0$	$n = N/2$	$n = 3N/4$	$n = 7N/8$
MLE	$0.26, 0.26$	$1.00, 1.00 - \gamma^4$	$2.10, 2.10 - \gamma^5$	$3.33, 3.33 - \gamma^6$
MSQ	$0.25, 0.25$	$0.99, 0.99 - \gamma^4$	$2.08, 2.08 - \gamma^5$	$3.32, 3.32 - \gamma^6$
BAS	$1.12, 1.12$	$2.47, 2.47 - \gamma^4$	$4.05, 4.05 - \gamma^5$	$5.64, 5.64 - \gamma^6$
EXP	$0.57, 0.57$	$1.43, 1.43 - \gamma^4$	$2.51, 2.51 - \gamma^5$	$3.74, 3.74 - \gamma^6$

We observe that Nash equilibriums depend on the value of the defense cost γ in this game. when the defense cost is zero, that is, $\gamma = 0$, (MSQ, $m = |\text{Trace}|/2$) is a pure-strategy Nash equilibrium in the left strategic form. And (MSQ, $n = 7N/8$) is a pure-strategy Nash equilibrium in the right strategic form. when $\gamma \neq 0$, from (27) and (28), we have $\gamma^1 = \alpha/8$, $\gamma^2 = \alpha/4$, $\gamma^3 = \alpha/2$, $\gamma^4 = \beta/2$, $\gamma^5 = 3\beta/4$, $\gamma^6 = 7\beta/8$. For the left strategic form, the Nash equilibrium is (MSQ, $m = |\text{Trace}|/2$) if $0 < \alpha \leq 0.84$ and (MSQ, $m = 0$) if $\alpha > 0.84$. For the right strategic form, the Nash equilibrium is (MSQ, $n = 7N/8$) if $0 < \beta \leq 3.89$ and (MSQ, $n = 0$)

Table 4: Complete information game for A2.

(a) The defender chooses D1

	$m = 0$	$m = \|\text{Trace}\|/8$	$m = \|\text{Trace}\|/4$	$m = \|\text{Trace}\|/2$
MLE_2	$0.37, 0.37$	$0.43, 0.43 - \gamma^1$	$0.57, 0.57 - \gamma^2$	$0.78, 0.78 - \gamma^3$
MSQ_2	$0.38, 0.38$	$0.44, 0.44 - \gamma^1$	$0.59, 0.59 - \gamma^2$	$0.79, 0.79 - \gamma^3$
BAS_2	$0.80, 0.80$	$0.97, 0.97 - \gamma^1$	$1.10, 1.10 - \gamma^2$	$1.35, 1.35 - \gamma^3$
EXP_2	$0.67, 0.67$	$0.80, 0.80 - \gamma^1$	$0.96, 0.96 - \gamma^2$	$1.18, 1.18 - \gamma^3$

(b) The defender chooses D2

	$n = 0$	$n = N/2$	$n = 3N/4$	$n = 7N/8$
MLE_2	$0.37, 0.37$	$0.50, 0.50 - \gamma^4$	$0.84, 0.84 - \gamma^5$	$1.43, 1.43 - \gamma^6$
MSQ_2	$0.38, 0.38$	$0.58, 0.58 - \gamma^4$	$1.11, 1.11 - \gamma^5$	$2.37, 2.37 - \gamma^6$
BAS_2	$0.80, 0.80$	$1.04, 1.04 - \gamma^4$	$1.58, 1.58 - \gamma^5$	$2.78, 2.78 - \gamma^6$
EXP_2	$0.76, 0.76$	$0.92, 0.92 - \gamma^4$	$1.43, 1.43 - \gamma^5$	$2.44, 2.44 - \gamma^6$

Table 5: Incomplete information game for A2.

(a) D1 and 10 ⟨time, location⟩ pairs

	$m = 0$	$m = \|\text{Trace}\|/8$	$m = \|\text{Trace}\|/4$	$m = \|\text{Trace}\|/2$
MLE_2	$1.01, 1.01$	$1.09, 1.09 - \gamma^1$	$1.26, 1.26 - \gamma^2$	$1.59, 1.59 - \gamma^3$
MSQ_2	$1.02, 1.02$	$1.11, 1.11 - \gamma^1$	$1.27, 1.27 - \gamma^2$	$1.61, 1.61 - \gamma^3$
BAS_2	$1.56, 1.56$	$1.69, 1.69 - \gamma^1$	$1.89, 1.89 - \gamma^2$	$2.18, 2.18 - \gamma^3$
EXP_2	$1.45, 1.45$	$1.56, 1.56 - \gamma^1$	$1.78, 1.78 - \gamma^2$	$2.05, 2.05 - \gamma^3$

(b) D2 and 10 ⟨time, location⟩ pairs

	$n = 0$	$n = N/2$	$n = 3N/4$	$n = 7N/8$
MLE_2	$1.01, 1.01$	$1.15, 1.15 - \gamma^4$	$1.61, 1.61 - \gamma^5$	$2.50, 2.50 - \gamma^6$
MSQ_2	$1.02, 1.02$	$1.26, 1.26 - \gamma^4$	$1.84, 1.84 - \gamma^5$	$3.17, 3.17 - \gamma^6$
BAS_2	$1.56, 1.56$	$1.86, 1.86 - \gamma^4$	$2.45, 2.45 - \gamma^5$	$3.65, 3.65 - \gamma^6$
EXP_2	$1.45, 1.45$	$1.75, 1.75 - \gamma^4$	$2.30, 2.30 - \gamma^5$	$3.25, 3.25 - \gamma^6$

(c) D1 and 15 ⟨time, location⟩ pairs

	$m = 0$	$m = \|\text{Trace}\|/8$	$m = \|\text{Trace}\|/4$	$m = \|\text{Trace}\|/2$
MLE_2	$0.51, 0.51$	$0.64, 0.64 - \gamma^1$	$0.79, 0.79 - \gamma^2$	$1.01, 1.01 - \gamma^3$
MSQ_2	$0.53, 0.53$	$0.65, 0.65 - \gamma^1$	$0.81, 0.81 - \gamma^2$	$1.03, 1.03 - \gamma^3$
BAS_2	$1.03, 1.03$	$1.18, 1.18 - \gamma^1$	$1.36, 1.36 - \gamma^2$	$1.56, 1.56 - \gamma^3$
EXP_2	$0.89, 0.89$	$1.03, 1.03 - \gamma^1$	$1.20, 1.20 - \gamma^2$	$1.45, 1.45 - \gamma^3$

(d) D2 and 15 ⟨time, location⟩ pairs

	$n = 0$	$n = N/2$	$n = 3N/4$	$n = 7N/8$
MLE_2	$0.51, 0.51$	$0.67, 0.67 - \gamma^4$	$1.04, 1.04 - \gamma^5$	$1.85, 1.85 - \gamma^6$
MSQ_2	$0.53, 0.53$	$0.74, 0.74 - \gamma^4$	$1.29, 1.29 - \gamma^5$	$2.58, 2.58 - \gamma^6$
BAS_2	$1.03, 1.03$	$1.27, 1.27 - \gamma^4$	$1.80, 1.80 - \gamma^5$	$2.97, 2.97 - \gamma^6$
EXP_2	$0.89, 0.89$	$1.16, 1.16 - \gamma^4$	$1.67, 1.67 - \gamma^5$	$2.68, 2.68 - \gamma^6$

(e) D1 and 20 ⟨time, location⟩ pairs

	$m = 0$	$m = \|\text{Trace}\|/8$	$m = \|\text{Trace}\|/4$	$m = \|\text{Trace}\|/2$
MLE_2	$0.27, 0.27$	$0.36, 0.36 - \gamma^1$	$0.43, 0.43 - \gamma^2$	$0.64, 0.64 - \gamma^3$
MSQ_2	$0.28, 0.28$	$0.37, 0.37 - \gamma^1$	$0.45, 0.45 - \gamma^2$	$0.67, 0.67 - \gamma^3$
BAS_2	$0.69, 0.69$	$0.82, 0.82 - \gamma^1$	$0.96, 0.96 - \gamma^2$	$1.18, 1.18 - \gamma^3$
EXP_2	$0.56, 0.56$	$0.69, 0.69 - \gamma^1$	$0.81, 0.81 - \gamma^2$	$1.03, 1.03 - \gamma^3$

(f) D2 and 20 ⟨time, location⟩ pairs

	$n = 0$	$n = N/2$	$n = 3N/4$	$n = 7N/8$
MLE_2	$0.27, 0.27$	$0.39, 0.39 - \gamma^4$	$0.70, 0.70 - \gamma^5$	$1.45, 1.45 - \gamma^6$
MSQ_2	$0.28, 0.28$	$0.46, 0.46 - \gamma^4$	$0.95, 0.95 - \gamma^5$	$2.18, 2.18 - \gamma^6$
BAS_2	$0.69, 0.69$	$0.92, 0.92 - \gamma^4$	$1.43, 1.43 - \gamma^5$	$2.56, 2.56 - \gamma^6$
EXP_2	$0.56, 0.56$	$0.80, 0.80 - \gamma^4$	$1.28, 1.28 - \gamma^5$	$2.29, 2.29 - \gamma^6$

if $\beta > 3.89$. In other words, $n = 7N/8$ or $m = |\text{Trace}|/2$ is the optimal defense strategy when γ is small, whereas $n = 0$ or $m = 0$ becomes the optimal strategy when γ is very large. Because a larger γ means a higher data accuracy, which restricts the defense measures.

5.1.2. Analysis of Incomplete Information Game. Generally, the defender does not know how much side information obtained by the adversary. To solve the problem, Harsanyi [27] introduce a new player named Nature that turns an incomplete information game into a game with complete but imperfect information. We assume that Nature chooses the probability that side information contains 10 pairs of ⟨*time, location*⟩ is p_1, the probability that side information contains 15 pairs of ⟨*time, location*⟩ is p_2, and the probability that side information contains 20 pairs of ⟨*time, location*⟩ is $1 - p_1 - p_2$, as shown in Table 3. We observe that MSQ is a strictly dominated strategy for the adversary. Nash equilibriums are (MSQ, $m = |\text{Trace}|/2$), (MSQ, $n = 7N/8$) if $\gamma = 0$.

When $\gamma \neq 0$, we study which are the optimal defense strategies at different values of α, β. As shown in Figure 2, the maximum point of each line corresponds to the optimal defense strategy. For example, In Table 3(c), the optimal defense strategy is $m = |\text{Trace}|/2$ if $0 < \alpha \leq 0.76$, $m = |\text{Trace}|/4$ if $0.76 < \alpha \leq 1.24$ and $m = 0$ if $\alpha > 1.24$. in Table 3(d), $n = 7N/8$ if $0 < \beta \leq 4.07$ and $n = 0$ if $\beta > 4.07$. In other words, when γ is small, more inserted bogus traces or deleted recorded samples show a better performance. When γ is very large, doing nothing becomes the optimal strategy.

5.1.3. Discussion. In the complete information game, the adversary prefers the strategy MSQ. When the cost of defense measures is 0 or very low, we observe that the defense measures are more effective if there are more inserted bogus traces or deleted sampled times. The method of deleting sampled times is more effective than the method of inserting bogus traces. When the cost of defense cost is high, the defender prefers to do nothing.

In the incomplete information game, the adversary also prefers the strategy MSQ, while the optimal defense strategies depend on the values of α, β. If the defense cost γ is small, that is, when $0 < \alpha \leq 1.20$, the optimal defense strategy is $m = |\text{Trace}|/2$, and when $0 < \beta \leq 3.51$, the optimal defense strategy is $n = 7N/8$. If the defense cost γ is high, that is, when $\alpha > 1.24$, the optimal defense strategy is $m = 0$, and when $\beta > 4.17$, the optimal defense strategy is $n = 0$.

5.2. Games for Scenario A2. In scenario A2, the adversary has four attack strategies: MLE_2, MSQ_2, BAS_2, and EXP_2, and the defender has two defense strategies. In addition,

Table 6: Complete information game for B1 and B2.

(a) D1 and 60 minutes

	$m = 0$	$m = \|\text{Trace}\|/8$	$m = \|\text{Trace}\|/4$	$m = \|\text{Trace}\|/2$
Bl	$2.27, 2.27$	$2.43, 2.43 - \gamma^1$	$2.59, 2.59 - \gamma^2$	$2.85, 2.85 - \gamma^3$
B2	$1.37, 1.37$	$1.54, 1.54 - \gamma^1$	$1.69, 1.69 - \gamma^2$	$1.96, 1.96 - \gamma^3$

(b) D2 and 60 minutes

	$n = 0$	$n = N/2$	$n = 3N/4$	$n = 7N/8$
Bl	$2.27, 2.27$	$3.27, 3.27 - \gamma^4$	$4.26, 4.26 - \gamma^5$	$5.28, 5.28 - \gamma^6$
B2	$1.37, 1.37$	$2.37, 2.37 - \gamma^4$	$3.38, 3.28 - \gamma^5$	$4.37, 4.37 - \gamma^6$

(c) D1 and 100 minutes

	$m = 0$	$m = \|\text{Trace}\|/8$	$m = \|\text{Trace}\|/4$	$m = \|\text{Trace}\|/2$
Bl	$1.68, 1.68$	$1.85, 1.85 - \gamma^1$	$2.01, 2.01 - \gamma^2$	$2.27, 2.27 - \gamma^3$
B2	$1.27, 1.27$	$1.44, 1.44 - \gamma^1$	$1.59, 1.59 - \gamma^2$	$1.85, 1.85 - \gamma^3$

(d) D2 and 100 minutes

	$n = 0$	$n = N/2$	$n = 3N/4$	$n = 7N/8$
Bl	$1.68, 1.68$	$2.68, 2.68 - \gamma^4$	$3.68, 3.68 - \gamma^5$	$4.68, 4.68 - \gamma^6$
B2	$1.27, 1.27$	$2.26, 2.26 - \gamma^4$	$3.27, 3.27 - \gamma^5$	$4.27, 4.27 - \gamma^6$

(e) D1 and 400 minutes

	$m = 0$	$m = \|\text{Trace}\|/8$	$m = \|\text{Trace}\|/4$	$m = \|\text{Trace}\|/2$
Bl	$0.37, 0.37$	$0.54, 0.54 - \gamma^1$	$0.69, 0.69 - \gamma^2$	$0.96, 0.96 - \gamma^3$
B2	$0.35, 0.35$	$0.52, 0.52 - \gamma^1$	$0.67, 0.67 - \gamma^2$	$0.94, 0.94 - \gamma^3$

(f) D2 and 400 minutes

	$n = 0$	$n = N/2$	$n = 3N/4$	$n = 7N/8$
Bl	$0.37, 0.37$	$1.37, 1.37 - \gamma^4$	$2.38, 2.38 - \gamma^5$	$3.37, 3.37 - \gamma^6$
B2	$0.35, 0.35$	$1.31, 1.34 - \gamma^4$	$2.35, 2.35 - \gamma^5$	$3.35, 3.35 - \gamma^6$

(g) D1 and 600 minutes

	$m = 0$	$m = \|\text{Trace}\|/8$	$m = \|\text{Trace}\|/4$	$m = \|\text{Trace}\|/2$
Bl	$0.14, 0.14$	$0.31, 0.31 - \gamma^1$	$0.46, 0.46 - \gamma^2$	$0.73, 0.73 - \gamma^3$
B2	$0.19, 0.19$	$0.36, 0.36 - \gamma^1$	$0.51, 0.51 - \gamma^2$	$0.77, 0.77 - \gamma^3$

(h) D2 and 600 minutes

	$n = 0$	$n = N/2$	$n = 3N/4$	$n = 7N/8$
Bl	$0.14, 0.14$	$1.14, 1.14 - \gamma^4$	$2.15, 2.15 - \gamma^5$	$3.14, 3.14 - \gamma^6$
B2	$0.19, 0.19$	$1.19, 1.19 - \gamma^4$	$2.18, 2.18 - \gamma^5$	$3.19, 3.19 - \gamma^6$

we assume that $m = 0, |\text{Trace}|/8, |\text{Trace}|/4, |\text{Trace}|/2$, and $n = 0, N/2, 3N/4, 7N/8$.

5.2.1. Analysis of Complete Information Game. Strategic form for complete information game in A2 is depicted as shown in Table 4. The defender has the knowledge about the side information obtained by the adversary. The side information contains 18 pairs of ⟨*time, location*⟩. We observe that Nash equilibriums also depend on the value of the defense cost γ. When $\gamma = 0$, the pure-strategy Nash equilibrium is (MLE_2, $m = |\text{Trace}|/2$) in Table 4(a), and (MLE_2, $n = 7N/8$) in Table 4(b). When $\gamma \neq 0$, the Nash equilibrium is (MLE_2, $m = |\text{Trace}|/2$) if $0 < \alpha \leq 0.82$ and (MLE_2, $m = 0$) if $\alpha > 0.82$ in Table 4(a). In Table 4(b), the Nash equilibrium is (MLE_2, $n = 7N/8$) if $0 < \beta \leq 1.21$ and (MLE_2, $n = 0$) if $\beta > 1.21$. From Table 2 and Table 4, we observe that the attacks in A2 have a better performance than that in A1, because the adversary can use the side information between two consecutive sampled times.

5.2.2. Analysis of Incomplete Information Game. Table 5 depicts the incomplete information game in scenario A2. MLE_2 is a strictly dominated strategy for the adversary. (MLE_2, $m = |\text{Trace}|/2$) and (MLE_2, $n = 7N/8$) are Nash equilibriums when $\gamma = 0$.

Figure 3 depicts the optimal defense strategies at different values of α, β. The maximum point of each line corresponds to the optimal defense strategy. In Figure 3(a), the optimal defense strategy is $m = |\text{Trace}|/2$ if $0 < \alpha \leq 1.16$ and $m = 0$ if $\alpha > 1.16$, and $n = 7N/8$ if $0 < \beta \leq 1.70$ and $n = 0$ if $\beta > 1.70$ in Figure 3(b). In Figure 3(c), the optimal defense strategy is $m = |\text{Trace}|/2$ if $0 < \alpha \leq 0.88$, $m = |\text{Trace}|/4$ if $0.88 < \alpha \leq 1.12$ and $m = 0$ if $\alpha > 1.12$, and $n = 7N/8$ if $0 < \beta \leq 1.53$ and $n = 0$ if $\beta > 1.53$ in Figure 3(d). In Figure 3(e), the optimal defense strategy is $m = |\text{Trace}|/2$ if $0 < \alpha \leq 0.74$ and $m = 0$ if $\alpha > 0.74$, and $n = 7N/8$ if $0 < \beta \leq 1.35$ and $n = 0$ if $\beta > 1.35$ in Figure 3(f). From Figure 2 and Figure 3, we also observe that the attacks in A2 have a better performance than that in A1.

5.2.3. Discussion. In the A2 complete information game, the adversary prefers the strategy MLE_2. When the cost of defense measures is 0 or very low, the defense measures are more effective if there are more inserted bogus traces or deleted sampled times. Compared with A1, the method of deleting sampled times in A2 has a lower performance, but still better than the method of inserting bogus trace. When the cost of defense cost is high, the defender also prefers to do nothing.

In the A2 incomplete information game, the adversary also prefers the strategy MLE_2, while the optimal defense strategies depend on the values of α, β. If the defense cost γ is small, that is, when $0 < \alpha \leq 0.74$, the optimal defense strategy is $m = |\text{Trace}|/2$, and when $0 < \beta \leq 1.35$, the optimal defense strategy is $n = 7N/8$. If the defense cost γ is high, that is, when $\alpha > 1.16$, the optimal defense strategy is $m = 0$, and when $\beta > 1.70$, the optimal defense strategy is $n = 0$.

5.3. Games for Scenario B1 and B2. Because the goal of the adversary is to identify as many traces as possible, the adversary does not need to use any inference strategy. We assume that the attack strategies are B1 and B2. The defender has two defense strategies, we set $m = 0, |\text{Trace}|/8, |\text{Trace}|/4, |\text{Trace}|/2$ in D1, and $n = 0, N/2, 3N/4, 7N/8$ in D2. Table 6 depicts the strategic form for complete information game in A2, where attack algorithm preformed 60, 100, 400, and 600 minutes. When $\gamma = 0$, the Nash equilibriums are (B2, $m = |\text{Trace}|/2$) and (B2, $n = 7N/8$) if the attack algorithm preformed 60, 100, and 400 minutes, and (B1, $m = |\text{Trace}|/2$) and (B1, $n = 7N/8$) if the attack algorithm preformed 600 minutes.

When $\gamma \neq 0$, the optimal defense strategies at different values of α, β for different preformed time are depicted

as shown in Figure 4. The maximum point of each line corresponds to the optimal defense strategy. From Figures 4(a)–4(h), we observe that the optimal defense strategy is $m = |\text{Trace}|/2$ when $0 < \alpha \leq 1.04$, $m = |\text{Trace}|/4$ when $1.08 < \alpha \leq 1.20$, $m = |\text{Trace}|/8$ when $1.20 < \alpha \leq 1.36$, $m = 0$ when $\alpha > 1.36$, and $n = 7N/8$ when $0 < \beta \leq 3.43$, $n = 0$ when $\beta > 3.43$.

In the complete information game, the adversary prefers B2 if the time that the attack algorithm performs is short, B1 if the time that the attack algorithm performs is long. It is because that when time is long, the adversary at one position can also meet other victims with a high probability. When $\gamma = 0$, the defense measures are more effective if there are more inserted bogus traces or deleted sampled times. When $\gamma \neq 0$, the optimal defense strategies depend on the value of α, β.

6. Conclusion

In this paper, we analyze data privacy aspects of VSNs by using a game-theoretic model. We first quantify attack power and defense objectives for recording and comparing to the performance. Then, we define an attack and defense game model which can capture the strategy selection decision behavior of the adversary and defender. We also show the effectiveness of defense strategies. Finally, we establish and analyze the complete information and incomplete information games for passive and active attack scenarios based on real world traffic data. Through the analysis results, we show that attack strategies in different scenarios show different performances. More inserted bogus traces or deleted recorded samples show a better performance when the cost of defense measures is small, whereas doing nothing becomes the best strategy when the cost of defense measures is very large. We also present the optimal defense strategy that provides the defender with the maximum utility when the adversary implements the optimal attack strategy. Therefore, our analysis results are useful for designing appropriate privacy protection mechanisms.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The authors would like to thank Xiang Lu from the Institute of Information Engineering, Chinese Academy of Science, for helping revise the typos and grammar mistakes throughout this paper. This study is supported in part by the China 973 under Grant no. 2011CB302902, the NSF China Major Program (60933011, 61202099), National High-Tech R&D Program of China (863) under Grant no. 2013AA011102, Scientific and Technological Pilot Project under Grant no. XDA06040100.

References

[1] C. Zhang, R. Lu, X. Lin, P. H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proceedings of the 27th IEEE Conference on Computer Communications (INFOCOM '08)*, Phoenix, Ariz, USA, April 2008.

[2] Google Map, "Collection of anonymous location data," https://support.google.com/gmm/answer/2839958?hl=en&ref_topic=2839910.

[3] K. Mershad and H. Artail, "A framework for secure and efficient data acquisition in vehicular Ad Hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 2, pp. 536–551, 2013.

[4] C. Y. T. Ma, D. K. Y. Yau, N. K. Yip, and N. S. V. Rao, "Privacy vulnerability of published anonymous mobility traces," in *Proceedings of the 16th Annual International Conference on Mobile Computing and Networking (MobiCom '10)*, pp. 185–196, 2010.

[5] X. Lin, R. Lu, C. Zhang, H. Zhu, P. H. Ho, and X. Shen, "Security in vehicular Ad Hoc networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 88–95, 2008.

[6] M. A. Razzaque, S. A. Salehi, and S. M. Cheraghi, "Security and privacy in vehicular Ad-Hoc networks: survey and the road ahead," in *Wireless Networks and Security*, Signals and Communication Technology, pp. 107–132, Springer, New York, NY, USA, 2013.

[7] Y. A. de Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel, "Unique in the crowd: the privacy bounds of human mobility," Nature Science Report 3, 2013.

[8] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Achieving guaranteed anonymity in GPS traces via uncertainty-aware path cloaking," *IEEE Transactions on Mobile Computing*, vol. 9, no. 8, pp. 1089–1107, 2010.

[9] M. Gruteser and D. Grunwald, "Anonymous ge of lotion-based services through spatial and temporal cloaking," in *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services (MobiSys '03)*, pp. 42–31, San Francisco, Calif, USA, 2003.

[10] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: an effective strategy for location privacy in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 86–96, 2012.

[11] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," in *Proceedings of the IEEE Symposium on Security and Privacy (SP '08)*, pp. 111–125, Oakland, Calif, USA, May 2008.

[12] L. Huang, K. Matsuura, H. Yamane, and K. Sezako, "Towards modeling wireless location privacy," in *Proceedings of the 5th International Conference on Privacy Enhancing Technologies (PET '05)*, pp. 59–77, Vigo, Spain, 2005.

[13] R. Shokri, G. Theodorakopoulos, C. Troncoso, J. P. Hubaux, and J. Y. le Boudec, "Protecting location privacy: optimal strategy against localization attacks," in *Proceedings of the 19th ACM Conference on Computer and Communications Security*, Raleigh, NC, USA, October 2012.

[14] M. E. Nergiz, M. Atzori, Y. Saygin, and G. Barış, "Towards trajectory anonymization: a generalization-based approach," *Transactions on Data Privacy*, vol. 2, no. 1, pp. 47–75, 2009.

[15] T. Alpcan and T. Başar, "A game theoretic analysis of intrusion detection in access control systems," in *Proceedings of the 43rd*

IEEE Conference on Decision and Control (CDC '04), pp. 1568–1573, December 2004.

[16] T. Alpcan and T. Basar, "An intrusion detection game with limited observations," in *Proceedings of the 12th International Symposium on Dynamic Games and Applications*, July 2006.

[17] J. Grossklags, N. Christin, and J. Chuang, "Secure or insure? A game-theoretic analysis of information security games," in *Proceedings of the 17th International Conference on World Wide Web (WWW '08)*, pp. 209–218, April 2008.

[18] M. Raya, M. H. Manshaei, M. Félegyházi, and J. P. Hubaux, "Revocation games in ephemeral networks," in *Proceedings of the 15th ACM conference on Computer and Communications Security (CCS '08)*, pp. 199–210, October 2008.

[19] S. Reidt, M. Srivatsa, and S. Balfe, "The fable of the bees: incentivizing robust revocation decision making in ad hoc networks," in *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS '09)*, pp. 291–302, November 2009.

[20] T. Alpcan and S. Buchegger, "Security games for vehicular networks," *IEEE Transactions on Mobile Computing*, vol. 10, no. 2, pp. 280–290, 2011.

[21] J. Freudiger, M. H. Manshaei, J. P. Hubaux, and D. C. Parkes, "On non-cooperative location privacy: a game-theoretic analysis," in *Proceedings of the ACM Conference on Computer and Communications Security (CCS '09)*, pp. 324–337, Chicago, Ill, USA, November 2009.

[22] T. Chim, S. Yiu, L. Hui, and V. Li, "VSPN: VANET-based secure and privacy-preserving navigation," *IEEE Transactions on Computers*, 2012.

[23] Dedicated Short Range Communications (DSRC) Home, http://www.leearmstrong.com/DSRC/DSRCHomeset.htm.

[24] C. Zhang, X. Lin, R. Lu, P. H. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 6, pp. 3357–3368, 2008.

[25] H. Nissenbaum, "Privacy as contextual integrity," *Washington Law Review*, vol. 79, no. 1, pp. 119–158, 2004.

[26] D. Fudenberg and J. Tirole, *Game Theory*, MIT Press, Boston, Mass, USA, 1991.

[27] J. C. Harsanyi, "Games with incomplete information played by "Bayesian" players, I–III. Part I. The basic model," *Management Science*, vol. 14, no. 3, pp. 159–182, 1967.

[28] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 7, pp. 3589–3603, 2010.

[29] D. Huang, S. Misra, G. Xue, and M. Verma, "PACP: an efficient pseudonymous authentication-based conditional privacy protocol for VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 3, pp. 736–746, 2011.

[30] H. Lu, J. Li, and M. Guizani, "A novel ID-based authentication framework with adaptive privacy preservation for VANETs," in *Proceedings of the Computing, Communications and Applications Conference (ComComAp '12)*, pp. 345–350, Hong Kong, China, January 2012.

[31] "IEEE draft standard for wireless access in vehicular environments—security services for applications and management messages," IEEE P1609.2-2013, 2013.

[32] X. Lin, X. Sun, P. H. Ho, and X. Shen, "GSIS: a secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[33] Datatang Company, *Taxi GPS data of one city in North of China (200903)*, http://www.datatang.com/data/2987.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 542891, 19 pages
http://dx.doi.org/10.1155/2013/542891

Research Article

Vehicle Safety Enhancement System: Sensing and Communication

Huihuan Qian,[1,2] Yongquan Chen,[1] Yuandong Sun,[1] Niansheng Liu,[3] Ning Ding,[1] Yangsheng Xu,[1,2] Guoqing Xu,[1,2] Yunjian Tang,[4] and Jingyu Yan[1,2]

[1] *Department of Mechanical and Automation Engineering, The Chinese University of Hong Kong, Shatin, Hong Kong*
[2] *Shenzhen Institute of Advanced Technology, Shenzhen, Guangdong, China*
[3] *School of Computer Engineering, Jimei University, Xiamen, Fujian, China*
[4] *Chongqing Research Center for Information and Automation Technology, Chongqing Academy of Science and Technology, Chongqing, China*

Correspondence should be addressed to Guoqing Xu; gqxu@mae.cuhk.edu.hk

Received 11 April 2013; Accepted 4 October 2013

Academic Editor: Liusheng Huang

With the substantial increase of vehicles on road, driving safety and transportation efficiency have become increasingly concerned focus from drivers, passengers, and governments. Wireless networks constructed by vehicles and infrastructures provide abundant information to share for the sake of both enhanced safety and network efficiency. This paper presents the systematic research to enhance the vehicle safety by wireless communication, in the aspects of information acquisition through vehicle sensing, vehicle-to-vehicle (V2V) routing protocol for the highly dynamic vehicle network, vehicle-to-infrastructure (V2I) routing protocol for a tradeoff in real-time performance and load balance, and hardware implementation of V2V system with on-road test. Simulations and experimental result validate the feasibility of the algorithms and communication system.

1. Introduction

Safety-on-road is an important concern by all the drivers and passengers. With the sharp increase of vehicles on road, this has become increasingly important and challenging due to the higher probability of accidents. There are two aspects which can help prevent the occurrence or the deterioration of an accident. (1) Notify the immediately following vehicles to prevent chained accidents. However, bad weathers, such as fog, will prevent the drivers from obtaining the accident occurrence on time if merely from vision. (2) Notify other vehicles which may take the path encountering the accident spot, so as to avoid traffic jam. However, the current radio-based broadcasting approach requires human interaction for both accident detection and broadcasting and thus cannot achieve satisfying real-time performance. Therefore, a real-time vehicle safety enhancement system is needed for collision detection and vehicle status information sharing with nearby vehicles.

Two subsystems are necessary in the vehicle safety enhancement system. One subsystem, vehicular information acquisition subsystem (VIAS), takes charge of vehicular status sensing, so as to detect the accident information (e.g., position, etc.), classify the severity level (e.g., slight bumping, rolling over, etc.), as well as to detect some hazardous driving behaviors (e.g., sudden slow down, S-shape driving, etc.). Current additive sensor technologies, (e.g., GPS, accelerometer, angular sensors, etc.), as well as the onboard vehicular signals (e.g., airbag deploying signal, brake pedal signal, vehicle speed signal, etc.), make possible the implementation of this subsystem.

The other subsystem, intervehicle wireless communication subsystem (IVWCS), is in charge of the intervehicular information sharing. Recent advances in wireless technologies have made vehicle-to-vehicle (V2V) communications and vehicle-to-infrastructure (V2I) communication possible by means of mobile ad hoc networks (MANETs) for intelligent transportation system (ITS). Vehicle ad hoc networks

(VANETs), considering the special features of vehicular environment, have clear benefits; that is, VANETs not only improve the overall safety for vehicular system, but also smooth the traffic flow.

Furthermore, in order to disseminate the vehicle status information to the traffic center, communication channels should be established. The current approaches utilize mobile phone channels, such as GSM, GPRS, or 3G, and so forth. However, the numerous vehicles on road will lay a tremendous burden on the mobile phone network. Hence, there have been proposals to establish a series of infrastructures along the road as information sinking ports and finally form the V2I network [1]. Nevertheless, before this giant scope of constructions, the robotic concept of mobile nodes can serve as sinking ports for establishing the overall car safety network framework, as a transitional and testing step.

Governments and prominent industrial corporations are involved in this field over the past ten years, such as GM, BMW, and Toyota. Several important projects were held to promote development of such VANETs system. Advanced Driver Assistance Systems (ADASE2) [2] and Crash Avoidance Metrics Partnership (CAMP) [3] were launched in the US. The project "FleetNet—Internet on the road" was set up in German [4]. "FleetNet" uses FleetNet network layer (FNL) to realize a vehicular ad hoc network. It is an adaptive protocol, and position information are used for routing and forward strategy. Taleb et al. proposed a scheme called ROMSGP to enhance the stability of the IVC and RVC communications in VANETs; the key idea is to group vehicles according to their moving directions [5]. Moreover, the Federal Communications Commission has allocated spectrum and new standards for VANETs, more recently called IEEE 802.11p. IEEE 802.11p is an approved amendment to the IEEE 802.11 standard to add wireless access in vehicular environments (WAVE). It defines enhancements to 802.11 required to support intelligent ITS applications.

Although the need for V2V communication is evident and many studies for VANETs have been done, so far few intervehicle communication systems for information sharing between vehicles have been put into operation. OnStar system is designed for vehicle safety by General Motors [6]. It is based on wireless cellular communications, such as GSM, GPRS, or 3G. This system works well but it limits the simple service between the driver and the OnStar Center when the crash accident happens. In addition, the service is available only for all vehicles that have the factory-installed OnStar hardware, like GM vehicles.

This paper proposes a vehicle safety enhancement system based on wireless communication. It takes into consideration the vehicular information acquisition, communication issues for V2V and V2I, and finally the hardware implementation. This paper is organized as below. Section 2 introduces the vehicular information acquisition subsystem, which collects signals for vehicle accident detection and classification, so as to share with the whole vehicle networks. In Section 3, we selected the benchmark routing protocol for V2V network by comparison of three classical protocols, that is, DSDV, DSR, and AODV. In Section 4, we consider the unique features of vehicle networks, that is, with availability of position and velocity, and modify the adopted AODV into GPS based AODV (GBAODV), which has been verified for better performance through simulation. Section 5 addresses the problem of vehicle-to-infrastructure (V2I) information sinking, in which we consider the optimization of time-delay and network load. In Section 6, we describe the real-time experiment. Section 7 concludes the paper.

2. Vehicular Information Acquisition [7]

Traffic collisions are serious threats to human lives. It is estimated that 1.2 million people were killed in motor-vehicle accidents globally [8]. There are various factors, such as road and traffic environment, vehicle states, and drivers' behaviors. Vehicular information, if obtained and shared among surrounding vehicles, can reduce the risk of accidents.

2.1. Collision and Potentially Hazardous State Classification. We classify and define the accidents or potential hazardous actions into 4 severity levels, as listed below.

(1) Level 1 (potentially hazardous): sudden slow down [9].

(2) Level 2 (minor accident): slight bumping [10].

(3) Level 3 (major accident): airbag deployed [11].

(4) Level 4 (serious accident): rolling over [12].

Different severity levels should be processed differently. If sudden slow down occurs, the immediately following vehicles ought to be notified, so as to prevent collision. For a minor accident, a flexible traffic police, for example, motorcycle police, will be adequate, and the most urgent need is to recover the traffic. If the airbag is activated or there is rolling over, ambulance should be connected automatically and promptly to save the injured. Even more, for the rolling over case, a crane may also be needed to remove the vehicle in accident.

2.2. Sensors for Collision Detection. During the driving, some real-time status signals are available inside the vehicle, such as airbag deployment signal. Aside of those, additional sensors are required to classify the signals into more delicate levels. These signals and sensors are listed in Table 1.

2.3. Sensor Data Fusion and Collision Estimation. We adopt the Freescale9s12XEP100 as the core MCU controller for data gathering and analysis. It is configured with 16 bit HCS12X CPU, 512 Kbyte Flash EEPROM, and 32 Kbyte RAM for digital signal processing.

According to the sensor information obtained from vehicle, the real-time estimation of collision is conducted, as shown in Figure 1.

Figure 2 illustrates the overall processing action flowchart for collision detection and dissemination.

Table 1: Sensors for vehicular information acquistion.

Sensor	Function
Airbag deployment LED (on dashboard)	Airbag deployment detection
Vehicle wheel sensor	Detect vehicle speed
GPS/SiRF starIII	Vehicle localization
6 G one-axis accelerometer	Sudden slow down detection
500 G one-axis accelerometer	Slight bumping detection
1.5 G three-axis accelerometer	Rolling over
Steering wheel angular sensor	S-shape steering detection

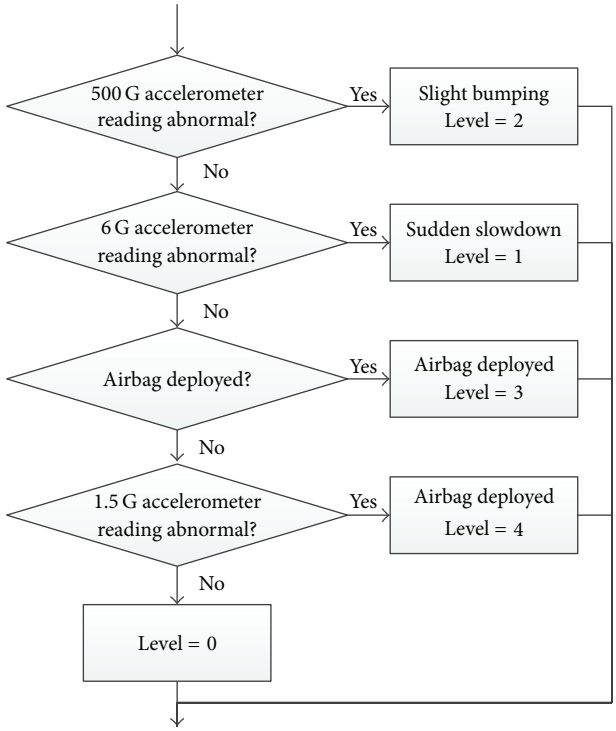


Figure 1: Flowchart for collision estimation.

3. Evaluation of Classical Routing Protocols in MANET [13]

The speed of vehicle moving on a freeway is fairly fast, at approximately 80 km/h in general. When the accident occurs on a freeway, the warning message must be instantly sent to other vehicles nearby via the VANET, so that the drivers nearby have enough time to avoid collision. In order to achieve reliable real-time communication, the performance of routing protocol used by the VANET is important [5, 14]. Different routing protocols have different network characteristics [15–17]. VANET on the freeway is a fast and highly dynamic mobile ad hoc wireless network without fixed router, hosts, or wireless based stations. A significant challenge in the freeway VANET is how to select an efficient routing protocol among numerous protocols. Thus, three classical routing

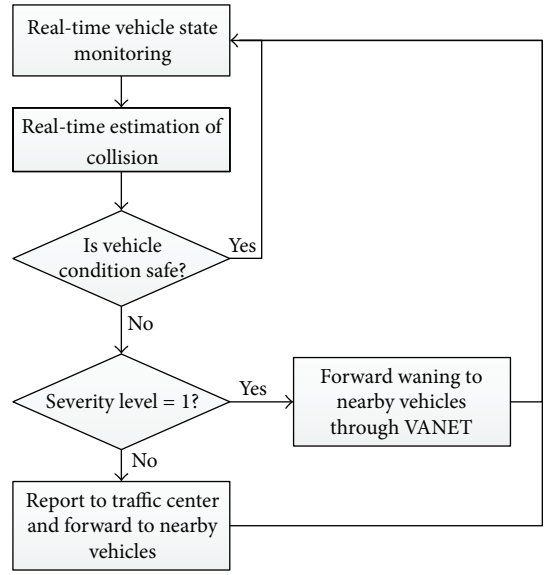


Figure 2: Algorithm flowchart of the collision evaluation.

protocols are evaluated and compared. A proper routing protocol will be selected, based on which modification can be made to bear the unique features for VANET.

3.1. Classical Routing Protocols for MANET. Numerous ad hoc routing protocols have been proposed by the Internet Engineering Task Force (IETF) Mobile Ad hoc Networks (MANET) Working Group [18]. These routing protocols are divided into two major classes based on the underlying routing information update mechanism employed, reactive (on-demand) or proactive (table-driven). For performance evaluation, we have compared three typical routing protocols in MANET for V2V application. Destination sequenced distance vector protocol (DSDV) is selected as an example for table-driven protocols, while both dynamic source routing (DSR) and ad hoc on-demand distance vector (AODV) protocols are selected as examples for on-demand protocols [19–21].

(1) *DSDV.* DSDV is based on the Bellman-Ford algorithm which can effectively solve routing loop problem [19]. Each node has a routing table, which contains the shortest path to every other node in the network. Each entry in the routing table contains a sequence number. The number is generated by the destination. If a node receives new information, it consults the routing table and uses the latest sequence number to forward . If the sequence number is the same as the one existing in the table, the route with the better metric is used. Stale entries are deleted by regular update of its routing tables. DSDV is suitable for creating a small-scale ad hoc network.

(2) *DSR.* DSR uses source routing instead of hop-by-hop packet routing in comparison with DSDV and has two major phases, which are route discovery and route maintenance [20]. Route discovery is used to set up a route from source node to destination by sending RouteRequest packet in

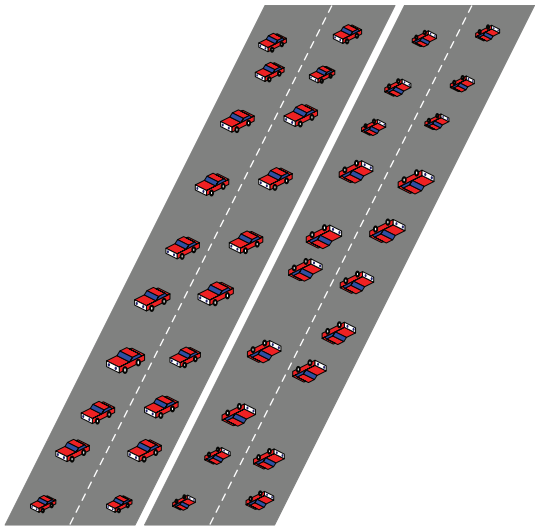


Figure 3: Simulation scenario of vehicles moving on a freeway.

the source node. If a node in the path moves away and breaks wireless communication, route maintenance will rebuild a route from source node to destination one by sending RouteError packet to the node adjacent to broken link. Each data packet carries corresponding routing information. Thus, it eliminates the need to periodically flood the network with table update messages which are required in a table-driven approach. However, DSR does not locally repair a broken link. The connection setup delay is higher than that of table-driven protocols.

(3) *AODV.* AODV is very similar to DSR [21]. It sets up a route to the destination by sending a RouteRequest message. The source node and the intermediate nodes store the next hop information corresponding to each flow for data packet transmission. The major difference between AODV and other reactive routing protocols is that it uses a destination sequence number (DesSeqNum) to find the latest route to the destination. A node updates its path destination only if the DesSeqNum of the current packet received is greater than the last DesSeqNum stored at the node. However, AODV requires more time to set up a connection than some other approaches [15, 17, 21].

3.2. Simulation Environment and Performance Evaluation. The simulator for evaluating three routing protocols is the Network Simulator (NS2, version 2.33). NS2 provides substantial support for simulation of wireless networks using discrete-event mode.

(1) *Basic Scenario.* The simulation scenario is designed according to the normal state of car running on a freeway shown in Figure 3. Assume that the freeway is 30 meters wide and 500 meters long. 40 vehicles are randomly distributed to the four bidirectional lanes of the freeway. Each vehicle is regarded as a mobile node moving forward in a random fashion. The maximum velocity of nodes is 35 m/s with simulation period of 200 seconds. The channel capacity is 2 Mb/s. The MAC type is IEEE 802.11. The CBR traffic model is used with data packet size 512 bytes and sending rate 160 Kbps.

Table 2: Packet loss rate of three routing protocols.

Time (second)	DSDV (%)	DSR (%)	AODV (%)
100	12.72	0.68	1.07
200	7.62	0.48	0.48

(2) *Performance Evaluation.* The performance evaluation of routing protocols is based on the measurement of the following parameters [16].

Packet Loss Rate (%). Packet loss occurs when one or more packets of data traveling across a VANET fail to reach their destinations. The packet loss rate is calculated as

$$p = \left(1 - \frac{N_r}{N_s}\right) \times 100\%, \quad (1)$$

where N_r and N_s represent the number of data packet received and sent, respectively.

End-to-End Delay (ms). End-to-end delay is defined as the time taken for a data packet to be transmitted across the network from the source to the destination.

Packet Jitter (ms). Packet jitter is defined as the delay variation between two consecutively received packets belonging to the same stream. In general, it is expressed as an absolute value of delay variation.

Throughput (Kilobits per Second). System throughput is the sum of the data rates that are delivered to all nodes in the network.

Protocol Overhead. Protocol overhead refers to the number of routing messages requested when a data packet is successfully delivered to the destination.

3.3. Simulation Results and Discussion. Throughout the simulation, we discuss the results as below.

(1) *Packet Loss Rate.* Table 2 shows the packet loss rate incurred by DSDV, AODV, and DSR. Both DSR and AODV on-demand routing schemes have considerably less packet loss rate than DSDV. Because each node is fast mobile in a random fashion, the network topology often changes. These packets sent may be lost once the routing table is not timely updated in DSDV. This results in a higher packet loss rate of DSDV.

(2) *End-to-End Delay.* Figure 4 shows the end-to-end delay of data packets. The statistical values of them are (7.440 ± 4.157) ms (DSDV, confidence level $\alpha = 0.95$), (8.167 ± 9.210) ms (DSR, $\alpha = 0.95$), and (8.107 ± 5.026) ms (AODV, $\alpha = 0.95$), respectively. They have no significant difference in the mean values. However, as a whole, the margin of delay fluctuation in DSR is the highest among the three protocols. In DSR, a neighbor displacement is noticed only after a packet is sent explicitly to that node. The network reacts

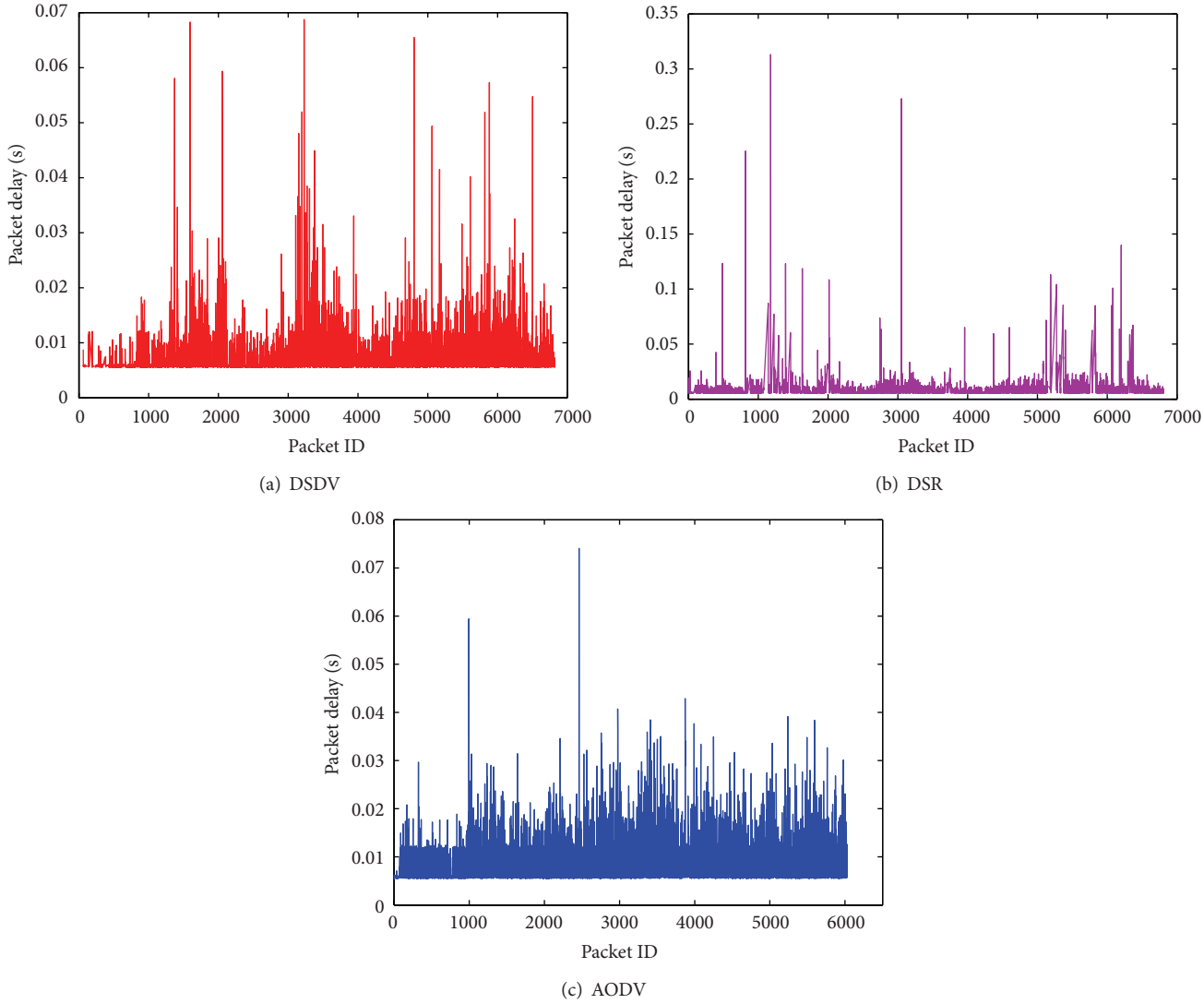


Figure 4: Packet delay of three routing protocols.

if an acknowledgement is not received. Consequently, this increases packet delay since the packet must wait until a new route is established.

(3) *Packet Jitter.* Figure 5 shows the jitter of data packets using three different routing protocols. The statistical values of them are (2.356 ± 4.199) ms (DSDV, $\alpha = 0.95$), (3.254 ± 10.630) ms (DSR, $\alpha = 0.95$), and (4.498 ± 4.498) ms (AODV, $\alpha = 0.95$), respectively. DSDV shows the most superiority than others. The average jitter of AODV is the biggest among the three protocols. Moreover, the standard deviation of jitter in AODV is larger than that in DSDV. Although the average jitter of DSR is not the largest among the three protocols, DSR has the largest jitter fluctuation among them. This means violent variation exists in the delay of a few data packets sent in DSR. The rapid change of jitter is attributed to the frequent change of network topology and the mechanism of inherent routing update.

(4) *Throughput.* Figure 6 shows the throughput comparison of DSDV, DSR, and AODV. All throughputs are ever-increasing with the time in general. This can be attributed to more active nodes to join network communication with time extension. The graph also reveals that AODV has higher throughput than DSR. In DSR, a route is chosen based on the short delay at the instance of route establishment. Although this path may be the best route at that instant, it may be also a route that lacks routing stability or has unacceptably high load. In contrast, AODV has a more robust update mechanism to avoid bottleneck and congestion and eventually improve throughput. In DSDV, high packet loss rate causes throughput to drop.

(5) *Protocol Overhead.* Table 3 shows the overhead comparison of DSDV, AODV, and DSR. AODV has the highest overhead among three routing protocols due to three main reasons. Firstly, AODV allows broadcast. Although the discovery packets are broadcasted only when necessary, such as establishing a new route, link breakage, or route error, the broadcast instances will often appear for a fast mobile VANET. Secondly, AODV allows mobile nodes to respond to link breakages and changes in network topology in a

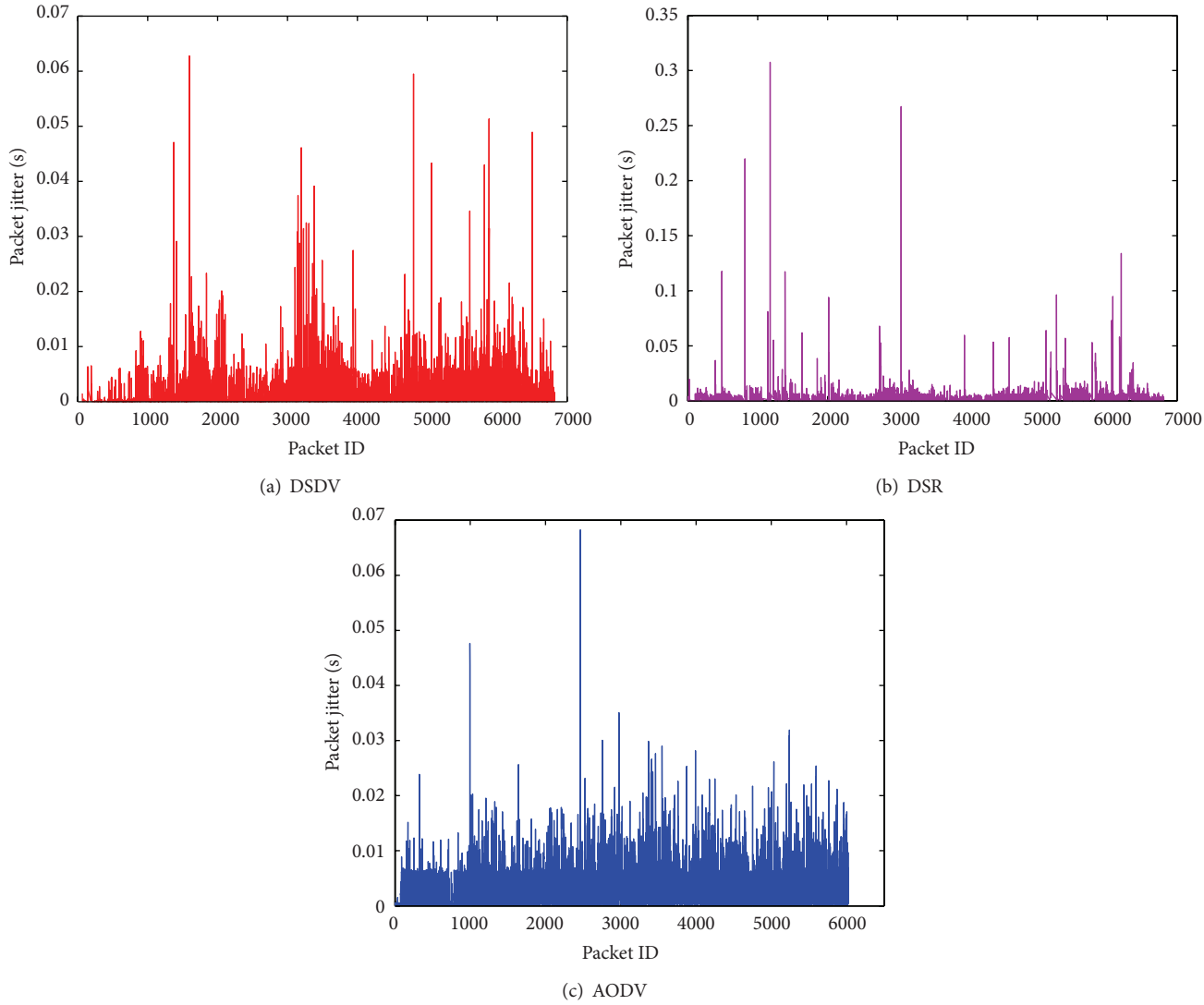


Figure 5: Packet jitter of three routing protocols.

timely manner. Thus, numerous routing messages are used to maintain an active route in AODV. Thirdly, AODV is derived from DSDV. It still has similar features of proactive routing protocols. When the network topology is often changed because of the fast mobility of nodes, proactive protocols must send more messages to maintain a valid routing table. The experimental results are shown in Table 3. DSR has the best protocol overhead performance among the three protocols. The DSR protocol is composed of the two main mechanisms of "route discovery" and "route maintenance," which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network. Some measures reducing overhead are adopted in the process of "Route Discovery" and "Route Maintenance" of DSR [21].

3.4. Conclusion. Based on the simulation results, we discovered that DSDV achieves marginal better packet delay and packet jitter than AODV and DSR. However, it has significantly higher packet loss rate and the smallest throughout among them. Although DSR has the best protocol overhead

Table 3: Overhead of three routing protocols.

Type	DSDV	AODV	DSR
Number of received data packets	5579	5999	5993
Number of sent message packets	25607	39488	1615
Protocol overhead	4.59	6.58	0.27

performance among three routing protocols, it has poorer jitter and throughput than AODV. As a whole, AODV is more appropriate for the freeway VANET according to the quality of service and the real time of packet delivery. The inherent reason producing this result is the effect of node mobility on the performance of the routing protocol.

4. GPS Based AODV Protocol for V2V Communication [22]

As we can find through the previous protocol evaluation, AODV is appropriate for the dynamic structure with mobile vehicles. The source node will find a route to destination

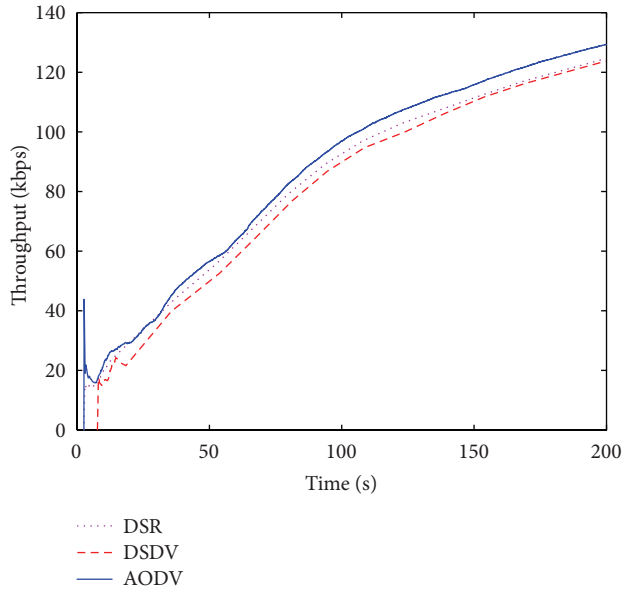


Figure 6: Throughput comparison of three routing protocols.

for data transmission. To find a route to the destination, the source broadcasts a route request packet (RREQ). The node receiving RREQ will reply a route reply packet (RREP) to the reverse path that RREQ went through if it is the destination of RREQ or if it has a recent route to the destination. Otherwise, the node will broadcast RREQ until either of the two situations above occurs. As RREP traverses back to the source, the nodes along the path enter the forward route into their routing tables. If a node leaves the network, the node that discovers this broken link will send a link failure notification (RERR) to the precursors. The RERR goes upstream until it reaches the source. The source will thereafter restart route discovery process if needed [23].

However, AODV is dedicated for MANET, and modification is necessary for VANET applications [24]. Since nodes in VANET are fast moving vehicles, the topology of the network changes all the time, making the position and velocity of the node critical factors while finding the routes. Therefore, besides conventional topology-based routing protocol (such as AODV), position-based routing protocol, which primarily uses the position information obtained by GPS to find a route, is applied in VANET [25].

In recent years, many researchers have tried to combine two types of routing together. In [26], Kim et al. proposed AODV-RRS which restricts the number of forwarding RREQs according to the concepts of stable zone and caution zone. PAODV [27] restricts the number of flooding RREQs based on the distance between current node and its neighbors. Both of them have similar mechanism and reduce the number of broken links. DAODV [28] establishes a route depending on the direction and position of source, intermediate, and destination node. Although it also reduces the number of broken links, DAODV assumes that source node knows the direction and position of all the nodes in the network. Actually this is impossible with the current GPS devices. We should find some mechanisms to get the geographic information of all the nodes. Thereby, in [29], Asenov and Hnatyshin proposed GeoAODV routing protocol. Each node will maintain an additional table, geotable, to keep track of the geographic information of all the nodes. RREQs are restricted flooding in the region determined by the geotable. However, it costs more resources to maintain two tables.

We go a step further in this section by proposing a GPS based AODV (GBAODV), which enhances the overall performance of AODV in VANET. In order to be attainable in physical implementation, GBAODV assumes that each node only knows its own position and velocity. Without maintaining a geotable [29], GBAODV is much more concise than GeoAODV.

4.1. Overview of GBAODV. With current GPS device, we can obtain the longitude (x coordinate) and latitude (y coordinate) of current node, and calculate the speed in each direction with two successive sets of coordinates. Without maintaining a geotable, we add geographic information into routing table to make the algorithm concise.

There are two main features in GBAODV. First is to reduce the number of RREQs. The node receiving an RREQ packet will check the distance and motion trend between the precursor and itself, so as to decide if this RREQ should be broadcasted. By restricting these flooding RREQs, it will avoid lots of packet collisions in the network. As a result, the packet delivery ratio and throughput of the network can be raised. Second is to mark the route according to the positions and velocities of source, intermediate, and destination. Higher mark means higher stability. Consequently, every node will choose a route with higher mark.

These two features require specifying flooding rules and marking standards, as well as some modifications in the routing table and routing packets.

4.2. Modified Structure of Routing Table, RREQ, and RREP

(1) *Modified Routing Table.* Original routing table contains the IP addresses of next hop and destination, sequence number of destination, and total hops. The routing table will update if the sequence number of destination is larger or total hops is less. We added the position and velocity of the destination node and the mark of this route into the routing table. Besides the two conditions above, the routing table will update when the mark is larger, which means that the route path is more stable.

(2) *Modified Frame Structure of RREQ.* We inserted position (x, y coordinates) and velocity (x, y direction) of the source and current node into RREQ packet. We also applied a reserved segment to record the mark of the route link from source to precursor.

(3) *Modified Frame Structure of RREP.* RREP is modified similar to RREQ. We inserted position and velocity of the destination and current node into RREP packet. We also

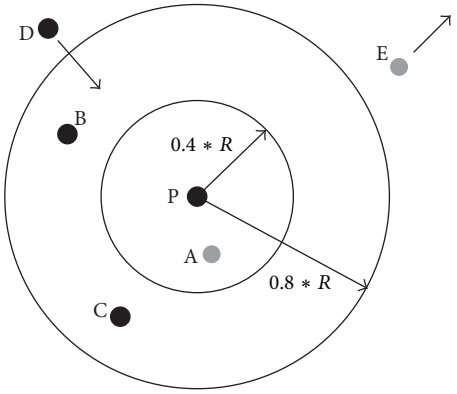


Figure 7: B, C, and D will broadcast RREQ received from P.

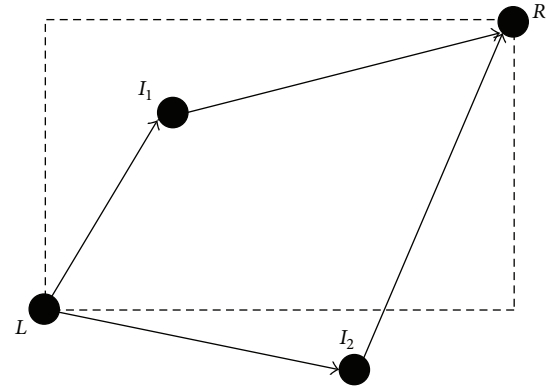


Figure 8: Different mark for different regions.

applied a reserved segment to record the mark of the route from destination to current node.

4.3. Flooding Rules and Marking Standards

(1) *Flooding Rules.* Let d stand for the distance between the precursor and current node and R stand for the maximum transmission distance of the wireless card. The flooding rules are as follows.

If ($d < 0.4\,R \parallel (d > 0.8R \&\& d$ is increasing))

discard RREQ;

Else,

broadcast RREQ.

The coefficients 0.4 and 0.8 are chosen empirically. We conducted simulations with the combinations of these coefficients to study numbers of RREQs and RERRs, packet loss ratio, and average end-to-end delay. Results show that the combination of 0.4 and 0.8 is the best among all.

In Figure 7, B, C, and D will broadcast the RREQ received from P, while A and E will discard it.

(2) *Marking Standards.* As illustrated in Figure 8, let LD_c stand for the current distance between node L and node I, LD_l stand for this distance a moment later, RD_c stand for the current distance between node I and node R, and RD_l stand for this distance a moment later. We specify the marking standards as follows:

$$\text{mark} = 2\,\text{sgn}\left(LD_c - LD_l\right) + 2\,\text{sgn}\left(RD_c - RD_l\right) + C, \quad (2)$$

where sgn() is a signum function.

C is a constant:

$$C = \begin{cases} 0 & \text{if } I \text{ is in the dashed rectangle} \\ -3 & \text{if } I \text{ is out of this rectangle.} \end{cases} \quad (3)$$

−3 is chosen experimentally according to simulations.

Since the transmission distance of wireless LAN card is limited, geographic distance of each hop is the key factor that affects the quality of communication. If the distance stays unchanged, then the route is really stable so that the source and destination can communicate steadily. If the distance is increasing, it is possible that one node in this route will exceed the transmission distance soon. If the distance is decreasing, then after some time, the two nodes may cross over and start to depart. It is better than increasing distance, but not as good as unchanged distance. So we set two values for each changed distance: 0 for each decreasing distance and −2 for each increasing distance, as shown in (2).

To find a path to the destination, the source broadcasts an RREQ containing the position and velocity of source and preset a standard mark value.

As illustrated in Figure 9, when a node receives an RREQ the following will occur.

(i) If it does not have a route to the source node, it will insert the route RREQ into its routing table.

(ii) If it has a route in routing table but the route needs to be updated, it will update routing table.

(iii) If it is the destination or has a route to destination, it will create an RREP in which the mark is a standard value (if it is the destination) or is obtained from routing table (if it has a route to destination).

(iv) If it is a node besides (3) and satisfies the broadcasting conditions (refer to flooding rules), it will add the mark of source → precursor → current to the present mark in RREQ. It will also update the position and velocity of current node in RREQ.

As illustrated in Figure 10, when a node receives an RREP the following will occur.

(i) If it does not have a route to the destination, it will insert the route, which RREP goes through, into its routing table.

(ii) If it has a route in routing table but the route needs to be updated, it will update routing table.

(iii) If it is the destination of RREP (i.e., the source of RREQ), it will insert the route into routing table.

(iv) If it is a forwarding node, before unicasting RREQ, it will add the mark of source → precursor → current

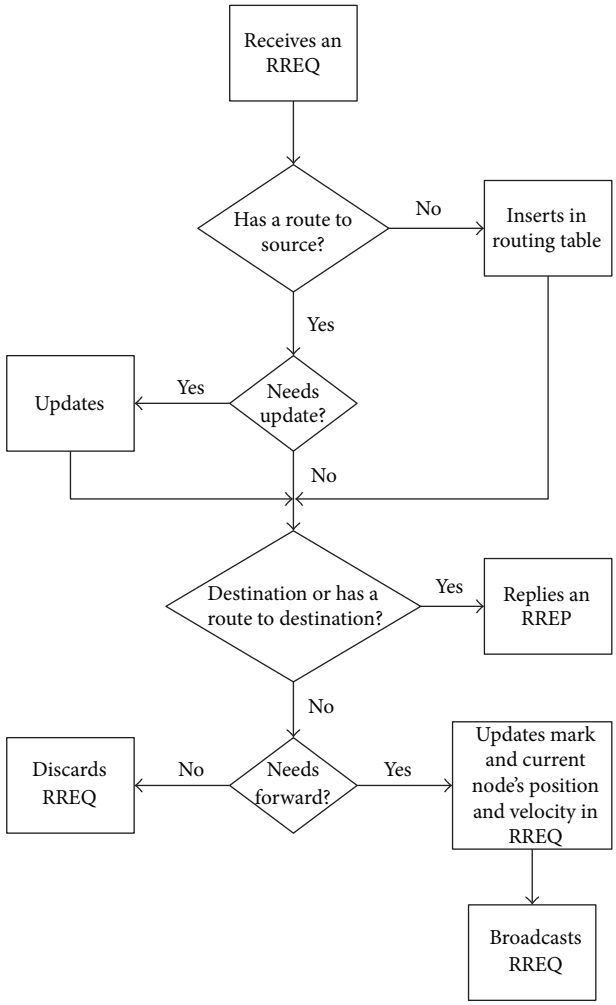


Figure 9: Flowchart of processing RREQ.

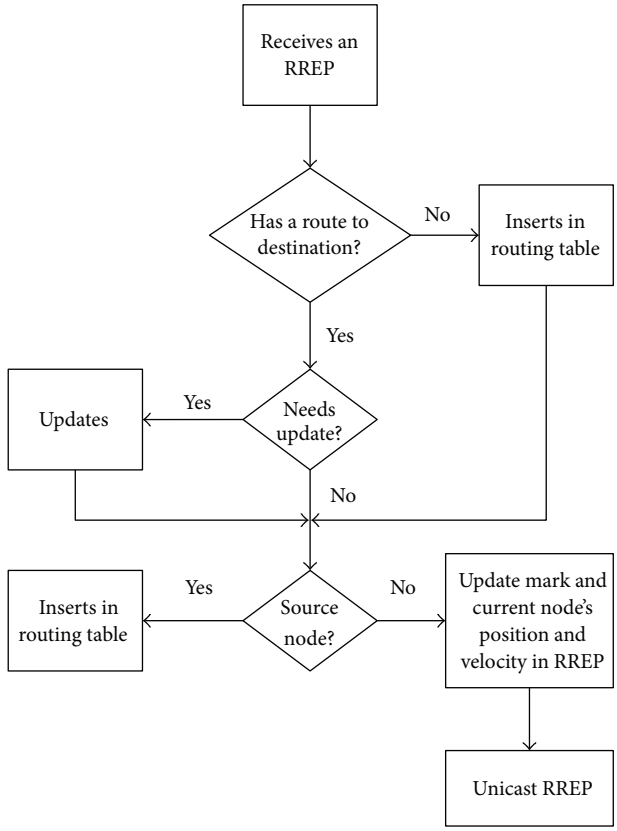


Figure 10: Flowchart of processing RREP.

to the present mark in RREP. It will also update the position and velocity of current node in RREQ.

4.4. Simulation Setup

(1) *Simulation Tools.* We chose VanetMobiSim 1.1 [30] for traffic simulation. This software can generate a traffic flow in the format suitable for NS2 [31], which can load GBAODV for network simulation.

With VanetMobiSim, we import maps from the US Census Bureau TIGER/Line database [32], which includes complete coverage of the United States, Puerto Rico, and so forth. Moreover, VanetMobiSim supports for multilane roads, differentiated speed constraints, and traffic light signals at intersections. All the vehicles can be set to Intelligent Driver Model with Lane Changing (IDM_LC) [33, 34]. For these reasons, the scenario in traffic layer is quite authentic, which makes the simulation in network layer reliable.

(2) *Parameter Settings.* In our simulation, we observed two types of traffic models: downtown and highway. TGR11001 [32] (district of Columbia, WA) is chosen as downtown map and TGR36001 [32] (Albany county, NY) is chosen as highway map. Multilanes and traffic lights are involved. All the vehicles follow the IDM_LC driving model. Tables 4 and 5 are the parameter settings of traffic and network simulation. Traffic flow and CBR (constant bitrate) data flow are both generated randomly.

Table 4: Parameter settings of traffic.

Traffic layer	Downtown	Highway
Area (m^2)	1000×1000	1000×1000
Number of lanes	3	3
Maximum number of traffic lights	10	None
Speed (km/h)	20~80	60~120
Simulation time (s)	250	1000

Table 5: Parameter settings of network.

Network layer	Downtown	Highway
Maximum transmission distance (m)	250	250
Number of sources	35	17
Number of connections	56	26
CBR packet size (bytes)	256	512
Transmission rate (pkt/s)	1	2
Simulation time (s)	250	1000

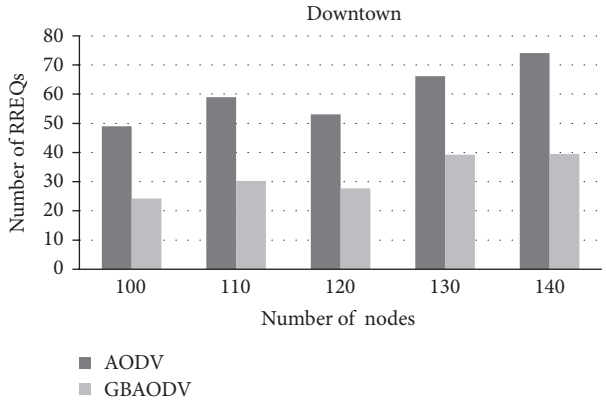


Figure 11: Number of RREQs received downtown per node per second.

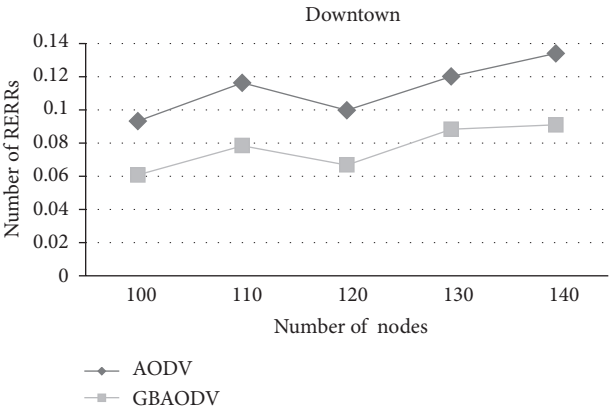


Figure 12: Number of RERRs sent in downtown scenario per connection per second.

4.5. Simulation Results

(1) *Downtown Model.* Figure 11 illustrates that the number of RREQs received per node per second is reduced by about 50%. This is caused by the application of flooding rules. In addition, we can notice that although it is normalized by the number of nodes, the number of RREQs still increases with the number of nodes. This means larger number of nodes induces larger amount of RREQs broadcasted in the whole network. Therefore, it is significant to reduce the broadcasted RREQs especially in high density traffic.

Figure 12 illustrates the number of RERRs sent per connection. The number of RERRs is also reduced a lot which means broken links have decreased a lot. This is an attribute to the application of marking standards since we choose every connection with high stability.

Figures 13 and 14 illustrate the packet loss ratio and average end-to-end delay. Compared with Figures 11 and 12, they show that packet loss ratio and average end-to-end delay are positive correlated to the numbers of RREQs and RERRs, because reducing the number of RREQs contributes to avoiding large amount of packet collisions in the network.

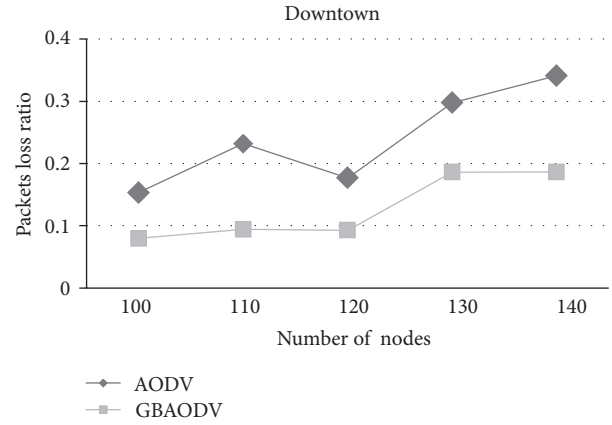


Figure 13: Packet loss ratio in downtown scenario.

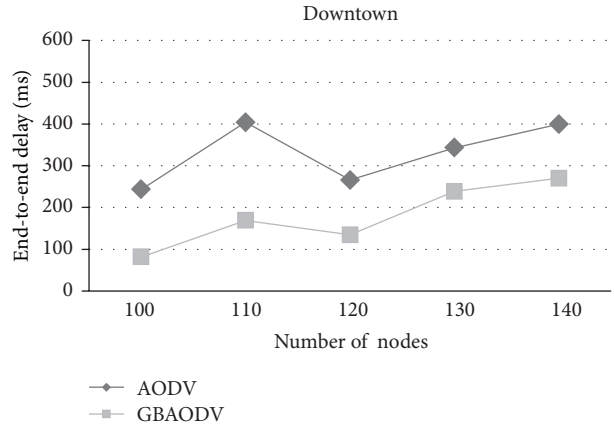


Figure 14: Average end-to-end delay in downtown scenario.

Meanwhile, reducing the number of RERRs (i.e., broken links) could smooth communication.

(2) *Highway Model.* The number of RREQs received per node per second is reduced by more than 50% (illustrated in Figure 15). Figure 16 shows that the number of RERRs sent per connection is also reduced. We also note that with the increase of number of nodes, the reduction of RERRs (i.e., broken links) increases. This means GBAODV is more efficient in high density traffic scenario. The conclusion is verified by Figure 17 (packet loss ratio) and Figure 18 (average end-to-end delay). Compared with Figures 13 and 14, the improvement of network performance is not as sharp as that which we obtained in downtown model.

The main reason is that the node density in highway model is relatively low. Firstly, lower node density leads to less number of RREQs flooding in the network (referring to Figures 11 and 15). The number of RREQs received per node per second in highway model is about 80% of that in downtown model. Therefore, packet collision in highway is slighter than in downtown. Although GBAODV weakens packet collision, it achieves no big improvement. Secondly, lower node density provides fewer choices of stable routes. If we restrict the number of RREQs, the effect caused by skipping some stable routes is larger than that in downtown

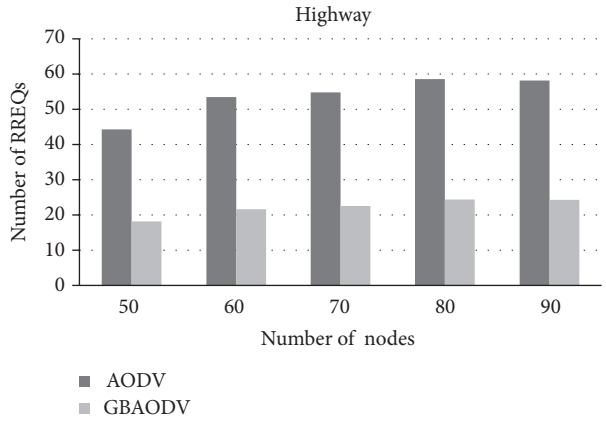


Figure 15: Number of RREQs sent in highway scenario per node per second.

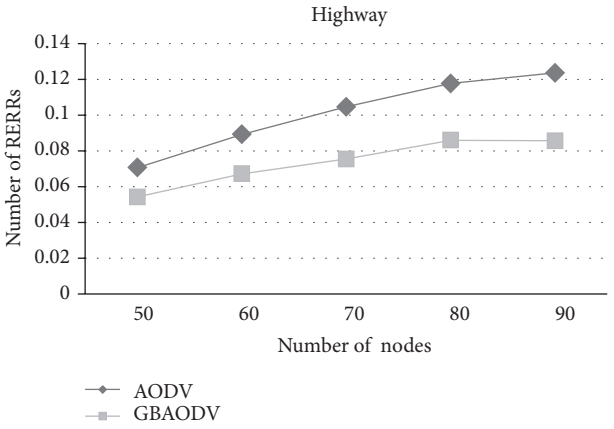


Figure 16: Number of RERRs sent in highway scenario per connection per second.

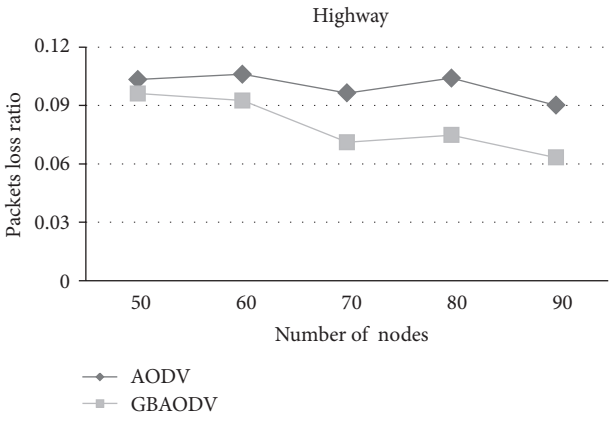


Figure 17: Packet loss ratio in highway scenario.

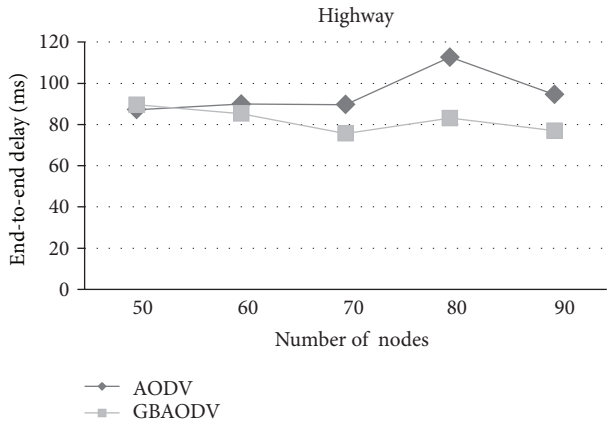


Figure 18: Average end-to-end delay in highway scenario.

model. That is the reason why the reduction of the number of RERRs in highway model is less than that in downtown model (referring to Figures 12 and 16).

To conclude, GBAODV is much better than AODV in both models. It releases the load of the network (less number of RREQs), reduces broken links and packet loss ratio, and shortens average end-to-end delay.

5. Vehicle Information Sinking Network Based on Mobile Nodes [35]

Aside of the mobile V2V network, the information from the vehicles should also be sent to the sink node, which will be normally performed by the roadside infrastructure. However, the construction of these infrastructure networks is expensive in both funding and time. Hence, mobile node acted by vehicles can firstly serve as the sinking port. This section elaborates a data gathering algorithm based on swarm intelligence. Although the computational resource and energy source of the on-board computer in vehicles, compared to field wireless sensor nodes, is abundant, applications may need to be extended to bicycle riders, with limited energy source. The transmitted information in the future will be extended as there will be applications aside of accident reporting, such as cloud computation, media access, and entertainment through the V2V and V2I network. Hence, in order to maximize the overall network efficiency, communication load of each vehicle node ought to be balanced.

