2010

Reliable Broadcasting in VANET

Pat Jangyodsuk
San Jose State University

Recommended Citation

Jangyodsuk, Pat, "Reliable Broadcasting in VANET" (2010). *Master's Projects*. 158.
https://scholarworks.sjsu.edu/etd_projects/158

CS 298 Report

Reliable Broadcasting in VANET

Pat Jangyodsuk

Spring 2010

Abstract

Vehicular Adhoc NETwork (VANET) is a rapid growing wireless ad-hoc network model where the vehicles play the nodes role in a network. Major application of VANET including hazard warning application requires effective broadcast mechanism. Typically, selection of the next relaying hop is the major problem in VANET broadcasting. To get the smallest propagational delay, the number of relaying hops must be minimize. Meanwhile, the transmission reliability must also be preserved. Both of these two constrains must be taken into consideration. However, these two aspects often collide to each other since increasing one of them always result in decreasing of another. In this paper, I will suggest a new protocol that can satisfy great reliability without sacrificing message propagational speed. The protocol is based on RTB/CTB [1] scheme which guarantees the successful reception of a report broadcasting. However, unlike the original RTB/CTB approach where the process is slow, the proposed scheme can work much faster, yet providing broadcasting reliability due to many enhancements added in the design such as fixed short length jamming duration, non-CTB iteration, non-wasting contention slot and protocol messages reduction. As we could observed from the simulation result that the proposed protocol performed better in term of bytes usage, reliability and propagational time when compared with Slotted p persistence and RTB/CTB.

Acknowledgement

To my wife, who is always a helping hand when most needed. To my parents, who always support me in desperate time and to most of all, to professor Melody Moh, for all advices and ideas to make this project a successful one.

Table of Contents

List of acronyms

ACK	Acknowledge
CBR	Constant Bit Rates
CTB	Clear to Broadcast
CTS	Clear To Send
CW	Congestion Window
GIS	Geographic Information System
GPS	Global Position System
IP	Internet Protocol
LAN	Local Area Network
LL	Link Layer
MAC	Multiple Access Control
MANET	Mobile Ad-hoc NETwork
NS-2	Network Simulator version 2
QoS	Quality of Services
REQ	Request
RTB	Request To Broadcast
RTS	Request To Send
SUMO	Simulator of Urban MObility
UDP	User Diagram Protocol
VANET	Vehicular Ad-hoc NETwork

1. Introduction

Vehicular Adhoc NETwork (VANET) is becoming a focusing point in researcher communities. Due to various kinds of applications including safety driving, parking lot finder, real-time route finder, it is becoming popular in recent years. Among all these applications, safety driving is deemed as the most important one since VANET was originally designed for the safety driving propose. The core function of this application is report broadcasting. Whenever there is an accident, an accident report must be generated and will be propagated to other vehicles via broadcast mechanism. However, the process of choosing the next relaying vehicle is somewhat complicated. Ideally, only one relaying hop per broadcasting round should be sufficed to minimize the number of transmitted messages. This way, there will be no redundant transmitted messages. Furthermore, this hop should have the furthest distance with respect to the previous hop to cover the largest area possible. However, following this idea would reduce the reception probability because of the greater distance. Therefore, the balance between the reception probability and the propagational speed must be well decided.

Originally, VANET was designed to offer more safety driving environment which could be achieved by communication among vehicles. Upon knowing information regarding accident or any danger on the road, the vehicle will tell others about the news so that they could avoid or prepare for bad situation. Please note that VANET is a new topic that just become popular in very recent years as the first VANET conference was held in year 2004 by ACM.

Up until the date of writing this document, there is no commercial product of VANET yet. Still, there are attempts to standardize VANET. For instances, IEEE 802.11p [23] is a MAC layer standard from IEEE task group. However, it has not yet been released as a complete draft yet. In IEEE 802.11p, the Dedicated Short Range Communication (DSRC) is a core function. DSRC is a US government project for vehicular network communication. It has been allocated 75MHz of spectrum in the 5.9GHz band in the USA. Again, it is not a full draft yet. From what we know, DSRC is a short range, high bandwidth wireless technology just like other 802.11 standard. However, the difference is that it is designed for fast mobility vehicular network. Therefore, all VANET characteristics and problems are included in the design.

Popular research topics in VANET are routing and broadcasting. Like MANET, VANET routing must deal with vehicle movement, changing of topology and other problems in ad-hoc network.

However, unlike MANET, VANET has much more predictable nodes movement as vehicles are constrained to move by road directions only. Nevertheless, this does not mean that the problem in VANET becomes easier as the node's speed is tremendous. In 10 seconds or less, the connection between vehicles can be broken in freeway speed. Broadcasting in VANET is the situation where a vehicle need to propagate the report to other vehicles. The broadcast initiator starts by broadcasting the report to its neighbors. Unfortunately, due to limitation in transmission radius, the report cannot be heard by every intended recipients. Therefore, some vehicles must relay the report. The arose question is who should do it so that bandwidth is minimally consumed. Yet, the broadcast is still reliable and delivered in fast fashion.

1.1 Major VANET applications

Examples of VANET applications are as following:

- Safety driving application – To provide more safety driving behavior. For instances, when there is an accident on the road, all vehicles moving to the accident spot will be given a warning not to go to that direction. Another example could be when a vehicle is about to reach a dangerous curve or slippery road, it will be warned of the danger.
- Path finder or location finder – To get the driver information regarding fastest route or the nearby points of interest. The function is very similar to that of the GPS device nowadays. However, unlike GPS devices, this information is totally dynamic and updated in real-time. Therefore, real-time critical information that was missing in GPS devices like traffic jam or car accident will be included in the route calculation which, in turn, offers much better route accuracy.
- Local vehicular network – with VANET, we can provide a communication channel between vehicles. Therefore, local network application like LAN gaming can be achieved.
- High speed Internet connection – Nowadays, we can achieve the Internet access anywhere anytime with cellular technology such as 3G network. However, 3G provide very limited bandwidth. With VANET, Internet access can be made with the existence of roadside equipment, a gateway to the backbone Internet. The bandwidth we get from VANET will be much higher since the ad-hoc network based on short range wireless technology like IEEE 802.11, naturally provides much higher bandwidth than cellular network such as 3G.

2. Background

Mobile Ad-hoc NETwork (MANET) is an ad-hoc network in which every node is both a router and a transceiver. When any node wishes to transmit a packet to other nodes, the packet will be sent along a set of nodes until it reaches the designated destination. VANET, a kind of MANET, is an ad-hoc network on the road in which the vehicles are nodes in the network. The intention of VANET is providing more safety and more convenience driving environment.

2.1 Technical challenges

Although VANET can give us many promising features and applications, there are still a lot of problems regarding VANET. One of VANET characteristics distinguishing it from other types of ad-hoc network is the fast mobility of vehicles. The tremendous speed of a vehicle makes most existing MANET routing protocol impractical in VANET usage. The major reasons are most routing protocols require the topology creation and maintenance. The idea will work fine for static or slow mobility networks. However, in VANET, where every node moves so fast such that the topology information can be out-dated very swiftly, the topology maintenance message overhead are so large and the information in routing table is inaccurate resulting in low performance routing.

While the previous mentioned problem is the uni-cast routing, the broadcasting is also a problem. As mentioned, the broadcast process is the core of the safety driving applications. When there is an urgent issue that needed to inform anyone moving to the same location, the broadcast process is used. The fundamental idea is simple. The message initiator first broadcast the message. Certainly, not everyone will hear this message because of the short transmission radius. Therefore, one or more vehicles have to relay the message. The problem is who should relay and how to provide most reliability to the broadcast by consuming network resources as least as possible. The goal is to providing the most reliable, fastest and the protocol must not overwhelming the network by transmitting too many messages. The selection of a relaying node can be difficult since there is no central coordinator in an ad-hoc network.

2.2 Related works

There are many works regarding VANET broadcast issue. Many of which adapt different strategies which fall into various categories including distance based, location based, probability based and topology based.

2.2.1 Distance based

The milestone solution of the issue is the distance based. The idea is very simple, the node with the greatest distance shall be the next relaying hop. To implement it, each node has its own timer. Upon receiving an accident report, it will start this timer. The duration of the timer is inversely proportional to the relative distance between itself and the broadcaster. When the timer is expired, it will relay the message. To suppress the number of messages, if a node hears the redundant message, meaning that other nodes have already relayed the report, it will stop its attempt. Thus, the node with the furthest distance to the broadcaster shall be the next relaying hop because its transmission waiting time is the shortest. With this idea in mind, we could achieve lowest message propagation delay due to the minimum number of hops used. However, the reception probability is a potential problem when using this approach because of the large distance.

2.2.2 Location based

Location based approach [2,3,4,5] is very similar to distance based. The difference is that: rather than using just the distance, we can use the location obtained from Global Position Devices (GPS) to get the area, map and other useful information as inputs to choose the next relaying hops. For instances, Hua & Villafane [2] suggested and idea to divide the road portion into multiple cells as depicted in figure 1 below.

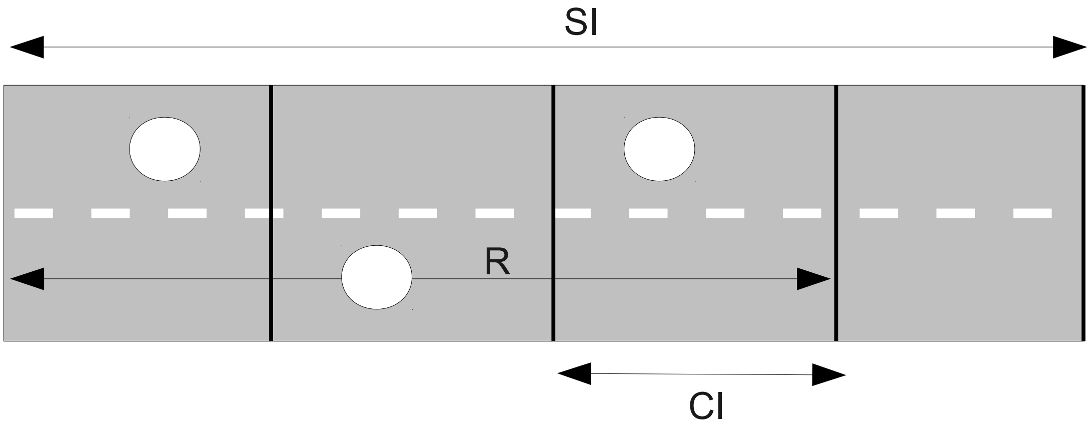

Figure 1 – Cell splitting

These cells have a basic requirement that vehicle's transmission radius must cover “at least” its adjacent node. For example, a transmission from vehicle in cell B2 must reach all vehicles in cell B1 and B3. When a node hears the report, the index of cell will be used in the calculation instead of the plain distance. Furthermore, In Hua & Villafane's work [2], if a map is known, a vehicle located at at an intersection will have higher priority of retransmission since their transmission covers larger area.

2.2.3 Using of beacon messages

Beacon messages are implemented in many location based approach [3,4,5]. With its own location information embedded in its beacon message, each node will have a knowledge of its neighbors. This neighbor information is very useful for retrieving many useful data such as vehicle density [6] , link reliability [4], transmission radius [5] etc. Suriyapaibonwattana & Pomavalai [3] suggested using of the neighbor location to see if the distance between itself and the previous broadcaster is the greatest. On the other hand, the approach proposed by Jiang, Guo, & Chen [4] is a lot complicated. In Jiang, Guo, & Chen's work [4], the neighbor's location is used to calculate each transmission reliable rate. If any vehicle has the highest number when transmitted, then it will be chosen as the next relaying hop.

Suriyapaibonwattana & Pomavalai suggested an interesting idea in their work [3] . Each vehicle submitted its location information in its advertised beacon message. Therefore, each vehicle will have a knowledge of its neighbors in term of both numbers of neighbors and their respective positions. The process to select next relaying hop is as following: when the report is broadcast, each vehicle will calculate the distance with respect to the broadcaster for itself and all of its neighbors from the information it has. If it turns out that your distance to the broadcaster is the longest, then you will rebroadcast the message. Otherwise, it means that you are not the chosen one. They will just simply remain silent.

Unlike using the distance, Jiang, Guo, & Chen [4] suggested using of the transmission reliable rate. Beacon messages carry the location information just like the previous mentioned work [3]. However, we do not use distance in the calculation. Rather, the distance is the input for the transmission reliable rate calculation. This number is the indication of how many vehicles would successfully receive the message if one rebroadcasts. Therefore, the vehicle with the greatest number is the winner. The step taken is the same as Suriyapaibonwattana & Pomavalai's work [3]. Each vehicle calculates the number for itself and all of its neighbor. If it found out that, its number is the greatest, then it will rebroadcast.

2.2.4 Probability based

In most topics, when there are too many contenders, probability is usually used to reduce chances of collision and number of transmitted messages. That idea is also applied to VANET [6,7]. These works adapted the probability to reduce the transmission chance. While some of the works used the fixed static number [7], many of which successfully adapted the adaptive number [6].

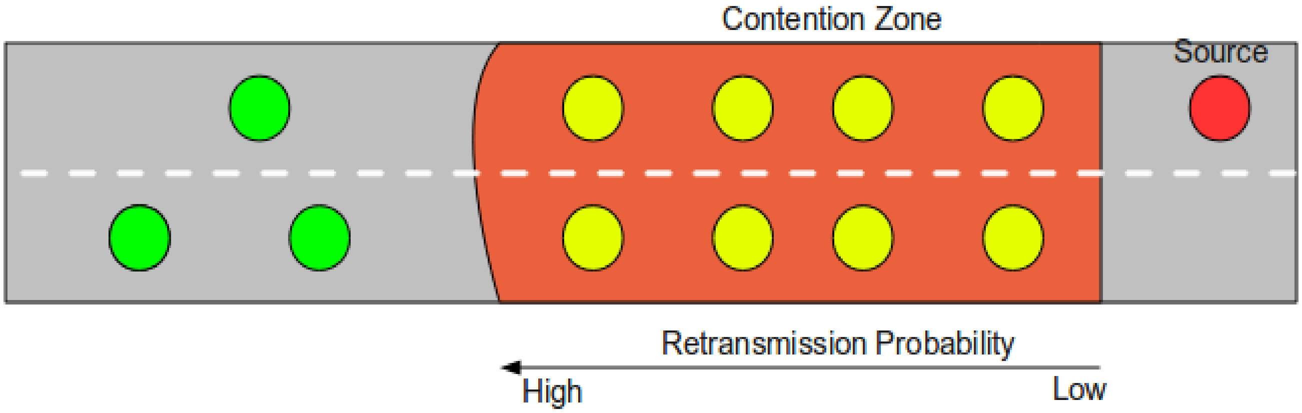

Figure 2 – Weighted p persistence

Weight p persistence [7] is the fundamental idea of probability usage in VANET. Upon message reception, instead of using delay timer, each vehicle will retransmit with probability p. However, using equal p to all vehicles is inappropriate since vehicle with further distance should have higher priority. Thus, the retransmit probability is proportional to the distance with respect to the broadcaster. Therefore, there is a higher chance that node whose distance to broadcaster is greater will relay the message. Figure 2 above illustrates weight p persistence model.

While using probability requires no overhead and simple to implement, the selection of p can drastically affect overall performance. On one hand, too small p could cause everyone to remain silent and the message cannot be further propagated or will be delayed if there is other backup mechanisms. On the other hand, too large p will cause message collisions and will be a waste of channel resources. In short, the selection of p must be carefully chosen. The important factor is the vehicle density. Theoretically, when there are n nodes, the probability should be 1/n because, mathematically, there will be only one node that will retransmit. Therefore, according to the theory, if the density is low, then we select large p so that there is someone to relay and if the area is dense with vehicles, small p would be more prefer to avoid unnecessary transmission.

Yang, Shen, & Xia [6]suggested an improvement to the probability based broadcasting protocol. The probability is adapted to vehicle density which is calculated from neighbor's locations obtained from beacon messages. With the location information carried in the beacon message, we will know how many neighbors there are. Therefore, the density can be derived from this information. The density along with the distance are the inputs to derive p for each vehicle.

2.2.5 Topology based

The next idea is graph topology. Topology based approach is the solution adapted widely in wireless sensor network. Since the change of topology in VANET is rapid, most of the time, topology solution is out of question. However, in some scenarios such as freeway where the road is straightforward, it can still be useful.

One good example of topology usage in VANET topic would be Bononi's work [8] in which all nodes creates the backbone topology. The criteria of selecting backbone nodes are speed and distance. The backbone nodes will be given responsibility of relaying. Since the topology is created and the relaying path has been established, there will be no contention or collision. However, the process of retaining and creating the backbone is always expensive and sophisticated in high velocity network such as VANET. Figure 3 below shows the vehicle topology.

