Cooperative Volunteer Protocol to Detect Non-Line of Sight Nodes in Vehicular Ad hoc Networks

Khaled Alodadi, Ali H. Al-Bayatti

Software Technology Research Laboratories (STRL)
The Gateway
De Montfort University
Leicester, England, LE1 9BH

khaledodadi@live.com, alihmohd@dmu.ac.uk

Nasser Alalwan

Computer Science Department, King Saud University,
Kingdom of Saudi Arabia,
Riyadh, 11451, P.O Box 2454

nalalwan@ksa.edu.sa

Abstract

A vehicular Ad hoc Network (VANET) is a special type of Mobile Ad hoc Network (MANET) application that impacts wireless communications and Intelligent Transport Systems (ITSs). VANETs are employed to develop safety applications for vehicles to create a safer and less cluttered environment on the road. The many remaining challenges relating to VANETs have encouraged researchers to conduct further investigation in this field to meet these challenges. For example, issues pertaining to routing protocols, such as the delivery of warning messages to vehicles facing Non-Line of Sight (NLOS) situations without causing a broadcasting storm and channel contention are regarded as a serious dilemma, especially in congested environments. This prompted the design of an efficient mechanism for a routing protocol capable of broadcasting warning messages from emergency vehicles to vehicles under NLOS conditions to reduce the overhead and increase the packet delivery ratio with reduced time delay and channel utilisation. This work used the cooperative approach to develop the routing protocol named the Co-operative Volunteer Protocol (CVP), which

uses volunteer vehicles to disseminate the warning message from the source to the target vehicle experiencing an NLOS situation. A novel architecture has been developed by utilising the concept of a Context-Aware System (CAS), which clarifies the OBU components and their interaction with each other to collect data and make decisions based on the sensed circumstances. The simulation results showed that the proposed protocol outperformed the GRANT protocol with regard to several metrics such as packet delivery ratio, neighbourhood awareness, channel utilisation, overhead, and latency. The results also showed that the proposed CVP could successfully detect NLOS situations and solve them effectively and efficiently for both the intersection scenario in urban areas and the highway scenario.

1. Introduction

Drivers response to an emergency siren is normally one of delayed reaction, which is mainly attributed to their lack of understanding and information about what to do and where to turn to (left or right). Thus, the reaction time they require to make a decision is longer than usual. Subsequently, this situation leads them to make wrong moves and decisions, thereby possibly resulting in fatal accidents on the road or some delay in the arrival of the emergency vehicle. As the emergency vehicle has limited time to reach its destination, the chances of collision with other vehicles are normally higher in the wake of an emergency. The term *emergency vehicle* in this paper means any vehicle authorised to use a siren such as police vehicles, fire engines, or ambulances, which are required by law to follow the traffic rules and regulations [1]. However, the latter is used to distinguish other vehicles on the road that do not have any authority to sound an emergency siren while moving on the road.

According to a report issued by the German Federal Highway Research Institute, the risk of an emergency vehicle being involved in serious accidents is eight times higher, and four times higher for fatal accidents [2]. Similarly, the risk of being involved in property damage is 17 times higher. This data clearly shows

that any mistake made by the driver of an emergency vehicle on the road can have disastrous consequences [3]. It has been reported that erroneous driving by emergency vehicle drivers can lead to 60% of accidents, out of which 30% are caused by faults made by other drivers driving vehicles on the road. Around 40% of such accidents take place at road intersections [4].

Furthermore, wrong decisions made by drivers of other vehicles can precipitate delays in the arrival of emergency vehicles at their destination points, in which could in turn have serious implications for the patients being rushed to hospitals in the case of ambulances or lead to criminals being pursued by police vehicles escaping. Of late, Intelligent Transportation Systems (ITSs) have been applied to augment surface transportation systems. Several ITS projects have been initiated in the USA, Japan, and Europe. These systems employ Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications to relay emergency messages to target vehicles within short times to enable the drivers to make quick decisions and avoid collisions with either emergency vehicles or other vehicles. The underlying network utilised by these communications (V2V) is termed a vehicular ad-hoc network (VANET), which is responsible for delivering the information in a timely and cost-efficient way [22][21][20].

However, there is no comprehensive communication protocol that can reduce the latency in the dissemination of messages by VANETs. The major challenge in this dissemination of messages is related to how to shorten the time period between the time of emergency event and the time of delivery of warning messages to other vehicles to avoid collisions. Maintaining coverage of all vehicles within the target range in terms of dissemination of messages is another issue. The high density of vehicles on the road at intersections means that the dissemination of messages is normally challenging. Other vehicles, buildings, and foliage can be major obstacles in the way of the dissemination of warning messages from an emergency vehicle to the target vehicles. This stresses the need for continuous research to detect the number of obstacles in the dissemination

of messages, which could ultimately be expected to result in the reduction of collisions because of the timely receipt of messages and quick decision-making processes of the drivers.