Much reference can be made from the current research on hand-held devices such as 3G mobile phone and PDA, which play role as mobile sink of wireless sensor network (WSN) node in applications [36, 37]. Thus the algorithm for the data gathering application should support the sink node mobility. It is a challenge in WSN algorithm design.

Based on the application of the sensor network, the data delivery model to the sink node can be categorized into three types: query-driven, event-driven, and continuous. In query-driven model, the sink node generates a query, and then a temporary route is built. The node which is checked receives query and returns result, for instance, DD [38] and ACQUIRE [39]. In event-driven model, because the event rate is much lower without temporal and spacial information, the event node triggers the data transmission and temporary route building, such as Rumor routing [40] and TTDD [41]. Focusing on these two types of data transmission model, the routes are temporary, so the sink node mobility has little influence on data transmission. In the continuous delivery

model, each sensor collects data periodically and sends data to the sink node for gathering. In data gathering application, the sink node builds the route usually; for instance, it has been concluded in TEEN [42], APTEEN [43], and MINA [44]. However, movement of the sink node often results in broken links. If the route is rebuilt frequently, not only the network energy consumption will be large, but also the regular data transmission will be blocked by the network storm, which will result in massive broadcasting messages.

Sink mobility brings new challenges in data gathering application, although some protocols and mechanisms have been proposed in recent years, such as TDD, SEAD [45], CODE [46], and others in [47, 48]. TTDD uses a grid structure so that only sensor located at the grid points needs to acquire the forwarding information. The route path for the moving sink node is maintained and refreshed by agent nodes. When there are several data sources in the network, the overhead is large. Meanwhile, the route needs to be rebuilt when the sink node moves out of the grid. SEAD protocol designs a dormancy mechanism for the nodes in grid to reduce energy consumption. The current route extends and recovers by itself while the sink node moves, but time delay remains a problem. CODE does not need to rebuild global path, but it needs other routing protocols to support, so the protocol is more complex. A local routing restoring mechanism is proposed in [47] that the sink node sends Sink_Claim message periodically. This message is used for the sink node detection. The sensor node would change its status according to this message. The main problem of this method is the large consumption caused in sending the Sink_Claim message in high frequency. Meanwhile, the throughput becomes smaller. As described in above, TTDD, SEAD, CODE, and others in [47, 48], they are all designed for query-driven or event-driven transmission model, so these methods are not much suitable for data gathering application.

For data gathering application in V2I, this section studies the equilibrium mechanism and proposes a swam intelligence data gathering algorithm for mobile sink (SIDGMS). The idea of SIDGMS algorithm is derived from swarm intelligence such as ants. In this algorithm, each vehicle node is a smart individual but with limited knowledge. SIDGMS defines two simple rules to describe the data forwarding. The problem how to choose next hop becomes multiobjective programming, which considers both the delay and load of the network. To solve link-break problem, a method of the power control for the Sink beacon message is proposed.

5.1. SIDGMS Algorithm. The idea of SIDGMS algorithm is derived from swarm intelligence. The preying behavior, as a typical behavior of swarm intelligence, has simple rules. If an individual discovers food, others will observe and study local behavior from the individuals in the region. As a result, everyone in group can find food.

Each node in a wireless sensor network (WSN) system has limited computational ability, memory space, energy, and wireless transmission range, so the nodes can only exchange information with neighbor nodes within the wireless communication range.

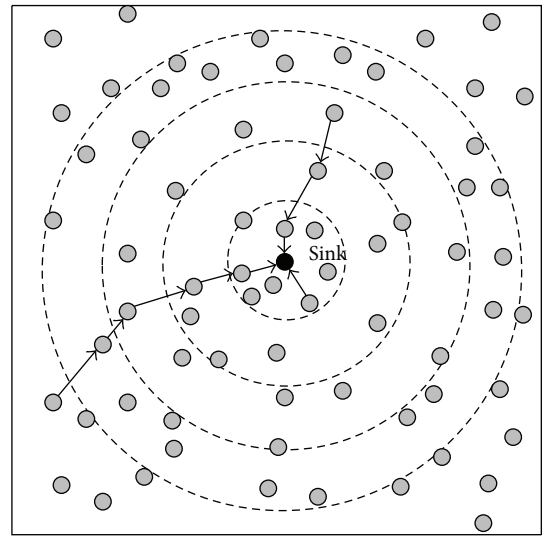


Figure 19: The structural relationship between the sink and vehicles.

Sink node can be regarded as food source, and the process of data gathering can be regarded as swarm foraging action. The sink node and other nodes are mapped on Figure 19.

The principle of data gathering works as below.

(i) The sink node broadcasts beacon periodically, which contains its current location information.

(ii) The internal nodes discover the sink node directly and start the data transmission with the sink node.

(iii) Meanwhile, the external nodes detect the data transmission between the internal nodes and the sink node, which helps the external nodes discover the sink indirectly and triggers the data transmission between them if needed.

(1) *SIDGMS Algorithm Mechanism.* In this algorithm, the nodes in WSN system can be separated into two types, the sink node with mobility and the sensor nodes. Two messages are defined as below.

Message 1. SINK_BEACON (sinkInfo), which is sent by the sink node to inform sensor nodes. sinkInfo includes the location component (x, y) and sequence number seq, which is incremental.

Message 2. SENSOR_DATA (nextAddr, data, sinkInfo, loadInfo), which is sent by sensor node. The sensor node collects its vehicular information (data) and then forwards it to next-hop node (nextAddr). The latest sink location component (sinkInfo) and load information component (loadInfo) are included in this message.

During the data transmission period, the sensor node saves location component of the sink node and refreshes this component once it receives a new one, which could be identified by the sequence number component (seq). At the same time, the sensor node changes its status according to the SINK_BEACON message. The status of sensor node is defined as follows

Definition 1. If sensor node receives the SINK_BEACON message at a interval time T (T is the periodic time of SINK_BEACON), the sensor node marks its status as Sink Adjacent (SA). Otherwise, it marks its status as Nonsink Adjacent (NSA).

According to different status of the sensor node, the algorithm has different data forwarding rules, which are listed as follows.

Rule 1. If the sensor node status is SA, the data is forwarded to the sink node directly.

Rule 2. For any sensor node in NSA status, it has two criteria to choose next hop. The first criterion is for less delay, and the other is for load balance of the network.

Generally, the sensor node which is closer to the sink node has less jumping hops, so its delay is smaller.

For any sensor node i, the distance from the sink node is calculated according to (4) as below:

$$d(i) = \sqrt{(x_i - x_{\text{sink}})^2 + (y_i - y_{\text{sink}})^2}. \tag{4}$$

For any sensor node i which is in NSA status, the best sensor node for next hop considering the fast transmission is solved according to (5):

$$J = \arg \min_{j \in N(i)} d(j), \tag{5}$$

where $N(i)$ denotes the neighbor nodes of the node i.

It is a complicated problem to calculate the loading of each sensor node. However, it can be estimated in two ways. In one hand, the key to maximize the WSN lifetime is to reduce energy consumption in each sensor node. We assume that each sensor node has the same hardware equipment. Thus the remaining battery energy in each node should be considered.

On the other hand, the time to forward messages in a WSN system is closely related to the network performance, such as the packet loss rate, time delay, and network congestion. Therefore, the total time of forwarding action could be used as indicator of the network loading. It could be denoted by the number of package buffer queue.

This mathematical model is elaborated as below.

Definition 2. The loading of sensor node in WSN system is

$$l(i) = k \frac{1 + q(i)}{e(i)}, \tag{6}$$

where $l(i)$ denotes the loading of the sensor node i, $e(i)$ is the battery dump energy, $q(i)$ is the mean number of the packages in the buffer queue, and k is scale factor.

For any sensor node i which is in NSA status, the best sensor node for next hop considering the load balance is calculated by

$$J = \arg \min_{j \in N(i)} l(j). \tag{7}$$

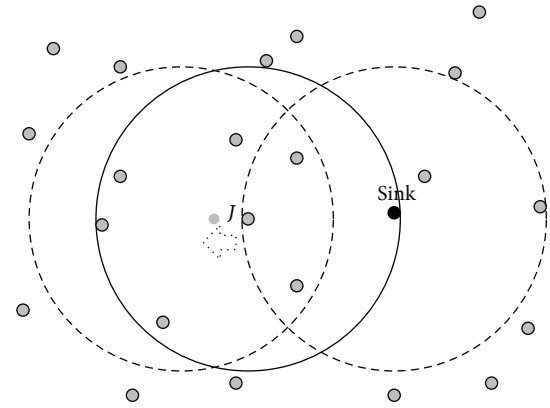


Figure 20: Same covering radius.

Definition 3. For the criterions of Rule 2, λ_d is defined as the distance weight coefficient with the sink node, and λ_l is defined as the loading weight coefficient for the sensor node. $\lambda_d \geq 0$, $\lambda_l \geq 0$, and $\lambda_d + \lambda_l = 1$.

The final optimization considers both the aspects of faster transmission and power balance, as below:

$$\begin{aligned} \min_{j \in N(i)} \quad & \left(\lambda_d \left| d(j) - d^0 \right| + \lambda_l \left| l(j) - l^0 \right|\right) \\ \text{s.t.} \quad & d(j) < d(i), \quad \lambda_d \geq 0, \\ & \lambda_l \geq 0, \quad \lambda_d + \lambda_l = 1, \end{aligned} \tag{8}$$

where d^0 is the minimum distance and l^0 is minimum loading. The distance weight coefficient λ_d and the loading weight coefficient λ_l are interrelated with application. For some applications which require high real-time response, λ_d would be increased. For some applications which focus on the energy equilibrium, λ_l will be increased. $d(j) < d(i)$ to prevent looping back.

5.2. Power Control Strategy

(1) *Node Coverage Radius.* The sink node broadcasts SINK_BEACON periodically. However, no matter how frequently the sink node broadcasts the SINK_BEACON message, packet loss would happen. That is because the linkage between the sink node and a sensor node in boundary area is fragile, due to the movement of the sink node. This case is shown in Figure 20, in which all the sensor nodes and sink node have the same transmission radii.

In order to solve this problem, we propose a new strategy to avoid link breaking, as shown in Figure 21. The transmission radius of the sink node is smaller than that of the sensor nodes. At present, most of the microcontrollers for WSN can support this by power control, such as CC2430, CC1100, and MC132x.

How to determine the transmission radius of the SINK_BEACON? As proposed in [49], with assumptions that the density of nodes is uniform and all nodes in WSN domain

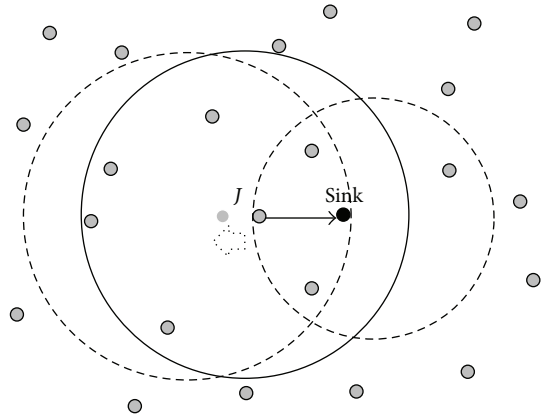


Figure 21: Different covering radius.

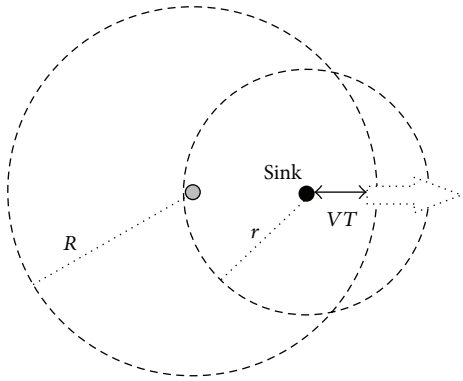


Figure 22: Partial address routing.

are subject to the Poisson distribution, the probability that m nodes exist in area S is

$$P(X = m) = \frac{(\rho S)^m e^{-\rho S}}{m!}. \quad (9)$$

Therefore, the problem of radius r could be translated into (10) as follows:

$$P(X > 0) = 1 - P(X = 0) \geq \alpha, \quad (10)$$

where α is the confidence, which denotes the probability that SA node appears.

Finally, the radius r can be determined as

$$r \geq \sqrt{\frac{\ln(1-\alpha)}{\pi\rho}}. \quad (11)$$

(2) *Cycle Time of SINK_BEACON.* It is shown in Figure 22. In this case, we assume the movement velocity of the sink node is V, the transmission radius of SENSOR_DATA message is R, and the transmission radius of SINK_BEACON message is r ($r < R$). Hence, cycle time of the SINK_BEACON message should satisfy this condition: $VT \leq R - r$.

Therefore, the cycle time of the SINK_BEACON is calculated as follows:

$$T \leq \frac{R-r}{V}. \quad (12)$$

```
timerStart(T, PERIOD_TYPE)
while (haveEnergy)
    if (timerFired)
        sendMsg(SINK_BEACON, sinkInfo)
    else if (receivedMsg)
        renderMsg()
    end
end
```

Pseudocode 1: The sink node pseudocode of SIDG-MS.

```
status:= NSA
while (haveEnergy)
    switch (receivedMsg)
        case: SINK_BEACON
            status:= SA
            recordSinkInfo()
            timerStart(T, SINGLE_TYPE)
            break
        case: SENSOR_DATA
            if (toSelf)
              computeNextHop()
              forward()
            else
              recordInfo()
            end
            break
    end
    if (timerFired)
      status:= NSA
    end
    if (sensorDataReady)
      computeNextHop()
      sendData()
    end
end
```

Pseudocode 2: The sensor node pseudocode of SIDGMS.

For example, if the transmission radius of SENSOR_DATA is 100 m, the transmission radius of SINK_BEACON is 50 m, and the moving velocity of the Sink node is 10 m/s, representing that the sinking vehicle moves slowly on the road; the max cycle time of SINK_BEACON is 5 s.

5.3. Experiment and Analysis. The simulation for evaluating SIDG-MS algorithm is implemented with NS2.

(1) *Implementation of SIDG-MS Algorithm.* The sink node takes charge of sending SINK_BEACON and data gathering. The pseudocode is listed in Pseudocode 1.

The sensor node collects vehicular data and forwards to the sink. It runs in distributed mode and the pseudocode in every node listed in Pseudocode 2.

(2) *Test Scenario.* The simulation scenario is designed according to a plane area, which is 800 meters wide and 800 meters long. There are totally 401 nodes in this WSN system,

Table 6: Simulation parameters.

Parameter	Value
Scene size	800 × 800 (m)
Node number	400 node + 1 sink
Mac	802.11
Application	CBR
Packet size	1024
Queue length	10
Channel model	Two-ray ground

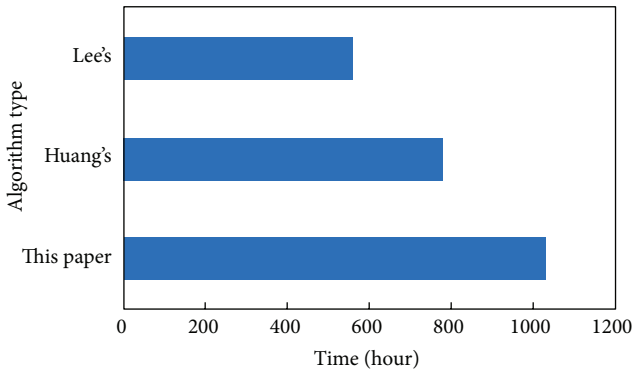


Figure 23: Network lifetime comparison.

including 1 sink node and 400 sensor nodes. The sink node moves randomly in the network with a constant speed 10 m/s. The sensor node collects the sensor data at a time interval every 10 s and its initialization energy is 50 J. Other simulation parameters are listed in Table 6.

We assume the energy consumption for collecting data is 1×10^{-5} J, the energy consumption for receiving data is 5×10^{-5} J, and the energy consumption for transmitting data is 1×10^{-4} J. The value of SINK_BEACON transmitting radius calculated according to (11) is larger than 50 meters ($r \geq 50$ m); in this simulation r it is initialized as 80 meter. The transmission radius of the sensor node for SENSOR_DATA message is initialized as 150 m. The periodic time of SINK_BEACON calculated according to (12) is smaller than 7 s ($T \leq 7$ s), so T is initialized as 5 seconds.

(3) *Simulation Result and Analysis.* The more incoming and outgoing message in MAC layer, the larger energy consumption will be. Therefore, we calculate the network energy consumption of every interval by counting the communication message in MAC layer is. The simulation result is shown in Figure 24, which illustrates the energy consumption character of SIDGMS, Huang et al. [47], and Lee et al. [48] algorithms. When the sink node is in motion, the energy consumption in literature [47] increases because the route path increases. In the algorithm of literature [48], the route path to the sink node is checked during each message packet transmission, so the energy consumption runs at a constantly high level. In SIDGMS algorithm, the location of the sink node could be refreshed during the motion. Thus this strategy has less energy consumption.

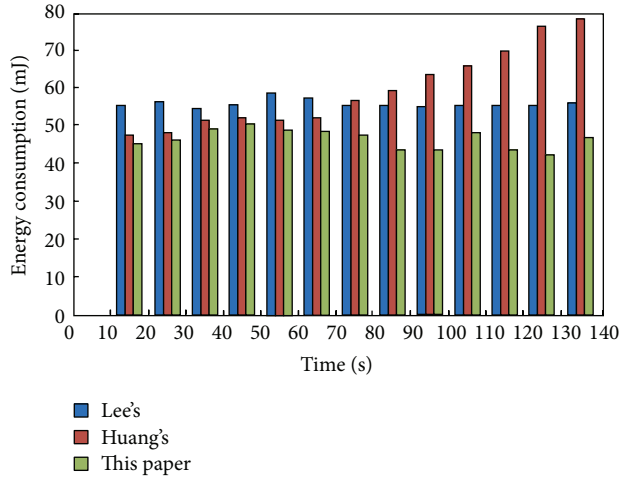


Figure 24: The energy consumption comparison between three methods.

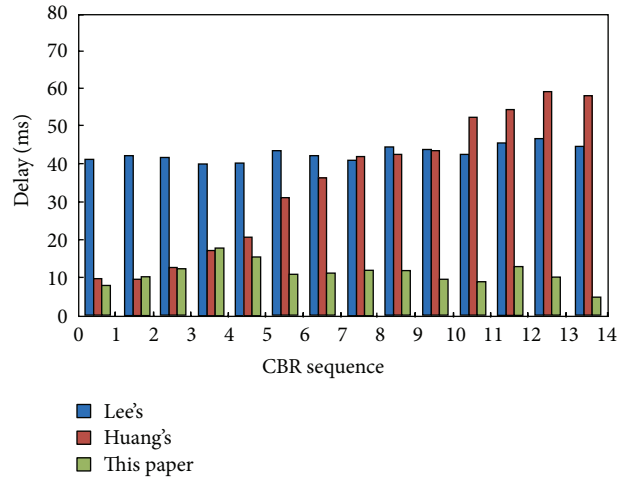


Figure 25: Time delay comparison.

The network lifetime is defined as the time period until one of the nodes dies. The simulation result with different methods is shown in Figure 23. The lifetime in literature [48] is the shortest due to the large energy consumption, such as many refreshing actions for route path. The lifetime in literature [47] is shorter than SIDGMS algorithm because there is no optimization for load balance. Some node's loadings are too heavy to support long lifetime.

Time delay is an important factor of WSN system, we analyze it by monitoring the CBR stream. The simulation result is shown in Figure 25. Time delay with the SIDGMS algorithm is significantly lower than the other two algorithms.

6. System Integration and Experiments [7]

To test the communication system, we developed a series of hardware as experimental platforms.

6.1. Platform Integration Architecture. Figure 26 shows the system architecture including two major components: onboard integration subsystem and V2V portable subsystem.

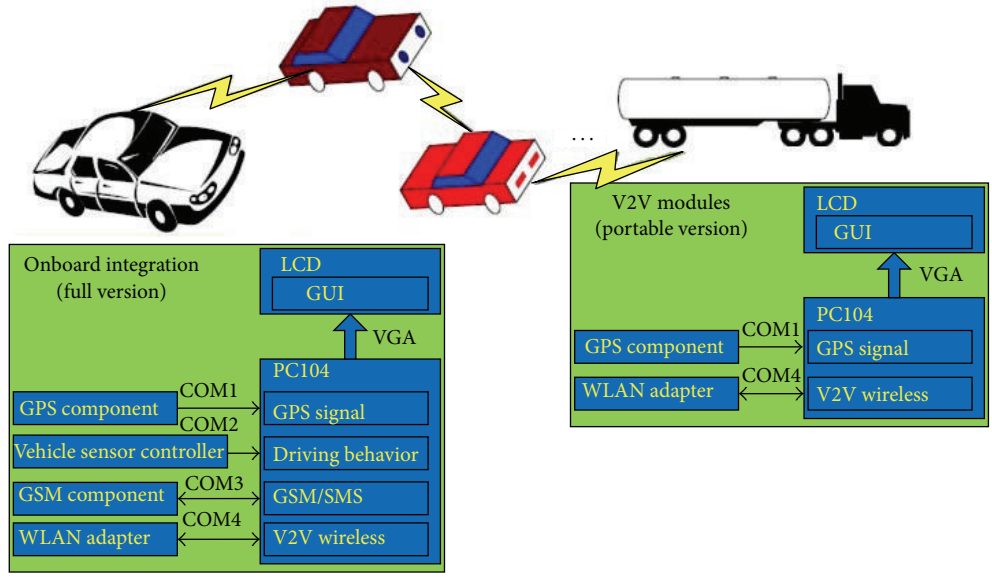


Figure 26: Platform integration architecture.

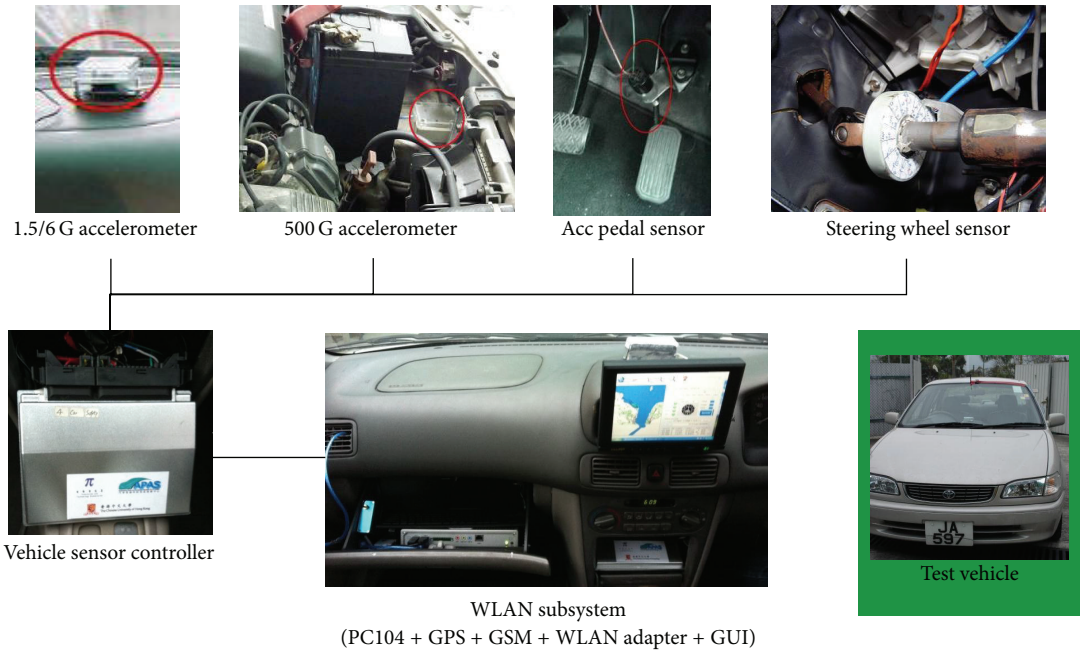


Figure 27: Onboard integration subsystem.

6.2. Integration for Onboard Subsystem. Onboard subsystem is full version for collision detection and classification, so all sensors as shown in Table 1 are installed onboard. Some main sensors are shown in Figure 27.

6.3. Integration for V2V Portable Subsystem. In order to design low cost platform for V2V application, we also need to develop a portable system to be installed on others test car. A series of portable V2V nodes have been developed and used for real road test, as shown in Figure 28.

Currently, we implement GBAODV based on AODV-UU [50]. Two threads are running under one main process. One is for routing in the network and the other is for reading GPS data through serial port directly.

Environment and devices for network test include

(i) Linux Fedora 7,

(ii) PC104 consortium [51],

(iii) Ralink RT2500 series wireless LAN card,

(iv) SiRF StarIII GPS module,

(v) touch screen and keyboard.

6.4. Road Test Scene. In this section, different experiments are conducted to demonstrate the functions and performance

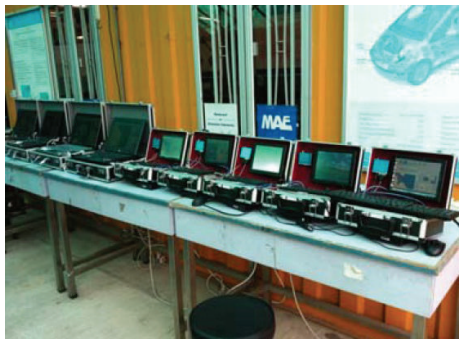


Figure 28: V2V portable subsystem.

Figure 29: The scene of experiments: Science Park, Hong Kong.

Table 7: Average packet loss ratio.

Number of nodes	AODV	GBAODV
4	45.5%	61.7%
5	63%	59%
6	73%	59%
7	56%	54.3%
8	51.5%	41%

of the integrated system. In these experiments, the key vehicle is a Toyota Corolla, equipped with the full version system, including WLAN-based component, GPS component, GPRS component, hazardous driving behavior detection subsystem, and collision detection and analysis subsystem. Aside of that, we prepared eight sets of portable systems. These portable systems include WLAN-based component and GPS component. The scene of experiments is the road near Hong Kong Science Park and the corresponding driving path is marked as a blue path in Figure 29.

6.5. V2V Communication Test. In this experiment (Figures 30 and 31), all vehicles are driven along a line with 30 km/hr. Different alarm signals are triggered manually by each of the vehicles randomly. The source sends 100 PING messages to destination continuously. The V2V communication system is then evaluated by checking whether the other vehicles can receive the PING message caused by status changing. The test result is shown in Table 7.

GBAODV performs better than AODV in general. Although the packet loss ratio is large, this is acceptable. Since there are barriers, such as buildings, in the experiment

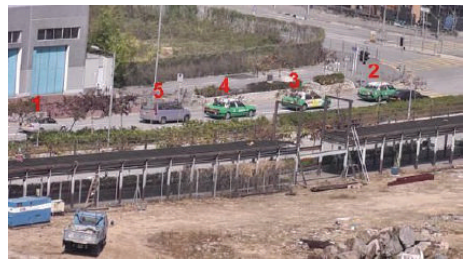


Figure 30: Vehicle experiment.

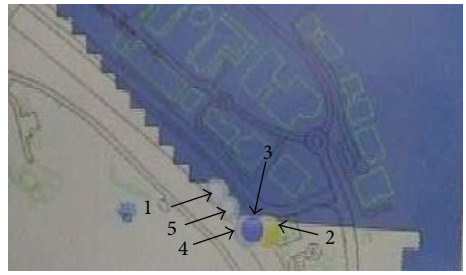


Figure 31: GUI for vehicle experiment.

environment, the signal attenuates rapidly. The packet loss ratio after one hop is approximately 20%. PING is round trip message. If source and destination cannot communicate directly, PING message traverses at least 4 hops. Therefore, the packet loss ratio is at least

$$1 - (1 - 0.2)^4 = 0.5904. \quad (13)$$

This is close to the experiment results. If the environment is clear enough, the results should be better.

7. Conclusion

In this paper, we presented a vehicle safety enhancement system based on wireless communication. The system can obtain vehicular signals, classify hazardous information, and make decision to trigger different actions to prevent the accident from occurrence or deterioration. To enhance the network performance, we evaluated DSDV, DSR, and AODV protocols and adopted AODV as the benchmark protocol. Thereafter, GPS information is integrated into AODV to further upgrade to GBAODV, which reduces packet loss rate and end-to-end delay, especially for downtown application in VANET. This paper also addresses V2I routing, by proposing the SIDGMS, which balances delay and network load. Simulation validates the V2I algorithm. Finally, we evaluate the V2V system by on-road test.

Acknowledgments

The authors would like to Dr. Xin Shi, Dr. Wing Kwong Chung, Mr. Yanbo Tao, Mr. Kai Wing Hou, Mr. Maxwell Chow for participating in the project and the on-road test. This paper is partially supported by the Hong Kong Innovation and Technology Fund project ITP/003/09AP and

RFD2012/2013 at Centre for Research on Robotics and Smart-city, The Chinese University of Hong Kong—Smart China.

References

[1] http://www.vehicle-infrastructure.org/.

[2] M. Heddebaut, J. Rioult, J. P. Ghys, C. Gransart, and S. Ambellouis, "Broadband vehicle-to-vehicle communication using an extended autonomous cruise control sensor," *Measurement Science and Technology*, vol. 16, no. 6, pp. 1363–1373, 2005.

[3] M. Shulman and R. Deering, "Third annual report of the crash avoidance, metrics partnership April 2003-March 2004," Tech. Rep. DOT HS 809 837, National Highway Traffic Safety Administration, Washington, DC, USA, 2005.

[4] W. Franz, R. Eberhardt, and T. Luckenbach, "Fleetnet—internet on the road," in *Proceedings of the 8th World Congress on Intelligent Transport Systems*, Sydney, Australia, 2001.

[5] T. Taleb, E. Sakhaee, A. Jamalipour, K. Hashimoto, N. Kato, and Y. Nemoto, "A stable routing protocol to support ITS services in VANET networks," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3337–3347, 2007.

[6] OnStar, http://www.onstar.com/.

[7] Y. Chen, Y. Sun, N. Ding et al., "A real-time vehicle safety system," in *Proceedings of the IEEE/SICE International Symposium on System Integration*, pp. 957–962, Fukuoka, Japan, December 2012.

[8] http://en.wikipedia.org/wiki/Traffic_collision.

[9] K. LaMance, "Auto accidents caused bysudden stops," http://www.legalmatch.com/law-library/article/auto-accidents-causedby-sudden-stops.html.

[10] Krystle, B. Robertson, N. Shaw, and et .al, "How to deal with a minor car accident," http://www.wikihow.com/Deal-With-a-Minor-Car-Accident.

[11] L. A. Wallis and I. Greaves, "Injuries associated with airbag deployment," *Emergency Medicine Journal*, vol. 19, no. 6, pp. 490–493, 2002.

[12] http://en.wikipedia.org/wiki/Rollover.

[13] N. Liu, H. Qian, J. Yan, and Y. Xu, "Performance analysis of routing protocols for vehicle safety communications on the freeway," in *Proceedings of the 3rd International Conference on Anti-Counterfeiting, Security, and Identification in Communication, (ASID '09)*, pp. 85–88, Hong Kong, August 2009.

[14] M. Zhang and R. S. Wolff, "Routing protocols for vehicular Ad Hoc networks in rural areas," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 126–131, 2008.

[15] S.-J. Lee, M. Gerla, and C. K. Toh, "Simulation study of table-driven and on-demand routing protocols for mobile ad hoc networks," *IEEE Network*, vol. 13, no. 4, pp. 48–54, 1999.

[16] A. Laouiti, P. Muhlethaler, F. Sayah, and Y. Toor, "Quantitative evaluation of the cost of routing protocol OLSR in a vehicle ad hoc network (VANET)," in *Proceedings of the IEEE Conference on Vehicular Technology*, pp. 2986–2990, Singapore, May 2008.

[17] L. Abusalah, A. Khokhar, and M. Guizani, "A survey of secure mobile ad hoc routing protocols," *IEEE Communications Surveys and Tutorials*, vol. 10, no. 4, pp. 78–93, 2008.

[18] IETF MANET Working Group, http://www.ietf.org/html.charters/manetcharter.html.

[19] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance vector routing (DSDV) for mobile computers," in *Proceedings of the Conference on Communications Architectures, Protocols and Applications (SIGCOMM '94)*, pp. 234–244, London, UK, September 1994.

[20] D. Johnson, Y. Hu, and D. Maltz, "The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4," IETF MANET Working Group Internet Draft (RFC4728), http://www.ietf.org/rfc/rfc4728.txt.

[21] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," IETF MANET Working Group Internet Draft (RFC3561), http://www.ietf.org/rfc/rfc3561.txt.

[22] Y. Sun, Y. Chen, and Y. Xu, "A GPS enhanced routing protocol for vehicular ad-hoc network," in *Proceedings of the IEEE International Conference on Robotics and Biomimetics*, pp. 2096–2101, Phuket, Thailand, December 2011.

[23] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, (WMCSA '99)*, pp. 90–100, New Orleans, La, USA, February 1999.

[24] W. Xiong and Q. Li, "Performance evaluation of data disseminations for vehicular ad-hoc networks in highway scenarios," *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, vol. 37, part B1, 2008.

[25] B. Mustafa and U. W. Raja, *Issues of routing in VANET [M.S. thesis]*, School of Computing, Blekinge Institute of Technology, Blekinge, Sweden, June 2010.

[26] W. Kim, D. Kwon, and Y. Suh, "A reliable route selection algorithm using global positioning systems in mobile Ad-hoc networks," in *Proceedings of the IEEE International Conference on Communications*, pp. 3191–3195, Helsinki, Finland, June 2001.

[27] O. Abedi, R. Barangi, and M. A. Azgomi, "Improving route stability and overhead of the AODV routing protocol and making it usable for VANETs," in *Proceedings of the 29th IEEE International Conference on Distributed Computing Systems Workshops*, Montreal, Quebec, Canada, June 2009.

[28] O. Abedi, M. Fathy, and J. Taghiloo, "Enhancing AODV routing protocol using mobility parameters in VANET," in *Proceedings of the IEEE/ACS International Conference on Computer Systems and Applications*, pp. 229–235, Doha, Qatar, March-April 2008.

[29] H. Asenov and V. Hnatyshin, "GPS-enhanced AODV routing," in *Proceedings of the International Conference on Wireless Networks (ICWN '09)*, Las Vegas, Nev, USA, 2009.

[30] VanetMobiSim, http://vanet.eurecom.fr.

[31] NS2, http://www.isi.edu/nsnam/ns.

[32] TIGER/Line/circledR, http://www.census.gov/geo/www/tiger.

[33] M. Treiber, A. Hennecke, and D. Helbing, "Congested traffic states in empirical observations and microscopic simulations," *Physical Review E*, vol. 62, no. 2, pp. 1805–1824, 2000.

[34] "VanetMobiSim Manual," http://www.scribd.com/doc/1107-52020/VanetMobiSim-1-0-Manual.

[35] Y. Chen, Y. Tang, G. Xu, H. Qian, and Y. Xu, "A data gathering algorithm based on swarm intelligence and load balancing strategy for mobile sink," in *Proceedings of the 8th World Congress on Intelligent Control and Automation, (WCICA '11)*, pp. 1002–1007, Taipei, Taiwan, June 2011.

[36] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," *Ad Hoc Networks*, vol. 3, no. 2, pp. 325–349, 2005.

[37] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *Ad Hoc Networks*, vol. 40, no. 8, pp. 102–105, 2002.

[38] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MOBICOM '00)*, pp. 56–67, Boston, Mass, USA, August 2000.

[39] N. Sadagopan, B. Krishnamachari, and A. Helmy, "The ACQUIRE mechanism for efficient querying in sensor networks," in *Proceedings of the IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 149–155, 2003.

[40] D. Braginsky and D. Estrin, "Rumor routing algorithm for sensor networks," in *Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications (WSNA '02)*, pp. 22–31, Atlanta, Ga, USA, September 2002.

[41] H. Luo, F. Ye, J. Cheng, S. Lu, and L. Zhang, "TTDD: two-tier data dissemination in large-scale wireless sensor networks," *Wireless Networks*, vol. 11, no. 1-2, pp. 161–175, 2005.

[42] A. Manjeshwar and D. P. Agrawal, "TEEN: a routing protocol for enhanced efficiency in wireless sensor networks," in *Proceedings of the 15th International Parallel and Distributed Processing Symposium*, pp. 2009–2015, San Francisco, Calif, USA, 2001.

[43] A. Manjeshwar and D. P. Agrawal, "APTEEN: a hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks," in *Proceedings of the 15th International Parallel and Distributed Processing Symposium*, 2002.

[44] J. Ding, K. Sivalingam, R. Kashyapa, and L. J. Chuan, "A multi-layered architecture and protocols for large-scale wireless sensor networks," in *Proceedings of the IEEE Vehicular Technology Conference, (VTC '03)*, vol. 3, pp. 1443–1447, Orlando, Fla, USA, October 2003.

[45] Y. C. Hu, D. B. Johnson, and A. Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks," *Ad Hoc Networks*, vol. 1, no. 1, pp. 175–192, 2003.

[46] L. X. Hung, D. H. Seo, S. Lee, and Y. K. Lee, "Minimum-energy data dissemination in coordination-based sensor networks," in *Proceedings of the 11th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications*, pp. 381–386, Hong Kong, August 2005.

[47] Q. Huang, Y. Bai, and L. Chen, "An efficient route maintenance scheme for wireless sensor network with mobile sink," in *Proceedings of the IEEE 65th Vehicular Technology Conference (VTC '07)*, pp. 155–159, Dublin, Irland, April 2007.

[48] D. Lee, S. Park, E. Lee, Y. Choi, and S.-H. Kim, "Continuous data dissemination protocol supporting mobile sinks with a sink location manager," in *Proceedings of the Asia-Pacific Conference on Communications, (APCC '07)*, pp. 299–302, Bangkok, Thailand, October 2007.

[49] T. S. Rappaport, *Wireless Communications: Principles and Practice*, IEEE Press, Piscataway, NJ, USA, 1996.

[50] AODV-UU, http://core.it.uu.se/adhoc.

[51] PC/104 Embedded Consortium, http://www.pc104.org/history.php.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 834596, 10 pages
http://dx.doi.org/10.1155/2013/834596

Research Article

Design and Implementation of an Application for Deploying Vehicular Networks with Smartphones

P. Caballero-Gil, C. Caballero-Gil, and J. Molina-Gil

Department of Statistics, Operations Research and Computing, University of La Laguna, 38271 Tenerife, Spain

Correspondence should be addressed to P. Caballero-Gil; pcaballe@ull.es

Received 11 May 2013; Revised 2 November 2013; Accepted 18 November 2013

Academic Editor: Shukui Zhang

A vehicular ad hoc network (VANET) is a wireless network that provides communications between nearby vehicles. Among the different types of information that can be made available to vehicles through VANETs, road traffic information is the most important one. This work is part of an experimental development of a wireless communication platform oriented to applications that allow improving road efficiency and safety, managing and monitoring road traffic, encouraging cooperative driving, and offering pedestrian services and other added-value uses. The proposed system consists of smartphones, sensors, and Wi-Fi hotspots 2.0, as well as complementary functionalities including access to network infrastructure via 3G, GPRS, and 4G. The developed wireless network prototype allows taking advantage of the potential benefits of VANETs. At the same time, the use of smartphones does not require large money investments either in public or restricted areas. The first implementations with smartphones have been useful to test the behaviour of the proposal in a real environment. We have also implemented a large-scale simulation by using NS-2 simulator. From the obtained data, we have estimated the minimum requirements necessary for the correct working of a VANET and the problems that can happen in case of possible attacks or communication overhead.

1. Introduction

There is an urgent need to improve traffic management throughout the world, particularly in large urban areas. The growing congestions, gradual increase of pollution, and concern for improving vehicle safety have prompted governments and automobile industry to explore the potential of intelligent transportation systems (ITS). However, the development of the theoretical standard IEEE802.11p for Vehicular Ad-Hoc Networks, which will offer many environmental, economic, and mobility advantages, has been physically impossible due to the enormous cost that would imply for users and institutions to adapt vehicles and roads. On the one hand, roads would require including road side units (RSUs), and on the other hand, users' vehicles would have to include on board units (OBUs).

In this paper, we propose a new approach for the deployment of VANETs using current Information and Communications Technologies (ICTs). The wide deployment of ICTs involves that different pieces of technology, such as mobile phones, sensors, and wireless technology, have become ubiquitous mainly due to the significant reduction in their prices. This type of technology has a potential that has not yet been explored for the implementation of ITS applications without any deployment of RSUs and OBUs.

In order to address the development and implementation of new vehicular applications by combining these devices, it is critical to have an overview of all the involved technologies. The field of vehicular communications can offer huge advantages for drivers, pedestrians, traffic managers, transportation service providers, traders, and so forth. However, it can suffer many types of attacks that can endanger human lives or decrease transport efficiency in strategic times and/or locations. For this reason, the design and development of the proposed application are to be run on current devices, taking into account safety and security systems, in both communications and relayed information.

This paper describes a set of tools for the implementation of the proposal in the Android platform. It consists of a set of applications forming a secure communication system for spontaneous and self-organizing networks based on smartphones, which does not require any infrastructure in

vehicles or on roads because its operating mode is completely distributed and decentralized. In particular, our proposal is based on Wi-Fi Direct in order to reduce the costs to zero, because today existing smartphones all over the world offers such connectivity and its use has no cost at all. Besides, other communication techniques such as 3G/4G can provide higher transmission speed, longer transmission distance, and larger network throughput. By combining Wi-Fi Direct and 3G/4G technology, we ensure communications everywhere and at every moment.

Here, we present the design of a secure communications system in a spontaneous and self-organized vehicular ad hoc network, without any infrastructure either on roadside or in vehicles, using only mobile devices. In particular, we present a hybrid software platform that integrates different types of wireless technologies, such as Wi-Fi Direct, Bluetooth, and 3G/4G, and focussed on different ITS applications:

(1) safety applications to avoid crashes, announce road hazards and serious traffic infringement, report about approximation of emergency vehicles, and so forth,

(2) applications for traffic management and monitoring, which allow warning and/or avoiding traffic jams,

(3) value-added applications for management of parking lots, geolocated advertising platform, weather information, optimized public transport, and so forth.

The rest of the paper has been organized as follows. Section 2 covers related research on security and applications of VANETs. The technology required by the system specifications is presented in Section 3. Section 4 contains a detailed description of VAiPho structure, including explanations of its main applications. Security issues related to information content and user anonymity are analysed in Section 5 considering different possible attacks, while Section 6 provides some details on simulation a real implementation of the proposal. Finally, conclusions are presented in Section 7.

2. State of the Art

The first prerequisite to be considered when designing a tool to create a self-organizing vehicular network for increasing road safety and passenger comfort is the accuracy and reliability of transmitted information. Thus, security is one of the most important topics to be taken into account when a communication system is designed for VANETs [1]. In the bibliography we can find several proposed schemes for self-organizing VANETs [2–4] and MANETs [5–7], which try to solve all or part of the security problems existing in these types of networks. However, a different approach is presented in this paper, where a practical and secure way to deploy VANETs nowadays is proposed. The work [8] has the same objective as this work, but it does not address the main aspect of connection security.

User privacy is an important issue that needs to be addressed for the development of vehicular networks. Our proposal uses a random pseudonym generator to guarantee with a high probability that it is not possible to track a vehicle either from other vehicles or from road infrastructures, and that coincidences between two generated pseudonyms could exist but are unlikely. In [9] a pseudonym-based scheme is proposed where the authors try to solve the privacy problem caused when GPS coordinates and speeds of vehicles are sent in the beacons. In our proposal, none of those data are sent in beacons. The more recent work [10] proposes a distributed traceable pseudonym management scheme based on a blind signature.

Nowadays, many centralized GPS software navigators offer traffic services based on information provided by local road authorities, police departments, and systems that track traffic flow. However, neither of them are real-time data as they do not reflect the events that have just produced, nor respect users' privacy, so people are reluctant to use them. Regarding the congestion detection problem, Google Traffic [11], TomTom [12], Sygic [13], and Waze [14] are solutions to detect traffic congestions. The main difference with our proposal is that all of them need a data connection (LTE, 3G, or GPRS) to work. Another disadvantage is that users completely lose their privacy because they have to provide information on their locations to the companies that support the service. Furthermore, sometimes user privacy is violated because those data are stolen from the servers of the companies.

With respect to the search for free parking spaces, recently other authors have proposed different solutions. However, unlike this paper, most of them are related to paid parking. References [15, 16] are proposals involving that a device is installed in the passenger door, and when an empty parking space is found, this information is reported to a centralized server through 3G or GPRS. In [17], the authors propose a solution where users can find empty parking spaces managed by RSUs. Reference [18] presents another system for the management of parking spaces in a radius, but its goal is not on how the information is obtained and transmitted through the network but on how it is managed.

Since the solution to find a parked car is quite easy to implement, several applications for it can be found in the different mobile platform markets [19, 20]. However, we want to clarify that such an application is simply an added value of the proposal, and not its main goal.

The main starting point of this paper is the idea that the introduction of a complete model of VANETs would be extremely expensive both for users, who would have to buy and install some devices in their vehicles, and for the state, which would have to deploy RSU on the roads to support VANET services. Therefore, this work proposes a self-organizing VANET based only on communications between vehicles, with no infrastructure. The idea is that this model can serve as a quick introduction to a more complex and complete VANET, all this with good levels of reliability and security.

Our main goal is to define a simple and scalable model for VANETs, where users can cooperate through their mobile devices to obtain updated information of interest about the traffic area in order to choose the best updated route to their destinations. Our proposal takes into account that the integration of VANETs will be gradual, so that at the beginning there will not be any kind of RSU, and the VANET

Figure 1: Minimum system specifications.

will start from a few vehicles, to grow to a larger number of vehicles. This growth will be faster or slower depending on the usability and offer of added-value services that the software for VANETs provides to the users. Thus, in this paper we focus on the first phase of VANET deployment. As soon as the VANET infrastructures are fully deployed, the proposed solution should be checked to avoid unnecessary communications so that the high number of communications does not degrade the network.

3. Used Technology

The system here proposed, called VANET in Phones (VAiPho), has been fully developed and tested for Windows Mobile. We know that this technology is obsolete so here we present a partially development for Android. Mobile application development has gone multiplatform, so we know that VAiPho will have to be developed for iOS and Windows Phone platform too. However, none of both platforms allow creating direct communications with other OS smartphones, so the implementation in these platforms will depend on the required opening of the native libraries.

The following technology (see Figure 1) is necessary for the optimal use of VAiPho.

Bluetooth/Bluetooth Low Energy. To connect the device with the vehicle, providing automatic activation of VAiPho services without requiring the user's attention.

Wi-Fi Direct. IEEE 802.11 b/g/n. For the direct exchange of information about possible events between different wireless devices.

Location Services. They include information from mobile phone towers, GPS antenna, and nearby Wi-Fi nodes to obtain the geographic coordinates where the different events happen as well as the speed and direction of the involved vehicle.

Storage Space. With the required capacity for storing the necessary apps, maps and data about users, and information.

Battery. To run the application and communicate with other nodes.

As we can see, VAiPho uses the powerful application platform capabilities of today's mobile devices. Thus, it is not expensive at all for users. Furthermore, people are used to working with mobile devices, so the user interface of VAiPho is not strange for users, which avoids the usual difficulties of learning to use new devices.

Most of the VAiPho information exchanges are performed using the Wi-Fi Direct standard. This standard is highly suitable for this type of communication because devices can connect directly to each other quickly and conveniently in order to do different tasks such as synchronization and sharing of data. The IEEE 802.11p standard of wireless communications [21] was specifically designed for the deployment of VANETs and therefore it is more appropriate for this type of communications. However, nowadays there are no devices capable of broadcasting in the frequency range that IEEE 802.11p uses. For this reason, VAiPho uses Wi-Fi Direct, which is based on the IEEE 802.11 family of standards for wireless local area network operation and has the ability to communicate under the IEEE 802.11b/g/n standard.

4. Application Structure

VAiPho structure consists of three main parts that have been implemented in different applications in order to test each one separately to find problems individually before integrating them into VAiPho implementation, as shown in Figure 2.

Bluetooth Launcher. It runs several services to detect available connections in the smartphone. It is a light program in charge of detecting Bluetooth, NFC, or charger connection to launch other services when the user is inside the car. It is especially useful if the device is connected with the Bluetooth hands-free car kit.

Smart Navigator. It launches the automatic application that is responsible for detecting and forwarding the events that happen on the road.

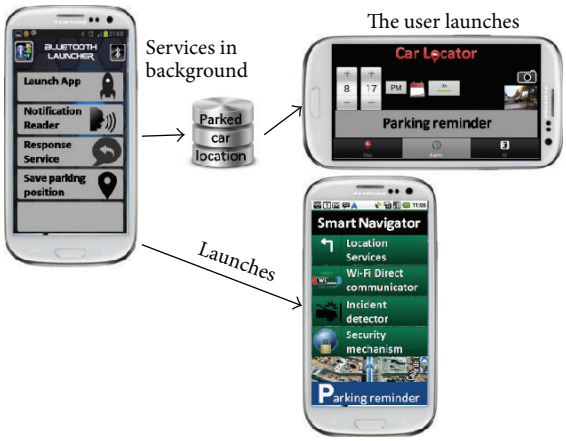


Figure 2: VAiPho structure.

Figure 3: Interface of Bluetooth Launcher.

Car Locator. It is designed to show the information saved by the Bluetooth Launcher about the car's position.

Geolocated Advertising. It is the source of VAiPho commercial profit.

This section presents these modules so that their internal structure is fully detailed.

4.1. Bluetooth Launcher. Bluetooth Launcher allows the automatic starting of the application via Bluetooth when the mobile phone connects to the hands-free car kit. This application is one of the most important parts of VAiPho from the point of view of road safety because it ensures that users keep the focus on driving, as distraction is a major cause of deaths on the road. For this reason, Bluetooth Launcher, which is a very light application, is a service that listens for the smartphone connections, so that when the smartphone connects with the hands-free car kit through Bluetooth, NFC, or charger, it automatically launches a navigation application (see Figure 3). In this way, it does not require the driver attention, which prevents possible distractions if the driver forgets to turn it up.

Bluetooth Launcher automatically launches the listening services when the user powers on the smartphone and, from then, it runs in background. It hardly consumes any resources because its unique function is to listen to a registry and to launch other applications like the Smart Navigator, if the device connects to the car through Bluetooth, NFC, or charger.

Another important characteristic of Bluetooth Launcher is that it reads the notifications aloud. Thereby, the user can listen to the notifications from chat apps like WhatsApp, Line, Viber, and so forth, or from SMS. It also shows these notifications in the smartphone screen with large fonts. Furthermore, it allows easily answering those messages without the need of using hands with the smartphone.

We are aware that the priority of mobile phones is to make phone calls and high battery consumption would cause discomfort to users. This fact has been taken into account when implementing Bluetooth Launcher, so it has very low battery consumption and it is not a drawback for VAiPho.

4.2. Smart Navigator. Smart Navigator is the main application of VAiPho. It is also the most complex one because it involves many different tasks. VAiPho requires both connectivity with other phones via Wi-Fi Direct and GPS. Thus, connectivity using standard interfaces is necessary. Besides, VAiPho uses GPS information, like maximum lane speed, vehicle speed, and geographic coordinates, in order to detect possible congestions or empty parking spaces. This information has to be processed, stored, and sent to other vehicles. For that purpose, the Smart Navigator implements the following functionalities: starting the wireless interface, creating an ad hoc network or connecting to other devices, loading data from the database and password file, loading and starting the client beaconing and the server, starting the maps app, and starting the incident detector.

The process followed when the Smart Navigator launched involves the following steps. First, the Wi-Fi Direct interface is launched and begins receiving and sending beacons from and to the network. If the interface finds a node, it connects with it via Wi-Fi Direct. Then, it creates and fills the database with user data like private/public key pair, secret key, pseudonym, and so forth. These security issues are detailed in Section 5. Then, the system is ready to communicate and exchange information about events with other devices in the range of transmission. This entire process is automatic and transparent to the user, and just a voice message indicates to the driver that VAiPho has begun.

Once the communication system is set, the GPS navigator is started and an incident detector system is launched. The main goal of Smart Navigator is to detect an abnormal situation automatically in order to produce the corresponding event warning and alert the driver and other users about that situation. This process uses GPS software to obtain data such as speed and location. Specifically for the real device implementation of this work we have used the Google Maps API.

Smart Navigator has the target of detecting possible congestions on the roads automatically, so it uses the function of the SDK that allows retrieving the actual location and speed as well as the speed limit of the current road. With this information, the event detector of VAiPho finds out whether the vehicle is travelling at an unusually low speed

and, in such a case, it concludes that the vehicle is stuck in a traffic jam. Once detected the incident, the process generates an event warning including the road name, direction of car movement, and geographic location in which the incident is located. This event is stored in the database and relayed to other vehicles. Thanks to these automatic event detections and the cooperation among devices, it is possible to know more about road conditions. This information is relayed to other vehicle, which can play different roles depending on their situation regarding the detected event. On the one hand, if the vehicle that receives the warning can confirm it because it is travelling on the same road and has also detected the same event, nodes use the data aggregation scheme described in Section 5, in order to avoid network overload. On the other hand, if a vehicle receives the warning but it cannot detect the event because it is not circulating on the same road where the event has been detected, or it is on the same road but far away from the incident, there are two possibilities.

(a) The road is not part of the receiver vehicle route: in this case, the vehicle acts as a simple packet transmitter and relays the packet to all the vehicles within its range of transmission.

(b) The road is part of the receiver vehicle route: this case takes more processing time because first the vehicle has to determine whether the busy road is in its route, and if so, it has to compute whether it is better to choose an alternative route or to keep the same one. If the system determines that it is better to use an alternative route, the new route is calculated.

Many security issues have been taken into account to implement all these processes because any attacker could try to generate false events, or to modify the contents of real packets, or even to deny relaying packets in order to attack the network operation. Therefore, communications among vehicles and information about detected events relayed in the network should provide evidence of being truthful. For this purpose, a security module presented in Section 5 has been created and added to VAiPho. In this section we explain possible attacks and how VAiPho resists each of them.

There is another important task of Smart Navigator, which is the detection of parking space availability. In this application, the procedure is simple. When a driver turns on the car, the mobile device synchronizes to the GPS signal and obtains the geographic coordinates where the vehicle is parked before it leaves the space. Then, Smart Navigator broadcasts these geographic coordinates as a potential empty parking space. Received events of parking spaces have a short expiration time that is configurable by the user. The default value is set to 1 minute in the implementation. Frauds and errors cannot be controlled for parking events because there are several situations where a vehicle can leave a certain location that is not a valid public parking space, such as a private outdoor parking space or a prohibited parking space. For this reason, when the tool announces a parking space, it indicates that it is a potential empty parking space, but there is no guarantee that the space continues to be available when the receiver reaches it. In order to use this tool, it is necessary

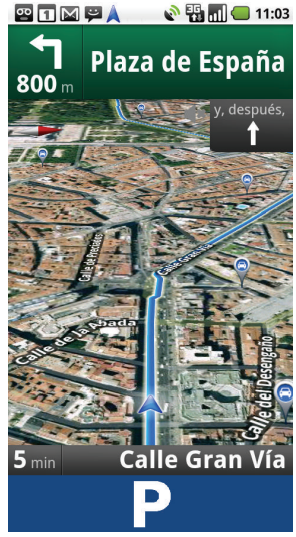


Figure 4: Driver Interface of Smart Navigator.

to launch the search for an empty parking space. When an empty parking space is detected, it is shown on the map and a voice message is then launched.

Figure 4 shows the interface that is displayed when the user is driving. It is very similar to that used by conventional GPS navigation applications. In order to prevent distracted driving, this interface not only uses icons on the maps but also voice messages. Therefore, when it detects traffic congestion or a possible empty parking space, an icon on the screen is shown and a voice message indicating congestion on the route or available parking is heard.

4.3. Car Locator. This application has a simple interface, which is shown when the user is not driving (see Figure 5). When the user turns off the car, the geographic coordinates where the vehicle is parked are stored in the database in order to help the user to find the parked vehicle. Often, it is difficult for users to find the places where they parked their cars, especially in large and unknown cities. In these cases, Car Locator uses the geographic coordinates of the parked vehicle stored in the database in order to draw a walking route to the car on the map.

Additionally, the users can check the events that are updated and stored in their mobile phones. In particular, Car Locator module provides a tool to locate where the vehicle is parked, if both Bluetooth Launcher was active when the car was parked and the parking space had location service coverage. For this purpose, Car Locator module provides a parking remainder button, marked with word *find*, which the users have to click on to locate their cars. This module launches the GPS navigator on walking mode to show the place where the vehicle is located and the route on the map between the user current location and the car. Figure 5 shows the case when the application indicates that the information on the vehicle location is available.

4.4. Geolocated Advertising. Companies or users that are interested in advertising through this tool may contact the

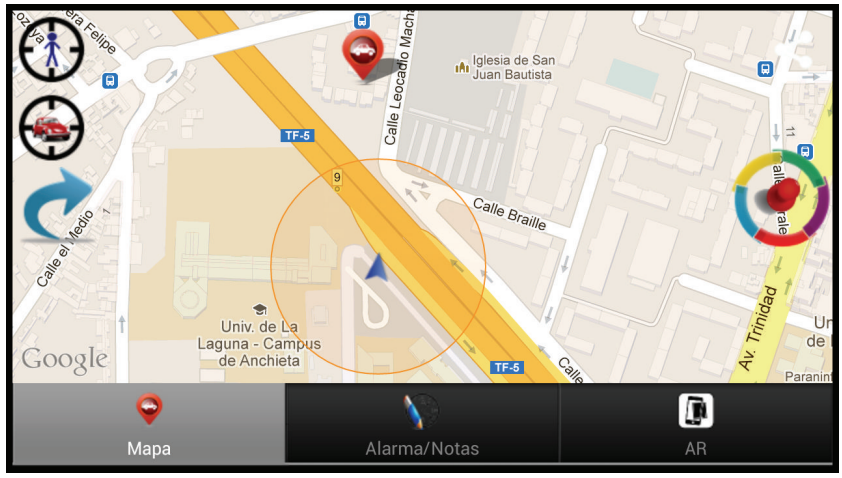


Figure 5: Pedestrian Interface of Car Locator.

administrators because VAiPho allows providing geolocated advertising as source for commercial profit. In particular, all registered users or companies can contract geolocated advertising.

Advertising data include name of the company, message, X coordinate, Y coordinate, area of interest, expiration date, and commercial logo. The message is limited to a short number of characters in order to be easily showed and read by the application. This information is processed and checked and, after the payment, the user receives a packet containing the advertising information and its certificate. The user then has to download the Geolocated Advertising application and store it in a predetermined path in its device. Afterwards, its device will broadcast the advertising information to all nearby VAiPho users, who will receive it if it is so defined in their advertising filters.

5. Security Mechanisms

An important challenge in VANETs is security, not only regarding the users that take part in the network but also the involved communications. Moreover, the relay information can affect driver decisions because they can reduce their speed and/or choose alternative routes based on a received report. Thus, a security scheme is necessary to determine whether the available road traffic information to the driver is trustful or not. Besides, the quality of communications in VANETs can be degraded if the number of noncooperative vehicles is very large. For this reason, VAiPho includes several security mechanisms to prevent possible attacks against data integrity and user privacy.

5.1. Reliability. The definition of trust relationships between users to define which devices are reliable inside the network is an important issue. In order to reach this purpose, a trust graph according to which key certificates are distributed is proposed. For this goal, people interested in VAiPho must register in the application, which allows generating a file of signatures and certificates that are required to use the application.

VAiPho is a self-management tool based on the trust between users defined through key certificates signed by the users who trust the corresponding key and owner. The more signatures a key certificate has received, the greater the trust from other nodes that can be used during its life in the network. Therefore, we can find a similarity between our network and social networking sites like Facebook, Twitter, and so forth. In this way, VAiPho operates according to what is called viral marketing; that is to say, it uses techniques based on preexisting social networks. In order to facilitate the registration process, VAiPho will use the APIs of the social networks (Facebook, Twitter, Google+) to enable the registry of the user in VAiPho services.

Furthermore, VAiPho allows users not involved in any social network to use their email account for trust goal. They can log in the application and register to get their pair of public and private keys in order to start using VAiPho. Once the users register their email credentials, the tool imports their contacts from their email accounts and searches in this list other users registered in the system. The resulting list is then displayed to the new users so that they can confirm who of these users will be used to sign their certificates. During the signing process, VAiPho website exchanges the generated certificates so that each user holds the signature generated by itself and the signatures produced by its friends. Each time a new mutual authentication is done, the application may download an updated file containing the certificates generated by the users and its friends, which is needed to generate the certificate graph of the trust network to allow secure communications within the network.

Users can download the application from Google Play. Once the application is installed on their devices, it generates the files containing the cryptographic information and stores them in a protected path.

5.2. Privacy and Legitimacy. Privacy and legitimacy are the most important issues regarding VANET security.

On the one hand, in VANETs it is completely undesirable that, through the communications, any attacker can track a

user. In centralized systems using long reach communications the situation could be even worse because an attacker could track all the vehicles at the same time from a single site. VAiPho mechanism does not use long reach communications so this centralized attack is not possible. However, the particular Wi-Fi Direct signal that VAiPho uses for communication could be tracked. In order to protect user privacy, the application uses variable pseudonyms associated with the phone MAC address as identifiers. In particular, VAiPho application changes its pseudonym in random time periods and warns about these changes through the beacons only to those nodes with which it is authenticated.

On the other hand, it is necessary to ensure that the device corresponds to a legitimate user of the VAiPho network. Checking this in a fully distributed network, where there is no central infrastructure to control identities, is complex. In this work, the mechanism to verify the authenticity of users is based on a zero-knowledge proof, which is an interactive method for one user to prove to another that it knows a secret, without revealing anything about it. Specifically, in VAiPho the secret is the public key of a third user that both communicating parties know according to their certificate graph. Hence, public keys are specially selected to fulfil the requirements of the used zero-knowledge proof. In this way, it is necessary that both users share a friend's public key to make authentication possible. Thus, it is important that users maintain their certificate repositories updated. According to the so-called rule of 6 degrees of separation [22], nodes in this type of network have in their local repository at least one node in common with a high probability. VAiPho automatically revokes certificates of users who repeatedly show bad behaviour, and information about revocations is exchanged between authenticated users.

5.3. Integrity. One of the most important issues in security is to be able to ensure that information relayed in the network is trusted. An attacker could simulate a nonexistent traffic congestion in order to convince other users not to choose a route and in this way to have the road free of vehicles. VAiPho uses a data aggregation mechanism to avoid this type of possible fraud. The procedure is as follows. When the application installed in a device detects an abnormal situation such as a speed much lower than expected for a long time, it sends a traffic congestion warning to its neighbouring devices. If neighbour applications detect that their speed is abnormal too, they sign the received information, corroborating it. When the promoter application receives a minimum number of signatures, it adds them to an aggregated packet with the information and sends it to all neighbours, who widespread the data [23].

Therefore, traffic congestions must be detected by different VAiPho users, which must sign the traffic event with their private key in order to allow the aggregation of these signatures in a single packet. Thus, we ensure that not only a vehicle has detected an incident but also that several vehicles have corroborated it. This security mechanism eliminates the possibility of spreading false traffic congestions created by a single attacker and avoids possible confusion generated by the system when a vehicle stops on the side of the road due to different reasons such as a flat tire or a vehicle failure.

The minimum number of required signatures depends on the deployment level of the VAiPho application, that is to say, the higher the number of vehicles with VAiPho, the greater the number of required signatures. This will also mean that the larger the number of VAiPho devices in the network, the lower the possibility of attack. In order to calculate the threshold number of required signatures, VAiPho checks the time since its first authentication in the current journey and computes the average number of users per minute. In the current VAiPho implementation, this average is lower than one per minute, so the number of required signatures is two. If the number is between one and four per minute, the number of required signatures is four, and if the average is higher than four per minute, the number of required signatures is five.

5.4. Availability. Since in VAiPho the packets are exchanged among vehicles using others as relaying nodes, an attacker could try to make that communications fail. This could cause a VANET to be broken into pieces so that the network cannot provide services such as packet forwarding. Thus, an attacker could launch a passive denial-of-service with the goal that the wireless network does not work properly.

In this sense, VAiPho includes a specific mechanism against these attacks, which uses encrypted exchange of data as a method to strengthen cooperation in relaying packets as it prevents passive nodes that do not cooperate in relaying packets to get benefit from encrypted information.

In this way, VAiPho application ensures that only those vehicles that belong to the network and help in its operation benefit from information relayed in it. The encrypted exchange of data prevents users who want to benefit from the VANET without helping in forwarding information because such a passive attack would degrade the functionality of tool and compromise the connectivity of the network.

6. Experimental Analysis

Simulation data and real implementation settings are briefly presented in this section to demonstrate that VAiPho is successful in accomplishing the goals of automatically detecting and warning about traffic congestions and helping people to find empty parking spaces. Furthermore, through the experimental analysis we have checked that the goal is accomplished in a safe way, both regarding data integrity and user privacy.

These proof-of-concept tests were intended to evaluate whether deploying VANETs through mobile phones can fulfil specific characteristics of VANETs such as hybrid architecture, high mobility, dynamic topology, scalability problems, and intermittent and unpredictable communications.

The first test consisted in checking that communications between smartphones with Wi-Fi Direct by using the IEEE 802.11b/g/n standard are feasible by using a simple client-server application between devices, when circulating with vehicles in urban environments or motorways at different speeds, using different numbers of devices. These tests were successful. After this, we created several simulations of the

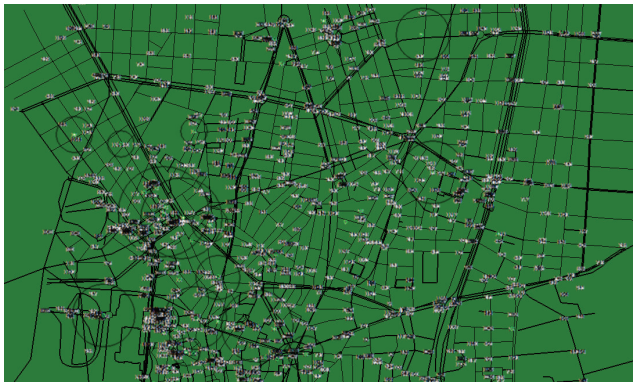


Figure 6: VAiPho simulation with SUMO and NS-2.

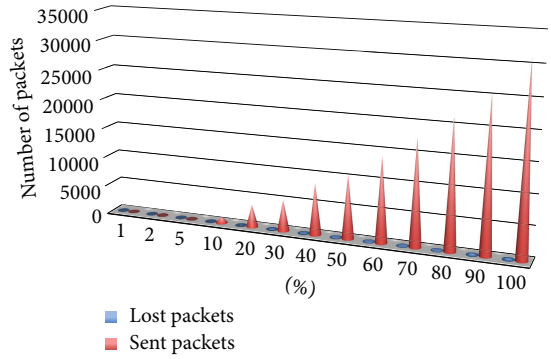


Figure 7: Numbers of packets in VAiPho simulation.

proposal by using SUMO and NS-2 in order to estimate the minimum number of vehicles that are required to deploy the network. Finally, we implemented and are now improving the complete set of applications that form VAiPho for Android smartphones.

6.1. Simulation. The main target of the simulations was to determine the minimum density of cars necessary to ensure the appropriate deployment of VANETs.

From the obtained results, we concluded that VAiPho is feasible in urban environments with a minimum percentage of vehicles that allow disseminating the information over the network. Under these conditions, both the feasibility and effectiveness of the approach were shown through the results.

In the first part of the simulation with NS-2 [24] and SUMO [25] (see Figure 6), the most relevant options selected for the demonstration were total number of vehicles: 600–15000, number of vehicles with OBUs: 1%–100%, simulation time: 100–216000 seconds, authentication period: 20 seconds, and distance between relay nodes: 75 meters.

The implemented simulations of VAiPho were studied in three different development levels: vehicle mobility, node energy, and Peer-TO-Peer (P2P) communication.

(i) The vehicle mobility level manages the node movement according to the movement pattern, which defines roads, lanes, different speed limits for each lane, traffic congestions, and so forth.

(ii) The node energy level is used to distinguish between vehicles with and without OBUs because vehicles without OBUs are on the road but do not make any contribution to the communications.

(iii) The P2P communication level is responsible for the definition of which nodes are in the transmission range of the retransmitting node at any time.

The simulations allowed us to know the number of connections in the network related to the percentage of vehicles with OBUs. From this information, the minimum number of vehicles with OBUs that is necessary to exchange information can be extracted. On the other hand, the percentage of vehicles with OBU necessary to avoid a drop in the quality of communications can be also estimated.

The simulations were run for different percentages of nodes with the same topology in order to illustrate the vehicular P2P network evaluation. Within the information obtained from the simulations (see Figure 7), we have the number of packets that have been generated, sent, broadcast, received, lost, and so forth by each node. Also, other computed information is the number of generated or lost packets in the whole network, which types of nodes generate packets and forward them, and so forth. In addition to all this information, another interesting aspect of simulations is that it provides a detailed image of what happens in each moment in the VANET thanks to the use of the NS-2 display. The traffic model was shown through the SUMO tool while the information was represented using the TraceGraph tool.

6.2. Real Implementation. Many communication tests have been made using the IEEE802.11b/g/n standard with VAiPho in mobile phones inside cars in urban environments.

The first conclusions of these tests are twofold. On the one hand, vehicles with VAiPho traveling in opposite directions do not have enough time to establish communications. On the other hand, vehicles in the same direction or inside cities, where the speed is lower, have enough time to establish communications and to exchange the data required by the proposal. Thus, the described system can be seen as a first approach to the real deployment of some interesting VANET applications with currents devices, which could be analysed as a proof of concept of the future WAVE-based VANETs [26].

For the evaluation, we built a set of VAiPho applications in different smartphones with Android using Java. Some videos showing how this tools works in real devices, vehicles, and roads can be found on the website [27].

The application has shown to be effective for traffic congestion recognition, parking detection, and parked vehicle finding. It also works well regarding authentication of users, protection of user privacy, and exchange of secret information with other devices. Devices running VAiPho that receive some information, display and forward such information correctly.

In particular tests showed good performance in:

Automatic Recognition and Warning of Traffic Congestions. The scenery is as follows. A vehicle is stuck in a traffic

jam. VAiPho application running on a device inside the car automatically detects it and broadcasts a warning message. Another device inside a car on the same route and direction detects the same traffic congestion and signs the received message, and the signed message is broadcast so that a third device displays the traffic congestion both on the screen and through voice messages.

Automatic Detection and Announcement of Empty Parking Spaces. The scenery is as follows. A vehicle leaves a parking space and broadcasts the announcement of an empty parking space. Nearby vehicles receiving this information forward it to other vehicles, and if they are looking for empty parking spaces, they show this information to the drivers on the map and through prompt messages.

Route to Parked Vehicle. The scenery is as follows. A vehicle is parked in a parking space and then the user leaves it. Afterwards, the user presses the parking reminder button and the tool shows the route on foot to the vehicle.

Geolocated Advertising. Advertisements are broadcast in their area of validity.

Systems for traffic congestion detection and warning were tested through several devices playing different roles. In this way, real traffic congestion situations were simulated. Different devices inside vehicles were in charge of detecting, signing, and aggregating the events, receiving those packets and checking the corresponding signatures in them before warning the driver and relaying the information. Figure 7 shows the number of packets that were sent and lost during the test. In order to check the parking detection tool, one of the cars was parked and turned off. After that, the car was started and when the device synchronized with GPS, it stored and broadcast the geographic coordinates to other devices in its range of emission. Those vehicles receiving this information, which had previously launched the Car Locator application, show the empty parking space on the map.

7. Conclusion

This paper presents an advanced implementation of a tool for deploying VANETs with current devices, called VAiPho. This application encourages the fast development of vehicular networks, which so far have not been possible to implement. It solves the problem of starting and deploying VANETs, involving, at the same time, maximum efficiency policies, information and user security, and minimum cost. Therefore, its development can act as an engine for other innovative projects in ITS.

In order to provide several VANET facilities, VAiPho involves several algorithms and corresponding software that can be run on current devices like smartphones, phablets, or tablets equipped with Wi-Fi Direct and location services. In particular, the main target of VAiPho is the development of both security applications and information services to prevent traffic accidents, enhance traffic management and mobility, improve transport efficiency, and so forth.

According to the experimental analysis, the proposed application can be effectively deployed in urban situations for specific applications using nowadays smartphones. The obtained results show that VAiPho guarantees efficiency and security of communications and is a powerful tool for several VANET applications. This is still a work in progress, so many aspects like the addition of new features and the implementation in other mobile platforms such as iOS and Windows Phone are being now developed.

Acknowledgments

This research was supported by the Spanish MINECO and the FEDER Fund under Projects TIN2011-25452 and IPT-2012-0585-370000.

References

[1] M. Raya and J. P. Hubaux, "The security of VANETs," in *Proceedings of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks (VANET '05)*, pp. 93–94, Cologne, Germany, September 2005.

[2] C. Adler, S. Eichler, T. Kosch, C. Schroth, and M. Strassberger, "Self-organized and context-adaptive information diffusion in vehicular ad hoc networks," in *Proceedings of the 3rd International Symposium on Wireless Communication Systems (ISWCS '06)*, pp. 307–311, Valencia, Spain, September 2006.

[3] S. Panichpapiboon and W. Pattara-Atikom, "Connectivity requirements for a self-organizing vehicular network," in *Proceedings of the IEEE Intelligent Vehicles Symposium*, pp. 968–972, Eindhoven, The Netherlands, June 2008.

[4] L. Wischhof, *Self-organizing communication in vehicular ad hoc networks [Ph.D. thesis]*, University of Hamburg, Hambourg, Germany, 2007.

[5] S. Capkun, L. Buttyán, and J.-P. Hubaux, "Self-organized public-key management for mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 2, no. 1, pp. 52–64, 2003.

[6] H. V. D. Parunak and S. Brueckner, "Stigmergic learning for self-organizing mobile ad-hoc networks (MANET's)," in *Proceedings of the 3rd International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS '04)*, pp. 1324–1325, New York, NY, USA, July 2004.

[7] Y. Park, Y. Park, and S. Moon, "Anonymous cluster-based MANETs with threshold signature," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 374713, 9 pages, 2013.

[8] S. Dornbush and A. Joshi, "StreetSmart traffic: discovering and disseminating automobile congestion using VANET's," in *Proceedings of the IEEE 65th Vehicular Technology Conference Spring (VTC '07)*, pp. 11–15, Dublin, Ireland, April 2007.

[9] L. Buttyán, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in VANETs," in *Security and Privacy in Ad-hoc and Sensor Networks*, Lecture Notes in Computer Science, pp. 129–141, Springer, Berlin, Germany, 2007.

[10] X. Zhu, Y. Lu, B. Zhang, and Z. Hou, "A distributed pseudonym management scheme in VANETs," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 615906, 9 pages, 2013.

[11] Google Maps, Traffic option, http://maps.google.com.

[12] TomTom, http://www.tomtom.com.

[13] Sygic GPS Navigation, http://www.sygic.com.

[14] Waze, http://www.waze.com.

[15] CityPark, Israel, https://play.google.com/store/apps/details?id=com.citypark.

[16] S. Mathur, T. Jin, N. Kasturirangan et al., "ParkNet: drive-by sensing of road-side parking statistics," in *Proceedings of the 8th ACM/USENIX Annual International Conference on Mobile Systems, Applications and Services (MobiSys '10)*, pp. 123–136, San Francisco, Calif, USA, June 2010.

[17] R. Panayappan, J. M. Trivedi, A. Studer, and A. Perrig, "VANET-based approach for parking space availability," in *Proceedings of the 4th ACM International Workshop on Vehicular Ad Hoc Networks (VANET '07)*, pp. 75–76, Montréal, Canada, September 2007.

[18] G.-Y. Chang, J.-P. Sheu, and C.-Y. Chung, "Zooming: a zoom-based approach for parking space availability in VANET," in *Proceedings of the IEEE 71st Vehicular Technology Conference-Spring (VTC '10)*, Taipei, Taiwan, May 2010.

[19] Car Finder, Android, https://play.google.com/store/apps/details?id=com.slickapps.

[20] Car Finder, iPhone, https://itunes.apple.com/es/app/encuentra-tu-coche-conar/id370836023?mt=8.

[21] D. Jiang and L. Delgrossi, "IEEE 802.11p: towards an international standard for wireless access in vehicular environments," in *Proceedings of the IEEE 67th Vehicular Technology Conference-Spring (VTC '08)*, pp. 2036–2040, Singapore, May 2008.

[22] J. Wu and S.-H. Yang, "SmallWorld model-based polylogarithmic routing using mobile nodes," *Journal of Computer Science and Technology*, vol. 23, no. 3, pp. 327–342, 2008.

[23] J. Molina-Gil, P. Caballero-Gil, and C. Caballero-Gil, "Aggregation and probabilistic verification for data authentication in VANETs," *Information Sciences*, 2013.

[24] NS-2, The Network Simulator, http://isi.edu/nsnam/ns.

[25] SUMO, Simulation of Urban MObility, http://sumo.sourceforge.net.

[26] WAVE, "Wireless access in vehicular environments," IEEE 1609 Working Group, http://vii.path.berkeley.edu/1609_wave/.

[27] P. Caballero-Gil, C. Caballero-Gil, and J. Molina-Gil, "VAiPho—VANET application for mobile phones to avoid traffic jams," PCT/ES2011/000220, University of La Laguna, Spain, 2010, http://www.vaipho.com.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 482695, 12 pages
http://dx.doi.org/10.1155/2013/482695

Research Article

An Empirical Study on Ad Hoc Performance of DSRC and Wi-Fi Vehicular Communications

Seungbae Lee and Alvin Lim

Department of Computer Science and Software Engineering, 3101 Shelby Center for Engineering Technology, Auburn University, Auburn, AL 36849-5347, USA

Correspondence should be addressed to Alvin Lim; lim@eng.auburn.edu

Received 12 April 2013; Accepted 26 September 2013

Academic Editor: Shukui Zhang

The primary motivation for developing vehicular safety applications is to provide information and assistance required to avoid collisions. Such applications depend on performance of vehicular communications which have critical requirements for various operating scenarios. However, there is still a lack of practical performance measurement data in the open literature that can be used to design robust and reliable applications for vehicle safety. This paper provides an overview of the current standards for vehicular communications and requirements for vehicular applications and analyzes ad hoc performance of commercial off-the-shelf DSRC and Wi-Fi radios in real vehicular environments. Also, it identifies important effects of messages size, message frequency, weather condition, and vehicle mobility on vehicular communications. For example, rainy weather significantly diminishes the communication range and vehicle mobility causes temporal variations in communication throughput. With a better comprehensive understanding of these effects on performance and reliability, quality of vehicular applications can be significantly improved.

1. Introduction

Dedicated short-range communication (DSRC) is designed to support a variety of applications based on vehicular communications. It is already in trial use and its products are out on the market. As vehicular communications rely on standards to ensure interoperability between vehicular equipments, there have been several international and regional standardization efforts, particularly the United States and Europe. In the US, for example, DSRC adopts IEEE 802.11p standard [1] for wireless access for vehicular environments (WAVE). IEEE 802.11p is based on IEEE 802.11 standard [2] for the physical (PHY) and medium access (MAC) protocol layers [3]. DSRC also employs a suite of IEEE 1609 standards [4–6]: 1609.2 (security services), 1609.3 (network services), and 1609.4 (multichannel operation) for the upper protocol layers. Most of these standards are recently published.

One important reason for the use of IEEE 802.11p, an amendment to the IEEE 802.11 standard, is that it may encourage IEEE 802.11 (Wi-Fi) manufacturers to support DSRC, which would spur rapid penetration of DSRC and efficiently lowering deployment costs. For instance, the majority of the commercial off-the-shelf DSRC radios currently have an embedded IEEE 802.11a Wi-Fi chipset. Since IEEE 802.11p employs the orthogonal frequency-division multiplexing (OFDM) technique for the PHY layer, which is originally adopted by IEEE 802.11a [7], DSRC radios using IEEE 802.11a Wi-Fi chipsets can support IEEE 802.11p to achieve fast and robust connections to moving vehicles by modifying the PHY and MAC layers of the IEEE 802.11 standard. However, DSRC radios are still not expected to penetrate the market with affordable prices until the deployment of DSRC equipment in vehicles is regulated, which will result in a demand for high-volume production.

Many current wireless network deployments are based on Wi-Fi technology that uses IEEE 802.11 standards, specifically 802.11a/b/g/n, to provide a high-speed network connection in wireless environments. The IEEE 802.11 standards were originally developed for extending wireless communication links between indoor local area network (LAN) equipments, but the use of Wi-Fi in outdoor environments has expanded quickly due to its high capacity and reliable coverage. For vehicular communications, the existing and emerging Wi-Fi technologies provide high throughput, predictable range,

and a variety of physical diversity mechanisms, thus ensuring network performance and reliability while lowering deployment costs. For this reason, DSRC radios are already employing Wi-Fi chipsets and IEEE 802.11p standard. Hence, the Wi-Fi technology can be investigated for vehicular networks to provide better usability and interoperability using existing pervasive Wi-Fi-based smart devices and infrastructures.

Vehicular networks have generated considerable research interests, where many researchers have proposed various solutions. However, it is difficult to determine if the solutions can be implemented in practice and if they are really reliable in practical implementation. This difficulty arises because most of prior research was developed and evaluated in typical network simulators based on limited scenarios and physical models including vehicle mobility and channel characteristics [8]. As the costs of real implementation and field experiments are extremely high, extensive measurements in vehicular environments are difficult. Most of the previous field experiments [9, 10] have focused only on measuring channel characteristics due to vehicle mobility in order to develop vehicular simulation models, for example, vehicle-to-vehicle (V2V) propagation channel model.