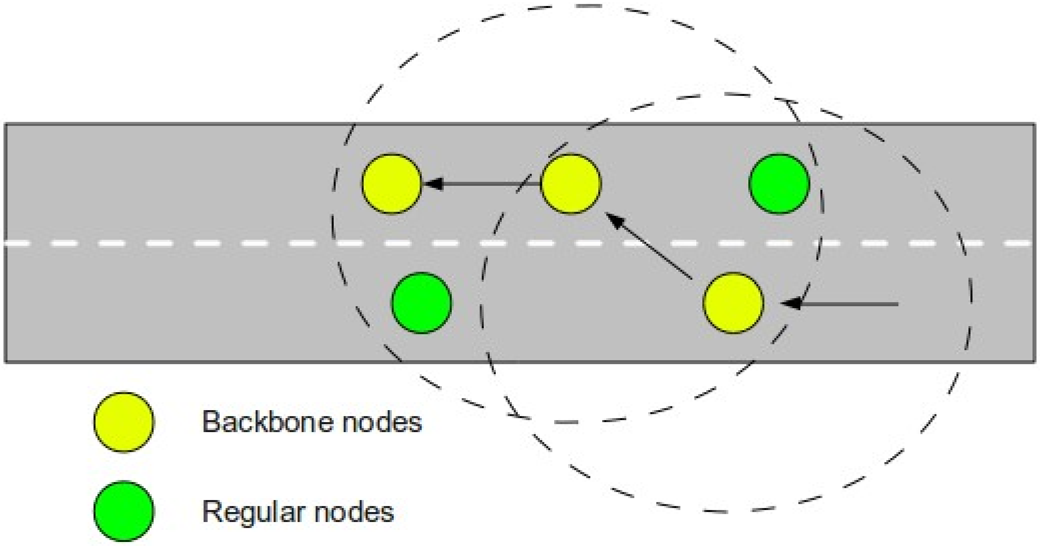

Figure 3 – Vehicle topology

Bako, Schoch, Kargl, & Weber [9] adapted the strategies from wireless sensor network into VANET. The dependency tree will be constructed. Parents are nodes from whom we hear the report and children are those we broadcast the report to. The goal is to providing the expected transmission probability to parents. This number is varied to the number of parents of each node. For instances, assuming that node A has three parents. These three parents will contend for retransmission and, theoretically, there should be only one node that transmit. Thus, the advertising probability sent from node A is 1/3. This probability is carried in beacon messages. For each node, the maximum number of expected probability is its adaptive p.

2.2.6 Reliability

Apart from the minimizing number of relaying hops, the broadcast reliability is also a major issue. Since RTS/CTS cannot be applied to broadcasting, the problem becomes a serious topic. Many works have been done regarding the concern.

Balon & Guo [10] modified 802.11 backoff mechanism to provide reliability. Every node has to keep track of frame sequences from its neighbors. Any lost or out of sequence frames will be marked. This frame sequence including number of lost and out of sequence frame will be used to estimate the congestion status of the local network. In turn, the backoff delay will be set according to the estimated network status. The severe the condition, the longer the delay.

One major difference between unicast and broadcast is the existence of ACKnowledge frame which makes broadcast unreliable because the sender does not know whether or not the recipients have received the packets. Shin, Yoo, & Kim [11] applied ACK frame to VANET broadcasting. Basically, their protocol is based on slotted p persistence model [7]. However, some adjustments have been made. Once the process of contending for next relaying hop has been finished, the winner must send an ACK back to the previous broadcaster. If any vehicle overhear ACK but cannot hear the report, they will send a report requesting message to the broadcaster who, in turn, replies back with the report. The process is depicted in figure 4 below. Once the relayer 1 relays the message {2}, it will know that I am the winner. Therefore, it will send ACK to the originator {3}. Assuming that there is one vehicle overhears the ACK but cannot hear the report from vehicle A {4}. This vehicle will send a request for report to relayer 1 {5}. Upon receiving the request, once again, relayer 1 will rebroadcast {6}.

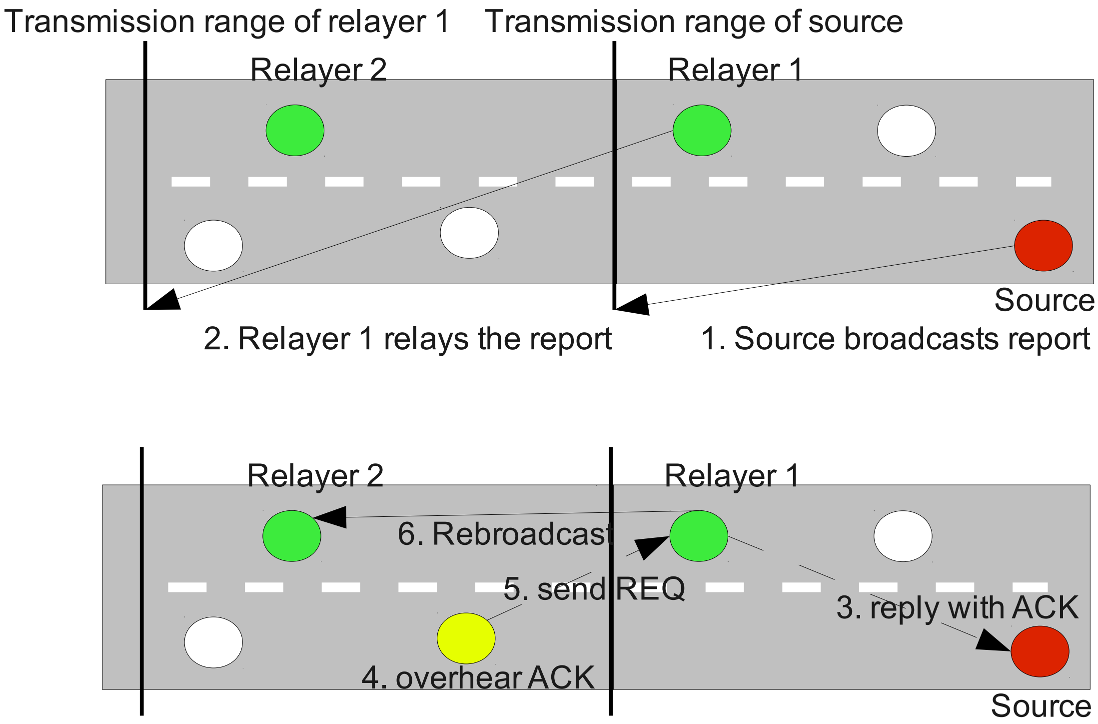

Figure 4 – Request of lost report scenario

It is a well known fact that, in wireless network, the closer you are to the sender, the more likely you will receive the packet. This is because there is less chance of collision due to the fact that the hidden/expose node problem is unlikely to happen. Furthermore, in term of wireless physical signal, the signal strength is stronger and the chance of obstruction is unlikely. Li [12] suggested retransmitting in the same area with closer expecting distance to increase the reception probability. As soon as the forwarder has been selected, the "make up" nodes which is the nodes in between the source and the forwarder, will rebroadcast again to increase the reception probability.

This "ensure" rebroadcasting will be repeated with smaller and smaller area until the reception probability reach a certain threshold where we are confident that the transmission is reliable. One can think of the process as a binary tree.

2.2.7 QoS

Apart from the previous topics, QoS is also another big issue in VANET broadcasting. The fact that there is no central coordinator makes it difficult to provide various traffic quality. Mak, Laberteaux, & Arbor [13] suggested idea to provide QoS in VANET with the requirement of roadside equipment. Roadside equipment is the network equipment located at the side of the road providing connectivity to Internet or other networks. The author assumed that the roadside equipment can behave as the central coordinator and all vehicles are equipped with two network interfaces. One interface is for the ad-hoc network and the other one is for centralized network. When a vehicle moves into roadside equipment transmission radius, the second interface will be activated and QoS can be achieved through the use of centralized network.

2.2.8 Other issues

2.2.8.1 Unequal transmission radius

Amoroso, Ciaschini, & Roccetti [5] introduced one problem that nobody has ever mentioned before, the unequal of transmission radius. In most papers, the authors assumed that the transmission radius of all vehicles is equal. Thus, the vehicle with the greatest distance with respect to the broadcaster should be the next relaying hop. This is not true if the assumption is incorrect. Figure 5 shows the scenario.

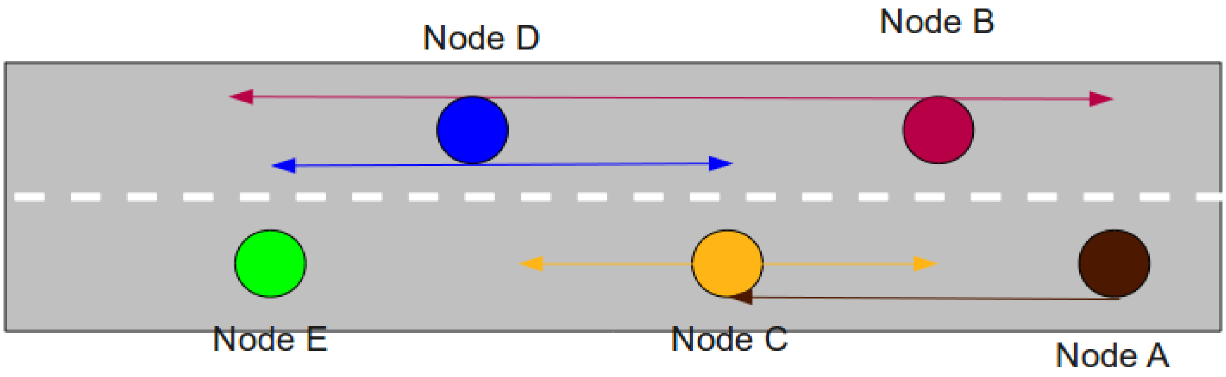

Figure 5 – Unequal transmission range scenario

From figure 5, vehicle A is the message initiator. According to the milestone idea, vehicle C suppose to be the next relaying hop since its distance to A is greatest. However, because of the varied transmission radius, it will take 2 relaying hops to reach vehicle E but it will take one hop if B is selected as the next hop. Therefore, beside the distance, the transmission radius, which will be included in beacon messages, will also be one of the inputs in selecting next hop algorithm.

2.2.8.2 Threshold value

Ni, Tseng, Chen, & Sheu [14] suggested four interesting ideas. Firstly, the author introduced the message transmission in the same area with the assumption that the more number of times you hear the message, the more likely that vehicles in curtain area will receive a report. When you first hear the message, the counter variable will be set to zero and the transmission timer will be set. If they hear redundant messages, the timer will be reset and the counter variable is increased. The attempt to retransmission will be stopped when the counter value reaches curtain threshold number.

The second idea is based on the distance. The fundamental idea arose from the fact that the closer you are to the broadcaster, the less additional area you can cover. Therefore, it means that you can dedicate less area if you are close to the broadcaster. Just like the counter based idea, one variable is adjusted every time we hear the message. The “distance” variable stores the distance to the closest broadcaster. Once the distance value is less than the threshold, a node stop attempting to rebroadcast.

Moving from the distance to the area is the third idea. While using the distance is straightforward and easy to implement, the assumption that you can cover less area if you are closer to the broadcaster might not be true since there are other factors to consider such as map and direction. In this third idea, the beacon message is implemented to provide location information. With the neighbor's location information, we can calculate how much additional area the broadcaster have already covered. Again, the variable is used. This time it is the additional area we can cover when retransmit. Every time a vehicle hear the message, it will calculate how much intersected area this broadcaster has already covered and it will subtract its transmission area with the intersected area accordingly. Once the value fall below the threshold, the attempt to rebroadcast will be stopped.

The last idea proposed by Ni, Tseng, Chen, & Sheu [14] is different from all previous three ideas. Each group of vehicles form a cluster. The cluster consists of three node types; head, gateway and member. The cluster head is a node whose transmission radius can reach everyone in the same cluster. However, the author did not specified precisely how to elect the cluster head. The gateway nodes are those who connect to the gateway nodes in other clusters. Finally, member are those who do not belong in both head and gateway group. Figure 6 shows the cluster structure.

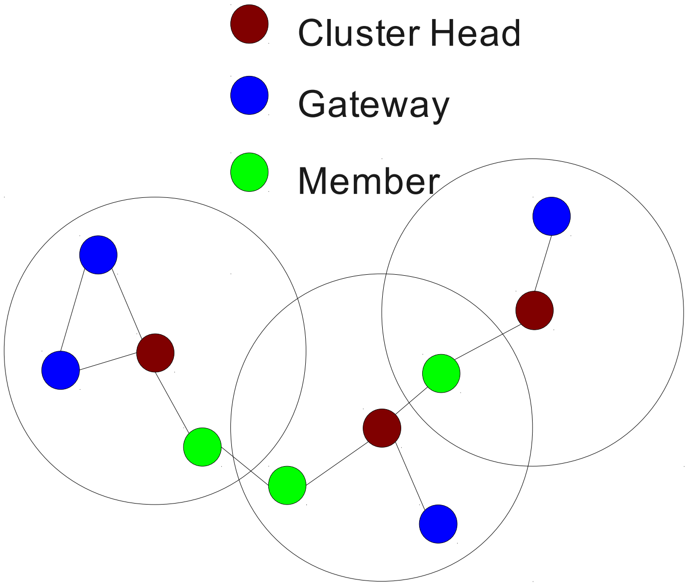

Figure 6 – Cluster structure

When a gateway node receive a message from other clusters, it will rebroadcast. This message will reach the head of a particular cluster since the head must be able to reach everyone in the same cluster. The cluster head, upon receiving the message, retransmit. This message would reach everyone in the cluster. The message will be furthered propagated by the gateway nodes connecting to other clusters.

2.2.8.3 Broadcast at an intersection

The road topology can greatly affect the protocol, for instances, when there are many intersections in the city road. In an intersection, the milestone distance idea could be a substantial problem as shown in figure 7 below.

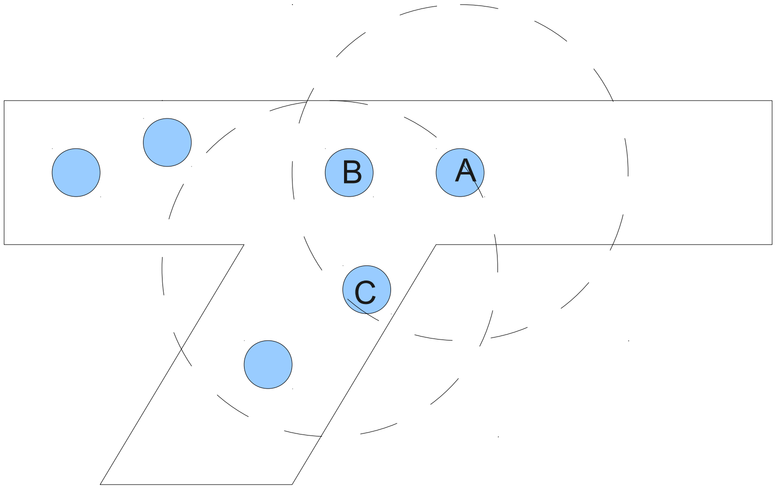

Figure 7 – Intersection problem

In the example, node A is the source. B and C will hear A's transmission. According to the distance based scheme, the node whose distance to the source is greatest will be the forwarder. In this case, the forwarder is C. However, because of intersection angel, nodes located further in horizontal direction will not hear the report from C. Furthermore, once B hears the redundant report from C, it will stop attempting its retransmission. Therefore, the report propagation will be ended at this intersection.

Acknowledging the problem, Lai et al and Nasri et al [15,16] suggested the same idea but with different implementation to solve the regarding issue. Both schemes use the angle to the broadcaster to decide whether or not to stop its attempt. First of all, vehicle's class is defined according to the angle with respect to the broadcaster. If the redundant message comes from a vehicle in the same class, it will stop. Otherwise, it will just ignore the message. Figure 8 illustrates the idea.

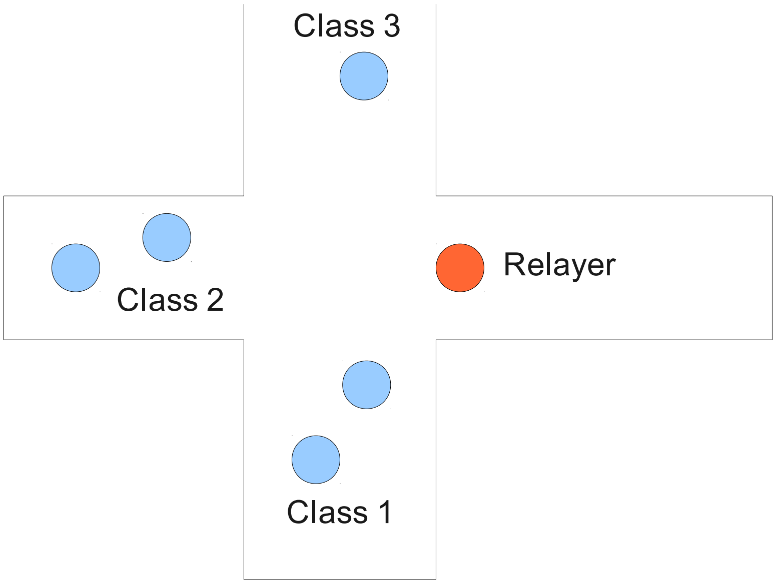

Figure 8 – Class defined on angle

As can be seen by the figure, vehicle classes are defined by the angle to mark which side of the intersection you are currently. If class 1's vehicle hears the redundant report from class 2's vehicle, it will not stop the retransmission timer. Therefore, the intersection problem can be solved.