Moving vehicles can constitute obstacles with different compositions, densities, speeds, and shapes, and this can give rise to additional non-line-of-sight (NLOS) situations, which can affect the communication of location information and updates among neighbouring vehicles. This could prevent the exchange of information between vehicles about the speed, location, direction, etc., and hence fatal accidents could happen on the road. Although a multi-hopping technique could be used to disseminate the message beyond the transmission range, unfortunately hidden nodes, interference, and packet-collisions can terminate the dissemination process during multi-hopping mediated broadcasting. Furthermore, the higher utility of wireless resources mediated by unnecessary re-transmissions is another problem associated with the employment of multi-hopping techniques for message broadcasting. These challenges associated with multi-hop broadcasting have diverted the focus to using a Co-operative Volunteer Protocol (CVP) to achieve reliable, effective, and efficient multi-hop message broadcasting. Most of the solutions proposed in this context rely on direct Line of Sight (LOS), which uses a Roadside Unit (RSU) or cellular networks to overcome the NLOS issue for disseminating the messages to vehicles close to each other. This shows that existing solutions are infrastructure based and require infrastructure for the dissemination of information among neighbouring vehicles. However, the major challenge lies in realising infrastructure-less communication of messages to vehicles in close proximity.

Therefore, this work involved the development of an effective CVP based on a VANET for warning message dissemination among emergency vehicles. Firstly, this is intended to reduce the number of NLOS situations by assuring the broadcast of emergency messages to each and every node within the coverage zone by utilising volunteer nodes to relay messages to those nodes lying outside

the coverage zone. Secondly, this is expected to help reduce the dissemination latency, thus delivering the warning messages to the target nodes efficiently and in a timely manner, all of which play a fundamental role in designing safety applications for emergency vehicles. Thirdly, the storm problem in message dissemination will be addressed using CVP. Finally, the proposed CVP aims to enhance the features of existing protocols, such as robustness, reliability, and coverage. The simulation tool EstiNet was used to evaluate the effectiveness of the proposed routing protocol in comparison with other protocols being used in the area of transmission of warning messages from emergency vehicles and other vehicles. EstiNet was selected as a simulation tool because of its special features, relatively easy manipulation of features, and its ability to simulate the various parameters and conditions at the intersection of roads.

The remainder of this paper is organised as follows. Section 2 introduces existing work that has been carried out in the field of non-line of sight and the definition of NLOS and when these situations can arise. An overview of the proposed context-aware architecture is given in section 3. The proposed Co-operative Volunteer Protocol for detecting NLOS is explained in section 4. Section 5 proposes the system simulation and validation, and the conclusion is given in Section 6.

2. Related work

Vehicle communications are vulnerable to signal interference as the vehicles travel in different environmental conditions. Physical objects and construction sites on the sides of the road (i.e., buildings, trees, and area topography) can interfere with radio signals and prevent proper communication. Moving objects such as trucks can also interfere with communication between vehicles and could block a drivers visual and communication line of sight, creating a non-line-of-sight (NLOS) state, which can lead drivers to make poor judgments when changing lanes or merging onto a highway. NLOS can be either intentional or unintentional. Intentional: malicious attacks, fake position. Unintentional: physical obstacles (trees, buildings) or moving obstacles (trucks, e.g., in an

industrial area). The proposed work considers unintentional NLOS based on either physical or moving obstacles [5][6][7].

Many researchers [5][6][7][8][9] covered the challenges that might cause or affect the NLOS issue from different perspectives in communication domains, the main challenges include signal strength, communication range, signal blockage, authentication, and signal interference. Similarly, in location verification and detection domains, the main issues include verification of position of the nodes, reliability of message senders, availability, and issues concerning with the quality and integrity of service. Other Several researchers have proposed location verification techniques for hidden nodes in wireless networks. These approaches are generally categorised into two classes, depending on the underlying principle of propagation models: distance information methods for location verification (infrastructure-based verification methods) and distance-free approaches (infrastructureless-based verification methods). A distance-based method such as the ECHO protocol for location verification that is proposed by [10] is based on the challenge response.

The location verification methods developed by [11] [12] verify the location of the hidden node by calculating the distance of three detecting nodes from the hidden node or target node. Similarly, [13] proposed a scheme that uses some reference points around the hidden node to verify the claim of the target node (node under NLOS). The second category of location verification the distance-free approach is based on the principle of utilising the distance information; and location claims are verified through location-measuring techniques, such as the angle of the radio signal communicated between the detecting and the target nodes [14]. However, in comparison with the distance-based technique, distance-free schemes do not require the exact estimation of the location of the hidden node, which is why they do not face the issue of localisation, especially in a sparse network. Therefore, the application of distance-free schemes (infrastructureless) is more beneficial than the distance information-based schemes [15][16]. Figure 1 shows the different approaches of position verification. This work is based on cooperative verification, which uses an infrastructure-less environment.