For vehicular application design, application requirements are derived from implementations that depend on the performance of vehicular communications, particularly DSRC. However, little attention has been paid to the performance of practical communication links in vehicular environments, such as effective single-hop communication range, available bandwidth (or sending rate), data loss, and latency time (or variation of delays). For example, road safety applications, for example, collision avoidance, need to transmit safety messages at 10 Hz, which should be received within a minimum range of 100 ms to track others' movement and take action to prevent potential collisions [11]. As each vehicular application has critical performance requirements, an approach that focuses on how to reliably satisfy the minimum performance requirements is necessary. Although some performance measurements have been reported, most of them are related to channel fading statistics. There still remains a need for pragmatic measurements of performance in real operating environments.

The goal of this study is to investigate the ad hoc performance of the promising technologies, DSRC and its base Wi-Fi standard, for vehicular communications, which can be a critical baseline for vehicular application design. In this work, there are three major discoveries from our experiments, which are the main contributions of this paper.

(1) We report performance measurements of ad hoc links using off-the-shelf DSRC and Wi-Fi radios at adjacent 5.860 GHz (DSRC) and 5.825 GHz (Wi-Fi) in real vehicular environments including a parking lot, test track, and highway. Our results show that performance of User Datagram Protocol (UDP) and broadcast, two most popular transport layer protocols in vehicular applications, is significantly affected by the size and rate of transmitting messages, which has an important impact on bandwidth efficiency in safety application design.

(2) We conducted field experiments under both sunny and rainy weather conditions to examine the effects of weather changes. Prior work provides just good results in clear weather conditions, many of which are based on nonrepresentative and nonreproducible measurements, but we present measurements showing that rainy weather substantially diminishes the radio communication coverage. The performance degradation from the varying weather condition has an important impact on reliability of vehicular safety applications.

(3) Our measurements indicate that ad hoc performance within desired communication coverage areas is quite stable even if the communicating vehicles are moving, whereas the performance shows a significant drop in throughput and substantial increase in data loss at longer ranges or varying distances. This suggests that the use of half channel bandwidth (10 MHz) has advantages (e.g., sustainability with channel fading and interference) and disadvantages (e.g., small communication capability) in performance and reliability.

The rest of this paper is organized as follows. We first introduce the background and work related to our study in Section 2. We then describe the details of our experimental setup including hardware setting, network configuration, and performance measurement procedures in Section 3. Then, we present and discuss our experimental results in Section 4 and conclude our investigation in Section 5.

2. Background and Related Work

In this section, we give an introduction to existing and emerging standards for vehicular communications and performance requirements for vehicular safety applications. Also, we present an overview of critical characteristics of vehicular communication environments.

2.1. Standardization of Vehicular Communications. Vehicular communications rely fundamentally on standards to ensure interoperability among devices from different manufactures, which is also crucial for cost-efficient deployment. Kenney [3] and Ström [12] introduce in detail the current standardization efforts primarily conducted by the United States and Europe. Most of vehicle communication standards are recently published.

In the US, DSRC uses IEEE 802.11p [1] for wireless access for vehicular environments (WAVE) based on IEEE 802.11 standard at the PHY and MAC layers. In upper protocol layers, DSRC utilizes a suite of IEEE 1609 standards: 1609.2 [4] for security service, 1609.3 [5] for network services, and 1609.4 [6] for multichannel operation. DSRC also supports prevalent Internet Protocols for the network and transport layer, such as Internet Protocol version 6 (IPv6), User Datagram Protocol (UDP), and Transmission Control Protocol (TCP). IEEE 1609.3 defines the bandwidth-efficient WAVE Short Message Protocol (WSMP) for vehicular safety messages. In cooperation with IEEE 1609 standards, the Society of Automotive Engineers (SAE) International has

Table 1: Major parameters of the OFDM PHY layer.

Parameters	IEEE 802.11p (DSRC)	IEEE 802.11a (Wi-Fi)
USA frequency	5.850–5.925 GHz	5.180–5.825 GHz
Channel spacing	10 MHz	20 MHz
Data rate (Mbps)	3, 4.5, 6, 9, 12, 18, 24, 27	6, 9, 12, 18, 24, 36, 48, 54
Subcarriers	52	
Modulation	BPSK, QPSK, 16-QAM, 64-QAM	
FEC rate	1/2, 2/3, 3/4	
Subcarrier spacing	0.15625 MHz	0.3125 MHz
Guard interval	1.6 μs	0.8 μs
Symbol interval	8 μs	4 μs

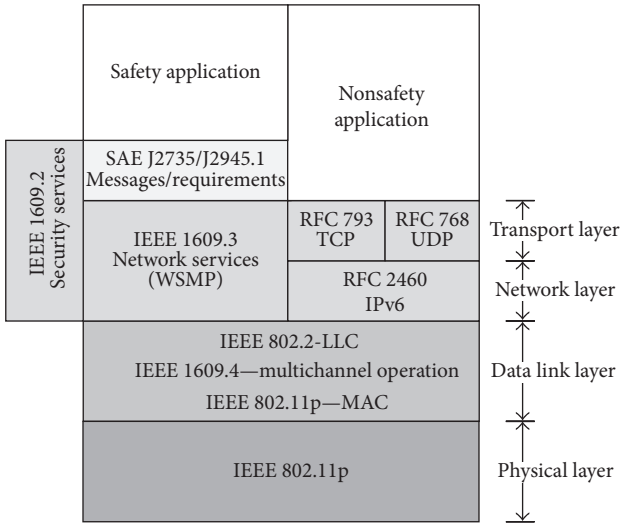


Figure 1: Protocol stack for vehicular communications.

been standardizing SAE J2735 [11] for Message Set Dictionary used by the WSMP and SAE J2945.1 draft [13] for minimum performance requirements. Figure 1 illustrates the protocol stack for vehicular communications in the US.

In Europe, the European Telecommunications Standard Institution (ETSI) and European Committee for Standardization (CEN) have been developing the European Intelligent Transport System (ITS) architecture. The European standards are generally different from those of the US, mainly in higher network layers. For example, European DSRC radios simultaneously listen to two separate channels, the control and service channel, for traffic safety applications, whereas US DSRC radios utilize only one channel, the control or service channel, with time-division based channel switching operation as defined in IEEE 1609.4. However, both sides are adopting IEEE 802.11p as physical and MAC layer protocols, which probably allows cost-efficient high-volume production and compatible standardization.

IEEE 802.11p, which is the foundation of standardized vehicular communications (DSRC), is an amendment to the IEEE 802.11 standard [2] that employs Orthogonal Frequency Division Multiplexing (OFDM) in the PHY layer and a Quality-Of-Service (QoS) extension in the MAC layer. OFDM was originally added to the IEEE 802.11a amendment [7]. IEEE 802.11p is designed to provide the minimum set of specifications required to ensure interoperability between wireless devices attempting to communicate in potentially rapidly changing communication environments where transactions must be completed in much shorter time frames compared to ad hoc and infrastructure IEEE 802.11 networks. Hence, IEEE 802.11p describes the functions and services to operate in a rapidly varying environment and to exchange messages without joining a Basic Service Set (BSS), and defines the signaling techniques and interface functions controlled by the IEEE 802.11 MAC.

The main variation of IEEE 802.11p from the IEEE 802.11 standard (specifically referred to as 802.11a when focusing on the OFDM technique in the 5 GHz band as Wi-Fi still uses this term to group its products) is the half-clocked OFDM PHY operation using 10 MHz channel spacing; OFDM is widely adopted by recent wireless technologies (e.g., WiMAX and LTE). The half clock operation has data payload communication capabilities of 3, 4.5, 6, 9, 12, 18, 24, and 27 Mbps, using 52 subcarriers that are modulated by BPSK, QPSK, and 16-QAM with Forward Error Correction (FEC) coding rate of 1/2, 2/3, or 3/4. Compared to the OFDM operation with 20 MHz channel spacing, this operation doubles symbol times and clear channel assessment (CCA) times and increases the length of the guard interval (GI) to guard against longer delay spreads. It also halves the subcarrier spacing, which allows for greater frequency selectivity. Utilizing the OFDM technique of IEEE 802.11 standard allows IEEE 802.11 manufacturers to easily support the IEEE 802.11p amendment, which would result in the rapid penetration of vehicular radios with reasonable deployment costs. Table 1 lists the major parameters of the OFDM PHY layer in the IEEE 802.11 standard.

2.2. Requirements for Vehicular Applications. Geographic standardization for vehicular applications, which reflects regional regulatory constraints and emphasizes the distinct characteristics of operating environments, makes interoperability difficult. Karagiannis et al. [14] give a good introduction to vehicular applications and their requirements in the US, Europe, and Japan, summarizing the current and past major ITS projects in those countries. To provide a brief overview, this section focuses on the requirements of

vehicular applications, based on the WAVE Short Message Protocol (WSMP) of IEEE 1609.3 and Basic Safety Message (BSM) of SAE J2735 in the US.

At the top of the IEEE 802.11p and IEEE 1609 protocol suite as illustrated in Figure 1, the SAE J2735 specifies a set of message formats that support a variety of vehicular applications. The most critical of these is the BSM that is used in multiple safety applications: Emergency Electronic Brake Lights (or Intelligent Brake Light Warning), Blind Spot Warning, Cooperative Adaptive Cruise Control, Cooperative Collision Warning, Cooperative Forward Collision Warning, Emergency Vehicle at Scene Warning, Lane Change Warning, Precrash Sensing, and so forth. In order to detect potential danger and take appropriate actions, the BSM provides situational awareness that includes the position, speed, and heading of all vehicles within range.

For instance, the Emergency Electronic Brake Lights (EEBL) application exchanges messages with other vehicles using the frequent BSMs that enable each vehicle to keep track of nearby vehicles and automatically apply brakes to prevent a collision between vehicles. As defined in the SAE J2735 standard, each moving vehicle updates and broadcasts its own BSM one way (i.e., message direction requirement) every 100 ms (i.e., message rate requirement) over the WSMP (i.e., priority requirement). Other nearby vehicles within a minimum range of 100 m (i.e., communication range requirement) detect this broadcast and process it. There is no handshaking or acknowledgment between the devices; there is no association or join process (i.e., priority requirement).

Although the SAE J2735 standard defines extensible messages sets including basic safety message, roadside alert message, and probe vehicle message for future vehicular applications, it is not sufficient to embrace all system capability requirements derived from a wide range of the use cases. Hence, emerging SAE J2945.1 standard is a work in progress to specify the minimum communication performance requirements of the DSRC message sets, associated data frames, and data elements defined in the SAE J2735 standard. SAE J2945.1 is expected to address optimal data rate, transmission power, data accuracy, security, QoS, and other specific performance requirements.

2.3. Characteristics of Vehicular Communications. Several measurement studies in typical vehicular environments have already been carried out by different researchers, for example, Cheng and Henty [9] and Alexander et al. [10], focusing on characterizing the 5.9 GHz DSRC channel in terms of path loss, fading, and propagation patterns. There have also been significant efforts towards developing statistical channel models for realistic simulations. Recent well-written reviews can be found in Molisch et al. [15] and Mecklenbraüker et al.'s work [16]. The characteristics of vehicular communications significantly differ from those of other mobile communications. These differences arise from the following specific features of vehicular environments.

(i) In vehicular communications, the transmitter and receiver are mostly at the same height as the vehicles; for example, the height of most mid-size vehicles is 4 to 5 ft. Consequently, the propagation patterns are different from other mobile wireless links, where radios are placed high above the road level. The radio propagation of vehicular links is largely affected by horizontal obstacles at the same level, especially other obstructing vehicles such as trucks.

(ii) Vehicular radios operate at high frequency (5.9 GHz band) which has high signal attenuation (or path loss). Moreover, channel fading is faster than any other mobile communications because both the transmitter and receiver are simultaneously moving in most cases. Therefore, the maximal range for effective communications is much shorter and communication performance is usually degraded with a large variation over a short period of time.

(iii) The propagation patterns in vehicular communications are significantly affected by vehicle geometry and antenna placement. A transmitter does not provide uniform coverage in a circular pattern, which actually creates coverage in intricate 3D patterns. Although rooftop mounting is intuitively considered as the best placement for vehicular antennas, there is still a need to empirically investigate the impact of vehicular antenna mounting on communication performance.

(iv) Vehicular radios operate at a high frequency under various weather conditions, where signal attenuation easily occurs as a result of absorption and scattering by such hydrometeors as rain, snow, cloud, and fog [17, 18]. In particular, wet snow may cause significant attenuation. Since examining the weather effects on the propagation and path loss in vehicular environments requires high expenses in cost and time, very few measurement experiments have been conducted to study weather-related effects on vehicular communications.

Although there have been standardization and characterization efforts to analyze vehicular communications as introduced in this section, there is still a lack of practical measurement data required for developing vehicular applications in the open literature. It should include communication performance between vehicles in real operating environments. Motivated by this fact, we carried out extensive measurements to gain a better understanding of the limitations and requirements for vehicular communications by comparing communication performance of DSRC and its base, Wi-Fi radios.

3. Experimental Setup

In our field experiments, we measured single-hop ad hoc performance of vehicular communications using two commercial off-the-shelf DSRC and small form-factor Wi-Fi platforms. The measurements were performed using two mid-size vehicles equipped with both DSRC and Wi-Fi platforms in typical vehicular environments.

Table 2: Experimental conditions of measurement sets.

Conditions	Set I	Set II		Set III		Set IV	Set V
Place	Laboratory	Parking lot	Parking lot	Parking lot	Parking lot	Test track	Highway
Weather	N/A	Sunny	Rainy	Sunny	Rainy	Sunny	Sunny
Temperature	N/A	85°F	65°F	70°F	65°F	68°F	70°F
Humidity	N/A	50%	90%	70%	83%	31%	70%
Pressure	N/A	29.94 in	29.85 in	30.28 in	30.26 in	30.11 in	30.28 in
Wind speed	N/A	4 mph	10 mph	5 mph	6 mph	10 mph	5 mph

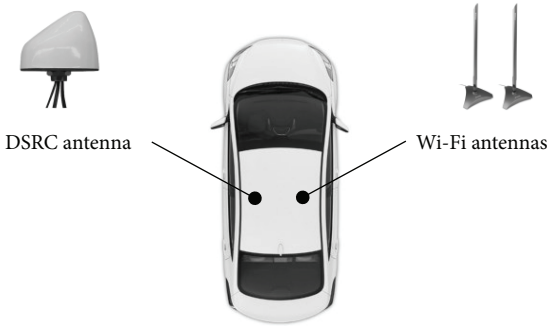


Figure 2: Antenna placement for experimental platforms.

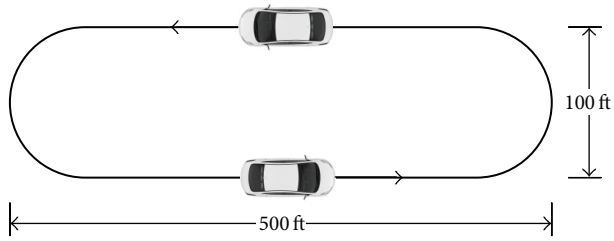


Figure 3: Test track and vehicle movement.

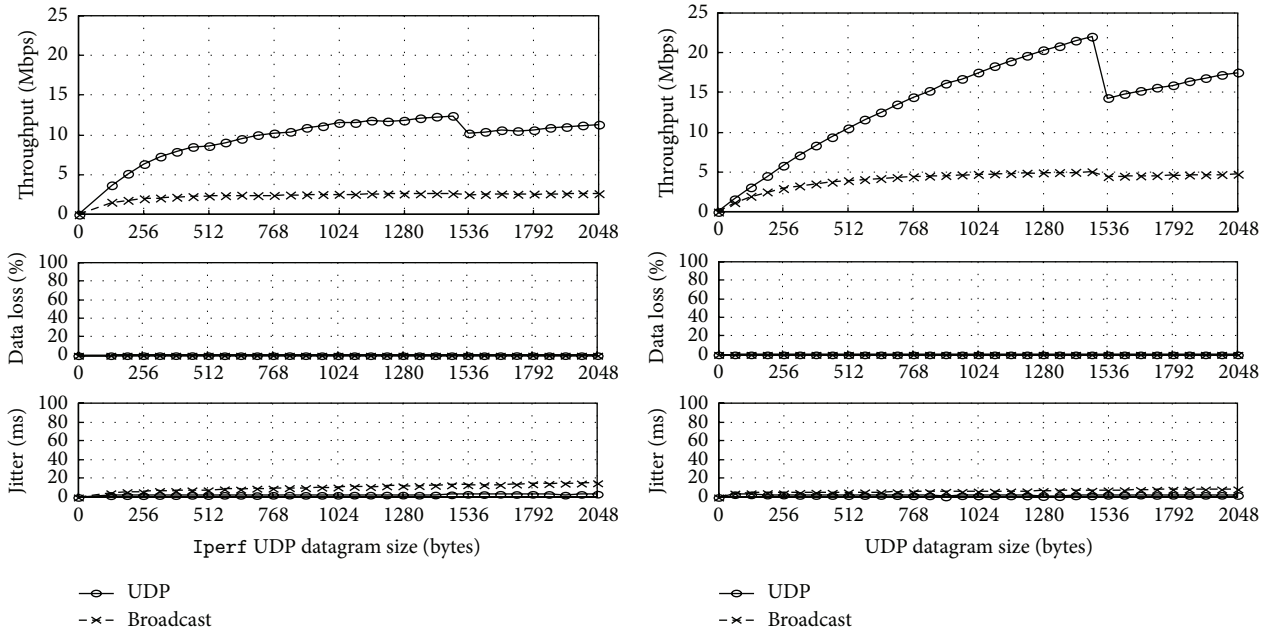
The DSRC platform (MCNU R1500S) developed by Kapsch is compliant with the US 5.9 GHz DSRC standards such as IEEE 802.11p and IEEE 1609.2-4; in our experiments, only IEEE 802.11p was employed for the basic ad hoc configuration. The platform running Linux kernel 2.6.14 is equipped with an Atheros IEEE 802.11a chipset controlled by `MadWifi` Linux driver [19]. A 4 dB rugged vehicle MIMO antenna that provides omnidirectional coverage was selected and magnetically mounted on the roof of each vehicle; see Figure 2. The transmission power was set to 18 dBm and the operating frequency was set to 5.860 GHz that is the lowest DSRC frequency, channel 172.

The Wi-Fi platform (MS-9A19) manufactured by MSI is a compact industrial system providing a mini-PCIe interface for the wireless adapter, which is suitable for vehicular use. An Atheros IEEE 802.11a/b/g/n chipset-based wireless adapter (Ubiquiti SR71-E) was used with two 7 dB omni-directional dipole antennas, which were mounted on the roof of each vehicle; see Figure 2. The transmission power is varied with the data rate (15–25 dBm). The platform runs Linux kernel 2.6.38 with the `compat-wireless` Linux wireless package [20] for the wireless adapter operation. For ad hoc configuration, we chose the highest channel 165 at 5.825 GHz that is the closest to the DSRC band and probably has very similar characteristics to DSRC frequencies.

Each set of DSRC and Wi-Fi experimental platforms was installed on the two mid-size vehicles; that is, each vehicle is equipped with both DSRC and Wi-Fi platforms, powered by the vehicle batteries. One in each set was configured as a transmitter and the other as a receiver. To investigate communication performance, we utilized `Iperf` [21], a commonly used network performance measurement tool, to generate UDP and broadcast traffic. We developed scripts to control continuous `Iperf` test runs and collect performance measurements (e.g., throughput, data loss, and jitter) by configuring the `Iperf` test parameters according to each experimental scenario. The script also collected wireless link statistics (e.g., data rate, received signal level, retransmission, and transmission failure) from the Linux wireless driver. We recorded link statistics only using the Wi-Fi platform that provided more accurate and reliable data.

We carried out UDP and broadcast performance tests because they are the most common transport layer protocols in vehicular communications. These tests provide measurements that are suitable for evaluating communication performance including efficient single-hop communication range, available bandwidth (or data rate), data loss, and latency (or variation of delays). As the performance of a wireless link is usually affected by the surrounding channel conditions, the experimental results may exhibit variations. To eliminate this effect, we first measured the communication performance at 100 ft range with an unobstructed line-of-sight before each experiment and conducted our experiments only when all measurements reported negligible differences.

The vehicular ad hoc communications were evaluated in three different environments: open parking lot, test track, and highway. The parking lot with no interfering obstacle and people was used to explore the variation of performance at different communication ranges in different weather conditions. The test track, which is an oval-shaped track 1200 ft long, was selected to examine the change of performance due to vehicle maneuvers; see Figure 3. Finally, one of the major interstate highways in the US, I-85, was chosen to observe the communication performance at high speed in a practical traffic condition. Details of the experimental parameters, including experiment place and weather condition (e.g., temperature, humidity pressure, and wind speed), are summarized in Table 2.



(a) DSRC performance

(b) Wi-Fi performance

Figure 4: Measurement set I: laboratory.

4. Experimental Results

This section presents our experimental measurements of ad hoc communication performance of DSRC and Wi-Fi radios in real operating environments and discusses practical considerations for designing and implementing vehicular applications based on the experimental observations.

4.1. Baseline Measurements of DSRC and Wi-Fi Performance. We performed preliminary experiments in our indoor laboratory with the experimental setup to present baseline measurements. These experiments are also intended to verify how the payload size (i.e., message length) affects the communication performance and what the maximum achievable performance (i.e., message rate) is. We measured the UDP and broadcast performance of each set of DSRC and Wi-Fi ad hoc links at 10 ft range, repeatedly running `Iperf` tests and gradually increasing the datagram size at intervals of 64 bytes every 10 seconds. Two experiments using DSRC and Wi-Fi radios are separately conducted.

Figure 4 shows results of the DSRC and Wi-Fi experiment. The maximum UDP throughput of 12.4 Mbps for DSRC and 22.0 Mbps for Wi-Fi was achieved with the datagram size of 1472 bytes. The maximum broadcast throughput of 2.5 Mbps for DSRC and 5.1 Mbps for Wi-Fi was relatively lower compared with the UDP throughput. The best datagram size of 1472 bytes was used in all the following experiments. According to our expectations, the Wi-Fi communication performs much better in this stationary configuration due to the use of full channel spacing (20 MHz). No data loss and a little variance of delay were observed during the experiments.

As we can see from the measurements for DSRC and Wi-Fi in the preliminary experiment, packet size (i.e., message length) is a significant performance factor, which means that frequent short-message transmission may degrade overall performance of vehicular communication, especially when using UDP protocol. In the case of broadcast, moreover, the transmitter is not able to determine successful reception and retransmit unsuccessful packets due to the lack of acknowledgments for broadcast packets, which leads to network collisions and degradation in performance and reliability.

The design of vehicular applications has raised two key questions: (1) what is the most efficient message size? (2) how often should messages be sent? It is generally accepted that large messages increase processing overheads for modulation and coding, and frequent small messages easily saturate the radio channel. Thus, the sizes and sending rates (i.e., frequency) of messages for critical vehicular safety applications need to be carefully determined based on accurate measurements in specific operating environments to efficiently provide safety information in a timely manner.

4.2. Performance Comparison in Different Weather Conditions. To investigate how the performance of vehicular links varies over the communication range in vehicular environments, we conducted our experiments using two vehicles equipped with our experimental platforms in the parking lot; see sets II and III in Table 2 for details. We measured the UDP performance of each DSRC and Wi-Fi ad hoc communication link between the stationary vehicles at ranges of 150, 300, 450, and 750 ft in two different weather conditions, continuously running `Iperf` tests and gradually increasing the test bandwidth at intervals of 1 Mbps every 10

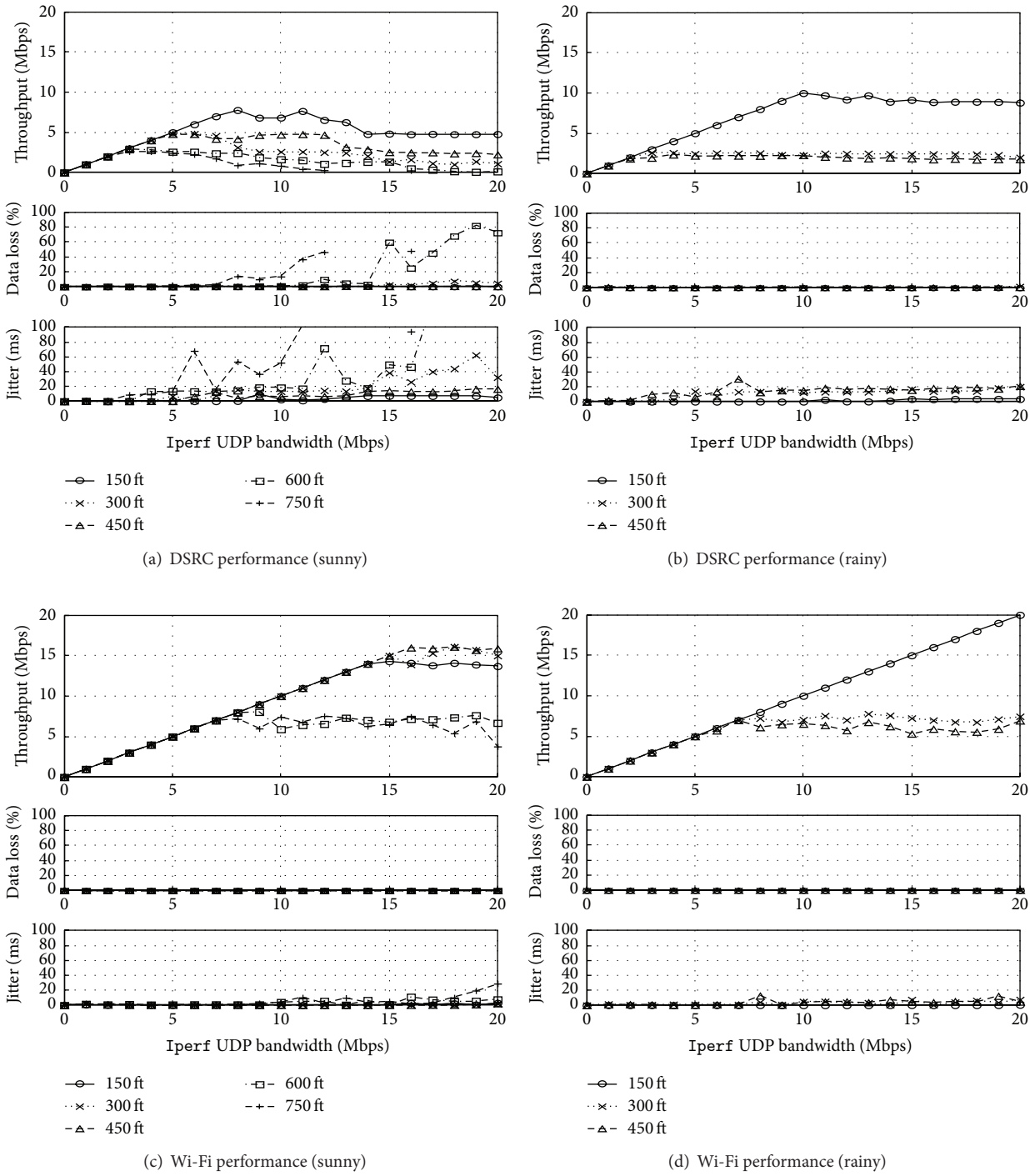
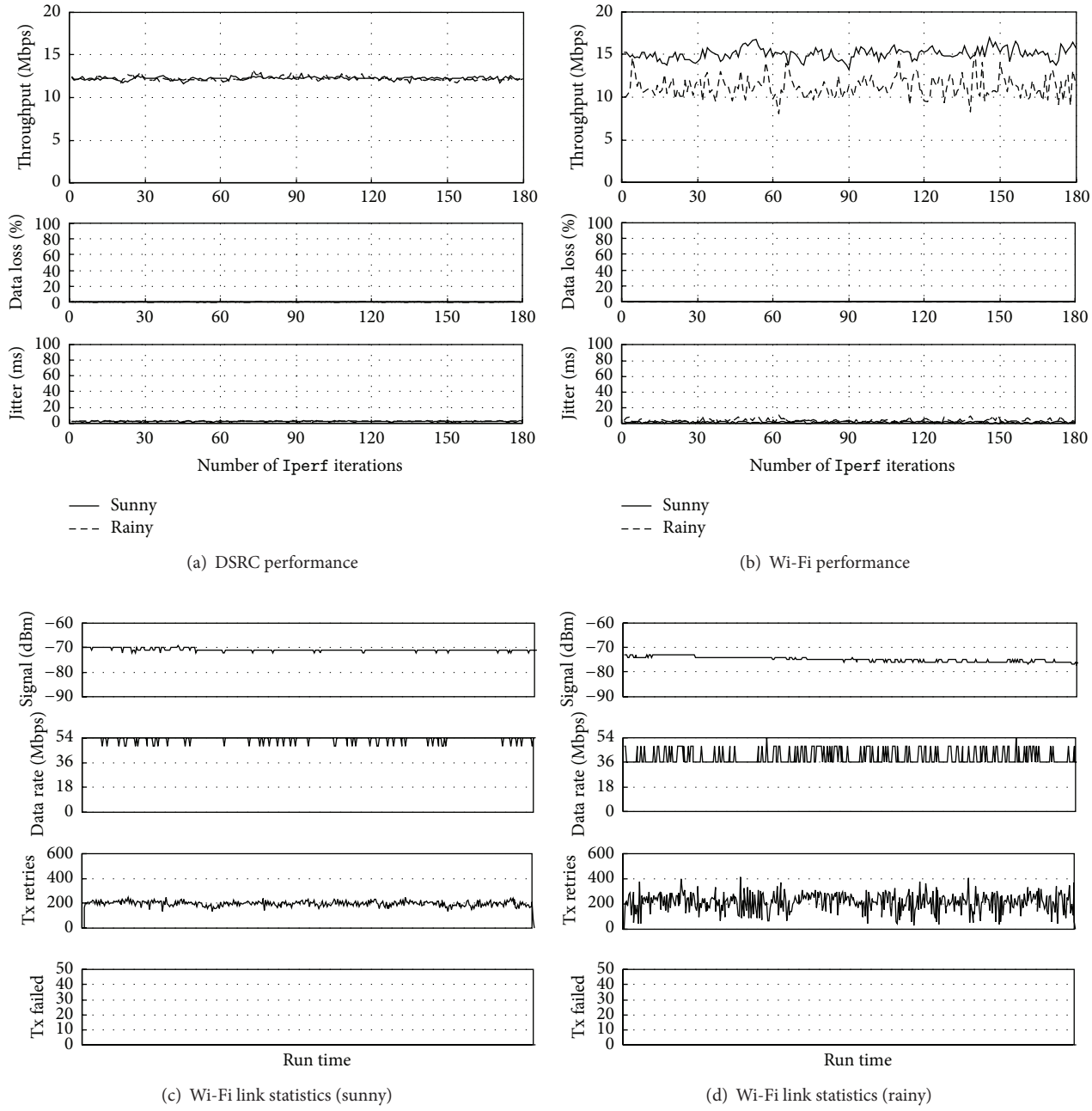


Figure 5: Measurement set II: parking lot.

seconds. We conducted the measurements at the maximum range of 750 ft because our DSRC platforms maintain reliable connection only within the distance even in good weather conditions.

Figure 5 displays two sets of DSRC and Wi-Fi measurements in typical weather conditions, sunny and rainy weather. The performance degrades as the communication range increases in both DSRC and Wi-Fi case, probably due to distance-dependant path loss. Compared to the preliminary measurements, the maximum achievable performance diminished greatly and the overall outdoor performance was not stable over the whole distance; especially, DSRC measurements at longer ranges (e.g., 600 and 750 ft) contain considerable data loss and jitter that may be caused by unreliable connectivity with small channel capacity. In addition, the rainy weather substantially reduces the effective



(a) DSRC performance

(b) Wi-Fi performance

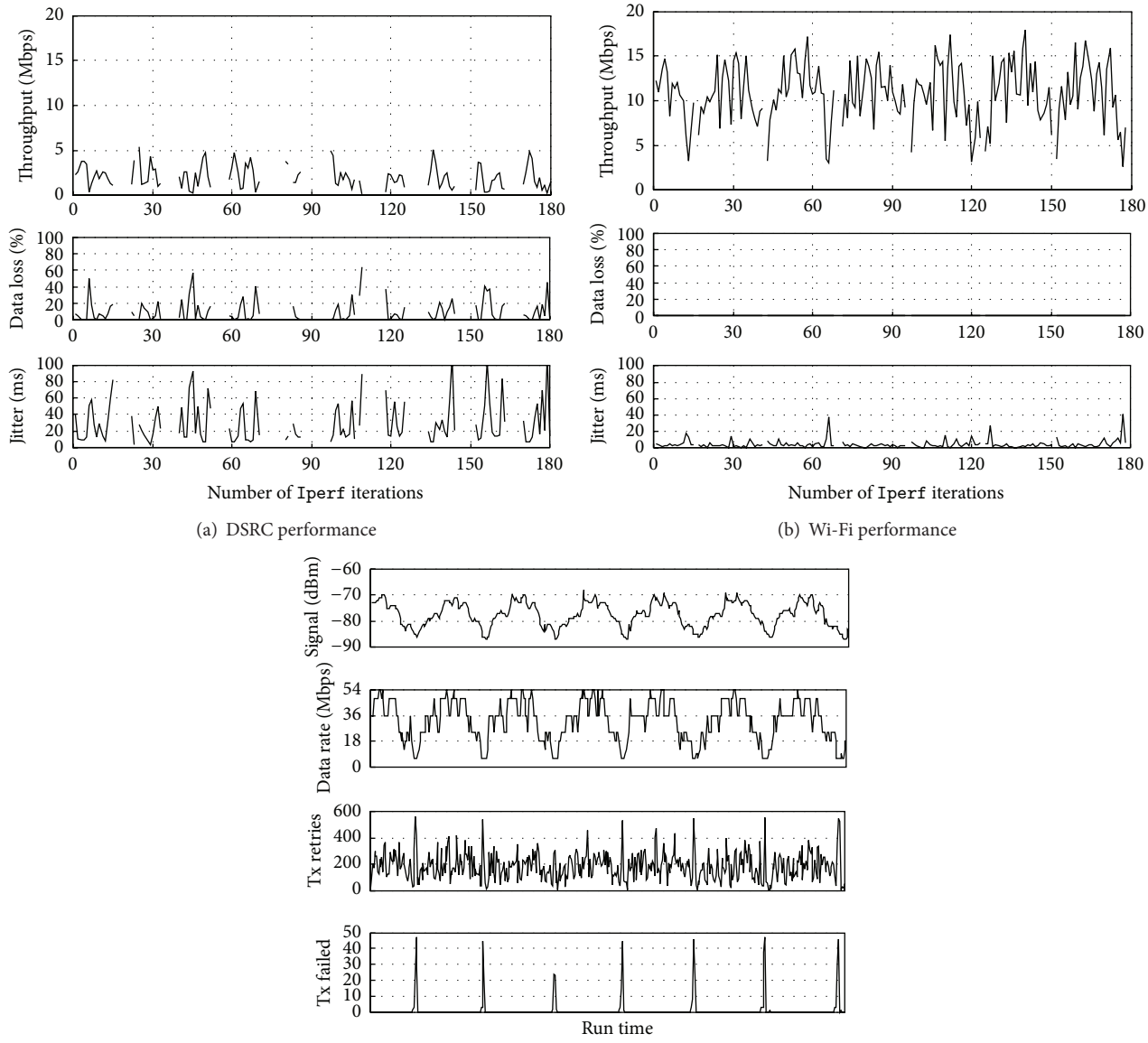
(c) Wi-Fi link statistics (sunny)

(d) Wi-Fi link statistics (rainy)

Figure 6: Measurement set III: parking lot.

communication range because signal attenuation at high frequencies easily occurs in rainy weather as described in the previous section. An interesting effect was observed at the range of 150 ft in rainy weather, where the performance was much better compared with the measurements in sunny weather. It could be speculated that rain also attenuated interfering signals, which led to clear channel at the short range. We also measured broadcast performance with the same experimental setup in all field experiments observing similar patterns to UDP performance, but those measurements are not presented in this paper for lack of space.

Figure 6 contains another set of measurements at range of 150 ft in different weather conditions. In this experiment, to examine temporal variations in communication performance, we measured the UDP performance by continuously transmitting as many datagrams as possible and recording the measurements per second; this `Iperf` test setup was used in the following experiments. The measurements indicate that the DSRC communication at a desired distance is quite stable in comparison with the Wi-Fi performance in both sunny and rainy weather because the Wi-Fi with 20 MHz channel bandwidth has more noise and interference for a given



(a) DSRC performance

(b) Wi-Fi performance

(c) Wi-Fi link statistics

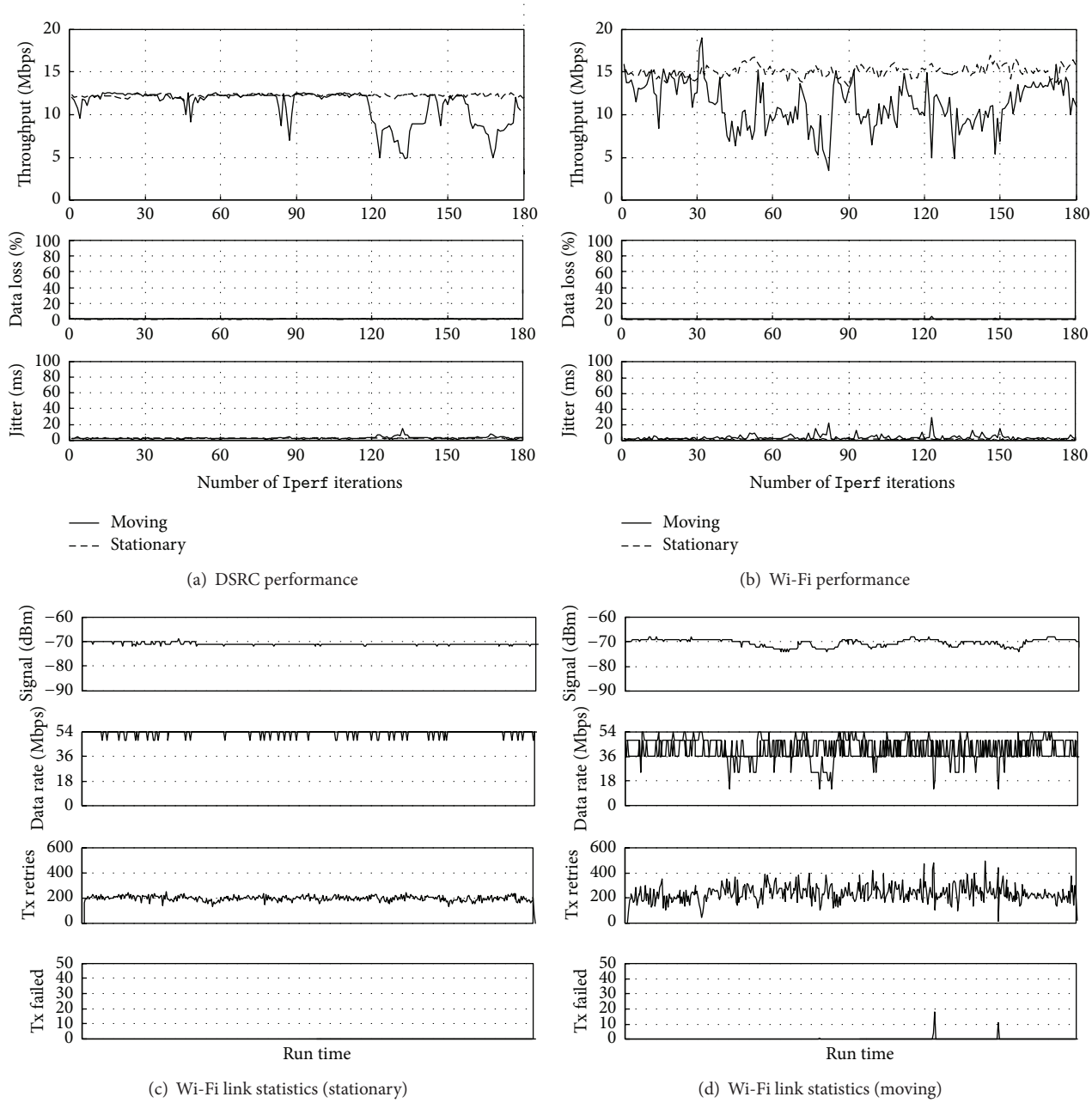
Figure 7: Measurement set IV: test track.

background spectral density. Figure 6 also includes the Wi-Fi link statistics that demonstrate how the Wi-Fi protocol reacted to the environmental change.

Although a quantitative comparison between DSRC and Wi-Fi could not be made due to the differences in transmission power and antenna pattern, we were able to get some measurements that illustrate how DSRC and Wi-Fi behave within the communication range under different weather conditions. Unfortunately, very few measurement studies that account for weather-related effects on vehicular communications, for example, propagation and path loss, have been conducted in any prior work. Thus, we believe that additional measurement studies on various weather conditions including severe weather such as storms are needed in order to design robust and reliable applications for dynamic vehicular environments.

4.3. Performance Comparison in Vehicle Mobility. We carried out our road experiments on the test track and highway to examine how the DSRC and Wi-Fi ad hoc performance between the two vehicles is affected by the vehicle maneuver and movement in sunny weather; see sets IV and V in Table 2 for the detail of experimental condition.

For the measurements on the test track, two vehicles on the opposite sides of the track started to move at the same time and went around the track continuously while keeping the speed of 10 mph with an unobstructed line-of-sight as illustrated in Figure 3. One vehicle was configured as a transmitter and the other as a receiver. We ran the `Iperf` UDP tests with the same parameters as previous tests to accurately measure temporal variations on throughput, data loss, and jitter. During the tests, we also collected wireless link statistics such as received signal level, transmission



(a) DSRC performance

(b) Wi-Fi performance

(c) Wi-Fi link statistics (stationary)

(d) Wi-Fi link statistics (moving)

Figure 8: Measurement set V: highway.

rate, retransmission, and transmission failure on the Wi-Fi platforms.

Figure 7 presents our measurements on the test track. The results of both DSRC and Wi-Fi communication link show wide fluctuations in performance. The communication range varied from 100 ft to 500 ft in a regular pattern that corresponds to the track shape and vehicle mobility, which made signal strength (quality) oscillate as illustrated in Figure 7(c). Apparently, the change of signal strength influenced the variations on performance and link statistics with similar pattern. Furthermore, the DSRC ad hoc link was frequently disconnected when DSRC antennas of the transmitter and receiver were facing each other horizontally. We experimentally found that our vehicular antennas for DSRC platforms do not have a uniform circular coverage; that is, there are horizontal blind spots. Thus, antenna pattern in vehicular communications has a major impact on reliability.

In the experiments on the highway, two vehicles moved at a speed of 60 mph while maintaining a distance of 150 ft between the vehicles with an unobstructed line-of-sight. The leading vehicle was configured as a receiver and the follower as a transmitter. We also measured the performance using `Iperf` and collected link statistics provided by the Linux wireless drivers. Before each road test, a stationary test was

conducted on the parking lot with the same distance for the purpose of comparative analysis.

Figure 8 provides performance measurements with link statistics on the highway. By and large, the Wi-Fi result was unstable compared to the DSRC performance. This indicates that Wi-Fi protocols are more sensitive to the operating channel condition due to use of the wider channel bandwidth, and the rate adaptation algorithm, `Minstrel` [22], for the Wi-Fi radio does not properly adapt to the fast varying channel, which result in the overall unreliable performance; see Figures 8(b) and 8(d). Although the DSRC radio employed a similar type of rate adaptation algorithm, `SampleRate` [23], that selects a higher or lower rate unsophisticatedly based just on the probability of packet reception or loss, DSRC reported small variations on performance due to the small gaps between adjacent rates as listed in Table 1. During the experiments, we also found that large trucks passing right by our experimental vehicles caused transient drops in performance, which can be observed evidently in the DSRC results; see Figure 8(a).

As observed in the field experiments, the temporal variations on communication performance arising from dynamic vehicle maneuver and movement in practical environments may have a significant impact on the reliability of critical vehicular applications.

5. Conclusion

As vehicular communications rely on standards to ensure interoperability between vehicular equipment, there have been great efforts for international and regional standardization. In the US, DSRC utilizes a combination of standards: IEEE 802.11p (an amendment to the IEEE 802.11 standard) for PHY and MAC protocol layer, a suite of IEEE 1609.x standards for upper protocol layers, and the SAE J2735, J2945-1 standards for vehicular application. Although there are several measurement studies in typical vehicular environments to characterize the 5.9 GHz DSRC channel, there is still a lack of practical measurements necessary for designing robust and reliable applications for dynamic vehicular environments.

For the purpose of providing practical measurements for developing vehicular applications, this paper first discussed the characteristics of vehicular communications and then reported ad hoc performance measurements with commercial off-the-shelf DSRC and Wi-Fi radios in real operating configurations. The experimental results indicate the effects of messages size, message frequency, weather condition, vehicle maneuver, and vehicle movement on communication performance in vehicular environments. As reported, (1) performance of two most popular transport layer protocols, UDP and broadcast, is significantly affected by the size and rate of transmitting data (e.g., the UDP goodput of 12.4 Mbps for DSRC was achieved with the data size of 1472 bytes), (2) signal attenuation (i.e., performance degradation) often occurs in rainy weather as vehicular radios operate at a high frequency under various weather conditions (e.g., the maximum communication range of DSRC was shortened from 750 to 450 ft), and (3) ad hoc performance within desired communication coverage is quite stable, whereas the performance shows a significant drop in throughput and substantial increase in data loss at longer ranges or varying distances (e.g., the difference between the maximum and minimum throughput of DSRC increased up to 8 Mbps).

Since having a better comprehensive understanding of these effects on performance and reliability enables improvements in development quality of vehicular applications, it is clear that continuous measurement studies in realistic application-specific scenarios are still required to provide the accurate foundation for robust, efficient, and practical vehicular applications.

References

[1] "IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Amendment 6: Wireless Access in Vehicular Environments," *IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009)*, pp. 1–51, 15 2010.

[2] "IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007)*, pp. 1–2793, 2012.

[3] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011.

[4] "IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages," *IEEE Std 1609.2-2013 (Revision of IEEE Std 1609.2-2006)*, pp. 1–289, 2013.

[5] "IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services," *IEEE Std 1609.3-2010 (Revision of IEEE Std 1609.3-2007)*, pp. 1 –144, 2010.

[6] "IEEE Standard for Wireless Access in Vehicular Environments (WAVE)–Multi-channel Operation," *IEEE Std 1609.4-2010 (Revision of IEEE Std 1609.4-2006)*, pp. 1 –89, 2011.

[7] "Supplement to IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements. Part 11: Wireless INTERNATIONAL JOURNAL OF DISTRIBUTED SENSOR NETWORKS, VOL. 0, NO. 0, SEPTEMBER 2013 10 LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-Speed Physical Layer in the 5 GHz Band," *IEEE Std 802.11a-1999*, 1999.

[8] S. Lee and A. Lim, "Reliability and performance of IEEE 802.11n for vehicle networks with multiple nodes," in *Proceedings of International Conference on Computing, Networking and Communications (ICNC '12)*, pp. 252–256, February 2012.

[9] L. Cheng, B. E. Henty, D. D. Stancil, F. Bai, and P. Mudalige, "Mobile vehicle-to-vehicle narrow-band channel measurement and characterization of the 5.9 GHz dedicated short range communication (DSRC) frequency band," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1501–1516, 2007.

[10] P. Alexander, D. Haley, and A. Grant, "Cooperative intelligent transport systems: 5.9-GHz field trials," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1213–1235, 2011.

[11] "Dedicated Short Range Communications (DSRC) Message Set Dictionary," *SAE Std J2735, SAE International, DSRC committee*, 2009.

[12] E. G. Ström, "On medium access and physical layer standards for cooperative intelligent transport systems in Europe," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1183–1188, 2011.

[13] "Dedicated Short Range Communication (DSRC) Minimum Performance Requirements," *SAE Draft Std J2945.1, SAE International, DSRC committee, 2010*.

[14] G. Karagiannis, O. Altintas, E. Ekici et al., "Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Communications Surveys and Tutorials*, vol. 13, no. 4, pp. 584–616, 2011.

[15] A. F. Molisch, F. Tufvesson, J. Karedal, and C. F. Mecklenbräuker, "A survey on vehicle-to-vehicle propagation channels," *IEEE Wireless Communications*, vol. 16, no. 6, pp. 12–22, 2009.

[16] C. F. Mecklenbraüker, A. F. Molisch, J. Karedal et al., "Vehicular channel characterization and its implications for wireless system design and performance," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1189–1212, 2011.

[17] "Propagation data and prediction methods required for the design of terrestrial line-of-sight systems," *ITU-R P.530-13, International Telecommunication Union, Radiocommunication Sector*, 2009.

[18] "Attenuation due to clouds and fog," *ITU-R P.840-4, International Telecommunication Union, Radiocommunication Sector*, 2009.

[19] "MadWifi project," http://madwifi-project.org/.

[20] "Compat-wireless Linux wireless drivers," http://linuxwireless.org/en/users/Download.

[21] "Iperf project," http://iperf.sourceforge.net/.

[22] "Minstrel rate control algorithm for mac80211," http://linuxwireless.org/en/developers/Documentation/mac80211/RateControl/minstrel/.

[23] "Bit-rate Selection Algorithms," http://madwifi-project.org/wiki/UserDocs/RateControl/.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 145254, 8 pages
http://dx.doi.org/10.1155/2013/145254

Research Article

A Cross-Layer Design Combining of AMC with HARQ for DSRC Systems

Gao Yuan Zhang,[1] Li Min Sun,[2] Hong Wen,[1] Bin Wu,[3] Xiping Zhu,[1] and Liang Zhou[1]

[1] *National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu 610054, China*
[2] *Institute of Software, Chinese Academy of Sciences, Beijing 100190, China*
[3] *School of Computer Science and Technology, Tianjin University, Tianjin 300072, China*

Correspondence should be addressed to Hong Wen; wcdma_2000@hotmail.com

Received 12 April 2013; Accepted 30 September 2013

Academic Editor: Liusheng Huang

A new cross-layer design combining adaptive modulation and coding (AMC) with Hybrid Automatic Repeat Qequest (HARQ) based on rate-compatible LDPC codes is proposed for IEEE Std. 802.11p in DSRC systems. Instead of considering AMC at the physical layer and ARQ at the data link layer separately, we propose a cross-layer design that combines these two layers judiciously to maximize either spectral efficiency or throughput. With ARQ correcting occasional packet errors at the data link layer, the stringent error control requirement is alleviated for the AMC at the physical layer. Numerical results demonstrate that the proposed AMC-HARQ design outperforms either application of AMC only at the physical layer or incorporation of ARQ with fixed modulation and coding scheme.

1. Introduction

Vehicular ad hoc networks (VANETs) are a type of mobile ad hoc networks where each vehicle serves as a node interconnected by wireless links. One of the most important features in VANETs is that each vehicle can only move in a predictable manner but at much higher speeds compared with the traditional mobile ad hoc networks (MANETs). The Dedicated Short Range Communication (DSRC) standard [1], which is currently under extensive development by the IEEE 802.11p [2] standardization committee, defines two types of communication in VANETs: vehicle to vehicle (V2V) and vehicle to infrastructure (V2I). An excellent overview on DSRC technology is also given in [3], which first gives a general description of the architecture by introducing the concepts, applications, and characteristics of the technology to be used for V2V and V2I communications. DSRC is committed to support a suite of safety applications such as collision warning, up-to-date traffic information, and active navigation and infotainment. With DSRC, each vehicle on the road is broadcasting routine traffic related messages with the information of position, current time instance, driving direction, speed, acceleration/deceleration, and possible traffic conditions. The frequency spectrum between 5.850 and 5.925 GHz is allocated for DSRC, which will enable vehicles to communicate with the road infrastructure and allows for a large number of ITS applications. This provides an opportunity for automakers, government agencies, and related commercial entities to improve highway safety. However, intervehicle communications must operate effectively within transmit power limits and under received signal strength fluctuations and Doppler spread. DSRC for intervehicle wireless communications can provide numerous safety applications, but these require reliable communications at a reasonable cost.

The DSRC standard employs convolutional codes for Forward Error Correction (FEC). The performance analysis of them has been extensively studied in the literature such as [4–9]. For instance, a feasibility study of delay-critical safety applications over vehicular ad hoc networks based on the emerging DSRC standard is conducted in [4]. Under the current static backoff schemes, the infrastructure data

collection mode of IEEE 802.11p standard does not perform well [5]. The performance of the DSRC system is evaluated under three different channels with convolutional codes, regular LDPC codes, and quasi-cyclic (QC) LDPC codes [6, 7]. It has shown that LDPC codes provide an attractive tradeoff between performance and complexity and should be considered as alternative error correction codes for DSRC systems. Similarly, Amditis and Uzunoglu [8] simulated the physical layer (PHY) of the upcoming vehicular communication standard IEEE 802.11p in V2V situation through two different scenarios under different modulation schemes. In [9], the results of evaluation of the performance of IEEE 802.11p PHY employing turbo coding are presented. In all these results, the LDPC codes are considered the better candidates due to their good performance and low encoding and decoding complexity, which is important to the real time communications in the VANETs.

In wireless communication networks, the demand for high data rates and quality of service (QoS) is growing at a rapid pace. The cross-layer design approaches are likely to provide much better results in practice. The study of [10] tries to achieve links scheduling and power assignment while meeting the data rate and peak power level constraints such that the resulting throughput is maximized. In [11], a cross-layer design along with an optimal resource allocation framework is formulated for wireless fading networks by employing the network coding. However, these cross-layer design methods are notoriously complicated and difficult to translate into practice.

The adaptive modulation and coding (AMC) [12] have been studied extensively and advocated at the physical layer, which can enhance throughput in future wireless data communication system. The automatic repeat request (ARQ) protocol at the data link layer that requests retransmissions for those received packers with error is also very important to throughput enhancement. It has proved that joint AMC-ARQ [13] design outperforms either application of AMC only at physical layer or ARQ only with a fixed modulation and coding scheme. In this paper, we consider the cross-layer design combining AMC and Incremental Redundancy HARQ (IR_HARQ), which is the most efficient ARQ scheme. In physical layer the AMC adjusts the data rates roughly according to the Channel State Information (CSI) by choosing different modulation modes while the data rates are accurately adjusted by HARQ according to the CSI with changing the maximum retransmission number in data link layer. One of the key problems for realizing AMC IR_HARQ is rate-compatible (RC) codes, which consist of a low-rate mother code and several higher rates achieved through compatible puncturing. Hence, the decoder for the lowest rate code is compatible with that for the higher rate codes and no additional complexity is needed. In this work we will employ RC-LDPC codes as the FEC codes for DSRC systems. By taking advantage of the cross-layer design combining AMC and IR_HARQ, the throughput is enhanced with low system complexity.

The rest of the paper is organized as follows. An overview of DSRC system is discussed in Section 2. Section 3 describes the proposed cross-layer design combining methods of AMC and IR_HARQ. The simulation results are presented and discussed in Section 4. Section 5 concludes our work.

Table 1: DSRC physical layer parameters.

Modulation	BPSK, QPSK, 16 QAM, 64 QAM
Data rate	3, 4.5, 6, 9, 12, 18, 27 Mbps
Coding rate	1/2, 2/3, 3/4
Number of subcarriers	52
Subcarrier spacing	156.25 KHz
Number of pilot tones	4
Guard interval	1.6 μsec
OFDM symbol duration	8 μsec
Signal bandwidth	10 MHz

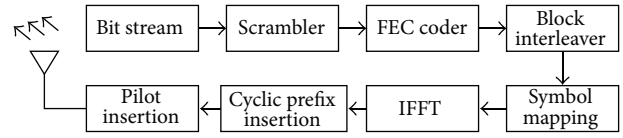


Figure 1: The DSRC transmitter model.

2. Overview of DSRC System

DSRC physical layer has the same frame structure, modulation, and training sequences as specified in the IEEE 802.11a standard, and its signal bandwidth is 10 MHz (half the IEEE 802.11a bandwidth). The basic DSRC parameters are shown in Table 1.

The block diagrams of the DSRC transmitter and receiver are shown in Figures 1 and 2, respectively [6, 7]. The input bit stream is first scrambled and then encoded with a convolution code, for which the constraint length is 7 and code rate is 1/2. The interleaving redistributes the bits before transmission, which reduces the effects of burst errors caused by the fading channel. Perfect timing and frequency synchronization is also assumed, and the received signal is transformed to the frequency domain using a Fast Fourier Transform (FFT). The resulting signal is then mapped to bits and deinterleaved. Finally, the soft information is input to channel decoder, and the output bits descrambled. The output of the scrambler is encoded using code rates $R = 1/2$, $2/3$, or $3/4$, depending on the desired data rate. The convolution encoder has rate $R = 1/2$ and constraint length 7 (memory length $m = 6$), as shown in Figure 3. Higher rates are obtained by puncturing the output bit stream.

3. The Cross-Layer Design Combining AMC and IR_HARQ

3.1. AMC Method Based on LDPC Codes. In this section, we provide the AMC method based on LDPC codes, which have demonstrated impressive error-correcting qualities under BPSK modulation and are also good codes to use in combination with higher-order modulations. Figure 4 shows a rate-adaptive coded modulation communication system.

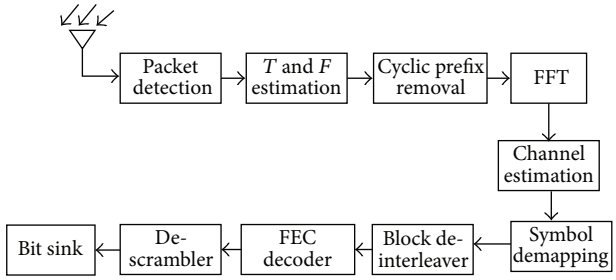


Figure 2: The DSRC receiver model.

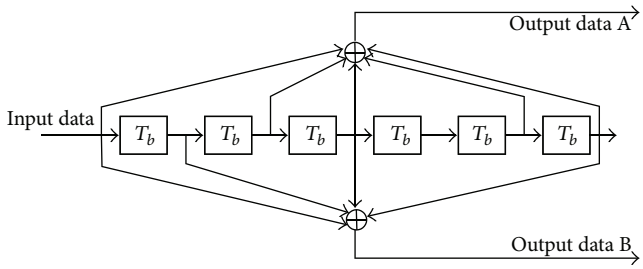


Figure 3: The convolutional encoder for a DSRC system based on the IEEE 802.11p standard.

The encoded bits are mapped into M-QAM constellations according to Gray code mappings. For each M-QAM constellation we construct an LDPC code such that the lengths of all codes are integer multiple of M-QAM symbols in the corresponding constellation.

Here our objective is to maximize the data rate, while maintaining the required performance. Let N denote the total available number of transmission modes. We assume constant power transmission and separate the total SNR range into $N + 1$, with no overlapping consecutive intervals, with boundary points denoted as $\{\gamma_i\}_{i=0}^{N}$. If the channel estimated SNR is γ, we have

$$\gamma \in [\gamma_i, \gamma_{i+1}), \quad \text{mode } i \text{ is chosen.} \tag{1}$$

The boundary point γ_i is determined for that the instantaneous block error rate (BLER) or bit error rate (BER) is guaranteed to be not greater than target BER_0 or BLER_0. So the value of γ_i is obtained by solving the following equation for each mode:

$$\text{BER}(\gamma_i) = \text{BER}_0 \tag{2}$$

or

$$\text{BLER}(\gamma_i) = \text{BLER}_0 \tag{3}$$

as the functions of the estimated SNR γ, $\text{BER}(\gamma_i)$, and $\text{BLER}(\gamma_i)$ are the BER and BLER for mode i, respectively.

3.2. AMC-HARQ Design. In this section, we develop a cross-layer design, which combines AMC at physical layer with HARQ at data link layer in order to maximize system throughput under performance requirements.

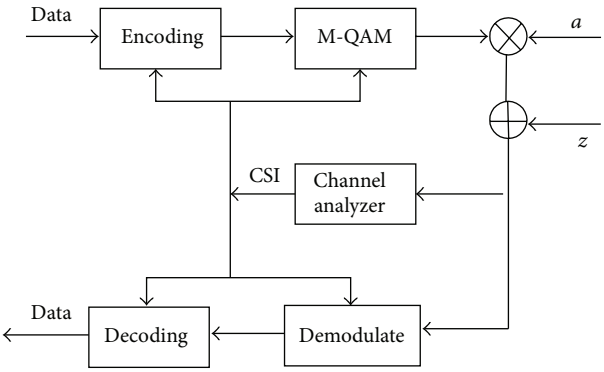


Figure 4: The ACM system based on LDPC codes.

Since only finite delays and buffer sizes can be afforded in practice, the maximum number of ARQ retransmissions has to be bounded. We denote the maximum number of retransmissions allowed per block by $N^{\max}$. Note that a block is dropped if it is received incorrectly after a maximum number of $N^{\max} + 1$ transmissions, that is, after $N^{\max}$ retransmissions. Let $\overline{\text{BLER}}$ denote the average block error rate and $\overline{\text{BLER}} = p$. The average number of transmissions per block is computed as

$$\overline{N}(p, N^{\max}) = 1 + p + p^2 + \cdots + p^{N^{\max}}. \tag{4}$$

When mode i is used, each transmitted symbol will carry $R_i = R_c \log_2 M_i$ information bits for mode adhering to a M_i-QAM constellation and a code with rate R_c. Define $P_r(i)$ as the probability that the mode i will be chosen. Therefore, the average spectral efficiency achieved at physical layer without considering possible retransmission is

$$\overline{S}_{e,\text{phy}} = \sum_{i=1}^{N} R_i P_r(i). \tag{5}$$

When HARQ is implemented, each block, and thus each information bit, is equivalently transmitted $\overline{N}(p, N^{\max})$ times. Hence, the overall average spectral efficiency, as a function of $N^{\max}$, is given by

$$\overline{S}_{e,\text{link}} = \frac{\overline{S}_{e,\text{phy}}}{\overline{N}(p, N^{\max})} = \frac{1}{\overline{N}(p, N^{\max})} \sum_{i=1}^{N} R_i P_r(i). \tag{6}$$

For a certain channel and modulation mode, the average spectral efficiency $\overline{S}_{e,\text{phy}}$ is a constant. So from (6) we can optimize the overall average spectral efficiency $\overline{S}_{e,\text{link}}$ at data link layer by changing the maximum number of retransmissions $N^{\max}$. The system model and layer structure of our cross-layer design are shown in Figures 5 and 6, respectively. Let I denote the total number of AMC available modes. For each mode we define the maximum number of retransmissions for IR_HARQ as $N^{\max}$. If $N^{\max}$ is J_i under ith AMC mode, the total available number of transmission modes of this system is $N' = J_1 + J_2 + \cdots + J_i + \cdots + J_I$. We assume that the instantaneous BLER is guaranteed to be not greater than target BLER_0 at

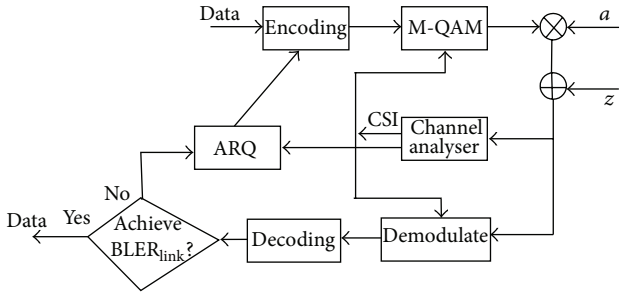


Figure 5: Cross-layer combining AMC with HARQ transmission system.

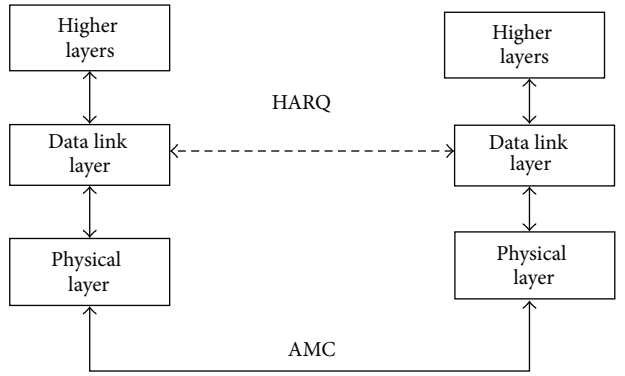


Figure 6: Cross-layer structure combining AMC with HARQ.

physical layer. The BLER is not greater than $\mathrm{BLER}_0^{N^{\max}+1}$ at data link layer. So we obtain

$$\mathrm{BLER}_0^{N^{\max}+1} \le \mathrm{BLER}_{\mathrm{link}}. \tag{7}$$

From (7), we have

$$\mathrm{BLER}_0 \le \mathrm{BLER}_{\mathrm{link}}^{(1/(N^{\max}+1))}. \tag{8}$$

The whole SNR range is divided into $N + 1$ intervals, with thresholds γ_i, $i = 0, 1, \ldots, N$. The instantaneous channel signal to noise ratio SNR is γ. When $\gamma \in [\gamma_i, \gamma_{i+1})$, mode i is chosen. The threshold γ_i is determined according to (3). In (3) the target BLER_0 at physical layer is determined according to (8).

By always selecting the acceptable code producing the highest spectral efficiency for a given channel estimated SNR value, we will maximize the spectral efficiency of the overall system, while the BER or BLER requirement is still maintained.

4. Performances

4.1. Extraction of the LLR of QAM Modulation. In LDPC coded QAM system, the calculation of the Log-Likelihood Ratio (LLR) on the coded bits is an important function of practical wireless receivers. In this section, the exact bit LLR for the M-QAM signal is presented [14].

As an example let us consider a 16-QAM transmitted symbol sequence $s_k = s_{Ik} + js_{Qk}$, with $s_{Ik}, s_{Qk} \in \{\pm 1, \pm 3\}$.

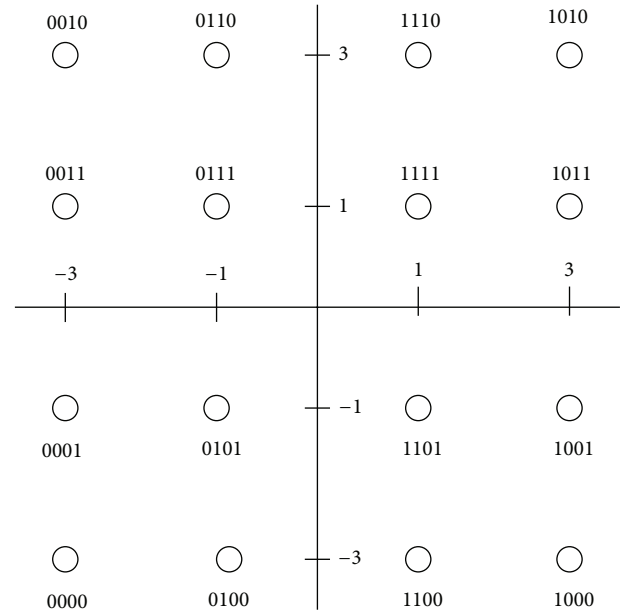


Figure 7: 16-QAM bit to symbol mapping.

According to the mapping rule $s_k = M(u_{k1}, u_{k2}, u_{k3}, u_{k4})$, each modulation symbol is obtained from the information bits $u_{k,i}$, $i = 1, \ldots, 4$. Without loss of generality, we assume $s_{Ik} = M_I(u_{k1}, u_{k3})$ and $s_{Qk} = M_Q(u_{k2}, u_{k4})$. An example of Gray code mapping is given in Figure 7.

Let X_k denote the baseband received signal sample corresponding to symbol s_k:

$$X_k = x_{Ik} + jx_{Qk} = a\sqrt{E_s}s_k + n_k. \tag{9}$$

In (9), $a \in R^+$, E_s represents the received signal symbol energy and $n_k = n_{Ik} + jn_{Qk}$ is additive white complex noise, with n_{Ik} and n_{Qk} being independent Gaussian processes with zero mean and variance $\sigma^2 = N_0/2$.

Let $\Lambda(u_{ki})$ indicate the LLR of bit u_{ki} given X_k, and in the case of equiprobable symbols

$$\Lambda\left(u_{k1}\right) = \log \frac{P\left\{u_{ki} = 1 \mid X_k\right\}}{P\left\{u_{ki} = 0 \mid X_k\right\}} = \log \frac{P\left\{X_k \mid u_{ki} = 1\right\}}{P\left\{X_k \mid u_{ki} = 0\right\}}. \tag{10}$$

Define by $S(u_{ki} = 1) = \{q : s^{(q)} = M(\ldots, u_{ki} = 1, \ldots)\}$ and $S(u_{ki} = 0) = \{q : s^{(q)} = M(\ldots, u_{ki} = 0, \ldots)\}$ the subsets of symbol indexes corresponding to $u_{ki} = 1$ and $u_{ki} = 0$ respectively, then

$$\begin{aligned} P\left\{X_k \mid u_{ki} = 1\right\} &= \sum_{q \in S\left(u_{ki}=1\right)} p\left(X_k \mid s^{(q)}\right), \\ P\left\{X_k \mid u_{ki} = 0\right\} &= \sum_{q \in S\left(u_{ki}=0\right)} p\left(X_k \mid s^{(q)}\right). \end{aligned} \tag{11}$$

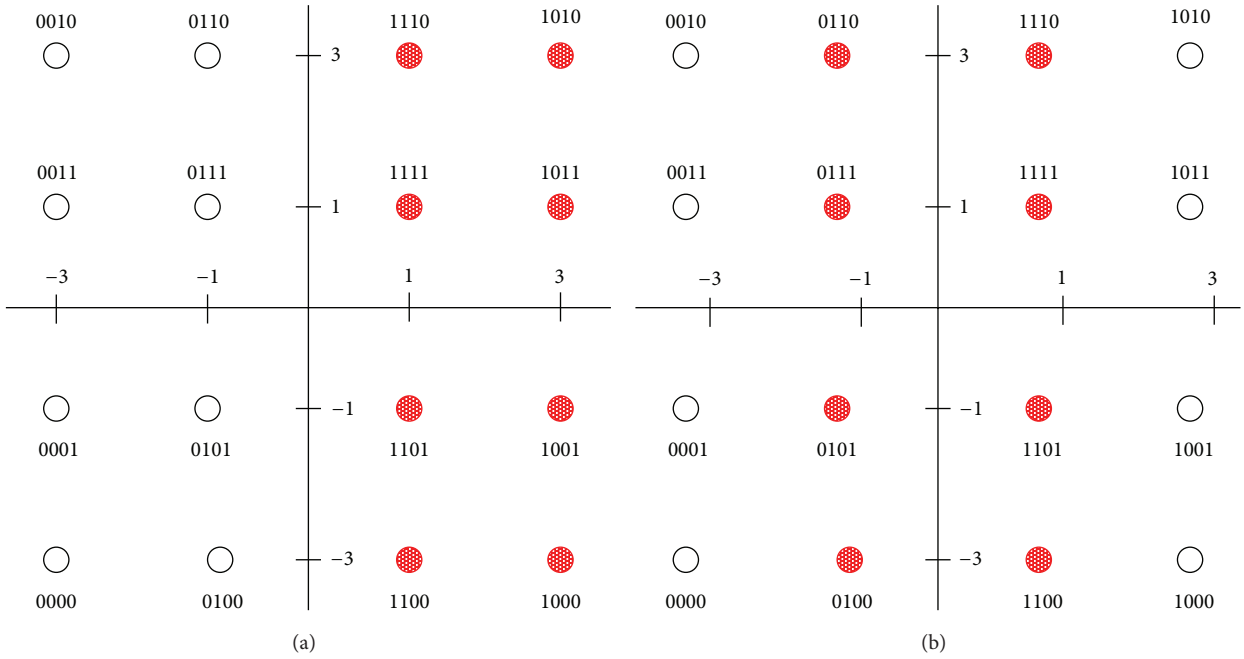


Figure 8: Symbol set partitioning for bit $u_{k,1}$ and $u_{k,2}$.

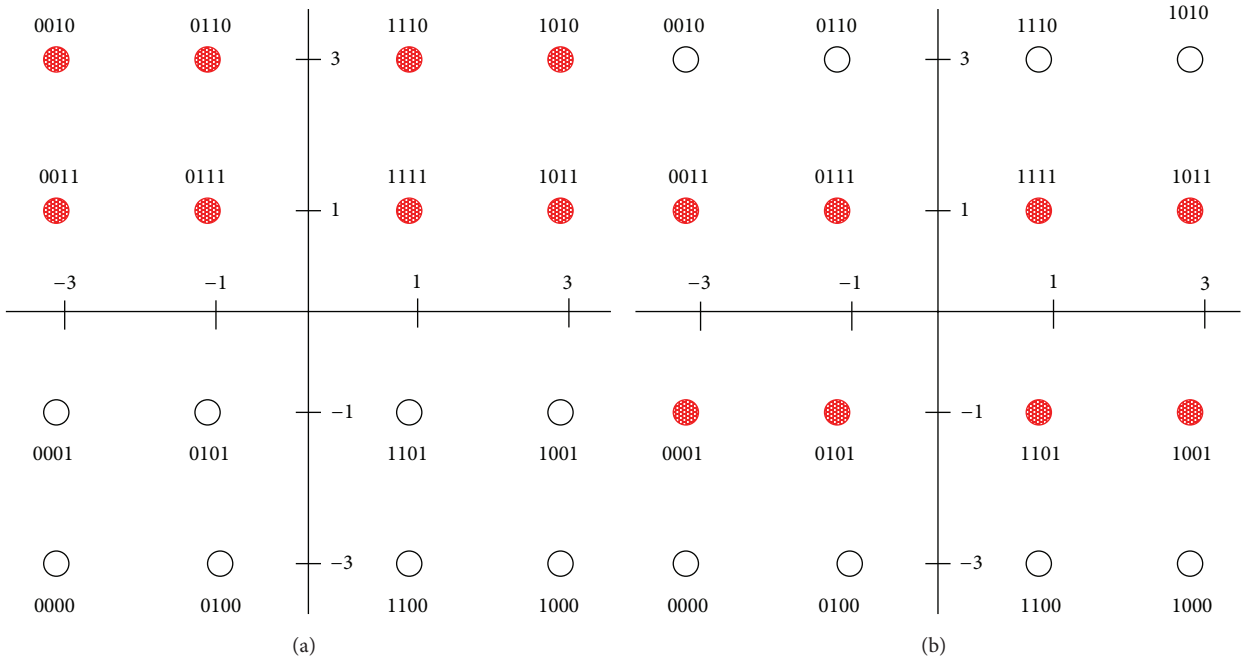


Figure 9: Symbol set partitioning for bit $u_{k,3}$ and $u_{k,4}$.

Figures 8 and 9 show the symbol set partitioning for the bits $u_{k,i}$, $i = 1, \ldots, 4$, respectively. From the assumption on the noise n_k, we have

$$p\left(X_k \mid s^{(q)}\right) = \frac{1}{\pi N_0} \exp\left(-\frac{\left|X_k - a\sqrt{E_s}s^{(q)}\right|^2}{N_0}\right). \quad (12)$$

Therefore, straightforward calculation gives

$$\Lambda\left(u_{k1}\right) = \log \frac{e^{-\left(X_k - a_k \cdot 1 \cdot \sqrt{E_s}\right)^2/2\sigma^2} + e^{-\left(X_k - a_k \cdot 3 \cdot \sqrt{E_s}\right)^2/2\sigma^2}}{e^{-\left(X_k + a_k \cdot 1 \cdot \sqrt{E_s}\right)^2/2\sigma^2} + e^{-\left(X_k + a_k \cdot 3 \cdot \sqrt{E_s}\right)^2/2\sigma^2}},$$

$$\Lambda\left(u_{k2}\right) = \log \frac{e^{-\left(x_k - a_k \cdot 1 \cdot \sqrt{E_s}\right)^2/2\sigma^2} + e^{-\left(x_k + a_k \cdot 1 \cdot \sqrt{E_s}\right)^2/2\sigma^2}}{e^{-\left(x_k - a_k \cdot 3 \cdot \sqrt{E_s}\right)^2/2\sigma^2} + e^{-\left(x_k + a_k \cdot 3 \cdot \sqrt{E_s}\right)^2/2\sigma^2}},$$

Table 2: Transmission modes in the AMC system under AWGN channel.

Model	MCS1	MCS2	MCS3	MCS4	MCS5	MCS6
Modulation	4 QAM	4 QAM	16 QAM	16 QAM	64 QAM	64 QAM
Coding rate	1/2	2/3	2/3	3/4	3/4	5/6
Spectral efficiency	1.00	1.33	2.67	3.00	4.50	5.00
SNR thresholds	1.8	3.4	9.4	10.6	15.6	16.7

Table 3: Transmission modes cross-layer combining AMC with HARQ (the maximum number of retransmissions $N^{\max}$ is fixed).

Model	MCS1	MCS2	MCS3
Modulation	4 QAM	16 QAM	64 QAM
Coding rate	5/6~1/2	5/6~1/2	5/6~1/2
Spectral efficiency	1.6667~1.00	3.333~2	5~3
Thresholds SNR under AWGN channel	4.8	10.9	16

Table 4: Transmission modes cross-layer combining AMC with HARQ under AWGN channel (the maximum number of retransmissions $N^{\max}$ is changeable).

Model	MCS1			MCS2			MCS3		
Modulation	4 QAM			16 QAM			64 QAM		
Coding rate	5/6~1/2			5/6~1/2			5/6~1/2		
Spectral efficiency	1.6667~1.00			3.333~2			5~3		
Maximum number of retransmissions	4	3	2	4	3	2	4	3	2
SNR thresholds	3.6	4.9	5.95	10	11	12.5	15.1	16.1	17.4

$$\Lambda(u_{k3}) = \log \frac{e^{-(Y_k - a_k \cdot 1 \cdot \sqrt{E_s})^2/2\sigma^2} + e^{-(Y_k - a_k \cdot 3 \cdot \sqrt{E_s})^2/2\sigma^2}}{e^{-(Y_k + a_k \cdot 1 \cdot \sqrt{E_s})^2/2\sigma^2} + e^{-(Y_k + a_k \cdot 3 \cdot \sqrt{E_s})^2/2\sigma^2}},$$
$$\Lambda(u_{k4}) = \log \frac{e^{-(Y_k - a_k \cdot 1 \cdot \sqrt{E_s})^2/2\sigma^2} + e^{-(Y_k + a_k \cdot 1 \cdot \sqrt{E_s})^2/2\sigma^2}}{e^{-(Y_k - a_k \cdot 3 \cdot \sqrt{E_s})^2/2\sigma^2} + e^{-(Y_k + a_k \cdot 3 \cdot \sqrt{E_s})^2/2\sigma^2}}. \quad (13)$$

The similar conclusion can be obtained for any other MQAM schemes in DSRC standard.

4.2. Simulation Results. To evaluate the performance of our algorithm, we have performed the simulations under AWGN channel. The transmission modes of AMC system are listed in Table 2 in ascending order of rate. The (2304, 1920) LDPC code with rate 5/6 is employed as a mother code, from which (2304, 1728) code with 3/4 rate, (2304, 1536) code with 2/3 rate, and (2304, 1152) code with 1/2 rate [15] can be obtained by puncturing. Decoded with Belief Propagation (BP) algorithm [16], is set to be the maximum number of iterations equal to 50. BER and BLER performances of modulation modes in Table 2 under AWGN channel and Rayleigh channel are shown in Figure 10. Let the constrained performance in physical layer be $\mathrm{BER}_0 = 10^{-3}$, from which we can determine the thresholds γ_i with (2).

The transmission modes of AMC-HARQ system with fixed maximum number of retransmissions based on RC-LDPC codes are listed in Table 3. We still use (2304, 1920) RC-LDPC codes with 5/6 rate as FEC, from which LDPC codes with 1/2, 2/3, 3/4, and 4/5 rate can be obtained by puncturing. Therefore, the maximum number of retransmissions of ARQ is 4. The BLER for 5/6 rate LDPC code as well as its punctured codes under AWGN channel is shown in Figure 11. Let the constrained performance in data link layer be $\mathrm{BLER}_0 = 10^{-2}$. From (8) the performance target BLER in physical layer is $\mathrm{BLER}_0 \le 0.001^{1/5} = 0.2512$. Let 4/5 rate punctured code as criterion thresholds γ_i can be determined according to (3), which is shown in Table 3.

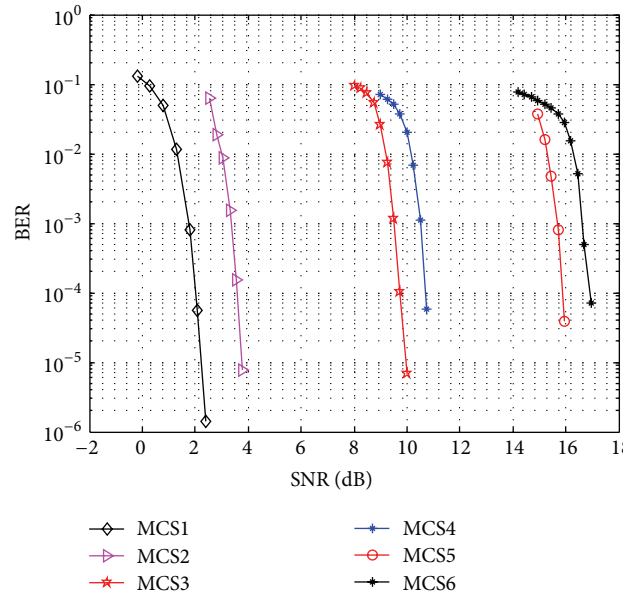


Figure 10: BER performance of modulation modes in Table 2 under AWGN channel.