2.2.8.4 Broadcast in sparse area

The art of broadcasting in VANET relies on the number of vehicles along the path. If there is no more vehicles in the propagation path, the report must be stopped at the point. The arose question is if there is a way to propagate the report in the sparse network. Tonguz et al [17] addressed the problem and propose a solution to the issue. Typically, a message is relayed by vehicles moving in the same direction as the message initiator. If there is no vehicle heading to the same direction, the propagation stops. However, in a bi-directional road, we can use vehicles in opposite direction as a “messenger”. This so called “messenger” will buffer a message and carry it while traveling in the opposite direction. The message will be released once it found vehicles in the opposite lane. Figure 9 shows the scenario.

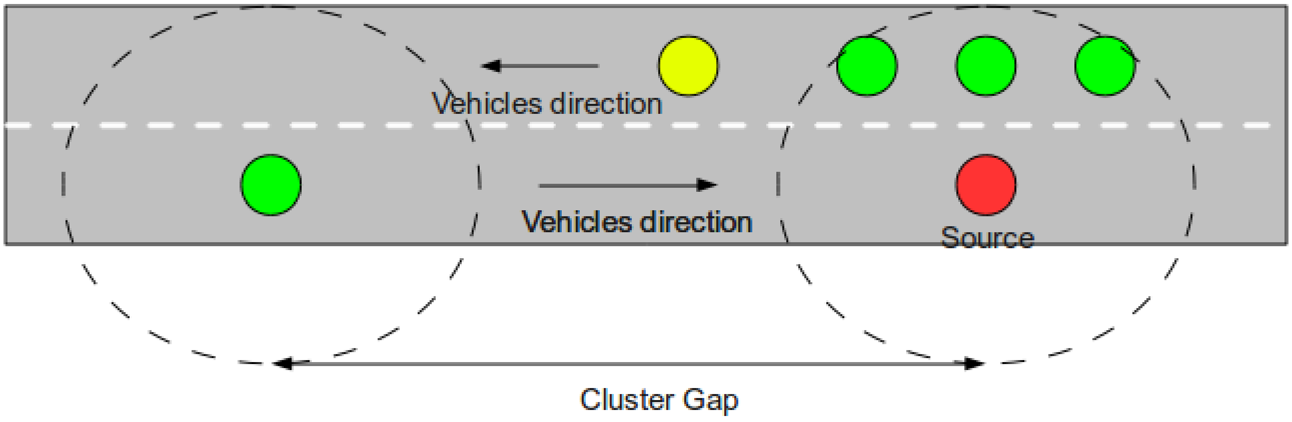

Figure 9 – Sparse network message propagation

Referring to figure 9, the message is generated by a red car and needed to notify all vehicles moving to the same direction. However, one could see that there is no vehicles in the same lane when the source broadcast it. Thus, the green vehicle moving in opposite direction will carry this message. Once some vehicles moving in the opposite direction are within its transmission radius, it will broadcast the message to them and the report propagation can be continued.

3. Proposed protocol

The proposed protocol is based on RTB/CTB [1] and slotted p persistence model [7]. The reason we picked RTB/CTB as the based protocol is because it is the only protocol that can guarantee the successful reception while the rest can only increase the likeliness of reception.

3.1 Overview of two original protocols

3.1.1 RTB/CTB

Just like RTS/CTS (Request To Send/ Clear To Send), RTB/CTB (Request to Broadcast/ Clear to Broadcast) is a pair of broadcast messages intended to eliminate hidden/exposed nodes problem. However, since the message is broadcast, it is not possible to enable every recipient to acknowledge back with CTB. Therefore, the jamming signal will be used to notify any potential hidden nodes to backoff because multiple jamming signals can be transmitted at the same time. Apart from eliminating hidden/expose nodes, jamming signal is also used as the mechanism to select the new relaying hop. The duration of jamming signal is proportional to the distance with respect to the broadcaster, the greater the distance, the longer the duration. As soon as it finishes sending jamming signal, it will check if it still hears the jamming signal from other nodes. If it cannot hear, then it will claim that it is the next broadcaster by sending CTB replying back to previous broadcaster. Thus, the node sending longest duration of jamming signal will be the next broadcaster. Figure 10 depicts the scheme frame.

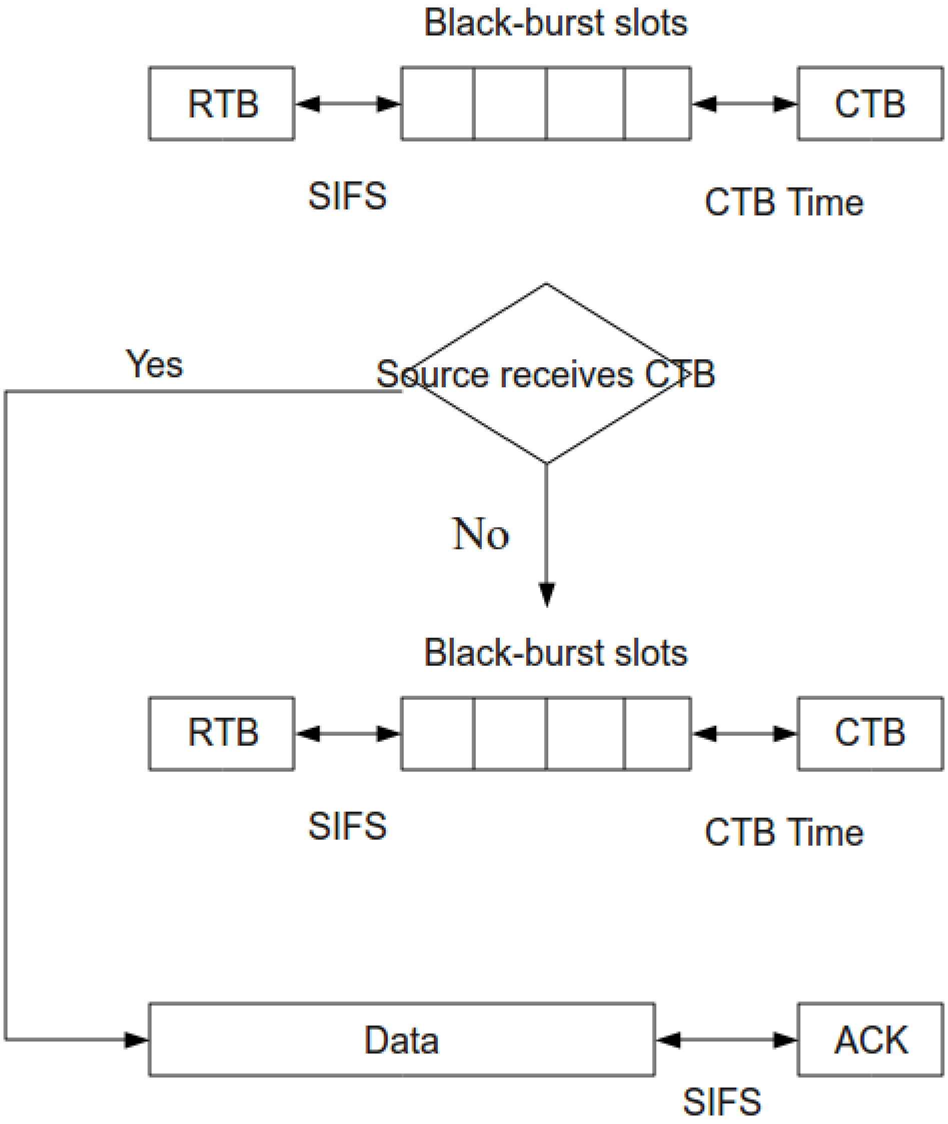

Figure 10 – RTB/CTB message scheme

According to figure 10, the sender will first transmit RTB indicating that I have a urgent report to broadcast. Upon receiving the RTB, all recipients will wait for SIFS and start sending jamming signal for some duration depending on its location with respect to the broadcaster. Once it finishes sending jamming signal, it will listen to the channel to see if it can still hear more jamming signal. If it does not, it means that I am the furthest node away from the sender and I will send CTB. Otherwise, the node will do nothing. Then, the sender will send the message after SIFS period and waiting for ACK from a node sending CTB.

The way each node calculates the jamming signal duration depends on the cell index, an estimate distance from the sender. For instances, assuming that the sender transmission radius is 1,000 meters and total number of cells is 5. Therefore, each cell width will be 1,000/5 = 200 meters. If vehicle A is 450 meters away from the sender, then it will be on cell number 3 (the first cell number starts at 1 which is the closest to the sender). If it is 150 meters away from the sender, then it will be on cell number 1. The formula to calculate the jamming duration is shown below.

$$L = floor\left(\frac{d}{Range} \times N_{max}\right) \times SlotTime$$

Where :L = Jamming signal duration
d = distance from the RTB sender
Range = RTB sender transmission radius
N_{max} = Maximum number of cells
SlotTime = Jamming duration for one slot time
floor = a math function that eliminate any decimal point precision

However, since the protocol uses cell index instead of the actual distance in jamming duration calculation, there is a chance that CTBs collision might happen. When it happens, the process is repeated but, this time, the number of contenders will be reduced as shown in figure 10. Only nodes sending collided CTB will participate this time and the contention zone will also be reduced to the cell width of last CTB contention iteration. The process will be repeated if there are still collisions until the number of round reaches threshold value. After that, the random phrase will come into play. The formula to calculate the jamming duration for i^{th} iteration of RTB is shown below

$$L = floor\left(\frac{d - Llongest_{i-1} \times W_{i-1}}{W_{i-1}} \times N_{max}\right) \times SlotTime$$

and

$$W_i = \frac{Range}{N^{max}_{i}}$$

Where :

L = Jamming signal duration

d = distance from RTB sender

Llongest$_{i=1}$ = longest black-burst duration in i-1 iteration

W$_{i=1}$ = segment width of i-1 iteration

N$_{max}$ = Maximum number of cells

SlotTime = Jamming duration for one slot time

Problems with original RTB/CTB protocol

In term of reliability, while most of the previous works suggested many interesting ideas, there are few that can guarantee the successful reception. To the best of our knowledge, RTB/CTB is the only protocol that can achieve this. However, RTB/CTB suffers a lot from the slow process due to various reason which are:

1. The protocol could end up in multiple iterations if the density is high. We could see this problem easily when contenders in the same cell send CTBs. Then, the iteration occurs and it could happen again and again if the density is really high. Therefore, time will be wasted by the process of selecting new relaying hop in just one round.
2. The jamming signal duration is variable length and it is even worse because this protocol always end up with the longest jamming duration (the node with the greatest distance will send the longest duration of jamming signal) resulting in slow report propagational time.

3.1.2 Slotted p persistence

Slotted p persistence model is the probability based broadcasting. Basically, it is based on both distance and probability in the selection of next relaying hop. Due to the easiness of implementation difficulty, the model has been adapted in many subsequent works [6,11]. In slotted p persistence model, the road will be divided into multiple cells. Each cell will be allocated with different time slot. The further one will be given lower number of time slot meaning that vehicles located in this cell would have a chance to retransmit message first. To reduce the collision probability and redundant messages, each node will retransmit with fixed probability p. Figure 11 depicts the protocol.

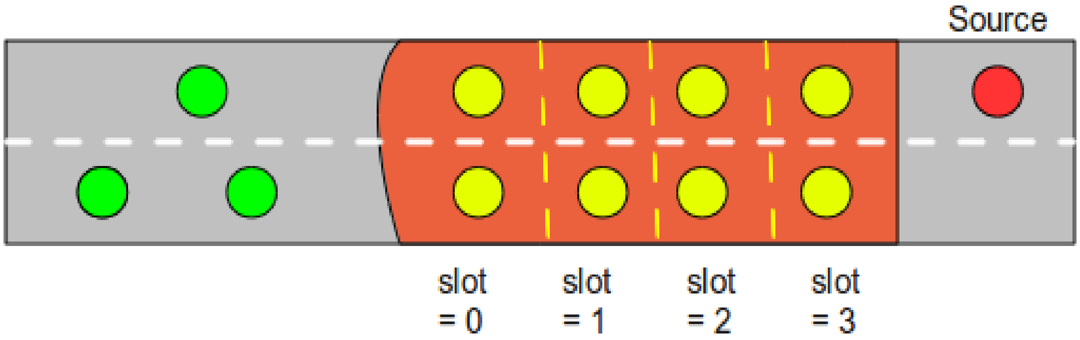

Figure 11 – Slotted p Persistence Scheme

As seen in figure 11, the source is on the right side. After it transmits report, each vehicle will calculate its corresponding cell index. The delay timer is set by the following formula.

$$Ts_{ij} = S_{ij} \times D_{ij}$$

$$S_{ij} = Ns \times \left(1 - \frac{D_{ij}}{R}\right)$$

Where D_{ij} : Distance between node i and j

R : Transmission radius of broadcaster

Ns: Maximum number of slots

S_{ij} : Slot index

Ts_{ij}: Delay time

According to the formula, the vehicles will know which cell it belongs to and they will set the delay according to the cell index properly . In the sample, vehicles on left most side (cell = 0) which are furthest away from the source rebroadcast immediately with probability p as soon as they get the message. Meanwhile, other vehicles on the other cells would set their timer depending on their respective cell number. If they hear the redundant message while their timers are still counting down, it means that some vehicles have relayed the message already. In response, they will simply cancel the timer stopping their attempt to retransmit. In contrast, if their timers have expired, it means that no one has successfully relayed the message. It could happen by many reasons such as:

- There are no vehicle on the previous cell
- Two or more vehicles on the previous cell decided to relay the message. Unfortunately, these messages are collided to each other
- Some vehicles on the previous cell decided to relay the message. Unfortunately, the messages are collided to other traffic.
- All vehicles in the previous cell decided not to retransmit.

Regardless of the reasons, if the delay timer of the vehicles are expired, they will retransmit with probability p. This process will go on for every other cells.

In order to assure that there will be some nodes who relay the message, there is a backup plan in slotted p persistence model. Any node decides not to retransmit must set its delay timer to (cell + 1) * slot_time meaning that I will try retransmitting again in the next slot time. However, this time, the transmission probability will be set to 1, a 100% probability. For examples, node A who is located in cell index 0 decides not to retransmit. It will set its delay timer to be expired in cell index 1 slot time. If, however, this timer has expired, it will certainly retransmit the report.

While this backup approach seems to assure the existence of relaying hop, it also increases the chance of collision. In any subsequent cells, if a node in the previous cell decide to join the contention, there is an increasing chance of collision because of the increasing node density. Furthermore, nodes from the previous cell have 100% chance of retransmit. Apparently, this will drastically increases chance of collision or in a better case, more redundant messages.

Another concerning issue with the slotted p persistence approach is the timer which is implemented in the application layer. Once the timer has expired, the message must be certainly released. In many cases, when two or more nodes decide to retransmit based on the same application timer delay, a collision might not happen. This statement is true because when any packet reaches MAC layer, there will be another timer waiting for counting down. This timer is a well known IEEE 802.11 backoff timer. The backoff timer duration depends on the number of congestion window which will be selected randomly. Therefore, the chance of collision is less. In addition to duration, the congestion window will stop counting down when it detects any packet transmission. Thus, if two node decides to transmit packets at the same time but with different congestion window, one node will completely receive the full packet of the other node before it even transmits its packet. In case of slotted p persistence scheme, this means that even if a node receives the redundant message completely in the MAC layer, it will continue transmit more redundant messages because the control timer is not implemented in the MAC layer and there is nothing it could do to stop sending more redundancy packets.

Problems with original slotted p persistence protocol

The p persistence model has many potential problems.

1. Wasted alloted slot: the allotted time slot will be reserved from the furthest one first. However, if there is no vehicle in previous cells, the time slot will be wasted for free.
2. Large size message contention: nodes will compete to send large size report which could easily cause collision. Also, the large number of redundant report means more wasted bandwidth since the report itself is large.
3. Backup plan will cause collision likeliness or more redundancy: when a node decides not to retransmit, it will delay its timer for one full slot as a backup plan. In case, there is no node retransmit, this node will retransmit in the next slot time. However, this will clearly increase the chance of collision in the next slot.