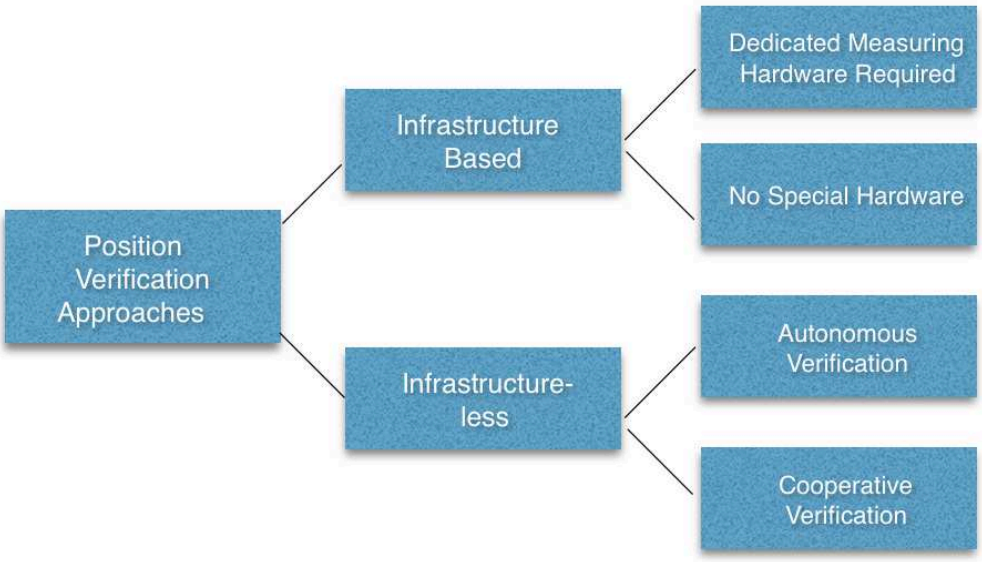

Figure 1: Position Verification Approaches

To conclude, the main difference between previous work and the proposed work is that, this current research attempts to tackle the issue of signal blockage by the obstacles during the communication of messages to other vehicles under NLOS situations i.e. hidden node. This paper also tries to verify the location of the hidden node so that the warning message can be delivered to avoid a fatal collision on the road. This is achieved using a context-aware cooperative volunteer protocol with higher success rate delivery of warning messages, reduced latency, accurate neighbour awareness and location verification, better channel utilisation, and better response time. Full details of the results and analysis are available in section 5.

3. OVERVIEW OF CONTEXT-AWARE ARCHITECTURE

The proposed architecture utilises a five-layered context-aware system to enhance the intelligence, awareness of surrounding events and cost effectiveness of the overall system. The On Board Unit (OBU) architecture that is presented

in this paper is used in every vehicle, in addition to a Warning Message Byte (WMB), which consists of warning message data packets that inform the system about upcoming emergency events to enable it to respond to these events separately. The architecture is a top-down approach consisting of three main phases. The three main phases interacts seemingly. First phase, represents the sensing layer where raw data is gathered from different components. Second phase is represented by three layers (raw data retrieval, processing and storage unit). Third and final phase is represented in the action layer, where the dissemination unit takes place. The next subsections describes each component in details and how they interact with each other to reach the goal of the system by reducing the delays for emergency vehicles crossing an intersection and avoiding the storm broadcast problem in order to prevent fatal accidents from occurring. The proposed architecture consists of three main phases as follows:

3.1. Sensing Phase

This phase represents the sensing layer in the framework (i.e., the proposed architecture) of the context aware system. It represents the gate of the system and is responsible for gathering the raw data collected by different sensors for processing in the next phase. There are two types of sensors: physical sensors, and virtual sensors.

Global Positioning System (GPS)

The ability to perform exact positioning is critical for a VANET. This is achieved by using GPS to obtain general information about the vehicles such as their speed, location, and direction [17]. GPS represents the physical sensor that collects physical data.

Information Data Sensor (IDS) IDS is a virtual sensor that gathers data from a software application and only operates in an emergency event by adding an emergency header to the packet (WMB). Processing emergency broadcasts separately has the advantage of reducing the delay and enabling a faster re-

sponse than processing it together with other broadcasts. In addition, this helps to address problems caused by broadcast storms. These sensors detect an approaching emergency vehicle by using their unique frequency channel. This sensor also captures information from surrounding nodes and processes the information quickly to avoid the unnecessary accumulation of packets in certain areas of the network, which could lead to a broadcast storm.

Route Information Table (RIT) Each vehicle has its own RIT, which is a table that contains all the information for the surrounding vehicles (speed, location, and direction), in order to send it to the processor to determine whether there is a NLOS condition, by using an NLOS Detecting Unit which is discussed later. RIT is used in two different scenarios: intersections and road disseminations (highway).