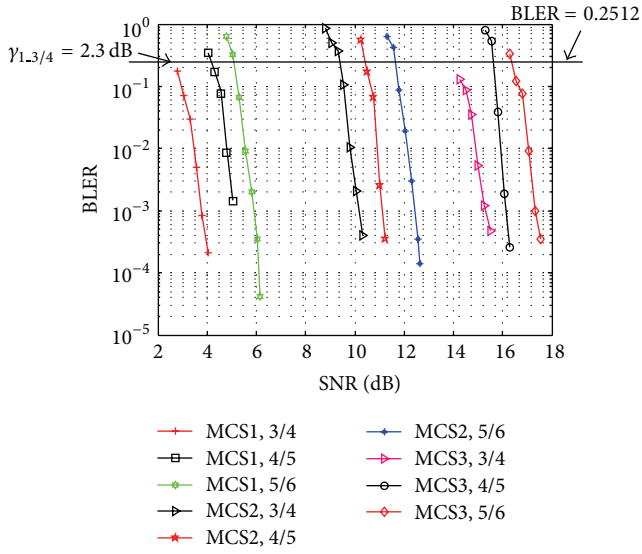


Figure 11: BLER for 2/3 rate LDCP code and its punctured codes under AWGN channel.

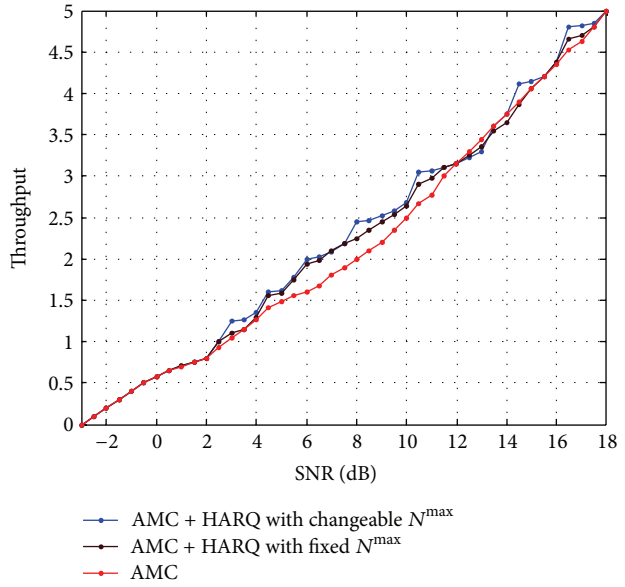


Figure 12: Average spectral efficiency versus average SNR for three different transmission systems under AWGN channel.

The transmission modes of AMC-HARQ system with changeable maximum number of retransmissions based on RC-LDPC codes are listed in Table 4. RC-LDPC codes (2304, 1920) [15] with 5/6 rate also are employed as FEC. The total number of modulation modes is MCS1, MCS2, and MCS3. We consider three values for the maximum numbers of retransmissions $N^{\max} = 2, 3$, and 4 for each modulation mode. Given the performance constraint at the data link layer is $\text{BLER}_0 = 10^{-2}$, we can get the performance target BLER in physical layer for each mode and the thresholds γ_i can be obtained according to (3), which are shown in Table 4. The simulations are performed for comparing the throughput

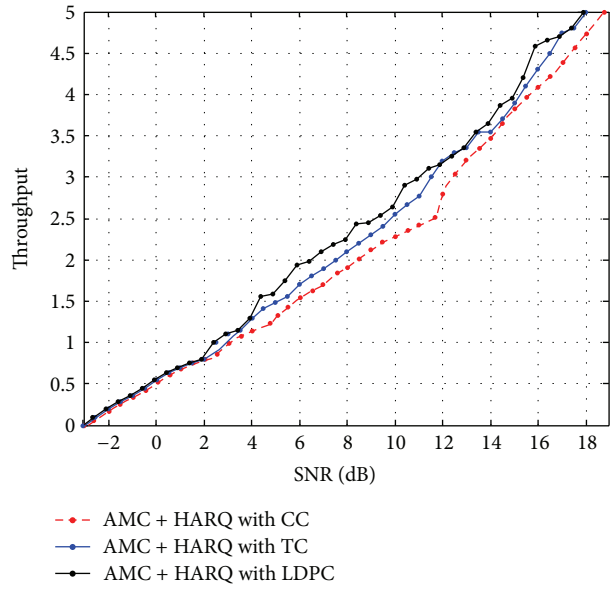


Figure 13: Average spectral efficiency versus average SNR under three channel coding methods.

of three systems under AWGN channel. We assume perfect channel estimation so that the receiver can obtain the exact channel quality SNR, and the feedback channel is error-free. The stopping-waiting IR_HARQ protocols are adopted. The maximum iterative decoding numbers of LDPC codes are 50. The results are shown in Figure 12, from which we can know that AMC-HARQ system with changeable maximum number of retransmissions outperforms the other two systems. We replace the LDPC codes by rate compatible convolutional codes (CC) and turbo codes (TC) in [2] and the simulation results are shown in Figure 13. The proposed AMC-HARQ system based on LDPC codes illustrates the best performance.

5. Conclusions

In this paper, we developed a cross-layer design, which combines adaptive modulation and coding at the physical layer with IR_HARQ at the data link layer in order to maximize system spectral efficiency under prescribed performance constraints. In physical layer the AMC adjusts the data rates roughly according to the CSI by choosing different modulation modes. In data link layer HARQ adjusts the data rate accurately according to the CSI by changing the maximum retransmission number. Numerical results demonstrated the rate improvement of our cross-layer design over AMC alone, as well as AMC-HARQ with fixed maximum number of retransmissions. In our proposed scheme, we employed RC-LDPC as channel codes due to their decoder for the lowest code rate being compatible with the ones for higher code rates. Our new method can improve the performance and no additional complexity is needed. All of our simulations are conducted under AWGN channel, and in the future,

we intend to perform further experiments under a more realistic channel model for the DSRC system.

Acknowledgments

The work is supported by the NSFC (Grant nos. 61032003, 61271172, and 61071100), RFDP (Grant nos. 20120185110025 and 20120185110030), NCET (Grant no. NCET-09-0266), and SRF for ROCS, SEM.

References

[1] C. Cseh, "Architecture of the dedicated short-range communications (DSRC) protocol," in *Proceedings of the 48th IEEE Vehicular Technology Conference (VTC '98)*, pp. 2095–2099, Ottawa, Canada, May 1998.

[2] Task Group p, "IEEE P802.11p: Draft Standard for Information Technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications," IEEE Computer Society, 2009.

[3] R. A. Uzcátegui and G. Acosta-Marum, "Wave: a tutorial," *IEEE Communications Magazine*, vol. 47, no. 5, pp. 126–133, 2009.

[4] J. Yin, T. Elbatt, G. Yeung et al., "Performance evaluation of safety applications over DSRC vehicular ad hoc networks," in *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks*, pp. 1–9, Philadelphia, Pa, USA, October 2004.

[5] Y. Wang, A. Ahmed, B. Krishnamachari, and K. Psounis, "IEEE 802.11p performance evaluation and protocol enhancement," in *Proceedings of the IEEE International Conference on Vehicular Electronics and Safety (ICVES '08)*, pp. 22–24, Columbus, Ohio, USA, September 2008.

[6] N. Khosroshahi and T. A. Gulliver, "Low density parity check codes for dedicated short range communication (DSRC) systems," in *Proceedings of the IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM '09)*, pp. 802–807, August 2009.

[7] N. Khosroshahi and T. A. Gulliver, "Quasi-cyclic low density parity check (LDPC) codes for dedicated short range communication (DSRC) systems," in *Proceedings of the 23rd Canadian Conference on Electrical and Computer Engineering (CCECE '10)*, pp. 1–5, May 2010.

[8] A. Amditis and N. K. Uzunoglu, "Simulation-based performance analysis and improvement of orthogonal frequency division multiplexing—802.11p system for vehicular communications," *IET Intelligent Transport Systems*, vol. 3, no. 4, pp. 429–436, 2009.

[9] G. C. Kiokes, G. Economakos, A. Amditis, and N. K. Uzunoglu, "Recursive systematic convolutional code simulation for Ofdm—802.11p system and FPGA implementation using an ESL methodology," in *Proceedings of the 12th Euromicro Conference on Digital System Design, Architectures, Methods and Tools (DSD '09)*, pp. 791–798, August 2009.

[10] G. Kulkarni, V. Raghunathan, and M. Srivastava, "Joint end-to-end scheduling, power control and rate control in multi-hop wireless networks," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '04)*, vol. 5, pp. 3357–3362, December 2004.

[11] K. Rajawat, N. Gatsis, and G. B. Giannakis, "Cross-layer designs in coded wireless fading networks with multicast," *IEEE/ACM Transactions on Networking*, vol. 19, no. 5, pp. 1276–1289, 2011.

[12] M.-S. Alouini and A. J. Goldsmith, "Adaptive modulation over Nakagami fading channels," *Wireless Personal Communications*, vol. 13, no. 1, pp. 119–143, 2000.

[13] Y. Z. Bang, F. Pin, and C. Z. Gang, "Cross layer design for service diferentiation in mobile ad hoc networks," in *Proceeding ofIEEEInternational Symposium on Personal, Indoor and Mobile Radio Communication*, vol. 1, pp. 778–782, 2003.

[14] S. Allpress, C. Luschi, and S. Felix, "Exact and approximated expressions of the log-likelihood ratio for 16-QAM signals," in *Proceedings of the Conference Record of the 38th Asilomar Conference on Signals, Systems and Computers*, pp. 794–798, Pacific Grove, Calif, USA, November 2004.

[15] Draft IEEE Standard for Local and metropolitan area networks-Part 16, "Air Interface for Fixed and Mobile Broadband Wireless Access Systems," IEEE P802.16e/D12, 2005.

[16] D. J. C. MacKay, "Good codes based on very sparse matrices," *IEEE Transactions on Information Theory*, vol. 45, no. 2, pp. 1645–1646, 1999.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 586193, 14 pages
http://dx.doi.org/10.1155/2013/586193

Research Article

VCAST: Scalable Dissemination of Vehicular Information with Distance-Sensitive Precision

V. Kulathumani, R. A. Moparthi, and Y. P. Fallah

Department of Computer Science and Electrical Engineering, West Virginia University, Morgantown, WV 26506, USA

Correspondence should be addressed to V. Kulathumani; vinod.kulathumani@mail.wvu.edu

Received 12 April 2013; Revised 31 July 2013; Accepted 13 September 2013

Academic Editor: Chunming Qiao

Real-time information about the state (location, speed, and direction) of other vehicles in the system is critical for both safety and navigation applications in future intelligent transportation systems. However, reliably obtaining this information over multiple hops in a capacity constrained, contention-prone wireless network poses a significant challenge. In this paper, we describe an algorithm *VCAST* that addresses this challenge by exploiting a notion of *distance sensitivity in information propagation*, in which information is forwarded at a rate that decreases linearly with distance from the source. By doing so, the required communication overhead per node can be significantly reduced, thereby reducing channel contention, allowing higher information supply rates, and scaling to larger network sizes. *VCAST* can be used to improve safety against collisions and to enable dynamic routing and navigation techniques by providing aggregate traffic information in an extended neighborhood. The performance of *VCAST* is validated using extensive ns-3 simulations under different network sizes and densities with an IEEE 802.11b transmission model and the advantages of *VCAST* in comparison to non-distance-sensitive approaches are highlighted.

1. Introduction

Infrastructureless, vehicle-to-vehicle (V2V) wireless communication is expected to be the basis for both safety and navigation applications in future intelligent transportation systems [1, 2]. Examples of safety applications in transportation scenarios include collision warnings, guidance on lane change and lane merge, and stopped vehicle alert. Examples of intelligent navigation applications include dynamic travel-time computations and rerouting based on real-time traffic information. A building block for all these applications is a real-time vehicular traffic mapping system on board every vehicle, which portrays information about current position of other vehicles in its vicinity and provides guidance about accidents, approaching emergency vehicles and traffic congestion over an extended neighborhood. In this paper, we design *VCAST*, a scalable, infrastructureless, peer-to-peer wireless network service for computing such a real-time traffic map over a given region surrounding each vehicle (This paper is a significant extension of a shorter version that appeared in IEEE VTC 2012 [3]. The specific additions are as follows. (1) Simulations are carried out in ns-3 using an IEEE 802.11 b transmission model to quantify the impact of network size, vehicular density, vehicular mobility, and time-varying intervehicular separations on the achievable staleness. (2) The average communication cost incurred by each vehicle is quantified. (3) The performance is compared analytically and using simulations with schemes that do not incorporate distance sensitivity, and the significant impact on scalability using *VCAST* is highlighted. (4) Complete proofs are included for all lemmas and theorems).

We assume that vehicles are equipped with a differential GPS that can estimate its location to an accuracy of about 1-2 m. As a result, by advertising this information, vehicles can learn about traffic within a one hop communication range. However, estimating traffic maps over a large area using multihop wireless communication is a much more challenging task. (1) Firstly, we note that forwarding each vehicle's information over multiple hops at a constant rate is unlikely to be scalable as it will cause the amount of communication required at each vehicle to grow with the number of vehicles in the region over which traffic information is required. As a result, both the allowable broadcast rate and the accuracy of the traffic map obtained at each

vehicle will decrease as vehicular density and size of the region increase. *Hence effective forwarding algorithms need to be designed to ensure that the system remains scalable with vehicular density, information supply rate, and region size.* (2) Secondly, there exist tradeoffs in choosing the rate and communication range of each broadcast. While higher broadcast rates and range promise greater tracking accuracy, in reality wireless channel contention can cause an adverse effect in tracking accuracy as these levels exceed a certain limit. Existing broadcast techniques for vehicular safety systems have primarily focused on balancing transmission rate and communication range to maximize the reliability of single hop wireless communication. However, in such an approach information about other vehicles is available only when intervehicular distance is too small which may not be enough to avert a collision [4] or to provide a timely re-route in the presence of traffic congestion. On the other hand, increasing the single-hop communication range or moving to multihop forwarding techniques to learn about vehicles in a larger area quickly decreases the achievable information supply rate from each vehicle (even those at smaller distances). *Hence, there remains a need for multihop broadcasting techniques that are able to supply timely information over large distances without compromising on data supply rates at smaller distances.*

Contributions. To address the above challenges and to ensure scalability when providing traffic maps over large regions in real time, we exploit a notion of *distance sensitivity* in propagating individual vehicle information: information about each vehicle is propagated at a rate that decreases linearly with the distance from the vehicle [5, 6]. The rationale behind exploiting distance sensitivity is that the reaction time available to a vehicle for taking safety actions or for computing new routes towards the destination is lesser with respect to the state of nearby vehicles than that of farther vehicles. *VCAST* maps this distance-dependent reaction time into delivery of information with quality that progressively decays as a function of distance.

We use staleness in vehicular state information as a metric for information quality as it reflects how old the current information about a particular vehicle is and show that traffic information in *VCAST* can be obtained with a worst-case staleness that is bounded by $O(d^2)$ where d is the distance from the source of the information. Thus, *VCAST* provides traffic information with *distance-sensitive precision* in which the error does not grow with the number of vehicles in the region and is independent of traffic density and network size. At the same time, the average communication cost (the required transmission rate at each node) also is only bounded by $O(p\sqrt{N})$, where p is the broadcast rate at the source. Lower communication overhead per node ensures lower channel contention and higher source broadcast rates, thus benefiting information supply at smaller distances. *VCAST* can be used to propagate actual vehicle location as well as to propagate aggregate traffic information such as average speed and density of vehicles over individual traffic *cells* inside a region. One possible scenario is to propagate actual vehicle location up to a distance of 500–1000 m and aggregate traffic information up to several miles. When propagating only aggregate cell information, we note that the required communication rate per node decreases further by a factor r_c, where r_c is the radius of each aggregation cell.

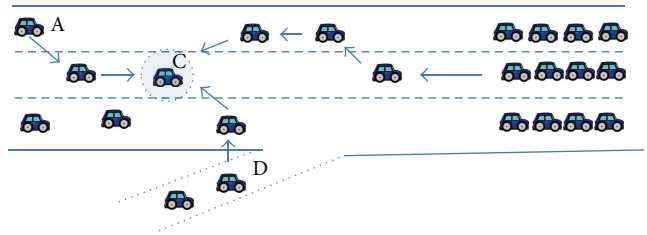


Figure 1: Utilization of multihop vehicular information for safety applications. The arrows indicate multihop information flow towards car C. Knowledge of states of A and D will guarantee safe lane change to left and right, respectively. Knowledge of congestion will allow safe, timely reaction.

The performance of *VCAST* is validated using extensive simulations in ns-3, a discrete event simulator for wireless networks, under different network sizes, network densities, source broadcast rates, and communication ranges. The results of our evaluation show that, by using distance-sensitive forwarding, *VCAST* is able to scale to larger network sizes as well as support much higher broadcast rates compared to non-distance-sensitive techniques. The reason for scalability was shown to be the significantly lower message overhead which reduces the channel contention in the network. We have also characterized the performance of *VCAST* under severe random mobility and studied information staleness when aggregated data is transmitted as opposed to individual vehicle information.

Impact. By forwarding traffic information over multiple communication hops, we expect several advantages: (1) vehicle location over a vicinity will be available even if the communication range is extremely low because of high density, thus improving vehicular safety, (2) information about approaching emergency vehicles will be available, (3) information about lane changing and merging vehicles will be available even if they are outside a single communication range, and (4) information about road blocks, accidents, and impending congestion will be available from several miles ahead, thus permitting higher level applications that dynamically re-route based on this information. Some of these scenarios, from a vehicular safety perspective, are illustrated in Figure 1. To achieve scalability, *VCAST* provides traffic information with an accuracy that degrades with distance, but we expect this to be a reasonable condition that is still sufficient for both vehicular safety and intelligent navigation. Finally, we note that *VCAST* does not require any special hardware or modification to vehicular transmission standards; instead, it can simply piggyback on the proposed *Here I am* communication [1, 2] for vehicular networks.

Outline of the Paper. In Section 2, we describe related work. In Section 3, we describe our system model, the *VCAST* algorithm, and provide an analysis for the expected accuracy and communication cost. In Section 4, we evaluate the

performance of our system in simulations. In Section 5, we present conclusions and state future work.

2. Related Work

The design of routing protocols for vehicular ad hoc networks and more generally in mobile ad hoc networks is a well-researched topic and a good survey of these techniques can be found in [7–9]. Many of these protocols have focused on delivering aperiodic, low bandwidth data such as emergency vehicle information to either a single vehicle (unicast) or a group of vehicles in a geographic region (geocast) with low latency [10–17]. On the other hand, the focus in this paper is on broadcasting information from each vehicle at high rates to support the design of safety and navigation applications.

The design of wireless broadcast protocols has also received a lot of research attention lately [1, 18–22] in the context of vehicular safety applications. There have been several recent papers that have focused on the problem of balancing broadcast range and reliability so as to maximize the number of successful receptions in close proximity of the sender [18–21]. A common foundation in these papers to handle the tradeoff is to reduce the communication range in regions of high density so as to improve the reliability of reception. However, these papers mainly focus on reliable one-hop message reception and not on multihop propagation. As a result, the information about vehicles outside the communication range is not available even when the range has to be very low because of high density. The trade-off in single-hop broadcast schemes is that a higher communication range causes larger staleness even for nearby vehicles, while a lower communication range prevents information availability from beyond that range. On the other hand, the algorithm developed in this paper can be used to propagate both individual vehicle information and aggregate traffic information over several communication hops and yet retain high data supply rates at smaller distances.

We also note that rate and power control algorithms [1, 18–21] developed for a single hop vehicular broadcast are complementary and can be used in conjunction with the distance-sensitive multihop forwarding algorithm designed in this paper. Thus decisions on source broadcast rate and range can be made commensurate with traffic density using the techniques proposed in [1, 18–21], and *VCAST* can be used to aggregate and forward this information over multiple hops.

Multihop broadcast algorithms [23–29] for vehicular networks have mainly focused on the choice of optimal forwarding vehicles and on the reduction of redundant forwarding vehicles using one of several heuristics proposed in [30]. A good survey of multihop broadcast techniques in mobile ad hoc networks is presented in [31]. The idea of distance-sensitive broadcasting rates developed in this paper for ensuring scalable all-all information broadcast has thus far not been explored in the context of mobile ad-hoc and vehicular networks. The improvement in communication overhead gained by exploiting distance sensitivity is characterized in Section 3.3.

The concept of distance sensitivity has previously found applications in several other networking fields in different forms. For example, route aggregation in the Internet utilizes this concept for efficiently distributing routing information [32]. Fisheye routing [33] uses this idea to propagate routing tables in mobile ad hoc networks. Fractionally cascaded information [34] is a form of distance-sensitive key sharing that is widely used for speeding up traversal of data structures. Distance sensitivity has also been used in wireless sensor network based querying and tracking applications to model communication latency and information quality as functions of distance [35–38]. In the context of network-wide continuous broadcast of system states, an algorithm has been designed in [39] for supplying global state information to all nodes in a static sensor network with distance-sensitive latency and error. In this paper, we show that distance sensitivity is a valuable tool for efficient and scalable propagation of state information even for *networks of mobile nodes (vehicles)*. Unlike the algorithm in [39], we design *VCAST* without assuming an underlying clustering or routing structure, thus avoiding the need for maintenance related communication.

3. System Description

In this section, we first state the system model and objective. We then describe *VCAST* and analytically characterize its accuracy and required communication rate.

3.1. System Model and Problem Statement. We model the vehicular network as a large geographic area with multiple traffic flows, each with potentially different traffic densities at different places. Let ρ denote the maximum density, that is, the maximum number of vehicles per unit area at any time in the whole region. Note that the geographic area will consist of regions with no traffic flows (i.e., no roads), as well as regions with high density traffic flows. When analyzing the impact of aggregation, we assume that the region is partitioned into geographic *cells* which allow representation of aggregated traffic information for that cell. The cells need not be of the same size, but for ease of explanation we assume that the area of each cell is constant and equal to A_C with a radius of r_c. In a realistic environment, these cells could be used to model critical traffic links such as the traffic in a region between two highway exits or traffic between two urban streets. Let r_h denote the single hop communication range for a vehicle. The objective of our system is to provide each vehicle with information about all vehicles and all cells within a radius R around itself where $r_h \ll R$. We call this area of radius R around each vehicle the *tracking zone* (We note that our system can also be specialized to propagate individual vehicle information within a smaller radius than aggregate cell information).

Let N denote the maximum number of vehicles within the tracking zone of each vehicle. Thus $N = \rho\pi R^2$. Let L denote the maximum number of cells in a radius of R around each vehicle. Thus $L = O(R^2/A_c)$. Note that by using a two dimensional model for the vehicular network, the bounds on communication cost in our analysis are expected to hold

for dense urban traffic scenarios as well as highway traffic scenarios in which the number of vehicles is expected to be lower.

Let p denote the frequency at which each vehicle broadcasts its own information. Let $d(i, j)$ denote the geographic distance between vehicles i and j. Let $d_c(i, j)$ denote the distance between vehicle i and cell j in terms of the smallest number of cells traversed to reach cell j from i. In the following subsections, we first describe *VCAST* assuming that only vehicle location is propagated up to a distance R. Then we describe the required changes when aggregate *cell* information is propagated. The communication cost and accuracy for both these cases are characterized in Section 3.3.

3.2. Distance-Sensitive Broadcast Algorithm. A naive technique would be to require each vehicle to obtain information about all vehicles in its tracking zone at a constant interval of $1/p$ seconds. However, in such a scenario each vehicle would have to broadcast information about at most N vehicles at p Hz, making the required communication rate at each node per unit time $O(Np)$. Note that the required communication rate grows with the number of vehicles in the region and is therefore directly proportional to the vehicle density and the area of the region. Also if C denotes the allowable wireless channel transmission capacity at a node in bits per second, we observe that the allowable broadcast rate p is limited by $p < C/N$, that is, inversely proportional to the number of vehicles. This in turn has an adverse effect on the latency with which traffic information is obtained and as a result the accuracy of the obtained traffic map information decreases with increasing vehicular density, which is not desirable.

To address these drawbacks, we propose to forward information about a vehicle at a rate that is proportional to the distance from that vehicle. Also, in *VCAST*, a vehicle suppresses forwarding of information about a vehicle in an interval, if some other vehicle has already forwarded information about the respective vehicle in that interval. By doing so, we show that the communication cost can be significantly reduced, leading to scalability. A more formal description of *VCAST* is presented below. A pseudocode in guarded command notation [40] is provided in Algorithm 1, which shows the program at each vehicle in the form of $\langle event \rightarrow action \rangle$ pairs.

In *VCAST*, each vehicle j maintains a list $j \cdot V$ of vehicles that are within a distance R from itself. Associated with each vehicle $i \in j \cdot V$ is the location $j \cdot X_i$ of i as most recently heard by j, a timestamp $j \cdot T_i$ associated with the location and $j \cdot \nu_i$ which is the number of times information about i has been heard since the last broadcast interval. A timer is fired at each vehicle every $1/p$ seconds for broadcasting information and a randomness is introduced in this interval because of CSMA based transmission. Let $\lambda = 1, 2, \ldots$ denote the timer sequence at vehicle j. Let $j \cdot V_\lambda$ denote the set of vehicles whose information is forwarded in the interval number λ at vehicle j. $j \cdot V_\lambda$ is initially set to be equal to $\{j\}$. Thus information about itself is broadcasted by a vehicle in every interval along with the current time which serves as the timestamp for this record. Node i is added into the set $j \cdot V_\lambda$ only if $\lambda \bmod d_h(i, j) = 0$ and if information about i has not been broadcasted by any other vehicle within j's range in the last $d_h(i, j)$ intervals. This ensures that information about nodes at a distance of k communication hops is broadcasted at most once every k interval in each communication neighborhood. In the presence of channel interference, we note that nodes may occasionally duplicate the transmission of information of a vehicle within a neighborhood. But we expect this to cause a much smaller overhead when compared with all nodes transmitting. Finally, whenever information about a vehicle i is heard by a node j, it is added to the list $j \cdot V$ if the timestamp of the incoming record is more recent than $j \cdot T_i$.

For the case where aggregate traffic information is to be propagated, each vehicle computes summary information such as density and average speed for the cell in which it resides based on the information it possesses about vehicles within its communication range. This summary is then propagated in a distance-sensitive manner: information about a cell at distance d_c is forwarded at a rate of p/d_c Hz.

3.3. Analysis

Theorem 1. *The average amount of data communicated per unit time by each node in VCAST to obtain information about all vehicles within a distance of R from itself is bounded by* $O(Rp/r_h)$.

Proof. Let B denote the average amount of data communicated per unit time, by each node in *VCAST*. We discretize distance in intervals of r_h (the communication range), as information forwarding rate decreases linearly after each time a vehicle's information is forwarded. The number of vehicles at a distance of at most hr_h away from a vehicle is bounded by $O(\rho h^2 r_h^2)$. The number of vehicles at a distance of at most $(h-1)r_h$ away from a vehicle is bounded by $O(\rho h^2 r_h^2)$. As a result, the number of vehicles between a distance of hr_h and $(h-1)r_h$ away from a vehicle is bounded by $O(\rho h r_h^2)$. Let us denote this as the distance interval h from the vehicle in terms of the communication range. Note that information about vehicles between a distance of hr_h and $(h-1)r_h$ is broadcasted only at p/h Hz. Thus the total amount of data to be communicated about vehicles in the distance interval of h is $O(\rho p r_h^2)$. Note that this information is broadcasted by at most one vehicle in every area πr_h^2. Hence, on average each node is responsible for communicating only $O(\rho p r_h^2 / \rho r_h^2)$ bits about vehicles at distance interval h from itself. Summing up over all distance intervals and by noting that each vehicle broadcasts its own state at p Hz, we get

$$B = O\left(p + \sum_{i=1}^{(R/r_h)} \frac{\rho p r_h^2}{\rho r_h^2}\right) = O\left(\frac{Rp}{r_h}\right). \quad (1)$$

□

Note that this result makes an assumption that information about nodes at a distance of k communication hops is broadcasted at most once every k intervals in each communication neighborhood. In the presence of channel contention

Protocol: VCAST
Vehicle: j
Var:
$j \cdot V$: List of vehicles within radius R
$j \cdot X_i \ \forall i \in V$: Location of i
$j \cdot T_i \ \forall i \in V$: Timestamp of i's record
$j \cdot \nu_i \ \forall i \in V$: Counter for i's information
$j \cdot \lambda$: Sequence number of current interval
$j \cdot V_\lambda$: Forwarding list for $j \cdot \lambda$
Actions:
$\langle A_1 \rangle$:: **Initialization:** $\longrightarrow$
$j \cdot V = j$; $j \cdot \nu_i = 0$; $j \cdot \lambda = 0$;
Timer.start $\left(\frac{1}{p}\right)$
$\langle A_2 \rangle$:: **Timer fired:** $\longrightarrow$
$j \cdot \lambda = j \cdot \lambda + 1$;
$j \cdot V_\lambda = j$;
$\forall i \in j \cdot V$
if $(\lambda \bmod d_h(i, j) == 0)$
if $j \cdot \nu_i < 2$
Add i to $j \cdot V_\lambda$
fi
$j \cdot \nu_i = 0$;
fi
$\forall i \in j \cdot V_\lambda$
Send $j \cdot X_i$, $j \cdot T_i$
$\langle A_3 \rangle$:: recv$_i(V)$ $\longrightarrow$
$\forall k \in i \cdot V$
if $\left(\left(j \cdot T_k < i \cdot T_k\right) \vee \left(k \notin j \cdot V\right)\right)$
$j \cdot X_k = i \cdot X_k$; $j \cdot T_k = i \cdot T_k$; $j \cdot \nu_k = 1$;
fi
elseif $\left(j \cdot T_k == i \cdot T_k\right)$
$j \cdot \nu_k = j \cdot \nu_k + 1$
fi

Algorithm 1: VCAST: protocol actions at vehicle j.

and hidden terminals, the assumption may be violated causing duplicate transmissions of vehicular information within a communication neighborhood and an increase in the amount of communication per node. The results of our simulation will include the impact of channel contention and duplicate transmissions.

Under a uniform distribution of vehicles in a 2d region, it can be inferred from the results of the previous theorem that the communication cost per node only grows as $O(p\sqrt{N})$. In contrast, without distance-sensitive forwarding the average communication incurred per node is $O(N)$, as discussed below.

Comparison with Multihop Broadcast Protocols without Distance Sensitivity. In order to analytically compare the bound on communication cost with multihop broadcast algorithms that do not incorporate distance sensitivity in message forwarding, first consider an algorithm in which information is simply flooded without suppression of redundant messages. In this case, each node broadcasts information about all nodes in the region at a rate of p times every second yielding a communication cost per node that is bounded by $O(\rho p R^2)$. This is clearly not scalable with the size of the network, and such an approach is likely to yield severe channel contention thus reducing the achievable broadcast rate p. Several heuristics have been proposed to address this broadcast storm problem so that redundant broadcasts of the same message can be eliminated; that is, information about every vehicle is broadcasted exactly once in every communication neighborhood per interval. In this case, the average communication cost reduces by a factor of $\rho\pi r_h^2$ over a naive flooding approach, yielding an average communication cost per node of $O(p(R/r_h)^2)$, that is, $O(pN)$. Thus, by comparison with Theorem 1, we see that the effective communication cost per node by applying distance-sensitive forwarding rules reduces by a factor of $\sqrt{N}$. Reducing the amount of communication incurred by each node results in smaller channel contention and allows a higher broadcast rate at smaller distances. This is especially crucial when forwarding information over large areas because it ensures that information supply rates at smaller distances are not penalized for having to forward information over multiple hops.

We now obtain a bound on how outdated the state information possessed by a vehicle is because of distance-sensitive forwarding. We refer to this as *staleness* in the information possessed by a vehicle.

Definition 2 (staleness (j,i)). The staleness $S(j,i,t)$ in the state of vehicle i as possessed by vehicle j at time t is the time elapsed since the timestamp of the state of $i(j \cdot T_i)$. Thus $S(j,i,t) = t - j \cdot T_i$.

Note that the staleness with respect to a vehicle is initially equal to the message latency from the source when information about the vehicle is received but continues to rise until the next update from the vehicle is received. The maximum staleness with respect to a vehicle thus occurs just before fresh information about the vehicle is received. Maximum staleness thus depends on the message latency as well as on the update interval. Staleness can further increase when messages containing information about a vehicle are lost. The effect of message losses will be quantified using simulations in Section 4.5.

Theorem 3. *The maximum staleness in the state of vehicle i at vehicle j in VCAST is bounded by* $O(d(i,j)^2/pr_h^2)$.

Proof. Consider a vehicle j at a distance between hr_h and $(h-1)r_h$ away from a vehicle i. Let us denote this by a distance-interval h from vehicle i in terms of the communication range r_h. Thus $h = \lceil d(i,j)/r_h \rceil$. Note that at a distance interval of $h-1$ from a vehicle i, information about i is updated only once every $h-1$ broadcast interval. As a result, the maximum time before which j hears fresher information about i from some vehicle at distance interval $h-1$ away from i is bounded by $(h-1)/p$ seconds. Likewise, the maximum time elapsed between a vehicle at distance-interval $h-2$ receiving information about i and a vehicle at distance-interval $h-1$ obtaining the same information is bounded by $(h-2)/p$ seconds. Summing from a distance interval of 1 to h, we get that the maximum latency in communicating the state of vehicle i to a vehicle j is bounded by $O(d(i,j)^2/pr_h^2)$. □

From Theorem 3, we note that the staleness at a distance d from a vehicle does not depend on the vehicular density or the region size, but only on the communication hop distance and the initial broadcast rate at the source. Hence, we expect that as the communication range increases the staleness should decrease. However, as the communication range increases, the interference within the vehicular transmission also increases and this can adversely affect the network reliability and system accuracy. In Section 4.5, we analyze the performance of our algorithm in large scale simulation and point out the impact of p and r_h on the staleness at different distances.

We now state the average communication rate and staleness when aggregate cell information is propagated instead of actual vehicle location information.

Theorem 4. *The amount of data communicated by each node in VCAST per unit time, when aggregate cell information is propagated, to obtain information about each cell at distance up to R from itself is bounded by* $O(Rp/\rho r_c r_h^2)$.

Proof. Let B_C denote the average amount of data communicated per unit time, by each node in *VCAST* when aggregate cell information is propagated. Recall that $d_c(i,j)$ denotes the *cell distance* between vehicle i and cell j, that is, the smallest number of cells traversed to reach cell j from i. The number of cells at a cell distance of at most d_c from a vehicle is bounded by $O(\rho d_c^2 r_c^2/\rho r_c^2)$, that is, $O(d_c^2)$. As a result, the number of cells at exactly distance d_c away from a vehicle is bounded by $O(d_c)$. Information about cells at distance d_c away is broadcasted at p/d_c Hz. Thus the total amount of data to be communicated about cells at distance d_c away is $O(p)$. Note that this information is broadcasted by at most one vehicle in every area πr_h^2. Hence, on average each node is responsible for communicating only $O(p/\rho r_h^2)$ bits about cells at distance d_c away from itself. Summing up over all cell distances from $d_c = 1$ to $d_c = R/r_c$, we get

$$B_c = O\left(\sum_{i=1}^{R/r_c} \frac{p}{\rho r_h^2}\right) = O\left(\frac{Rp}{\rho r_c r_h^2}\right). \quad (2)$$

□

In comparison with the result from Theorem 1, we note that the average communication rate reduces by a factor equal to the number of vehicles in each cell ($\rho r_c r_h$) because only aggregate information about the cell is propagated with distance-sensitive rate as opposed to propagating information about each vehicle in the cell.

Theorem 5. *The staleness in the state of cell z at vehicle j in VCAST, when aggregate cell information is propagated, is bounded by* $O(d_c(j,z)d_h(j,z)/p)$, *where* $d_h(j,z)$ *denotes the communication hop distance between j and the closest vehicle to j in cell z.*

Proof. Consider a vehicle j and cell z. The lowest broadcast rate about cell z that is available for vehicle j is $d_c(j,z)/p$. Also the number of communication hops between j and the closest vehicle in z is $d_h(j,z)$. Hence, latency in forwarding information about cell z to vehicle j is bounded by $d_c(j,z)d_h(j,z)/p$. Also note that the subsequent update about cell z will be available within $d_c(j,z)/p$ seconds. The result follows. □

4. Performance

We evaluate the performance of *VCAST* using simulations in ns-3, a discrete event simulator for wireless, and mobile ad hoc networks.

Network Models. We use an IEEE 802.11 b physical layer communication model with a DSSS rate of 11 Mbps at each node. We first model vehicular traffic by considering vehicles to be in grids of different sizes (28×28, 25×25, 20×20, and 15×15) with uniform separation between the vehicles at all times (i.e., traveling with uniform speed). For the case of aggregated data forwarding, we have also simulated a network size of

3600 nodes which allows us to test over larger intervehicular distances. We consider intervehicular separations of 60 m, 50 m, 40 m, and 30 m, thus simulating different densities. Note that a uniform separation of 45 m would correspond to a headway time of 1.5 s at a speed of 70 mph (and a proportionately lower headway time at lower speed), which are typically observed separations on roadways. We have chosen densities that create vehicular separation around this range. We also consider source broadcast rates of 1 Hz, 5 Hz, and 10 Hz, and communication ranges of 75 m, 100 m, 125 m, and 150 m, which are within the range of expected transmission rate and range values of *Here I am* messages for intelligent transportation systems [1, 2]. These simulations characterize the performance of *VCAST* when it is used to disseminate vehicular state information to a network of the corresponding size. The grid model allows us to emulate 2d network traffic of different densities in a region and by simulating uniform velocity, the relative distance between vehicles is maintained during the course of the simulation allowing the clear characterization of distance versus information staleness. We use this model to compare *VCAST* with non-distance-sensitive approaches and to systematically study the impact of density, source broadcast rates, and communication range on the performance. Next, we consider a 2d model of vehicles with nonuniform mobility incorporated—the goal here is to study if time varying densities impact the performance and therefore we use a random waypoint model to simulate mobility which generalizes possible vehicular traffic patterns.

Measurement Strategy. Each vehicle's state information is assumed to be 10 bytes long. In any given slot, a vehicle may transmit a variable number of such records. At each vehicle, we measure the maximum staleness with respect to every other vehicle by measuring the time elapsed since the information originated at the source, just before fresh information about a vehicle is received. For information aggregation, we consider the cell size to be equal to the communication range of each vehicle, propagate only aggregate cell information instead of individual vehicle information, and measure the maximum staleness with respect to every cell in the region. All simulations are run for 20 seconds except simulations at 1 Hz which are run for 40 second due to higher staleness values. We then group the maximum staleness based on pairwise distances between vehicle-vehicle and vehicle-cell, respectively. The average of these measurements over multiple experiments is used in our evaluations.

4.1. Impact of Distance Sensitivity. The objective of this section is to quantify the performance gains achieved by using distance-sensitive forwarding as opposed to forwarding information about all vehicles at the same rate.

Scaling in Number of Nodes. In Figure 2(a), we show the maximum staleness as a function of intervehicular distance for $p = 10$ Hz at a network size of 225 nodes for both *VCAST* as well as non-distance-sensitive forwarding; that is, information about all vehicles is forwarded at the source broadcast rate by every node. Here, we observe that the non-distance-sensitive scheme is able to keep staleness low at all distances and the growth is linear with distance. On the other hand, *VCAST* has low staleness at small distances while the staleness is observed to grow as $O(d^2)$ at higher distances, as expected. However, at a network size of 625 (see Figure 2(b)), the non-distance-sensitive approaches show much higher staleness even at smaller distances. However, *VCAST* is able to maintain low staleness at small distances while the staleness is observed to grow as $O(d^2)$ at higher distances. Information within 400 m is obtained in under 300 ms using *VCAST* while it takes about 3 seconds in the case of a non-distance-sensitive approach. The reason is that as the number of nodes increases, the channel contention increases at a much higher rate in the non-distance-sensitive forwarding causing message losses and consequently increase in staleness (i.e., quantified in our analysis on message complexity). By reducing channel contention, *VCAST* is able to achieve scalability in number of nodes. In Figure 3, we show the maximum staleness as a function of intervehicular distance for $p = 10$ Hz at a network size of 225, 400, 625, and 784 nodes for *VCAST*. *We observe that staleness values are preserved at corresponding intervehicular distances, irrespective of network size.*

Scaling in Source Broadcast Rate. In Figures 4(a) and 4(b), we fix the network size to 784 nodes and vary the source broadcast rate. In Figure 4(a), we observe that, at s source broadcast rate of 1 Hz, the-non-distance-sensitive scheme is able to scale to large distances and has lower latencies at larger distances compared with *VCAST* since there is no staggered forwarding. *However, when attempting to reduce the staleness at smaller distances, by increasing the source broadcast rate, non-distance-sensitive forwarding fails.* This is shown in Figure 4(b) for broadcast rates of 10 Hz. The non-distance-sensitive approaches show much higher staleness even at smaller distances. On the other hand, *VCAST* is able to deliver lower staleness at smaller distances even at a network size of 784 nodes by increasing the source broadcast rate and progressively increasing the staleness at larger distances. *This allows the network bandwidth to be utilized where it is needed and to achieve scalability.*

Message Complexity: The Reason Behind Successful Scaling in VCAST. In Figures 5(a) and 5(b), we show the number of vehicular records transmitted per second by every node for varying network sizes and varying source broadcast rates, respectively. These figures highlight the significantly lower message complexity in *VCAST* which reduces the contention even as network size and broadcast rates grow.

4.2. Impact of Communication Range, Source Broadcast Rate, and Density. In this subsection, we evaluate the performance of *VCAST* under different communication ranges, source broadcast rate, and network densities. The aim is to highlight the scalability of *VCAST* and identify the *tipping point* in

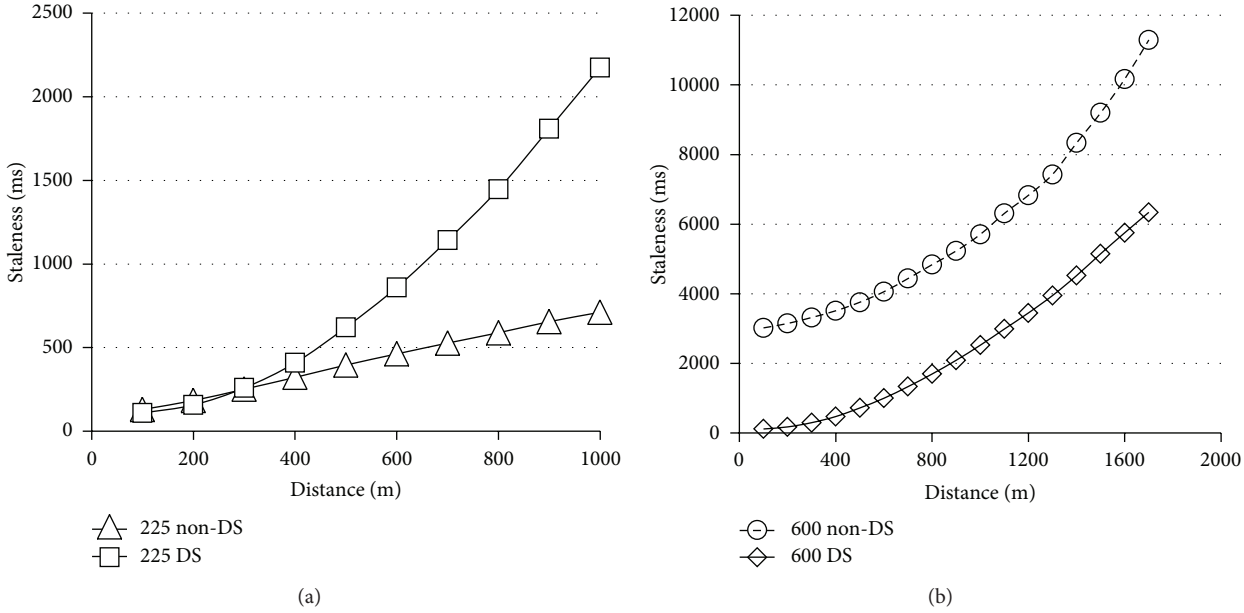


FIGURE 2: Impact of network size: *VCAST* versus non-distance-sensitive forwarding. (a) Maximum staleness versus pairwise vehicular distance: $p = 10$ Hz at 225 nodes. (b) Maximum staleness versus pairwise vehicular distance: $p = 10$ Hz at 625 nodes.

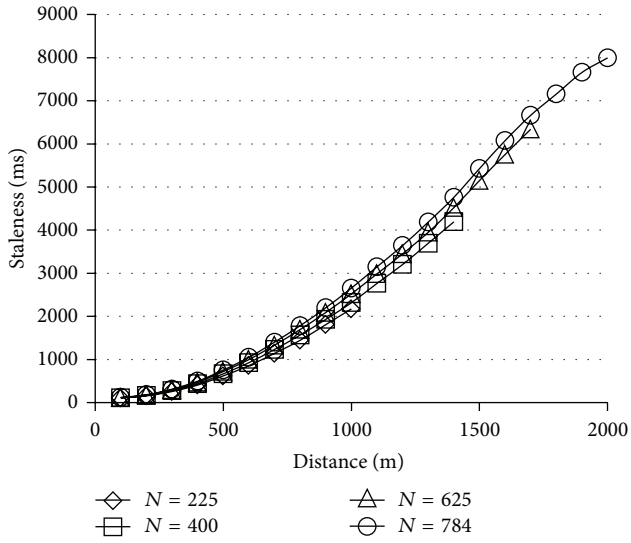


FIGURE 3: Maximum staleness versus pairwise vehicular distance for *VCAST*: $p = 10$ Hz, network sizes of 225, 400, 625 and 784 vehicles, communication range 100 m, separation 50 m. Staleness values are preserved at corresponding intervehicular distances, irrespective of network size.

terms of each of these parameters for *VCAST*, that is, the point at which channel capacity is exceeded.

Communication Range. In Figure 6, we plot the maximum staleness in vehicle information against the intervehicular distance for a 784 node network with $p = 10$ Hz at different communication ranges. As range increases from 75 m to 125 m, we observe that staleness at larger distances decrease (due to fewer number of hops), while the staleness at smaller distances increase slightly due to increased contention. However, starting from a range of 150 m, we observe that the channel contention within a single hop starts increasing and at a range of 200 m, we observe a tipping point leading to higher message losses and much higher staleness at smaller distances (the corresponding plot is shown in red).

Source Broadcast Rate. In Figure 7(a), we plot the maximum staleness in vehicle information against the intervehicular distance for a 784 node network with a communication range of 100 m for different source broadcast rates. As rate increases from 5 Hz to 10 Hz, we observe that staleness decreases as expected. However, with a rate of 20 Hz, we observe that the channel contention starts increasing, leading to disproportionate staleness values at smaller distances. Figure 7(b) shows a zoomed-in version of Figure 7(a) at smaller distances. Here, we observe that staleness values for 20 Hz are higher than those at 10 Hz due to higher channel contention.

Network Density. In Figure 8(a), we plot the maximum staleness in vehicle information against the intervehicular distance for a 784 node network with a communication range of 100 m and rate of 10 Hz for different intervehicular separations. Note that, in Figure 8(a), the plots for separations of 50 m, 40 m, and 30 m only extend to 2, 1.7, and 1.2 Km, respectively, because these are the possible maximum intervehicular distances at the corresponding densities for a given network size of 784 vehicles. We observe that going from a separation of 60 m to 40 m, the staleness at larger distances decreases. This is because of fewer number of *hops* required to reach a given distance. However, with a separation of 30 m, we observe that channel capacity is exceeded causing message losses and higher staleness values (the corresponding plot is shown in red). In Figure 8(b), we have shown the

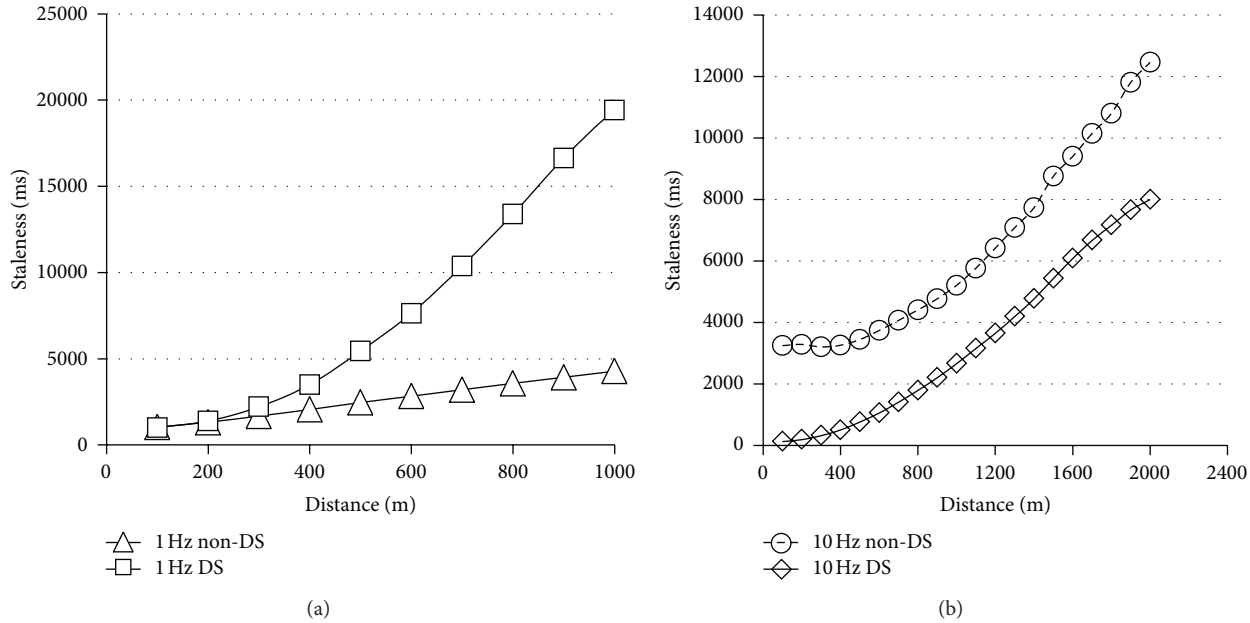


Figure 4: Impact of source broadcast rate: *VCAST* versus non-distance-sensitive forwarding. (a) Maximum staleness versus pairwise vehicular distance: p = 1 Hz at 784 nodes. (b) Maximum staleness versus pairwise vehicular distance: p = 10 Hz at 784 nodes.

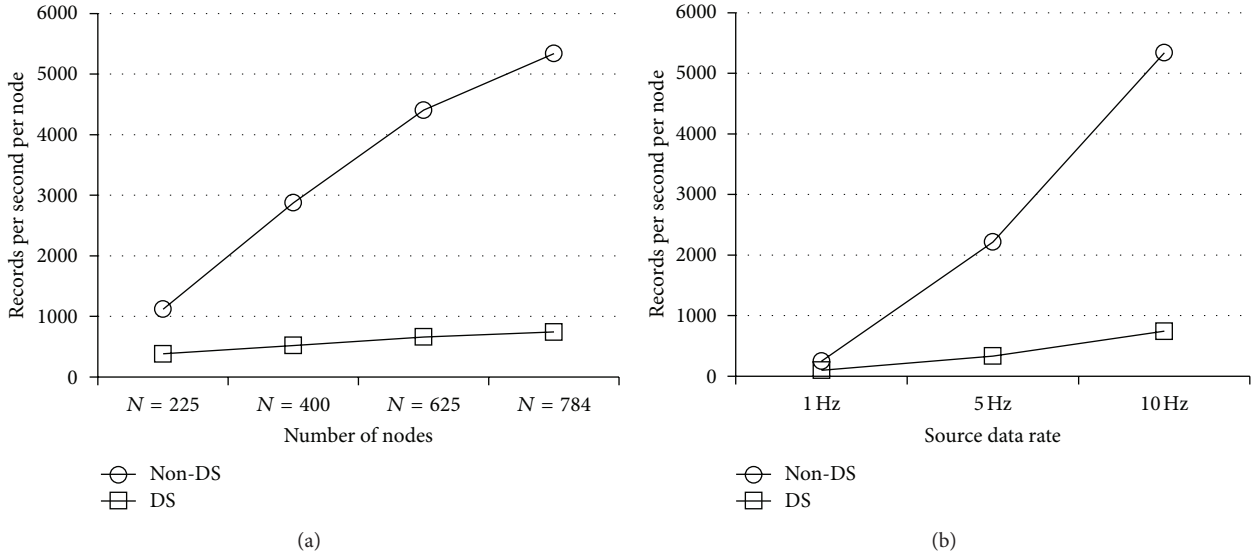


Figure 5: Comparison of message complexity: *VCAST* versus non-distance-sensitive forwarding. (a) Number of vehicular records transmitted per second per node at different network sizes for p = 10 Hz and range 100 m. (b) Number of vehicular records transmitted per second per node at different source broadcast rates for 784 nodes and range 100 m.

corresponding message complexity at different intervehicular separations. Here we observe a drastic increase in messages per second, at a separation of 30 m which explains the corresponding increase in message losses and information staleness.

4.3. Impact of Time Varying Intervehicular Separations. The aim of this subsection is to characterize the performance of *VCAST* in the presence of time varying intervehicular separations caused by nonuniform mobility patterns. We note that there are potentially several traffic mobility patterns that can arise in a real vehicular network scenario. Our goal here is to analyze the scalability of *VCAST* and one of the important underlying factors that can impact performance in the context of these mobility patterns is the time varying density. There could be instants when a vehicle has a lot of neighbors within communication range and also instances when there are no neighbors. Therefore, in this simulation, we have chosen the *random 2d walk mobility pattern* with time varying speeds in the range of 20 m/s to 40 m/s, a potentially

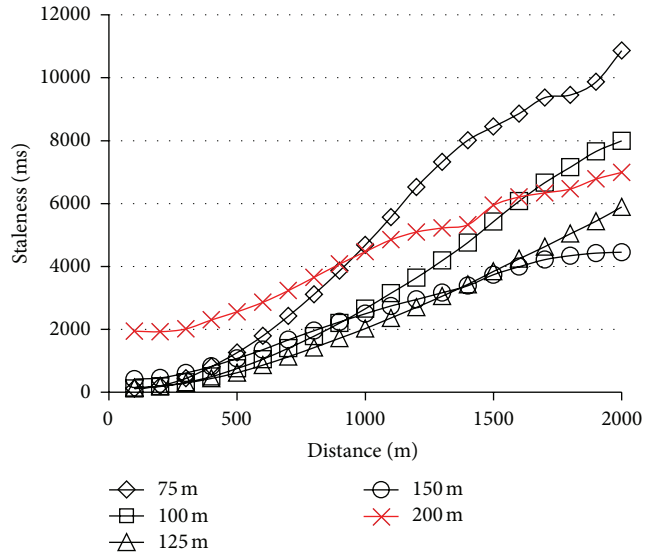


FIGURE 6: Impact of communication range on *VCAST*: maximum staleness versus pairwise vehicular distance for *VCAST*: p = 10 Hz, 784 vehicles, separation 50 m, communication range 75 m, 100 m, 125 m, 150 m, and 200 m.

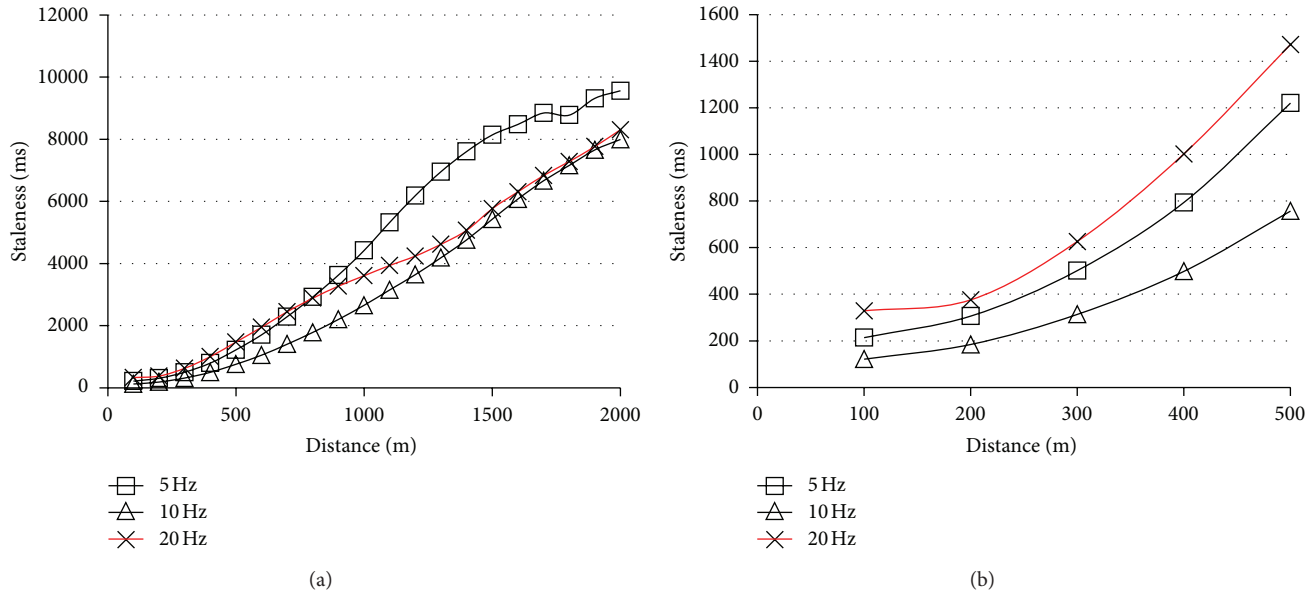


FIGURE 7: Impact of source broadcast rate on *VCAST*: (a) maximum staleness versus pairwise vehicular distance with 784 vehicles, separation 50 m, communication range 100 m, source broadcast rates of 5 Hz, 10 Hz, and 20 Hz. (b) Zoomed-in version at smaller distances.

severe form of mobility that captures the essence of time varying separations and interference zone, caused in a traffic scenario.

In Figures 9(a) and 9(b), we compare the information staleness graphs for the random and uniform mobility patterns at 5 Hz and 10 Hz source broadcast rates with 784 nodes. As seen from these figures, the graphs are quite similar, highlighting that random mobility does not significantly impact the performance. Staleness values at larger distances are observed to be slightly higher for the case of random mobility. However, the reason for this is not higher communication cost but rather the fact that the severe random mobility scenario often creates sparse and disconnected regions within the network, thereby increasing the number of hops traversed between two vehicles at a given distance. This effect is more pronounced at larger distances.

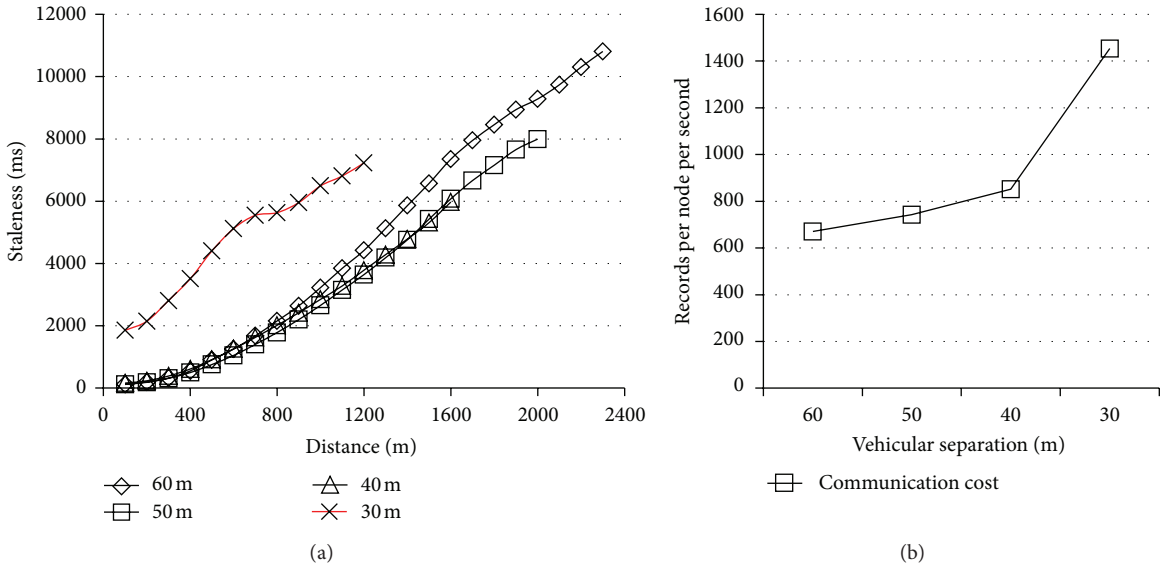


FIGURE 8: Impact of network density on *VCAST*: (a) maximum staleness versus pairwise vehicular distance with 784 vehicles, Communication range 100 m, source broadcast rat 10 Hz, separation 60 m, 50 m, 40 m, and 30 m. (b) Number of vehicular records transmitted by each node per second with 784 vehicles, communication range 100 m, source broadcast rat 10 Hz, separation 60 m, 50 m, 40 m, and 30 m.

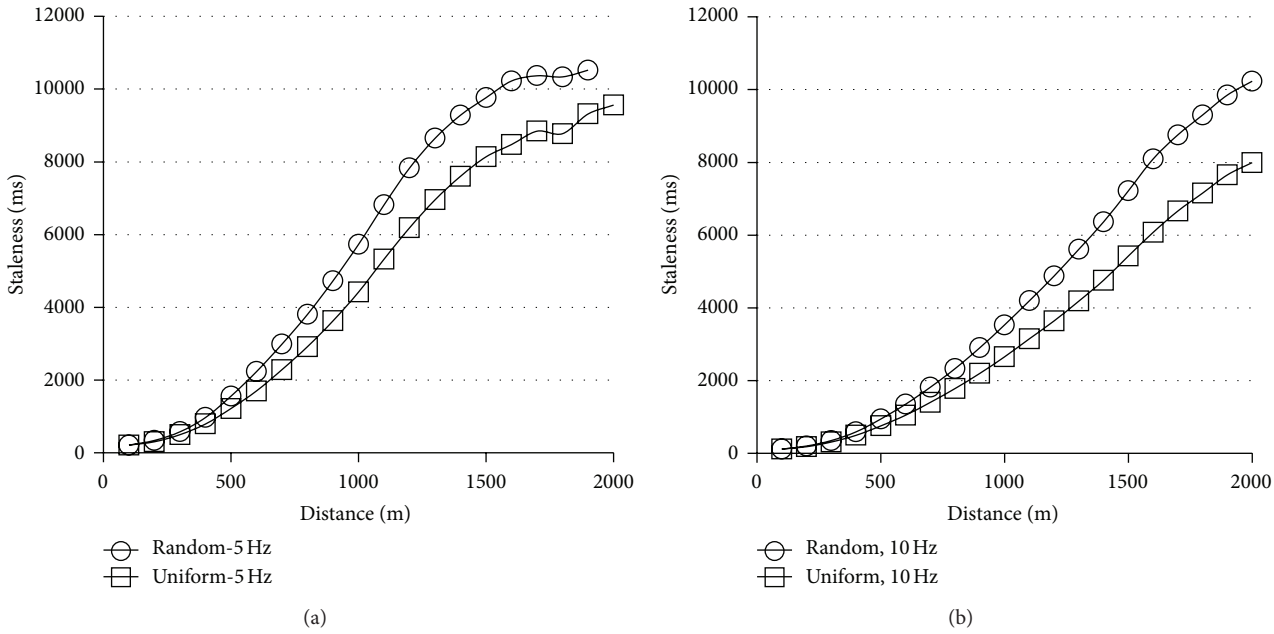


FIGURE 9: Impact of time varying random mobility pattern on *VCAST*: (a) maximum staleness versus pairwise vehicular distance for uniform and random mobility with 784 vehicles, communication range 100 m, source broadcast rate 5 Hz. (b) Maximum staleness versus pairwise vehicular distance for uniform and random mobility with 784 vehicles, communication range 100 m, source broadcast rate 10 Hz.

In Figure 10, we compare the average communication cost for the random and uniform mobility scenarios. This graph highlights the fact that communication costs do not increase in the random mobility scenario—in fact a small decrease is observed in the average communication cost over several random patterns.

4.4. Impact of Aggregation. In this section, we evaluate *VCAST* when aggregate information about a cell is transmitted over multiple hops as opposed to individual vehicle information. The region being simulated is divided into square *cells* of equal size. The width of each cell is assumed to be equal to the single hop communication range. In

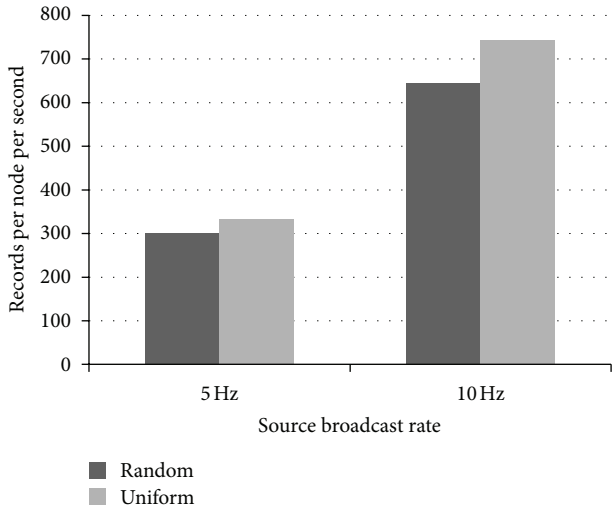


Figure 10: Impact of time varying random mobility pattern on *VCAST* (comparison of communication cost): number of vehicular records transmitted by each node per second at 5 Hz and 10 Hz source broadcast rates under uniform and random mobility patterns.

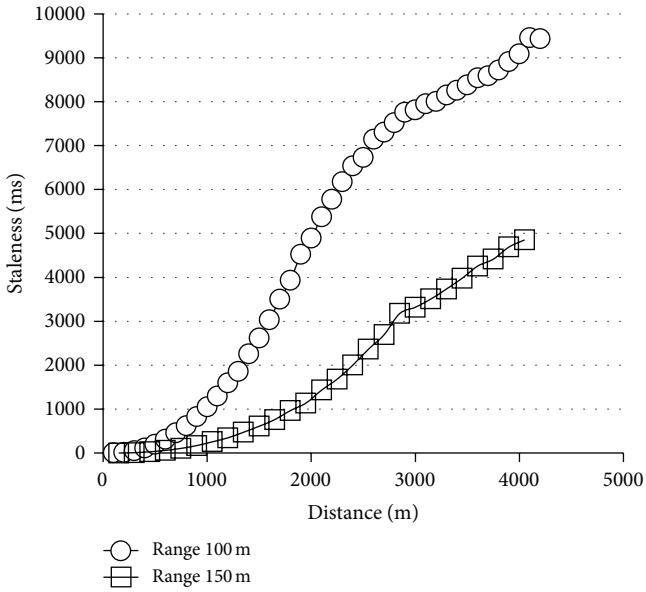


Figure 11: Impact of aggregation on *VCAST*: maximum staleness versus vehicle-cell distance with 3600 vehicles, source broadcast rat 10 Hz, communication range 100 m and 150 m.

this evaluation, we have increased the network size to 3600 nodes, thereby allowing us to evaluate staleness over larger distances. Figure 11 shows the information staleness graphs with a communication range of 100 m ad 150 m, both with a source broadcast rate of 10 Hz. As seen in these graphs, information up to 4 Km can be obtained in less than 5 seconds, without the need for any infrastructure—while still maintaining extremely low staleness values at smaller distances.

4.5. Summary of Results. Our experimental results show that by using distance-sensitive forwarding, *VCAST* is able to scale to larger network size as well as support much higher broadcast rates compared to non-distance-sensitive techniques. The reason for scalability is the significantly lower message overhead which reduces the channel contention in the network. We also characterized the performance of*VCAST* under severe mobility and studied information staleness when aggregated data is transmitted as opposed to individual vehicle information.

From all of the above experimental evaluations, we note that an ideal parameterization for *VCAST* is to set communication range to a small value and increase the source broadcast rate. By doing so, information at smaller distances can be obtained at high rates with low contention due to the small communication range. At the same time, information to larger distances can be transmitted with progressively increasing staleness. Moreover, by limiting the propagation of individual vehicular information up to distances of about 500–1000 m (for utilization by safety applications) and only propagating aggregate information beyond that, we observe that information from several miles ahead can be obtained within a few seconds without the need for any communication infrastructure.

5. Conclusions

We have presented an algorithm,*VCAST*, for obtaining individual vehicle location and aggregate traffic information over a multihop wireless vehicular network without the need for expensive roadside infrastructure, any special hardware, or modification to vehicular transmission standards. To ensure scalability in forwarding information over multiple hops, traffic information is propagated at a rate that decreases linearly with distance from the source. By doing so, the required communication rate per node can be reduced when compared with schemes that do not utilize distance sensitivity in information forwarding. This results in lower channel contention, thereby enabling higher source broadcast rates and better information quality at smaller distances while still being able to propagate information to large distances. Despite staggered forwarding, traffic information can be obtained with a staleness, which is a measure of error in the traffic information that is bounded by $O(d^2)$ where d is the communication hop distance from the source of the information.

The performance of *VCAST* was validated using extensive ns-3 simulation under different network sizes, network densities, source broadcast rates, and communication ranges. The results of our evaluation showed that by using distance-sensitive forwarding, *VCAST* is able to scale to larger network sizes as well as support much higher broadcast rates compared to non-distance-sensitive techniques. The reason for scalability was shown to be the significantly lower message overhead which reduces the channel contention in the network. We also characterized the performance of *VCAST* under severe mobility and studied information staleness

when aggregated data is transmitted as opposed to individual vehicle information.

In future work, we would like to integrate *VCAST* with control algorithms for vehicular safety and navigation that utilize information with distance-sensitive quality. We would like to design optimal control laws for vehicular acceleration under models of distance-sensitive information availability that ensures the safety of the integrated control-communication system. We would also like to integrate our vehicular traffic mapping service with a navigation front end for dynamic computation of alternate routes and evaluate the impact of distance sensitivity on the quality of navigation performance.

References

[1] Y. P. Fallah, C. Huang, R. Sengupta, and H. Krishnan, "Design of cooperative vehicle safety systems based on tight coupling of communication, computing and physical vehicle dynamics," in *Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS '10)*, pp. 159–167, April 2010.

[2] U. S. Department of Transportation, "Achieving the vision: from VII to IntelliDrive," Policy white paper, 2010.

[3] V. Kulathumani and Y. Fallah, "Vcast: an infrastructure-less vehicular traffic information service with distance sensitive precision," in *Proceedings of the IEEE Vehicular Technology Conference (VTC '12)*, 2012.

[4] Y. Liu and F. Dion, "Safety assessment of information delays on intelligent vehicle control system performance," Proceedings of Transportation Research Board Conference, 2006.

[5] V. Kulathumani and A. Arora, "Aspects of distance sensitive design of wireless sensor networks," in *Proceedings of the IEEE Workshop on Spatial Computing*, October 2008.

[6] V. Kulathumani, A. Arora, and S. Ramagiri, "Pursuit control over wireless sensor networks using distance sensitivity properties," *IEEE Transactions on Automatic Control*, vol. 56, no. 10, pp. 2473–2478, 2011.

[7] F. Li and Y. Wang, "Routing in vehicular ad hoc networks: a survey," *IEEE Vehicular Technology Magazine*, vol. 2, no. 2, pp. 12–22, 2007.

[8] K. C. Lee, U. Lee, and M. Gerla, "Survey of routing protocols in vehicular ad hoc networks," in *Advances in Vehicular Ad-Hoc Networks: Developments and Challenges*, pp. 149–170, IGI-Global, 2009.

[9] Y.-W. Lin, Y.-S. Chen, and S.-L. Lee, "Routing protocols in vehicular Ad Hoc networks: a survey and future perspectives," *Journal of Information Science and Engineering*, vol. 26, no. 3, pp. 913–932, 2010.

[10] J. Zhao and G. Cao, "VADD: vehicle-assisted data delivery in vehicular ad hoc networks," in *Proceedings of the 25th IEEE International Conference on Computer Communications*, April 2006.

[11] C. Lochert, M. Mauve, H. Fera, and H. Hartenstein, "Geographic routing in city scenarios," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 9, no. 1, pp. 69–72, 2005.

[12] Y.-S. Chen, Y.-W. Lin, and C.-Y. Pan, "DIR: diagonal-intersection-based routing protocol for vehicular ad hoc networks," *Telecommunication Systems*, vol. 46, no. 4, pp. 299–316, 2011.

[13] V. Naumov and T. R. Gross, "Connectivity-aware routing (CAR) in vehicular ad hoc networks," in *Proceedings of the 26th IEEE International Conference on Computer Communications*, pp. 1919–1927, May 2007.

[14] T. Taleb, E. Sakhaee, A. Jamalipour, K. Hashimoto, N. Kato, and Y. Nemoto, "A stable routing protocol to support ITS services in VANET networks," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3337–3347, 2007.

[15] W. Sun, H. Yamaguchi, K. Yukimasa, and S. Kusumoto, "GVGrid: a QoS routing protocol for vehicular ad hoc networks," in *Proceedings of the 14th IEEE International Workshop on Quality of Service (IWQoS '06)*, pp. 130–139, June 2006.

[16] A. Skordylis and N. Trigoni, "Delay-bounded routing in vehicular ad-hoc networks," in *Proceedings of the 9th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 341–350, May 2008.

[17] H. P. Joshi, M. Sichitiu, and M. Kihl, "Distributed robust geocast multicast routing for inter-vehicle communication," in *Proceedings of the WEIRD Workshop on WiMax, Wireless and Mobility*, 2007.

[18] H. Lu and C. Poellabauer, "Balancing broadcast reliability and transmission range in VANETs," in *Proceedings of the IEEE Vehicular Networking Conference (VNC '10)*, pp. 247–254, December 2010.

[19] M. Torrent-Moreno, J. Mittag, P. Santi, and H. Hartenstein, "Vehicle-to-vehicle communication: fair transmit power control for safety-critical information," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 7, pp. 3684–3703, 2009.

[20] L. Cheng and R. Shakya, "VANET Adaptive power control from realistic propagation and traffic modeling," in *Proceedings of the IEEE Radio and Wireless Symposium*, pp. 665–668, January 2010.

[21] L. Yang, J. Guo, and Y. Wu, "Channel adaptive one hop broadcasting for VANETs," in *Proceedings of the 11th International IEEE Conference on Intelligent Transportation Systems (ITSC '08)*, pp. 369–374, December 2008.

[22] C. Chigan and J. Li, "A delay-bounded dynamic interactive power conftol algorithm for VANETs," in *Proceedings of the IEEE International Conference on Communications (ICC '07)*, pp. 5849–5855, June 2007.

[23] A. Bachir and A. Benslimane, "A multicast protocol in ad hoc networks inter-vehicle geocast," in *Proceedings of the 57th IEEE Semiannual Vehicular Technology Conference (VTC '03)*, pp. 2456–2460, April 2003.

[24] Y.-S. Chen, Y.-W. Lin, and S.-L. Lee, "A mobicast routing protocol in vehicular Ad-Hoc networks," *Mobile Networks and Applications*, vol. 15, no. 1, pp. 20–35, 2010.

[25] M. N. Mariyasagayam, T. Osafune, and M. Lenardi, "Enhanced multi-hop vehicular broadcast (MHVB) for active safety applications," in *Proceedings of the 7th International Conference on Intelligent Transport Systems Telecommunications (ITST '07)*, pp. 223–228, June 2007.

[26] J. Fukuyama, "A probabilistic protocol for multi-hop routing in VANETs," in *Proceedings of the IEEE International Conference on Communications Workshops*, June 2009.

[27] D. Kumar, A. A. Kherani, and E. Altman, "Route lifetime based optimal hop selection in VANETs on highway: an analytical viewpoint," in *Proceedings of the International IFIP-TC6 Networking Conference*, 2006.

[28] T. Fukuhara, T. Warabino, T. Ohseki et al., "Broadcast methods for inter-vehicle communications system," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '05)*, pp. 2252–2257, March 2005.

[29] F. Bai, D. D. Stancil, and H. Krishnan, "Toward understanding characteristics of Dedicated Short Range Communications (DSRC) from a perspective of vehicular network engineers," in *Proceedings of the 16th Annual Conference on Mobile Computing and Networking (MobiCom '10)*, pp. 329–340, September 2010.

[30] S. Ni, Y. Tseng, Y. Chen, and J. Sheu, "The broadcast storm problem in a mobile ad hoc network," in *Proceedings of the ACM/IEEE international conference on Mobile computing and networking*, 1999.

[31] B. Williams and T. Camp, "Comparison of broadcasting techniques for mobile ad hoc networks," in *Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '02)*, pp. 194–205, June 2002.

[32] L. Peterson and B. Davie, *Computer Networking: A Systems Approach*, Elsevier, 2011.

[33] G. Pei, M. Gerla, and T.-W. Chen, "Fisheye state routing in mobile Adhoc networks," in *Proceedings of the ICDCS Workshop on Wireless Networks*, pp. 71–78, June 2000.

[34] F. Dehne, A. Ferreira, and A. Rau-Chaplin, "Parallel fractional cascading on hypercube multiprocessors," *Computational Geometry*, vol. 2, no. 3, pp. 141–167, 1992.

[35] S. Funke, L. Guibas, and Y. Zhang, "Distance sensitive information brokerage in sensor networks," in *Proceedings of the International Conference on Distrbuted Computing in Sensor Systems (DCOSS '06)*, pp. 234–251, Springer, 2006.

[36] M. Demirbas, A. Arora, and V. Kulathumani, "Glance: a lightweight querying service for wireless sensor networks," *Theoretical Computer Science*, vol. 410, no. 6-7, pp. 500–513, 2009.

[37] V. Kulathumani, A. Arora, M. Sridharan, and M. Demirbas, "Trail: a distance-sensitive sensor network service for distributed object tracking," *ACM Transactions on Sensor Networks*, vol. 5, no. 2, pp. 1–40, 2009.

[38] J. Gao, L. J. Guibas, J. Hershberger, and L. Zhang, "Fractionally cascaded information in a sensor network," in *Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks (IPSN '04)*, pp. 311–319, April 2004.

[39] V. Kulathumani and A. Arora, "Distance sensitive snapshots in wireless sensor networks," in *Principles of Distributed Systems*, vol. 4878, pp. 143–158, 2007.

[40] E. W. Dijkstra, "Self-stabilizing systems in spite of distributed control," *Communications of the ACM*, vol. 17, no. 11, 1974.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 853014, 11 pages
http://dx.doi.org/10.1155/2013/853014

Research Article

MCNC: Data Aggregation and Dissemination in Vehicular Ad hoc Networks Using Multicast Network Coding

Lingzhi Li,[1] Shukui Zhang,[1,2] Yanqin Zhu,[1] and Zhe Yang[1]

[1] *School of Computer Science & Technology, Soochow University, Suzhou 215006, China*
[2] *State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093, China*

Correspondence should be addressed to Shukui Zhang; zhangsk2000@163.com

Received 12 April 2013; Accepted 4 September 2013

Academic Editor: Liusheng Huang

Nowadays, more and more APs are deployed for the wireless access. The roadside APs are able to improve the bandwidth of VANETs. In this paper, we design a Multicast Network Coding (MCNC) method to aggregate and disseminate data in VANETs. It is appropriate for the areas where APs have been deployed but cannot cover the all range of vehicles movement. Data transmission is divided into 3 stages in MCNC. Network coding, multicast aggregating, and decoding are implemented in the 3 stages, respectively. Simulation results show that MCNC is able to cut down 2/3 overhead messages of Epidemic when the cover area of the APs is only 1/5. Its loss rate and delay are lower than the other methods. We also discuss its benefit for the deployment of VANETs.

1. Introduction

Vehicular networks are usually regarded as a class of ad-hoc networks, where mobile nodes are vehicles exchanging data with each other. Vehicle can communicate with nearby vehicles when their distance is less than the communication range. Data are delivered among vehicles via Vehicle-to-Vehicle (V2V) protocol. Vehicular Ad hoc Networks (VANETs) will diverse applications associated with traffic safety [1], traffic efficiency [2], entertainment, file sharing [3, 4], and so on [5]. However, vehicles move at different speeds and form dynamic networks over time. VANET changes so fast; it is often difficult to find a path between a pair of vehicles using ordinary ad hoc routing protocol. Epidemic is the high reliability protocol, but it will waste too much bandwidth and reduce the scalability of networks [6].

Deploying infrastructures is a method to improve the reliability of data delivery. Intelligent VANET is a way of integrating on multiple wirelesses such as IEEE 802.11, 3G cellular systems, and IEEE 802.16e in vehicular networks [7]. Vehicles communicate with roadside infrastructures via Vehicle-to-Infrastructure (V2I) protocol. The infrastructures are connected via the wired networks and are able to buffer more data than vehicles. The experiments in [8] show that the deployment of infrastructures can bring up to the improvement of performance in delivery ratio. With the increasing use of smart phones, 3G cellular systems become a popular infrastructure, but the research in [9] suggests that cellular data bandwidth is likely to remain limited and expensive. With the recent development of the IEEE 802.11p [10] 5.9G DSRC/WAVE radios, Wi-Fi based Access Points (APs) on the side of road will be more as the infrastructures of VANETs.

Most applications of VANETs focus on planning vehicle paths, such as detecting remote road conditions [11]; sensing traffic lights [12]; avoiding rear collisions [10]. These applications require disseminating data to part of vehicles in some regions. The receivers are dynamic and cannot be identified by senders because of vehicles constant movement. It is impossible that infrastructures signal covers all of regions reached by vehicles. Multihop communications among vehicles are necessary to destinations or infrastructures. So routing packet remains to be a challenge in such network architecture which integrates V2V communication with V2I communication. However, vehicle movements are constrained to roads. Even though lots of vehicles are equipped with GPS receivers or smart phones to define their routes, their movements are probably constrained to preset paths. It is another characteristic of VANETs that it is possible to predict the vehicle movement [13].