3.2 Proposed protocol design

3.2.1 Overview

As mentioned, the proposed protocol is based on RTB/CTB [1] and slotted p persistence [7]. We would like to achieve the reliable transmission by RTB/CTB. However, we do not want to spend too much time in multiple iterations when the vehicle density is high as in the original protocol. Thus, the jamming signal is only used as a tool to notify all hidden nodes to remain silent during report transmission and nothing more. Thus, we can specify the jamming duration to be short fixed period and this value can be static. However, since we do not use jamming signal duration to find the next relaying hop, another process must be done to select the next round winner. Slotted p persistence is the process we chose. However, to initiate the beginning of the next round, instead of sending a whole report, only small size RTB will be sent. Furthermore, by using jamming signal, we can estimate the distance to the closest and furthest node. With this information, there will be no wasted slot since all nodes know a number of slots and a radius that are adjusted. Furthermore, rather than putting a delay timer in the application layer, we will implement the protocol in MAC layer. This way, there will be lesser chance of collision. If the collision happens, it means that both VANET delay timer and Congestion Window (CW) timer are expired at the same time. Finally, unlike the original slotted p persistence where, when a node decides not to retransmit, it will set a delay timer to send in the next slot with probability equal to 1 as backup plan, we do not do so unless the nodes are in the last cell. The reason why we can do this is because the recipients would know what the last cell index is. Thus, unless it is in the last cell, it will know that there is some nodes behind them in the subsequent time slots waiting to retransmit.

3.2.2 Protocol Description

The proposed protocol is based on RTB/CTB [1] and slotted p persistence [7]. The protocol follows the stop below.

1. After waiting for SIFS, the initiator transmits RTB to clear the passage. The source also mark a timestamp what the sending time is.
2. Upon receiving RTB, if it has not transmitted sending jamming signal, it will do so after SIFS time. Unlike original RTB/CTB, this jamming signal duration is minimal because its purpose is to providing clear channel for upcoming report transmission only.
3. When the source first hears the jamming signal, it will calculate the estimated distance to the closest node by the following formula:

$$Distance = \frac{CurrentTime - Timestamp - TxTime(RTB) - SIFS}{2} \times SpeedOfLight$$

4. Once the jamming signal transmission stop, the source will calculate the estimated distance to the furthest node as following:

$$Distance = \frac{CurrentTime - Timestamp - TxTime(RTB) - JammingDuration - SIFS}{2} \times SpeedOfLight$$

5. As soon as the path to transmit the report is clear. The source transmits the report which is suppose to be received by everyone in the designated direction. This report also include the number of slots and the adjusted radius so that there will be no wasted slot.

6. After every node hears the report, the contention period will begin based on slotted p persistence model. However, unlike the original protocol, nodes will contend for transmitting RTB to signaling the beginning of the next round. In addition, the chance of collision is less since we implemented the process in MAC layer where there is another backoff timer which will selected randomly.

7. The backup plan in slotted p persistence will not be adapted unless the nodes' cell index is equal to number of slots which means that it is located in the last cell.

3.2.3 Benefits

1. Eliminating hidden/exposed nodes: using RTB/Jamming provides clear path for the report transmission yielding the reliable transmission where every node will receive a report without any "ensure" retransmission required.

2. Short jamming period: the jamming signal is transmitted in short and fixed period. This will eliminate the variable length duration. Meanwhile, the protocol still achieves the goal of eliminating hidden/expose nodes problems.

3. No CTB, ACK: in the proposed protocol, CTB and ACK are not necessary. Therefore, we could save some bandwidth.

4. No multiple iterations as in RTB/CTB: recall that RTB/CTB will have to re-run the process over and over again if there are two or more nodes sending CTB at the same

time. This could cause long delay if the vehicle density is high. However, the proposed protocol does not follow the same rule. Thus, it will not be a problem.

5. Contention with less chance of collision: since the proposed protocol is based on slotted p persistence model, there will be a contention phase. However, there is less chance that the collision will happen. The contending message is a small size RTB not the full size report. The small size message have lesser chance of colliding with other packets since the transmission time is short.

6. Less redundant message: we implemented the protocol in the MAC layer. After the VANET timer is expired, the backoff window in MAC layer will be selected randomly according to 802.11 algorithm. If the VANET timers of two nodes named node A and B are expired at the same time. Assuming that while node A is waiting for its backoff timer expiration, node B transmits RTB at that instance. Node A would stop its attempt to transmit RTB at that point. On the other hand, this does not applied to original slotted p persistence. If the VANET timer expired at the same time, at least two reports will be generated. Furthermore, if redundant RTB is transmitted, it still consumes less bandwidth than the whole report in slotted p persistence.

7. Smart backup plan: in the original slotted p persistence, the backup plan is to “certainly” transmit the report in the next slot. This will increase the chance of collision in the next slot. In our scheme, the same strategy is applied but only to the vehicles in the last cell. Therefore, the chance of using backup plan is greatly lessen.

8. No wasted slots: since the number of slots and transmission radius are adjusted, there will be no wasting slots which is the time that we wasted for free. For instances, assuming the following parameters; radius = 1,000 and number of cells = 5. This will make the cell width to be 200 meters each. We also assume that the furthest away vehicle is at 400 meters from the broadcaster. In the original slotted p persistence, there will be wasted three slots time. However, this does not happen to the propose scheme.

The node who is 400 meters away from the broadcaster will retransmit RTB immediately because its calculated cell index will be 0.

3.2.4 Message format

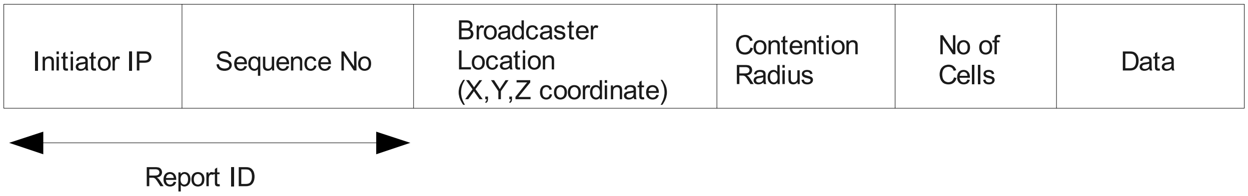

Figure 12 – Report Format

The following are the fields in the report header

- Initiator IP – An IP address of a node who generate the report
- Sequence No. - The sequence number which is increased once for every generated report on each node. Together with the initiator IP, this is the report ID.
- Broadcaster location – The location of the broadcaster in a given round.
- Contention radius – The "estimated" distance to the furthest listener.
- Number of Cells – The expected number of contention cells.
- Data – Other payload data.

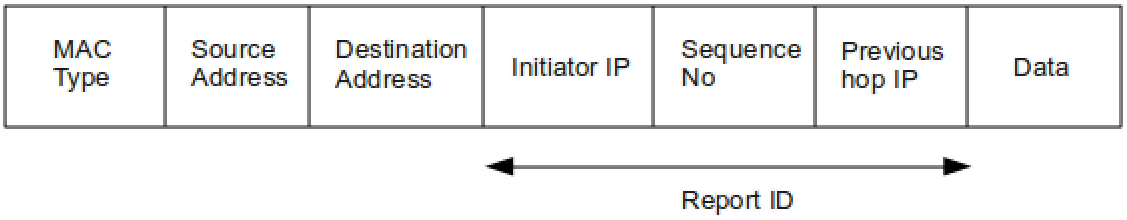

Figure 13 – RTB Format

Below are the fields in the RTB header

- MAC Type – A field indicating packet type (set to RTB type for RTB packet)
- Source address – source MAC address
- Destination address – always set to broadcast address

- Initiator IP – The IP address of the report generator. This field is copied from the report.
- Sequence No. - The report sequence number. This field is copied from the report
- Previous hop IP – The IP address of a node from which the RTB sender hears the report. This field is required to prevent the confusion when hearing RTB. In other words, to make sure that a node will stop its attempt to transmit RTB if and only if it hear a RTB which the previous hop is the same as it has.
- Data – Other payload data

3.3 Protocol summary

Table 1 – Protocol comparison

Characteristics	RTB/CTB	Slotted p persistence	Proposed
Reliable transmission	Yes, with RTB/CTB pair, the hidden/exposed nodes problem shall be eliminated	No	Yes, with RTB/Jamming signal pair, the hidden/exposed nodes problem shall be eliminated
Nodes contend to transmit	CTB	Report	RTB
Multiple attempts in a single round	Yes, if there is a CTB collision, the process must be repeated	No	No
Probability based	No	Yes	Yes
Implement in what layer	MAC	Application	MAC
Require extra messages / cooperate with other layers	Yes	No	Yes
Contention is based on	Cell index	Cell index	Cell index
The precise number of cells is known	No	No	Yes, by using jamming signal, the broadcaster can estimate the furthest and the closest nodes distance.

3.4 Protocol limitations

There are still some limitation in the proposed scheme such as:

1. Integration to MAC layer – the proposed protocol relies heavily on MAC layer integration. Therefore, the MAC layer must be built with VANET broadcasting in mind. This requires MAC layer to have special rules just for one certain type of application. However, this should be feasible because the upcoming VANET MAC standard, IEEE 802.11p, is designed specifically for VANET. Therefore, having special rules for curtain VANET applications should be practical.
2. Jamming signal limitation – In the proposed protocol, we use the jamming signal duration to estimate the distance to the closest and the furthest nodes by the propagational delay. However, this might not be feasible in real world implementation because hardware might not be able to process swiftly enough in the very short duration of propagational delay. Yet, this is in-line with IEEE 802.11 QoS standard, which uses the duration of the blackout jamming signal to determine the QoS level of a network node.

4. Simulation

We have conducted a simulation experiment to measure the performance matrices. We used ns-2 (Network Simulator Version 2) [18] to simulate the network. In order to add VANET broadcasting capability, we have modified some parts of the original ns-2 source code. Three protocols were simulated and compared the results. These protocols are slotted p persistence, RTB/CTB and the proposed protocol.

4.1 Network topology

The network topology is a 4 lanes freeway which is actually a portion of I-10 freeway in Florida state. There were a lot of format conversions before we can get the road topology ready for ns-2 usage. Below are the steps.

1. Originally, the road is in a shapefile format obtained from Florida Department Of

Transportation website [19] .

2. This shapefile was modified using Quantum GIS program [20] to select only a portion of a freeway.
3. This modified shapefile was converted to SUMO (Simulator of Urban Mobility) [21] format by the tools provided by SUMO program itself.
4. From SUMO format, TranS tool [22] converted into ns-2 ready map. In addition, the number of vehicles and the vehicle speed are also defined using TranS program.
5. We have a ns-2 map that we can specify traffic, connections and other simulation parameters.

4.2 Simulation scenario

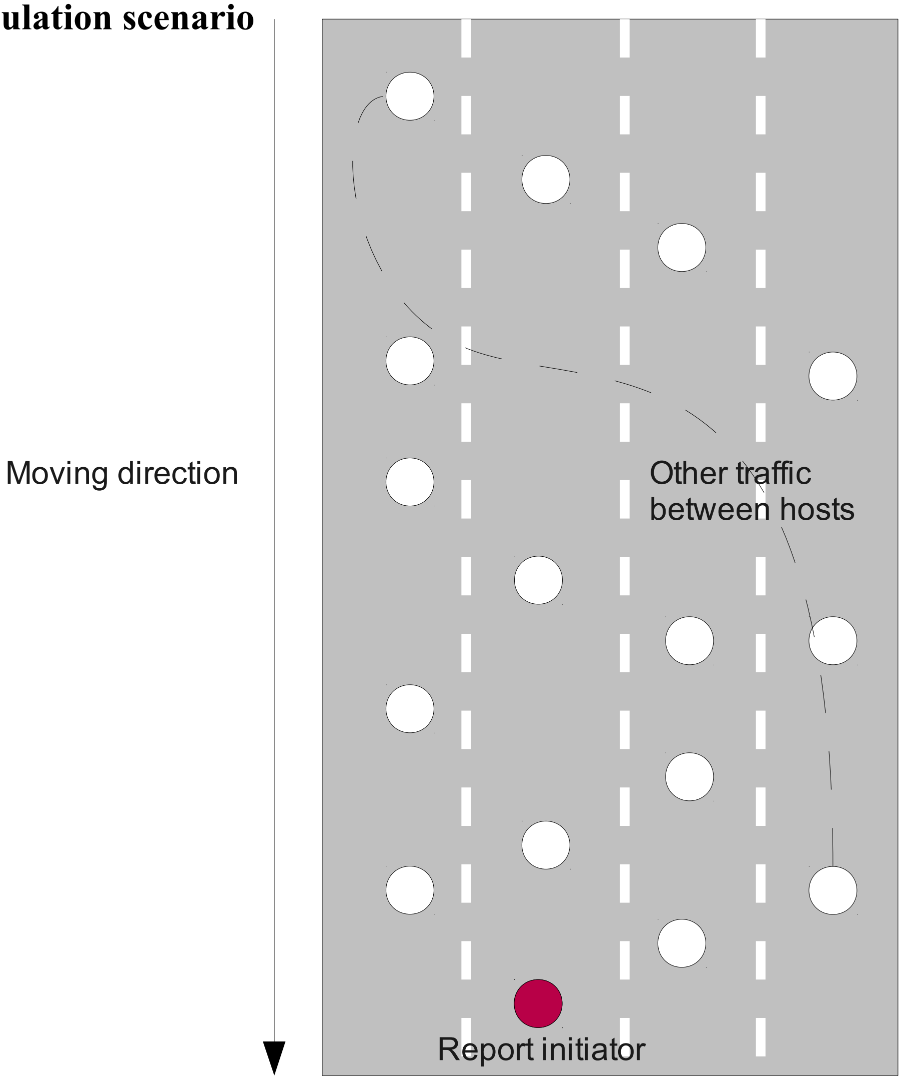

Figure 14 – Simulation scenario

As can be seen from figure 14, the topology is a 4 lanes free way road. Please note that, unlike the figure, the road is not a straightforward line. A vehicle leading other vehicles in front is the report initiator. In addition, there are also some background traffic between other pair of vehicles. These connections are there to give more realistic scenario.

4.3 Input parameters

The following parameters were adjusted in the simulation.

1. *Number of vehicles* – this parameter adjusts the vehicle density on the road
2. *Maximum speed* – the maximum speed of a vehicle on a given road
3. *Number of background connections* – as mentioned in previous section, there are background connections in the scenario. This number of connections will be varied. In addition, the traffic sender and receiver are selected randomly to ensure randomness in our simulation.

4.4 Measurement matrices

The following matrices are measured:

1. *Bytes usage* – The actual number of protocol related bytes transmitted. This number includes every protocol messages and the report. For instances, all transmitted RTB, CTB, ACK and report will be added up to this parameter.
2. *Number of recipients* – The number of vehicles who successfully receive the report. These are nodes which were notified the accident.
3. *Report collisions* – The total number of report collisions.
4. *Other collisions* – The total number of other protocol packets collisions such as RTB, CTB and ACK.
5. *Time spent* – The total time spent to propagate the report to the last recipient. This parameter is defined as the time gap between when the initiator broadcast the report and when the last recipient successfully retrieve it.

4.5 Default parameters

The following table is the default parameters value in our simulation.

Table 2 – Default parameters setting

Parameters	RTB/CTB	Slotted p persistence	Proposed
MAC	Based on IEEE 802.11a		
Transmission Radius	1,000 meters		
Number of contention cells	5		Varied
Cell width	200 meters		
Slot time	1 ms	0.0046395 s	
Jamming duration	1ms * SlotIndex	None	1 ms
Relaying probability	None	0.5	
Link layer queue	50		
Queue	Priority Queue		
Routing protocol	AODV		
Background traffic	Stream type: Constant Bit Rates (CBR) Transport layer: UDP Bit rates: 256 kbps Packet size: 512 bytes		
Wireless channel model	Two ray ground		
Antenna	Omni antenna		
Number of vehicles	Varied (300 nodes by default)		
Maximum speed	Varied (80 miles/hr by default)		
Number of background connections	Varied (3 connections by default)		

5. Result

5.1 Slotted p persistence vs RTB/CTB vs proposed protocol

5.1.1 Varied vehicle density

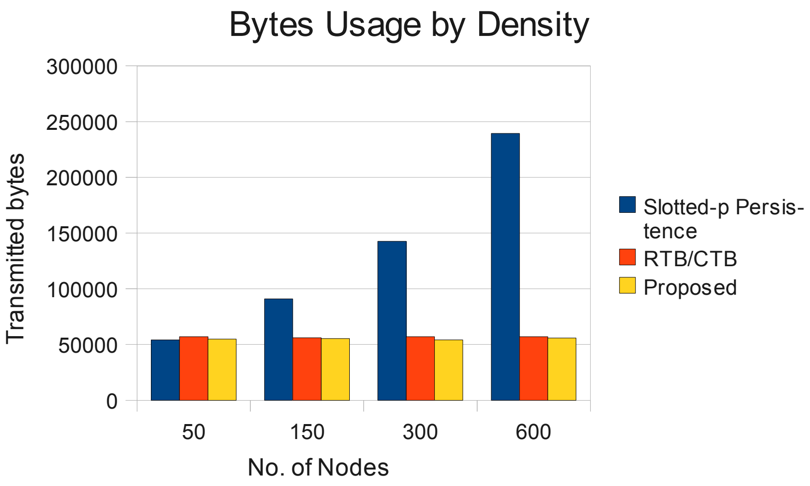

Figure 15 – Byte usage by vehicle density

According to the result shown in figure 15, the slotted p persistence schemes spent the most number of bytes. This is because nodes contend to transmit a big size report. When there is a transmission redundancy, the number of bytes spent will be rapidly increased. In addition, the byte usage number is proportional to the number of vehicles or vehicle traffic density. This is because there is likeliness that more number of nodes transmit the report because of the increasing number of vehicles.