3.2. Thinking/Processing Phase

The processing phase is the core of the proposed system, representing three layers in the framework of the context-aware system, namely raw data retrieval, processing, and storage. This phase directs the system as to what to do next by interpreting and converting the raw data into action, to start the CVP to notify hidden vehicles about upcoming events.

Location and Direction Unit (LDU) This unit is responsible for obtaining the general information about the emergency vehicle that sent the dissemination broadcast by indicating location and direction. GPS is used to help to obtain this information. This unit is located in the OBU of the normal units, and will detect the location and direction of the emergency vehicles.

Emergency Dissemination Unit (EDU) This part is responsible for receiving the raw data from the Information Data Sensor (emergency sensor) in order to interpret it. Receiving serious emergency broadcasts separately ensures it has high priority and enables it to respond faster. This unit contains one unit

as follows:

Intersection & Road Coverage Control Unit (ICCU) Crossing an intersection is one of the most dangerous situations for emergency vehicle mobility, because it is critical to cross it safely without any delay that would affect the vehicle arrival time. Using RIT will help to control intersections by knowing the position of every vehicle in the network. This unit processes road dissemination to detect if there is a NLOS situation. The unit is responsible for detecting the hidden node in either an intersection or highway.

Storage Unit This part represents the system database, which stores any information that needs to be accessed and processed by other components in the system, which will enable the system to react suitably in the next phase. This unit contains the maps for both roads and intersections in the following unit:

Road & Intersection Maps The main storage unit contains pre-loaded maps of the roads and all the intersections. After obtaining the direction information about vehicles in the system, this unit will help to use the maps to determine where every vehicle is heading and try to prevent fatal accidents from occurring.

Non-Line of Sight Detecting Unit (NLOS-DU) This part is responsible for all the tasks in the system. It is the core part of the proposed architecture, and is responsible for detecting whether the vehicle is in NLOS or not by comparing its RIT with that of the emergency vehicle to check whether there is any vehicle in the original RIT (meaning there is a higher chance of it being in an NLOS position). This activates the next phase to ensure that the vehicle responds appropriately. The processing in this unit decides whether to send the packet to the Directional Dissemination Unit (DDU) to either start the voluntary process or ignore it (which is explained in the third phase).

3.3. Action Phase

Once the system has received the raw data and sent it to the processor, it reaches the final stage, which is the fifth layer in the framework of the context aware system. This phase represents the result of the system by sending a directional message to the intended vehicles to notify them about the upcoming situation (figure 2). Then the CVP triggers the result by sending the WMB to notify the hidden nodes about the upcoming events. Section 4.1 explains this mechanism in detail.

Directional Dissemination Unit (DDU) This unit sends the voluntary package (WMB) to the vehicles that are in NLOS conditions after receiving confirmation from the emergency vehicle. Directional dissemination will help to reduce storm broadcasts by allocating the broadcasting to one sender. Finally, figure 2, provides an overview of how the components of the OBU architecture interact with each other.

4. CO-OPERATIVE VOLUNTEER PROTOCOL (CVP)

The main purpose of this protocol is to solve NLOS by using a mediator node, which acts to deliver the warning message to the hidden node in time, and then to reply to the emergency vehicle that it is clear to pass the intersection. Moreover, using CVP is very important in safety applications and requires Non-DTN (Delay Tolerant Network) routing protocol issues to be addressed, because this network is only based on position. In contrast, a DTN-based routing protocol cannot be utilised in this research because of the carry and forward mechanism that cannot be applied in the proposed protocol as a result of the delay that might occur because of this issue.

4.1. CVP Mechanism

As explained earlier, in density networks NLOS situations is a major concern due to obstacles such as buildings, trees or even vehicles. The need of V2V