In this paper, we present a Multicast Network Coding (MCNC) method to aggregate and disseminate data in VANETs. Data are divided into short fixed-size blocks in source vehicle and disseminated to the other vehicles. The vehicles nearby APs implement network coding and send the coding blocks to APs. The blocks are aggregated and recoded among APs multicast tree. Finally, the blocks are sent out in APs that the destinations are predicted to close. The experiments show that MCNC is able to reduce overhead messages and enhance the reliability of transmission. MCNC is designed according to the former characteristic of VANETs and appropriate for the areas that Wi-Fi based APs have been set up but cannot cover entirely.

The remainder of this paper is organized as follows. In the next section, we discuss the related work. Section 3 presents the description and implementation of the MCNC. The evaluation and analysis of the MCNC are showed in Section 4. The paper is concluded in Section 5.

2. Related Works

In recent years, many studies focus on deploying infrastructures in VANETs. It is proved [8] to bring up the improvement of data delivery. Cabernet [14] proposes one-hop Internet access schemes using open Wi-Fi based APs in VANETs. In [15], Bychkovsk et al. analyze the feasibility that vehicles can access open Wi-Fi based APs providing the wired network connections in VANETs. They define the prime method of data delivery from APs to vehicles. Throwboxes [16] as infrastructures can hold packets and later forward the packets to other nodes. It helps relay messages between mobile clients in a Delay Tolerant Network (DTN) and saves power in scheduling sleep. MAR [17] as an infrastructure is a commuter router that exploits wireless diversity to provide improved data for users. It can be placed in moving vehicles to enable high-speed data access. DP [18] on the roadside is proposed to address the data dissemination in VANETs. Data poured from the source are buffered and rebroadcast at the intersections. It focuses on data dissemination, and no buffer allocation scheme is proposed. MobTorrent [19] is a framework designed for vehicles accessing to roadside Wi-Fi APs. Vehicles inform the selected APs to fetch data. The scheduling algorithm in MobTorrent replicates the data on mobile helpers.

A few studies have been attracted on utilizing vehicle trajectory information for VANETs of deploying APs. More and more vehicles are equipped with satellite navigation systems. With increasing usage of smart phones like Apple iPhone or Android phones, navigation systems based on smart phones are popular. Vehicle trajectory information has become a valuable input for data forwarding. In [20], a protocol is proposed to enable efficient multihop routing capabilities. It fully supports two-way communications between mobile vehicles and APs. Vehicular mobility is predicted on the information offered by the navigation system in terms of final destination and path. TSF [21] considers a reliable, efficient APs-to-vehicles data delivery by minimizing the packet delivery delay. Data delivery is performed through the computation of a target point based on the destination vehicle's trajectory information. Roadside APs can be selected as relays where destination vehicle is expected to pass by. Selecting AP optimally minimizes the packet delivery delay. TBD [22] utilizes vehicle trajectory information to improve communication delay and delivery probability for vehicles-to-APs destination communications. A delay model of packets routing along roads is set up. The path with minimum delay can be found with the help of the real-time traffic condition information.

There is also some research leveraging roadside parking to distribute data in VANETs. ParkCast [23, 24] assumes that the parked vehicles are grouped into a line cluster at roadside. It defines the communication between moving vehicles and parked ones. The wireless device on vehicles has a battery for supporting the communication in parking. APs are replaced by parked vehicles to delivery data in VANETs. PASS [2] is a parking-lot-assisted carpool method. It optimizes transport utilization by sharing ride among drivers. A user can get vehicles information from the drivers in PASS. The drivers decide whether to provide carpooling services or not. In fact, many V2V protocols are also able to be used as vehicles-to-APs communications. Epidemic Routing [25] is the first proposed to reliably deliver messages in intermittently connected networks. It is not optimized for the VANETs. PRoPHET [26] was proposed to select the next hops using the history of encounters. Both of them are used as the typical protocols of VANETs and will be analyzed in our simulation.

Network coding has been proven to be a promising approach that can improve the reliability of communication. A few studies focus on using network coding in VANETs. CodeTorrent [27] is a file swarming protocol based on network coding for VANETs. It deals with typical mobile network issues such as dynamic topology and intermittent connectivity. CodeOn [28] is a push-based scheme for popular content distribution in VANETs. Data are actively broadcasted to vehicles from APs and further distributed among vehicles. It uses network coding to reduce the lossy of data. In [29], M. Sathiamoorthy et al. analyze the benefits of distributed storage using erasure codes for file sharing in VANETs. Distributed storage codes not only offer the reduction of bandwidth occupied by large file copy but also provide significant reduction of cost in VANETs. In [30], Palma et al. propose a data dissemination technique based on Fountain codes. Its goal is provide the real-time service in a lossy vehicular network. It achieves an improvement on arrival times of packets towards destination vehicles. The works adopt network coding to handle content distribution in VANETs and are referred for coding and transmission of this paper.

3. MCNC and Its Implementation

The process of information delivery is similar in the network architectures which integrate V2V with V2I communication. The sources firstly forward data to infrastructures in multi-hop communications among vehicles. Data are transmitted in wired networks formed by infrastructures and then are sent

from a few infrastructures to the destinations in multihop wireless communications. In our MCNC method, we define the 3 stages as ToInfra, BeInfra, and ToVehic.

In this section, we present, respectively, the method of data transmission on the 3 stages of MCNC. It firstly composes network coding and multicast to aggregate data in VANET.

3.1. ToInfra Stage. Data dissemination is unreliable when information is announced by the source far away from infrastructures. Before the vehicle is able to contact with infrastructures, the generic routing algorithm for VANETs is used among vehicles. We select the epidemic routing in this moment to describe our method. When vehicles sense a route to infrastructures, they will aggregate and send out data in the way of network coding. If data meet part of destinations in epidemic routing [26], they will be received directly by these nodes.

The communication between vehicles and infrastructures needs to be completed in a very short time when vehicles are moving fast. In order to transmit data integrally and realize the network coding operation, the source data are divided into a number of blocks that are the same as maximum length. Every data block contains a vehicle ID and a block ID. $B(p, q, t)$ is denoted as the block q sent by vehicular p. t is the time to the block timeout discarded. Every block has the live time to avoid heavy network load. The current value of t is taken to next hop to continue reducing over time. Block is discarded while $t = 0$.

The live time $T_{\max}$ is the maximum values of t. t is counted down at $T_{\max}$ while the block is generated from the source. $T_{\max}$ can be computed by (1)

$$T_{\max} = \frac{w_0 * C}{\operatorname{int}(\operatorname{Flow}(t) + 1)}, \tag{1}$$

where C is the class of the packet QoS and w_0 is the constant adjusting $T_{\max}$ to proper value. Int() is the integral function. Flow(t) is the current vehicle flow and given by

$$\operatorname{Flow}(t) = \alpha * \operatorname{Sum}(t) + (1 - \alpha) * \operatorname{Flow}(t - 1). \tag{2}$$

Sum(t) is the sum of vehicles that communicate with this vehicle in time t. The coefficient α is a constant value between 0 and 1, representing the degree of Flow(t) decreases. The greater the value, the faster the older affects are depreciated.

Infrastructures send active messages periodically. l is the TTL of active message. $l = l - 1$ when the message is forwarded by a vehicle. Vehicles send the active message immediately after receiving it and then do not send the same message. The active message will not be forwarded any more while $l = 0$. $L_{\max}$ is the TTL of the active message sent by infrastructures. $L_{\max}$ can be computed by (3) as follows:

$$L_{\max} = \operatorname{int}\left(E \times \left(w_1 * \ln\left(1 + \frac{\sum_{i=1}^{\operatorname{Sum}(t)} v_i}{\operatorname{Sum}(t)}\right) + w_2 * \operatorname{Sum}(t) + w_3\right)^{-1}\right), \tag{3}$$

where E is the signal intensity sent by infrastructures. The higher the power of infrastructures, the more the TTL of active message will be. Sum(t) is the sum of vehicles that communicate with this infrastructure in time t. v is the velocity of these vehicles. The more the vehicles are connected by the infrastructure and the faster the vehicles move, the less the TTL of active message will be. w_1, w_2, *and* w_3 are the weights of the former parameters, respectively. $L_{\max} = 1$ while the value obtained by (3) is less than 0. $L_{\max} = 15$ while the value obtained by (3) is more than 15. In other words, $1 \leqslant L_{\max} \leqslant 15$.

Linear network coding begins immediately when the vehicle receives the active message of infrastructures. The blocks $B(p, q, t)$ where $t > 0$ will be encoded and sent to infrastructures. In order to reduce the complexity of decoding operation, the dimension of encoding vector is taken a fixed value ω. A row vector contains ω consecutive blocks sent by the same vehicle. The blocks IDs in the vector i are from $(i - 1) * \omega + 1$ to $i * \omega$, where $i = 1, 2, 3, \ldots$. If the blocks of ID within this range are not received, their values will be set to 0.

The blocks sent by the vehicle p are divided into block vectors in sequence of q. $B(p, q, t)$ should equal to the element j of the vector i, i and j are given by

$$\begin{aligned} i &= \operatorname{int}\left(\frac{q}{\omega}\right) + 1, \\ j &= q - \omega * i. \end{aligned} \tag{4}$$

$x(p)_{ij}$ is denoted as the element j of block vector i sent by vehicle p. $x(p)_{ij}$ can be given by

$$x(p)_{ij} = B(p, (i - 1) * \omega + j, t). \tag{5}$$

$X(p)$ is the matrix consisting of all block vectors sent by vehicle p. $X(p)$ is denoted as

$$X(p) = \begin{bmatrix} X(p)_1 \\ X(p)_2 \\ \vdots \\ X(p)_v \end{bmatrix} = \begin{bmatrix} B(p, 1, t) & B(p, 2, t) & \cdots & B(p, \omega, t) \\ B(p, \omega + 1, t) & B(p, \omega + 2, t) & \cdots & B(p, 2\omega, t) \\ \vdots & \vdots & \vdots & \vdots \\ B(p, (v - 1) * \omega + 1, t) & B(p, (v - 1) * \omega + 1, t) & \cdots & B(p, v * \omega, t) \end{bmatrix}. \tag{6}$$

K is the local encoding matrix of the vehicle receiving the active message. All of elements in the matrix originate a pseudorandom sequence produced according to the vehicle ID. We reform the Fibonacci Algorithm [31] to generate the

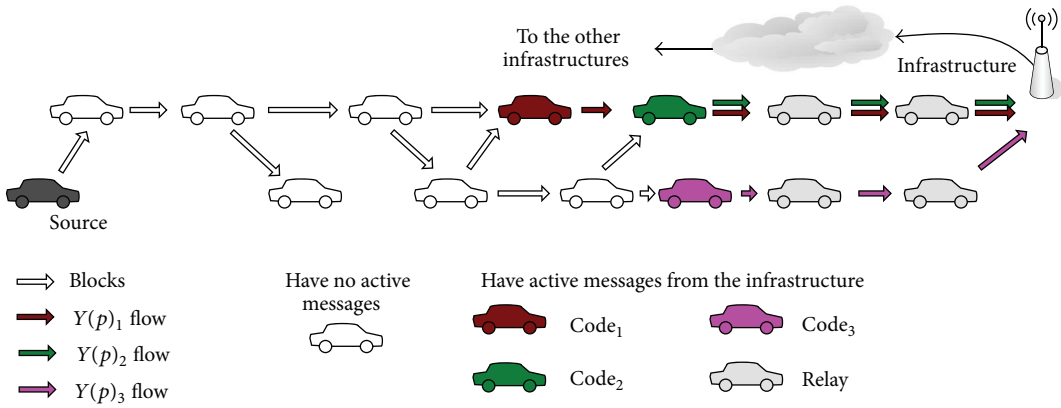


Figure 1: Data dissemination among vehicles on ToInfra stage.

sequence. Seq k denotes the pseudorandom sequence and is given by

$$\begin{aligned} \text{Seq}\, k_a &= \frac{Sn_a}{\varpi}, \quad a = 1, 2, 3, \ldots, \\ \varpi &= \max(\omega, \upsilon), \\ Sn_a &= (Sn_{a-2} + Sn_{a-1}) \bmod \varpi, \\ Sn_{-1} &= \text{VID}_{\text{source}} \bmod \varpi, \qquad Sn_0 = \text{VID}_0 \bmod \varpi, \end{aligned} \tag{7}$$

where $\text{VID}_{\text{source}}$ is the unique identification of the source vehicle and VID_0 is the unique identification of the vehicle executing network coding. The element k_{ij} in the matrix K is gotten from Seq k and given by

$$k_{ij} = \text{Seq}\, k_{i*\omega+j}. \tag{8}$$

K is the global coding matrix with $\lambda \times \omega$ dimension and can be denoted as follows:

$$\begin{aligned} K &= \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1\omega} \\ k_{21} & k_{22} & \cdots & k_{2\omega} \\ \vdots & \vdots & \vdots & \vdots \\ k_{\lambda 1} & k_{\lambda 2} & \cdots & k_{\lambda\omega} \end{bmatrix} \\ &= \begin{bmatrix} \text{Seq}\, k_1 & \text{Seq}\, k_2 & \cdots & \text{Seq}\, k_\omega \\ \text{Seq}\, k_{\omega+1} & \text{Seq}\, k_{\omega+2} & \cdots & \text{Seq}\, k_{2*\omega} \\ \vdots & \vdots & \vdots & \vdots \\ \text{Seq}\, k_{(\lambda-1)*\omega+1} & \text{Seq}\, k_{(\lambda-1)*\omega+2} & \cdots & \text{Seq}\, k_{\lambda*\omega} \end{bmatrix}. \end{aligned} \tag{9}$$

Implementing linear network coding on the blocks from the vehicle p is formalized as computing the product of two matrixes. It is denoted as

$$Y(p) = K \cdot X(p)^T. \tag{10}$$

The dimension of matrix $Y(p)$ is $\lambda \times \upsilon$, and its element $y(p)_{ij}$ can be computed by

$$\begin{aligned} y(p)_{ij} &= \sum_{m=1}^{\omega} k_{im} * x(p)_{jm} \\ &= \sum_{m=1}^{\omega} \text{Seq}\, k_{i*\omega+m} * B(p, (j-1)*\omega + m, t). \end{aligned} \tag{11}$$

The blocks sourced from the different vehicles have the different opportunity if they send the whole matrix $Y(p)$ successively. It is possible that the blocks sent later are not able to reach infrastructures. The movements of vehicles make the path unreachable. In order to make the equal opportunity for every vehicles transmitting information, the vehicles receiving active message only send an element of $Y(p)$, then send an element of $Y(p+1)$, and so on.

An infrastructure can receive multiple network codes that source from the same ω consecutive blocks but are computed by local encoding matrix of different vehicles (see Figure 1). Receiver can decode the ω blocks of row i completely when $Sc(p, i) \geq \omega$. $Sc(p, i)$ denotes the number of nonlinear codes received by the infrastructure and encoded by the i row blocks of the vehicle p. The element of $Y(p)$ in the same row is the nonlinear codes of the same ω blocks. The other vehicles also encode the ω blocks and send to the infrastructure. So the receiver maybe decodes the ω blocks completely when a vehicle only sends a few front elements of a row. The vehicle will send elements of coding matrix by columns. The infrastructure will send Break messages to the coding vehicles when $Sc(p, i) \geq \omega$. The vehicle breaks off network coding process when receiving Break messages.

When the vehicle on ToInfra stage receives a message, its process is formally shown in Figure 2.

Network coding algorithm on Figure 2 is described in Algorithm 1.

3.2. BeInfra Stage. Infrastructures are connected by wired media. They consist of wireless APs, network nodes, servers, and so on. It is able to guarantee the reliability and the real-time of data transmission among infrastructures.

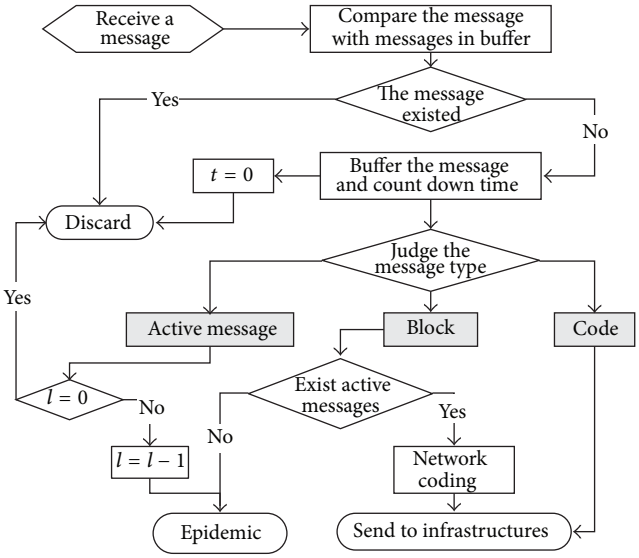


Figure 2: The process flowchart of vehicle on ToInfra stage.

The destinations of most blocks are not all of vehicles in VANET. We use multicast as the way of communication to aggregate data on BeInfra stage. Unicast and broadcast are regarded as two especial types of multicast in the method. Their group members are all or one node.

When wireless AP receives the coding blocks from vehicles, it will send these blocks to another node according to their destinations. The node is the root of multicast tree. The root aggregates and recodes these blocks according to their destinations and then sends them to egress APs following the tree. Creating tree for every multicast group will make more forward states on middle node and cause more delay in data transmission. We aggregate all of multicast groups in a few share trees to resolve the former problem on BeInfra stage.

3.2.1. Constructing Multicast Shared Tree. The multicast group means the set of the APs leading to members rather than the set of the members themselves. The domain of infrastructures contains at least one Network Manager Server (NMS). It controls the computation of all shared trees. NMS maintains a link-state database describing the topology of infrastructures.

There are one ingress router and multiple egress routers in a shared tree. The shared tree is rooted as a network node and leafing as egress APs. NMS selects routers as the root and leaves and computes the topology of shared tree. We partition all APs into subsets and cluster the members of all multicast group in the subsets in here then select the leaves and root of the shared tree. The method includes the detailed steps as the following.

(*1*) *Partitioning Aps.* All APs are partitioned according to the topology of infrastructure networks. Clustering algorithms are required in here. We use fuzzy clustering algorithm to partition APs into subsets. First, r_{ij} denotes the relation strength between AP i and j and is given by

$$r_{ij} = \begin{cases} 1 & i = j; \\ \left[\min\left(D_{ij} * \left(H_{ij}\right)^{\gamma}\right)\right]^{-1} & i \neq j. \end{cases} \tag{12}$$

γ is a constant to adjust the weight of D_{ij} and H_{ij}, and $\gamma \geq 0$. D_{ij} is the minimum delay (or the shortest path length) from AP i to j, and H_{ij} is the hop count of the path. The value of r_{ij} is concerned with the shortest distance between two APs. The less the distance is, the more the r_{ij} value is. The relational matrix R' is defined as the following equation:

$$R' = \left(r_{ij}\right)_{n\times n}, \tag{13}$$

where n is the total number of APs in VANETs.

In order to prove a fuzzy equivalence relation, we must demonstrate that R' is reflexive symmetrical and transitive [32]. R' is reflexive because all its diagonal elements are equal to 1. Suppose all links are dull-duplex in here, and their shortest path sourced either extremities is the same between AP i and j, and so $r_{ij} = r_{ji}$, $R' = (R')^{-1}$, R' is symmetrical. All of the other elements are less than diagonal elements, and so the inner product of R' is computed by

$$\left(R'\right)^2 = R' \circ R' = \left(\bigvee_{k=1}^{n}\left(r_{ik} \wedge r_{kj}\right)\right)_{n\times n} = \left(r_{ij}\right)_{n\times n} = R'. \tag{14}$$

R' is transitive because $(R')^2 \subseteq R'$. Therefore R' is a fuzzy equivalence relation.

The partition of APs set can be got from λ-cut sets of the fuzzy equivalence relation R'. The cut set is denoted as $(R')^{\lambda}$, and the value of its elements r_{ij}^{λ} is obtained by the following equation:

$$r_{ij}^{\lambda} = \begin{cases} 0 & r_{ij} < \lambda \\ 1 & r_{ij} \geq \lambda. \end{cases} \tag{15}$$

The set of All LERs are partitioned into many subsets. The λ belongs to $[0, 1]$; the less the value of λ is, the more the number of subsets is.

(*2*) *Aggregating Members.* NMS gives an identifier to every sub-set in the infrastructures domain and finds members of every multicast group according to the route-state tables of APs. Multicast member is replaced with the ID of sub-set including the member, and the multicast group G (member$_1$,..., member$_N$) is transferred to G'(ID$_1$,..., ID$_M$), which is defined as Class Group. The same IDs are merged into one element in G'. All multicast groups are indexed in G' and saved as their registration in NMS.

NMS contrasts the G' in term of sub-set ID. The number of G' with the same ID is denoted as the compression parameter C. If C is more than a specific threshold α ($\alpha \geqslant 2$), those groups are aggregated to use a Class Group.

(*3*) *Selecting Leaves.* There is only one leaf for a shared tree in every sub-set. The leaf is an AP in or out the sub-set. NMS

```
Sn_{-1} = VID_source mod ϖ, Sn_0 = VID_0 mod ϖ
For i = 1 to λ
  For j = 1 to ω
    Sn = (Sn_{-1} + Sn_0) mod ϖ;
    Sn_{-1} = Sn_0; Sn_0 = Sn;
    k[i, j] = Sn/ϖ;
For j = 1 to υ
  For every vehicle p
    For i = 1 to λ
      sum = 0;
      For m = 1 to ω
        sum = sum + k[i, m] * B[p, (j − 1) * ω + m];
      Y[p, i, j] = sum;
      Send Y[p, i, j] to next hop
      If receiving Break Message exit.
```

Algorithm 1: Formal description of network coding on ToInfra stage.

finds the multicast groups, which are aggregated to one Class Group G'. Then NMS divides all members of those multicast groups into Vertex set according to sub-set ID. The members in same G' and sub-set are placed a Vertex set. The Vertex set is linked into a sub-graph of the infrastructures domain. The nodes of the sub-graph consist of all APs in the Vertex set and the routers as intermediate nodes.

We select the median point of the sub-graph as the leaf of shared tunnel. The parameter D_i, which denotes the sum of distances from a node i in the sub-graph to all members of Vertex set, is computed by

$$D_i = \sum_{j=1}^{m} \left(d_{\min}(i,j) * \left(\sum_{k=1}^{C} b(j,k) \right) \right), \tag{16}$$

where $d_{\min}(i, j)$ is the length of shortest path between node i and member j and m is the number of members in the Vertex set. The parameter $t(j, k)$ is the bandwidth that multicast group k spares member j. The compression parameter C is the number of multicast groups aggregated into the shared tree. $b(j, k) = 0$ when multicast group k does not include member j. NMS selects the node with the minimum parameter D as the leaf of shared tree in the sub-set.

(*4*) *Selecting Multicast Root*. The root of shared tunnel is selected by the method similar to the selecting leaves. It can be any node in the infrastructures domain. The parameter P_i, which denotes the sum of distances from a node i to all sources of multicast group aggregated into the tree, is defined by the following equation:

$$P_i = \sum_{j=1}^{C} \left(d_{\min}(i,j) * T_j \right), \tag{17}$$

where $d_{\min}(i, j)$ is the length of shortest path between node i and source j and T_j is the bandwidth occupied by multicast flow from source j. NMS selects the node with the minimum parameter P as the root of the shared tree. So the P of root P_r must satisfy the following condition:

$$P_r = \min_{1 \le i \le N} \left(\sum_{j=1}^{C} \left(d_{\min}(i,j) * T_j \right) \right). \tag{18}$$

N is the number of nodes in the infrastructures domain.

(*5*) *Computing Multicast Shared Tree*. NMS computes the shared tunnel tree for the Class Group which connects the selected root and leaves. It can use any existing multicast tree algorithm [22] (e.g. the Dijkstra's algorithm, Steiner tree-based heuristic routing algorithm with the objective of minimizing the cost on multi-QoS constraint). How the multicast tree is computed in the algorithms is outside the scope of this paper.

3.2.2. Recoding on Root. APs send coding blocks to the roots of multicast shared tree according to their destinations. The root discards the same coding blocks and send Break messages to the coding vehicles when $Sc(p, i) \ge \omega$. Then the root will recode to the coding blocks with the same destinations and sources. The recoding blocks are transferred to the APs along the multicast shared tree. The APs in the tree cover the area where destinations vehicles arrive at or will arrive at.

ω nonlinear codes of blocks in the same row are selected to recode with the global coding matrix, which is denoted as F. The matrix F is unique and constant to the infrastructures and need not be transferred on VANETs. All vehicles have the duplicate copy of F and decode the recoding blocks using F. All of elements in F originate a pseudorandom sequence. Seq$f$ denotes the pseudorandom sequence and is given by

$$\begin{aligned} \text{Seq}\, f_a &= \frac{(\arcsin Sm_a)}{\pi} + 0.5, \quad a = 1, 2, 3, \ldots, \\ Sm_a &= 1 - 2 * Sm_{a-1}^2, \quad Sm_{a-1} \in (-1, 0.5) \cup (0.5, 1). \end{aligned} \tag{19}$$

Sm_a is an intermediate variable to produce the sequence. Sm_0 can be designated by the VANET administrator, and its

```
Sm = 0.3;
For i = 1 to ξ
   For j = 1 to ω
      Sm = 1 − 2 ∗ Sm^2;
      f[i, j] = arcsin(Sm)/π + 0.5;
Select ω received rows from Y to Y^s;
For j = 1 to υ
   For every vehicle p
      For i = 1 to ξ
         sum = 0;
         For m = 1 to ω
            sum = sum + f[i, m] ∗ Y[p, m, j]^s;
         Z[p, i, j] = sum;
         Send Z[p, i, j] to leafs of multicast shared tree;
         If receiving ACK Messages of all leaves exit.
```

Algorithm 2: Formal description of recoding on root.

default value is equal to 0.3. The element f_{ij} in the matrix F is gotten from Seq$f$ and given by

$$f_{ij} = \text{Seq}\, f_{i*\omega+j}. \tag{20}$$

The dimension of matrix F is $\xi \times \omega$, and its row sum ξ can be computed by

$$\xi = \beta * \frac{\omega}{\Pr(t)}, \quad \Pr(t) \le 1, \tag{21}$$

where $\Pr(t)$ is the probability that blocks arrive at destination from the infrastructure in time t; it can be designated by the VANET administrator according to the APs density. β is a guaranteed factor, where $\beta \ge 2$.

Implementing recoding on the coding blocks is formalized as computing the product of matrixes. It is denoted as

$$Z(p) = F \cdot Y(p)^s = F \cdot \left(K \cdot X(p)^T\right)^s. \tag{22}$$

$Y(p)^s$ is the ω nonlinear rows in matrix $Y(p)$, and they are received and selected by root. The dimension of matrix $Z(p)$ is $\xi \times \upsilon$, and its element $z(p)_{ij}$ can be computed by

$$z(p)_{ij} = \sum_{m=1}^{\omega} f_{im} * y(p)_{mj}^s = \sum_{m=1}^{\omega} \text{Seq}\, f_{i*\omega+m} * y(p)_{mj}^s. \tag{23}$$

The process of recoding on root is described in Algorithm 2.

3.3. ToVehic Stage. The leaves on multicast tree are the APs that may send blocks to destination vehicles within the designated time $T_{\max}$. Their communication ranges cover the location where vehicles are passing or will pass. The blocks are immediately sent out from APs after being recoded completely. Their live time $t = T_{\max}$. The function and computation of live time are the same as the ToInfra stage. AP stops sending the recoded blocks of the same row when it receives the ACK message from vehicles and then returns the message to the root of multicast tree. AP also stops sending when the ξ recoded blocks are sent completely but does not return the ACK message.

The vehicles buffer and send the blocks which $t \ne 0$. The destination vehicle will return the ACK message when it receives the ω nonlinear recoded blocks of the same row and then begins decoding. The method of reducing packet includes the detailed steps as the following.

(*1*) *Computing Coefficient Matrix.* Coefficient matrix consists of the factors which the ω blocks multiply. It is denoted as G. $(Z(p)^s)^\omega$ is the received ω local encoding vectors and can be given by

$$\left(Z(p)^s\right)^\omega = G \cdot X(p) = \left(F^s\right)^\omega \cdot \left(K^s\right)^\omega \cdot X(p). \tag{24}$$

$(F^s)^\omega$ is the ω rows of local encoding matrix in root. $(K^s)^\omega$ is the ω rows of local encoding matrix in vehicles. The number of rows is sent with the blocks. Their elements are generated from the designated pseudorandom sequence. Destination vehicle can generate the sequence in the same rule. The element g_{ij} in G can be computed by

$$\begin{aligned} g_{ij} &= \sum_{m=1}^{\omega} k_{im}^s * f_{mj}^s \\ &= \sum_{m=1}^{\omega} \text{seq}\, k_{(i+a)*\omega+m} * \text{seq}\, f_{(m+b)*\omega+j}. \end{aligned} \tag{25}$$

a and b are the values that the received number of rows subtract the number of row in $(F^s)^\omega$ and $(K^s)^\omega$, respectively.

(*2*) *Decoding the Recoding Blocks.* The designated row of $(F^s)^\omega$ is constant to a VANET. The row of $(K^s)^\omega$ is variable because it changes with the vehicle IDs of source and coding. We do not decode the $Z(p)$ to $X(p)$ directly but decode two blocks successively, because the constant matrix $(F^s)^\omega$ is easy to preprocess. The recoding blocks can be decoded by the below equation:

$$\left(Y(p)^s\right)^\omega = \left(\left(F^s\right)^\omega\right)^{-1} \cdot \left(Z(p)^s\right)^\omega. \tag{26}$$

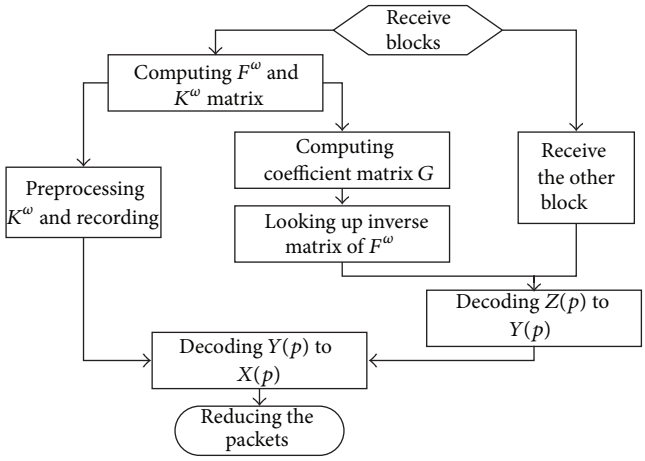


Figure 3: The process flowchart of destination vehicle on ToVehic stage.

Matrix inverse is not usually used in the decoding process because it is complex and can exhaust the computing resource. In our case, $(F^s)^{\omega}$ is the subset of constant matrix F. All subsets of F inverse can be precalculated in the mainframe computer. Their inverse matrixes are stored in vehicles as the table. The space occupied by the tables is $C_{\xi}^{\omega} * \omega^2$. This is storable to the vehicle. In this step, vehicles need not compute the inverse matrix, and they can find quickly the inverse matrix in the table according its rows sequence. So the decoding of the recoding blocks can be finished rapidly in (26).

(*3*) *Decoding the Coding Blocks*. Destination vehicles can decode $Y(p)$ to $X(p)$ in any decoding algorithm on the step. We improve the step in preprocessing $(K^s)^{\omega}$ matrix. To obtain $X(p)$ matrix, a variant of the Gaussian elimination is used. A typical Gaussian elimination or LU decomposition restricts us to wait until we decoded the recoding block and ω had the $\omega \times \omega$ coefficient matrix [33]. However, decoding operation is started early in our case, and $(K^s)^{\omega}$ is preprocessed as the first block arrives.

$Y(p)$ is confirmed of the sequences of the rows and the IDs of coding vehicles on the root. The first block can carry this information to the destination vehicle. Destination computes the $(K^s)^{\omega}$ matrix in advance. It preprocesses the $(K^s)^{\omega}$ in Gaussian elimination while receiving $Z(p)$ and records the processing steps. These steps contain the processing order of rows and the multiplying coefficients of every row. After $Z(p)$ is decoded to $Y(p)$, the vehicle decodes $Y(p)$ in the steps of preprocessing $(K^s)^{\omega}$. Processing objects are only the elements of $Y(p)$, and decoding $Y(p)$ is speed-up.

(*4*) *Reducing the Packets*. Destination composes the blocks of $X(p)$ into the packets. The packets are reduced completely.

The steps are formally shown in Figure 3.

4. Evaluation

In this section, we generate the movement of vehicles on the ONE simulator [34] and evaluate the performance of our MCNC method in contrast with Epidemic, PRoPHET routing, and generic Wi-Fi.

4.1. Simulation Setup. The ONE simulator uses the Helsinki city map and generates node movement and routing [35]. We extract the area with the range of 4000 m × 3000 m from the map and configure two types of network nodes. Vehicle node moves on the map at the speed of 10 to 50 km/h and waits time of 10 to 120 seconds to stop communication after arriving to the destination. The vehicles choose random destinations on the map and move there following the shortest path. AP node is static and communicates with other APs in wired links. The radio range is configured as 200 m, and the MAC protocol is IEEE 802.11.

Epidemic replicates messages to all encountered nodes that do not have them yet. PRoPHET only sends messages to the nodes that have the highest chances to deliver the messages to the destination. They are two typical routing protocols for ad hoc networks and have been implemented by the users of the ONE simulator as add-ons. In generic Wi-Fi, vehicles data must be delivered by APs in the radio range, and the routing capability of vehicles is disabled.

Two scenarios are generated in the evaluation. A sparse network with 30 vehicles simulates the rural area. A dense network with 150 vehicles simulates the urban area.

The other parameters of MCNC method are listed as follows. The TTL of the active message $L_{\max} = 2$ or 5. The live time of blocks among vehicles $T_{\max} = 300$ seconds. The dimension of encoding vector $\omega = 10$. The number of APs is variable.

4.2. Performance Analysis. The measured parameters on the simulator are the block loss rate, transmission delay, and overhead messages. Block loss rate [13] is the ratio of lost blocks to the sending blocks from sources. Transmission delay is the time of a block delivered from the source to all destinations. Overhead ratio [13] is the effective blocks as the percentage of all forwarding blocks among vehicles. They synthetically reflect the performance of MCNC. The simulation lasts for 30 minutes. The 10 sources in 2 scenarios are selected to generate flows for the evaluation. The average values of the 3 parameters are presented as the basis for analyzing their performance.

Figure 4 shows the average blocks loss rate in the sparse scenario. It is easy to see that as the number of APs increases, blocks loss rate decreases in the five data plots. When the number of APs is 80, the radios of APs cover the whole area and blocks loss rate is 0 for all the method. Epidemic has the less loss rate than the others, since it sends copies to all encountered vehicles and transmits successively in the greatest probability. Generic Wi-Fi is the most loss rate and cannot be used while APs only cover part of area. PRoPHET also cannot delivery many blocks to the destinations in the sparse scenario. MCNC is close to Epidemic in blocks loss rate. When the cover area of APs is 1/5 (the number of APs is 16 in Figure 4), the blocks loss rate of MCNC is less than 0.2, and it can reach the target of transmission reliability. $L_{\max}$ has some influence on the parameter. The values of the parameter

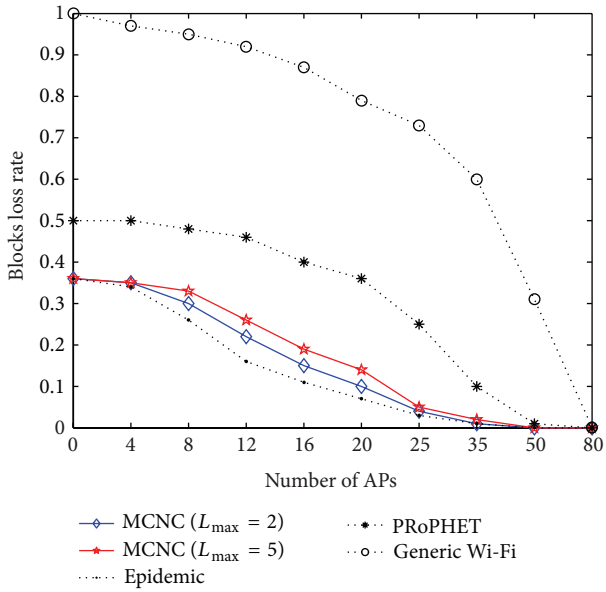


Figure 4: Blocks loss rate in the sparse scenario.

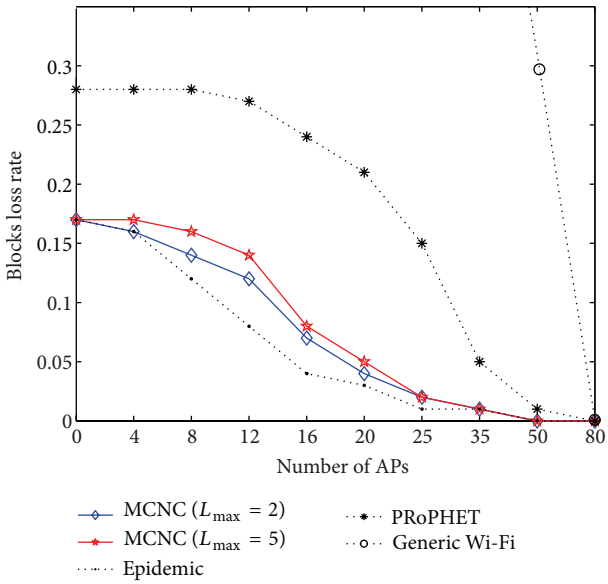


Figure 5: Blocks loss rate in the dense scenario.

will increase weakly while L_{max} is changed from 2 to 5. With the increase of hops after network coding and aggregating, the block loss rate only increases 0.04 when the number of APs is 16.

Figure 5 is similar to Figure 4. Generic Wi-Fi is unchangeable in different scenarios. Figure 5 only shows a part plot of generic Wi-Fi. The other methods all decrease their blocks loss rate in dense scenario. MCNC in the scenario is closer to Epidemic than the sparse scenario. When the cover area of APs is 1/5, the blocks loss rate of MCNC decreases to less than 0.08. The changes of L_{max} do not have strong influence on the transmission reliability of MCNC.

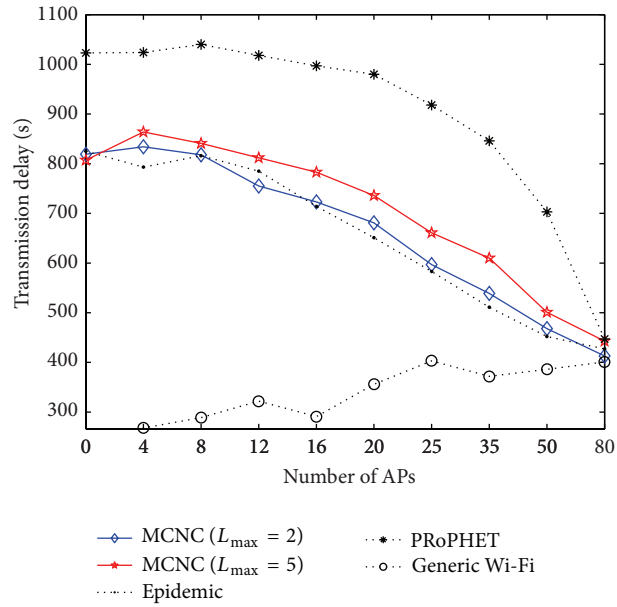


Figure 6: Transmission delay in the sparse scenario.

Figure 6 shows the average delay of blocks that are transmitted successively to destinations in the sparse scenario. Generic Wi-Fi only deliver few blocks to destinations while the number of APs is less than 20. Its delay changes randomly and does not associate with the number of APs and vehicles. The other methods all decrease the transmission delay with the increase of APs. PRoPHET only takes one of encountering vehicles as the next hop. Although the vehicle has the highest chance to destinations, it maybe moves more time to send block. So the delay of PRoPHET is more than the other methods. MCNC is also near to Epidemic in delay. Their delays are same in no AP setting. MCNC use APs to delivery blocks, but increase in little delay. When the cover area of APs is 1/5, the delay of MCNC is more 8% than Epidemic, and it can reach the target of transmission real-time. The changes of L_{max} have some influence on the delay of MCNC. The delay increases less than 10% when L_{max} is changed from 2 to 5.

The delays of four methods in dense scenario are shown in Figure 7, which is similar to Figure 6. They all decrease their delays in the dense scenario. Their delays are closer than the sparse scenario. When the number of APs is 16, the delay of MCNC is more than 6% Epidemic, PRoPHET is more than 22% Epidemic, and the delay increases less than 3% with the change of L_{max} from 2 to 5.

Figure 8 shows the average overhead radios, which are the same in all test scenarios. Generic Wi-Fi does not generate overhead messages on any conditions, and its values are always least in four methods. Epidemic generates most overhead messages, which rise with the increase of APs, since AP also sends Epidemic message to the other vehicles. For this reason, PRoPHET also generates more overhead messages while setting more APs. MCNC has the same overhead ratio with Epidemic in no AP setting. With the increase of the number of APs, the overhead messages begin to decrease rapidly in MCNC. The rate of decrease is diminished after

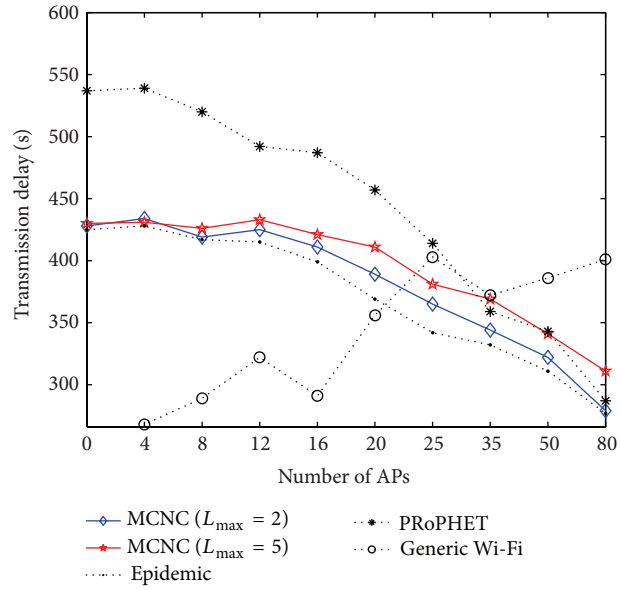


Figure 7: Transmission delay in the dense scenario.

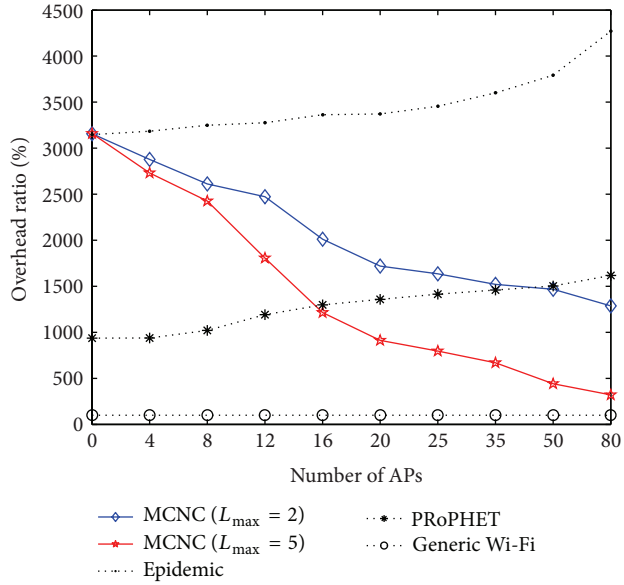


Figure 8: Overhead ratio of the four methods.

the cover area of the APs is more than 1/4 (the number of APs is 16). MCNC reduces the overhead message after network coding and aggregates the flows in multicast share trees on infrastructures. So its aggregating ability is obvious.

The changes of L_{max} have huge influence on the overhead ratio of MCNC. The greater L_{max} is, the less the overhead ratio is and the more the aggregating ability is. With L_{max} changing from 2 to 5, the overhead ratio cuts down more than 1/2 after the cover area of the APs is more than 1/4. If L_{max} and the number of APs satisfy the requirements, blocks can be coded and sent to APs after leaving the sources. The overhead ratio of MCNC (L_{max} = 5) is 1200% when the cover area of the APs is 1/5. This value is the 1/3 of Epidemic and even less than PRoPHET. So the 2/3 overhead messages are cut down, and the scalability of VANETs is improved.

Given all that, MCNC is able to achieve lower overhead ratios than both Epidemic and PRoPHET. Its blocks loss ratio and delay are tiny higher than Epidemic but lower than the other methods. It aggregates greater part of overhead messages using multicast and network coding. Installing APs in part of area can improve the performance of MCNC in any scenario. MCNC is appropriate for the areas that APs have been deployed but cannot cover entirely.

5. Conclusion

VANET can use APs as the infrastructures to improve its performance. Our works aggregate messages in multicast trees on infrastructures networks mainly consisted of APs and implement network coding on the vehicles that the hop to APs is less than L_{max}. We divide data transmission into 3 stages: ToInfra, BeInfra, and ToVehic. Network coding, multicast aggregating, and decoding are implemented in the 3 stages, respectively. Data dissemination uses the generic routing algorithm for VANETs before network coding.

The experiments show that our MCNC is able to cut down 2/3 overhead messages of Epidemic when the cover area of the APs is 1/5. The costs of aggregations are a tiny improvement of delay. The blocks loss ratio and transmission delay of MCNC are also lower than the other methods. The performance of MCNC is similar in sparse scenario and dense scenario. In many places, Wi-Fi based APs can be deployed, but their radios cannot cover the whole area of vehicles movement, and MCNC will exert the promoting affluence on the development of VANETs.

Acknowledgments

The work is supported in part by the National Science Foundation of China under Grant nos. 61202378, 61070169, and 61070170, University Science Research Project of Jiangsu Province under Grant no. 11KJB520017, the Natural Science Foundation of Jiangsu under Grant no. BK2011376, and Suzhou Application Foundation Research Project under Grant nos. SYG201238 and SYG201118.

References

[1] F. Farnoud and S. Valaee, "Reliable broadcast of safety messages in vehicular Ad hoc networks," in *Proceedings of the IEEE INFOCOM 2009*, pp. 226–234, Rio de Janeiro, Brazil, April 2009.

[2] J. Zhu, Y. Feng, and B. Liu, "PASS: parking-lot-assisted carpool over vehicular Ad hoc networks," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 491756, 9 pages, 2013.

[3] K. C. Lee, S. H. Lee, R. Cheung, U. Lee, and M. Gerla, "First experience with CarTorrent in a real vehicular Ad hoc network testbed," in *Proceedings of the Mobile Networking for Vehicular Environments (MOVE '07)*, pp. 109–114, Anchorage, Alaska, USA, May 2007.

[4] U. Lee, J. Lee, J. Park, and M. Gerla, "FleaNet: a virtual market place on vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 1, pp. 344–355, 2010.

[5] G. Karagiannis, O. Altintas, E. Ekici et al., "Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Communications Surveys and Tutorials*, vol. 13, no. 4, pp. 584–616, 2011.

[6] M. J. Khabbaz, C. M. Assi, and W. F. Fawaz, "Disruption-tolerant networking: a comprehensive survey on recent developments and persisting challenges," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 2, pp. 607–640, 2012.

[7] S. Olariu and M. C. Weigle, *Vehicular Networks: From Theory to Practice*, CRC Press/Taylor & Francis, 2009.

[8] Y. Wu, Y. Zhu, and B. Li, "Infrastructure-assisted routing in vehicular networks," in *Proceedings of the IEEE INFOCOM 2012*, pp. 1485–1493, Orlando, Fla, USA, March 2012.

[9] J. Jaehoon, G. Shuo, G. Yu, H. Tian, and D. Du, "TBD: trajectory-based data forwarding for light-traffic vehicular networks," in *Proceedings of the 29th IEEE International Conference on Distributed Computing Systems Workshops (ICDCS '09)*, pp. 231–238, Montreal, Canada, June 2009.

[10] D. Jiang and L. Delgrossi, "IEEE 802.11p: towards an international standard for wireless access in vehicular environments," in *Proceedings of the IEEE Vehicular Technology Conference-Spring (VTC '08)*, pp. 2036–2040, Singapore, May 2008.

[11] J. Eriksson, L. Girod, B. Hull, R. Newton, S. Madden, and H. Balakrishnan, "The pothole patrol: using a mobile sensor network for road surface monitoring," in *Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services*, pp. 29–39, June 2008.

[12] Y. M. Zhu, X. M. Liu, M. L. Li, and Q. Zhang, "POVA: traffic light sensing with probe vehicles," in *Proceedings of the INFOCOM 2012*, pp. 2661–2665, 2012.

[13] A. Palma, P. R. Pereira, and A. Casaca, "Multicast routing protocol for vehicular delay-tolerant networks," in *Proceedings of the IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '12)*, pp. 753–760, Barcelona, Spain, October 2012.

[14] J. Eriksson, H. Balakrishnan, and S. Madden, "Cabernet: vehicular content delivery using WiFi," in *Proceedings of the 14th Annual International Conference on Mobile Computing and Networking (MobiCom '08)*, pp. 199–210, September 2008.

[15] V. Bychkovsky, B. Hull, A. Miu, H. Balakrishnan, and S. Madden, "A measurement study of vehicular internet access using in situ Wi-Fi networks," in *Proceedings of the 12th Annual International Conference on Mobile Computing and Networking (MOBICOM '06)*, pp. 50–61, September 2006.

[16] N. Banerjee, M. D. Corner, and B. N. Levine, "An energy-efficient architecture for DTN throwboxes," in *Proceedings of the 26th IEEE International Conference on Computer Communications (IINFOCOM '07)*, pp. 776–784, Anchorage, Alaska, USA, May 2007.

[17] P. Rodriguez, R. Chakravorty, J. Chesterfield, I. Pratt, and S. Banerjee, "MAR: a commuter router infrastructure for the mobile internet," pp. 217–230, 2004.

[18] J. Zhao, Y. Zhang, and G. Cao, "Data pouring and buffering on the road: a new data dissemination paradigm for vehicular Ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, part 1, pp. 3266–3277, 2007.

[19] B. B. Chen and M. C. Chan, "MobTorrent: a framework for mobile internet access from vehicles," in *Proceedings of the IEEE INFOCOM 2009*, pp. 1404–1412, Rio de Janeiro, Brazil, April 2009.

[20] I. Leontiadis, P. Costa, and C. Mascolo, "Extending access point connectivity through opportunistic routing in vehicular networks," in *Proceedings of the IEEE INFOCOM 2010*, pp. 1–5, San Diego, Calif, USA, March 2010.

[21] J. Jeong, S. Guo, Y. Gu, T. He, and D. Du, "Trajectory-based statistical forwarding for multihop infrastructure-to-vehicle data delivery," *IEEE Transactions on Mobile Computing*, vol. 11, no. 10, pp. 1523–1537, 2012.

[22] J. Jeong, S. Guo, Y. Gu, T. He, and D. H. C. Du, "Trajectory-based data forwarding for light-traffic vehicular Ad hoc networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 5, pp. 743–757, 2011.

[23] N. Liu, M. Liu, G. Chen, and J. Cao, "The sharing at roadside: vehicular content distribution using parked vehicles," in *Proceedings of the IEEE INFOCOM 2012*, pp. 2641–2645, Orlando, Fla, USA, March 2012.

[24] N. Liu, M. Liu, W. Lou, G. Chen, and J. Cao, "PVA in VANETs: stopped cars are not silent," in *Proceedings of the IEEE INFOCOM 2011*, pp. 431–435, Shanghai, China, April 2011.

[25] W. Vogels, R. Renesse, and K. Birman, "The power of epidemics: robust communication for large-scale distributed systems," *ACM SIGCOMM Computer Communication Review*, vol. 33, no. 1, pp. 131–135, 2003.

[26] A. Lindgren, A. Doria, and O. Schelen, "Probabilistic routing in intermittently connected networks," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 7, no. 3, pp. 19–20, 2003.

[27] U. Lee, J. Park, J. Yeh, G. Pau, and M. Gerla, "CodeTorrent: content distribution using network coding in VANET," in *Proceedings of the 1st International Workshop on Decentralized Resource Sharing in Mobile Computing and Networking (MobiShare '06)*, pp. 1–5, ACM, September 2006.

[28] M. Li, Z. Yang, and W. Lou, "CodeOn: cooperative popular content distribution for vehicular networks using symbol level network coding," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 1, pp. 223–235, 2011.

[29] M. Sathiamoorthy, A. G. Dimakis, B. Krishnamachari, and F. Bai, "Distributed storage codes reduce latency in vehicular networks," in *Proceedings of the IEEE INFOCOM 2012*, pp. 2646–2650, Orlando, Fla, USA, March 2012.

[30] V. Palma, E. Mammi, A. M. Vegni, and A. Neri, "A fountain codes-based data dissemination technique in vehicular Ad-hoc networks," in *Proceedings of the 11th International Conference on ITS Telecommunications (ITST '11)*, pp. 750–755, August 2011.

[31] S. Primak, V. Lyandres, O. Kaufman, and M. Kliger, "On the generation of correlated time series with a given probability density function," *Signal Processing*, vol. 72, no. 2, pp. 61–68, 1999.

[32] Z. Pawlak, "Rough sets," *International Journal of Computer and Information Science*, vol. 11, no. 5, pp. 341–356, 1982.

[33] T. Ho, M. Médard, R. Koetter et al., "A random linear network coding approach to multicast," *IEEE Transactions on Information Theory*, vol. 52, no. 10, pp. 4413–4430, 2006.

[34] The ONE, http://www.netlab.tkk.fi/tutkimus/dtn/theone/.

[35] A. Keränen, T. Kärkkäinen, and J. Ott, "Simulating mobility and DTNs with the ONE," *Journal of Communications*, vol. 5, no. 2, pp. 92–105, 2010.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 616059, 9 pages
http://dx.doi.org/10.1155/2013/616059

Research Article

A Type of Node Deployment Strategy Based on Variable Acceleration Motion for Wireless Sensor Networks

Chao Sha,[1] Ru-chuan Wang,[1,2,3] and Hai-ping Huang[1,2,3]

[1] *College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China*
[2] *Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210003, China*
[3] *Key Lab of Broadband Wireless Communication and Sensor Network Technology, Ministry of Education, Nanjing 210003, China*

Correspondence should be addressed to Chao Sha; shac@njupt.edu.cn

Received 6 April 2013; Accepted 25 August 2013

Academic Editor: Limin Sun

For the purpose of balancing node energy consumption in Wireless Sensor Networks and in the premise of considering network coverage, a kind of node broadcasting scheme at fixed intervals under variational acceleration straight-line movement model is proposed in this paper. Simulation results illustrate that the approach proposed in this paper has a superior performance on balance of energy consumption compared to IEA method and uniform broadcasting as well as random broadcasting methods. And the energy saving effect is close to that of the theoretical deployment model of data fusion and nondata fusion.

1. Introduction

Energy balance is a key metric impacting the performance of Wireless Sensor Networks (WSNs) [1, 2]. One of the most efficient methods to achieve energy balance is to optimize the deployment and configuration of WSNs [3–9]. However, it is well known that designing a Wireless Sensor Network is a difficult task, especially the sensor node deployment which has an impact on the coverage, the network connectivity, and the network lifetime as well as the cost of the WSNs [10].

For practical applications, deterministic deployments can be time-consuming and error-prone, since they have the utmost challenge of guaranteeing connectivity and proper area coverage upon deployment. The deployment problem has been the topic of much research work. However, the majority of the work focuses on theoretical lab-appropriate approaches for carefully positioning nodes to meet research requirements [11–13].

On the other hand, currently, random broadcasting and uniform clustering methods are adopted in most multihop WSNs [14]. By communicating among nodes and sleep scheduling, it could save more energy to extend network lifetime. However, it is difficult to achieve an energy balance [15–17]. In the multihop communication network of WSNs, the closer to the base station, the energy of the node will be consumed faster. If a large number of nodes nearby the base station are dead, there will be an isolated subnet with the base station, and then the data will not be able to reach the base station anymore. This is also known as hot spot problem of the multihop network [18]. Therefore, how to design a flexible deployment and broadcasting model for nodes is a chief problem in WSNs [3].

2. Related Works

There is considerable literature addressing various aspects of energy balancing deployment. Fan et al. [19] propose a type of deployment strategy with relay nodes to ensure energy balance. By computing the most proper transmission distance, several relay nodes are set between source nodes and the base station to achieve balance between the energy consumption of sensor nodes and relaying nodes. However, this strategy takes a considerable cost in time and cannot be applied in large-scale networks; Fei [20] proposes a grid based network deployment algorithm. In this algorithm, each grid defines an inner node, which has the least distance from the grid center as its cluster. Besides, it utilizes the gateway to gather the information in a cluster then deliver it to the nearest cluster head. This deployment strategy owns

the advantages for the convenience of information management and data fusion. But it should be noted that energy unbalance is also a key problem in this network. In addition, Liu [21] proposes a new method of deployment using ant colony iteration in grid models which reaches the goal of coverage with minimum nodes.

Besides optimizing deployment schemes, heterogeneous initial energy allocation and modulation modes are proposed by some literatures as well to achieve energy balance. Ren et al. [22] provide a method called IEA. In this method, initial energy of each node is allocated according to its distance from the base station. Then, the initial energy difference between neighboring nodes is simplified as a constant value. However, the error in IEA cannot be neglected, and in real networks it is usually impossible to prior allocate initial energy. Soltan et al. [23] propose another method to achieve energy balance. In a circular network, they choose noncoherent BFSK with low complexity and high SNR for the nodes near the base station, and coherent BPSK with high complexity and relative low SNR for the nodes far from the base station. But, like IEA, this method cannot achieve self-adaptation in a varied network. In addition, heterogeneous modulation causes low transmission efficiency.

By computing network lifetime after deployment, Hou et al. [24] adjust the location of relay nodes to maximize the network lifetime. But this method takes a heavy cost for the process of iteration and cannot adapt itself with varied networks. Ren et al. [25] propose a distance-based energy efficient placement in circular networks. Though coverage has been taken into consideration in this deployment, it fails to analyze the energy consumption on the condition of data fusion. In addition, [26–28] provide a similar method in which circular networks are to be divided into several rings with different radii. By utilizing this method to figure out the minimum value of the objective function, it is easy to get the optimum radius for each ring. However, it also ignores the network coverage problem.

Based on the above researches and taking real physical environment into account, this paper proposes a new broadcasting method, in which the thrower is undergoing a straight-line motion with varied acceleration and broadcasts at a fixed rate. Section 3 of this paper provides a detailed realization process, and the simulation of this method is shown in Section 4. The conclusion is provided in Section 5.

3. Method Description

3.1. Energy Balance Oriented Theoretical Deployment Model of WSNs. The major properties of WSNs are random broadcasting and multihop transmission [3–6]. As a result, it is wise to firstly analyze the energy balance of a linear multihop network model. As Figure 1 shows, a network has N nodes: $S_1, S_2, \ldots, S_N$ and a base station B. S_1 is the source and B is the destination node. Node S_k is the forerunner of node S_{k+1} which is the successor of S_k. The hop distance between S_k and S_{k+1} is d_k. P_i $(i = 1, 2, \ldots, N)$ is the size of packet needed to be gathered and delivered by node S_i $(i = 1, 2, \ldots, N)$. Without the consideration of data fusion, except the first

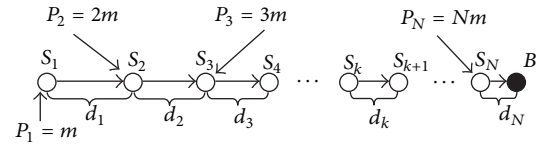


Figure 1: Linear multihop network model.

node S_1, every node will receive the data package from its forerunner, combine them with its own data, then deliver to its successor until reaching the base station. According to [15], the following equation is valid:

$$E_k = m\left[(k-1)E_{\text{elec}} + kE_{\text{elec}} + k\varepsilon_{\text{amp}}d_k^2\right],$$
$$E_{k+1} = m\left[kE_{\text{elec}} + (k+1)E_{\text{elec}} + (k+1)\varepsilon_{\text{amp}}d_{k+1}^2\right], \quad (1)$$

where E_k and E_{k+1} are the energy consumption during a single-time data transmission by node S_k and S_{k+1}, respectively. m is defined as number of bits of single-time data gathered by one node. E_{elec} is the unit energy consumption of a transceiver, while ε_{amp} is the unit energy consumption of an amplifier. Moreover, it is generally recognized that the energy of sink node is sufficient. As a result, to achieve energy balance, E_k should be equal to E_{k+1} $(k = 1, 2, \ldots, N-1)$, which is shown as the following:

$$(k-1) \times E_{\text{elec}} + kE_{\text{elec}} + k\varepsilon_{\text{amp}}d_k^2 = kE_{\text{elec}} + (k+1)E_{\text{elec}} + (k+1)\varepsilon_{\text{amp}}d_{k+1}^2. \quad (2)$$

Based on this equation, the relation of different hop distances in this linear structure should meet

$$d_{k+1} = \sqrt{\frac{k \times d_k^2}{k+1} - \frac{2E_{\text{elec}}}{\varepsilon_{\text{amp}} \times (k+1)}}. \quad (3)$$

It is obvious to find that d_{k+1} is always smaller than d_k, but their difference is approaching zero with the increase of k.

This linear model is similar to the models in literature [26–28] and can be generalized into circular networks, as Figure 2 shows. The network region is made up of a solid circle with radius L and the base station is located on the center of the circle. So, several multihop transmission models of the linear structures compose an energy balancing circular network model. The hop distance of every node in the linear structure should meet

$$\sum_{i=1}^{N} d_i = L. \quad (4)$$

From Figure 2, it should be noted that nodes in the network will form several concentric circles with different radii, and the difference between radiuses is not uniform (as the dotted lines in Figure 2 show). It is also easy to find that given the network size, the angle of two neighboring linear structures (as angle θ in Figure 2) determines the number of nodes required to be deployed as well as the network coverage.

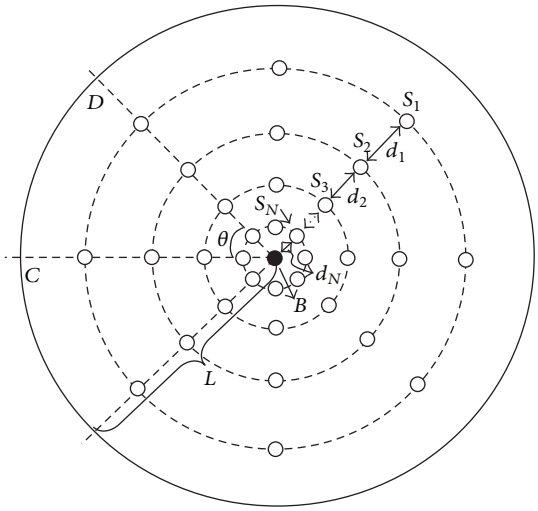


Figure 2: Energy balance oriented deployment model in circular networks without data fusion.

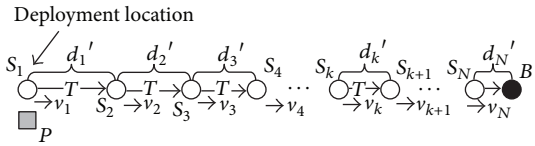


Figure 3: Deployment model based on variable acceleration straight-line movement.

3.2. Deployment Model Based on Variable Acceleration Straight-Line Movement. Though energy balance can be achieved in both the linear deployment model and the concentric circular deployment model, it is difficult to locate nodes accurately. As a result, based on (3) which describes the relation between neighboring hop distances, a new deployment strategy is proposed here to simulate and substitute for the energy balance oriented theoretical deployment model. In this strategy, the thrower is undergoing a straight-line motion with an acceleration which is varying at a constant rate and deploying nodes during a fixed time interval. As Figure 3 demonstrates, an object P undergoes a decelerated straight-line motion with a decreasing acceleration. Its motion starts with the initial speed v_1 and an initial acceleration a_0, which decreases at a rate r. Let $a(t)$, $v(t)$, and $S(t)$ denote the instantaneous acceleration and instantaneous velocity and displacement; then we know

$$\begin{aligned} a(t) &= a_0 - rt, \\ v(t) &= v_1 - \int_0^t a(t)\,dt = v_1 - a_0 t + \frac{1}{2}rt^2, \\ S(t) &= \int_0^t v(t)\,dt = v_1 t - \frac{1}{2}a_0 t^2 + \frac{1}{6}rt^3. \end{aligned} \tag{5}$$

Let P deploy a node at its instantaneous position with a fixed time T interval. According to the rule of straight-line motion with variable acceleration, the distance between two neighboring nodes will be smaller, which is similar to the energy balance oriented deployment scheme demonstrated in Section 3.1. Figure 3 points out the deployment positions $S_1, S_2, \ldots, S_N$ ($v_1, v_2, \ldots, v_N$ are the instantaneous velocity of P at this deployment position), where the nodes should be deployed. So, we get

$$\begin{aligned} d_1' &= v_1 T - \frac{1}{2}a_0 T^2 + \frac{1}{6}rT^3, \\ d_2' &= v_1 T - \frac{3}{2}a_0 T^2 + \frac{7}{6}rT^3, \\ d_3' &= v_1 T - \frac{5}{2}a_0 T^2 + \frac{19}{6}rT^3. \end{aligned} \tag{6}$$

By mathematical induction

$$\begin{aligned} d_k' &= v_1 T - \frac{1}{2}(2k-1)\,a_0 T^2 + \frac{1}{6}\left(3k^2 - 3k + 1\right)rT^3, \\ d_{k+1}' &= v_1 T - \frac{1}{2}(2k+1)\,a_0 T^2 + \frac{1}{6}\left(3k^2 + 3k + 1\right)rT^3. \end{aligned} \tag{7}$$

Then we get

$$d_{k+1}' = d_k' - a_0 T^2 + krT^3. \tag{8}$$

Equation (3) shows that we should ensure d_k is larger than d_{k+1} for all k, in order to achieve an energy balance. So, (8) can be transformed to

$$krT^3 - a_0 T^2 < 0, \tag{9}$$

so

$$k < \frac{a_0}{rt}. \tag{10}$$

Equation (8) illustrates, similar to (3), with the increase of k, d_{k+1}' is approaching d_k' indefinitely, proving that the tendencies of these two equations are the same. So, it is feasible to adopt straight-line motion with variable acceleration to simulate energy balance oriented deployment scheme in WSNs.

However, in most practical cases, broadcasting by air is used as a major deployment way. As a result, it needs to take some improvement, as shown in Figure 4. Similar to Figure 3, $S_1, S_2, \ldots, S_N$ are broadcasting points for an aircraft undergoing a straight-line motion with a decreasing acceleration, while $S_1', S_2', \ldots, S_N'$ are the points where the nodes have landed. Let h denote the height of the aircraft, and T denote the broadcasting interval. It is obvious that, after being broadcasted, the nodes undergo free fall motion in vertical direction and uniform motion with velocity $v_1, v_2, \ldots, v_N$ in horizontal direction.

From Figure 4, it can be inferred that the relation between d_k', the distance between two neighboring broadcasted points, and d_k'', the distance between two neighboring real landed points, is shown as

$$d_k'' = d_k' - V((k-1)T) \times \sqrt{\frac{2h}{g}} + V(kT) \times \sqrt{\frac{2h}{g}}. \tag{11}$$

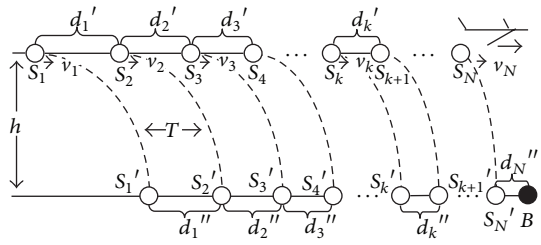


Figure 4: Broadcasting by air based dispersal model.

Similarly,

$$d''_{k+1} = d'_{k+1} - V(kT) \times \sqrt{\frac{2h}{g}} + V((k+1)T) \times \sqrt{\frac{2h}{g}}. \quad (12)$$

So, from (8), (11), and (12), it can be inferred that

$$d''_{k+1} = d''_k - a_0 T^2 + krT^3 + rT^2 \sqrt{\frac{2h}{g}}, \quad (13)$$

$$k < \frac{1}{T}\left(\frac{a_0}{r} - \sqrt{\frac{2h}{g}}\right). \quad (14)$$

From (13), if the thrower undergoes a straight-line motion with a variable acceleration and is broadcasting nodes with a fixed time interval T, the real linear structures formed by landed nodes in network region are similar to the structure under the energy balance oriented linear network deployment. In addition, on the condition of air broadcasting, the difference between neighboring hop distances is much smaller than that in other deployments.

From what has been discussed above, we assume that the thrower undergoes a decelerated motion with a decreasing acceleration first and then an accelerated motion with an increasing acceleration along a diameter of the network region. Thus, the deployment of nodes in the linear structure along that diameter can be accomplished.

The initial velocity is v_1, initial acceleration is a_0, and its decreasing rate is r. The broadcasting interval is also T. Once the thrower reaches the base station located at the center of the network, its motion changes to be an accelerated motion with an increasing acceleration. The new initial velocity is v_{N+1}, new initial acceleration is $a(N \times T)$, and its increasing rate is r. This process is shown in Figure 5.

From Figure 2, in order to ensure energy balancing, the location of deployed nodes will form several concentric circles and the difference of radii of neighboring circulars obeys (3). Similarly, after several air broadcastings, the deployed nodes will form several concentric circles, whose radius are different and their difference is not uniform. The difference between radiuses of neighboring circles meets (13).

3.3. Coverage Guaranteed Air Broadcasting Deployment Scheme. By the model of air broadcasting under variable acceleration straight-line movement, a linear network can be well deployed. Then, how many times should a thrower move and broadcast to guarantee to cover the whole network region? The key is up to the angle θ shown in Figure 2. From the discussion above, θ determines the number of nodes which are needed to be deployed. In this sense, θ relates with not only the whole energy consumption, but also the network coverage rate.

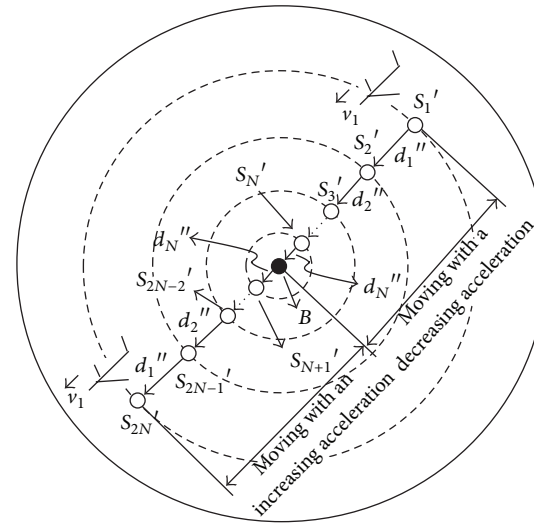


Figure 5: Result of single air broadcasting with straight-line motion.

In [25], in a concentric circle deployed network, the author finds that the whole circular region could be ensured covered if and only if the circumference composed of the outermost nodes satisfies the requirement of network coverage rate. Assume node sensing radius is R. Let $d_1 = R$ and make sure the sensing circles of two outermost nodes, which are deployed in neighboring broadcastings, are tangent. Figure 6 proves that when the broadcasting angle is θ, except in several small regions at the fringe of the network (demonstrated as the shaded parts in Figure 6), a casual point in the network is covered by at least one node. Consider

$$\sin\theta = \frac{2R\sqrt{\left(\sum_{i=1}^{N} d_i''\right)^2 - R^2}}{\left(\sum_{i=1}^{N} d_i''\right)^2}, \quad (15)$$

$$R + \sum_{i=1}^{N} d_i'' = L.$$

So

$$\theta = \arcsin \frac{2R\sqrt{\left(\sum_{i=1}^{N} d_i''\right)^2 - R^2}}{\left(\sum_{i=1}^{N} d_i''\right)^2}. \quad (16)$$

To the whole network, the number of times of straight-line broadcastings is $\lceil \pi/\theta \rceil$, while the number of deployed nodes is $2N\lceil \pi/\theta \rceil$. In addition, v_1 should meet the following equation:

$$v_1 \times \sqrt{\frac{2h}{g}} = R. \quad (17)$$

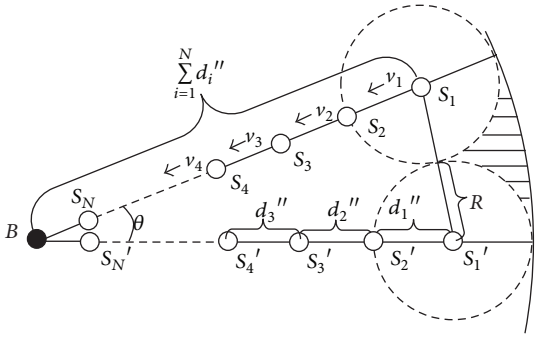


Figure 6: Coverage rate guaranteed air broadcasting deployment scheme.

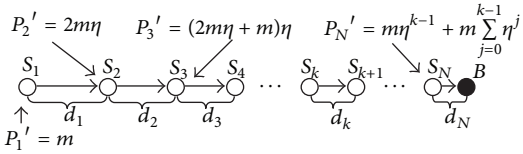


Figure 7: Energy balance oriented deployment with data fusion.

3.4. Energy Balancing Deployment Scheme with Data Fusion. In a previous energy balance oriented deployment strategy and fixed interval air broadcasting with a variable acceleration motion, it is assumed that the schemes ignore the data fusion. However, in real WSNs, as the sensing regions overlap and the redundancy cannot be neglected, it is necessary to do data fusion in relaying nodes.

Here, we analyze the deployment method for linear structures as Figure 7 shows. Given that the data fusion ratio is η and the bit number of data one-time gathered by a node is m, then it is easy to figure out that the bit numbers of transmitted data are $P_1' = m$, $P_2' = 2m\eta \cdots P_N' = m\eta^{k-1} + m\sum_{j=1}^{k-1}\eta^j$. Then we can infer

$$\begin{aligned} E_2 &= mE_{\text{elec}} + 2m\eta E_{\text{elec}} + 2m\eta\varepsilon_{\text{amp}}d_2^2 + 2me, \\ E_3 &= 2m\eta E_{\text{elec}} + (2m\eta + m)\eta E_{\text{elec}} \\ &\quad + (2m\eta + m)\eta\varepsilon_{\text{amp}}d_3^2 + (2m\eta + m)e \\ &\vdots \end{aligned} \tag{18}$$

Denote e as the energy expenditure for fusion of unit number bit of data. Use mathematical induction and then get

$$\begin{aligned} E_k &= \left(m\eta^{k-2} + m\eta^{k-1} + m\sum_{j=1}^{k-2}\eta^j + m\sum_{j=1}^{k-1}\eta^j\right)E_{\text{elec}} \\ &\quad + \left(m\eta^{k-1} + m\sum_{j=1}^{k-1}\eta^j\right)\varepsilon_{\text{amp}}d_k^2 \\ &\quad + \left(m\eta^{k-2} + m\sum_{j=0}^{k-2}\eta^j\right)e \quad (k \geq 2). \end{aligned} \tag{19}$$

As η is a number less than one, η^k is approaching zero. So, E_k can be expressed approximately as

$$\begin{aligned} E_k &\approx \left(m\sum_{j=1}^{k-2}\eta^j + m\sum_{j=1}^{k-1}\eta^j\right)E_{\text{elec}} \\ &\quad + \varepsilon_{\text{amp}}d_k^2 m\sum_{j=1}^{k-1}\eta^j + em\sum_{j=0}^{k-2}\eta^j. \end{aligned} \tag{20}$$

In the same way, we get

$$\begin{aligned} E_{k+1} &\approx \left(m\sum_{j=1}^{k-1}\eta^j + m\sum_{j=1}^{k}\eta^j\right)E_{\text{elec}} \\ &\quad + \varepsilon_{\text{amp}}d_{k+1}^2 m\sum_{j=1}^{k}\eta^j + em\sum_{j=0}^{k-1}\eta^j, \end{aligned} \tag{21}$$

then we can infer

$$d_{k+1} = \sqrt{\left(\frac{1-\eta^{k-1}}{1-\eta^k}\right)d_k^2 - \left[\frac{\left(\eta^{k+1}+\eta^k\right)E_{\text{elec}} + \eta^{k-1}e}{\varepsilon_{\text{amp}}\sum_{j=1}^{k}\eta^j}\right]}, \tag{22}$$

for $(1-\eta^{k-1})/(1-\eta^k)$ is always less than one and is approaching one while the value of $((\eta^{k+1}+\eta^k)E_{\text{elec}} + \eta^{k-1}e)/\varepsilon_{\text{amp}}\sum_{j=1}^{k}\eta^j$ is approaching zero with the increase of k; d_{k+1} is always smaller than d_k and will approach d_k with the increase of k as well. It is similar to the energy balancing deployment and air broadcasting method with a variable acceleration movement, which is not considering data fusion. Therefore, the new strategy in this paper can be simulated as the deployment with data fusion.

4. Simulation Results

4.1. Simulation Environment. To testify the properties of the deployment of broadcasting nodes with a variable acceleration movement, the simulation is operated under Omnet++3.2 and Matlab7.0. The values of the deployment under test are deployment effect, network residual energy, and its standard deviation. Then we compare the result of the test with that of IEA method and the uniform and random broadcasting methods. Set the network as a circle with 900 meters radius and the major parameters are shown in Table 1.

4.2. Simulation Result. Figures 8 and 9 show the simulation results of broadcasting with variable acceleration straight-line movement and energy balancing deployment without data fusion. From the simulation, the effects of the two deployments are nearly the same, and the density of nodes increases as the distance from the base station decreases. In the method proposed in this paper, the hop distance between two nodes far away from the base station is a little less than the hop distance in energy balancing deployment model, while the density of nodes near the base station is a little less than that in energy balancing deployment model.

Table 1: The major parameters of simulation.

Simulation parameters	Symbol	Value	Unit
Network size	S	$900^2 \times \pi$	m^2
Maximum node sensing radius	R	100	m
Node initial energy	E_{init}	10	J
Height of broadcasting	h	125	m
Initial velocity of thrower	v_1	20	m/s
Initial acceleration of thrower	a_0	0.3	m/s^2
Acceleration changing rate	r	0.003	m/s^3
Unit energy consumption of transceiver	E_{elec}	50	nJ/bit
Unit energy consumption of amplifier	ε_{amp}	100	$pJ/bit/m^2$
Broadcasting interval	T	12	s

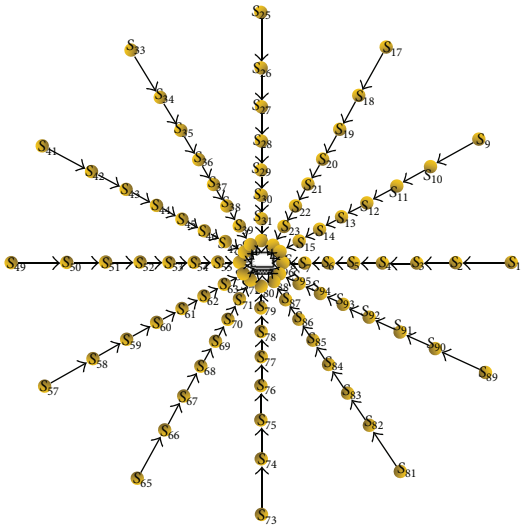


Figure 8: Effect of broadcasting with variable acceleration straight-line movement.

Figures 10 and 11 show the average residual energy of nodes and their standard deviation. As the broadcasting result of our method is similar to the result of energy balancing linear deployment model, the residual energy will reach its maximum and its standard derivation will reach its minimum, which means it has the best energy balance. In a nascent condition of the network, IEA method can achieve a good energy balance as well, and it is nearly the same with the air broadcasting with variable acceleration movement. However, its initial energy setting is just based on the distance from that node to the base station, and the difference of initial energy of neighboring nodes is constant, so after the network operates for a long time, the energy balance will be broken and the result of IEA is close to uniform broadcasting. It is also easy to find that the residual energy of a node is least and the property of energy balancing is worst under random broadcasting deployment.

It should be noted that after the network operates for 1800 turns, the standard derivations of node residual energy in uniform and random broadcasting undergo a significant decrease. It is because there appear a lot of dead nodes, and the number of living nodes reduces rapidly. Therefore, the difference of each node's residual energy is not significant.

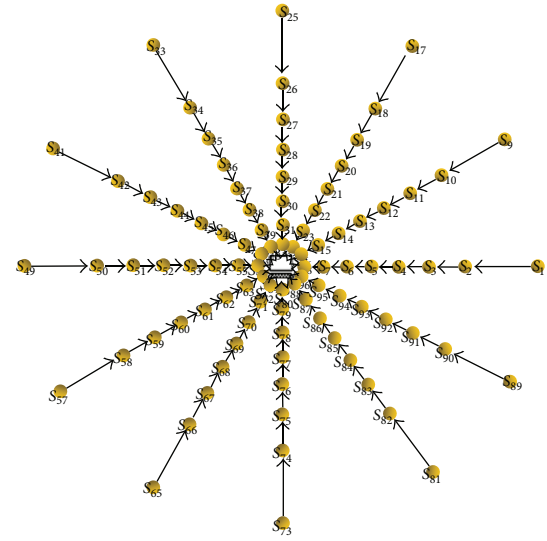


Figure 9: Effect of energy balancing deployment.

Figures 12 and 13 demonstrate a comparison between our method and the two energy balancing ensured theoretical deployment models. It can be concluded that whether or not to execute data fusion, our method shows no difference in residual energy and its standard derivation. So, it is proved that the deployment of air broadcasting with variable acceleration movement is able to, in some sense, achieve an energy balance. In addition, the deployment on the condition of data fusion should pay attention to the energy balance for data transmission and fusion; its property of energy balancing is a little worse compared with the condition of not adopting data fusion operation, and their property difference will be enhanced as the network operates.