On the other hand, both RTB/CTB and proposed protocol did not spend much number of bytes usage as slotted p persistence did. Since both protocols have each node contends sending small size packet, when there is a transmission redundancy, it will not affect much to the total bytes spent. For RTB/CTB, this contending message is CTB while the proposed scheme is RTB and both messages are small size MAC packets. However, the proposed scheme adapts slightly less number of bytes spent. This is because the proposed scheme does not use ACK and CTB packets as original RTB/CTB does. Additionally to that, the proposed protocol does not have a CTB iterations round, the repeating contention process when there are collisions, as RTB/CTB has.

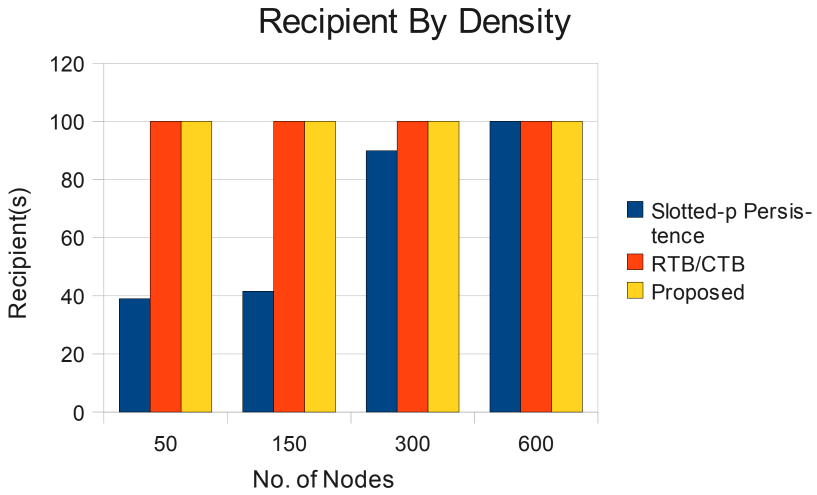

Figure 16 – Number of recipients by density

In term of the number of recipients, both RTB/CTB and the proposed protocol always demonstrate 100% of the report receivers. The fact behind this is because both protocols are reliable. Using of jamming signal eliminates the hidden/expose node problems offering reliable report transmission. On the other hand, this does not apply to slotted p persistence scheme where report transmission can be interfered with other traffics. One interesting thing we can observed from the result is when the number of density grows higher, the reliability of slotted p persistence is also increased. Why? We believe that, when the density is low, the number of potential listeners of a single broadcast is also lower and the distance between the listeners and the broadcaster is increased. This increases the probability that no one will ever hear the message because 1) there is less number of listeners. 2) the distance is greater and it will be more vulnerable to hidden/exposed nodes problem. When this happens , the report propagation will be stopped at that point.

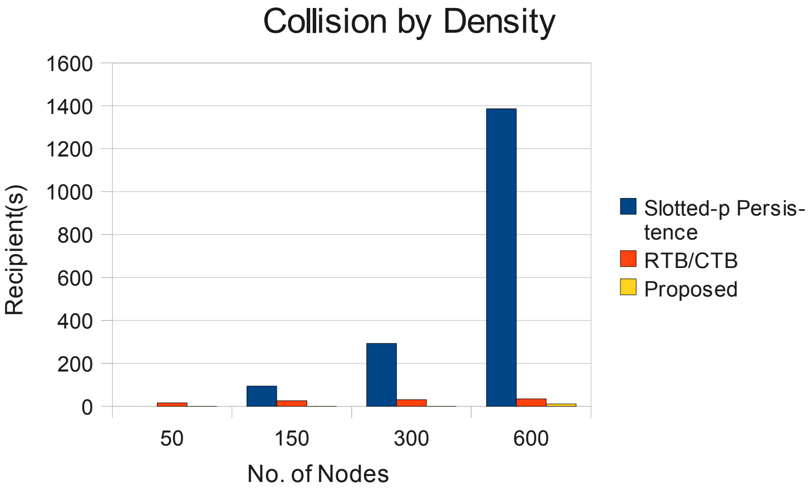

Figure 17 – Number of collisions by density

The number of collisions result showed what we had expected. Slotted p persistence scheme exhibited very large number of the collisions. Due to the contention of report transmission, the number grows quickly when the density is increased because of the number of contenders. On the other hand, both RTB/CTB and proposed scheme have very few collisions number because of the their transmission reliability.

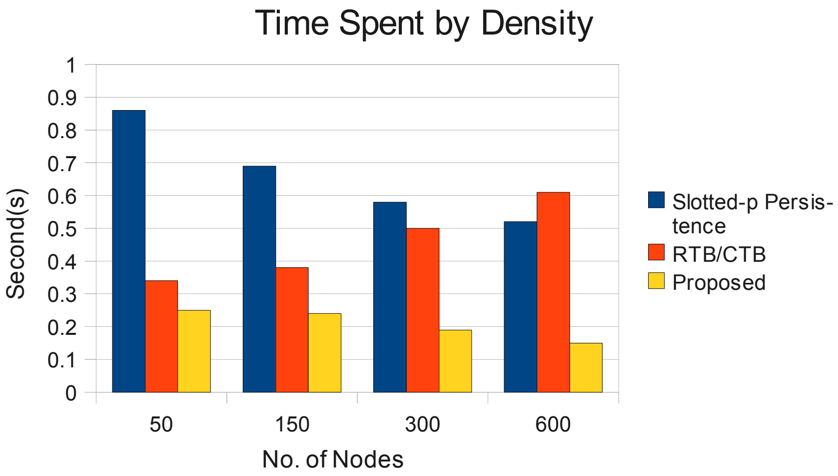

Figure 18 – Time spent by density

From figure 18, the result is pretty interesting. For slotted p persistence and proposed protocol, the amount of time spent is decreased when the vehicle traffic is more dense. The reason is, when the vehicle density is higher, there are more listeners of a single report transmission. Therefore, the number of required transmission rounds to reach all nodes is reduced resulting in less time spent. On the other hand, this is an opposite for RTB/CTB. In RTB/CTB scheme, more vehicle density leads to more CTB contention rounds which, in turn, results in longer time spent.

Comparing three protocols together, slotted p persistence spent the longest amount of time. In slotted p persistence, each contention slot requires longer time than jamming slot since the slot duration must includes the time interval necessary to transmit one packet including DIFS, average CW time and propagational delay. On the other hand, jamming slot requires only the propagational delay. Furthermore, there are also wasted slots utilized by none. All of these reasons contributes to the large amount of time duration spent. For RTB/CTB, the time spent is less than slotted p persistence due to much smaller slot duration. However, when the node density is high, the performance in term of propagational duration is lower than slotted p persistence. The reason is as mentioned in previous paragraph, the increasing of CTB contention rounds. Proposed protocol exhibits the best number. It performs better than RTB/CTB because it does not have a CTB contention iterations. Also, the jamming duration is also reduced to the minimum interval possible. When comparing to slotted p persistence, it demonstrated much better even if the contention slot duration is the same. This is because there is no wasted slot like slotted p persistence has.

5.1.2 Varied vehicle speed

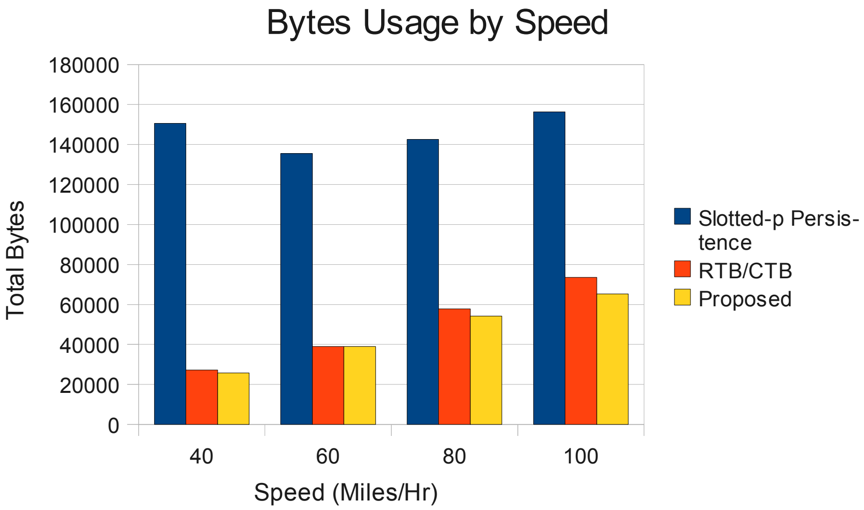

Figure 19 – Bytes usage by speed

When the average vehicle speed is increased, all three schemes generates more bytes into the network. When vehicles moving with fast speed, the gap between vehicles are greater. Therefore, the density is lower. With the same reason as the time spent by vehicle density, the number of required report transmission is increased and that reflected to the total bytes usage.

Again, slotted p persistence exhibited the worst performance because of the large size report contention. The proposed scheme showed a slightly better performance than RTB/CTB because no ACK and CTB iterations are required.

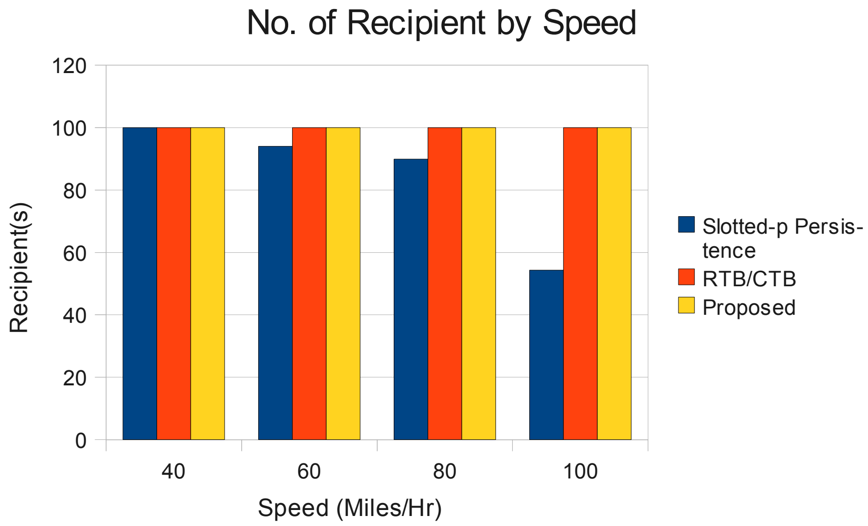

Figure 20 – Number of recipients by speed

When we varied vehicle speed, the result is pretty much the same as we varied the density. For RTB/CTB and the proposed protocol, the number of recipients is always 100% because of reliable transmission. Again, on the other hand, slotted p persistence scheme does not achieve the same thing. As the speed grows, the number of recipients is reduced. The reason is the vehicle density becomes more sparse as speed increases. Thus, the number of listeners is less making more likely that there will be no one who hears the transmission.

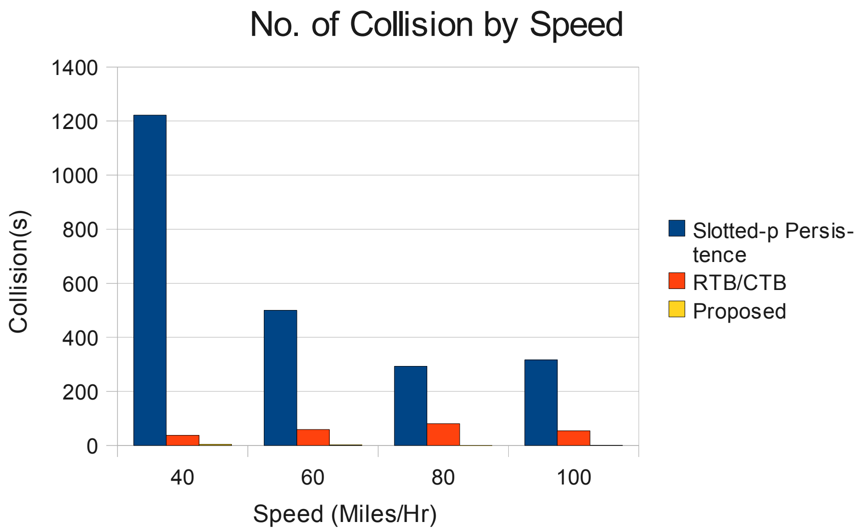

Figure 21 – Number of collisions by speed

Referring to figure 21, again, slotted p persistence suffers heavily from the collisions because of unreliable transmission. Nevertheless, the number of collisions is reduced when the speed is increased since the vehicle traffic become more sparse as the speed grows, which, in turn, reduces the number of contenders. The proposed protocol showed the minimum number of collisions with a slightly better performance than RTB/CTB. We believe this is because of lesser number of protocol messages

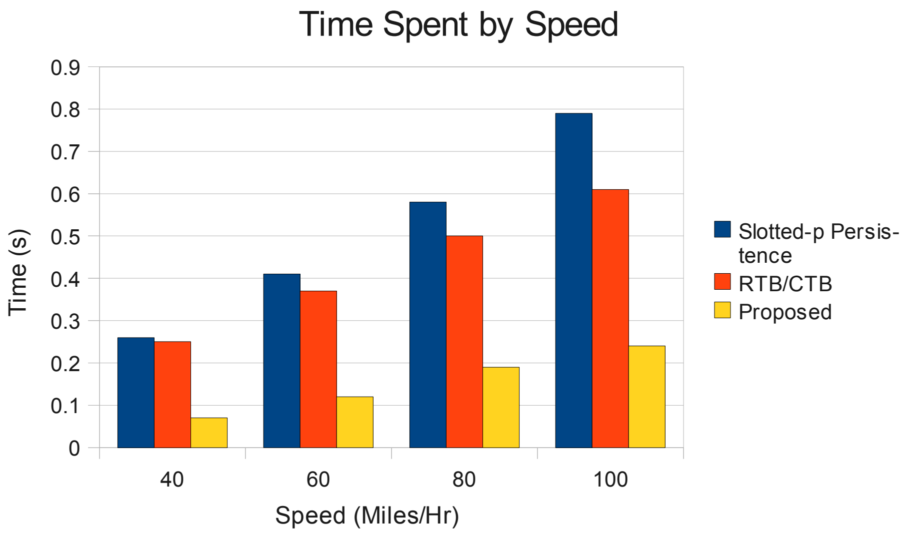

Figure 22 – Time spent by speed

The report propagational time for all three protocols are increasing when the speed grows higher. This is because the network becomes more sparse as the speed increases. Consequently, the number of required transmission round to reach all nodes is increased resulting in higher propagational time. Again, the proposed protocol demonstrates the best performance as it does not have multiple CTB contention as RTB/CTB has or wasted contention slot like slotted p persistence.

5.1.3 Varied background traffic

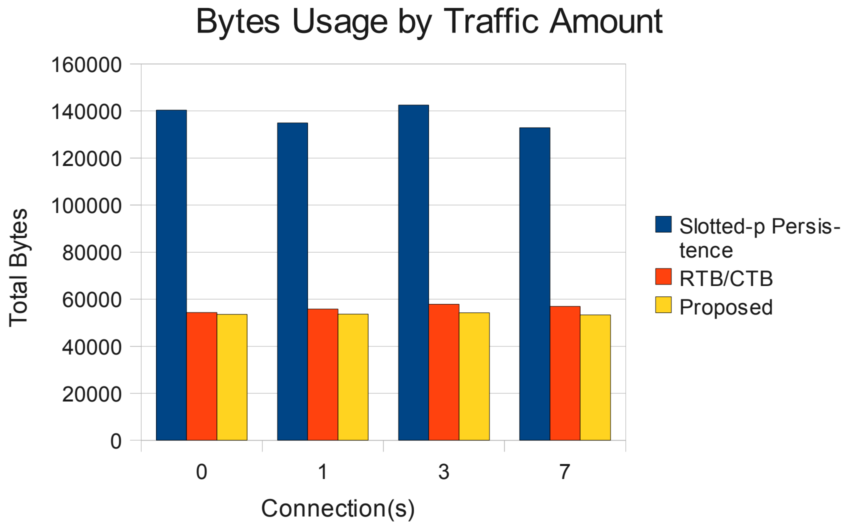

Figure 23 – Bytes usage by background traffic

In term of bytes usage when we adjusted the background traffic, to our surprise, there is not much difference when the parameter changed especially for slotted p persistence. After thoroughly analyzed, the report transmission contenders are likely to hear the transmission of other contenders even if there are background traffic. This is true because they are close to each other. Therefore, the hidden/expose node problem is unlikely to happen. For the other two protocols, the traffic will not affect much because of the jamming signal which will eliminate other interference traffic. As usual, the proposed protocol showed the best performance with the reason as described in previous sections.