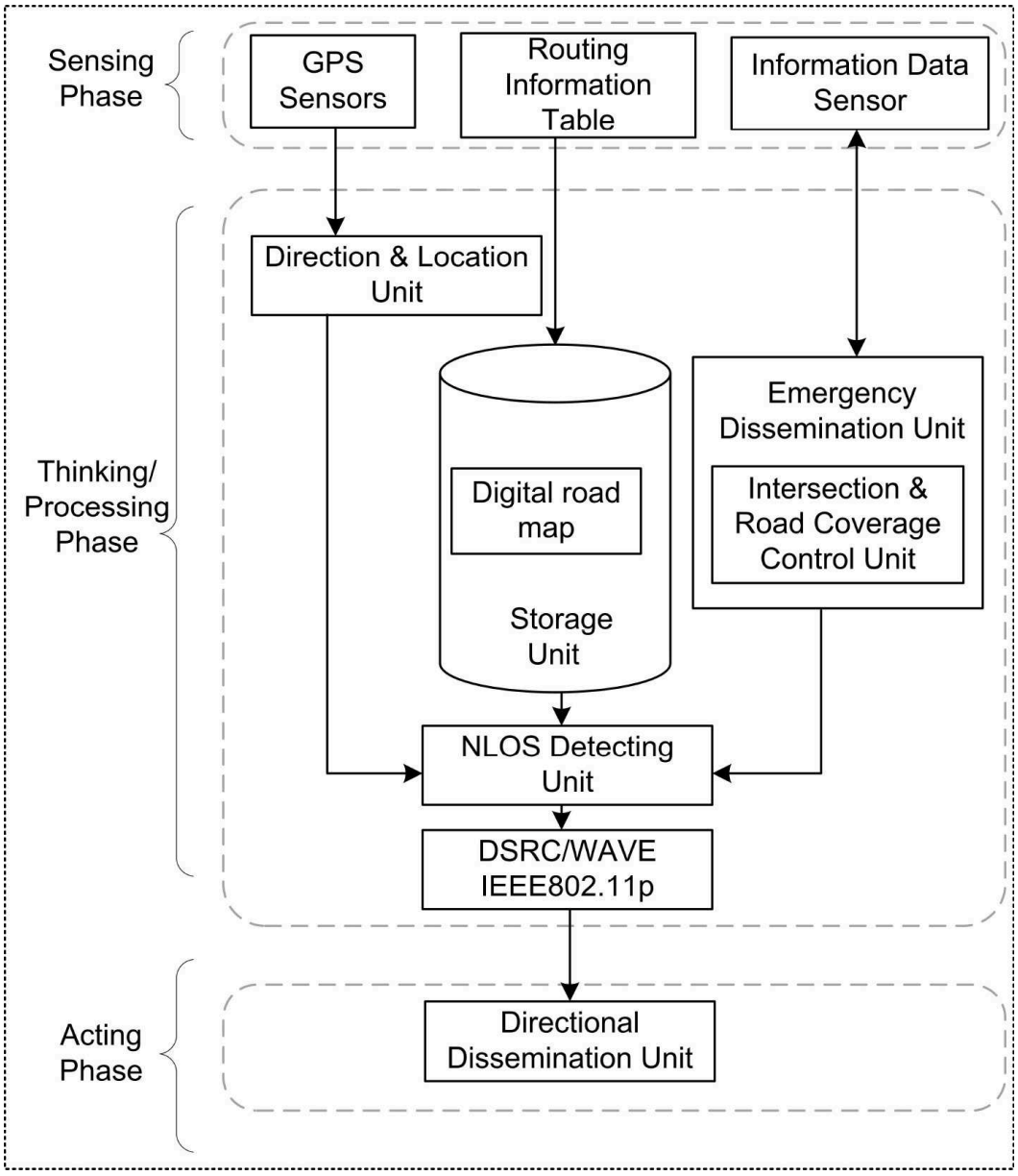

Figure 2: OBU Context-aware Architecture

communications arises due to the high expense of installing the needed infrastructure, especially in rural areas. Therefore, the proposed work will be based on infrastructures-less systems i.e. V2V communications, which means some vehicles must act as a repeater to assure that warning messages will reach every vehicle in the network to avoid fatal accidents occurring. We assume that every vehicle in the system is equipped with GPS (Global Positioning System), NS (Navigation System) and can exchange RITs (Routing Information Table), in addition to periodic messages which will be sent all over the network regularly.

The main purpose of designing CVP protocol is to solve NLOS by using a mediator node, which will deliver the warning message in time to the hidden node (suffering from NLOS), and reply to any emergency vehicle that it is clear to pass the intersection. Moreover, using CVP protocol is essential in safety application, with the need of Non-DTN (Delay Tolerant Network) routing protocol issues, which is based only on position. In contrast, DTN-based routing protocol cannot be utilised in this research due to the carry and forward mechanism which cannot be applied in our proposed protocol in order to the delay that might occur because of this issue.

The detailed two stages of the CVP protocol are introduced in the subsections below: Detecting the NLOS and Packet Delivery.

4.1.1. Detecting Non-Line of Sight

Before delving into detecting NLOS in our scenarios, the RIT must be covered in details as it is an essential component in the system.

Routing Information Table (RIT) As the system is designed to process infrastructure-less environments with the need to detect the NLOS by any volunteer vehicle, this detection will be based on the Routing Information Table (RIT). The RIT contains a history of all activities being performed by each node in the network [17]. It stores a record of the activities of all the neighbours and their neighbours, which serves to enhance location verification to facilitate the detection of NLOS situations. This section presents the creation of the RIT and explains how the comparison is performed according to the CVP protocol.