To testify the effects of the variation of parameters in the simulation, we set T to 10 s, 12 s, and 14 s, respectively, and then observe and compare the effect of the deployment and energy consumption. The comparison is shown in Figures 14 and 15.

From the figures, we note that a too large or short interval T will make the effect of deployment depart from the promised prospect, causing an unbalance of energy consumption. If T is set to a feasible value, after an air broadcasting with a variable acceleration movement, the hop distance between neighboring nodes in the network will correspond with the energy balancing deployment model, showing a good energy balance.

Figures 16 and 17 show the energy balancing analysis on the condition of different data fusion ratio. If the ratio of data fusion is low ($\eta = 0.9$), the data transmission pressure of nodes is not significantly decreased. In such circumstance, the effect of network deployment is like that of the energy balance oriented deployment which makes a good energy balance. However, if the ratio of data fusion is relatively high ($\eta = 0.7$), the quantity of transmission data is significantly decreased, especially for the nodes near the base station. In this circumstance, the standard derivation of residual energy comes to increase but, however, is still far less than the derivation in uniform and random broadcasting.

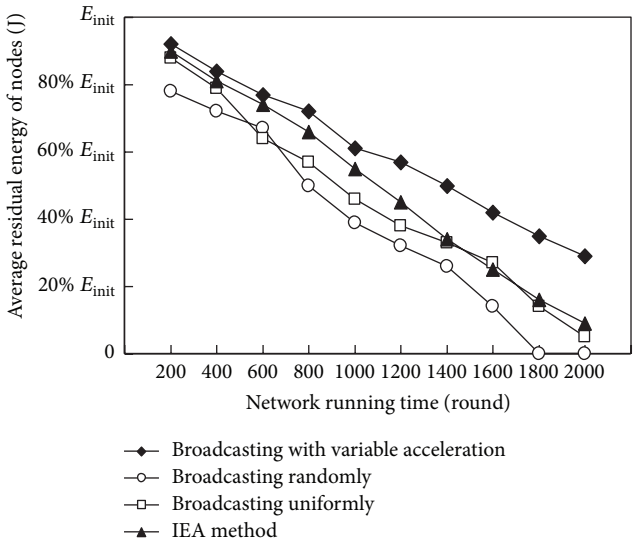


Figure 10: Average node residual energy in different deployments.

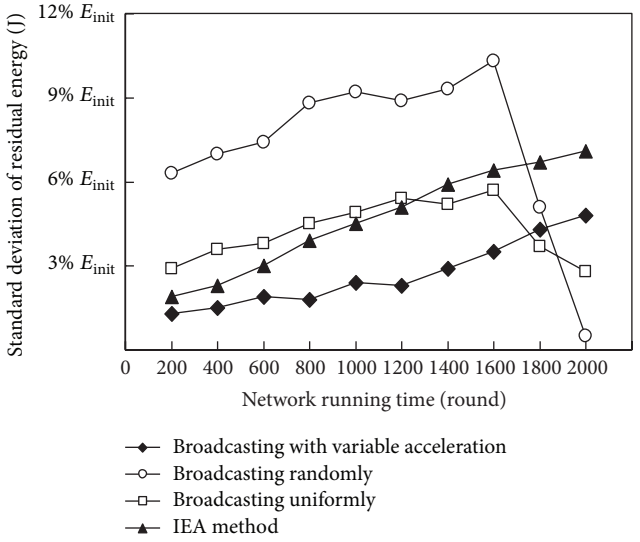


Figure 11: Standard derivation of residual energy in different deployments.

5. Conclusion

This paper utilizes a variable acceleration movement model to propose a broadcasting scheme to simulate the energy balance oriented deployment model. Based on the consideration of coverage rate, a practical implementation process is provided. The analysis of its simulation result proves this new deployment approaches the theoretical deployment and achieves a good energy balance.

Acknowledgments

The subject is sponsored by the National Natural Science Foundation of China (61202355), Research Fund for the Doctoral Program of Higher Education of China (20123223120006), China Postdoctoral Science Foundation (2013M531394), Natural Science Foundation of Jiangsu Province (BK2012436), Jiangsu Provincial Research Scheme of Natural Science for Higher Education Institutions (11KJB520014), Postdoctoral Foundation of Jiangsu Province(1202034C), the Scientific Research Fund Project for Translation Talents of Nanjing University of Posts and Telecommunications (NY211018) and a Project funded by Priority Academic Program Development of Jiangsu Higher

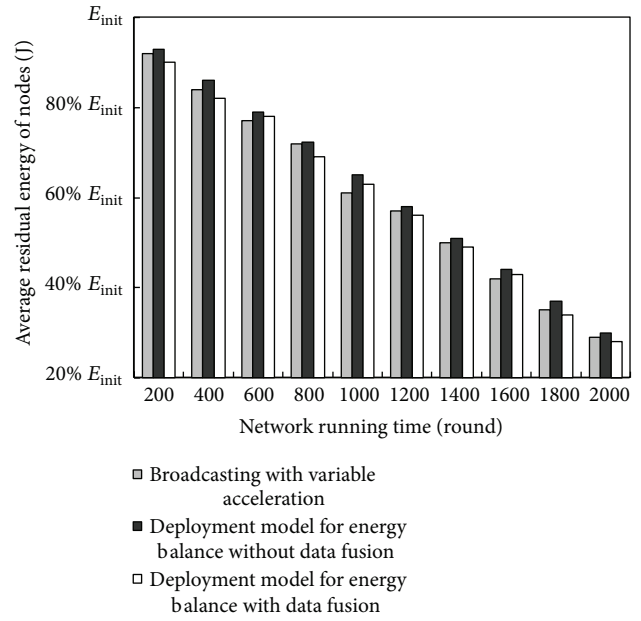


Figure 12: Average node residual energy in air broadcasting with variable acceleration movement and energy balancing deployment.

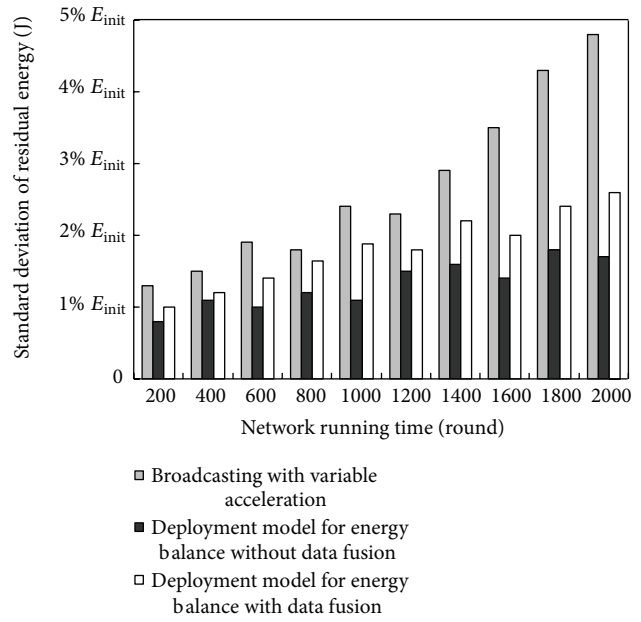


Figure 13: Standard derivation of residual energy in air broadcasting with variable acceleration movement and energy balancing deployment.

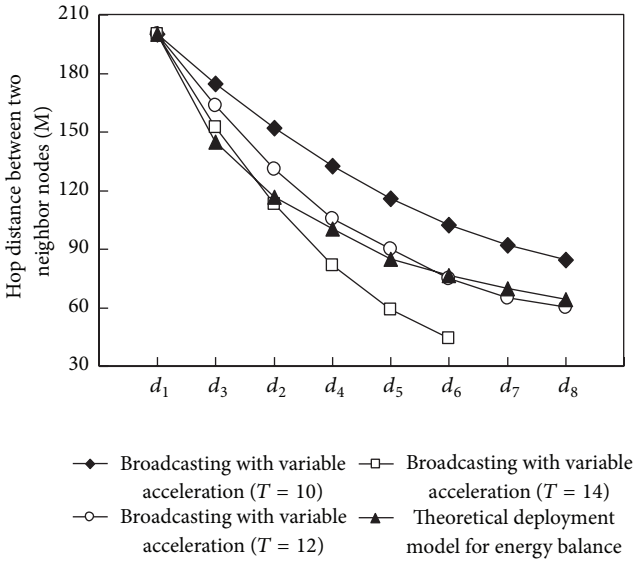


Figure 14: Effects of deployments with different interval.

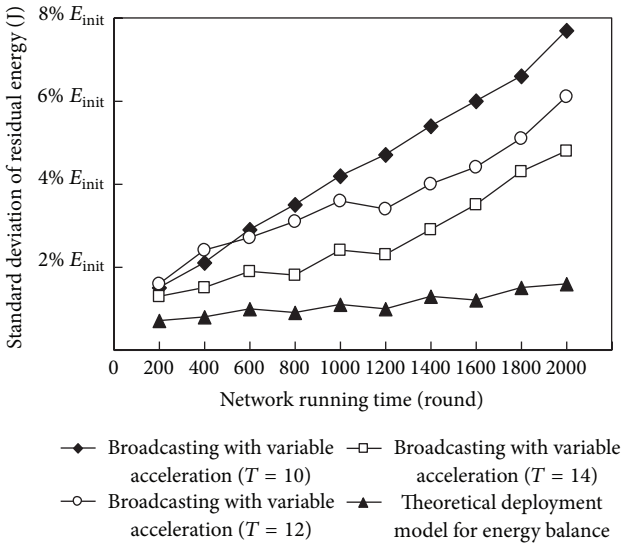


Figure 15: Standard derivation of node residual energy of deployments with different interval.

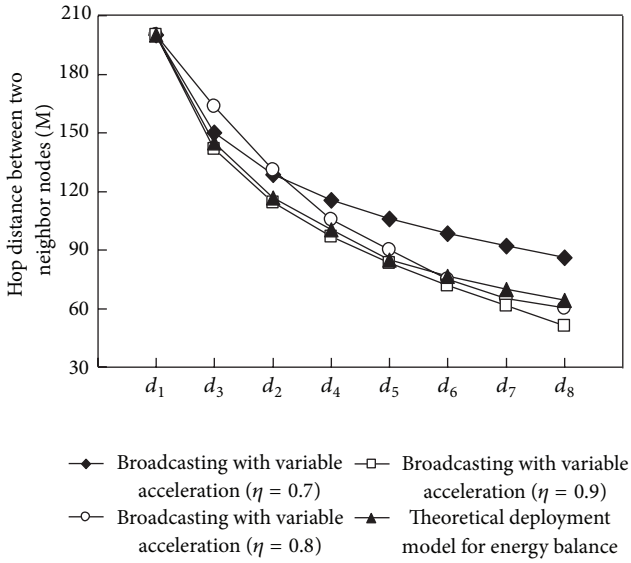


Figure 16: Effects of different deployment with different data fusion ratio.

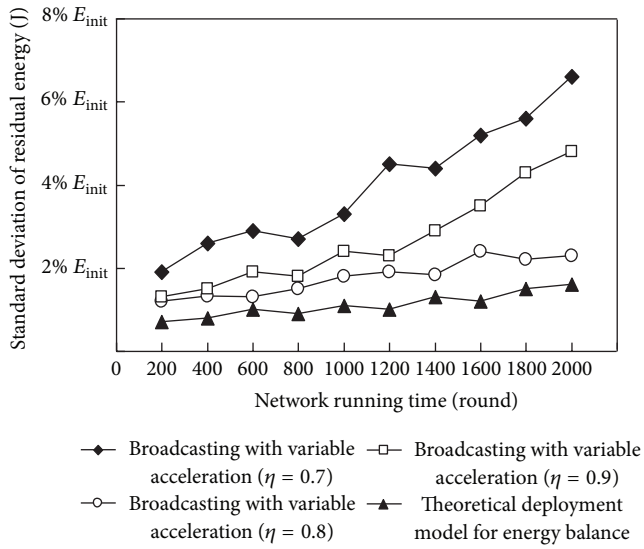


Figure 17: Standard derivation of node residual energy with different data fusion ratio.

Education Institutions (Information and Communication, YX002001).

References

[1] Z. Yun, X. Bai, D. Xuan, W. Jia, and W. Zhao, "Pattern mutation in wireless sensor deployment," *IEEE/ACM Transactions on Networking*, vol. 20, no. 6, pp. 1964–1977, 2012.

[2] K. Xu, H. Hassanein, G. Takahara, and Q. Wang, "Relay node deployment strategies in heterogeneous wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 9, no. 2, pp. 145–159, 2010.

[3] L. Qing, Q. Zhu, and M. Wang, "Distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks," *Journal of Software*, vol. 17, no. 3, pp. 481–489, 2006.

[4] Y. Shen, W. Qi, and H. Dai, "Energy efficient clustering protocol for surveillance sensor networks," *Journal of Software*, vol. 19, no. 9, pp. 2432–2441, 2008.

[5] G. Lu, M. Zhou, K. She, X. Niu, H. Liu, and F. Zheng, "Lifetime analysis on routing protocols of wireless sensor networks," *Journal of Software*, vol. 20, no. 2, pp. 375–393, 2009.

[6] X. Wang, S. Han, Y. Wu, and X. Wang, "Coverage and energy consumption control in mobile heterogeneous wireless sensor networks," *IEEE Transactions on Automatic Control*, vol. 58, no. 4, pp. 975–988, 2013.

[7] R. Yan, H. Sun, and Y. Qian, "Energy-aware sensor node design with its application in wireless sensor networks," *IEEE Transactions on Instrumentation and Measurement*, vol. 62, no. 5, pp. 1183–1191, 2013.

[8] T. M. Chiwewe and G. P. Hancke, "A distributed topology control technique for low interference and energy efficiency in wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 8, no. 1, pp. 11–19, 2012.

[9] Y. Liu, Q. Zhang, and L. Ni, "Opportunity-based topology control in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 3, pp. 405–416, 2010.

[10] S. Chamberland, L. Cobo, F. Mourchid, and A. Quintero, "A wireless sensor network deployment model with target localization constraints," in *Proceedings of the 15th International Symposium on Telecommunications Network Strategy and Planning (NETWORKS '12)*, pp. 1–4, 2012.

[11] C. E. Otero, I. Kostanic, A. Peter, A. Ejnioui, and L. D. Otero, "Intelligent system for predicting wireless sensor network performance in on-demand deployments," in *Proceedings of the IEEE Conference on Open Systems (ICOS '12)*, pp. 1–6, 2012.

[12] X. Liu, "Sensor deployment of wireless sensor networks based on ant colony optimization with three classes of ant transitions," *IEEE Communications Letters*, vol. 16, no. 10, pp. 1604–1607, 2012.

[13] X. Wang and S. Wang, "Hierarchical deployment optimization for wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 10, no. 7, pp. 1028–1041, 2011.

[14] M. Liu, H. Gong, Y. Mao, L. Chen, and L. Xie, "Distributed energy-efficient data gathering and aggregation protocol for wireless sensor networks," *Journal of Software*, vol. 16, no. 12, pp. 2106–2116, 2005.

[15] A.-F. Liu, G.-J. Yang, and Z.-G. Chen, "Energy hole avoid by alternately working with different cluster-radius for wireless sensor networks," *Journal on Communications*, vol. 31, no. 1, pp. 1–8, 2010.

[16] M. H. Chaudhary and L. Vandendorpe, "Performance of power-constrained estimation in hierarchical wireless sensor networks," *IEEE Transactions on Signal Processing*, vol. 61, no. 3, pp. 724–739, 2013.

[17] R. Majumder, G. Bag, and K.-H. Kim, "Power sharing and control in distributed generation with wireless sensor networks," *IEEE Transactions on Smart Grid*, vol. 3, no. 2, pp. 618–634, 2012.

[18] X. Zhao, Z. Zhou, Z. Li, and Z. Qin, "Redundancy deployment strategy based on energy balance for wireless sensor networks," in *Proceedings of the International Symposium on Communications and Information Technologies (ISCIT '12)*, pp. 702–706, 2012.

[19] Y. Fan, X. T. Zhang, Y. D. Wan, and Q. Wang, "Nodes placement strategy for even energy consumption in wireless sensor networks," *Computer Engineering*, vol. 33, no. 16, pp. 11–14, 2007.

[20] H. Fei, *Balanced Energy Consumption Routing Schemes in WSN*, Dalian University of Technology, Dalian, China, 2007.

[21] L. Yan, *The Research of Key Technologies Based on Energy Efficiency in WSN*, Shandong University, Shandong, China, 2008.

[22] L.-J. Ren, Z.-W. Guo, and R.-Z. Ma, "Energy assignment to prolong the lifetime in heterogeneous wireless sensor network," in *Proceedings of the 7th International Conference on Machine Learning and Cybernetics (ICMLC '08)*, pp. 4057–4061, Kunming, China, July 2008.

[23] M. Soltan, I. Hwang, and M. Pedram, "Modulation-aware energy balancing in hierarchical wireless sensor networks," in *Proceedings of the 3rd International Symposium on Wireless Pervasive Computing (ISWPC '08)*, pp. 355–359, May 2008.

[24] Y. T. Hou, Y. Shi, H. D. Sherali, and S. F. Midkiff, "On energy provisioning and relay node placement for wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 4, no. 5, pp. 2579–2590, 2005.

[25] L. Ren, Z. Guo, and R. Ma, "Distance-based energy efficient placement in wireless sensor networks," in *Proceedings of the 3rd IEEE Conference on Industrial Electronics and Applications (ICIEA '08)*, pp. 2031–2035, June 2008.

[26] J.-F. Dou, Z.-W. Guo, J.-B. Cao, and G. Zhang, "Probabilities based energy balance algorithms for wireless sensor networks," *Journal of Electronics and Information Technology*, vol. 30, no. 5, pp. 1226–1229, 2008.

[27] Y. Sun, B. Jing, and Z. Zhang, "Energy efficient node placement method of wireless sensor networks based on uneven ring belt model," *Chinese Journal of Sensors and Actuators*, vol. 19, no. 4, pp. 1287–1289, 2006.

[28] M. Shuhui, *Study on the Key Algorithms Based on Energy in Wireless Sensor Networks*, Beijing University of Posts and Telecommunications, Beijing, China, 2007.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 932673, 14 pages
http://dx.doi.org/10.1155/2013/932673

Research Article

A Proximity-Based Concurrent Access Strategy to Improve Throughput in VANETs

Chen Chen,[1] Qingqi Pei,[1] Yanan Jin,[1] Shengjin Ge,[2] Xiaoji Li,[3] and Weizhi Dai[1]

[1] *State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China*
[2] *CCCC First Highway Consultants Co. Ltd., Xi'an 710075, China*
[3] *Guilin University of Electronic Technology, Guilin 541004, China*

Correspondence should be addressed to Chen Chen; cchen44@utk.edu

Received 12 April 2013; Accepted 17 June 2013

Academic Editor: Shukui Zhang

Intervehicle communication gives vehicles opportunities to exchange packets within limited transmission ranges and self-organize with ad hoc manner into VANETs (vehicular ad hoc networks). However, due to shared spectrum and present collisions' resolution mechanism which reject new admissions when wireless medium is busy, communications between vehicles have experienced severe throughput degradation and been restrained for concurrent transmissions. In this paper, a PCM (proximity-based concurrent transmission MAC) protocol has been proposed to permit concurrent access in shared channel for improving goodput in VANETs. By introducing game theory to the concurrent transmission opportunities determination process, PCM could provide extra access chances between active nodes or vehicles based on our defined proximity. To make PCM practical, we further give a detailed implementation method on NS2 to evaluate its performance. Numerical results show that PCM is not only feasible and reasonable in theory, but also has great improvement on average transmission delay, delivery ratio, and throughput performance in test.

1. Introduction

1.1. Introduction of VANET. Vehicular ad hoc networks [1–3] (VANETs) are distributed, self-organizing communication networks built up by moving vehicles and RSUs (roadside units), and are thus characterized by very high node mobility and limited degrees of freedom in the mobility patterns. The discussed IEEE 1609 Wireless Access in Vehicular Environments [4] (WAVE) draft is being developed for VANETs applications including mainly safety-related scenarios, such as cooperative forward collision warning [5] (CCW), traffic signal violation warning [6], lane change warning [7], and some information applications [8]. The success of these critical applications all greatly depend on the effective information exchange between different vehicles or vehicles and RSUs. Unfortunately, current standard or draft does not well support the rigor requirements for these applications and has some drawbacks on throughput improvement strategies.

1.2. Motivation. In VANETs, applications, especially those safety-related, extremely rely on the successful receiving of packets on road. For instance, an emergent broadcasting for accident notification should be reliably delivered to destinations to avoid crash. In bad weather, detected sloppy or frozen road surface condition needs to be rapidly notified to following vehicles by wireless signals. In highway ramp merge case, wireless packets should be received by the possible collided vehicles to prompt the mutual existence accurately. Even in non-safety-related scenarios, effective information receiving also impacts greatly on experience for trip comfortableness and convenience. When the traffic light is red, vehicles are assembling around intersections, and it is a good chance for them to exchange their local collected information within limited time. When intervehicle media sharing or video game has been established, high packets throughput means fluent playback and few frames skipping. In general, effective information exchange is curial to services in VANETs.

However, the present popular protocol stacks, such as IEEE 802.11p which has been referenced as a de facto standard for next generation vehicular networks, is suffering a great throughput degradation which may severely decrease information exchanging efficiency. In MAC layer description in IEEE 802.11p, EDCA (enhanced distribution coordinate access) still serves as the mechanism for multiuser access. Although differentiated service is introduced, the throughput could not be greatly increased due to the CSMA/CA-based collision resolution strategy. For instance, when using RTS/CTS handshakes as contention resolve solution, all neighbors should be silent during the period indicated by the network allocation vector (NAV) in RTS or CTS packets. In other words, an ongoing transmitting under CSMA/CA mechanism inevitably affects others due to the shared spectrum. In fact, even small wireless devices can cause strong interferences for others, thus severely decreasing the overall throughput. Thereupon, a well designed strategy should be presented to overcome this inborn drawback of CSMA/CA and increase the achievable network throughput by permitting concurrent ongoing transmissions. In our work, to increase the precious access opportunity, we designed a new MAC layer protocol which permits concurrent ongoing transmissions existence based on IEEE 802.11p draft. We proposed a metric "proximity" to help to determine the requirement for concurrent transmission and also gave the implementation details to carry out our protocol in VANETs.

The rest of this paper is organized as follows. In Section 2, we outline previous related works. In Section 3, the proposed proximity-based concurrent transmission game is introduced. The implementation details are issued in Section 4. Numerical results and discussions are given in Section 4 followed by conclusion in Section 5 and acknowledgment section.

2. Related Works

In VANETs, which in general lack fixed communication infrastructure, a wise and intelligent decision is hard to be made in a distributed manner. However, RSUs, which are introduced to enhance network performance, can make this work easy. After enough information is collected on RSUs, an intelligent decision could be made with fairness and effectiveness. However, although RSUs can act as the decision-making center, they also readily become the bottleneck of its covered area especially when multiple packets are possibly transmitted to it simultaneously. Therefore, how to handle the concurrent transmitting and make full use of the provided broad bandwidth is very crucial to the up-to-datedness of information and driving safety.

To reach this goal, a distributed algorithm on each node is necessary to make its own decision whether to transmit to the RSUs or not. If choosing to send, the concurrent transmitted signals on the fly could together output a feasible SINR for each participated node and not make the network load saturation. For this distributed decision making problem, one of the best candidates is the game theory which has been largely applied to the wireless resource allocation scenarios [9–12]. The main advantage of a game-theory-based scheme is that, by turning nodes into selfish players for pursing high payoff, an otherwise complex system can reach efficient outcomes in a lightweight and distributed manner. To apply game theory to our discussed problem, the difficulty lies in obtaining complete information of nodes under dynamic network state variation and high mobility, where information broadcasting is also useless to reflect the exact and real-time distributed global situations. Although there were some topics on wireless resource allocation [13], attacks classification [14], transmission selection [15], and others in ad hoc network based on incomplete information game, to our best knowledge, for our later described "proximity"-based concurrent transmission strategy which relies on incomplete information game, there are few related works.

For concurrent transmission strategy research, there mainly exist two categories of schemes: game-theory-based and TPC-(transmission power control-) based concurrent transmission proposals. The former can be further classified into three classes: NE-based backoff time adaptation [9], NE-based power control [16, 17], and NE-based transmission schemes depending on channel conditions [18]. For NE-based determination scheme used in wireless networks especially in ad hoc networks, most works have been done around wireless resources allocation such as radio frequency, available bandwidth, and transmitting power. Generally speaking, any resource-limited allocation or assignment problems are candidates for NE determination. Usually, since concurrent transmission opportunity is decided by SINR, the most relevant resources for this determination problem are NE-based power control. Saraydar et al. [19] proposed a game-theory-based power control algorithm for data transmissions in cellular networks to increase capacity and extend lifecycle. Although the paper was not putting focus on concurrent transmission, the work has been recognized as the base of followed concurrent transmission research papers because capacity growing is common to concurrent transmission opportunities increasing. Wang et al. [20] proposed G-MAC with adaptive power control to make nodes plan their transmissions simultaneously in an ad hoc manner. Their works frame the concurrent transmission problem as a complete information noncooperative power control game to find the transmitting power threshold meeting SINR need. Adlakha et al. [21] proposed a Bayesian game with incomplete interference information about opponents. The game is static, say simultaneous move between nodes, for selecting a power profile over the entire available bandwidth to maximize Shannon's capacity. Lee et al. [17] developed a channel access game, which considered concurrent transmissions with different access points, under the influence of intercluster interferences. After successfully finding the Bayesian Nash equilibrium, they further presented a simple dynamic implementation procedure for nodes to efficiently find a Nash Equilibrium without knowing the number of total active nodes.

For TPC-based concurrent transmission schemes, their objectives mainly focus on either energy conservation [22, 23] or throughput improvement [24–26]. In PCMA [26], a flexible "variable bounded power" collision suppression

model was introduced. Each receiver advertises its calculated interference margin by sending busy tone pulses over a separate control channel. The PCDC protocol [25] uses two channels for data and control packets, respectively. They do not use the RTS/CTS exchange to silence the neighboring nodes. Instead, collision avoidance information is inserted into the CTS packets and is sent over the control channel. The information is used to dynamically bound the transmitting power of potentially interfering nodes in the vicinity of a receiver to allow for interference-limited simultaneous transmissions. Being different from the above two multichannel concurrent transmission schemes, POWMAC [24] uses a single channel for both data and control packets. The scheme adjusts the transmitting power of data packets to allow for some interference margin at the receiver. Therefore, multiple interference-limited transmissions near a receiver are allowed to overlap in time, provided their multiaccess interference (MAI) effects do not lead to collisions at nearby receivers. Although there were some works focusing on concurrent transmission solutions in VANETs, such as those of Sun et al. [27] and Nittel et al. [28], there are design schemes under multi-channel or enabling cognitive radio, which is much different from our work only requiring single channel.

In summary, our work has mainly two contributions as follows. First, we have given a simple but efficient way to determine the concurrent transmission occasion in our discussed scenario in VANETs; second, we implemented this scheme on NS2 platform and evaluated the output performance.

3. Model Description

3.1. Discussed Scenario and Assumptions. The discussed scenario is demonstrated in Figure 1.

There are two kinds of vehicles, that is, high-speed cars numbered from 1 to N and the low-speed buses which have access points installed with large radio coverage. The buses here serve for the packets exchange between different cars or cars and internet. For information exchange between cars, the buses act as store-carry-forward nodes to provide indirect connections between sources and destinations. In this way, the packets or bursts can be stored temporarily when target is not reachable and forwarded later with movement. Another important capability of buses is serving as the mobile RSUs, which are necessary equipments in VANETs to provide broad access bandwidth and large communication range.

Before giving our proposed model, we first present the definition of "proximity" and some assumptions.

Definition 1. Proximity is defined as the intimacy level between cars and buses and expressed by

$$e_i = \frac{1}{d_i} \tag{1}$$

for car i, where d_i is the distance between i and its affiliated bus.

The affiliate relation indicates whether the given car is within the radio range of the investigated bus. If there is more than one bus covering the same car, the affiliated bus is the one with the maximum proximity to i. To make our model practical, the following assumptions are given.

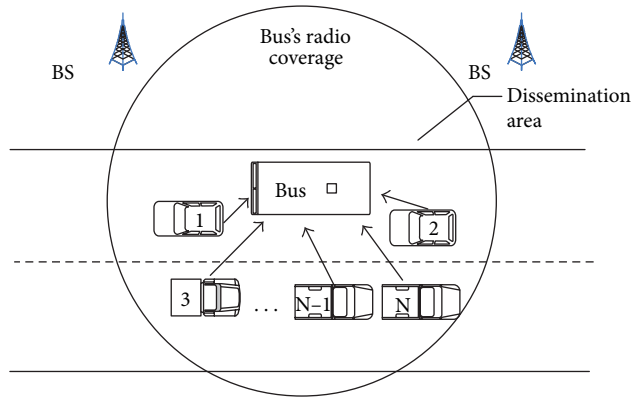


Figure 1: Discussed scenario.

Assumption 2. The total amount of active nodes can be obtained by some estimation methods [29, 30].

Assumption 3. Transmission power is fixed to 1 for simplicity and adaptive power control (APC) is disabled considering hardware complexity.

Assumption 4. The packets to be sent are delay tolerant and could be buffered for future transmission. This assumption is reasonable for the low-duty cycle periodical applications such as road condition report and congestion notification.

Assumption 5. The distances between sources and destinations can be readily obtained by the receive signal strength indicator (RSSI) under LOS (line of sight) environment or hybrid TOA/AOA [31] algorithms under NLOS (non-line-of-sight) circumstance.

3.2. Transmission Model. Now we describe the proposed transmission model and propagation model. We discuss the scenario in which all vehicles communicate on the same channel. Thus, for a given transmitter, any other signal at the intended receiver is regarded as the interference to this transmission. We assume that packets from a particular vehicle can be transmitted to its intended receiver at a rate not exceeding C bps, provided that the SINR at the receiver does not fall below a threshold $\mathrm{SINR}_{\mathrm{th}}$. In general, $\mathrm{SINR}_{\mathrm{th}}$ depends on the modulation technique, the desired bit error rate, the required transmission rate, and the coding strategy employed. Here, according to Figure 1, we define the SINR for the successful transmission of any given vehicle i as

$$\gamma_i = \frac{h_i P_i}{\alpha \sum_{j \in \chi_i} h_j P_j + \sigma^2} \geq \mathrm{SINR}_{\mathrm{th}}, \tag{2}$$

where P_i is the power of vehicle i and h_i is the channel gain between i and its receiver. α is the crosstalk interference ratio to adjust the influence from signal interferences. χ_i is the set of all interfering nodes for i and σ^2 is the variance of

AWGN with mean 0. Then, for any given propagation model in wireless communications, we have the following equation:

$$P_r(t) = P(t)\, h(d(t)), \tag{3}$$

where $P(t)$, $P_r(t)$ indicate the transmitting power at sender and the signal strength at receiver, respectively, at moment t. $h(d)$ denotes the channel gain as a function of the distances between sources and destinations. In most of the previous studies [32, 33], $h(d)$ is expressed as $(d)^{-\beta}$, where β is the path loss factor with an empirical value of $\beta = 1.6 \sim 6$. Nevertheless, this relation becomes invalid when the distance d between transmitter and receiver drops below 1, where $P_r(t)$ will exceed $P(t)$ based on (3) and $P_r(t)$ will have arbitrarily large value as d becomes sufficiently small. This problem was also noticed in aforementioned works [26, 27], and some measurements have been given to handle it. In our work, to obtain reasonable results when d is less than 1 and at the same time keep the relationship when d is greater than or equal to 1, the following channel gain expression was presented:

$$h(d) = (1+d)^{-\beta}, \quad d > 0. \tag{4}$$

Now, with (1) and (4), we have

$$h_i = \left(1 + \frac{1}{e_i}\right)^{-\beta}. \tag{5}$$

3.3. Proposed Proximity-Based Concurrent Transmission Game (PCM). Based on the above transmission model and the proximity concept, we could define a channel access strategy by introducing incomplete information game theory. The definitions of utility function for reflecting award and price are expressed as follows.

Definition 6 (static channel access game). We formulate an interference-aware channel access game as follows.

(i) *Players*: there are a bus and N players, with each player $i \in \{1, 2, \ldots, N\}$ having a distance d_i from the bus, where $d_i \geqslant 0$.

(ii) *Actions*: $a_i \in \{T, W\}$; that is, transmit or wait for all players.

(iii) *Payoff function*:

$$u_i(a_i, \mathbf{a}_{-\mathbf{i}}; e_i) = \begin{cases} \prod_{i=1}^{n} (W, \mathbf{a}_{-\mathbf{i}}) = 0, & a_i = W, \\ \prod_{i=1}^{n} (T, \mathbf{a}_{-\mathbf{i}}) = R_i(a_{-i}) - c(P_i), & a_i = T. \end{cases} \tag{6}$$

$R_i(\mathbf{a}_{-\mathbf{i}})$ is the network throughput, which is expressed by

$$R_i(\mathbf{a}_{-\mathbf{i}}) = \begin{cases} \log(1+\gamma_i) & \gamma_i \geq \mathrm{SINR}_{\mathrm{th}}, \\ 0 & \text{else}, \end{cases}$$

$$\gamma_i = \frac{(1+(1/e_i))^{-\beta}}{\alpha \sum_{j \in \chi_i} \left(1 + \left(1/e_j\right)\right)^{-\beta} + \sigma^2}, \qquad \chi_i = \left\{ j \neq i : a_j = T \right\}. \tag{7}$$

$c(P_i) = \mu(P_i/h_i) = \mu/(1+(1/e_i))^{-\beta}$ is the price formula denoting the cost for transmission. The definition for price function has twofold meanings: one for pricing each transmitting attempt indicated by μ and the other for denoting the relation that channel gain is in inverse proportion to the transmitting cost or price. That is, the larger the channel gain is, the less the cost is needed for nodes to transmit. The definition also presents the potential meaning for the proximity variable, that is, e_i. That is, a bigger e_i will make node i more intimate with the bus, thus paying less effort to contact with the bus. In other words, a larger proximity or a shorter distance between a given node and the bus indicates the smaller probability for severe channel fading or gain degradation.

Definition 7. $a_i^*(e_i)$ is a Bayesian Nash equilibrium if and only if

$$\begin{aligned} a_i^*(e_i) &\in \arg\max_{a_i} \sum_{e_{-\mathbf{i}}} p_i(e_{-\mathbf{i}} \mid e_i) \cdot u_i(a_i, \mathbf{a}_{-\mathbf{i}}^*(e_{-\mathbf{i}}); e_i, e_{-\mathbf{i}}) \\ &= \arg\max_{a_i} E\left[\prod_{i=1}^{n} (a_i, \mathbf{a}_{-\mathbf{i}}^*(e_{-\mathbf{i}}) \mid e_i)\right]. \end{aligned} \tag{8}$$

Definition 8. In a Bayesian Nash equilibrium, player i will play Transmit if and only if

$$E\left[\prod_{i=1}^{n} (T, \mathbf{a}_{-\mathbf{i}}^*(e_{-\mathbf{i}}) \mid e_i)\right] \geq E\left[\prod_{i=1}^{n} (W, \mathbf{a}_{-\mathbf{i}}^*(e_{-\mathbf{i}}) \mid e_i)\right]. \tag{9}$$

3.4. Proof for the Existence and Uniqueness of NE

Lemma 9. *The NE for our proposed game is existent. To prove this proposition, the nonemptiness of strategy space and convex/quasiconvex property of utility function is needed to be verified.*

Proof. (a) Obviously, the strategy space of our game is nonempty.

(b) The payment function is continuous and quasiconvex due to

$$\begin{aligned} \frac{\partial^2 u_i}{\partial {e_i}^2} &= -\frac{1}{\left((1+(1/e_i))^{-\beta} + \alpha \sum_{j \in \chi_i} \left(1 + \left(1/e_j\right)\right)^{-\beta} + \sigma^2\right)^2} \\ &\quad - \frac{2\mu}{(1+(1/e_i))^{-3\beta}} < 0. \end{aligned} \tag{10}$$

□

Lemma 10. *The NE for our proposed game is unique. To prove this proposition, the positive definiteness and monotonicity of our game are needed to be verified.*

(a) Positive definiteness: that is, prove

$$E\left[\prod_{i=1}^{n} (T, \mathbf{a}_{-\mathbf{i}}(e_{-\mathbf{i}}) \mid e_i)\right] > 0. \tag{11}$$

Proof.

$$\frac{\partial E\left[\prod_{i=1}^{n}\left(T,\mathbf{a}_{-\mathbf{i}}\left(e_{-\mathbf{i}}\right)\mid e_i\right)\right]}{\partial e_i}>0. \tag{12}$$

The BNE about e satisfies

$$E\left[\prod_{i=1}^{n}\left(T,\mathbf{a}_{-\mathbf{i}}\left(e_{-\mathbf{i}}\right)\mid e_{\text{th}}\right)\right]=0. \tag{13}$$

So, with (12) and (13), one has

$$E\left[\prod_{i=1}^{n}\left(T,\mathbf{a}_{-\mathbf{i}}\left(e_{-\mathbf{i}}\right)\mid e_i\right)\right]>0\quad\left(e_i>e_{\text{th}}\right). \tag{14}$$

□

(b) Monotonicity: that is, prove that for all $\varepsilon>0$,

$$E\left[\prod_{i=1}^{n}\left(T,\mathbf{a}_{-\mathbf{i}}\left(e_{-\mathbf{i}}\right)\mid e_i+\varepsilon\right)\right]\geq E\left[\prod_{i=1}^{n}\left(T,\mathbf{a}_{-\mathbf{i}}\left(e_{-\mathbf{i}}\right)\mid e_i\right)\right]. \tag{15}$$

Proof.

$$\begin{aligned}&E\left[\prod_{i=1}^{n}\left(T,\mathbf{a}_{-\mathbf{i}}\left(e_{-\mathbf{i}}\right)\mid e_i\right)\right]\\&=\sum_{\chi_i\cup\overline{\chi}_i=\{1,\ldots,n\}-\{i\}}\int_{\psi}\left(\log\left(1+\frac{\left(1+\left(1/e_i\right)\right)^{-\beta}}{\alpha\sum_{j\in\chi_i}\left(1+\left(1/e_j\right)\right)^{-\beta}+\sigma^2}\right)\right.\\&\qquad\left.-\frac{\mu}{\left(1+\left(1/e_i\right)\right)^{-\beta}}\right)\cdot p\left(e_{-\mathbf{i}}\right)de_{-\mathbf{i}},\end{aligned} \tag{16}$$

where

$$\begin{aligned}\psi=\Bigg\{&e_{-\mathbf{i}}\mid\sum_{j\in\chi_i}\left(1+\frac{1}{e_j}\right)^{-\beta}\\&\leq\frac{1}{\alpha}\left(\frac{\left(1+\left(1/e_i\right)\right)^{-\beta}}{\text{SINR}_{\text{th}}}-\sigma^2\right),\\&a_i\left(e_i\right)=T,\ \forall j\in\chi_i;\ a_j\left(e_j\right)=W,\ \forall j\in\overline{\chi}_i;\Bigg\}\subset\\\overline{\psi}=\Bigg\{&e_{-\mathbf{i}}\mid\sum_{j\in\chi_i}\left(1+\frac{1}{e_j}\right)^{-\beta}\\&\leq\frac{1}{\alpha}\left(\frac{\left(1+\left(1/\left(e_i+\varepsilon\right)\right)\right)^{-\beta}}{\text{SINR}_{\text{th}}}-\sigma^2\right),\\&a_i\left(e_i\right)=T,\ \forall j\in\chi_i;\ a_j\left(e_j\right)=W,\ \forall j\in\overline{\chi}_i;\Bigg\}.\end{aligned} \tag{17}$$

Because

$$\begin{aligned}&\int_{\overline{\psi}}\left(\log\left(1+\frac{\left(1+\left(1/\left(e_i+\varepsilon\right)\right)\right)^{-\beta}}{\alpha\sum_{j\in\chi_i}\left(1+\left(1/e_j\right)\right)^{-\beta}+\sigma^2}\right)\right.\\&\qquad\left.-\frac{\mu}{\left(1+\left(1/\left(e_i+\varepsilon\right)\right)\right)^{-\beta}}\right)p\left(e_{-\mathbf{i}}\right)de_{-\mathbf{i}}\\&\geq\int_{\psi}\left(\log\left(1+\frac{\left(1+\left(1/\left(e_i+\varepsilon\right)\right)\right)^{-\beta}}{\alpha\sum_{j\in\chi_i}\left(1+\left(1/e_j\right)\right)^{-\beta}+\sigma^2}\right)\right.\\&\qquad\left.-\frac{\mu}{\left(1+\left(1/e_i+\varepsilon\right)\right)^{-\beta}}\right)p\left(e_{-\mathbf{i}}\right)de_{-\mathbf{i}}\\&\geq\int_{\psi}\left(\log\left(1+\frac{\left(1+\left(1/e_i\right)\right)^{-\beta}}{\alpha\sum_{j\in\chi_i}\left(1+\left(1/e_j\right)\right)^{-\beta}+\sigma^2}\right)\right.\\&\qquad\left.-\frac{\mu}{\left(1+\left(1/e_i\right)\right)^{-\beta}}\right)p\left(e_{-\mathbf{i}}\right)de_{-\mathbf{i}},\end{aligned} \tag{18}$$

thus, we have

$$E\left[\prod_{i=1}^{n}\left(T,\mathbf{a}_{-\mathbf{i}}\left(e_{-\mathbf{i}}\right)\mid e_i+\varepsilon\right)\right]\geq E\left[\prod_{i=1}^{n}\left(T,\mathbf{a}_{-\mathbf{i}}\left(e_{-\mathbf{i}}\right)\mid e_i\right)\right]. \tag{19}$$

So, conditions (a) and (b) are both satisfied. □

3.5. NE Analysis. Section 3.2 verifies the existence and uniqueness of NE for our proposed game. To further explain the working mechanism of our proximity-based access model, we then give a detailed illustration to our scheme under different number of active vehicles.

To verify the feasibility of our game by instance, we first introduce 2 vehicles and then extend this case to more nodes ($n>2$) later.

(1) $n=2$. It means that both vehicles i, j are considered as interferences for each other. We then calculate the BNE about proximity e as the concurrent transmission threshold for both vehicles. If action $a_i=T$, there are two cases.

(i) While $e_j<e_{\text{th}}$, $a_j=W$, this means that only node i could transmit. In addition, if $\gamma_1=(e_i/(e_i+1))^{\beta}/\sigma^2\geq\text{SINR}_{\text{th}}$, the sent packets from node i will be received successfully. As a result, the payoff function is

$$u_{ts1}=\log\left(1+\frac{\left(e_i/\left(e_i+1\right)\right)^{\beta}}{\sigma^2}\right)-\mu\times\left(\frac{e_i+1}{e_i}\right)^{\beta}. \tag{20}$$

(ii) While $e_j\geq e_{\text{th}}$, there are also two cases. One case is that node i transmitted and is received successfully; that is, $\gamma_2=(e_i/(e_i+1))^{\beta}/((e_j/(e_j+1))^{\beta}+\sigma^2)\geq\text{SINR}_{\text{th}}$. We define

$(e'_{\text{th}}/(e'_{\text{th}}+1))^{\beta} = ((e_i/(e_i+1))^{\beta}/\text{SINR}_{\text{th}}) - \sigma^2$; it means that the payoff function is

$$u_{ts2} = \log\left(1 + \frac{(e_i/(e_i+1))^{\beta}}{\left(e_j/\left(e_j+1\right)\right)^{\beta} + \sigma^2}\right) - \mu \times \left(\frac{e_i+1}{e_i}\right)^{\beta}, \tag{21}$$

while $e_j \geq e'_{\text{th}} = 1/((((1+d_i)^{-\beta}/\text{SINR}_{\text{th}}) - \sigma^2)^{-(1/\beta)} - 1)$. The other case is that node i transmitted but collided with j due to $\gamma_2 = (e_i/(e_i+1))^{\beta}/((e_j/(e_j+1))^{\beta} + \sigma^2) < \text{SINR}_{\text{th}}$. Thus, the payoff function is

$$u_{tf} = 0 - \mu \times \left(\frac{e_i+1}{e_i}\right)^{\beta}, \tag{22}$$

while $e_j > e'_{\text{th}}$.

With (21)–(25), we have the following.

When $e_j < e_{\text{th}}$,

$$u_{ts1} = \log\left(1 + \frac{(e_i/(e_i+1))^{\beta}}{\sigma^2}\right) - \mu \times \left(\frac{e_i+1}{e_i}\right)^{\beta}. \tag{23}$$

When $e_j \geq e_{\text{th}}$, if $e_j \leq e'_{\text{th}}$,

$$u_{ts2} = \log\left(1 + \frac{(e_i/(e_i+1))^{\beta}}{\left(e_j/\left(e_j+1\right)\right)^{\beta} + \sigma^2}\right) - \mu \times \left(\frac{e_i+1}{e_i}\right)^{\beta}.$$

$$\text{Or } e_j > e'_{\text{th}}, \qquad u_{tf} = 0 - \mu \times \left(\frac{e_i+1}{e_i}\right)^{\beta}. \tag{24}$$

We define the cumulative distribution function of random variable x as $F_e(x)$, and $\overline{F}_e(x) = 1 - F_e(x)$. With the aforementioned discussion, both nodes could optimally response to maximize their expected utilities. For instance, if node i transmits, there exists

$$\begin{aligned}
&E\left(\prod\left(T, a_j\left(e_j\right)\right) \mid e_i\right) \\
&= p\left(e_j < e_{\text{th}}\right)\left[\log\left(1+\gamma_1\right) - \mu \times \left(\frac{e_i+1}{e_i}\right)^{\beta}\right] \\
&\quad + p\left(e_j \geq e_{\text{th}}\right) \\
&\quad \times \left[p\left(\gamma_2 \geq \text{SINR}_{\text{th}} \mid e_j \geq e_{\text{th}}\right)\right. \\
&\qquad \cdot E\left(\log\left(1+\gamma_1\right) - \mu \times \left(\frac{e_i+1}{e_i}\right)^{\beta} \mid e_{\text{th}} \leq e_j \leq e'_{\text{th}}\right) \\
&\qquad \left. + P\left(\gamma_2 < \text{SINR}_{\text{th}} \mid e_j \geq e_{\text{th}}\right)\left(0 - \mu \times \left(\frac{e_i+1}{e_i}\right)^{\beta}\right)\right] \\
&= F_e\left(e_{\text{th}}\right)\left[\log\left(1+\gamma_1\right) - \mu \times \left(\frac{e_i+1}{e_i}\right)^{\beta}\right] + \overline{F}_e\left(e_{\text{th}}\right) \\
&\quad \times \left[F_e\left(e'_{\text{th}} - e_{\text{th}}\right)\right. \\
&\qquad \cdot E\left(\log\left(1+\gamma_2\right) - \mu \times \left(\frac{e_i+1}{e_i}\right)^{\beta} \mid e_{\text{th}} \leq e_j \leq e'_{\text{th}}\right) \\
&\qquad \left. - \mu \times \left(\frac{e_i+1}{e_i}\right)^{\beta}\right].
\end{aligned} \tag{25}$$

If node i chooses to wait, it has $E(\prod(W, a_j(e_j)) \mid e_i) = 0$. Therefore, node i will choose to send if and only if $E(\prod(T, a_j(e_j)) \mid e_i) \geq E(\prod(W, a_j(e_j)) \mid e_i)$. The bigger the e_i is, the greater the expected utility of node i will be.

(2) $n > 2$. With the aforementioned discussion based on two vehicles, we could readily extend the analysis to more nodes. First, we define a random variable expressing the channel gain for each link between the given vehicles and bus. The random variable is independent identically distributed and is expressed as

$$D_k = \sum_{i=1}^{k}\left(\frac{e_i}{e_i+1}\right)^{\beta}. \tag{26}$$

Then, denoting the cumulative distribution function of D_k as $F_{g,k}(x)$, and the conditional cumulative distribution function as $F_{g,k}(x \mid \text{G})$, we have

$$\begin{aligned}
&E\left(\prod_i (T, \mathbf{a}_{-\mathbf{i}}(e_{-\mathbf{i}})) \mid e_i\right) \\
&= \sum_{k=0}^{n-1}\binom{n-1}{k}\overline{F}_e(e_{\text{th}})^k F_e(e_{\text{th}})^{n-1-k} \\
&\quad \cdot \left[F_{g,k}\left(E'_{\text{th}} \mid \Gamma_k\right) \cdot E\left(\log\left(1+\gamma_i\right) \mid A_k, E_k \leq E'_{\text{th}}\right)\right. \\
&\qquad \left. - u \times \left(\frac{e_i}{e_i+1}\right)^{\beta}\right],
\end{aligned} \tag{27}$$

where

$$\begin{aligned}
\gamma_i &= \frac{(e_i/(e_i+1))^{\beta}}{\alpha D_k + \sigma^2}, \\
\left(1 + D'_{\text{th}}\right)^{-\beta} &= \frac{1}{\alpha}\left(\frac{(e_i/(e_i+1))^{\beta}}{\text{SINR}_{\text{th}}} - \sigma^2\right), \\
\Gamma_k &= \left\{e_{j_1} \geq e_{\text{th}}, e_{j_2} \geq e_{\text{th}}, \ldots, e_{j_k} \geq e_{\text{th}},\right. \\
&\qquad \left. e_{j_{k+1}} < e_{\text{th}}, e_{j_{k+2}} < e_{\text{th}}, \ldots, e_{j_{N-1}} < e_{\text{th}}\right\}.
\end{aligned} \tag{28}$$

If node i chooses to wait, it has $E(\prod(W, a_j(e_j)) \mid e_i) = 0$. So, node i chooses to send if and only if

$$E\left(\prod\left(T, a_j\left(e_j\right)\right) \mid e_i\right) \geq E\left(\prod\left(W, a_j\left(e_j\right)\right) \mid e_i\right). \tag{29}$$

Finally, we could calculate the Bayesian Nash equilibrium regarding the distance as the transmission threshold between vehicles, that is,

$$E\left(\prod_i \left(T, \mathbf{a}_{-\mathbf{i}}\left(e_{-\mathbf{i}}\right)\right) \mid e_{\text{th}}\right) = 0. \quad (30)$$

4. Model Implementation and Performance Evaluation

In this section, we will first give the PCM implementation details on NS2 and then evaluate its performance with different parameters settings.

4.1. PCM Implementation on NS2. For typical IEEE802.11x CSMA scheme, the packets will be collided and dropped when they arrive at the physical interface of the receiver at the same time. The reason is that there are lots of hidden nodes which cannot sense the sender's ongoing transmission and at last result in collisions. Although there are some venders implementing the "capture effect" on hardware, this mechanism actually works with very strict limitation. For instance, on NS2 platform, the "capture effect" will only be triggered when the strength difference between received signals from various senders is larger than 10 times. Even though the "capture effect" could work well, it only permits the successful reception of the most powerful packets which has captured the channel. In other words, concurrent reception is still not permitted. Besides, in IEEE802.11x protocols, the "duration" field in MAC header, as shown in Figure 2, sets a NAV (network allocation vector) value to restrain the transmitting attempts from neighboring nodes of transmitters, which will further reduce the channel utilization ratio especially when concurrent transmissions are possible. Our proposed PCM scheme tries to explore the simultaneous transmission opportunities between nodes and made the following revisions to the original CSMA mechanism.

(a) First, we set the higher priority for concurrent transmission when it is available than for NAV indication. In other words, if concurrent transmission is available currently, the NAV field will be useless.

(b) Second, we revised the collision processing module in IEEE802.11x CSMA protocol to allow the interferences computing for all incoming packets whereby the successfully decoded packets can be queued in the physical interface buffer. In this way, because the delimiter in the preamble could certainly distinguish the incoming packets, a dropped packet will only occur when physical decoding fails.

We also revised the standard IEEE 802.11 module in NS2 and coded our PCM model on it. The reason is that NS2 focuses on protocol simulation and optimization which is not expert in iteration computation. Therefore, we implemented the game-theory-based NE searching with MATLAB toolkits on Linux platform. In this way, by releasing our MATLAB codes in Linux executable binary format, NS2 could readily invoke the complex computation part and concentrate on protocol performance evaluation. The numerical analyses of our proposed proximity-based concurrent transmission strategy involve two parts: one for algorithm correctness verification and the other for network performance inspection in VANETs simulation environment with real settings.

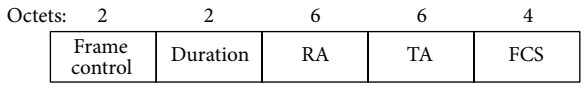


Figure 2: IEEE802.11x MAC common header.

Table 1: Algorithm simulation parameters settings.

Parameters	Values	Parameters	Values
Channel model	Rayleigh	Distribution of received signal power	Exp (1)
α	0.05	SINR_{th}	10 dB
σ	0.1	μ	2.5

Table 2: Relationship between proximity e and the number of active nodes.

Numbers	e	d
1	0	No sense
2	0.009381	106.6
3	0.010027	99.7
4	0.010443	95.7
5	0.010817	92.4
6	0.01119	89.4
7	0.011407	87.6
8	0.011604	86.1
9	0.011804	84.7
10	0.011953	83.6
11	0.012095	82.6
12	0.01219	82
13	0.012387	80.7
14	0.012509	79.9
15	0.012501	80
16	0.012682	78.8
17	0.012815	78
18	0.012871	77.7
19	0.012932	77.3
20	0.013089	76.4
21	0.013125	76.2

4.2. Algorithm Correctness Verification. The simulation parameters for algorithm correctness evaluation are listed in Table 1. The relationship between calculated proximity e and number of active nodes is depicted in Table 2, and the corresponding curve is plotted in Figure 3.

The proximity, which indicates the affinity between normal vehicles and buses, increases dramatically with the growing of the number of active vehicles as shown in Figure 3.

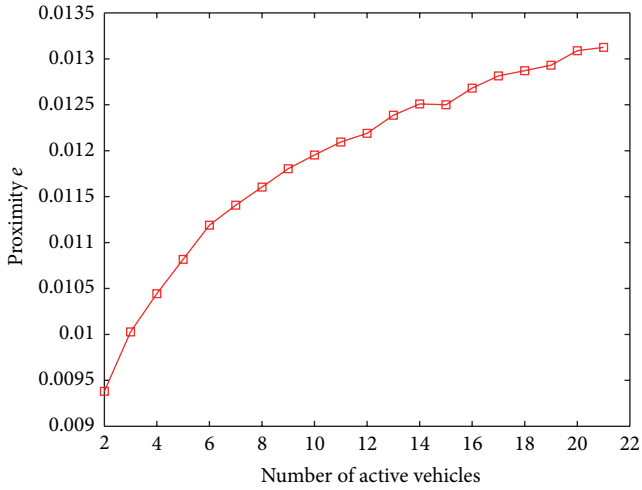


Figure 3: The corresponding curve for Table 2.

From the approximately linear relationship, we could conclude that our proposed scheme is also fair among vehicles where more active vehicles need more "loves" from buses. On the other hand, larger proximity corresponds to lower distance between normal vehicles and buses, for instance, 106.6 meters for 2 active vehicles and 76.2 meters for 21 active vehicles. It means that for a given transmitting power for all vehicles, a larger number of active vehicles require short distances from buses which may make successful concurrent receptions at buses possible due to bigger SINR and less frequent channel gain changing. The word "possible" here denotes the possibility of reception failure due to channel gain changing during the process of concurrent transmission.

In Figure 4, the performance evaluations by the other possible influences are simulated involving mutual interference ratio, $SINR_{th}$, variance of AWGN, and coefficient of transmitting cost. The proximity increases as the mutual interference ratio and the number of active vehicles grow as shown in Figure 4(a). The reason is that larger mutual interference ratio introduces more interference among vehicles resulting in more needs for proximity from buses to anti-interferences. Figure 4(b) shows that the growing of $SINR_{th}$ also makes the proximity increase due to lower interferences bearing capability. Figure 4(c) indicates that the rise of variance of noise also causes the increase of final proximity with the number of active vehicles augmenting. The reason is almost the same with the impact of $SINR_{th}$ on proximity performance. The effect of the coefficient of transmitting cost on proximity is plotted in Figure 4(d), where the resulted proximity is increasing with the growing of the coefficient, which expresses the price brought by transmitting attempts. It could be observed that the more the vehicles need to pay for the transmitting, the less the proximity will be.

4.3. Network Performance Inspection. In this section, we will evaluate the performance of our proposed scheme on NS2. The used parameters of our PCM model are the same as listed in Table 1. The general parameters for our network performance evaluation are listed in Table 3. The Queue model used in our simulation is just DropTail strategy due to the simplified setting for routing scheme, that is, DumbAgent, which implies that no routing is actually required. The simulation topology, which is a snapshot of the NS2 NAM (Network Animator), is plotted in Figure 5 in a 1000 m∗1000 m circular field where 50 vehicles are uniformly distributed in 4 lanes and move following the freeway [34] mobility model. The other parameters of freeway model are listed in Table 4. The acceleration speed is set as Acceleration_speed = 10% ∗ Maximum velocity according to [34]. There are 8 buses circled by red color taken as the mobile access points/gateways, which are placed to approximately cover all the vehicles within their radio ranges. Other vehicles choose to access the nearest mobile bus to finish messages exchanging. The following simulation scenarios will increase the number of vehicles according to the uniform distribution on the simulation area, but the number of buses will never change.

Table 3: Scenario settings.

Parameters	values
Lane number	4
Lane distance (m)	5
Max. velocity (m/s)	30
Direction	2
Min. velocity (m/s)	20
Rate (packets/s)	10

Figure 6 has shown the performance comparisons between IEEE802.11x CSMA scheme and PCM. Note that although the simulation period is set to 300 seconds, the tests will be actually ended before it due to queues overflow, too many packets drops, or out-of-radio range. By Figures 6(a) and 6(c), we could notice that the average transmission delay has clear relation with the number of active nodes and data rate. However, for average speed, which follows a uniform (min. velocity, max. velocity) distribution, it shows uncertain relevance with average transmission delay as shown in Figure 6(e). The reason is that a higher average driving speed make the topology more dynamic thereby lots of sent packets could not be received due to mobility, which will trigger the retransmission procedure to retry to the limit. Therefore, the average transmission delay will become larger and jittering.

As shown in Figure 6(a), where 1 Mbps data rate is configured, our PCM mechanism always has better average transmission delay performance than IEEE802.11x CSMA. The number of active nodes is the total number of vehicles attempting to transmit to buses within our measurement period, that is, 0.1 s in our simulation. However, the concurrent transmission proximity for each bus is computed based on the number of active nodes around it. The average transmission delay is an arithmetical average of delays for all received packets at all buses. It can be noticed that when the number of active nodes is less than 80, PCM shows better performance than CSMA because there are lots of concurrent transmission opportunities for vehicles around each bus.

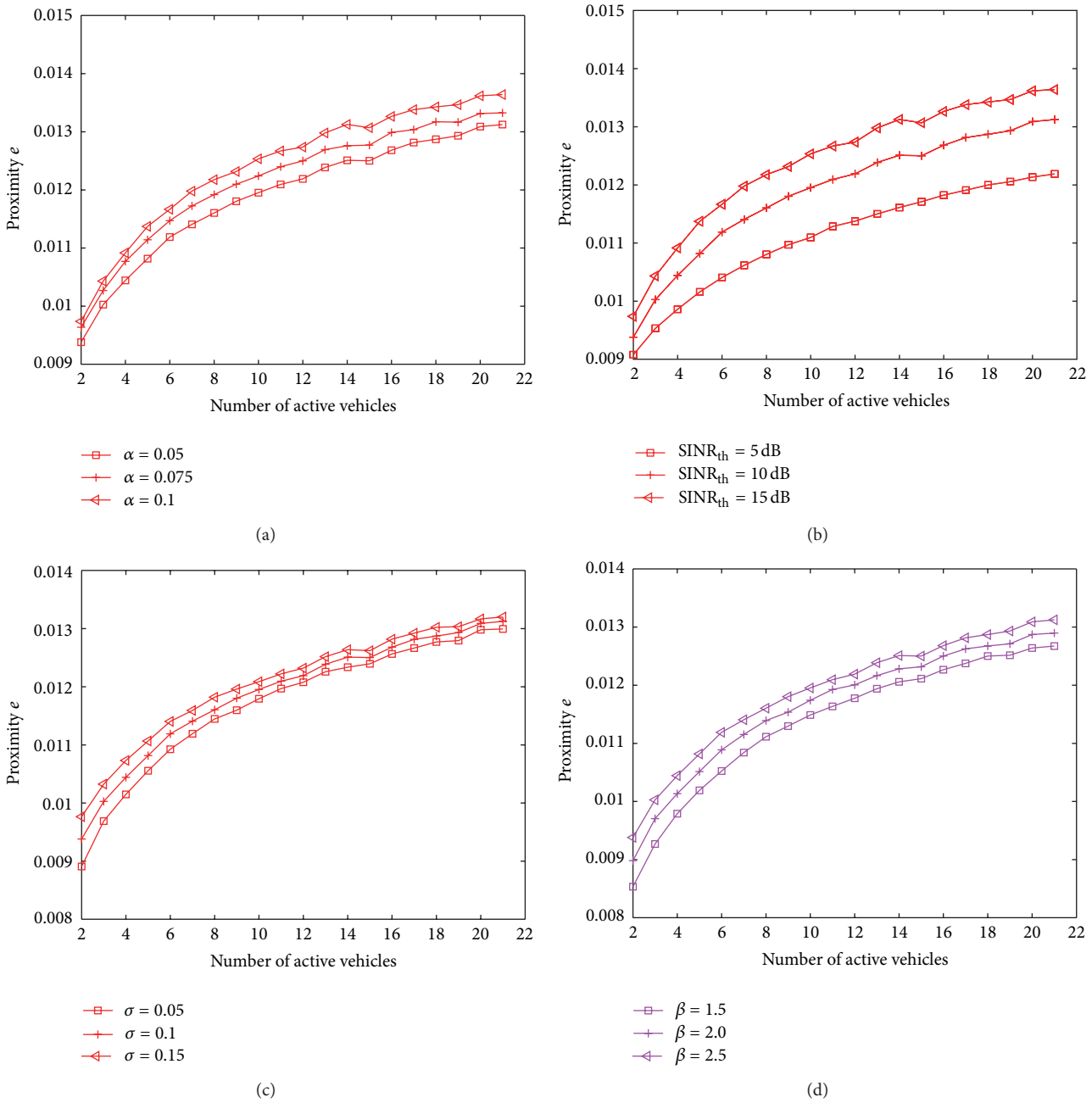


FIGURE 4: Numerical results of our PCM scheme. (a) The effect of mutual interference ratio on proximity. (b) The effect of $SINR_{th}$ on proximity. (c) The effect of variance of AWGN on proximity. (d) The effect of the coefficient of transmitting cost on proximity.

In fact, for a given calculated concurrent transmission proximity e, any node or vehicle with proximity larger than e could attempt to transmit. In Figure 6(c), we increase the data rate, which indicate the provided bandwidth by physical layer, to investigate the output performance. The number of active nodes for Figure 6(c) is 100 involving the buses. Note that the average transmission delay decreases dramatically for CSMA when data rate increases, whereas our PCM scheme, although still has lower average delay than CSMA before 5 Mbps, shows a relatively slow falling compared with CSMA and finally has a higher average transmission delay than CSMA at 6 Mbps. The reason is that, for a large data rate, CSMA could greatly reduce the collision possibility due to smaller air flying time for packets. However, for our PCM mechanism, although increase of data rate could further reduce the needed period for either concurrent/nonconcurrent transmissions, the concurrent transmission opportunities are still the same with cases under lower data rate. Figure 6(e) denotes that there is no apparent relationship between average vehicles' speed and average transmission delay where the number of deployed vehicles is still 100 with 1 Mbps data rate.

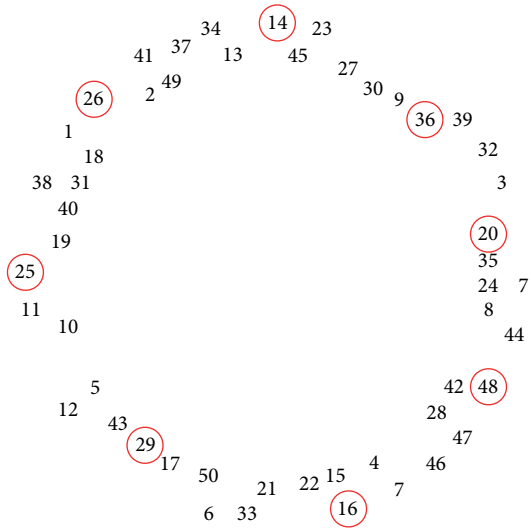


Figure 5: Simulation topology.

Table 4: Network simulation parameters settings.

Parameters	values
Propagation model	Two-ray ground
Queue length/packets	50
Routing	DumbAgent
Default number of vehicles	100
Packet size/b	250
Simulation field/m $*$ m	1000×1000
$SINR_{th}$/dBm	-90
Max. radio range/m	300
Queue model	DropTail
Mac	802.11 extent
Default data rate/Mbps	1
Packets generation period/s	20
Simulation period/s	300
Path loss factor	2.2
P_t/mW	0.3754
Frequency/Hz	$5.9e + 9$

Figures 6(b), 6(d), and 6(f) show the delivery ratio performance under different number of active nodes, data rate, and average speed. The parameters are the same with the simulations for Figures 6(a), 6(c), and 6(e). As shown in Figure 6(b), with the increase of the number of active nodes, the delivery ratio of CSMA mechanism greatly decreases. The reason is that there are lots of collisions and failed retransmissions resulting in a lower delivery ratio. In our simulation, when the number of active nodes is 200, there are 20051 sent packets but just 6765 have been successfully received with CSMA protocol. However, for our PCM scheme, the number of received packets rises to 15640. As for the influence of data rate on the final delivery ratio, the effect from larger data rate is clearer on CSMA than on our PCM. The conclusion is consistent with Figure 6(c) that the concurrent transmission opportunities are not changing with various data rates. The relation between delivery ratio and average speed is also obscure as shown in Figure 6(f). However, we can conclude from Figure 6(f) that our PCM is not suitable for high dynamic vehicular networks.

Figures 6(g), 6(h), and 6(i) show the throughput performance comparisons between our PCM and CSMA. Here, (xN), (xS), and (xR) in these figures indicate the number of active nodes, the average speed, and the data rate, respectively. The other unspecific parameters are the same as shown in Tables 3 and 4. In Figure 6(g), we can conclude that our PCM always has better throughput performance than CSMA in lower dynamic network when the number of vehicles changes. However, when the average speed is continuously increasing, PCM begins to show poorer performance than CSMA especially when average speed is beyond 25 m/s as shown in Figure 6(h). As for throughput performance under different data rate, the results from Figure 6(i) are consistent with Figure 6(d), where more data rate has little effect on final throughput for our PCM scheme due to no more concurrent transmission opportunities increasing. However, for CSMA mechanism, growing of data rate has greatly improved the final throughput regarding less collisions and retransmissions.

To verify PCM in real application scenario, we also implemented it on our vehicular communication testbed composed of 8 cars as shown in Figure 7. The red circled car here is taken as the BUS node, and the other cars try to access the bus. The small car is equipped with a wireless radio device which consists of an ATMEL Atmega128L MCU (microprogrammed control unit), a Chipcon 2420 SmartRF, a Maxim IC MAX3232 transceiver, and some other chips for storage and debug. The PCM protocol is coded on the embedded Linux platform on this device. Our cars can move autonomously with predefined routes or be controlled through infrared. The size of the car is 20 cm (length) $\times$ 7.5 cm (width) and the area of the test field is 100 m (length) $\times$ 3.5 m (width). The speeds of the 8 cars are uniformly chosen from [100 cm, 3 m] per second and the radio range of the transceiver is 8 meters. We run an 80 seconds test and repeat it 20 times to output the arithmetic average. The other settings like SINR threshold, packet size, data rate, packets generation period, and so forth are the same as in Table 4. Here, we just show the throughput performance compared with the typical IEEE 802.11a protocol. Due to the different PHY and MAC layer mechanisms, we use a USB WLAN adapter for testing which can be connected to the peripheral board of the wireless communication device.

The throughput results are plotted in Figure 8. Note that the throughput performance in real environment is more fluctuant than in simulation. The reason is that the wireless signal is much susceptible to interferences and influences in practice such as unstable transmitting power, other wireless devices' disturbance, nonideal propagation channel, and statistical errors. But for all this, the trend in Figure 8 is still clear and shows that our proposed PCM always outperforms IEEE 802.11a on throughput. The reason is simple and the same as previous simulation results; say there are lots of concurrent transmission opportunities for vehicles running with our PCM. However, with typical WLAN protocol, the throughput

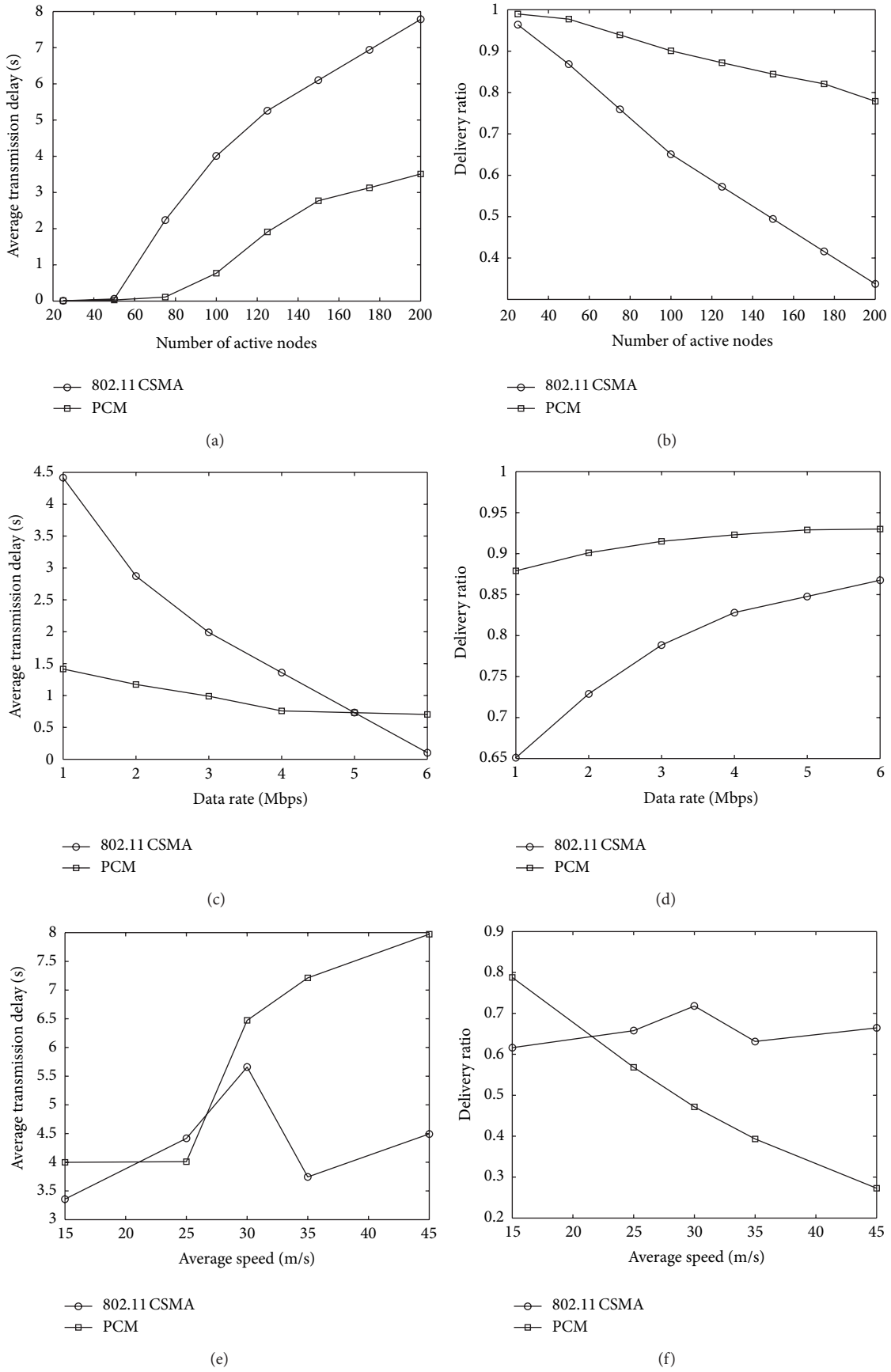


Figure 6: Continued.

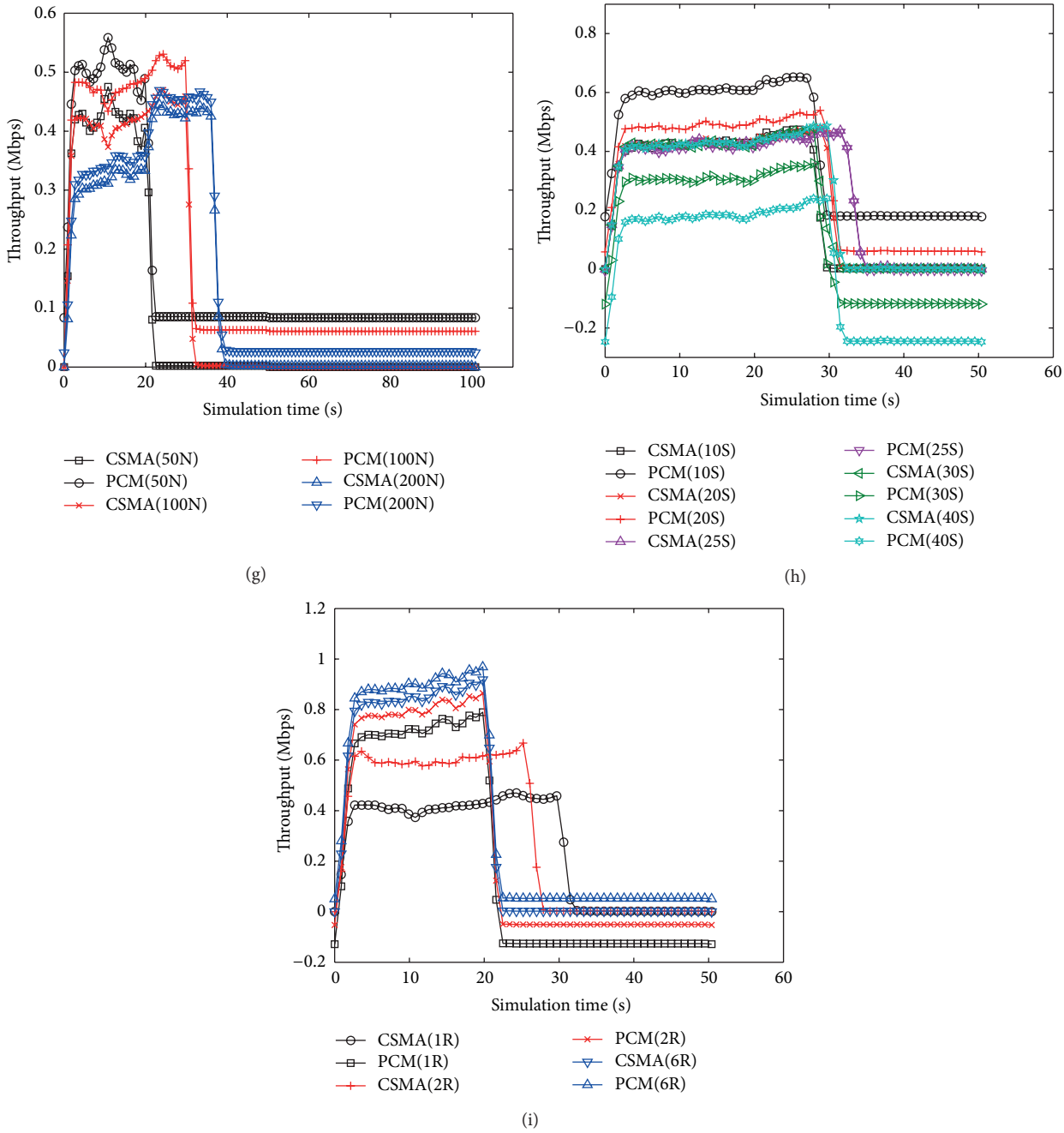


Figure 6: PCM performance evaluation results. (a) Average transmission delay versus number of active nodes. (b) Delivery ratio versus number of active nodes. (c) Average transmission delay versus data rate. (d) Delivery ratio versus data rate. (e) Average transmission delay versus average speed. (f) Delivery ratio versus average speed. (g) Throughput performance under different number of active nodes. (h) Throughput performance under different average speed. (i) Throughput performance under different data rate.

will degrade due to CSMA/CA-based collision release mechanism.

5. Conclusion

In this paper, we have proposed a proximity-based incomplete information game to solve the concurrent transmission problem between vehicles and mobile RSUs. By detailed analysis and simulations, the correctness and effectiveness have been proofed for our proposed PCM scheme. Besides, we also give the implementation procedure of our PCM on NS2 simulation platform to verify its practicality. Although PCM could better work under lower dynamic networks, it shows poor performance when topology changes frequently. Our future work will focus on reducing the computation and time complexity of PCM and increasing its scalability and adaptability in high mobility networks.

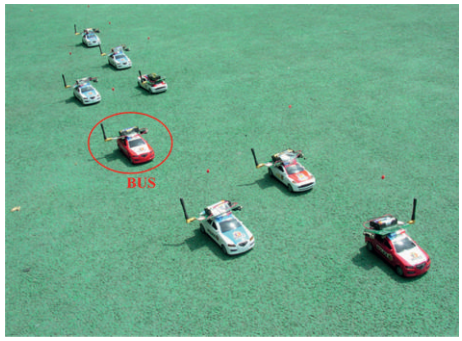


Figure 7: Testbed with programmable autonomous cars.

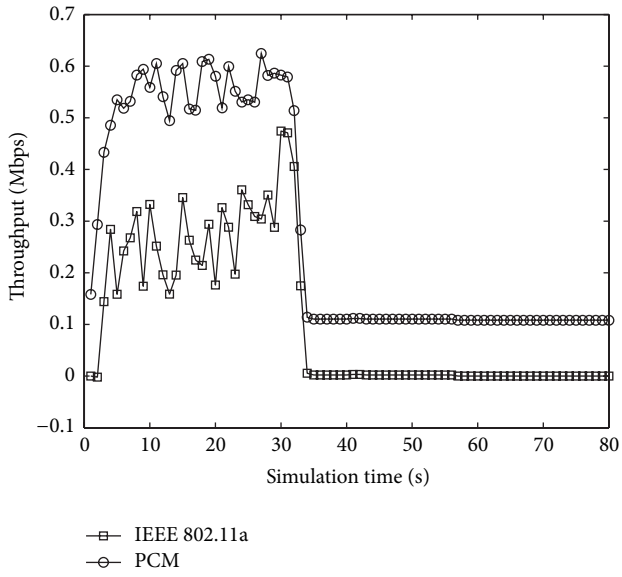


Figure 8: Throughput performance on real testbed.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (61201133, 61172055, and 61072067), Xian Municipal Technology Transfer Promotion Project (CX12178(6)), the Fundamental Research Funds for the Central Universities (K5051301011), the Postdoctoral Science Foundation of China (20100481323), the Program for New Century Excellent Talents (NCET-11-0691), the "111 Project" of China (B08038), and the Foundation of Guangxi Key Lab of Wireless Wideband Communication & Signal Processing (11105).

References

[1] L. Bononi and M. Di Felice, "A cross layered MAC and clustering scheme for efficient broadcast in VANETs," in *Proceedings of the IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems (MASS '07)*, pp. 1–8, October 2007.

[2] M. Bakhouya, J. Gaber, and P. Lorenz, "An adaptive approach for information dissemination in Vehicular Ad hoc Networks," *Journal of Network and Computer Applications*, vol. 34, no. 6, pp. 1971–1978, 2011.

[3] A. Daeinabi, A. G. Pour Rahbar, and A. Khademzadeh, "VWCA: an efficient clustering algorithm in vehicular ad hoc networks," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 207–222, 2011.

[4] S. Eichler, "Performance evaluation of the IEEE 802.11p WAVE communication standard," in *Proceedings of the IEEE 66th Vehicular Technology Conference (VTC '07)*, pp. 2199–2203, Baltimore, Md, USA, October 2007.

[5] T. ElBatt, S. K. Goel, G. Holland, H. Krishnan, and J. Parikh, "Cooperative collision warning using dedicated short range wireless communications," in *Proceedings of the 3rd ACM International Workshop on Vehicular Ad Hoc Networks (VANET '06)*, pp. 1–9, September 2006.

[6] A. Carter, "The status of vehicle-to-vehicle communication as a means of improving crash prevention performance," Tech. Rep., NHTSA, 2005.

[7] E. Schoch, F. Kargl, M. Weber, and T. Leinmüller, "Communication patterns in VANETs," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 119–125, 2008.

[8] H. Hartenstein and K. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Communications Magazine*, vol. 46, no. 6, pp. 164–171, 2008.

[9] V. Srivastava, J. Neel, and A. B. MacKenzie, "Using game theory to analyze wireless ad hoc networks," *IEEE Communications Surveys and Tutorials*, vol. 7, no. 4, pp. 46–56, 2005.

[10] A. T. Campbell, M. Conti, and S. Giordano, "Editorial: mobile ad hoc networks," *Mobile Networks and Applications*, vol. 8, no. 5, pp. 483–484, 2003.

[11] M. Mejia, N. Peña, J. L. Muñoz, O. Esparza, and M. A. Alzate, "A game theoretic trust model for on-line distributed evolution of cooperation inMANETs," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 39–51, 2011.