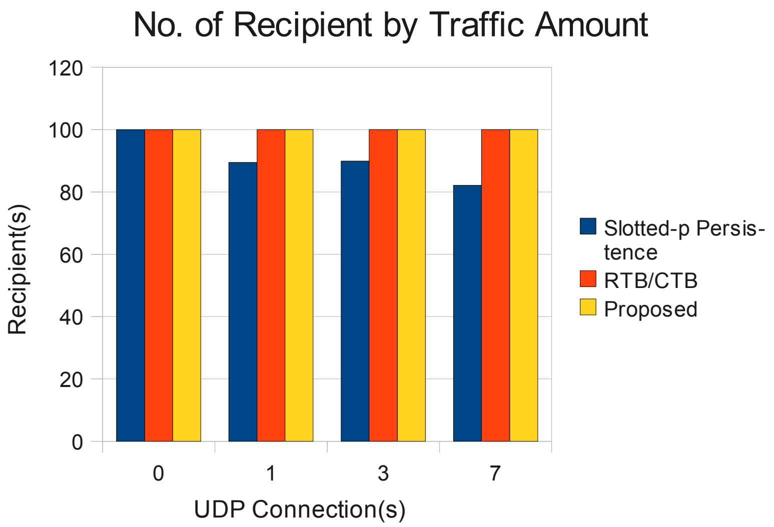

Figure 24 – Number of recipients by background traffic

As expected, RTB/CTB and the proposed protocols still preserved 100% rate of the receivers. Slotted p persistence shows the dwindling of the recipients as the traffic goes up. The reason is because of the background traffic interfering with the report transmission resulting in some nodes cannot hear the report transmission.

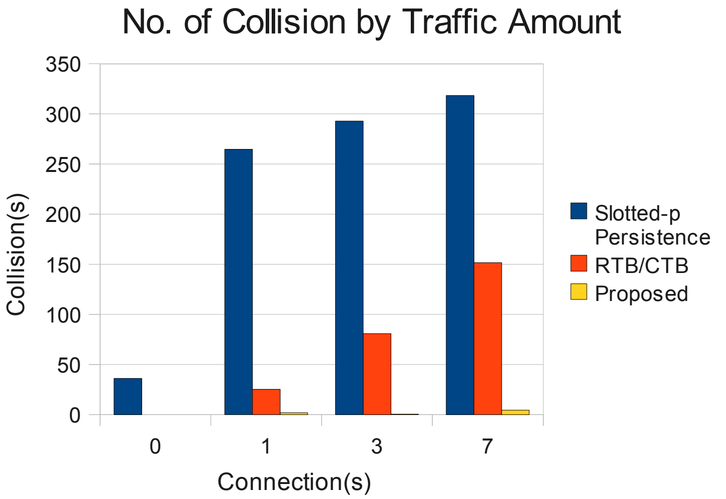

Figure 25 – Number of collisions by background traffic

According to the result, the number of collisions rises up as the traffic increased especially for slotted p persistence. Apparently, since there are more traffic, the likeliness to collide with the report transmission is increased. Thus, this reflects to the number of collisions. Meanwhile, this does not apply to the proposed protocol as can be seen from the result because the path will always be clear.

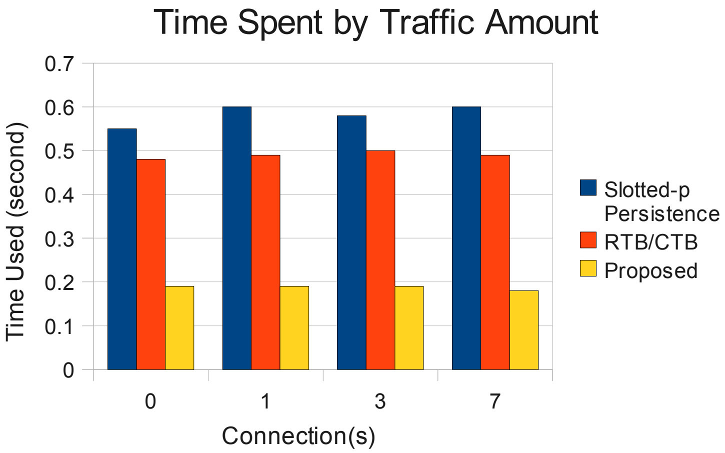

Figure 26 – Time spent by background traffic

The total time spent is not affected by the amount of background traffic regardless of the protocols. We believe that, even in a congested network, RTB messages or reports can get through to reach at least one listener who will response back. Consequently, the protocol will not be delayed and the process is continued normally. Therefore, the time spent will not be affected by this parameter.

5.2 RTB vs CTB

From the previous result set, we found out that proposed protocol provide best performance. However, it is unclear that how better it is from RTB/CTB since it is difficult to see the difference because slotted p persistence protocol showed so large number. In this section, I will give the result set comparing between RTB/CTB and proposed protocol only.

5.2.1 Varied vehicle density

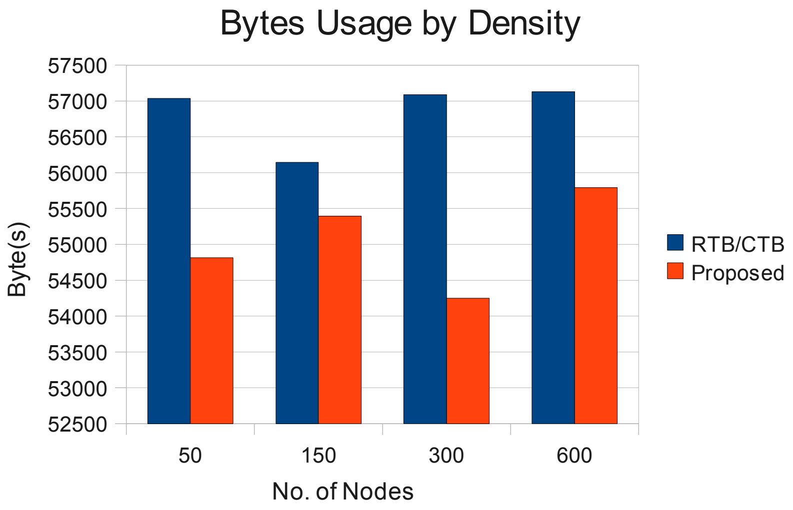

Figure 27 – Bytes usage by vehicle density

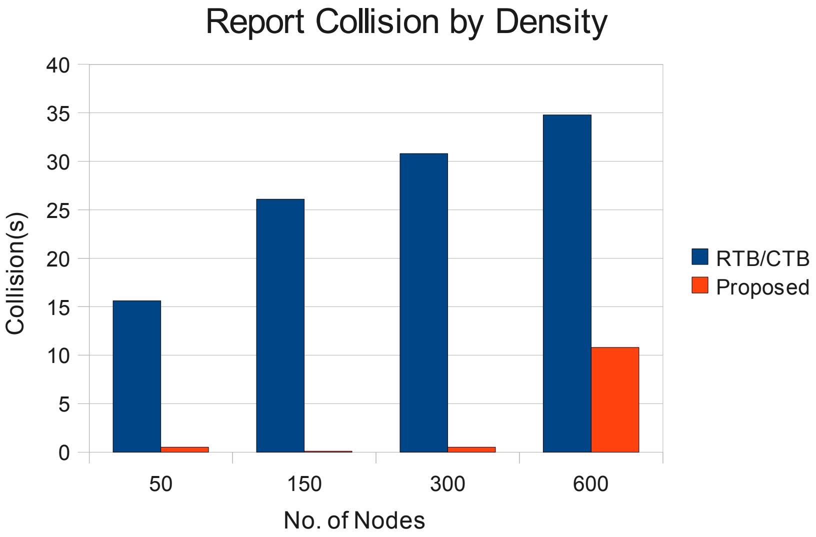

Figure 28 – Report collision by density

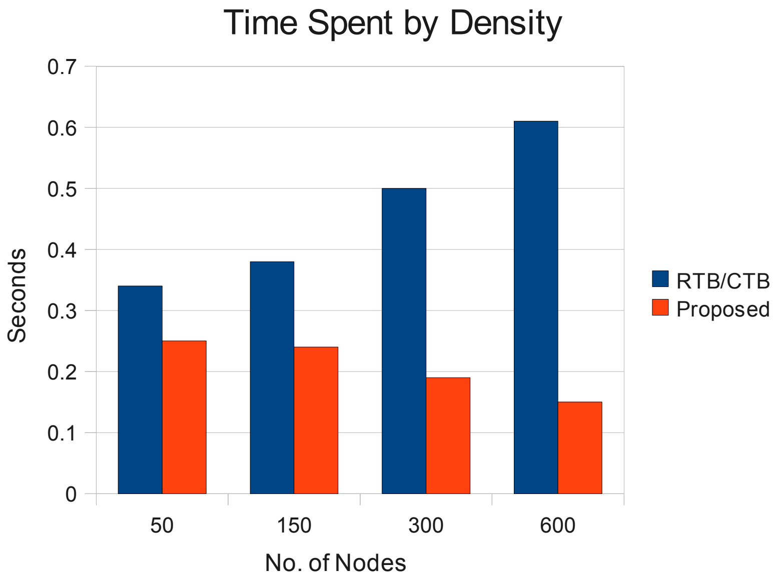

Figure 29 – Time spent by density

Referring to figure 29, RTB/CTB always spent more bytes than the proposed protocol. This is because RTB/CTB requires additional protocol messages such as CTB and ACK while the proposed protocol does not. In addition, CTBs might be sent in multiple contention rounds if there was collisions. This could increase the amount of bytes usage significantly in RTB/CTB protocol.

The number of collisions is increasing as the density is increased. This is because there are more contenders. Nevertheless, the proposed protocol has less number of collisions.

In term of propagational time spent, RTB/CTB spent more time when the vehicle density is increased because more number of CTB contention rounds must be done. In contrast, the proposed protocol use lesser time as the density grows since there will be more listeners in one broadcast round. Regardless of the density, the proposed protocol always spent less time than the RTB/CTB because there is no CTB iteration and this fact becomes more obvious to notice in the high density network.

5.2.2 Varied speed

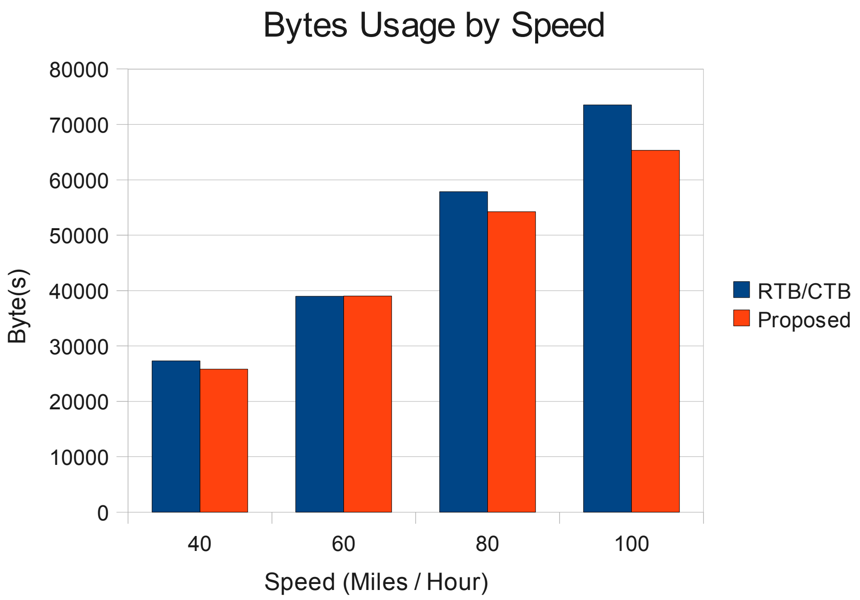

Figure 30 – Bytes usage by speed

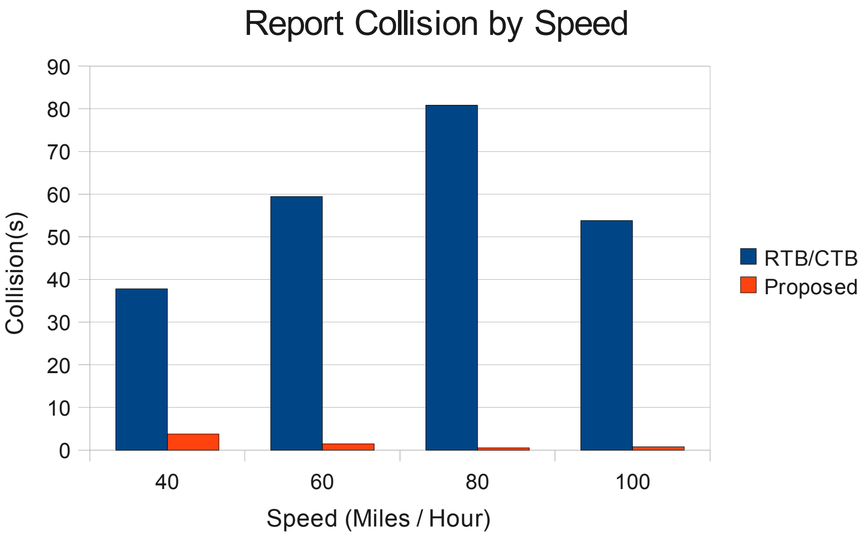

Figure 31 – Report collisions by speed

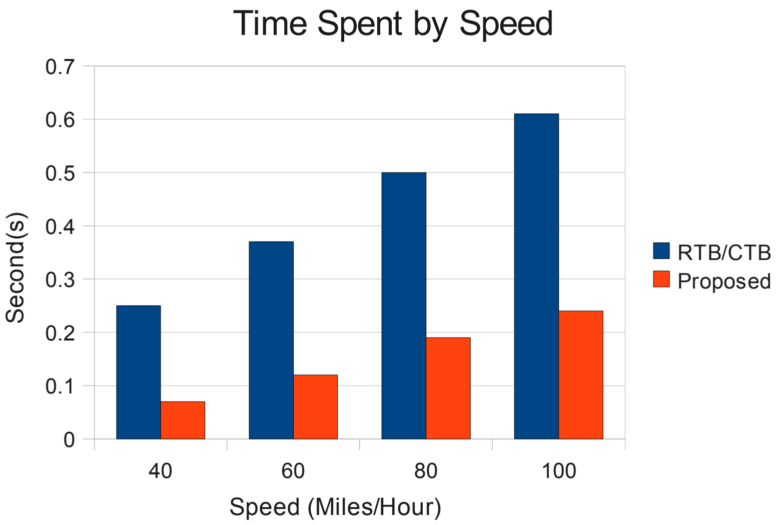

Figure 32 – Time spent by speed

For both protocol, the bytes usage is increased as the vehicle moves faster. When vehicle moves fast, it increases the distance between vehicles. Therefore, it will requires more broadcasting rounds in order to reach every node in the network. Consequently, this increases the number of bytes usage. The proposed protocol utilize less bandwidth than RTB/CTB as the mentioned reason; no ACK, CTB and no CTBs iterations.

For both the collisions and the time spent, the proposed protocol demonstrated better performance. The total time spent is increased when vehicles moving in high speed because the network becomes more sparse resulting in more number of broadcasting rounds. Also, the proposed protocol adapt less time because it does not have CTB iterations.