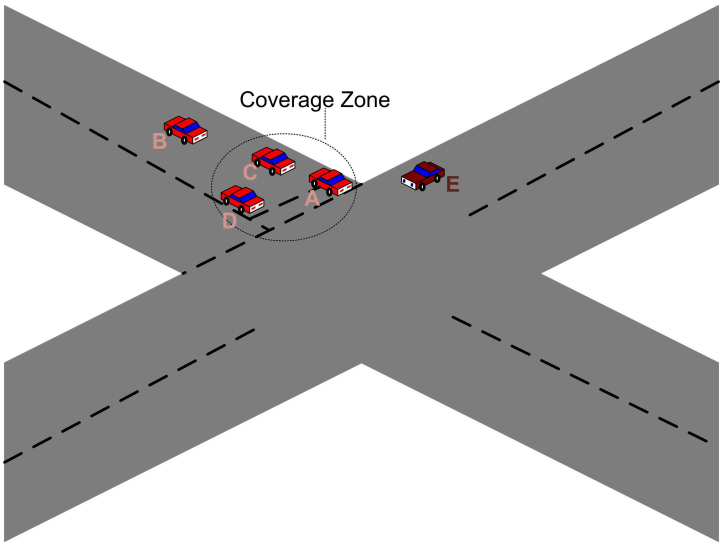

Figure 3: Target vehicle out of the coverage zone

Each node in the network sends periodic messages to its neighbours including its position, velocity, direction, and emergency status, which is supposed to be saved in the RIT and be exchanged with its neighbours. Therefore, after acquiring these data, each vehicle acquires the data about its neighbour and the neighbours of the neighbouring node, which is extracted from the RITs. Each vehicle in the network periodically scans its environment every 3 seconds for inconsistencies in the stored list of its neighbour; this means that the RIT is used to check for possible NLOS situations in its surrounding traffic network using (Algorithm 1: NLOS detecting).

Actually, the RIT table transmitted as part of the packet of the previous sender is compared with that of the receiver, and if any inconsistency in the RIT is detected, this may be attributed to one of two scenarios: either the node is outside the coverage zone or in an NLOS situation because of an obstacle, as shown in figure 3 and 4, respectively. Both of these scenarios demand different actions to ensure vehicle-to-vehicle communication under NLOS. In the case of the node being outside of the coverage zone in Figure 3, the vehicle will not appear in the RIT, which means it is not in the surrounding area; therefore,

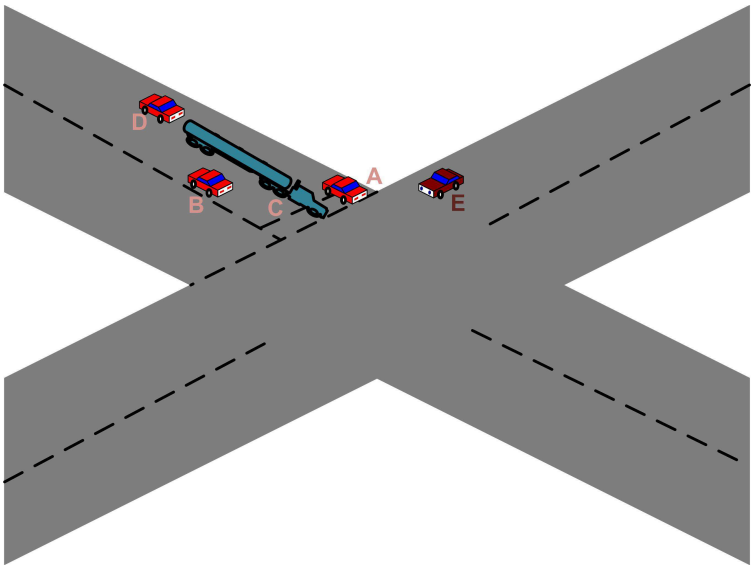

Figure 4: NLOS (Intersection obstructed by a truck)

it provides the opportunity for another vehicle to detect the NLOS in which case the CVP will be triggered. In case the NLOS situation in Figure 4, is detected, it confirms the NLOS for itself and triggers the CVP action using (Algorithm 2: the CVP trigger). In this case, the receiver node declares itself against NLOS by triggering the NLOS status based on (Algorithm 1: NLOS detecting). Concurrently, the node also piggybacks the NLOS query during the transmission of the next warning beacon interval.

As shown in Figure 4, the emergency node E sends a warning message to the vehicles approaching the road intersection. Every node is supposed to have its own RIT (Tables 1-4) which holds general information about its neighbours such as the ID, direction, distance from the road intersection, position in the lane, and most importantly, an indication of the nodes intended to receive the packet and highlighting those nodes that are in the neighbourhood but did not receive the warning packets because of some NLOS situation in the network.

Table 1 presents the RIT of node E in the proposed scenario in Figure 4, which shows that nodes A and B are within the coverage zone and should therefore receive the warning message.

Table 1: Routing Information Table for Node E

ID of neighbour nodes	Distance from intersection	Direction	Lane/position
Node A	x	y	L1/L2
Node B	a	b	L1/L2

Table 2: Routing Information Table for Node A

ID of neighbour nodes	Distance from intersection	Direction	Lane/position
Node E	x	y	L1/L2
Node B	a	b	L1/L2

(The values for distance direction and lane positions are assumed here in the table for nodes A and B. The values x, y, a, b are repeated as assumed values for the RIT tables referred to later on)

Tables 2, 3 and 4 show the RIT for nodes A, B, and D, respectively, whereas node C acts as an obstacle that prevents communication between A and D.