[12] X. Liu, X. Fang, X. Chen, and X. Peng, "A bidding model and cooperative game-based vertical handoff decision algorithm," *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1263–1271, 2011.

[13] K. Akkarajitsakul, E. Hossain, and D. Niyato, "Distributed resource allocation in wireless networks under uncertainty and application of Bayesian game," *IEEE Communications Magazine*, vol. 49, no. 8, pp. 120–127, 2011.

[14] X. Liao, D. Hao, and K. Sakurai, "Classification on attacks in wireless ad hoc networks: a game theoretic view," in *Proceedings of the 7th International Conference on Networked Computing and Advanced Information Management (NCM '11)*, pp. 144–149, June 2011.

[15] S. Sergi, F. Pancaldi, and G. M. Vitetta, "A game theoretical approach to the management of transmission selection scheme in wireless Ad-Hoc networks," *IEEE Transactions on Communications*, vol. 58, no. 10, pp. 2799–2804, 2010.

[16] F. Wang and O. Younis, "GMAC: a game-theoretic MAC protocol for mobile ad hoc networks," in *Proceedings of the 4th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, pp. 1–9, 2006.

[17] H. Lee, H. Kwon, A. Motskin, and L. Guibas, "Interference-aware MAC protocol for wireless networks by a game-theoretic approach," in *Proceedings of the 28th Conference on Computer Communications (IEEE INFOCOM '09)*, pp. 1854–1862, April 2009.

[18] D. Krishnaswamy and M. Van Der Schaar, "Adaptive modulated scalable video transmission over wireless networks with a game theoretic approach," in *Proceedings of the IEEE 6th Workshop on Multimedia Signal Processing*, pp. 107–110, October 2004.

[19] C. U. Saraydar, N. B. Mandayam, and D. J. Goodman, "Efficient power control via pricing in wireless data networks," *IEEE Transactions on Communications*, vol. 50, no. 2, pp. 291–303, 2002.

[20] F. Wang, O. Younis, and M. Krunz, "Throughput-oriented MAC for mobile ad hoc networks: a game-theoretic approach," *Ad Hoc Networks*, vol. 7, no. 1, pp. 98–117, 2009.

[21] S. Adlakha, R. Johari, and A. J. Goldsmith, "Competition in wireless systems via Bayesian interference games," *CoRR, Informal Publication*, 2007.

[22] S. Agarwal, R. H. Katz, S. V. Krishnamurthy, and S. K. Dao, "Distributed power control in ad-hoc wireless networks," in *Proceedings of the 12th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC '01)*, vol. 2, pp. F59–F66, October 2001.

[23] V. Kawadia and P. R. Kumar, "Power control and clustering in ad hoc networks," in *Proceedings of the 22nd Annual Joint Conference on the IEEE Computer and Communications Societies (INFOCOM '03)*, pp. 459–469, April 2003.

[24] A. Muqattash and M. Krunz, "POWMAC: a single-channel power-control protocol for throughput enhancement in wireless ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 5, pp. 1067–1084, 2005.

[25] A. Muqattash and M. Krunz, "Power controlled dual channel (PCDC) medium access protocol for wireless ad hoc networks," in *Proceedings of the 22nd Annual Joint Conference on the IEEE Computer and Communications Societies*, pp. 470–480, April 2003.

[26] J. P. Monks, V. Bharghavan, and W. W. Hwu, "A power controlled multiple access protocol for wireless packet networks," in *Proceedings of the 20th Annual Joint Conference on the IEEE Computer and Communications Societies (IEEE INFOCOM '01)*, pp. 219–228, April 2001.

[27] Y. Sun, E. M. Belding-Royer, and C. E. Perkins, "Internet connectivity for ad hoc mobile networks," *International Journal of Wireless Information Networks*, vol. 9, no. 2, pp. 75–88, 2002.

[28] S. Nittel, M. Duckham, and L. Kulik, "Information dissemination in mobile ad-hoc geosensor networks," in *Geographic Information Science*, pp. 206–222, Springer, Berlin, Germany, 2004.

[29] T. Vercauteren, A. L. Toledo, and X. Wang, "Batch and sequential bayesian estimators of the number of active terminals in an IEEE 802.11 network," *IEEE Transactions on Signal Processing*, vol. 55, no. 2, pp. 437–450, 2007.

[30] W. Xiuchao and A. L. Ananda, "Link characteristics estimation for IEEE 802.11 DCF based WLAN," in *Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN '04)*, pp. 302–309, November 2004.

[31] S. Venkatraman and J. Caffery Jr., "Hybrid TOA/AOA techniques for mobile location in non-line-of-sight environments," *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '04)*, vol. 1, pp. 274–278, 2004.

[32] P. Gupta and P. R. Kumar, "The capacity of wireless networks," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 388–404, 2000.

[33] M. Grossglauser and D. N. C. Tse, "Mobility increases the capacity of ad hoc wireless networks," *IEEE/ACM Transactions on Networking*, vol. 10, no. 4, pp. 477–486, 2002.

[34] F. Bai, N. Sadagopan, and A. Helmy, "IMPORTANT: a framework to systematically analyze the Impact of Mobility on Performance of RouTing protocols for Adhoc NeTworks," in *Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications (INFOCOM '03)*, vol. 2, pp. 825–835, 2003.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 143024, 7 pages
http://dx.doi.org/10.1155/2013/143024

Research Article

The RSU Access Problem Based on Evolutionary Game Theory for VANET

Di Wu,[1] Yan Ling,[1] Hongsong Zhu,[2] and Jie Liang[3]

[1] *School of Computer Science and Engineering, Dalian University of Technology, Dalian 116023, China*
[2] *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China*
[3] *School of Engineering Science, Simon Fraser University, Burnaby, BC, Canada V5A1S6*

Correspondence should be addressed to Yan Ling; lingyan321.love@163.com

Received 11 April 2013; Accepted 19 June 2013

Academic Editor: Limin Sun

We identify some challenges in RSU access problem. There are two main problems in V2R communication. (1) It is difficult to maintain the end-to-end connection between vehicles and RSU due to the high mobility of vehicles. (2) The limited RSU bandwidth resources lead to the vehicles' disorderly competition behavior, which will give rise to multiple RSUs having overlap area environment where RSU access becomes crucial for increasing vehicles' throughput. Focusing on the problems mentioned above, the RSU access question in the paper is formulated as a dynamic evolutionary game for studying the competition of vehicles in the single community and among multiple communities to share the limited bandwidth in the available RSUs, and the evolutionary equilibrium evolutionary stable strategy (ESS) is considered to be the solution to this game. Simulation results based on a realistic vehicular traffic model demonstrate the evolution process of the game and how the ESS can affect the network performance.

1. Introduction

Vehicle ad hoc network (VANET) is a special case of mobile ad hoc network. The motions of vehicles are restricted to a geographical pattern. Further, the communication patterns of VANET include vehicle to vehicle (V2V) and vehicle to road side unit (V2R). RSU is referred to as road side unit, which is a wireless transceivers and receivers and has the characters of data storage, computing power, and router. In recent years, V2R communication has received considerable attentions [1–4]. In this paper, we mainly research the RSU access problem.

When vehicles drive through RSU, it will ask the RSU for service requirements. However in VANET, (1) it is difficult to maintain the end-to-end connection between vehicles and RSU due to the high mobility of vehicles; (2) the limited RSU bandwidth resources lead to the vehicles' disorderly competition behavior, which may reduce the network throughput; (3) due to the uneven distribution of vehicles, RSU's load may become diversification, which will lead to the load imbalance of RSU. In order to solve the problems above and achieve good network throughput, one question needs to be addressed: in the highly dynamic network, when and which RSU should be accessed. Focusing on the problem, the paper puts forward evolutionary game theory.

Game theory provides a mathematical modeling for the study of competition strategies in a game where players have conflicting benefits or goals and consider the rivals' strategy to make their own strategy [5, 6]. Evolutionary game theory describes game models in which players choose their strategies through a trial-and-error process in which they learn over time that some strategies work better than others [7, 8]. In this paper, we analyze the RSU access problem under the framework of game theory as the vehicles are noncooperative and competitive and need to consider the strategy of other vehicles to make their own strategy. In addition, vehicles are controlled by bounded rational entities, such as human or organization [9], and the traditional game theory assumed that the players are perfectly rational, so we adopt the evolutionary game theory to analyze the access problem.

The research scene includes multiple vehicles versus two RSUs and multiple vehicles versus multiple RSUs. We divide the vehicles into different populations according to the strategies. The two RSU's scene belongs to a single-community evolutionary game as all vehicles' strategy set is the same, while the multiple RSU's scene belongs to multiple communities evolutionary game as vehicles in different populations have different strategies. The payoff function of our model is the difference of the throughput and the cost. In our paper, the cost contains two aspects: bandwidth occupation cost and handoff cost. The Nash equilibrium is evolutionarily stable strategy (ESS), that is, the probability of vehicles access to RSU. In order to ensure the accuracy and reliability of research results, the paper adopted the traffic flow simulator VanetMobiSim to generate the real vehicle moving track. The simulation results demonstrate the evolution process of the game and how the ESS can affect the network performance.

The main contributions of this paper can be summarized as follows.

(1) An evolutionary game-theoretic approach is presented to solve the RSU access problem in VANET. In particular, the replicator dynamics is quoted to investigate the dynamics of vehicle behavior and solution.

(2) Under two RSU's scene and multiple RSU's scene, the paper sets up single-community and multiple-community evolutionary game models to analyze the dynamic evolutionary process and the effect on network performance.

The rest of this paper is organized as the following. Section 2 reviewed problem description. In Section 3, we introduced the related work. Section 4 formalized the system model, which includes single-community and multiple-community evolutionary game models. The numerical experiments were performed in Section 5. Finally, we draw our conclusions in Section 6.

In the paper, we also use the terms "population" and "species" to refer to the VANET community.

2. Problem Definition

In VANET, vehicles have no Internet access and arrive randomly in VANET; vehicles have to access to RSU if they want to obtain the Internet services.

RSU broadcasts the beacon messages to vehicles periodically when the vehicle lies in the coverage area of an RSU, from which the vehicle can get the current state information of the RSU and the network. For simplicity, we assume that RSU's transmission range is equal, and we divide the road into different areas according to the RSUs' coverage area, which is defined as $S = \{S_1, S_2, \ldots, S_K\}$. As shown in Figure 1, the road is divided into four areas $S = \{S_1, S_2, S_3, S_4\}$. In different areas, vehicles can access different RSUs. Vehicle requests services from RSU when driving through RSU, and it can get the service profit from RSUs, while it also incurs a cost in requesting for RSU, where the cost can be the price that vehicles spend on RSUs' bandwidth, buffer size, and other resource. Besides, when vehicles drive from an RSU to another, the vehicles have to pay for the handoff cost. The payoff function of vehicles is

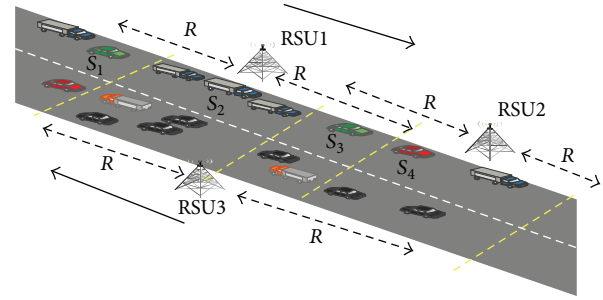


Figure 1: The RSU's access scene.

$$F = Q_i^j - P_i^j - h_i^j, \tag{1}$$

where Q_i^j is the achievable throughput of vehicle i got from RSU j

$$Q_i^j = \delta * \left(T_i^j - t^j\right) * c_i^j * N^j \tag{2}$$

T_i^j is the time when vehicle i is driving in the coverage area of RSU j

$$T_i^j = \frac{R^j}{v_i}. \tag{3}$$

t^j represents the communicate delay when vehicles communication with RSU j

$$t^j = \frac{N^j}{f_s}. \tag{4}$$

P_i^j stands for the resource cost

$$P_i^j = \beta * N^j * \alpha_i * \frac{l_i}{c_i^j}, \tag{5}$$

where l_i/c_i^j is the time that vehicle i should communicate with RSU j if it wants to finish its request. α_i is the importance index of vehicle i's request file. If $\alpha_i > 2$, the request file is urgent, such as emergency information, $1 < \alpha_i < 2$ means that the request is less important, such as road information, and the request is video and audio streams if $\alpha_i < 1$.

c_i^j is the transmission rate of vehicle i

$$c_i^j = w^j * \log_2\left(1 + \frac{S/N}{N^j * \overline{(d_i^j)^r}}\right). \tag{6}$$

h_i^j is the handoff cost

$$h_i^j = \varphi * t_{\text{left}} * T_{\text{left}}, \tag{7}$$

where t_{left} is the request files that have finished and T_{left} is the distance that vehicles have driven in RSU's coverage. Detailed parameters are listed in Table 1.

Table 1: The parameters.

Symbol	Semantics
N^j	The total number of vehicles in the coverage area of RSU j
R^j	The transmission radius of RSU j
v_i	The speed of vehicle i
l_i	The request file length of vehicle i
S/N	The signal-to-noise ratio
d_i^j	The distance between vehicle i and RSU j
w^j	The link bandwidth of RSU j
f_s^j	The communication frequency of RSU j
γ	The path loss exponent
Φ, β, δ	The weighting coefficient

3. Related Work

A number of previous results have been reported on the RSU access problems. In [10], a distributed association algorithm according to the number of mobile users (MUs) associated with APs was introduced. Besides, reference [11] built a game model according to the potential link rate and the number of WSs access to RSU, which can ensure that each WS gets achievable throughput. Reference [12] presented a new load balancing technique by controlling the size of WLANs (i.e., APs' coverage range) to ensure the load balancing among APs. As we know, vehicles in VANET are highly mobile and the network typology changes dynamically, which demonstrated that the approaches ignore VANET's mobile properties. Besides, these approaches only consider the profit of RSU but vehicles and the papers above all assumed that the players are perfectly rational, which did not fit the realities that human and organizations and other players are bounded rationality. In a word, these methods were not applicable for VANET.

In recent years, evolutionary game theory has been used in wireless network in many fields. Reference [13] that showed the evolutionary game is used to obtain the forward probability of nodes in two-hop DTN and analyze the stability of ESS. In [14], the authors presented two algorithms, namely, population evolution and reinforcement-learning algorithms, for network selection and formulated the game to model the competition among populations of users in the different service areas in heterogeneous wireless networks. Reference [15] presented a model based on evolutionary game theory (EGT) in which it demonstrated that the model was able to encourage selfish nodes to cooperate and forward packets from others with only one period of punishment if nodes are sufficiently patient. As we know, the traditional game theory has been used in VANET for some applications [16–18]; however, the evolutionary game theory's applications in VANET are growing due to the following reasons. (1) The evolutionary equilibrium of evolutionary game is a refined solution, which ensures stability (i.e., population of players will not change their chosen strategies over time). (2) An evolutionary game changes their strategies slowly to achieve the solution eventually, and the traditional game makes decisions immediately. (3) The replicator dynamics is useful for investigating the trajectory of the players' strategies [14]. In our paper, we solve the RSU access problem in VANET by using evolutionary game.

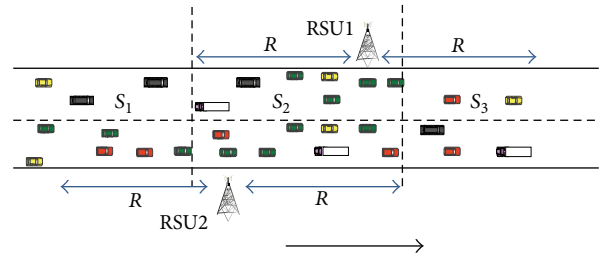


Figure 2: The two RSUs' scene.

4. Evolutionary Game Model

The evolutionary game for our paper can be described as follows.

(i) Players: the vehicle in the coverage area of RSU is a player of the game.

(ii) Population: the vehicles that have the same strategy set are a population. In different populations, the number of vehicles is defined separately as $N = \{N^1, N^2, \ldots, N^j, \ldots\}$.

(iii) Strategy: the strategy set is $X^j = \{x_0^j, x_1^j, \ldots, x_i^j, \ldots, x_N^j\}$, $i = 1, 2 \ldots, N$, where x_i^j means the access probability that player i chooses RSU j.

(iv) Payoff: the payoff function is $F = Q_i^j - P_i^j - h_i^j$, which is the difference of the throughput of that strategy and the cost. In multiple communities, the payoff of the vehicle depends on not only the strategy played by the number of vehicles from the same population but also other populations that participate to the game.

In this section, we present the evolutionary game model in two RSU's scene and multiple RSU's scene, respectively.

4.1. Two RSUs' Scene. As shown in Figure 2, in two RSU's scene, there is a set of vehicles who want to request services from RSU1 and RSU2. Vehicles can only access RSU2 when they enter S1 and may change its selection when they enter S2. We assume that the vehicle needs to pay for the handover cost if it does not finish its service request while it performs the handoff operation. On the contrary, If the vehicles' requested services have been finished, the handoff cost is zero and vehicles get their strategy based on their location, the file size, service type, and so on. The vehicles in RSU1 and RSU2's coverage area are a single-community evolutionary game, in which all vehicles' strategy set is the same. The payoff matrix is as described in Table 2.

In the game, we let $X := \{(x, x-) \mid x+x- = 1\}$ be the set of probabilities distributions of population i. x and y represent the probabilities of vehicles in population i accessing RSU1 and RSU2, respectively, $1 - x - y$ means vehicles do not

Table 2: Two RSUs' payoff matrix.

	RSU1	RSU2	None
RSU1	$\theta^1 - \varphi(P^1 + h^1)$	$\theta^1 - (P^1 + h^1)$	$\theta^1 - (P^1 + h^1)$
RSU2	$\theta^2 - (P^2 + h^2)$	$\theta^2 - \varphi(P^2 + h^2)$	$\theta^2 - (P^2 + h^2)$
None	0	0	0

access any RSUs' probability, and φ is the congestion index. The payoff function is as follows.

The profit of vehicles accessing RSU1 is

$$F(x,1) = x * \left(\theta^1 - \varphi * \left(P^1 + h^1\right)\right) + y\left(\theta^1 - \left(P^1 + h^1\right)\right) + (1 - x - y) * \left(\theta^1 - \left(P^1 + h^1\right)\right). \tag{8}$$

The profit of vehicles accessing RSU2 is

$$F(y,2) = x * \left(\theta^2 - \left(P^2 + h^2\right)\right) + y * \left(\theta^2 - \varphi * \left(P^2 + h^2\right)\right) + (1 - x - y) * \left(\theta^2 - \left(P^2 + h^2\right)\right). \tag{9}$$

The payoff of vehicles in population 1 and population 2 which do not choose any RSU is 0.

The average payoff of populations is

$$\overline{F} = x * F(x,1) + y * F(y,2) + (1 - x - y) * 0. \tag{10}$$

In a dynamic evolutionary game, an individual from a population, who is able to replicate itself through the process of mutation and selection, is called replicator. In this case, a replicator with a higher payoff can reproduce itself faster. The game is a repeated game, and in each period, a player observes the payoff of other players in the same community. Then, in the next period, the player adopts a strategy that gives a higher payoff. The speed of the vehicle in observing and adapting the RSU access is controlled by the parameter μ.

In the case of single community, the replicator dynamics is:

$$\frac{dx}{dt} = \mu\left[F(x,1) - \overline{F}\right] * x, \qquad \frac{dy}{dt} = \mu\left[F(y,2) - \overline{F}\right] * y. \tag{11}$$

4.2. Multiple RSUs' Scene. Figure 3 depicts the multiple RSUs' scene, in which vehicles in different populations have different strategies. So it is a multiple-community evolutionary game. As shown in Figure 3, area 1 is the overlap area of RSU1 and RSU2, and area 2 is the overlap area of RSU1, RSU2, and RSU3. The set of strategies for the players in area 1 is {RSU1, RSU2}, while that for the players in area 2 is {RSU1 RSU2, RSU3}. Area 1 and area 2 depict a two community evolutionary game. The vehicles in multiple-community evolutionary game will compete with each other within population and also carry on the competition among the populations. During the evolutionary process, the vehicles adjust their strategies according to their payoff until all the vehicle's strategies maintain stable, and the strategy is ESS at this time.

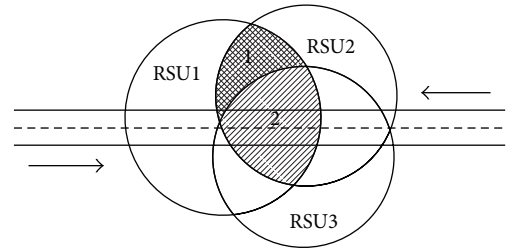


Figure 3: Multiple RSUs' scene.

The payoff function of vehicles in population i accessing RSU j is

$$F_i^j = \theta_i^j - P_i^j - h_i^j. \tag{12}$$

The payoff of vehicles in population i which do not access any RSU is 0.

The average payoff of all populations is

$$\overline{F^i} = \sum_{j=1}^{M} x_j^i * F_j^i. \tag{13}$$

The replicator dynamics of population i is

$$\frac{dx_j^i}{dt} = \mu\left[F_j^j - \overline{F^i}\right] * x_j^i. \tag{14}$$

5. Simulations and Evaluations

VANET is a special network, it has a highly dynamic typology, vehicles are highly mobile, and the motions of vehicles are restricted to a geographical pattern. In order to make the simulation results more realistic, we use VanetMobiSim and Google Earth map tools to simulate traffic track. As shown in Figure 4, the paper chooses Zhongshan district, Dalian, as the simulation area, and the area size is 2.0 km by 2.0 km. VanetMobiSim is a simulation tool which can generate vehicle trajectory. In our simulation, we need to use the VanetMobiSim to get the movement trajectory of vehicles.

We study the access problem through the following two aspects: the evolutionary process of the ESS and the effect of resource cost parameters on network performance. We set the simulation parameters as described in Table 3.

In Figures 4 and 5, the horizontal axis stands for the number of evolution, while the vertical axis stands for the ESS.

Figure 4 demonstrates the influence on ESS along with the vehicle speed, package size changing. In the simulation we set the number of vehicles as 150, the vehicles speed as 15 m/s for Figure 4(a), and the package size as 20 for Figure 4(b). With size increment, the probability that vehicles finish their service within RSU's coverage area decreases, leading to the

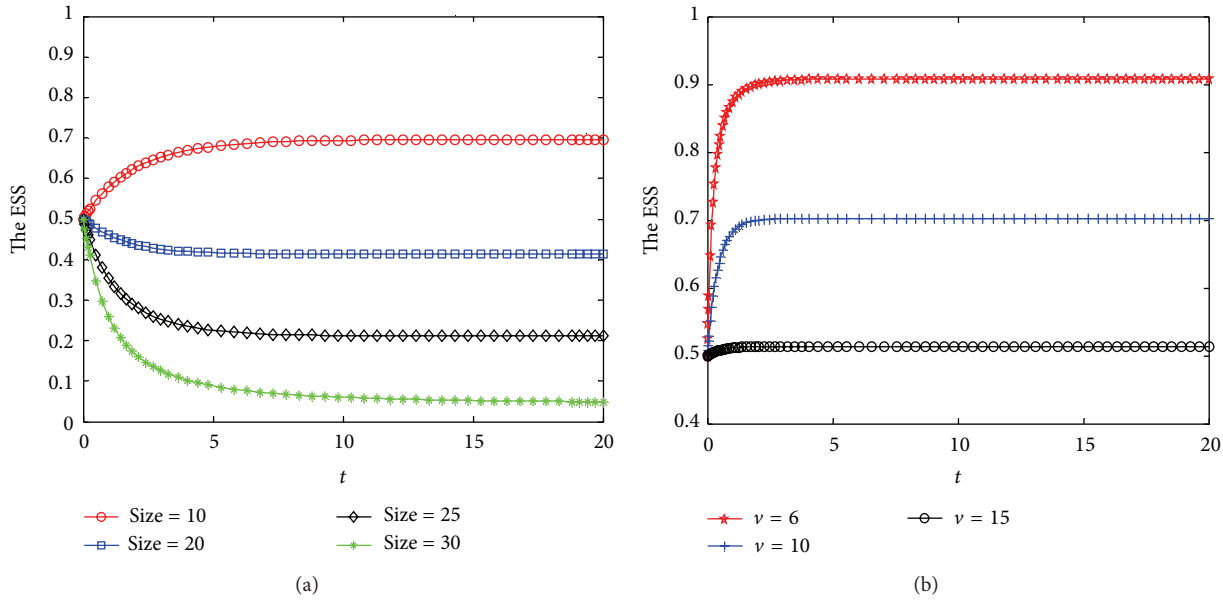


FIGURE 4: (a) The effect on ESS of packet size. (b) The effect on ESS of vehicle speed.

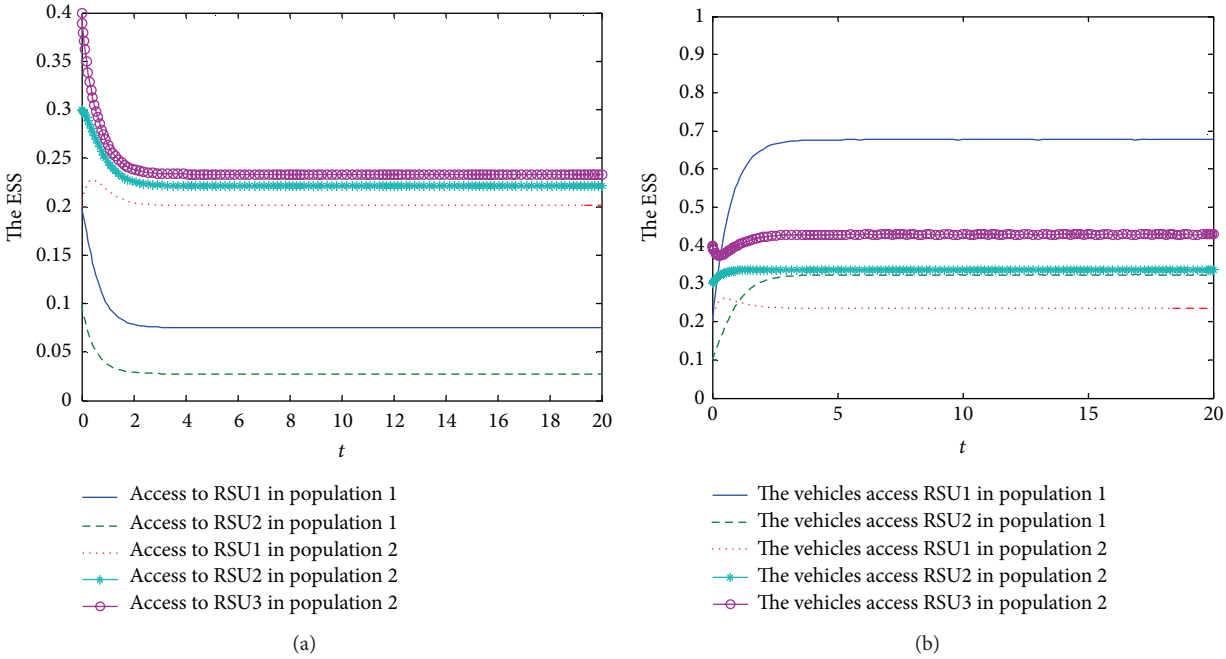


FIGURE 5: (a) The number of vehicles in community is 100. (b) The number of vehicles in community is 70.

decrease in the probability that vehicles access RSU. Similarly, the probability of vehicles accessing to RSU increases if the speed decreases or the number of vehicles having accessed RSU decreases.

Figure 5 shows the influence of N^j, $j = 1, 2$, on ESS in two-community evolutionary game. Figure 5(a) shows the ESS when $N^j = 100$ while Figure 5(a) shows the ESS when $N^j = 70$. As the simulation result demonstrates that the traffic load and the cost of RSU1, RSU2, and RSU3 in population 2 decrease when N^2 reduces, which makes the vehicles in population 2 would like to access RSU1, RSU2, and RSU3, vehicles in population 1 are also more inclined to access RSU1 and RSU2 as they thought the number of vehicles accessing RSU1 and RSU2 decreases. As shown in Figure 5, the ESS $x = (0.14, 0.06, 0.23, 0.14, 0.06)$ in Figure 5(a) increases to Figure 5(b) $x = (0.68, 0.3, 0.22, 0.33, 0.42)$ if N^2 decreases.

Figure 6 shows the service types' effect on average throughput. The RSU's price increases along with the increase of the request file importance index (a), which makes the number of vehicles accessing RSU decreases. Meanwhile,

Table 3: Simulation parameter values.

Parameter	Value
RSU's transmission radius R	1000 m
S/N	30 dB
Bandwidth W	20 MHz
Path loss exponent γ	2
The congestion index φ	1.2
Weight coefficient β	0.15
Weight coefficient δ	0.1
Weight coefficient Φ	0.1

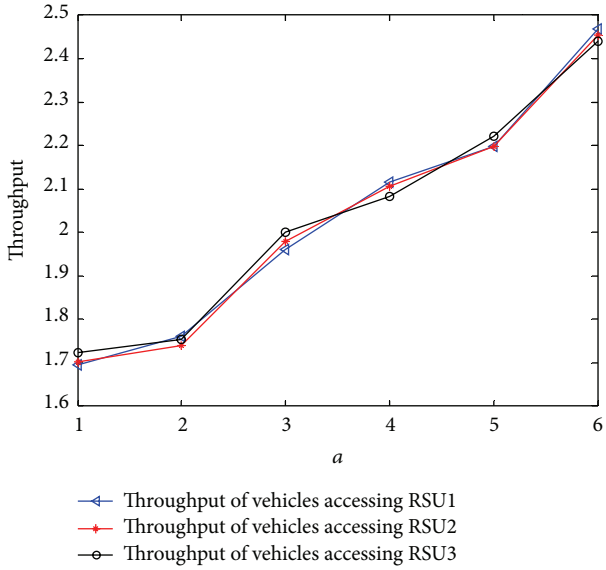


Figure 6: The request service type on throughput.

the average bandwidth which the RSU assigned to vehicles increases as the population did not change, which makes the average throughput increase.

Figure 7 represents the load balancing of RSUs. RSU's pricing and the average bandwidth maintain stable when the number of vehicles in communities is the same, which makes the traffic load balancing; RSU's traffic load retained around 0.99. The number changing leads to the changing of RSU's pricing and the probability of accessing RSU, so the RSU's balance index decreased to 0.92.

6. Conclusions

In this paper, we have set up an evolutionary game model to formulate the competition among vehicles in the same community and different communities with bounded rationality in VANET for RSU access problem. We have investigated the dynamic evolutionary process of ESS when vehicles drive through RSU. A vehicle accesses RSU based on its payoff, which is a function of throughput and cost. The dynamics of RSU access has been mathematically modeled by the replicator dynamics that describes the adaptation in proportions of vehicles accessing different RSUs. The ESS has

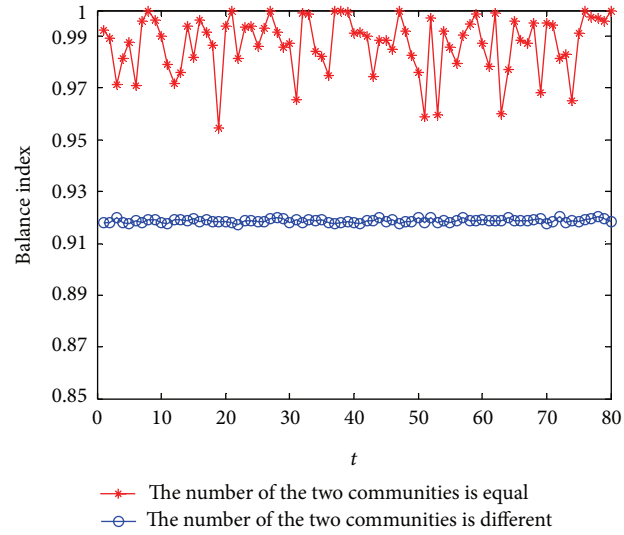


Figure 7: The effect on balance index of the number of vehicles in community.

been considered to be the stable solution for which all vehicles receive identical payoff from difference RSUs. Detailed analyses have shown the evolutionary process. Besides, in the simulation result we can know that the package size, vehicle speed, and the number of vehicles in community have effects on the ESS, which then affect the network throughput and load balancing.

Due to the limited communication time between vehicles and RSU, in the future work, we can use cooperative download method to improve the network throughput.

Acknowledgments

This work is supported by the Scientific Research Foundation for the Returned Overseas Chinese Scholars, High-Tech 863 Program (no. 2012AA111902) and State Key Program of National Natural Science of China (no. 60933011).

References

[1] M. H. Cheung, F. Hou, V. W. S. Wong, and J. Huang, "Dynamic optimal random access for vehicle-to-roadside communications," in *Proceedings of the IEEE International Conference on Communications (ICC '11)*, June 2011.

[2] O. Trullols-Cruces, M. Fiore, and J. M. Barcelo-Ordinas, "Cooperative download in vehicular environments," *IEEE Transactions on Mobile Computing*, vol. 11, no. 4, pp. 663–678, 2012.

[3] J. Liu, J. Bi, Y. Bian, X. Liu, and Z. Li, "SRelay: a scheme of cooperative downloading based on dynamic slot," in *Proceedings of the IEEE International Conference on Communications (ICC '12)*, pp. 381–386, 2012.

[4] Y. Zhang, J. Zhao, and G. Cao, "On scheduling vehicle-roadside data access," in *Proceedings of the 4th ACM International Workshop on Vehicular Ad Hoc Networks (VANET '07)*, pp. 9–18, September 2007.

[5] A. Mas-Colell, M. D. Whinston, and J. R. Green, *Microeconomic Theory*, Oxford University Press, 1995.

[6] R. J. Aumann, *Handbook of Game Theory With Economic Applications*, Elsevier, Amsterdam, The Netherlands, 1994.

[7] J. Weibull, *The Evolutionary Game Theory*, Shanghai People's Publishing House, 2006.

[8] F. Vega-Redondo, *Evolution, Games, and Economic Behaviour*, Oxford University Press, Oxford, UK, 1996.

[9] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott, "Impact of human mobility on the design of opportunistic forwarding algorithms," in *Proceedings of the 25th Conference on Computing and Communication (INFOCOM '06)*, Barcelona, Spain, 2006.

[10] Y. Fukuda, A. Fujiwara, M. Tsuru, and Y. Oie, "Analysis of access point selection strategy in wireless LAN," in *Proceedings of the VTC*, pp. 2532–2536, 2005.

[11] L.-H. Yen, J.-J. Li, and C.-M. Lin, "Stability and fairness of AP selection games in IEEE 802.11 access networks," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 3, pp. 1150–1160, 2011.

[12] Y. Bejerano and S.-J. Han, "Cell breathing techniques for load balancing in wireless LANs," *IEEE Transactions on Mobile Computing*, vol. 8, no. 6, pp. 735–749, 2009.

[13] R. El-Azouzi, F. De Pellegrini, and V. Kamble, "Evolutionary forwarding games in delay tolerant networks," in *Proceedings of the 8th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt '10)*, pp. 76–84, June 2010.

[14] D. Niyato and E. Hossain, "Dynamics of network selection in heterogeneous wireless networks: an evolutionary game approach," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 4, pp. 2008–2017, 2009.

[15] C. A. Kamhoua, N. Pissinou, J. Miller, and S. K. Makki, "Mitigating routing misbehavior in multi-hop networks using evolutionary game theory," in *Proceedings of the IEEE Globecom Workshops (GC '10)*, pp. 1957–1962, December 2010.

[16] T. Chen, L. Zhu, F. Wu, and S. Zhong, "Stimulating cooperation in vehicular ad hoc networks: a coalitional game theoretic approach," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 2, pp. 566–579, 2011.

[17] W. Wang, F. Xie, and M. Chatterjee, "Small-scale and large-scale routing in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 9, pp. 5200–5213, 2009.

[18] S. Bitam and A. Mellouk, "QoS swarm bee routing protocol for vehicular ad hoc networks," in *Proceedings of the IEEE International Conference on Communications (ICC '11)*, pp. 1–5, June 2011.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 676850, 12 pages
http://dx.doi.org/10.1155/2013/676850

Research Article

Comprehensive Vehicular Networking Platform for V2I and V2V Communications within the Walkie-Talkie Project

José Santa,[1] Fernando Pereñíguez,[1] Juan C. Cano,[2] Antonio F. Skarmeta,[1] Carlos T. Calafate,[2] and Pietro Manzoni[2]

[1] *Department of Information and Communication Engineering, University of Murcia, 30100 Murcia, Spain*
[2] *Department of Computer Engineering, Polytechnic University of Valencia, 46022 Valencia, Spain*

Correspondence should be addressed to José Santa; josesanta@um.es

Received 7 March 2013; Accepted 12 June 2013

Academic Editor: Xu Li

Communication architectures integrating vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications will be the key of success for the next generation of cars. Nevertheless, the integration of these communication partners in the same platform is a challenging issue because most of the literature is focused on individual parts, such as V2V routing protocols or specific safety services. The Walkie-Talkie project was proposed to fill this gap, focusing on the integration of V2V and V2I systems to equip vehicles with a set of intelligent services addressing safer, smarter, and sustainable driving. This paper describes the developed communications platform. The network design is based on IPv6 to support middleware and applications executed on both the vehicle and infrastructure sides. Whereas V2I is focused on the usage of IPv6 network mobility, V2V is provided by means of a hybrid solution based on intelligent delivery and delay tolerant networks. On top of the networking protocols, a service access middleware exploiting concepts from next generation networks is proposed, together with a proper on-board application management based on the open service gateway initiative. A prototype of the network and real evaluations are also presented as a proof of concept of our platform.

1. Introduction

It is increasingly apparent that, with the support of wireless communication, intelligent transportation systems (ITSs) will play a leading role in our society, where each automotive vehicle will be, in the future, a unique node in a global and ubiquitous vehicular communications network. These intelligent communication systems will support scenarios where the interactions within the vehicle, with the surrounding environment, and directly with nearby vehicles, will offer real-time communication among the thousands of cars daily crossing our cities and highways and opening new opportunities to many challenging applications dealing with security, management, and entertainment on the road. The Walkie-Talkie project (http://www.grc.upv.es/walkietalkie/) looks at the emerging intelligent transportation system environments and is aimed at analyzing challenges and offering solutions to enable safer, smarter, and greener transportation for the next generation of smart cars.

In the same way that communication between vehicles and infrastructure has been crucial for the success of current applications used in vehicular scenarios, where the best example has been the widespread adoption of the GPS technology, communication architectures integrating vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and infrastructure-to-vehicle (I2V) communications will be the key to success for the next generation of smart cars. In fact, major automobile manufacturers, as well as public and private entities dealing with traffic management, are currently considering applications that require a high level of connectivity, including (a) active safety, accident detection, and traffic management applications, (b) smart route planning applications that will improve traffic efficiency, (c) fleet management and vehicle monitoring applications, (d) entertainment and

comfort applications, and, more recently, (e) new services aimed at reducing the effects of CO_2 emissions, thereby improving greener transportation.

These new applications depend on efficient vehicle-to-vehicle and vehicle-to-infrastructure cooperative communications, an area that so far is only evidenced in traditional radio data systems and traffic message channel (RDS/TMC) networks, as well as in the new e-call system. It is therefore mandatory to promote research in the field of vehicular networks based on technologies such as vehicular ad hoc networks (VANETs) in order to provide intelligent transportation systems integrated into "on-board" units, thus providing intelligent cooperative communication interfaces on the road. Towards this direction, the Walkie-Talkie project focuses on the integration of V2V, V2I, and I2V communication systems to equip vehicles with a set of intelligent services addressing safer, smarter, and sustainable driving.

The proposal presented in this paper covers two key points: (1) the integration of technologies and protocols for V2V and V2I communications in a common networking platform, and (2) the provision of a vehicular service framework ready to deploy new-age infotainment applications in the road domain. In order to cope with the previously mentioned aims, a comprehensive vehicular platform has been conceived in Walkie-Talkie, and the main findings are presented here, detailing innovative proposals in the areas of the following:

(i) V2V communication, presenting a hybrid solution based on intelligent broadcast delivery and delay tolerant networks (DTNs).

(ii) Infrastructure-based vehicular networks, on the basis of secure IPv6 network mobility.

(iii) Service provision and management, through a remote service access middleware based on next generation networks and a proposal for local application management that uses the open service gateway initiative (OSGi).

(iv) Experimental evaluation, by testing essential modules of the platform using a proper prototype.

This way, the paper is organized as follows: Section 2 overviews the most important previous works in the area; Section 3 presents the overall network architecture of the proposal; Section 4 details the vehicle-to-infrastructure communication subsystem, while Section 5 presents the V2V subsystem; Section 6 presents the developed service-access framework; Section 7 presents the developed network testbed and shows experimental results; and, finally, Section 8 concludes the paper.

2. State of the Art

Practical proposals for vehicular communications similar to the one developed in the Walkie-Talkie project are not frequent in the literature, due to the tough design and development efforts needed. For example, the work presented in [1] proposes an on-board solution for providing vehicular communications through an entity called "Car Gateway" acting as a mobile router. However, this solution is highly coupled with the vehicular platform, and it does not develop a generic communication stack to be instantiated on the different elements of an ITS network, as encouraged by the ISO/ETSI guidelines for the development of cooperative vehicular systems.

More related solutions can be found on recent proposals from field operational tests (FOTs) projects, since they offer the needed framework for implementing integral communication modules. In this sense, authors in [2] present the Drive C2X ITS station proposal, which integrates an OSGi-based software platform for applications and where communication issues are addressed at the network level. However, what is noticeable in this work is that IP networking has been left out, being UMTS-based communications only used for management and testing purposes. A similar contribution can be found in [3] where authors present some investigations developed in the context of the simTD project. More precisely, this work introduces a novel communication architecture providing enhanced security and privacy communications thanks to the use of a public key infrastructure. Nevertheless, this solution does not integrate IP communications.

Researchers have identified IPv6 communications as the key to ITS cooperative systems deployment [4]. Consequently, a combined solution for IPv6-based network mobility and security for noncritical vehicular services is necessary. The work presented in [5] follows this research line, presenting a solution based on V2I and V2V communications. Nevertheless, unlike the solution proposed by the Walkie-Talkie project, this contribution employs a constrained and nonautonomous communications stack that is used for experimental evaluation of specific routing and flow management subsystems.

In the particular case of V2V communications, also known as vehicular ad hoc networks (VANETs), extensive research has taken place in recent years [6]. These technologies, based on short-range communication radios such as IEEE 802.11p, support many different services and active applications between vehicles. Although many different unicast routing approaches have been proposed for VANETs [7], the Walkie-Talkie project does not forecast services and applications under pure unicast routing approaches. In contrast, due to rapid topology changes and frequent disconnection, we envision services taking advantage of routing approaches based on intelligent broadcast delivery for emergency and delay sensitive services and unicast routing approaches based on the concepts of delay tolerant networks to support noncritical services.

Regarding intelligent broadcast delivery, over the years several schemes have been proposed. In [8] we can find some of the most interesting schemes: counter-based, distance-based, and location-based. Note that all of these are based on inhibiting certain vehicles from rebroadcasting, reducing message redundancy, channel contention, and message collisions. In particular, they inhibit vehicles from rebroadcasting when the additional coverage area is very low. Additional efforts to find efficient broadcast delivery schemes can be found in [9–13].

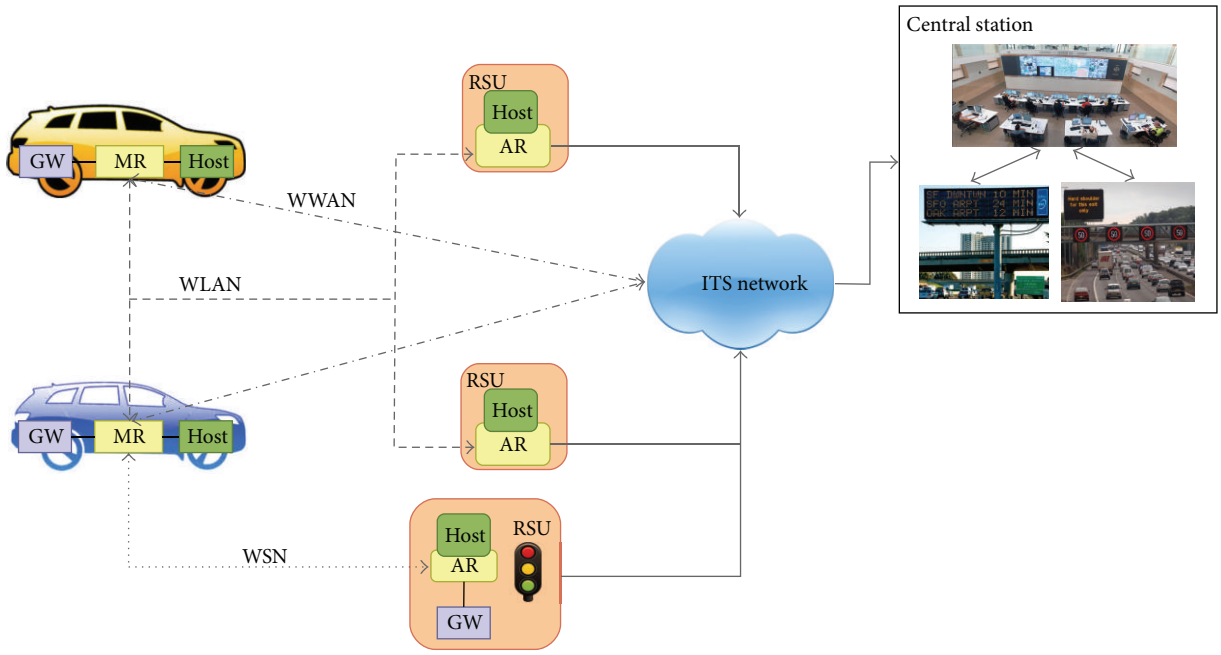


Figure 1: Overall architecture of the Walkie-Talkie communication platform.

When DTN proposals are considered, schemes can be divided in flooding and forwarding strategies. In the flooding family, each node delivers multiple copies of each message to other nodes, which act as relays, without using prior information about the network structure. Some examples of these protocols are presented in [14], such as Direct Contact (data transmitted in one hop), Two-Hop Relay, and Tree-Based Flooding. In epidemic routing [15], all nodes will eventually receive all messages, obtaining a maximum delivery ratio at the cost of consuming network resources heavily (channel, buffer, etc.). Algorithms in the forwarding family require adding some knowledge about the network that is used to select the best path from the source to the destination. The simplest approach is using a distance metric to estimate the cost of delivering messages between nodes (Location-Based Routing). Other more sophisticated schemes such as the Per-Hop Routing, where the forwarding decision is made by the intermediary node which determines the next hop, and the Per-Contact Routing, where the routing table is recomputed each time a contact is available, are presented in [16].

3. System Architecture

In the following we describe the Walkie-Talkie communications system architecture. First, the ITS network design is presented, identifying both types of ITS station nodes and communication patterns among them. Next, the general communication stack is presented, detailing the particularities that arise when it is instantiated on the different ITS station nodes.

3.1. Overall Network Design. The communication network envisaged in the Walkie-Talkie project covers V2V and V2I communications, as well as the interconnection between both subsystems. For this purpose, it takes into account three fundamental parts of networked ITS architectures: the on-board equipment of the vehicle, roadside units, and the remote service centre. The architecture follows the guidelines marked by ISO TC 204 and ETSI TC ITS, with the recent European Communication Architecture [17]. Figure 1 shows an overview picture of the developed communication network. Cars communicate among them using a V2V routing protocol or with infrastructure units using common Internet protocols over IPv6.

Vehicles are provided with three key functions: gateway (GW), mobile router (MR), and host, as can be seen in Figure 1. The MR is in charge of performing routing tasks for V2I and V2V connectivity, so that the rest of hosts in the vehicle are not aware of the network complexity. A host could be a common IP-based smartphone or a tablet, which uses the vehicle MR to connect with the ITS network and the Internet. Finally, a GW entity is provided to connect with the various sensors available in the vehicles using the adequate protocols. In the Walkie-Talkie project, for instance, this entity is in charge of providing access to vehicle status information provided through the controller area network (CAN) bus. Similar to the communication architecture proposed by standardization bodies like ISO and ETSI [18, 19], there exists an in-vehicle network through which GW, MR, and in-vehicle hosts are connected, usually in the form of a WiFi access provided by the MR.

At the roadside, a set of *roadside units* (RSUs) are provided with a communications stack able to communicate using IPv6 and acting as an attachment point for vehicles using wireless local area networks (WLANs) based on technologies such as 802.11b/g (common WiFi) or 802.11p (ETSI G5).

The networking tasks of the RSU entity are performed by the access router (AR), whereas host functionalities allow the

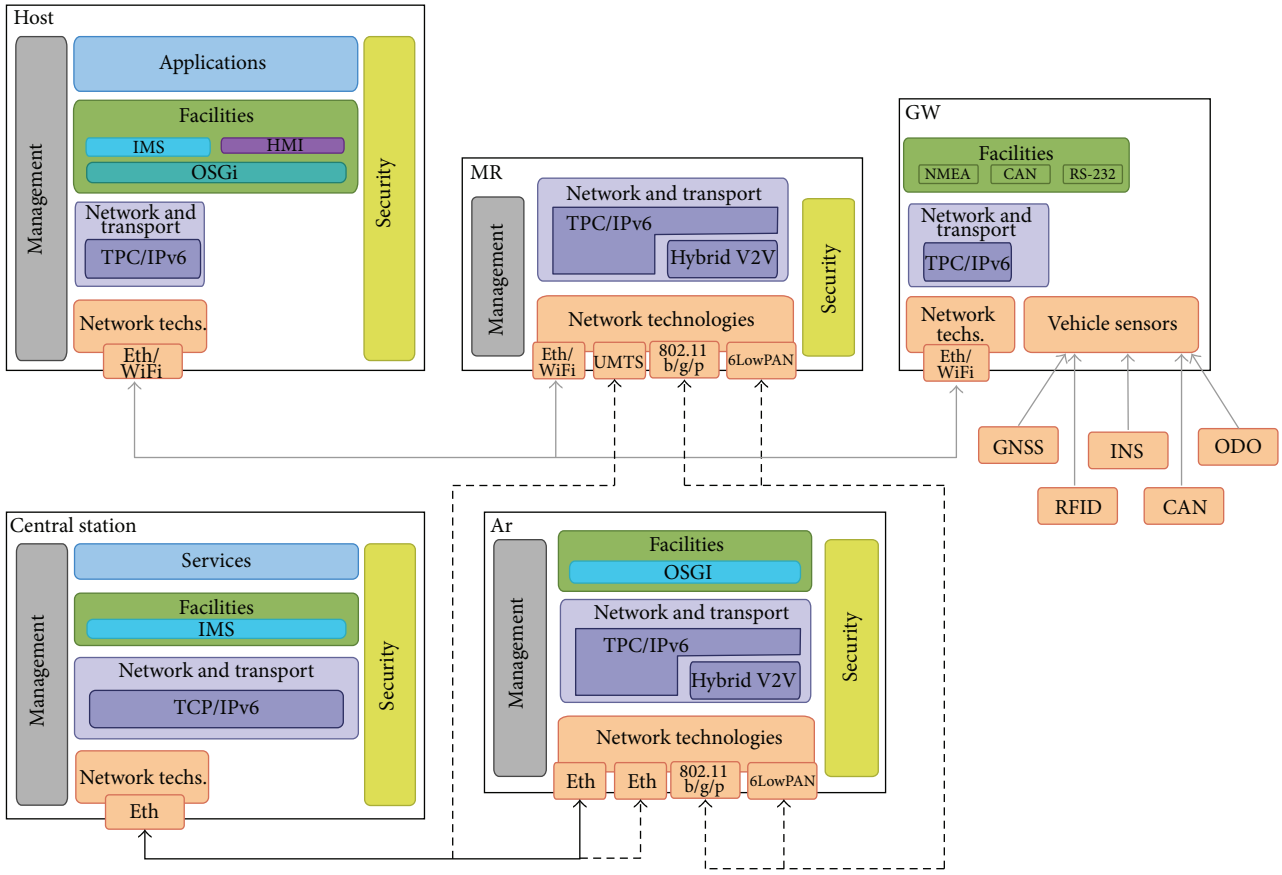


Figure 2: Walkie-Talkie vehicular communications stack.

execution of any necessary application. Nevertheless, the host load of the RSU is expected to be much less relevant than in the vehicle and central sides, and this is the reason why these functionalities are expected to be integrated together with the AR. Additionally, since some RSUs can be connected with former road devices such as semaphores or variable message signs, a GW entity is also needed. In this case, a communications channel is also provided by using wireless sensor networks (WSNs). In particular, the Walkie-Talkie project envisages the use of IPv6 over low power wireless personal area networks (6LowPAN) to connect with special RSUs embedded in the pavement, road signs, and gantries.

The last key element depicted in Figure 1 is the central station, where services are hosted. Other important functions assigned to the central station are the maintenance of the IPv6 addressing of the vehicle and interfacing with the Internet offering IPv6 to IPv4 transition solutions, as it is explained in Section 4.

3.2. Communications Stack. According to the reference ISO/ETSI ITS communications architecture [18, 19], a reference OSI-based stack with four horizontal layers (access technologies, network and transport, facilities and applications) and two vertical layers (management and security) should be instantiated in the form of ITS station (ITS-S) nodes in vehicles, nomadic devices (mobile hosts), roadside units, and central systems. In the following we present such instantiation for the case of the vehicle, roadside equipment, and the road operator control centre. Figure 2 shows the main modules of the communication stack included in the three vehicles nodes, roadside AR and central station. Some nodes could instantiate the stack using more than one physical machine. This is true, for instance, in the case of the central station, as explained later on.

The design shown on the top of Figure 2 shows the instantiation of the Walkie-Talkie communications stack in the vehicle, where the whole stack functionality is split in three nodes: host, MR, and GW, as introduced in the previous section. The MR includes the required functionalities to hide networking tasks to in-vehicle hosts. An unlimited number of hosts could connect with the ITS network by means of the access router through a common WiFi (e.g., 802.11a/b/g) or Ethernet connection. To maintain external communication with roadside equipment, control centre, and the rest of vehicles, the Walkie-Talkie platform currently supports the use of the following communication technologies: 3G/UMTS, common WiFi, 802.11p (ETSI G5), and 6LowPAN. Nevertheless, 802.11p is the most appropriate technology for V2V communications. IPv6 is used as a common network-level protocol for all nodes in the architecture, and the connectivity with the infrastructure is supported by the set of elements included within the networking and transport layer of the MR. V2V communication is enabled through another module which implements a hybrid solution based on intelligent

broadcast delivery and DTN. As can be seen, IPv6 packets can be encapsulated in the V2V network using the proper VANET protocol. Finally, apart from the modules in charge of network operations, the MR is equipped with the elements required to secure communications. More details about the network modules for V2I and V2V communications are given in Sections 4 and 5, respectively.

The stack just on the left of the MR belongs to the vehicle host, which is in charge of executing user-level applications that could access remote services. This stack includes a common networking middleware based on the transport control protocol (TCP) and the user datagram protocol (UDP). An essential part of the host protocol stack is the facilities layer. A Java virtual machine (JVM) is used as the basis for the open service gateway initiative (OSGi) framework. OSGi acts as the lifecycle manager of both middleware parts and applications, simplifying the communication among software modules installed in the host. Above OSGi, another relevant facility is the IMS (IP Multimedia Subsystem) client, which is directly used by applications to access remote services in a normalized way, as explained in Section 6.

The GW communications stack is shown on the top right corner of Figure 2. Apart from the minimal functionality necessary to communicate with the rest of modules of the vehicles, it performs access and adaptation tasks for communicating with other vehicles subsystems, like the global navigation satellite system (GNSS), radio-frequency identification (RFID), inertial navigation system (INS), CAN bus, and odometry.

The communications stack instantiated in the roadside access router (lower right part of Figure 2) acts as a network attachment point for vehicles using short/medium-range communication technologies. Similarly to the MR, the available wireless technologies to communicate with vehicles are common WiFi, 802.11p (ETSI G5), and 6LowPAN. The AR could communicate with the central station using either an UMTS link or a common wired connection.

The last stack of Figure 2 is the one developed for the central station, on the lower left corner. Without loss of generality, we assume that this entity brings together the functionalities that are necessary at the road operator's control centre to maintain vehicle connectivity and support the infrastructure-based Walkie-Talkie services. The facilities layer now includes the necessary software to provide the IMS server-side capabilities for accessing services and hosting applications. These functionalities could be provided in a distributed way, using independent servers.

4. Infrastructure-Based Vehicular Communications

The network stack conceived by Walkie-Talkie includes a set of features enabling efficient communication between vehicle and infrastructure. In fact, this kind of vehicular communication is of paramount importance since it is in the V2I/I2V segment where novel traffic efficiency, comfort services, and relaxed safety applications can be initially tested and deployed due to the penetration issues associated to V2V communications. Furthermore, as has been acknowledged by the research community [4], communications based on the *Internet protocol* (IP) will be the key for successfully deploying future ITS applications, since it is a widely adopted protocol whose operation has been deeply verified. In particular, *IP version 6* (IPv6) has enough addressing capabilities for being used in vehicular environments where potentially millions of entities (passengers, traffic lights, road sensors, etc.) will coordinate and exchange information.

For this reason, as depicted in Figure 2, the presented vehicular platform integrates the functionality necessary for establishing IPv6 communications. The following common IPv6 functionalities are supported by the communication stack regardless of the type of ITS node where it is instantiated:

(i) IPv6 address autoconfiguration. One of the first tasks to be developed by ITS nodes when they connect to the IPv6 network relies on the acquisition of a valid IPv6 address. This process is supported by our communications stack using either stateless [20] or dynamic auto-configuration based on the DHCPv6 protocol [21].

(ii) IPv6 signaling. The basic operation of IPv6 requires nodes to support basic functionalities necessary during the establishment of IPv6 communications with other nodes. This is supported by the communication stack using the Neighbour Discovery protocol [22] and the Internet Control Message Protocol (ICMPv6) [23].

According to the ITS station reference architecture jointly standardized by ISO and ETSI, the Walkie-Talkie vehicular communications architecture is conceived to allow vehicle hosts to connect to the IPv6 network through the MR in a transparent manner. Therefore, apart from the aforementioned basic functionalities, MRs include additional features to support IPv6 reachability and session continuity of the in-vehicle network. More precisely, this feature is carried out by using *network mobility basic support* (NEMO) [24], a protocol that allows maintaining global reachability of the in-vehicle network while hiding the mobility tasks to vehicle hosts.

In NEMO, mobility capabilities are distributed between the MR and a new entity called home agent (HA), in order to maintain the IPv6 addressing for the mobile network. An unchangeable IPv6 *mobile network prefix* (MNP) is delegated by the home network to the MR for assigning addresses to the *mobile network nodes* (MNNs) that in our case are the vehicle hosts. Following the NEMO model, upon the reception of a *router advertisement* (RA) message from a roadside access router, the MR is aware of the existence of a new network. In this case, the MR, which already has a fixed IPv6 address within its home network (*Home Address* or HoA), generates a new autoconfigured IPv6 address within the new visited network. This address is called care-of address (CoA), and it is immediately notified to the HA. This notification is performed by the MR through a *binding update* message, which is acknowledged with a *binding ACK* sent by the HA. Only the MR and the HA are aware of the network change, since MNNs remain connected with the MR using the same

address. Hence, when any node outside the home network (*correspondent node* or CN) communicates with any of the hosts connected in the vehicle, it uses the home address as destination, and, hence, packets follow the route towards the home network. Then, HA redirects these IPv6 packets to the current IPv6 CoA of the MR, which finally distributes the packets within the mobile network. In the same way, when packets are sent from any MNN to a CN, they are routed by the MR towards the HA, which forwards them to the destination. Hence, the HA and the MR perform an IPv6 into IPv6 encapsulation to create a mobility tunnel.

As described in Section 3.1, MRs are expected to maintain multiple network interfaces (802.11a/b/g, UMTS, etc.). In this scenario, the mobility experience offered by NEMO to vehicle hosts can be improved by enabling the MR to maintain network mobility across multiple interfaces. This feature is integrated in our communications stack by using the *multiple care-of addresses registration* (MCoA) [25] extensions, thanks to which the HA is aware that the MR is reachable through a set of CoAs.

The proposed vehicular communications platform not only supports the basic mobility management functionalities, but it also includes different elements to secure mobility-related traffic. More precisely, the provision of a secure mobile experience is achieved by means of the *IP Security* (IPsec) protocol [26], which is an enhancement to the basic IP protocol that defines a set of security services for protecting IP traffic. Since it is defined at IP level, the security protection is transparent to other protocols carried over IP like, in our case, NEMO and MCoA. Mobility traffic exchanged between MR and the HA is protected thanks to the establishment of an IPsec tunnel, thus providing both confidentiality and integrity. A mandatory step prior to the tunnel establishment consists in the negotiation of the so-called *security associations* (SAs) where both mobile router and HA agree on the set of security parameters (e.g., cryptographic algorithms or key material) to be used for protecting the mobility traffic. The *Internet key exchange version 2* (IKEv2) protocol [27] is used for this purpose since it has been specially conceived to provide such functionality.

5. Vehicle-to-Vehicle Communications Approach

As anticipated earlier on, the Walkie-Talkie project bets on intelligent broadcast delivery for emergency and delay sensitive services and DTN unicast routing for noncritical services. In our scheme, vehicles operate in either warning or normal mode. Normal mode represents a default behavior; however, when a vehicle detects a dangerous condition, it will start operating in warning mode. Warning mode vehicles inform other vehicles about abnormal situations by disseminating warning messages periodically using the highest priority in the 802.11p MAC layer. We consider abnormal situations as any condition that could affect the traffic security and probably cause an accident, for example, slippery road, a previous accident where the involved vehicles are an obstacle for the normal traffic flow, works on the road, and so forth. Only messages representing these situations will be disseminated using the highest priority, while messages for comfort, entertainment, and, in general, noncritical applications, will be sent using lower priorities. Hence, normal vehicles use the DTN protocol, while warning vehicles use the smart dissemination delivery approach. Next, we briefly describe both communication approaches.

5.1. V2V Based on Smart Dissemination. In VANETs, intermediate vehicles act as message relays to support end-to-end vehicular communications. For applications such as route planning, traffic congestion control, and traffic safety, the flooding of broadcast messages might be considered a straightforward approach to achieve a widespread dissemination. However, if flooding is done blindly, broadcast storms may arise, with several disadvantages to the dissemination process [8]. For this reason, we propose the use of the *enhanced message dissemination based on roadmaps scheme eMDR* [28] to efficiently disseminate critical information in VANETs. Our novel proposal takes into account the effect that buildings have over the signal propagation to improve message dissemination in real urban scenarios. At the frequency of 5.9 GHz (i.e., the frequency band adopted by the 802.11p standard), radio signals are highly directional and will experience a low depth of penetration in urban scenarios. Hence, in most cases, buildings will absorb radio waves at this frequency, making communication only possible when vehicles are in line-of-sight.

In *eMDR*, when a vehicle starts the broadcast of a message m, it sends m to all of its neighbors. When any nearby vehicle receives m for the first time, it rebroadcasts it by further relaying m to its neighbors. To this end, every vehicle rebroadcasts m to the surrounding vehicles only when the distance between sender and receiver is higher than a distance threshold, or when the receiver is in a different street than the sender. We consider that two vehicles are in a different street when (i) both are indeed in different roads, or (ii) the receiver, in spite of being in the same street, is near to an intersection. This navigation information is obtained through a navigation system facility installed on the vehicle host, which is consulted based on the position calculated by the GPS receiver and accessed through the vehicle GW. Hence, warnings can be rebroadcasted to vehicles which are traveling on other close by streets, thus overcoming the radio signal interference due to the presence of buildings.

A formal description of our approach can be found in [28], where we demonstrate the offered benefits with respect to several previously existing proposals [8, 29, 30], when evaluating the performance of disseminating critical information in VANETs under realistic city maps.

An example of critical applications is the case of a service in charge of disseminating information about accidents. Figure 3 shows the information that our *eMDR* protocol will disseminate just after an accident takes place. This packet is encapsulated in IPv6 datagrams and then forwarded using our protocol. It includes the following information: (a) the time when the accident has occurred, (b) the location of the vehicle to determine the location of the incidence, (c) the characteristics of the vehicle and the profile of the occupants

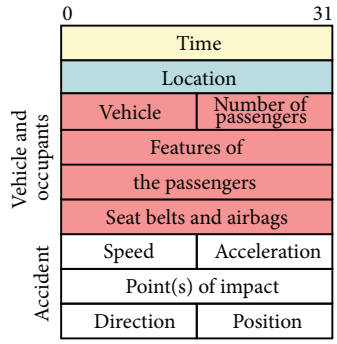


Figure 3: Essential information elements to be transmitted in case of accident detection.

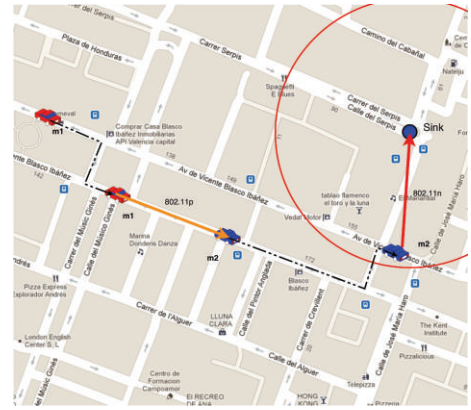


Figure 4: Typical situation for MSDP: dashed lines represent the movement of the nodes, while solid lines represent wireless transmissions.

(for supporting emergency services in the assistance), and (d) accident details, such as the speed and acceleration of the vehicle when the impact occurred, along with the impact details. All these data help in determining the severity of the impact, making it possible to save lives, manage resources efficiently, and enable crashed vehicles to be removed from the site, restoring traffic flow quickly.

5.2. VANETs as Delay-Tolerant Networks. Our previous approach based on broadcasting techniques is able to rapidly inform as many vehicles as possible, but it also imposes a heavy load on the channel. A delay tolerant scheme could be a solution for this, apart from being appropriate for those applications and services where notification delays are not critical.

Vehicles in a VANET are, typically, sparsely spread across the roadmap, creating time-varying clusters of nodes due to the distance between vehicles and the signal blockage due to buildings. This environment is subject to disruption, disconnection, and long delays. Hence, a complete source to destination forwarding path is not always available. Under these conditions, where only intermittent connectivity and opportunistic contact take place, we propose, for noncritical services, the use of DTNs to deliver data packets. DTNs allow sharing information even in the presence of high delays, and, when a route to the destination of a message does not exist, the message is stored and carried until a route becomes available (this is known as the "store-carry-forward" paradigm). Moreover, by having location information, the packet forwarding can be enhanced.

In the Walkie-Talkie project we propose the map-based sensor-data delivery protocol (MSDP), a DTN routing protocol that, using the digital cartography facility integrated in the MR stack, searches for the best next forwarding node. The novelty of our proposal is that, with the aim of efficiently delivering data packets, it bases its routing decisions not only on distance or directions but also on the programmed route of the node, the amount of data stored in the mobile router's buffer, and the trustworthiness of the data source. This way, it is mandatory that all vehicles maintain a certain degree of knowledge about their travel plan. The basis of the MSDP protocol is a utility index (UI). This index is used to make routing decisions, and it is based on several factors, such as the trustworthiness of the location, the time to reach the next node, and the transmission availability. In other words, a higher UI value indicates that the node is a better candidate to reach the destination. In fact, this destination tends to be an RSU, since one of the main goals of MSDP is the collection of information gathered from the road side in the RSUs.

Figure 4 presents a typical situation for MSDP, where dashed lines represent the movement of the nodes, while solid lines represent wireless transmissions. In this example, the sender node is m_1. Our protocol can be shortly explained as follows: information messages are generated by bundling information from different sensors of the vehicle using the GW. Large messages are split into packets that are stored in the MR's buffer. In MSDP, those nodes which have packets in their buffers are called *custodians*. Initially the sender node m_1 is a custodian. Custodians periodically broadcast messages announcing their presence and their UI. Nodes which receive those announcements are called *candidates*. Candidates will respond to these announcements by broadcasting their presence and their UI. If the candidate UI is higher than the custodian UI, it can transmit the packets to this candidate. The candidate confirms the reception of the packets through an ACK message. It is important to remark that a custodian will never remove a message until a candidate confirms itself as the new custodian. For example, in Figure 4, the custodian node m_1 has contacted with the candidate node m_2, which has a higher UI. Hence, it decides to transmit its packets to m_2 using the 802.11p interface. So, from now on, m_2 is the new custodian node. Finally, when a *custodian* reaches an RSU, it will try to use this communication opportunity to deliver as many packets as possible. This is the final hop of our example, when custodian node m_2 transmits the packet to the RSU, now using 802.11n instead in this particular example. This information is then handled by a facility installed in the AR, which processes the data and sends a notification to the proper service in the central station. Evaluations performed showed that MSDP has a reasonable delivery time with a reduced overhead compared to other previous solutions [31].

6. Service Provision in Walkie-Talkie

The *open services gateway initiative* (OSGi) is a framework intended to facilitate the software management in Java environments. OSGi provides important advantages when deploying new applications, achieving software modularity and solving intermodule dependencies. In this framework, each application is implemented as one or more OSGi modules, called *bundles*, which are deployed together with extra meta-information attached in a manifest file. Among other data, this metainformation lists the exported packages (packages visible by other bundles) and the imported ones (packages needed for the current bundle). With this information, the OSGi framework manages the dependencies automatically. Thanks to this feature, it is possible to build a module hierarchy, from the most basic middleware to user applications.

Due to its numerous benefits, the OSGi framework has been integrated within the proposed communications stack to facilitate the management of ITS applications. In the following, we describe two relevant software modules that have been implemented above OSGi: the *IP multimedia subsystem* (IMS) and the *human-machine interface* (HMI).

6.1. IMS-Based Service Access Middleware. Nowadays different services coexist in the field of ITS, from a simple video call to an advanced service for traffic monitoring. Therefore, a common framework for the provision and access to these services is needed. IMS can be an efficient solution in this frame and existing works demonstrate its potential on the ITS field [1, 32]. For this reason, the Walkie-Talkie communications stack includes a service access middleware based on the 3GPP IMS, which is placed at the facilities layer. IMS is a next generation network proposal that provides mechanisms for session establishment and negotiation of capabilities between client applications and services. Although IMS provides a mobility solution at the service level, this capability has not been used since the communications stack already includes network mobility support for the in-vehicle network (see Section 4). Thanks to the NEMO protocol operation, each IMS *terminal equipment* (TE), included in the vehicle host, will have a permanent IPv6 address independently of the IMS domain in which the user is registered.

The process of host registration in the IMS domain and the subscription to a service is carried out by using the SIP protocol, which is the basis technology to support IMS. First, the TE needs to register in the IMS domain. This is carried out by an initial SIP exchange with the IMS core, located in the central station, indicating the identity of the subscriber, the authentication method, and the user credentials. Once the subscriber is registered, the TE is able to subscribe to IMS services by means of a new SIP transaction using the desired service parameters, for example, the quality of service (QoS) or the session lifetime. The IMS core entities forward this request to the corresponding SIP application server (SIP-AS), which decides whether it is able to accept these parameters. In this way, a negotiation is maintained between TE and the service edge. If the negotiation is successful, the service session is established and the data flow between the TE and the service edge executed in the SIP-AS starts.

6.2. Human-Machine Interface. When a graphical interface is used, as in the case of the vehicle host, another important resource to deal with is the screen and how applications can gain access to it in a homogeneous manner. For this purpose, and because of the several requirements that an HMI must accomplish [33], the Walkie-Talkie communications stack integrates a modular HMI service. This OSGi bundle shows a main interface in which all applications installed in the vehicle host are integrated. This service has three fundamental aims.

(i) It is in charge of drawing interface objects for all the installed applications. Each application must define an XML description of its interface, which is provided to the HMI service as an argument to paint the graphical elements (buttons, labels, etc.).

(ii) The HMI module provides the unique input/output channel with the user, and it is in charge of distributing interface information among all applications.

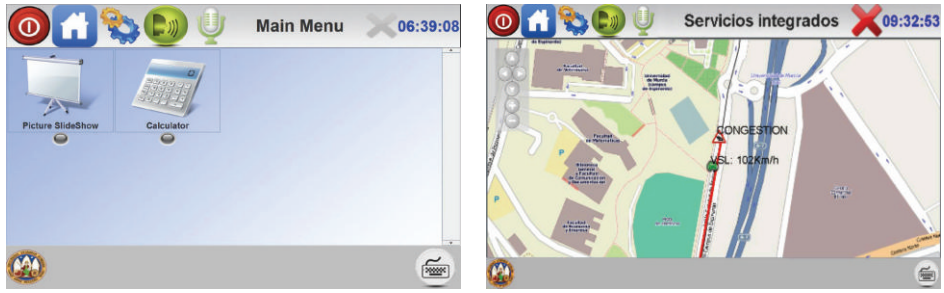
(iii) The developed HMI provides accessibility tools to host applications, such as on-screen keyboard, speech synthesizer/recognition, and map capabilities. The map OSGi service integrated in the platform is powered by openstreetmap.org, whereas the speech synthesizer and recognition is based on the Loquendo API. This is used to give spoken alerts from applications, such as incoming incidences or asynchronous events, and recognize voice interface commands, in order to avoid distractions.

As observed in Figure 5(a), the main window of the HMI interface is divided into three key areas. First, the upper bar includes general functions, such as the name of the active application, the status of the voice synthesizer and recognition, or basic functions for controlling the host. The second main part on the interface contains the icons of the installed applications. In this case a couple of tools for the user are showed, although other applications are installed for speed limit, router planning, or incidence notifications. The on-screen keyboard is also available in a button placed on the lower right part of the window.

Figure 5(b) shows the HMI interface when the application called "Integrated Services" is active. This application integrates a unique map view with information coming from incidence-based services that are subscribed. As can be seen, the HMI capabilities enable the integration of applications in a friendly and nondistractive way, showing a map with all notifications that are notified by the voice synthesizer facility.

7. Evaluation Experience

Although the usefulness of the vehicular networking platform has been validated at service level through a proper HMI and several reference applications, which have been presented in previous Section 6, an analysis of the low-level operation of the network is also necessary to test the correct operation of



(a) Main view (b) Service operating in the map view

FIGURE 5: Screenshots of the HMI and applications running on the top of the communications stack.

the essential platform modules. For this reason, a reference network testbed has been developed in Walkie-Talkie following the scheme provided in Figure 1 and using an implementation of the communication stack shown in Figure 2. For the moment, only V2I communications have been experimentally tested, since this type of communications is essential for accessing infrastructure services (like Internet), and, consequently, it is found to be of paramount importance in the short-term deployment of vehicular networks on real roads. Nevertheless, as explained in the conclusion section, the experimental evaluation of the V2V communication model proposed in this paper (described in Section 5) is an important future work item in Walkie-Talkie.

7.1. Testbed Setup. The set-up scenario consists of one vehicle (integrated by a host and an MR), one roadside station (AR), and the home central ITS station for the vehicle (divided into an HA and an IMS server). The hardware equipment and associated software used for each node can be found in Table 1. The testbed has been deployed at the University of Murcia, near the Faculty of Computer Engineering and taking advantage of the ring road that surrounds the campus. The MR is provided with three different types of communication interfaces. On the one hand, the MR can communicate with roadside units using 802.11b/g/n or 802.11p technologies. On the other hand, the MR can directly communicate with the central ITS through the 3G/UMTS network.

During the implementation and setup of the testbed we faced some technical problems. The first problem we encountered was caused by the use of IPv6 communications. Since the network infrastructure available at the University of Murcia natively supports IPv6, we could easily support IPv6 communications with roadside units through the 802.11b/g/n and 802.11p communication interfaces. Nevertheless, most of the 3G providers (including the used one) still offer IPv4 Internet. Therefore, to enable an IPv6 access to the central station through the 3G interface, we need to employ an IPv4 to IPv6 transition solution. In particular, we used the *OpenVPN* tool between the MR and the node acting as HA within the central ITS station.

Another notorious challenge is related to the securitization of the network mobility operation. The IPsec security associations (SAs) to protect mobility traffic (e.g., *Binding Update* and *Binding Ack* messages) should be established using the address assigned within the home domain, that is, the home address (HoA). This is necessary to allow these associations to survive upon a possible change of the locally assigned care-of address (CoA) when the MR performs a handoff. However, the IKEv2 SAs, which are used internally by the IKEv2 protocol to protect the IPsec association establishments, are created using CoAs as endpoint. Therefore, each time a handover occurs, IKEv2 SAs need to be re-established with the new CoA. To avoid this inefficiency, NEMO and IKEv2 need to cooperate to allow IKEv2 SAs to be simply updated with the new configured CoAs [25] and avoid the costly SA renegotiation process. Given that current software implementations lack such interoperation, we have developed an interprocess communication between NEMO and IKEv2 daemons to allow the former to keep the latter informed about new configured CoAs.

Finally, regarding the configuration of 802.11p equipment, we experimented the restrictive line-of-sight requirements of this communication technology that operates in the 5 GHz frequency band. In fact, this requirement provoked us to install the AR on edge of the building roof and opted by using a two-storey building in order to improve the communication when vehicles circulate under the AR coverage area.

7.2. Analysis of Results. The developed testbed has been used to evaluate the network operation using 3G (UMTS) and 802.11p wireless technologies. Global reachability of the in-vehicle network is achieved by using NEMO, whose operations are protected using IPsec and IKEv2 protocols. It is worth mentioning that MCoA extensions have been disabled in order to better appreciate the performance degradation caused by the handover. The roadside unit is connected on the top of the Faculty of Computer Science, and it has been installed to only give 802.11p coverage to a small stretch of a near road. A common vehicle mounting the on-board equipment is driven around the building at an urban-like speed between 20 and 40 km/h. When the vehicle is under the coverage area of the roadside unit, the MR automatically performs a handoff from 3G to 802.11p. In these tests the network bandwidth (measured in Mbps) through a TCP flow maintained at the maximum allowable speed from the vehicle host to a CN connected within the central ITS station network. This traffic flow has been generated with the Iperf utility (http://sourceforge.net/projects/iperf/) (version 2.0.4).

Table 1: List of hardware equipment.

Networked nodes		
Node	Model	Features
Vehicle host	PC Viliv X70	Atom 1.3 Ghz/1 GB, Windows 7
Mobile router	Laguna	ARM11/128 MB, Linux OpenWrt
Access router	Laguna	ARM11/128 MB, Linux OpenWrt
Home agent	mini-ITX PC	Via 532 Mhz/476 MB, Ubuntu 10.4
IMS server × 4	Xen VM	P-4 D 2 Ghz/256 MB, Ubuntu 10.4
Network interfaces		
Technology	Hardware	
3G/UMTS	Ovation MC950D modem	
802.11p	Unex DCMA-86P2 mini-PCI (AR and MR)	
Relevant software		
Node	Description	
Mobile router	NEMO (UMIP 0.4), IKEv2 (OpenIKEv2 0.96)	
Home agent	NEMO (UMIP 0.4) and IKEv2 (OpenIKEv2 0.96)	
IMS server	Fraunhofer Open IMS and Kamailio 3.1.2	

The period of RA notifications from the AR is set to a random time between three and four seconds (to avoid RA collisions with possible nearby ARs). Additionally, the expiration time of the pair CoA-HoA used is set to 30 seconds in both the MR and the HA.

The results obtained are shown in Figure 6. As can be seen, the slow-start algorithm of TCP tries to adapt to the wireless medium during the whole test, affected by the mobility of the vehicle. The first handoff from 3G to 802.11p occurs at time 310 s (see Figure 6(b)) and the second one, from 802.11p to 3G, at time 445 s (see Figure 6(c)). At these moments the data rate is null for a while, due to the time needed to change the CoA used against the HA. Nevertheless, the connectivity gap is more evident in the second handoff, because 802.11p technology is preferred when both 3G and 802.11p technologies are present. The handover mechanism waits for a Router Advertisement received through the 802.11p interface, but, if it is not received, the CoA-HoA association timeout indicates that the 802.11p connectivity is over and the handoff to the 3G technology must be performed. Moreover, we can appreciate the quite better performance obtained while the 802.11p link is maintained, with peaks near to 6 Mbps. Between times around 100 and 200 s the high speed packet access (HSPA) channel allocation algorithm adapts better, since the vehicle moves near the UMTS base station. It can be noted that the performance of the 3G link is similar at the beginning and the end of each test because the circuit is circular.