5.2.3 Varied traffic

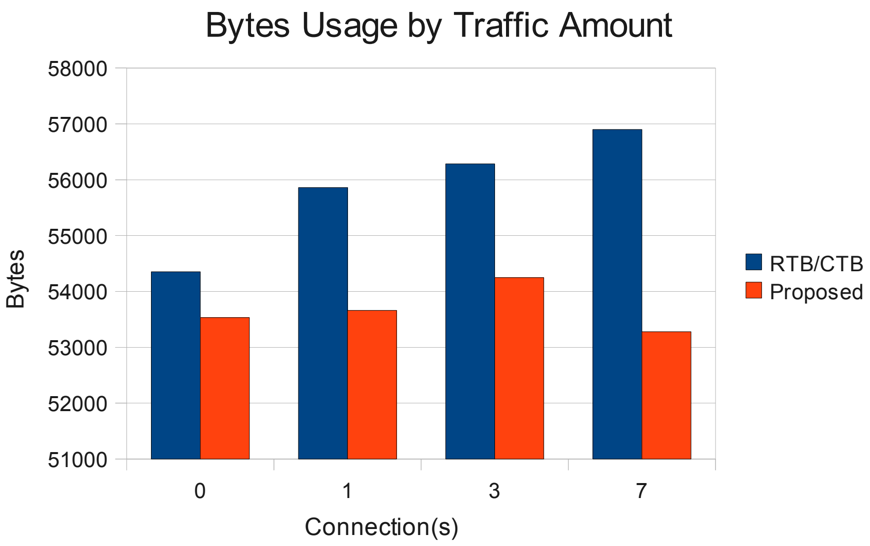

Figure 33 – Bytes usage by traffic amount

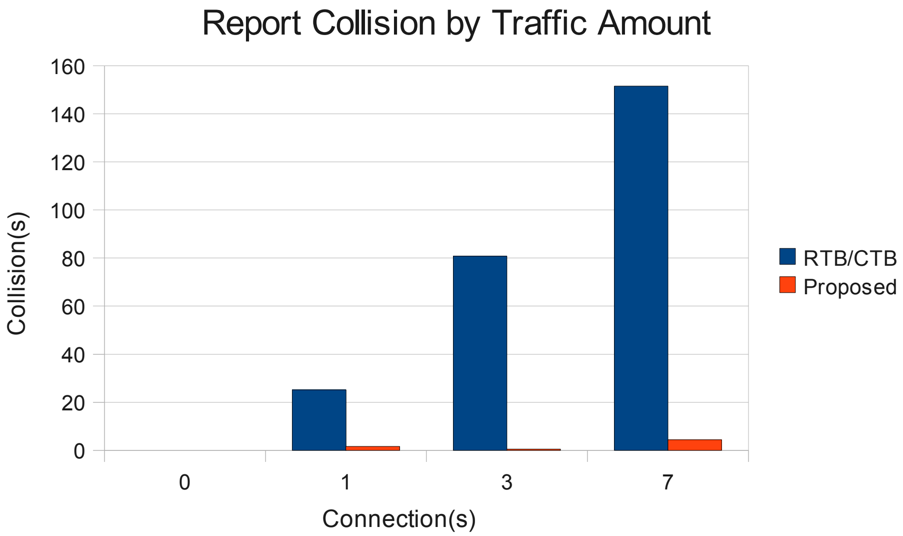

Figure 34 – Report collisions by traffic amount

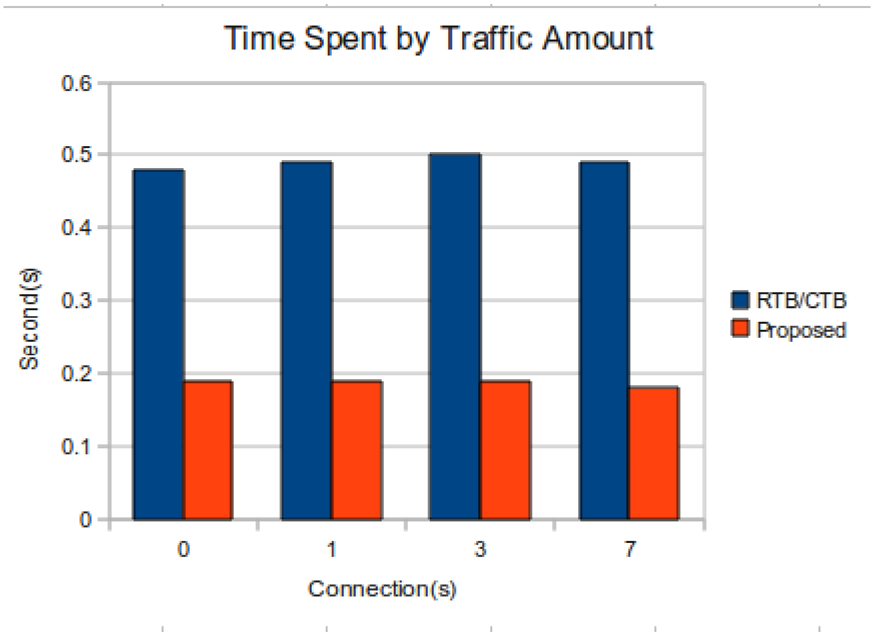

Figure 35 – Time spent by traffic amount

As the number of connections increased, the bytes transmitted by both protocols is also going up. The reason is there is more likely that collisions will happen. Consequently, some contenders will not hear the winner transmission and will transmit more messages into the network. Therefore, more bytes are transmitted to the network. Again, the proposed protocol beats RTB/CTB in term of bandwidth usage by the the reasons mentioned in the previous sections, no CTB iterations. In term of collisions, the proposed protocol showed less number of collisions once again. However,, we do not see any difference in time spent when we adjusted the background traffic amount. We believe that, even in a congested network, RTB message can get through to reach at least one listener who will send back the jamming signal. As long as there is jamming signal, the protocol will not be delayed and the report will be propagated normally. Therefore, the time spent is not affected by the traffic amount. Also, as usual, the proposed protocol spent less time because there is no CTB iterations required.

5.3 Retransmission probability experiment

In the previous result sets, those are the comparison results between protocols which showed that the proposed scheme demonstrated the best performance. However, we use fixed retransmission probability at 0.5 which we do not know whether or not this is the best number. Therefore, we have run another test varying rebroadcast probability just for the proposed scheme only to see if which probability number yields the best performance.

5.3.1 Varied density

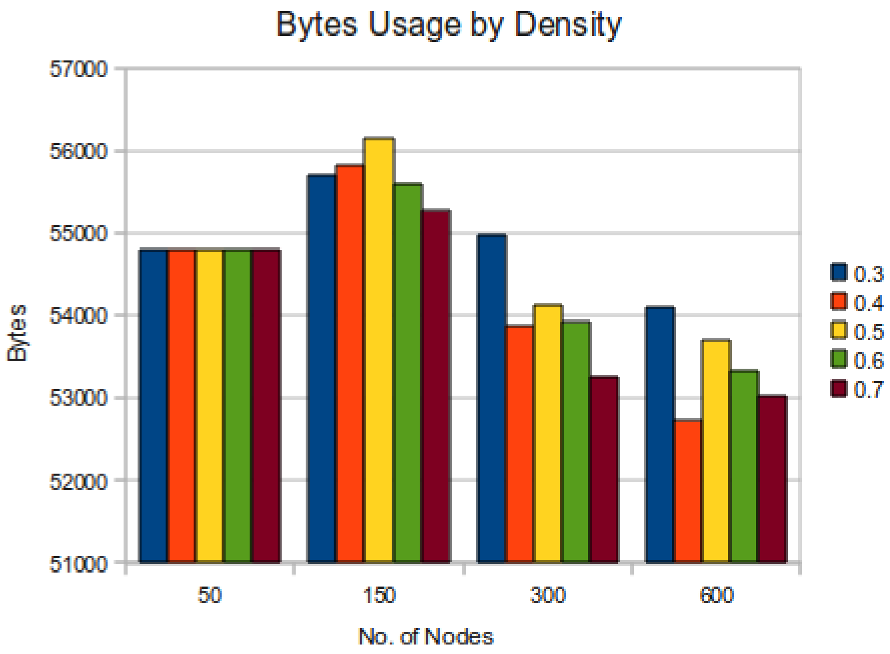

Figure 36 – Bytes usage by density

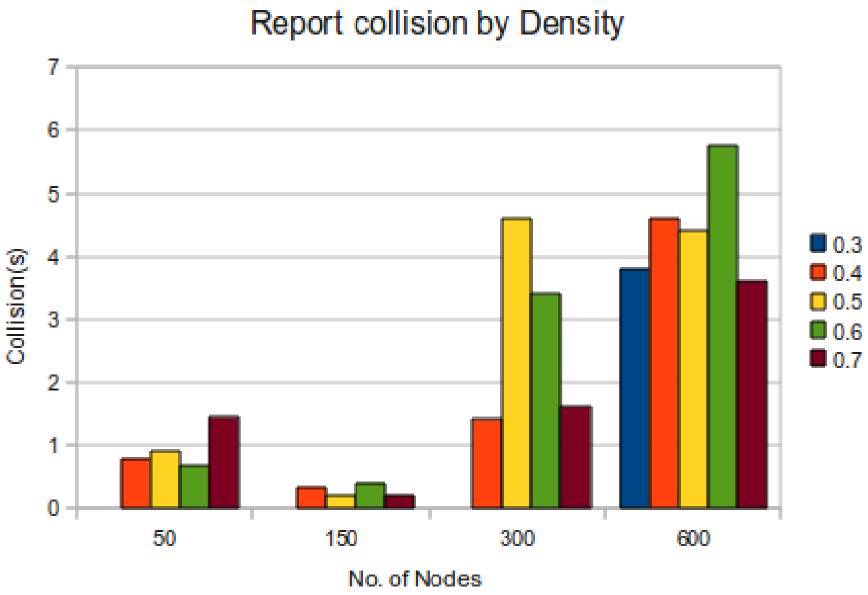

Figure 37 – Collisions of report by density

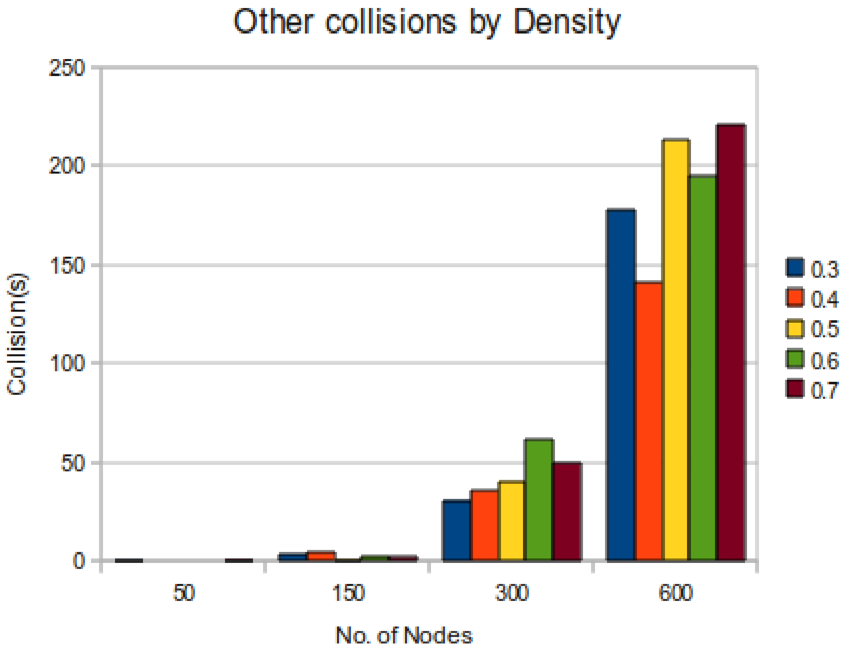

Figure 38 – Other collisions by density

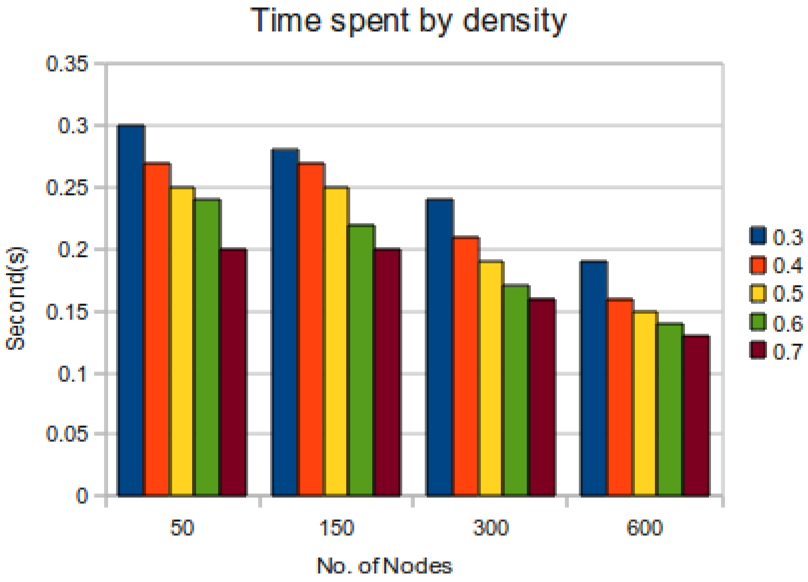

Figure 39 – Time spent by density

When we varied the vehicle density, it is difficult to point out which probability number is the best. In term of bytes usage, the bytes usage amount is shown randomly and we cannot conclude which probabilistic number yields the best. For the number of collisions, as expected, high probability such as

0.7 exhibited high number of collisions than the rest since nodes are more aggressive and are more likely to transmit messages increasing collision chances. This reason explains both report collisions and other protocol messages collisions results. However, in term of time spent, using high retransmission probability reduces overall propagational time since there is likely that nodes in first cell will rebroadcast resulting in less time spent.