After receiving the warning message, each node will receive the RIT of node E. This RIT is then compared with its own RIT to check for any hidden node in the system. The comparison process for node A is shown in Table 5, where T=True, which means LOS communication is possible, and F=False, which means there is no direct communication with this node.

Apparently, the table did not show any indication of hidden nodes or NLOS, and both RITs show that they can build LOS communication with each other

Table 3: Routing Information Table for Node B

ID of neighbour nodes	Distance from intersection	Direction	Lane/position
Node E	x	y	L1/L2
Node A	a	b	L1/L2
Node D	c	d	L1/L2

Table 4: Routing Information Table for Node D

ID of neighbour nodes	Distance from intersection	Direction	Lane/position
Node B	x	y	L1/L2

Table 5: Comparison Process for Node A

ID	E RIT	A RIT
Node E	-	T
Node A	T	-
Node B	T	T
Node D	F	F

and with node B. On the other hand, neither of them can locate node D. However, after receiving the comparison process for node B, Table 6 shows that nodes E and B have direct communication with each other and with node A. Yet, from the table it can be concluded that node E has no direct contact with node D. Meanwhile, node D is in the LOS of node B; therefore, CVP will be triggered to solve the NLOS issue that has occurred in the system because of node E having no direct communication with node D, either because it is outside its coverage zone or under NLOS. Thus, a fatal accident could occur if the warning message is not received in time. In this scenario, an NLOS situation occurs because the obstacle (node C) prevented communication from occurring between nodes D and A, and D and E.

Table 6: Comparison Process for Node B

ID	E RIT	A RIT
Node E	-	T
Node A	T	T
Node B	T	-
Node D	F	T

Trigger of CVP by RIT data in node B Here the assumption is that the nodes facing NLOS would appear to be missing from the RIT table, and the detecting vehicle (A) will automatically forward the data to another neighbouring node (B) for comparison and verification of information in the RIT tables of A and B. Vehicle B being in direct line of sight with D confirms to vehicles A and E that vehicle D did not receive the packet; and B volunteer to deliver the packet to D itself. In this way, RIT tables of all the concerned nodes in the network share information about neighbouring nodes and find the missing nodes in the RIT, detect them and suitable vehicles within direct line of sight (which is B in this scenario) of the missing node transfer the data to the node facing an NLOS situation.

CVP allows B to trigger the rebroadcast process rather than waiting for E to assign the job to it. B avoids storm problems by notifying E about the situation to check if there is no other node capable of performing this action. Once E receives the notification, it adds the new node to its RIT to notify other nodes about the changes to avoid duplication. This notification is based on the three-handshake technique, which needs acknowledgment that the packet has been received. This is expected to enhance the robustness of the CVP as will be discussed later in this section.

NLOS Detection Algorithms

If a node detects a potential NLOS situation in its transmission range, it constructs warning message bytes (WMB), which can assume two forms: WMB-req and WMB-rep. The former is a request from nodes experiencing NLOS that simultaneously tries to verify the current traffic situation in the respective neighbourhood, whereas WMB-rep is the reply to the cognate query. From the standpoint of the requesting node, if the receiver receives multiple queries regarding nodes experiencing NLOS situations in the same area, the replying nodes reply collectively by sending one response to all of these queries instead of relying on an individual basis to avoid the storm issue and communication channel contention. For example, if two nodes are moving close to each other

and experiencing the same state of NLOS, they may raise the NLOS alarm regarding the same area; therefore, only a single reply for both of them is needed. The format of both WMBs is given as follows:

Request

$$(RR||((req_{id1}, pos_{start}, status), (req_{id2}, pos_{start}, status), \ldots, ((req_{idn}, pos_{start}, status))))$$

Reply

$$(RR||((rep_{id1}, pos_{start}, status), (rep_{id2}, pos_{start}, status), \ldots, (rep_{idn}, pos_{start}, status)))$$

Here RR represents the request or response based on the contents of the request or response. In the above communication, the request or response is presented in the form of triplets containing the unique ID regarding the situation under consideration, the starting position of the respective area, and the status of the area by taking into consideration the traffic dynamics which, in our case, represents the number of nodes. The response is generated in the same manner.