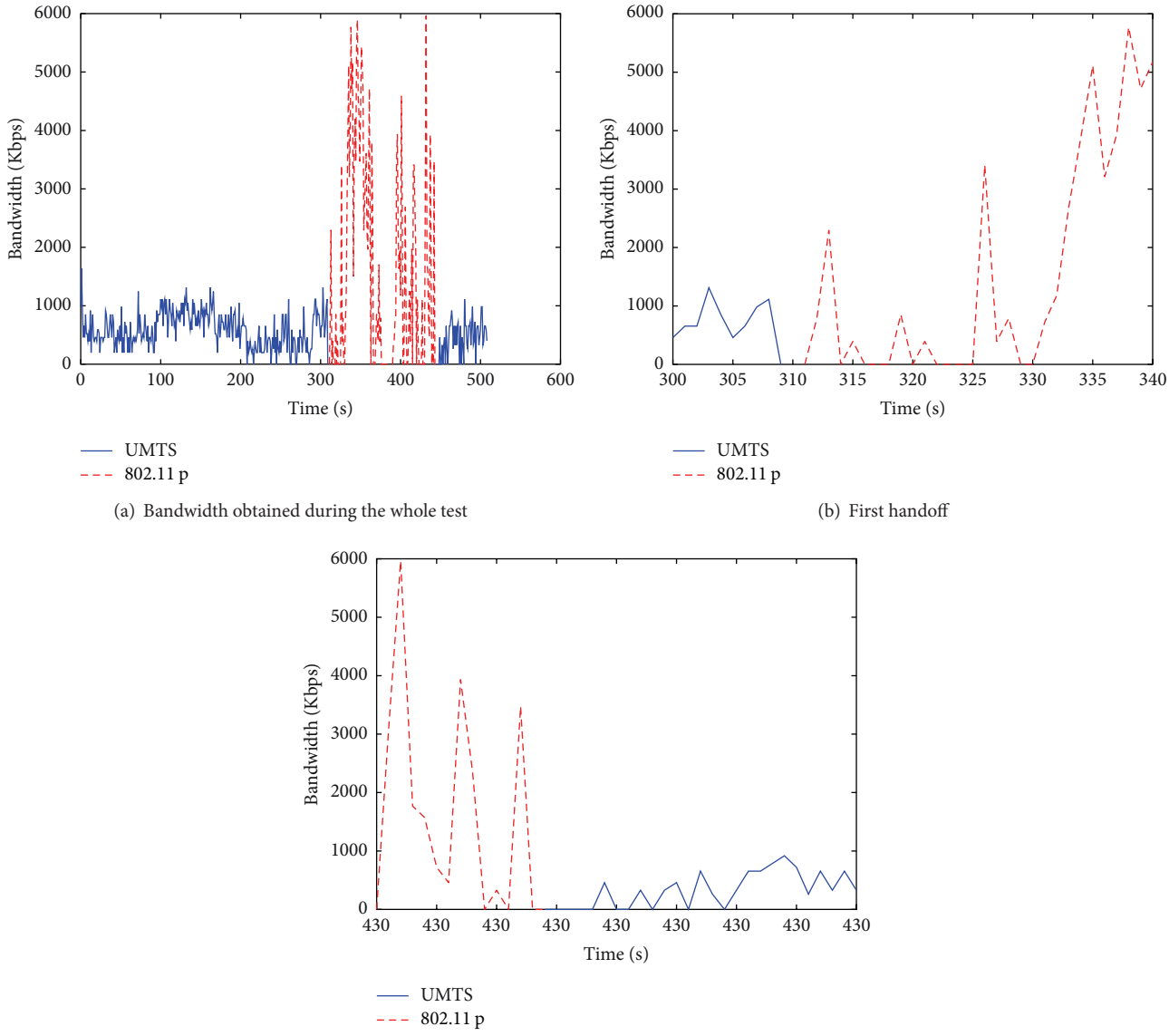
Considering the final results, we can confirm that network mobility and security modules perform efficiently under a real intertechnology handoff, the most difficult to accomplish. The communication stack operates correctly, maintaining the in-vehicle network connectivity and showing good performance results. Unless high-quality multimedia transmissions are required, the bandwidth results indicate that the data rate required by most of the traffic efficiency and comfort cooperative services can be covered.

8. Conclusion

This paper proposes a complete vehicular network framework where all the essential nodes in the vehicle, roadside, and central infrastructure have been designed, both in terms of the network architecture and the communications stack for each node type. Notice that both V2I and V2V communications are considered, maintaining IPv6 networking as the lowest common denominator. While V2I communications are based on IPv6 network mobility through NEMO/MCoA protocols to maintain the connectivity upon the change of network attachment point by the vehicle mobile router, V2V communications are achieved through a hybrid approach based on intelligent broadcast delivery and delay tolerant networks.

The whole network architecture is complemented with the necessary framework for offering infrastructure-based services to vehicles and deploying in-vehicle applications. IMS and OSGi are used for hosting remote services and managing the lifecycle of local applications on vehicles and roadside units, respectively. The middleware integrated in the facilities layer of the vehicle host and the central station include these capabilities, as well as other applications supporting software, such as a flexible on-board human machine interface for the case of the vehicle host. Moreover, essential modules of the networking platform have been prototyped and tested in a real environment. According to our tests, good performances are achievable in the V2I segment when using multiple communication technologies during vehicle handoffs across roadside access routers.

This work is framed within the Walkie-Talkie project, whose current tasks are now focused on extending the performance assessment of the whole architecture through a set



(a) Bandwidth obtained during the whole test

(b) First handoff

(c) Second handoff

Figure 6: Maximum bandwidth using TCP.

of testing scenarios covering both V2I and V2V. To this aim, the collaborations with the current European projects ITSSv6 (http://www.itssv6.eu/) and FOTsis (http://www.fotsis.com/) are essential. In the short term, the immediate steps of the consortium include the extension of the experimental tested to support the V2V communication proposal. Additionally, further tests are also planned to analyze the network stability in terms of packet losses and the latency of uplink and downlink communication directions. In the long term, future work lines are focused on the contextualization of vehicles and infrastructure nodes for providing extended pervasive services to users and the extension of the platform to cover smart city environments, where additional infrastructure entities will be networked. Here, the synergy among vehicles, road infrastructure, individuals, and buildings will become the key of our future research.

Acknowledgments

This work has been mainly sponsored by the Ministry of Science and Innovation, through the Walkie-Talkie project (TIN2011-27543-C03), and partially by the European Seventh Framework Program, through the ITSSv6 Project (contract 270519), and the Seneca Foundation, by means of the GERM program (04552/GERM/06).

References

[1] C. Pinart, P. Sanz, I. Lequerica, D. Garcia, I. Barona, and D. Sanchez- Aparisi, "DRIVE: a reconfigurable testbed for advanced vehicular services and communications," in *Proceedings of the 4th International Conference on Testbeds and Research Infrastructures for the Development of Networks & Sommunities (TridentCom '08)*, pp. 1–8, 2008.

[2] R. Stahlmann, A. Festag, A. Tomatis, I. Radusch, and F. Fischer, "Starting european field tests for car-2-X communication: the drive C2X framework," in *Proceedings of the 18th ITS World Congress and Exhibition (ITS World Congress '11)*, 2011.

[3] C. Weiß, "V2X communication in Europe: from research projects towards standardization and field testing of vehicle communication technology," *Computer Networks*, vol. 55, no. 14, pp. 3103–3119, 2011.

[4] International Organization for Standardization, "Intelligent transport systems—Communications Access for Land Mobiles (CALM)—IPv6 Networking," ISO, 21210, International Organization for Standardization, January 2011.

[5] M. Tsukada, J. Santa, O. Mehani, Y. Khaled, and T. Ernst, "Design and experimental evaluation of a vehicular network based on NEMO and MANET," *EURASIP Journal on Advances in Signal Processing*, vol. 2010, Article ID 656407, 18 pages, 2010.

[6] H. Hartenstein and K. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Communications Magazine*, vol. 46, no. 6, pp. 164–171, 2008.

[7] F. Li and Y. Wang, "Routing in vehicular ad hoc networks: a survey," *IEEE Vehicular Technology Magazine*, vol. 2, no. 2, pp. 12–22, 2007.

[8] Y.-C. Tseng, S.-Y. Ni, Y.-S. Chen, and J.-P. Sheu, "The broadcast storm problem in a mobile ad hoc network," *Wireless Networks*, vol. 8, no. 2-3, pp. 153–167, 2002.

[9] N. Wisitpongphan, O. K. Tonguz, J. S. Parikh, P. Mudalige, F. Bai, and V. Sadekar, "Broadcast storm mitigation techniques in vehicular ad hoc networks," *IEEE Wireless Communications*, vol. 14, no. 6, pp. 84–94, 2007.

[10] K. Suriyapaibonwattana and C. Pomavalai, "An effective safety alert broadcast algorithm for VANET," in *Proceedings of the International Symposium on Communications and Information Technologies (ISCIT '08)*, pp. 247–250, October 2008.

[11] K. Suriyapaiboonwattana, C. Pornavalai, and G. Chakraborty, "An adaptive alert message dissemination protocol for VANET to improve road safety," in *Proceedings of the IEEE International Conference on Fuzzy Systems*, pp. 1639–1644, August 2009.

[12] M. Slavik and I. Mahgoub, "Stochastic broadcast for VANET," in *Proceedings of the 7th IEEE Consumer Communications and Networking Conference (CCNC '10)*, pp. 1–5, Las Vegas, Nev, USA, January 2010.

[13] Y. Bi, L. X. Cai, X. Shen, and H. Zhao, "A cross layer broadcast protocol for multihop emergency message dissemination in inter-vehicle communication," in *Proceedings of the IEEE International Conference on Communications (ICC '10)*, May 2010.

[14] E. P. C. Jones, L. Li, J. K. Schmidtke, and P. A. S. Ward, "Practical routing in delay-tolerant networks," *IEEE Transactions on Mobile Computing*, vol. 6, no. 8, pp. 943–959, 2007.

[15] A. Vahdat and D. Becker, "Epidemic routing for partially-connected ad hoc networks," Tech. Rep., Duke University, 2000.

[16] E. P. C. Jones, L. Li, and P. A. S. Ward, "Practical routing in delay-tolerant networks," in *Proceedings of the ACM SIGCOMM workshop on Delay-tolerant networking (WDTN '05)*, pp. 237–243, New York, NY, USA, August 2005.

[17] T. Kosch, I. Kulp, M. Bechler, M. Strassberger, B. Weyl, and R. Lasowski, "Communication architecture for cooperative systems in Europe," *IEEE Communications Magazine*, vol. 47, no. 5, pp. 116–125, 2009.

[18] International Organization for Standardization, "Intelligent transport systems—Communications Access for Land Mobiles (CALM)—architecture," ISO, 21217, International Organization for Standardization, April 2010.

[19] European Telecommunications Standards Institute, "Intelligent Transport Systems (ITS), (Communications Architecture)—Architecture," ETSI EN 302 665, European Telecommunications Standards Institute, September 2010.

[20] S. Thomson, T. Narten, and T. Jinmei, "IPv6 stateless address autoconfiguration," RFC, 4862 (Draft Standard), Internet Engineering Task Force, 2007, http://www.ietf.org/rfc/rfc4862.txt.

[21] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," RFC,3315 (Proposed Standard), Internet Engineering Task Force, updated by RFCs 4361,5494, 2003, http://www.ietf.org/rfc/rfc3315.txt.

[22] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)," RFC, 4861 (Draft Standard), 2007, http://www.ietf.org/rfc/rfc4861.txt.

[23] A. Conta, S. Deering, and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification," RFC, 4443 (Draft Standard), Internet Engineering Task Force, 2006, http://www.ietf.org/rfc/rfc4443.txt.

[24] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network Mobility (NEMO) basic support protocol," RFC,3963 (Proposed Standard), 2005, http://www.ietf.org/rfc/rfc3963.txt.

[25] R. Wakikawa, V. Devarapalli, G. Tsirtsis, T. Ernst, and K. Nagami, "Multiple care-of addresses registration," RFC, 5648 (Proposed Standard), Internet Engineering Task Force, 2009, http://www.ietf.org/rfc/rfc5648.txt.

[26] V. Devarapalli and F. Dupont, "Mobile IPv6 operation with IKEv2 and the revised IPsec architecture," RFC, 4877, Internet Engineering Task Force, 2007, http://tools.ietf.org/html/rfc4877.

[27] C. Kauffman, "Internet Key Exchange (IKEv2) Protocol," iETF RFC 4306, 2005.

[28] M. Fogue, P. Garrido, F. Martinez, J. C. Cano, C. T. Calafate, and P. Man- zoni, "Evaluating the impact of a novel message dissemination scheme for vehicular networks using real maps," *Transportation Research Part C*, vol. 25, pp. 61–80, 2012.

[29] P. Costa, D. Frey, M. Migliavacca, and L. Mottola, "Towards lightweight information dissemination in inter-vehicular networks," in *Proceedings of the 3rd ACM International Workshop on Vehicular Ad Hoc Networks (VANET '06)*, pp. 20–29, New York, NY, USA, September 2006.

[30] W. Viriyasitavat, F. Bai, and O. K. Tonguz, "UV-CAST: an urban vehicular broadcast protocol," in *Proceedings of the IEEE Vehicular Networking Conference (VNC '10)*, pp. 25–32, Amsterdam, The Netherlands, December 2010.

[31] S. Martinez, C. Calafate, J. Cano, and P. Manzoni, "A map-based sensor data delivery protocol for vehicular network," in *Proceedings of the 11th Annual Mediterranean Ad Hoc Networking Workshop (MedHocNet '12)*, pp. 1–8, Ayia Napa, Cyprus, 2012.

[32] L. Foschini, T. Taleb, A. Corradi, and D. Bottazzi, "M2M-based metropolitan platform for IMS-enabled road traffic management in IoT," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 50–57, 2011.

[33] A. Amditis, L. Andreone, K. Pagle et al., "Towards the automotive HMI of the future: overview of the AIDE—Integrated project results," *IEEE Transactions on Intelligent Transportation Systems*, vol. 11, no. 3, pp. 567–578, 2010.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 686713, 14 pages
http://dx.doi.org/10.1155/2013/686713

Research Article

R-MAC: Risk-Aware Dynamic MAC Protocol for Vehicular Cooperative Collision Avoidance System

Weijie Guo,[1,2] Liusheng Huang,[1,2] Long Chen,[1,2] Hongli Xu,[1,2] and Chenglin Miao[1,2]

[1] *School of Computer Science and Technology, University of Science and Technology of China, Hefei, Anhui 230027, China*
[2] *Suzhou Institute for Advanced Study, University of Science and Technology of China, Suzhou, Jiangsu 215123, China*

Correspondence should be addressed to Weijie Guo; ustcer86@mail.ustc.edu.cn

Received 28 February 2013; Accepted 27 April 2013

Academic Editor: Shukui Zhang

The key for cooperative collision avoidance (CCA) systems is the real-time and reliable delivery of safety-related messages among vehicles, which include periodical beacons and risk-triggered warning messages. In this paper, we first design a risk-aware dynamic medium-access control (R-MAC) protocol tailored for vehicular CCA applications. In this protocol, each frame is divided into two parts: TDMA segment for transferring beacons and CSMA segment for delivering warning messages. Then, we propose a stochastic model to predict the average total number of potential collisions in a platoon of vehicles, which determines the size of CSMA segment in the R-MAC protocol meticulously. Monte Carlo simulations validate that our model is reliable and practical. The performance of the R-MAC protocol is verified through theoretical analysis and extensive simulations under different traffic scenes. Simulation results show that R-MAC outperforms the traditional IEEE 802.11p protocol in terms of packets delivery rate and transmission delay, as well as the Jain's fairness index of the medium access between beacons and warning messages.

1. Introduction

As a potential technology for intelligent transportation system, vehicular ad hoc network (VANET) has received considerable attention by academic communities and major car manufactures around the world. The Federal Communications Commission (FCC) has allocated a dedicated 75 MHz spectrum for vehicular applications in 1999 [1], and some important projects (e.g., Advanced Driver Assistance Systems (ADASE2) [2], CarTALK2000 [3]) have been launched subsequently. Through wireless vehicle-to-vehicle and vehicle-to-roadside communications, VANET can provide various safety-related services. As a typical representation, cooperative collision avoidance (CCA) systems have greatly evolved in the past years [4, 5], which helps to reduce the probability of vehicular collisions and the corresponding damage significantly. Within a CCA system, when a vehicle in the platoon encounters an obstacle or collision, a warning message will be broadcast backwards to the following vehicles. Upon receiving a warning message, the following drivers will promptly brake instead of reacting to the brake light ahead immediately in tradition, which saves a lot of time before the following drivers are aware of the accidents in the front [6].

In this paper, we study efficient and fair delivery of different messages in the considered scenario of CCA systems, where many vehicles form a platoon (or a chain) moving along the same road toward the same direction. Within this system, there are mainly two kinds of messages: beacons and warning messages. Beacons are disseminated among vehicles periodically to inform neighbors about their movement states, such as speed, acceleration, and direction. Warning messages are triggered by a specific vehicle which experiences a hazard or collisions and are propagated from the source to following vehicles as far as possible to inform them of the accidental situation. As a result, such messages have a higher priority [7] compared with beacons. One key for a CCA system is the real-time and reliable delivery of warning messages as well as beacons. In traditional CCA applications [4, 5], some simple approaches are employed to deliver messages, which may lead to several problems in an emergent situation. First, message collisions are more likely to occur with the increasing number of vehicles in the platoon due to

a large number of redundant warning messages pertaining to the same emergent event, which results in a serious message-delivery latency and packets loss. Then, the overemphasis on the higher delivery priority of warning messages makes the beacons lose the chance of medium access, especially in the IEEE 802.11p protocol which is based CSMA/CA mechanism. In addition, vehicles will become blind to others without knowledge of their latest movement states, which, in turn, may cause more accidental collisions among the platoon. To overcome these shortcomings, we design a risk-aware dynamic medium access control (R-MAC) protocol tailored for vehicular CCA systems, which makes a good tradeoff between efficient delivery and fairness of messages with different priorities.

To this end, our protocol is based on traditional TDMA mechanism, in which time is divided into periods called frames and each frame can be subdivided into tiny time slots uniformly. However, each frame in R-MAC includes two parts: CSMA segment for sending warning messages and TDMA segment for beacon transmission. In order to ensure the higher transfer priority of warning messages, we allocate slots to CSMA segment prior to TDMA segment in each frame. The number of slots reserved for CSMA segment is determined by the average total number of potential vehicle collisions among the platoon in the next few frames, which can be computed though a stochastic collision prediction model. After allocation for CSMA segment, the left slots fall into the TDMA segment. In this way, both efficiency and fairness of the medium access between the above two kinds of messages can be achieved in R-MAC. In addition, with the rapid spread of 3G and WIFI in recent years, the V2I communications has been feasible. In this paper, the prediction process of average total number of potential collisions operates on a roadside unit (RSU), such as 3G stations, WIFI hot spots.

The main contributions of the paper are listed below.

(1) Considering the efficiency and fairness of delivering beacons and warning messages on the medium access, we design a risk-aware dynamic (R-MAC) protocol tailored for vehicular CCA systems, which is based on a dynamic TDMA mechanism.

(2) Since the size of CSMA segment in each frame is determined by the average total number of potential collisions among the platoon in the next few frames, a stochastic collision prediction model is presented, which is based on minimum safety distance and a homogeneous Markov chain.

(3) Moreover, extensive simulations under various traffic loads show that R-MAC outperforms the traditional IEEE 802.11p protocol in terms of packet delivery rate and transmission delay, as well as the Jain's fairness index of the medium access between beacons and warning messages.

The remainder of this paper is organized as follows. In Section 2, we briefly review the related work on MAC protocols and vehicle collision models in VANET. Section 3 delineates the operation of the R-MAC protocol in detail. In order to compute the average total number of potential collisions used in R-MAC, the derivation of a stochastic collisions prediction model is introduced in Section 4. The performance of R-MAC is evaluated in different setups in Section 5, which also provides an in-depth analysis of the simulation results. We conclude the paper in Section 6.

2. Related Work

In recent years, various MAC protocols have been proposed to guarantee the real-time and reliable communications in VANET. These protocols are mainly based on two approaches: Carrier Sense Multiple Access (CSMA) and time division multiple access (TDMA). However, most of them cannot be applicable well to the vehicular scenarios with high mobility and fast changing topology.

The TDMA approach operates in a time slotted structure, where time slots are grouped into frames. Due to the collision-free nature of TDMA, it has been widely adopted and become the foundation of several TDMA based protocols [8, 9] in vehicular network. R-ALOHA [10] is the earliest dynamic channel reservation scheme, which enables nodes to reserve a time slot for transmission in a fixed period. RR-ALOHA [11] and ADHOC-MAC [12] are completely distributed TDMA schemes, but both of them are based on the assumption that the network topology stays static. Simulation results show that the throughput reduction of ADHOC MAC protocol can reach up to 30% for an average vehicle speed of 50 km/h [13]. Lam and Kumar designed a DCR protocol with the help of GPS in [14]. However, his work is not suitable for heavy traffic situations. Omar et al. [15] proposed a TDMA-based MAC protocol for reliable broadcast in VANET. This scheme reduces transmission collisions caused by vehicle mobility, but it assumed that there were two transceivers on each vehicle, one used for control channel and the other for service channel.

In CSMA-like random schemes, the prime example is IEEE 802.11 [16], which is a simple, flexible, and contention-based medium access control protocol. In the protocol, when a vehicle wants to transmit messages, it first listens to the desired channel. If the channel is free (not occupied by other vehicles), the vehicle is allowed to transmit. Otherwise, the vehicle has to defer its transmission to the next contention period. Although the approach is simple and flexible, the data delivery delay will increase significantly if the vehicles density is high, especially when an exponential back-off mechanism is employed to resolve the robust contention issues among different vehicles [16]. In order to be delivered timely, warning (emergency) message is assigned a higher priority to contend for the wireless channel with a small contention window size in the IEEE 802.11 p EDCA [17]. Although the small contention window size allows the warning message to be transmitted with a small delay, it introduces the unfairness between warning messages and beacons (with a lower priority than warning message) on the medium access and the delivery delay of beacons is increased greatly. Another limitation for CSMA schemes is that no RTS/CTS exchange is used, which results in a serious hidden terminal problem and

reduces packets delivery rate. Consequently, the effectiveness of CCA applications decreases substantially.

However, to the best of our knowledge, little effort has been devoted to design risk-aware MAC protocol by exploiting reliable and practical vehicle collision models. Detailed models of vehicle motion and collision dynamics were given in [18, 19], but they are completely based on deterministic equations for the occurrence of collisions, whereas in fact, randomness is always present introduced by high mobility and driver behavior. In [20], the authors explored the necessary conditions for chain collisions. However, it is assumed that all the vehicles have the same initial speeds and intervehicle distance. A more recent work [21] derived a stochastic model for the number of accidents in the platoon of vehicles equipped with a warning messages communication system. Nevertheless, all the parameters in the model were described by random variables, which cannot give a reliable collision prediction for the real-time traffic scenario. Thus, based on the analysis method in [21], we derive a more reliable and practical stochastic collision prediction model, which takes full advantage of the beacons and warning messages.

In this paper, by combing vehicle collisions model with TDMA-based mechanism, we design a risk-aware and dynamic MAC protocol for the considered CCA application. Besides the reliable and real-time delivery of messages, the fairness between beacons and warning messages on the wireless medium access are also achieved.

3. Details of Risk-Aware Dynamic MAC Protocol

This section mainly presents the detailed description of the dynamic and risk-aware MAC protocol, including the considered traffic scenario, specification of frame structure, and slots allocation algorithm for CSMA and TDMA segments. The number of slots in the CSMA segment is determined by the average total number of potential collisions among the platoon and the corresponding computing method based on a stochastic collision prediction model is given in Section 4.

3.1. The Traffic Scenario. Prior to the detailed description of the proposed protocol, it is essential to give an overview of the considered traffic scenario in which our R-MAC operates. As shown in Figure 1, each RSU and all vehicles under its coverage form a vehicular Ad hoc subnet, which is similar to the model proposed in our previous work [22]. For sake of simplicity, we only consider a platoon of vehicles on highway, which travel along the same road towards the similar direction. However, with vehicles moving on roads at high speeds, the number of vehicles N and the corresponding vehicle density ρ_r in a particular subnet are always varying. In this paper, the vehicle density ρ_r is defined as the average number of vehicles per meter, which can be computed by

$$\rho_r = \frac{N}{R}, \tag{1}$$

where R refers to the coverage range of an RSU. As surrounding conditions of an RSU might affect its practical wireless transmission range, an RSU updates its current transmission range t_r in the following manner [16]:

$$t_r = T_{\max} \cdot (1 - \varepsilon), \quad 0 < \varepsilon \le 1, \tag{2}$$

where $T_{\max}$ and ε indicate the maximum wireless transmission range of an RSU and the wireless channel fading conditions at the current position, respectively. If there are many high-rise buildings or the weather is rainy, ε is set as a larger value, vice versa. GPS and sensors deployed on an RSU are used to obtain terrain and meteorological information so that the parameter ε can be appropriately estimated. For simplicity of illustration, R is set as $2t_r$ approximately. In addition, we assume that every RSU can dynamically compute the corresponding vehicle density in its coverage by communications between the vehicles and RSU in a subnet.

3.2. R-MAC Frame Structure. Now, we give the detailed specification of frame in R-MAC, which is a dynamic TDMA protocol. In R-MAC, we divide the time into periods called frames and then each of them is subdivided into tiny time slots uniformly. Every frame is divided into RSU segment and vehicle segment (see Figure 2). The RSU segment is reserved for RSU to disseminate control message and the latter is used for vehicles to transmit beacons and warning messages. In our protocol, the RSU segment always begins from the head of a frame and its size is a constant denoted by α, which means that the length of the vehicle segment is also determined. Based on the different priorities between beacons and warning messages, the vehicle segment is divided into two parts: CSMA segment which is responsible for transmitting warning message in emergency situations and TDMA segment which is in charge of delivering beacons. Without any loss of generality, we introduce β and γ to indicate the corresponding size of CSMA and TDMA segment, respectively.

Based on the above description, we define three sets S_0, S_1, and S_2 as (3), which refer to the slots falling into the RSU, CSMA, and TDMA segments, respectively:

$$\begin{aligned} S_0 &= \{R_i \mid 1 \le i \le \alpha\}, \\ S_1 &= \{C_i \mid 1 \le i \le \beta\}, \\ S_2 &= \{T_i \mid 1 \le i \le \gamma\}, \\ S_0 \cup S_1 \cup S_2 &= Q, \\ S_i \cap S_j &= \varnothing, \quad \forall i, j \in \{0, 1, 2\}, \ i \ne j. \end{aligned} \tag{3}$$

Q means the set of all slots in a whole frame. As illustrated in Figure 2, R_i indicates the yellow slots in RSU segment, C_i refers to the blue slots reserved for CSMA segment, and the white slots allocated to TDMA segment are denoted by T_i. It is worth noting that the corresponding slots of CSMA and TDMA segments are dynamic, which are determined by an RSU according to the real-time collisions situation in the platoon frame by frame. In order to describe the division of a frame into the above three sets intuitively, we introduce "slot

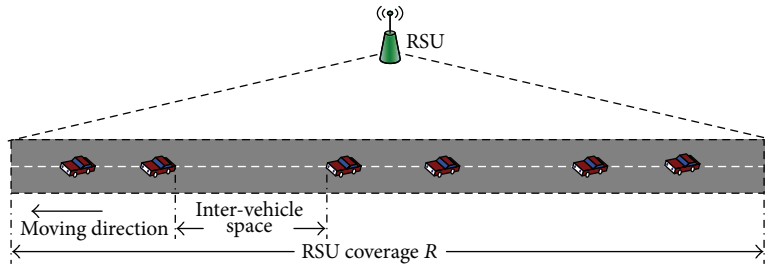


Figure 1: Traffic scenario under consideration.

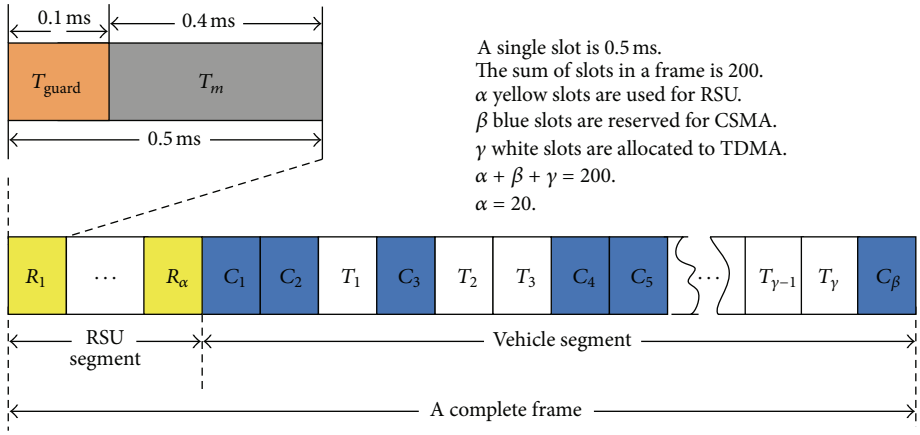


Figure 2: R-MAC frame structure.

assignment map" denoted by a vector state, which marks a slot s as the following rules:

$$\text{State}[s \cdot \text{id}] = \begin{cases} 0, & \text{if } s \in S_0, \\ -1, & \text{if } s \in S_1, \\ \text{ID}, & \text{if } s \in S_2, \end{cases} \tag{4}$$

where ID indicates the id of a particular vehicle, which is a positive integer between 1 and N. With the control messages of an RSU, the slot assignment map is broadcast to vehicles every frame.

Then, we define the time duration parameters according to the US standards within IEEE. The update frequency is $f_p = 10$ Hz. Therefore, the total frame size is 100 ms. The slot time is given by

$$T_{\text{slot}} = \frac{P}{M} + T_{\text{guard}}, \tag{5}$$

where the packet size of message in VANET is $P = 300$ bytes, the data transmission rate is 6 Mbits/s, and the guard time T_{guard} is 100 μs between two adjacent slots [23]. So a single slot reserved for a vehicle is 0.5 ms and the total number φ of available slots in each frame can be given as

$$\alpha + \beta + \gamma = \varphi = 200. \tag{6}$$

In the following, we give more detailed specifications for RSU and vehicle segments, separately.

3.2.1. Specification of RSU Segment. As shown in Figure 2, the number of slots reserved for an RSU is fixed and the size of set S_0 is 20. Moreover, twenty consecutive slots at the beginning of a frame are allocated to an RSU, and the total time T_{rsu} reaches up to 10 ms. According to slot assignment map, we set the variable State$[i] = 0$, $1 \le i \le 20$. Similar to (5), the maximum packet size of an RSU control message can be given by

$$S_{\text{control}} = \frac{1}{8}\left(T_{\text{rsu}} - \alpha \cdot T_{\text{guard}}\right) \cdot M, \tag{7}$$

where α is the size of the set S_0. Obviously, the size of an RSU control packet S_{control} can reach up to 6 Mbytes which are enough to transmit the control message for a whole frame [23]. In our R-MAC, the control message mainly consists of the slot allocation map in every frame.

3.2.2. Specification of Vehicle Segment. In contrast to the RSU segment, the vehicle segment of a frame is further divided into CSMA segment and TDMA segment. For the TDMA segment, a vehicle with a chosen slot will send beacon which contains safety-related information to vehicles around it and the corresponding RSU. However, for the CSMA slots, only delivery of warning (emergency) messages is allowed to contend the medium access in CSMA mode. When a vehicle desires to send a warning message, it first listens to the channel and waits for the CSMA slots. If the medium is idle, the vehicle is allowed to transmit. If the medium is busy, the vehicle will defer its transmission to the next

CSMA slot, which is different from the exponential back-off mechanism executed in IEEE 802.11 MAC protocol [16]. In order to ensure sufficient slots for vehicles to sending warning messages, the size of CSMA segment is set as the average total number of potential collisions among the platoon in the next several frames. In our protocol, TDMA and CSMA segments coexist in each frame dynamically, which helps to achieve the delivery fairness between beacons and warning messages. In the worst case, all the slots of a frame are allocated for CSMA segment to transmit the massive amounts of warning messages and no slots are left for beacons, in which our protocol operates as a traditional CSMA-based MAC protocol just like IEEE 802.11p. Indeed, once the case above appears, the traffic accident must be disastrous and the whole network has to be flooded by massive of emergency messages. However, the probability of this case is little and both of beacons and warning messages have corresponding slots reserved to be transmitted for most case.

3.3. Slot Allocation Algorithm for CSMA and TDMA (SACT). In this section, we describe how to allocate slots for CSMA and TDMA segments. The whole slot allocation algorithm abbreviated as SACT includes three steps: slot allocation for CSMA, slot reservation for TDMA and slot allocation map broadcast. In consideration of the higher priority of delivering warning messages triggered by vehicle collisions, we allocate slots to CSMA segment prior to TDMA segment. For ease of description, we assume that each slot in a frame will be labeled with a number from 1 for the first slot to φ for the last one consecutively, which is called the id of each slot.

3.3.1. Slot Allocation for CSMA. The slot set of CAMS segment S_1 is determined by the following two steps. (i) The RSU analyzes the risk of collision and computes the average total number of potential collision $\mathrm{NUM}_{\mathrm{acc}}$ among the vehicles under its coverage. The detailed computation for $\mathrm{NUM}_{\mathrm{acc}}$ will be given in Section 4, which is another important contribution of this paper. (ii) The RSU selects $\mathrm{NUM}_{\mathrm{acc}}$ appropriate slots from the vehicle segment for delivering warning messages in the mode of CSM A, whose ids are between $\alpha+1$ and φ. Obviously, there are $\binom{\mathrm{NUM}_{\mathrm{acc}}}{\varphi-\alpha}$ selections for the set S_1. Since the generation of warning messages is random absolutely, it is hard to make the optimal selection for S_1. For simplicity, we assure that the ids of $\mathrm{NUM}_{\mathrm{acc}}$ slots are uniformly distributed between $\alpha+1$ and φ. Once $\mathrm{NUM}_{\mathrm{acc}}$ available slots are determined, all of them are marked as occupied by CSMA segment and pushed into the set S_1. Moreover, the slots are denoted by C_i, where the value of i is from 1 to α consecutively. According (4), we set the variable $\mathrm{State}[C_i \cdot \mathrm{id}] = -1$, $1 \le i \le \beta$. So the slot allocation map of CSMA segment is finished here.

3.3.2. Slot Allocation for TDMA. Once the slot set S_1 has been determined, the left slots in vehicle segment will be used for TDMA, all of which fall into the corresponding slot set S_2 uniquely. For ease of description, the size of set S_2 is denoted by γ. T_i indicates the slots in the set S_2, where $1 \le i \le \gamma$. Then, a RSU allocates a particular slot T_i to a vehicle in its coverage,

SACT Algorithm:
Begin: $S_1 = S_2 = \varnothing$
Step 1: Slot Allocation for CSMA
Compute the average total number $\mathrm{NUM}_{\mathrm{acc}}$ of potential collisions among the vehicles platoon by Algorithm 2;
Select $\mathrm{NUM}_{\mathrm{acc}}$ integers from $[\gamma+1,\ \varphi]$ uniformly.
Push the slots whose id equals to the above selected $\mathrm{NUM}_{\mathrm{acc}}$ integers into set S_1, denoted by $C_1, C_2, \ldots, C_\alpha$,
$\alpha = \mathrm{NUM}_{\mathrm{acc}}$;
For $i = 1$ to α
State$[C_i \cdot \mathrm{id}] = -1$
Step 2: Slot Reservation for TDMA
$S_2 = Q - S_0 - S_1$, $\overline{S_2} = \varnothing$,
For each vehicle in the coverage of a RSU
If the RSU received a beacon in the last three Frame
Then select a slot s from set S_2 randomly,
remove s from S_2 and add it to $\overline{S_2}$,
State$[s \cdot \mathrm{id}]$ = vehicle.ID;
Else remove the vehicle from the vehicle list under its coverage;
Step 3: Broadcasting the slot allocation map
The RSU broadcast the vector State$[i]$, $1 \le i \le \varphi$ to all the vehicles

Algorithm 1: Formal description of the SACT Algorithm.

as the following steps. (i) If there are beacons received from a vehicle in the last frame, the RSU will select a available slot s randomly from set S_2 for the vehicle and attach the vehicle ID to it, namely, $\mathrm{State}[s \cdot \mathrm{id}] = \mathrm{vehicle} \cdot \mathrm{ID}$, which marks s as occupied by a particular vehicle. Moreover, once T_i has been occupied by a vehicle, it will be removed from S_2 to the set $\overline{S_2}$. Obviously, the sizes of the two sets meet the following equation:

$$\left|S_2\right| + \left|\overline{S_2}\right| = \gamma. \tag{8}$$

(ii) In a case of an anomaly, in which a vehicle fails to send its beacons in the last consecutive three frames, the RSU will believe the vehicle has moved out of its coverage and no slots will be allocated to it in the next frame. According to these rules, RSU is able to complete the corresponding slot allocation map of TDMA segment.

In fact, the slot allocation procedure, including CSMA segment selection and TDMA slot allocation, is conducted on a particular RSU. Then, the RSU broadcasts the final slot allocation map to all vehicles moving under its coverage. Based on the above description, the integrated SACT algorithm is formally described in Algorithm 1.

4. Computation of the Size of CSMA Segment

As described in the SACT algorithm in Section 3, the corresponding size of CSMA segment in a frame is determined by the average total number of potential collisions $\mathrm{NUM}_{\mathrm{acc}}$ among the platoon in the following several frames, which is the focus of R-MAC. Therefore, in this section, we give a novel computation method of total average number of

potential accidents among the platoon (CMAA) as follows. First, a stochastic collision prediction model is introduced to compute the parameter $\mathrm{NUM}_{\mathrm{acc}}$ in the platoon, and then the probability of collision between adjacent vehicles is derived, which is an input parameter in the prediction model. Moreover, extensive Monte Carlo simulations are conducted to verify the performance of the stochastic model in the end.

4.1. Stochastic Collision Prediction Model. Prior to a detailed description of the envisioned stochastic collision prediction model, we point out a number of assumptions regarding the considered traffic scenario in this paper, which are listed as follows.

(i) The distance between two neighboring vehicles, named intervehicle space, is a random variable. Moreover, it is an exponentially distributed random variable with parameter λ, which represents the density of vehicles on the road and equals to ρ_r computed by (1).

(ii) Each vehicle is capable of estimating its motion state accurately, including velocity, regular acceleration.

The first assumption is based on the fact that interspace calculated by real-time coordinates on map benefit from GPS and GIS is not accurate and reliable, because the positioning precision of GPS hardly meets the need of the considered scenario. In the worse case, a vehicle is evolving into more critical areas; there may be certain undesired problems in the availability of GPS in certain scenarios where GPS signals may not be detected (e.g., such as inside tunnels and underground parking). Moreover, it has been shown that exponential distribution describes well the intervehicles space when traffic densities are small [24]. In addition, it is easy to get accurate velocity and acceleration of a vehicle, via adequately deployed sensor monitoring the motion state of a vehicle in real-time.

The collision scenario considered in our paper is a platoon (or a chain) of N vehicles traveling along the same road toward the same direction. As a vehicle V_a among the vehicle platoon collides with an obstacle or the preceding vehicle on the road, at time $t_0 = 0$, it immediately sends a warning message to the following vehicle V_j, $j \in a+1, \ldots, N$. Upon receiving the warning message, all the following vehicles start to brake at the maximum deceleration. That is, after a time lapse t_{res}. Let us remark here that the time lapse t_{res} is mainly determined by the reception delay of the warning message generated by the communication system and the reaction time of the driver, denoted by T_d and T_r, which will be used again is next section. Each warned driver will decelerate immediately, even if the preceding vehicle has not started to decelerate (see Figure 3). For simplicity, we assume every vehicle has the same maximum deceleration $a_{\max}$.

Within this model, the accidental vehicle V_a, $a \in 1, \ldots, N$, may collide with an obstacle and stop suddenly, which only increases the likelihood of a crash for the following vehicles behind the accident spot. Moreover, the final outcome (collision or stop successfully) of a following vehicle depends on the outcome of the preceding vehicles. Therefore, the collision model is based on the construction of the probability graph depicted in Figure 4, the length of which is $N - a + 1$ [21]. We consider an initial state in which no vehicle has collided. Once the danger of collision has been detected at vehicle V_a, the first vehicle in the following chain V_{a+1} (immediately after the accidental one) may collide or stop successfully. Similarly, for each vehicle behind V_{a+1}, there are two possible cases: collision with its preceding vehicle or successful stop. As a result, at the right-most of the probability graph, there are $N - a + 1$ possible final outcomes which represent the number of collided vehicles between 0 and $N - a$. And $c_{m,n}$ represents the state with m collided vehicles and n successfully stopped vehicles (see Figure 4).

The transition probability between two nodes in the graph is the corresponding collision probability between adjacent vehicles in the chain p_j, $j \in a+1, \ldots, N$ (or the complementary: $1 - p_j$), which will be used in the model. The detailed computation method is described in Section 4.2. Next, we should note that every path in the graph from the left source node $c_{0,0}$ to the right-most nodes leads to a possible outcome involving all the following vehicles behind V_a. The probability of the particular path is determined by all the transition probabilities of nodes which belong to the whole path. Noting that there are multiple paths which may lead to the same final outcome (different paths may end at the same node) referring to a right-most node in the probability graph, the probability of a final outcome is the sum of the resulting probabilities of all possible paths ending at it.

To compute the probabilities of the final outcomes, we can construct a Markov chain whose state diagram is based on the previously discussed probability graph. If the following accidental collisions are caused by the vehicle V_a, there are $(N - a + 1)(N - a + 2)/2$ vertices in the probability graph. And a homogeneous Markov chain can be established with a state set $C = (c_{0,0}, c_{1,0}, c_{0,1}, \ldots, c_{N-a,0}, c_{N-a-1,1}, c_{N-a-2,2}, \ldots, c_{1,N-a-1}, c_{0,N-a})$, whose size equals to $(N - a + 1)(N - a + 2)/2$. In addition, the transition matrix $\mathbf{P}$ of the corresponding Markov chain is a square matrix of dimension $(N-a+1)(N-a+2)/2$. It's worth noting that there are at most two other states to reach each state in the state set C, which ensures the matrix $\mathbf{P}$ is sparse. For ease description, a brief example is illustrated in Figure 5, where only two vehicles V_{N-1} and V_N follow with the leading accidental vehicle V_{N-2}.

Then, we compute the probabilities of paths which start from state node $c_{0,0}$ to each of the $N - a + 1$ final states by computing $\mathbf{P}^{N-a}$. In fact, the final outcome probabilities are the last $N - a + 1$ entries of the first row of the matrix $\mathbf{P}^{N-a}$. Let $\sum k$ be the probability sum of all the paths reaching the final outcome states with k collided vehicles in the following vehicles behind V_a, namely, state $c_{k,N-a-k}$. Therefore, $\sum k$ equals to the $((N-a+1)(N-a+2)/2) - k$th entry of the first row in matrix $\mathbf{P}^{N-a}$, which can be given as follows:

$$\sum k = \mathbf{P}^{N-a}\left[1, \frac{(N-a+1)(N-a+2)}{2} - k\right], \quad a \in 1, \ldots, N. \tag{9}$$

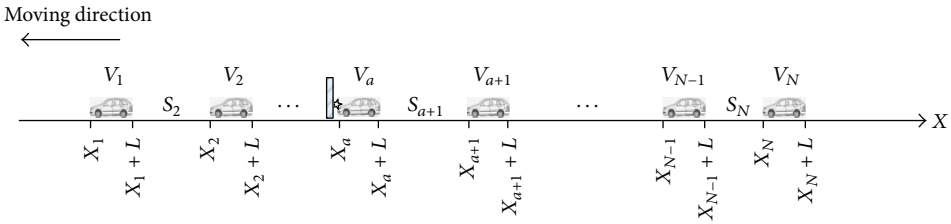


Figure 3: Collision model under consideration.

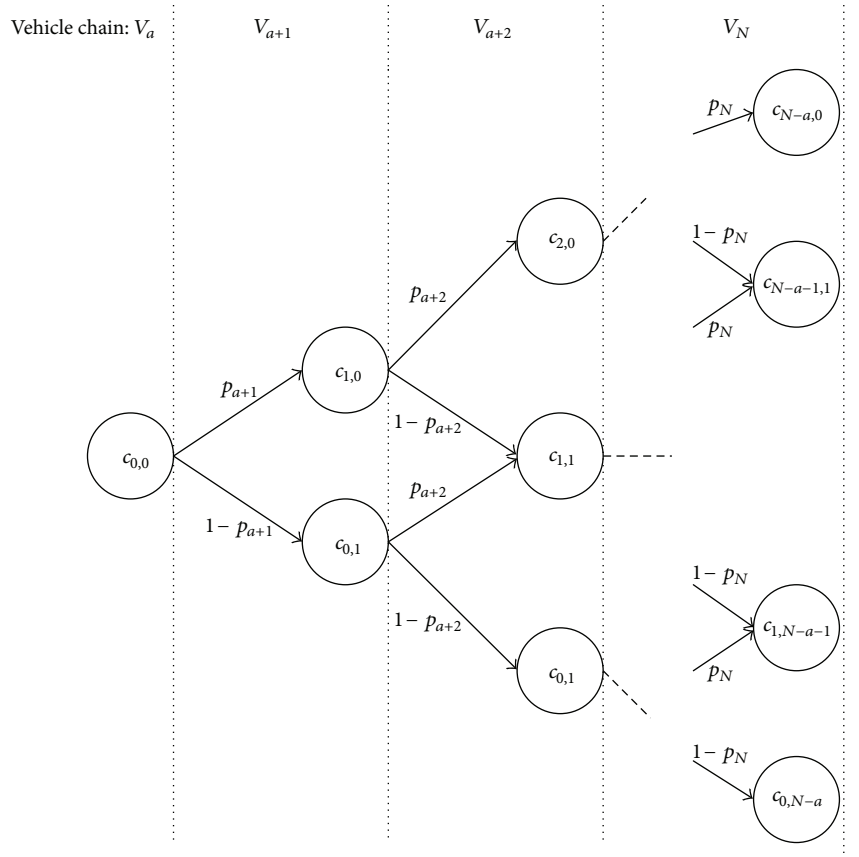


Figure 4: Probability graph defined in the collision model.

Then, the average total number of collisions caused by a particular accidental vehicle V_a in the chain is obtained by the weighted sum as (10):

$$N_{\text{acc}} = \sum_{k=1}^{N-a} k \cdot \sum k, \quad a \in 1, \ldots, N. \tag{10}$$

In order to facilitate statistics, we assume that each vehicle in the platoon has the same probability $1/N$ to be the accidental vehicle. In other words, for the vehicle V_a, the parameter a is a uniformly distributed variable between 1 and N. Therefore, from the perspective of a RSU in the CCA system as described in Section 3, the average total potential collisions NUM_{acc} in the whole platoon can be computed by (11) as follows:

$$\text{NUM}_{\text{acc}} = \frac{1}{N} \sum_{a=1}^{N} \sum_{k=1}^{N-a} k \cdot \sum k, \quad a = 1, 2, 3, \ldots, N. \tag{11}$$

4.2. Compution of the Adjacent Vehicles Collison Probability. In this section, we come to the problem of computing the collision probabilities p_j, $j \in a + 1, \ldots, N$ for adjacent vehicles, which is an important variable used in our stochastic collision prediction model. To the end and for ease of description, we first explore the movement features of vehicles especially when braking, and then a novel method based on minimum safety distance (MSD) is introduced, which takes into full

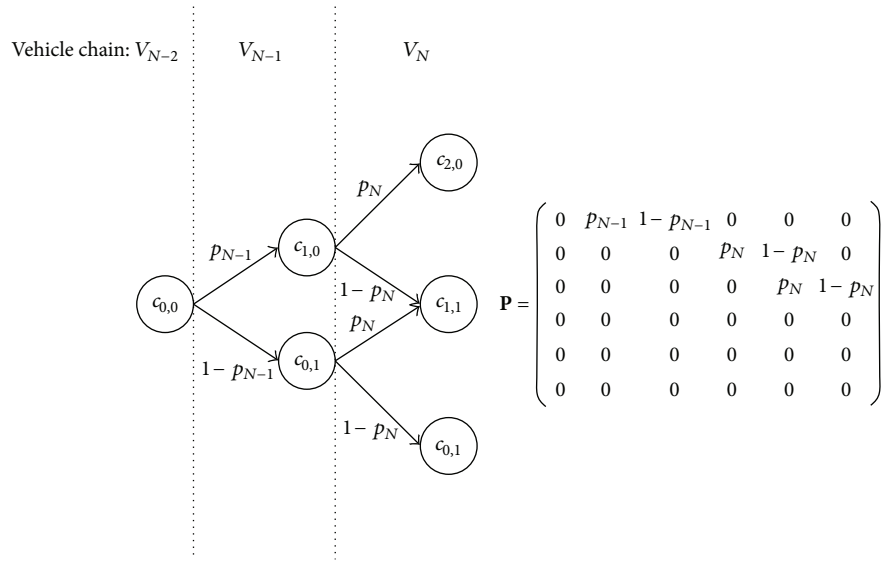


Figure 5: Probability graph and corresponding transition matrix for scenario where the collision is caused by vehicle V_{N-2}.

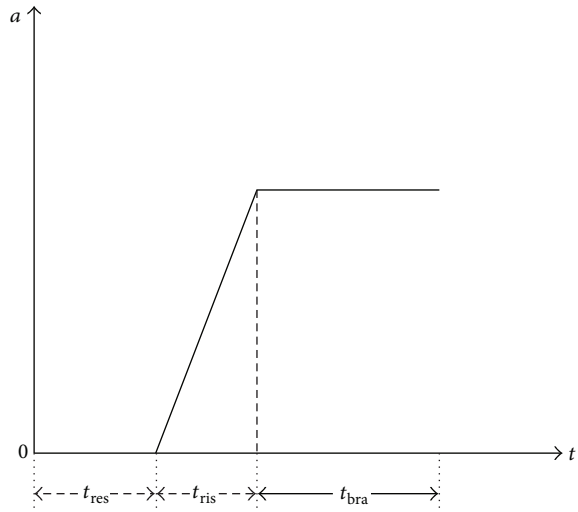


Figure 6: A complete vehicle braking process.

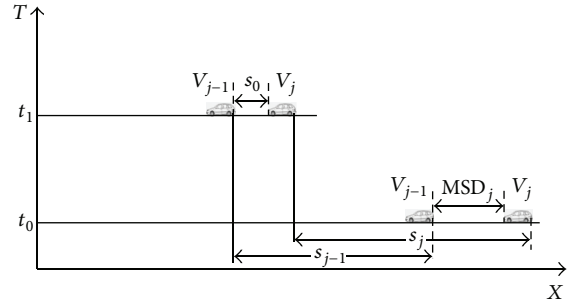


Figure 7: MSD model for vehicles V_j and V_{j-1}.

account of different movement states of adjacent vehicles, to compute collision probabilities p_j.

Based on the analysis of the vehicular moving procedure for vehicle in [20, 25], a complete braking procedure is divided into three different stages where acceleration a of a vehicle varies along with time as shown in Figure 6. As mentioned above in the collision prediction model, we still let V_a denote the accidental vehicle which encounters an obstacle and stops suddenly in the platoon. t_{res} indicates the braking response time from the instant V_a sends warning messages to the instant when the following drivers are aware of the collision ahead. In fact, it is mainly determined by the reception delay of the emergency message generated by the communication system and the reaction time of the driver, denoted by T_d and T_r, respectively. To consider a worse communication system and without loss of generality, we set T_d as 0.1 ms, which is the maximum delay for warning messages that vehicular communication standards specify [26]. Generally, the average reaction time of drivers is set as $T_r = 0.9$ s [6]. As shown in Figure 6, the value of deceleration speed is still rising during the process t_{ris}, which is about 0.1-0.2 s and is overlooked for easy of calculation. During the period of t_{bra}, a vehicle keep its maximum deceleration $a_{\max}$ until collision with the preceding vehicle occurs or stops successfully. Here, for simplicity, we assume that all the following vehicles behind the accidental vehicle V_a has the same braking response time $t_{\text{res}} = T_d + T_r = 0.1 + 0.9 = 1$ s, which is the sum of reception delay of warning messages T_d and the reaction time of drivers T_r. During the period of t_{res}, we assume that a particular vehicle V_j still keeps its original movement state. After t_{res}, its speed will linearly decrease due to the braking operation with the maximum deceleration speed. Then, $v_{0,j}$ and a_j denote the initial velocity and acceleration of a vehicle V_j during the period of t_{res}, respectively. From [4], the movement state during time $(0, t_{\text{res}})$ can be expressed as

$$v_j(t) = v_{0,j} + a_j \cdot t, \quad t < t_{\text{res}}. \tag{12}$$

After the period t_{res}, the vehicle speed is linearly decreasing with the maximum deceleration $a_{\max}$ as following:

$$v_j(t) = v_{0,j} + a_j \cdot t_{\text{res}} - a_{\max}\left(t - t_{\text{res}}\right), \quad t > t_{\text{res}}. \tag{13}$$

In order to compute the collision probabilities p_j, we introduce a Minimum Safety Distance (MSD) model for the vehicles in a platoon. Based on this model, an RSU can compute the accurate minimum safety distance MSD_j for each vehicle V_j in the platoon according to the current movement state, which mainly includes velocity v_j and acceleration a_j. We let d_j denote the distance between a particular vehicle V_j and its preceding vehicle V_{j-1} in the platoon, which is an exponentially distributed random variable with parameter λ as mentioned in assumption (i). It is obvious that if intervehicle distance d_j is greater than or equals to corresponding minimum safety distance MSD_j, the vehicle V_j can stops successfully without collision with its preceding vehicle V_{j-1}. Otherwise, there will be a collision between vehicle V_j and V_{j-1}. So for any vehicle V_j, $a+1 \le j \le N$, the collision probability p_j will be computed as follows:

$$\begin{aligned} \lambda &= \rho_r = \frac{N}{R}, \\ p_j &= P\left(d_j < \text{MSD}_j\right) \\ &= 1 - e^{1-\lambda\cdot\text{MSD}_j}, \quad a+1 \le j \le N. \end{aligned} \tag{14}$$

Based on the aforementioned analysis, we give the MSD computation model as Definition 1.

Definition 1. Minimum safety distance in our work is defined as the needed minimum distance between two adjacent vehicles to avoid collision based on V2V communications, both of which receive a warning message and start to brake hard at the same time.

For simplicity, we assume that all the vehicles have the same mechanical brake performance with a common maximum deceleration value $a_{\max}$. However, the velocity and regular acceleration of vehicles before the time are different with each other, denoted by v_j and a_j, respectively. Without loss of generality, we select a particular vehicle V_j and its preceding vehicle V_{j-1} to describe the minimum safety distance MSD_j (see Figure 7), both of which receive the same warning messages from the front of the platoon at the same time. t_0 indicates the instant a warning message is triggered by a accidental vehicle V_a in the front of the platoon and sent backwards, while t_1 denotes the instant when collision between V_j and V_{j-1} has been successfully avoided. The displacements of V_j and V_{j-1} are denoted by s_j and s_{j-1} during the period between t_0 and t_1, respectively. s_0 refers to the permitted minimum distance between V_j and V_{j-1} at t_1 [4], which can be set an appropriate constant according to different safety requirements in CCA systems. Based on the above analysis, the MSD for vehicle V_j is given as follows:

$$\text{MSD}_j = s_j - s_{j-1} + s_0, \quad j = a+1, \ldots, N. \tag{15}$$

According to the different movement states, we further divide the computation of MSD into three cases as follows. In case 1, the vehicle V_j follows the accidental vehicle V_a immediately, where j equals to $a+1$. Whereas in case 2, j doesn't equal to $a+1$ and the velocity of V_j is greater than that of V_{j-1} before the time t_{bra}. In contrast to case 2, j doesn't equal to $i+1$ either while the velocity of V_j is less than or equals to that of V_{j-1}. Here, we continue to adopt the notations as above: let $v_{0,j-1}$ and $v_{0,j}$ indicate the initial speed of V_{j-1} and V_j, while a_{j-1} and a_j denote the corresponding acceleration/deceleration during the period of t_{res}, respectively.

Corollary 2. *If the vehicle V_j follows the accidental vehicle V_a immediately, the MSD for V_j is*

$$\begin{aligned} \text{MSD}_j = {} & \text{signal}\left(v_{0,j} + a_j \cdot t_{\text{res}}\right) \\ & \cdot \left(v_{0,j} \cdot t_{\text{res}} + \frac{1}{2} a_j \cdot t_{\text{res}}^2 + \frac{\left(v_{0,j} + a_j \cdot t_{\text{res}}\right)^2}{2a_{\max}} \right) \\ & + \text{signal}\left(-\left(v_{0,j} + a_j \cdot t_{\text{res}}\right)\right) \cdot \frac{v_{0,j}^2}{2a_{i+1}} + s_0, \quad j = a+1, \end{aligned} \tag{16}$$

where the signal function signal(x) is defined as follows:

$$\text{signal}(x) = \begin{cases} 0, & \text{if } x < 0, \\ \dfrac{1}{2}, & \text{if } x = 0, \\ 1, & \text{if } x > 0. \end{cases} \tag{17}$$

Proof. Noting that the accidental vehicle V_a encounters an obstacle and stops immediately, its displacement is overlooked ($s_i = 0$). Obviously, the MSD of V_{a+1} is the displacement s_{i+1} of the vehicle V_{a+1} before it stops successfully without collision with its preceding vehicle V_a. Based on the description of braking procedure, there are two parts generally: the reaction time of braking operation and the linearly decreasing stage. During the period of braking reaction stage, the V_j keeps its initial velocity and acceleration/deceleration speed.

If $v_{0,j} + a_j \cdot t_{\text{res}} > 0$, the distance of V_{a+1} traveling during $(0, t_{\text{res}})$ is:

$$s'_{a+1} = v_{0,j} \cdot t_{\text{res}} + \frac{1}{2} a_j \cdot t_{\text{res}}^2. \tag{18}$$

The displacement of the vehicle V_{a+1} during the period of t_{bra} until it stops safely is

$$s''_{a+1} = \frac{\left(v_{0,j} + a_j \cdot t_{\text{res}}\right)^2}{2a_{\max}}. \tag{19}$$

So the total displacement s_{a+1} for V_{a+1} is

$$s_{a+1} = s'_{a+1} + s''_{a+1}. \tag{20}$$

Else if $v_{0,j} + a_j \cdot t_{\text{res}} < 0$, it means that vehicle V_{a+1} has stopped regularly before the stage of linearly decreasing stage. Then the total distance for V_{a+1} to stop successfully is

$$s_{a+1} = \frac{v_{0,j}^2}{2a_{a+1}}. \tag{21}$$

In conclusion, with (20), (21) and (15), we obtain (16). □

Corollary 3. *If the vehicle V_j doesn't follow the accidental vehicle V_a immediately and the velocity of V_j is greater than that of V_{j-1} before linearly decreasing procedure, the MSD for V_j can be given by* (22)*:*

$$MSD_j = \frac{\left(v_{0,j} + a_j \cdot t_{\text{res}}\right)^2 - \left(v_{0,j-1} + a_{j-1} \cdot t_{\text{res}}\right)^2}{2a_{\max}} + s_0, \quad j = a+2, \ldots, N. \tag{22}$$

Proof. Based on the assumption that V_j and V_{j-1} have the same maximum braking deceleration $a_{\max}$, the distance between V_j and V_{j-1} becomes smaller and smaller if the velocity of V_j is greater than that of V_{j-1} before linearly decreasing stage. Two vehicles are safe only when both of them have stopped without collision.

Obviously, the displacement for vehicle V_j to stop safely is

$$s_j = \frac{\left(v_{0,j} + a_j \cdot t_{\text{res}}\right)^2}{2a_{\max}}. \tag{23}$$

Similar to V_j, the displacement s_{j-1} of V_{j-1} is

$$s_{j-1} = \frac{\left(v_{0,j-1} + a_{j-1} \cdot t_{\text{res}}\right)^2}{2a_{\max}}. \tag{24}$$

So, with (23), (24), and (15), (22) is derived. □

Corollary 4. *In this situation, the velocity of V_j is less than or equal to that of V_{j-1} before linearly decreasing procedure, the MSD for V_j is expressed as follow:*

$$MSD_j = s_0. \tag{25}$$

Proof. In contrary to case 2, the distance between V_j and its preceding vehicle V_{j-1} is always increasing until both of them have stopped one after another. So in this situation, it's always safe for the two consecutive vehicles. We set the minimum safety distance MSD_j as the initial permitted minimum distance s_0. □

4.3. Validation of Stochastic Collision Prediction Model. Based on the above detailed description in Sections 4.1 and 4.2, the integrated computation method of the total average number of potential accidents in the platoon (CMAA) is formally described in Algorithm 2. In order to verify the effectiveness of stochastic collision prediction model, we conduct a Monte Carlo simulation and compare the simulation results with that of CMAA algorithm. In the simulation, the initial speed v_i and regular acceleration a_i of vehicles before emergency brake are uniformly distributed variables from $[15, 32]$ m/s and $[4, 8]$ m/s^2. The maximum deceleration value $a_{\max}$ is set as 8 m/s^2. The above parameters are the same with that listed in Table 1. However, for simplicity, the number of vehicles in the platoon is $N = 40$, $t_{\text{res}} = T_d + T_r = 0.1 + 0.9 = 1$ s and the minimum distance between vehicles $s_0 = 1.3$ m, which has been described in Section 4.2. Without loss of generality, all the Monte Carlo simulations have been performed many times per simulation point. Two dotted lines in Figure 8 denote the 95% confidence intervals of the simulation results. Figure 8 shows that the mean error between the results of our model and the Monte Carlo simulation does not exceed 6%. So the stochastic collision model is correct and reliable.

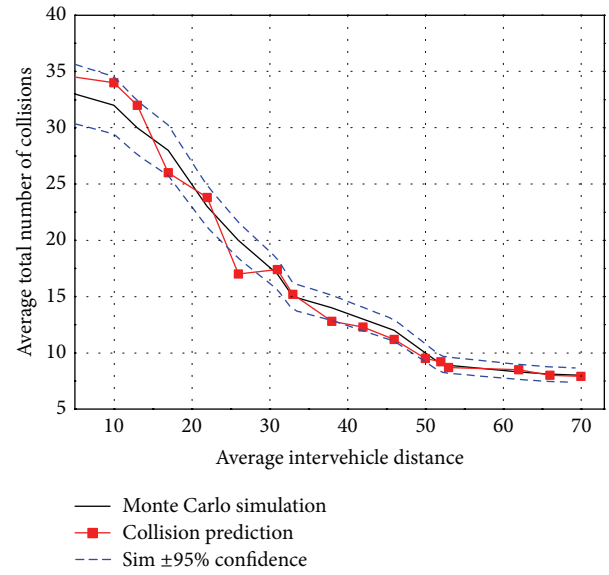


Figure 8: Average total number of collisions in the platoon versus average intervehicle distance.

5. Performance Evaluation

In this section, we describe the simulation results to demonstrate the efficiency of the proposed R-MAC protocol. In our simulation, we implement our R-MAC protocol on the NS-2 simulator and evaluate its performance fairly against the IEEE 802.11p, which is the standardized MAC protocol for VANET. The objective is two-fold: (1) evaluate the fairness of the medium access between beacons and warning message and (2) compare the performance of R-MAC and IEEE 802.11p on the packet loss rate and transmission delay.

5.1. Simulation Settings. The R-MAC protocol is implemented on the network simulator (NS-2.33). In order to conform to the realistic traffic scenario, a 1000 m × 300 m rectangle road network with a straight 4-lane highway is created, where a 3G station is introduced to act as a RSU. Different

CMAA Algorithm:
Begin: $\mathrm{NUM}_{\mathrm{acc}} = N_{\mathrm{acc}} = 0$
For vehicle V_a $a = 1$ *to* N
Step; 1: Computation of Minimum Safety Distance MSD_j **of** V_j
For $j = a + 1$ *to* N
If $j = a + 1$
Then MSD_j is computed through (16)
Else if $v_{0,j} + a_j \cdot t_{\mathrm{res}} > v_{0,j-1} + a_{j-1} \cdot t_{\mathrm{res}}$
Then MSD_j is computed through (22)
Else $\mathrm{MSD}_j = s_0$
End for
Step; 2: Computation of collision probabilities of p_j
For $j = a + 1$ *to* N
$p_j = P(d_j < \mathrm{MSD}_j) = 1 - e^{1-\lambda \cdot \mathrm{MSD}_j}$
End for
Step; 3: Construction of Matrix P
Compute the matrix $\mathbf{P}^{N-a}$
For $k = 1$ *to* $N - a$
$\sum k = \mathbf{P}^{N-a}[1, (((N - a + 1)(N - a + 2))/2) - k]$,
$N_{\mathrm{acc}} = N_{\mathrm{acc}} + k \cdot \sum k$,
End for
End for
$\mathrm{NUM}_{\mathrm{acc}} = N_{\mathrm{acc}}/N$

Algorithm 2: Formal description of the CMAA Algorithm.

traffic loads of the road are considered by setting various vehicle numbers. All the traffic scenario and vehicle mobility patters are generated from the VanetMobiSim engine [27]. For each traffic loads, the simulation are conducted ten times to take the average result.

During our simulation, each vehicle broadcasts a beacon packet of 300 bytes every 100 ms. When a vehicle encounters an obstacle or collision with its preceding vehicle, a packet of 300 bytes is sent immediately backwards to simulate a warning message. For simplicity, we assume that a collision will happen when the intervehicle space is less than the permitted minimum distance s_0, which is set as 1.3 m. The initial velocities and regular accelerations of vehicles are uniformly distributed variables from [15, 32] m/s and [4, 8] m/s^2, which are selected randomly but constant in a simulation case. Detailed parameters are listed in Table 1.

5.2. Evaluation Metrics. The performance of the R-MAC protocol is evaluated in terms of average packet delivery rate, delay and fairness. The particular evaluation metrics are defined as follows.

5.2.1. Packet Delivery Rate. Packet delivery rate is defined as the rate of the total number of data packets transmitted successfully to the total number of data packets sent from source vehicles to the destination vehicles in the whole simulation.

5.2.2. Delay Metric. In our simulations, we just consider the delay caused in the MAC layer, which is defined as the total time elapsed since the message's (beacon or warning) generation till it accesses the medium and is sent out successfully by a vehicle. And we count the average delays of beacons and warning messages together.

Table 1: Parameters used in simulations.

Parameters	Values
Number of lanes	4
Number of vehicles, N	[20, 160]
Bandwidth for channel, M (Mbps)	6
Beacon interval (ms)	100
Speed of vehicles, v_i (m/s)	[15, 32]
Regular acceleration/deceleration, a_i (m/s^2)	[4, 8]
Maximum brake deceleration, $a_{\max}$ (m/s^2)	8
Packets size (byte)	300
Delay time in MSD model, t_{res} (s)	1.0
Transmission range of vehicle (m)	180
Simulation time (s)	60
The permitted minimum distance, s_0	1.3

5.2.3. Fairness of the Medium Access. In order to quantitatively evaluate the fairness of the medium access between beacons and warning messages, we adopt the Jain's fairness index in [28]. Prior to the particular definition of Jain's fairness index in this paper, we first introduce the medium utilization for both beacons and warning messages, denoted by u_b and u_w, respectively. The medium utilization of beacons is defined as the rate of all the slots reserved for beacons to the total number of beacons. And the medium utilization of warning messages u_w is similar to u_b. Without loss of generality, let bs_i denote the number of slotsassigned to a vehicle for beacon transmission and bn_i denote the number of all the beacons to be broadcasted in the simulation. So u_b can be expressed as

$$u_b = \frac{\sum_1^N bs_i}{\sum_1^N bn_i}. \tag{26}$$

Similarly, the medium utilization of warning messages u_w can be computed by

$$u_w = \frac{\sum_1^N ws_i}{\sum_1^N wn_i}. \tag{27}$$

Based on the above description, the Jain's fairness index is defined as $(u_b + u_w)^2/2 \cdot (u_b^2 + u_w^2)$ [17]. It indicates how well the medium utilizations are distributed between beacons and warning messages. If Jain's fairness index equals to 0.5, it means that the warning messages preempt all the resource of the medium access. While Jain's fairness index is 1, the beacons and warning messages share the medium access fairly.

5.3. Simulation Results. The first set of experiment mainly investigates the performance of R-MAC on the average packets delivery rate, where beacons and warning messages

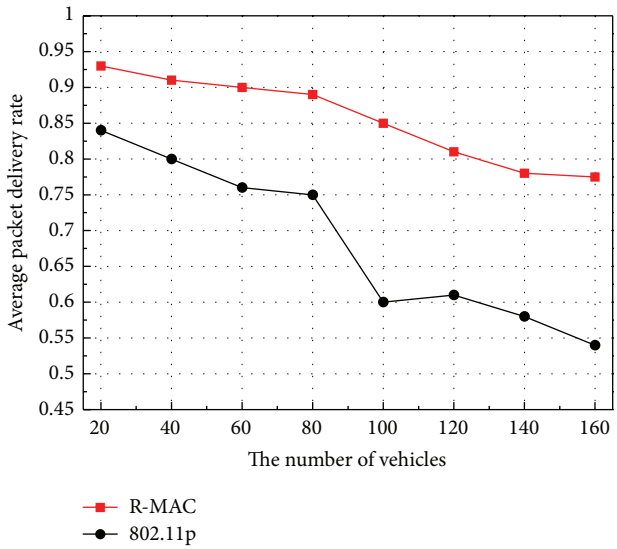


Figure 9: The packets delivery versus number of vehicles.

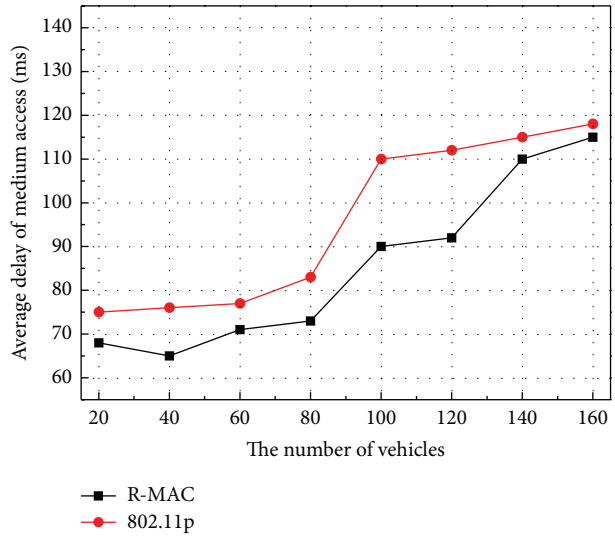


Figure 10: Average delay of the medium access versus number of vehicles.

are counted together. We vary the number of vehicles from 20 to 160 with an interval of 20 to simulate various traffic loads. As the number of vehicles increases, more packet collisions will occur, which leads to the decrease of the average packets delivery rate. Figure 9 shows that the average packet delivery of 802.11p experiences an abrupt fall from 75% to 60%. While in our R-MAC protocol, the average packets delivery rate is kept above 85% before the number of vehicles reaches 100. Even in a heavy traffic scenario where the number of vehicles is up to 160, the average packet delivery rate is still around 75%, which guarantees the Qos in safety-related applications greatly.

The second experiment mainly observes the performance of the R-MAC protocol on the average delay of the medium access. Similar with the first experiment, we count the delay of beacons and warning messages together. Figure 10 shows that the average delay of the medium access increases with the increase of the vehicle number. In addition, the delay gap between R-MAC and 802.11p becomes larger and larger (better) with the increase of the vehicle number, which verifies a good performance of average delay in our R-MAC. Nevertheless, as seen from Figure 10, R-MAC and 802.11p reach nearly the same delay performance (reaching up to 115 ms) when the number of vehicles increases to 140. Obviously, neither the R-MAC nor 802.11p protocol can work well in the heavy traffic situations. So, we will study the traffic overload tolerant R-MAC in the future.

In the third set of experiments, we mainly investigate the performance of R-MAC on the medium utilizations between beacons and warning messages. Various traffic loads are configured the same as the first experiment. As seen from Figure 11, when the number of vehicles on the road is small (less than 40), the medium utilizations of warning messages approach 100% in both R-MAC and 802.11p. That is because there are few warning messages generated when the traffic is light, and there are enough slots and chance for them to be transmitted. With the increase of vehicles, particularly

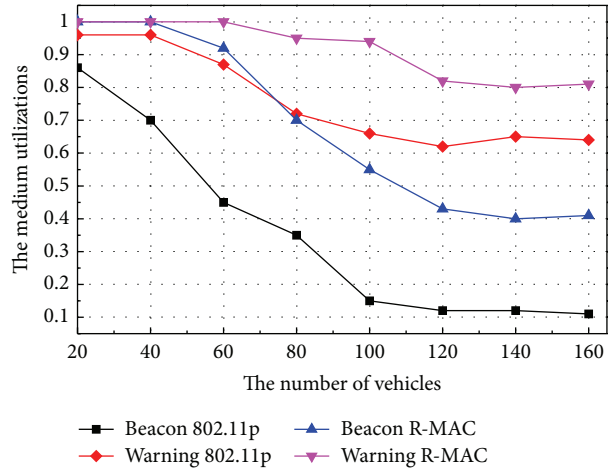


Figure 11: The medium utilization versus number of vehicles.

from 60, the medium utilizations of warning messages and beacons decrease dramatically in 802.11p, which is caused by the more and more collisions among messages. However, even in a heavy traffic (number of vehicles more than 140), Figure 11 shows that the medium utilizations of beacons and warning messages are greater than 82% and 40% in our R-MAC, respectively.

In order to demonstrate the fairness of the medium access between beacons and warning messages, the final experiment is conducted with the same settings as the third one. The Jain's fairness index is computed and plotted in Figure 12. As shown in Figure 12, the Jain's fairness index decreases dramatically with the increase of vehicles in 802.11p, which is caused by inherent attribute of contest in CSMA and different priorities of messages. When the number of vehicles reaches up to 140, the Jain's fairness index in 802.11p even drops to 0.65, which almost indicates the worst case. However, the Jain's fairness index in R-MAC always floats between 0.9 and 1.0, which

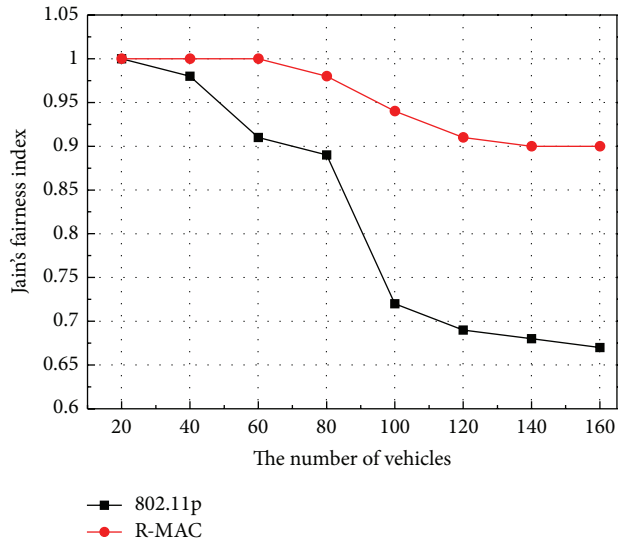


Figure 12: Jain's fairness index versus number of vehicles.

means that a good fairness between beacons and warning messages is achieved. Compared with 802.11p, our proposed R-MAC protocol can improve the Jain's fairness index by about 39% even in heavy traffic scenarios.

6. Conclusions

This paper has studied the dynamic MAC protocol problem to satisfy real-time and reliable delivery of messages while achieving the fairness of the medium access between different kinds of messages in cooperative collision avoidance (CCA) systems. We have designed a risk-aware dynamic medium-access control (R-MAC) protocol for this problem. In order to ensure the accuracy of risk-aware in R-MAC, a stochastic prediction model of the average total number of potential collisions in the platoon is presented. Extensive Monte Carlo simulations verify that our model is reliable and practical enough. Efficiency and fairness of R-MAC are verified by simulations against the standardized MAC 802.11p protocol of VANET. The simulation results show that R-MAC can improve the Jain's fairness index by about 39% compared with 802.11p. Even in heavy traffic scenarios, the packet delivery rate is still above 80% in R-MAC and the average delay is reduced significantly, which meets the communication requirements in CCA systems adequately in general scenarios. From the simulations, we have found that the transmission delay is relatively lager in overload traffic scenario. As a future work, we will study the traffic overload tolerant R-MAC protocol for CCA applications.

Acknowledgments

This paper is supported by the National Grand Fundamental Research 973 Program of China under Grant No. 2011CB302905, the National Science Foundation of China under Grant No. 61170058, 61272133 and 61228207, National Science and Technology Major Project under Grant No. 2011ZX03005-004-04 and 2012ZX03005009, Special Project on Industry Technology of Suzhou (No. ZXG201041), and China Postdoctoral Science Foundation under Grant No. 20110490821.

References

[1] IEEE P1609. 0TM/D0, 8 Drafe Standard for Wireless Access in Vehicular Environments (WAVE)-Architecture, May 2009.

[2] M. Heddebaut, J. Rioult, J. P. Ghys, C. Gransart, and S. Ambellouis, "Broadband vehicle-to-vehicle communication using an extended autonomous cruise control sensor," *Measurement Science and Technology*, vol. 16, no. 6, pp. 1363–1373, 2005.

[3] L. Andreone and C. Ricerche, "Activities and applications of the vehicle to vehicle and vehicle to infrastructure communication to enhance road safety," in *Proceedings of the 5th European Congress and Exhibition on Intelligent Transport Systems and Services (ITS' 05)*, Hannover, Germany, June 2005.

[4] S. Biswas, R. Tatchikou, and F. Dion, "Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety," *IEEE Communications Magazine*, vol. 44, no. 1, pp. 74–82, 2006.

[5] C. E. Palazzi, M. Roccetti, and S. Ferretti, "An intervehicular communication architecture for safety and entertainment," *IEEE Transactions on Intelligent Transportation Systems*, vol. 11, no. 1, pp. 90–99, 2010.

[6] G. johansson and K. Rumar, "Driver's brake reaction times," *Human Factors and Ergonomics Society*, vol. 13, no. 1, pp. 23–27, 1979.

[7] M. Khabazian, S. Aissa, and M. Mehmet-Ali, "Performance modeling of message dissemination in vehicular ad hoc networks with priority," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 1, pp. 61–71, 2011.

[8] H. Menouar, F. Filali, and M. Lenardi, "A survey and qualitative analysis of MAC protocols for vehicular ad hoc networks," *IEEE Wireless Communications*, vol. 13, no. 5, pp. 30–35, 2006.

[9] C. Zhu and M. S. Corson, "A five-phase reservation protocol (FPRP) for mobile Ad Hoc networks," *Wireless Networks*, vol. 7, no. 4, pp. 371–384, 2001.

[10] W. R. Crowther et al., "A system for broadcast communication: reservation-ALOHA," in *Proceedings of the 6th Hawaii International Conference on Systems Sciences*, pp. 371–374, Honolulu, Hawaii, USA, January 1973.

[11] F. Borgonovo, A. Capone, M. Cesana, and L. Fratta, "RR-ALOHA, a reliable R-ALOHA broadcast channel for Ad-Hoc inter-vehicle communication networks," in *Proceedings of the MedHocNet*, 2002.

[12] F. Borgonovo, A. Capone, M. Cesana, and L. Fratta, "ADHOC MAC: new MAC architecture for ad hoc networks providing efficient and reliable point-to-point and broadcast services," *Wireless Networks*, vol. 10, no. 4, pp. 359–366, 2004.

[13] F. Borgonovo, L. Campelli, M. Cesana, and L. Fratta, "Impact of user mobility on the broadcast service efficiency of the ADHOC MAC protocol," in *Proceedings of the IEEE 61st Vehicular Technology Conference (VTC '05)*, pp. 2310–2314, June 2005.

[14] R. K. Lam and P. R. Kumar, "Dynamic channel partition and reservation for structured channel access in vehicular networks," in *Proceedings of the 7th ACM International Workshop on VehiculAr InterNETworking (VANET '10)*, pp. 83–84, September 2010.

[15] H. A. Omar, W. Zhuang, and L. Li, "VeMAC: a novel multi-channel MAC protocol for vehicular ad hoc networks," in *Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS '11)*, pp. 413–418, Shanghai, China, April 2011.

[16] T. Taleb, A. Benslimane, and K. B. Letaief, "Toward an effective risk-conscious and collaborative vehicular collision avoidance system," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 3, pp. 1474–1486, 2010.

[17] "IEEE standard for information technology-telecommunications and information exchange between systems-local metropolitan area networks-specific requirements part 11: wireless lan medium access control (MAC) and physical layer (PHY) specifications amendment 6: wireless access in vehicular environments," IEEE standard 802. 11-2007, pp. 1–1184, June 2007.

[18] A. Touran, M. A. Brackstone, and M. McDonald, "A collision model for safety evaluation of autonomous intelligent cruise control," *Accident Analysis and Prevention*, vol. 31, no. 5, pp. 567–578, 1999.

[19] T. Kim and H. Y. Jeong, "Crash probability and error rates for head-on collisions based on stochastic analyses," *IEEE Transactions on Intelligent Transportation Systems*, vol. 11, no. 4, pp. 896–904, 2010.

[20] A. Chakravarthy, K. Song, and E. Feron, "Preventing automotive pileup crashes in mixed-communication environments," *IEEE Transactions on Intelligent Transportation Systems*, vol. 10, no. 2, pp. 211–225, 2009.

[21] C. Garcia-Costa, E. Egea-Lopez, J. B. Tomas-Gabarron, J. Garcia-Haro, and Z. J. Haas, "A stochastic model for chain collisions of vehicles equipped with vehicular communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 13, no. 2, pp. 503–518, 2012.

[22] W. Guo, L. Huang, L. Chen, and H. Xu, "An adaptive collision-free MAC protocol based on TDMA for inter-vehicular communication," in *Proceedings of the 4th International Conference on Wireless Communications and Signal Processing*, October 2012.

[23] K. Ray Lama and P. R. Kumar, "Dynamic channel reservation to enhance channel access by exploiting structure of vehicular networks," in *Proceedings of the IEEE 71st Vehicular Technology Conference*, pp. 1–5, Taipei, Taiwan, May 2010.

[24] N. Wisitpongphan, F. Bai, P. Mudalige, V. Sadekar, and O. Tonguz, "Routing in sparse vehicular ad hoc wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1538–1556, 2007.

[25] M. Brackstone and M. McDonald, "Car-following: a historical review," *Transportation Research F*, vol. 2, no. 4, pp. 181–196, 1999.

[26] "IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Multi-Channel Operation," IEEE Std. 1609. 4-2010, 2011.

[27] "VanetMobiSim project home page," http://vanet.eurecom.fr/.

[28] R. Jain, D. M. Chiu, and W. Hawe, "A quantitative measure of fairness and discrimination for resource allocation in shared computer system," Tech. Rep., Digital Equipment Corporation, 1984.