5.3.2 Varied speed

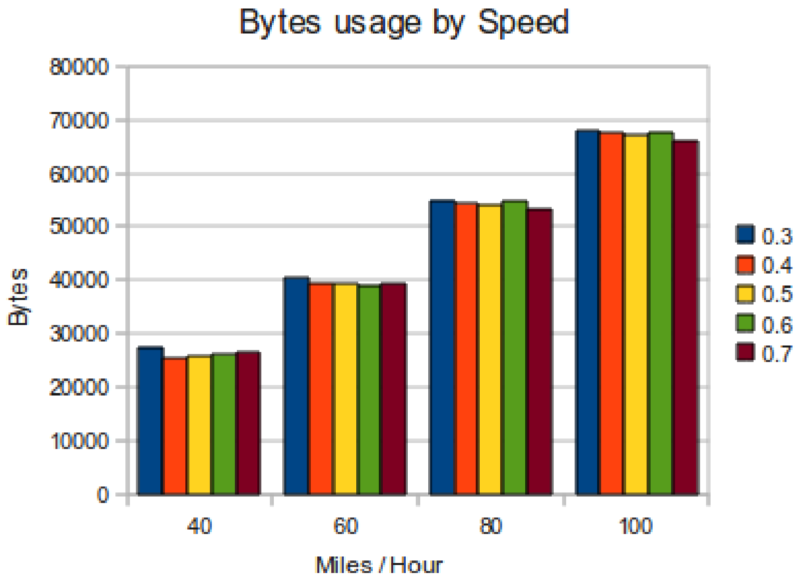

Figure 40 – Bytes usage by speed

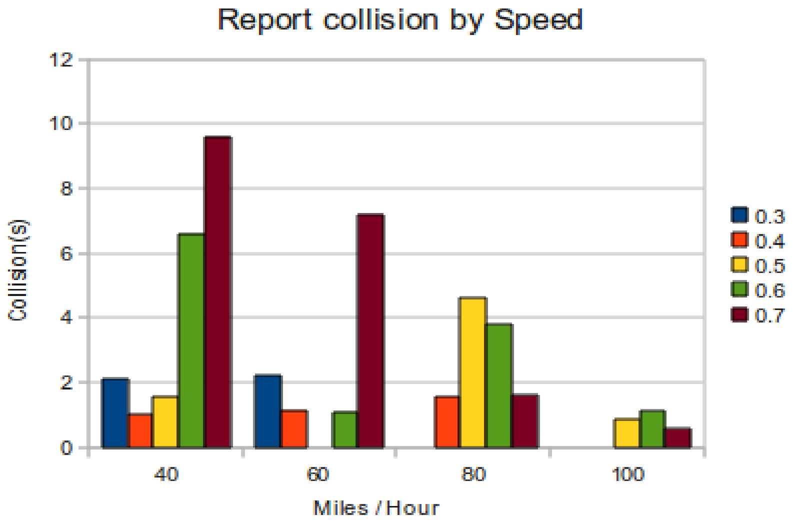

Figure 41 – Collisions of report by speed

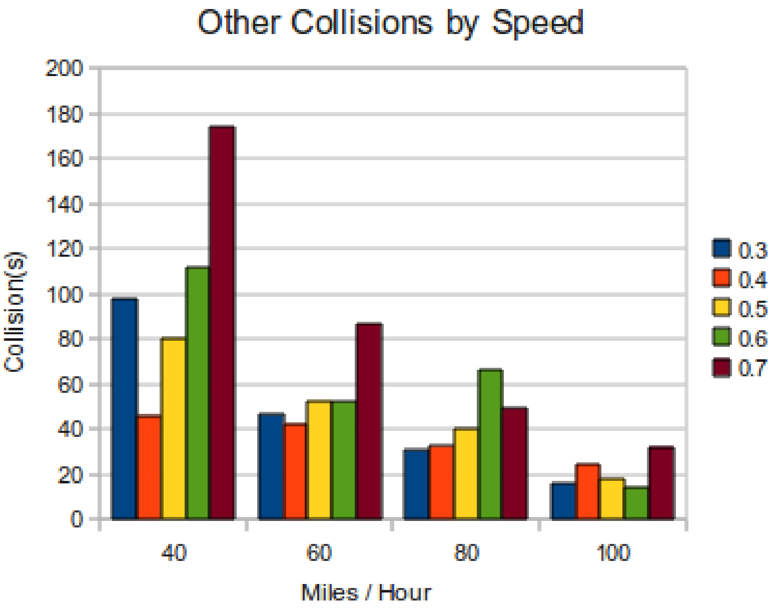

Figure 42 – Other collisions by speed

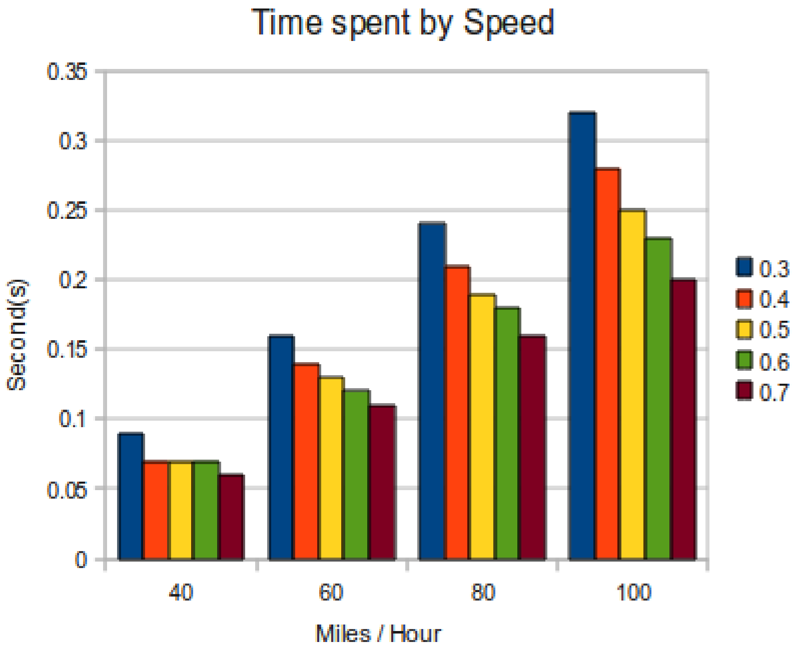

Figure 43 – Time spent by speed

The result when we varied the speed is pretty much as what have already showed. The bytes usage and time spent are increased while the number of collision is decreased as the speed grows. The reason is the same as what we already have explained, vehicle speed increases the distance to each other. Looking at the bytes usage, every testing number gave roughly the same result regardless of the probability value. Again, the high probability gave higher collision rate while it can reduce the total time spent because of the retransmission aggressiveness.

5.3.3 Varied traffic amount

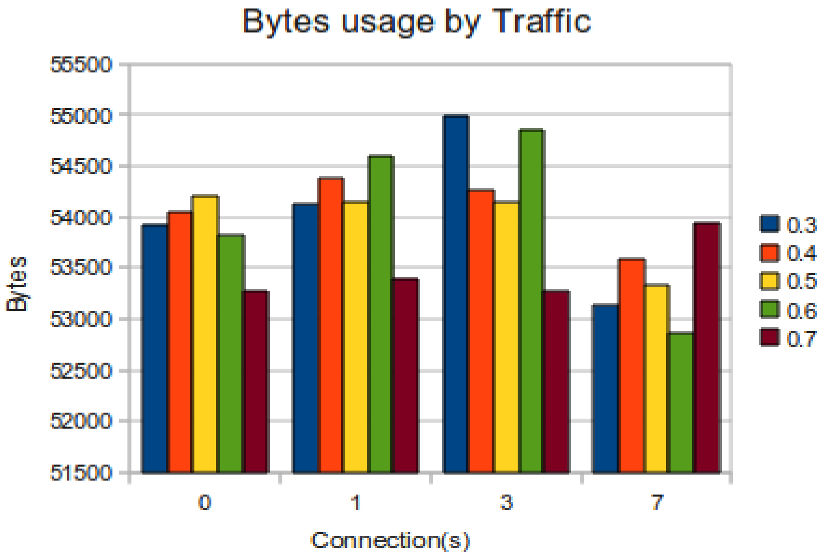

Figure 44 – Bytes usage by traffic amount

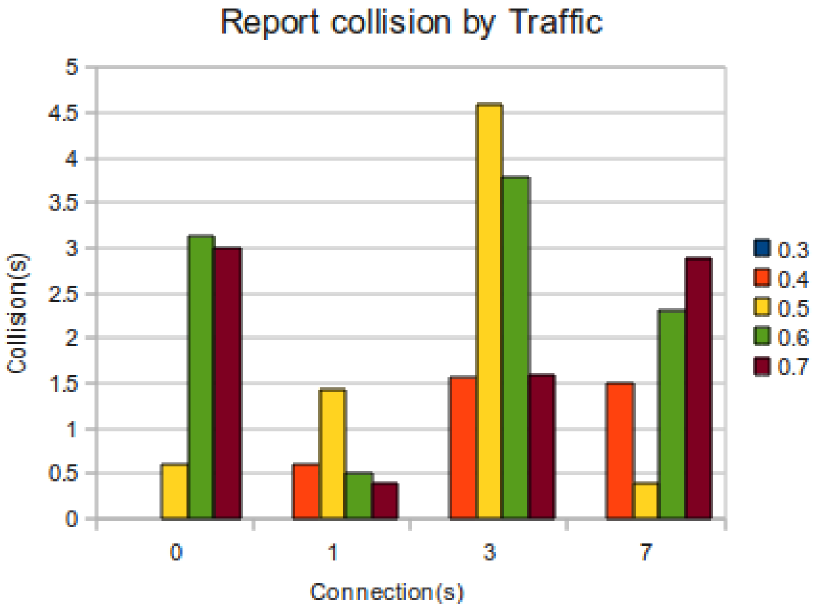

Figure 45 – Collisions of report by traffic amount

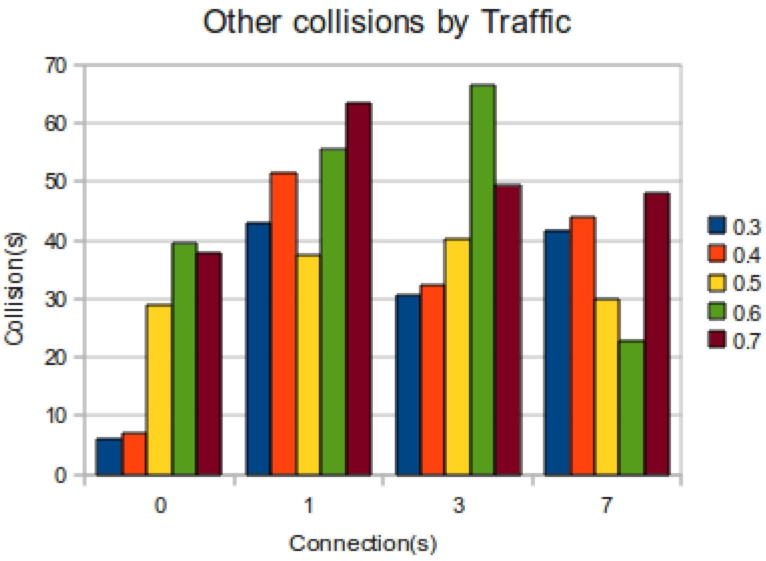

Figure 46 – Other collisions by traffic amount

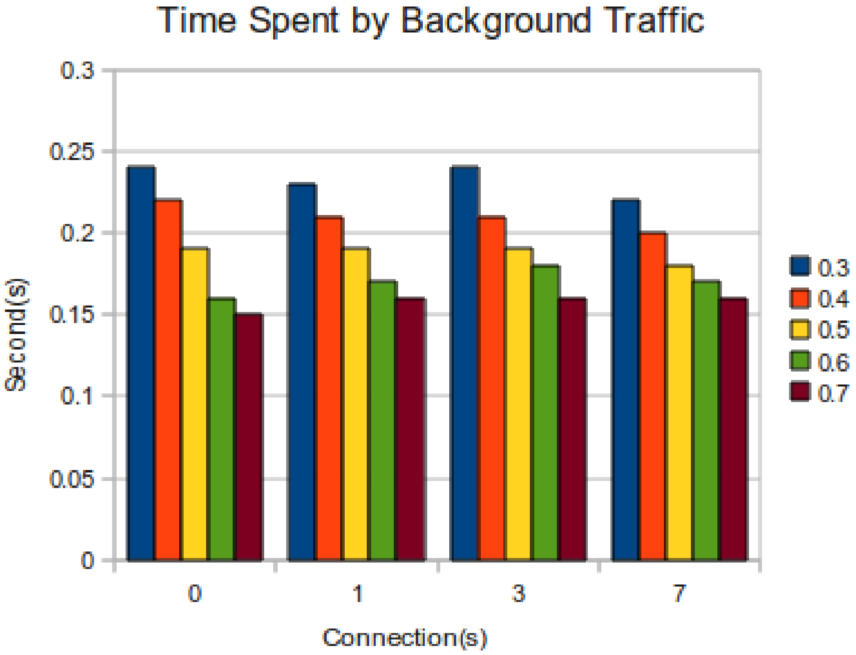

Figure 47 – Time spent by traffic amount

The result set when varied the traffic amount is the same as the rest. The bytes usage result exhibited randomly result set and difficult to point out which probability number is the best. Again, high probability works great in term of time spent but performs poorly in term of number of message collisions regardless of message type.

6. Conclusion and future works

We have proposed a new VANET broadcasting protocol based on slotted p persistence and RTB/CTB schemes. A lot of enhancement was added to the proposed protocol. For instances, there is neither wasting contention slots like slotted p persistence nor CTB iteration like RTB/CTB. Furthermore, the retransmission suppression works much better since the contention timer is embedded in MAC layer. According to the simulation result where we varied vehicle density, speed and background traffic amount, the proposed protocol achieved high reliability and demonstrated better performance than both slotted p persistence and RTB/CTB in every performance matrices including bytes usage, number of collisions and report propagational time. Nevertheless, it is difficult to point out what probability number yield the best performance. While high probability gave better propagational time, it suffers heavily in term of number of collisions. In sum, we cannot conclude what the best probabilistic number is for our proposed scheme.

The future work might include some new ideas such as adaptive probability without using any beacon messages or distance approximation by other methods than jamming signal. Or to the best thing we can think of is providing reliability without using jamming signal since the jamming signal will obviously interfere with other traffics.

7. Appendix

7.1 Network Simulator version 2 (NS-2)

Network Simulator version 2 or ns-2 for short is a very popular choice of network simulator software in an academic world. Ns-2 is a free, open source software written in C++. Originally, ns-2 was developed by many top computer science schools people on earth including, UC Berkeley and Carnegie Mellon. At first, ns-2 is only capable of simulate wired network. However, later on, the wireless function was added to the existing code. In addition to the standard ns-2 version, people around the globe continued to contribute partial or updated source code offering additional functionality such as the ability to simulate new protocols including Voice over IP (VoIP), WiMAX, Video streaming etc. These useful additional patches can be found on Ns contributed page at

http://nsnam.isi.edu/nsnam/index.php/Contributed_Code.

Currently, the latest version of ns is ns-3 (Network Simulator version 3). In ns-3, the whole programming structure have been re-organized to provide much better development environment. However, due to the lack of patches and supports available on ns-3, it is not yet a popular choice of simulator as ns-2 is.

7.2 Simulator of Urban MObility (SUMO)

Simulator of Urban MObility or SUMO for short is a road traffic simulator. Just like ns-2, SUMO is a free, open source software designated to run in Linux environment. In SUMO, one can create roads, vehicles, intersections, buses, traffic lights and a lot more option in the traffic environment. SUMO provides realistic functions such that you can specify the behavior of traffic light, buses routine, vehicle speed etc. In additional to these functions, it also compatible with many existing GIS format such as shapefile, Tiger etc.

7.3 TranS - Traffic and Network Simulation Environment

It is not long until recent years that VANET becomes popular in a research world. Therefore, the ability to simulate realistic VANET scenario is inadequate because most network simulators do not have an option to generate realistic road and vehicle movement model. In response to the problem, TranS was developed.

TranS is a free software written in Java. It is capable of transforming a SUMO vehicle traffic scenario file into ns-2 ready tcl file. From SUMO file, it will read the road structure, vehicle movement, vehicle speed and other parameters in the file and convert these values into ns-2 compatible format. A user is also able to create vehicle traffic from the existing SUMO map file, specify speed, network traffic and other ns-2 parameters at the same time.

References

[1] G. Korkmaz, E. Ekici, and F. Özgüner, "Urban multi-hop broadcast protocol for inter-vehicle communication systems," Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, 2004.

[2] K. Hua and R. Villafane, "A near-optimal broadcast technique for vehicular networks," *2009 Wireless Telecommunications Symposium*, 2009, pp. 1-8.

[3] K. Suriyapaibonwattana and C. Pomavalai, "An Effective Safety Alert Broadcast Algorithm for VANET," *2008 International Symposium on Communications and Information Technologies*, 2008, pp. 247-250.

[4] H. Jiang, H. Guo, and L. Chen, "Reliable and Efficient Alarm Message Routing in VANET," *2008 The 28th International Conference on Distributed Computing Systems Workshops*, 2008, pp. 186-191.

[5] A. Amoroso, M. Ciaschini, and M. Roccetti, "The farther relay and oracle for VANET. preliminary results," *Proceedings of the 4th Annual International Conference on Wireless Internet , ACM*, 2008.

[6] Q. Yang, L. Shen, and W. Xia, "Distributed Probabilistic Broadcasting for Safety Applications in Vehicular Ad Hoc Networks," *Wireless Communications & Signal Processing, 2009. WCSP 2009. International Conference*, 2009, pp. 0-4.

[7] O.K. Tonguz, N. Wisitpongphan, J.S. Parikht, F. Bait, P. Mudaliget, and V.K. Sadekart, "On the Broadcast Storm Problem in Ad hoc Wireless Networks," *BROADNETS 2006. 3rd International Conference*, 2006.

[8] L. Bononi, "A Cross Layered MAC and Clustering Scheme for Efficient Broadcast in VANETs," *Mobile Adhoc and Sensor Systems, 2007. MASS 2007. IEEE Internatonal Conference*, 2007.

[9] B. Bako, E. Schoch, F. Kargl, and M. Weber, "Optimized Position Based Gossiping in VANETs," *2008 IEEE 68th Vehicular Technology Conference*, 2008, pp. 1-5.

[10] N. Balon and J. Guo, "Increasing broadcast reliability in vehicular ad hoc networks," *Proceedings of the 3rd international workshop on Vehicular ad hoc networks - VANET '06*, 2006, p. 104.

[11] D. Shin, H. Yoo, and D. Kim, "EMDOR : Emergency Message Dissemination with ACK-Overhearing based Retransmission ب," *Ubiquitous and Future Networks, 2009. ICUFN 2009. First International Conference*, 2009, pp. 0-4.

[12] M. Li, "Opportunistic Broadcast of Emergency Messages in Vehicular Ad Hoc Networks with Unreliable Links," *Proceedings of the Fifth International ICST Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness*, 2008.

[13] T.K. Mak, K.P. Laberteaux, and A. Arbor, "A Multi-Channel VANET Providing Concurrent Safety and Commercial Services," *Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks*, 2005, pp. 1-9.

[14] S.Y. Ni, Y.C. Tseng, Y.S. Chen, and J.P. Sheu, "The broadcast storm problem in a mobile ad hoc network," *Proc. of the 5 th annual ACM/IEEE international conference on Mobile computing and networking*, vol. pp, pp. 151-162.

[15] A. Nasri, M. Fathy, and R. Hajisheykhi, "A Cross Layered Scheme for Broadcasting at Intersections in Vehicular Ad Hoc Networks," *2009 International Conference on Future Networks*, 2009, pp. 13-17.

[16] P. Lai, X. Wang, N. Lu, and F. Liu, "A reliable broadcast routing scheme based on mobility prediction for VANET," *2009 IEEE Intelligent Vehicles Symposium*, 2009, pp. 1083-1087.

[17] O. Tonguz, N. Wisitpongphan, F. Bai, P. Mudalige, and V. Sadekar, "Broadcasting in VANET," *Proc. of IEEE Mobile Networking for Vehicular Environments*, vol. pp, pp. 7-11.

[18] "the network simulator - ns-2."

[19] "Florida TranStat Geographic Information System (GIS)."

[20] "Quantum GIS Project."

[21] ""Simulation of Urban MObility" (SUMO)."

[22] "TRANS - Realistic Simulator for VANETs."

[23] “Status of Project IEEE 802.11 Task Group p”