Algorithm 1. NLOS Detecting

1. **Assumption:** two adjacent statuses for the neighbourhood are saved in interval $[t_{i-1}, t_i]$
2. **For** $N1$ to Nn **do** check coverage zone
3. Check consistency of two consecutive states
4. **If** $(Ni_{vib} = ?)$ then construct WMB for the respective Node
5. **Set** WMB
6. **Break**
7. **Else** no action
8. **End if**
9. **End for**
10. **For** $N1$ to Nn do NLOS Detect
11. **If** $(Ni_{vis} = ?)$ **then** wait()
12. **If** WMB received **then**
13. **Break**
14. **Else** send info to mediator node
15. **End if**
16. **End if**
17. **End for**
18. **If** RIT = missing node **then** trigger$_{NLOS}$
19. **Return** Status$_{NLOS}$ = TRUE/FALSE
20. **End if**

4.1.2. Packet Delivery Phase

In this section, the delivery of packets from the source node to the destination node is explained. This constitutes the packet delivery phase.

Communication in NLOS When a node detects an NLOS situation through the data stored in the RIT maintained by each vehicle in the network, it triggers the CVP, which piggybacks on the WMB through the next beacon to its immediate neighbour in both directions. The neighbours, after reception of the

WMB, perform plausibility checks to find the vehicle under NLOS. In addition, each node performs checks of the NLOS situation in its own area and the areas in question. In the case of the issuance of such an NLOS situation by the receiver node, it waits for the response from another node with a clear LOS for the area in question. If the receiver already has LOS for the node under NLOS, then it constructs WMB-rep and replies to the requester(s). The possibility that the surrounding vehicles have clear LOS in the requested area also exists. In that case, the request is forwarded by the neighbour vehicle with a timestamp. The overall scenario is implemented through Algorithm 2, which is given below:

Algorithm 2. Trigger CVP

1. **Assumption:** two immediate statuses for neighbours are
saved in any interval $[t_{i-1}, t_i]$)
2. WMB received with RIT
3. **For** N_1 to N_n **do**
4. Compare RIT for the same area for direct communication
5. **If** report is issued already **then Break**
6. **else if** (NLOS in the same area and are under
request shows same node info) **then**
7. **Construct** WMB-rep
8. **Forward** the node information to the requester
9. **else if** (NLOS in neighbour's list) **then**
10. **Forward** the information at hand with timestamp
11. **End if**
12. **End if**
13. **End if**
14. **End for**
15. **Return** CVP Triggered

Acknowledgement of receipt of WMB

In case a WMB is received from a node under NLOS (N_{NLOS}), it issues

a reply to the requesting NLOS confirming that the WMB was received and action is taken according to the contents of the request. The NLOS, according to the protocol, sends the verification message to the originator of the request, which is an emergency vehicle in our case, to let NEV know that WMB to the N_{NLOS} has been delivered and action has been taken accordingly. The following Algorithm 3 describes the whole scenario:

Algorithm 3. Acknowledgement receipt of NLOS communication

1. **Assumption:** two immediate statuses for neighbours are
saved in any interval $[t_{i-1}, t_i]$)
2. **Verify** the reception of WMB-req by N_{NLOS} **do**
3. Update the RIT
4. **if**
5. The requester node is not in communication range **then**
6. **Break**
7. **Else if** N_{NLOS} in communication range
8. **Send** WMB-rep to N_{NLOS},
9. NLOS update the RIT and
10. WMB-rep to N_{EV}
11. **End if**
12. **End if**
13. **Return** WMB Received
14. **Return** NLOS Cleared

The overall process of NLOS detection and resolving the NLOS situation is described by the flowchart in figure 5.

4.2. Assumptions/Hypotheses

The following assumptions have been made for constructing the CVP and interpretations of its working principles.

- The simulation was performed in a virtual environment rather than a real-life situation to validate the functions of CVP

- The RIT tables are generated in OBU of all normal vehicles for the purpose of comparison and detection of missing nodes
- The missing nodes in the RIT are considered to be nodes that either face an NLOS situation or are located in a non-coverage zone
- The data generated in the RIT of one vehicle is automatically shared with neighbouring vehicle
- RIT tables are updated periodically every 3 seconds to take into account both new nodes and existing nodes
- The RIT contains data regarding the distance of vehicles from the intersection, ID of neighbouring vehicles, and the direction and lane positions of neighbouring nodes/vehicles

5. SIMULATION METRICS AND RESULTS

This section introduce the readers with the simulation setup and the motivation behind using Estinet. EstiNet 8.1 is the commercial version of NCTUns network simulator and emulator [18], which is a world-renowned tool and has been used by more than 20,000 registered users coming from 144 countries [19]. EstiNet provide important capabilities including, the most up-to-date IEEE 802.11p/1609 VANET network simulation, and realistic destination-oriented vehicle movement on the road for VANET [19].

Figure 6 shows the integration of IEEE 802.11p/1609 and EstiNet module frameworks or planes, which are divided into the data and management planes. The data plane supports IP and non-IP services, such as IPv6 and the Wireless Access Vehicle Environment (WAVE) short message protocol (WSMP). When a higher layer application must transmit or receive data packets, service settings, such as provider, user, WSM, and Control Chanel (CCH) services, are sent to standard 1609.3, enabling identification of the correct channel for receiving or transmitting during the transmission of packets. The WME module, located

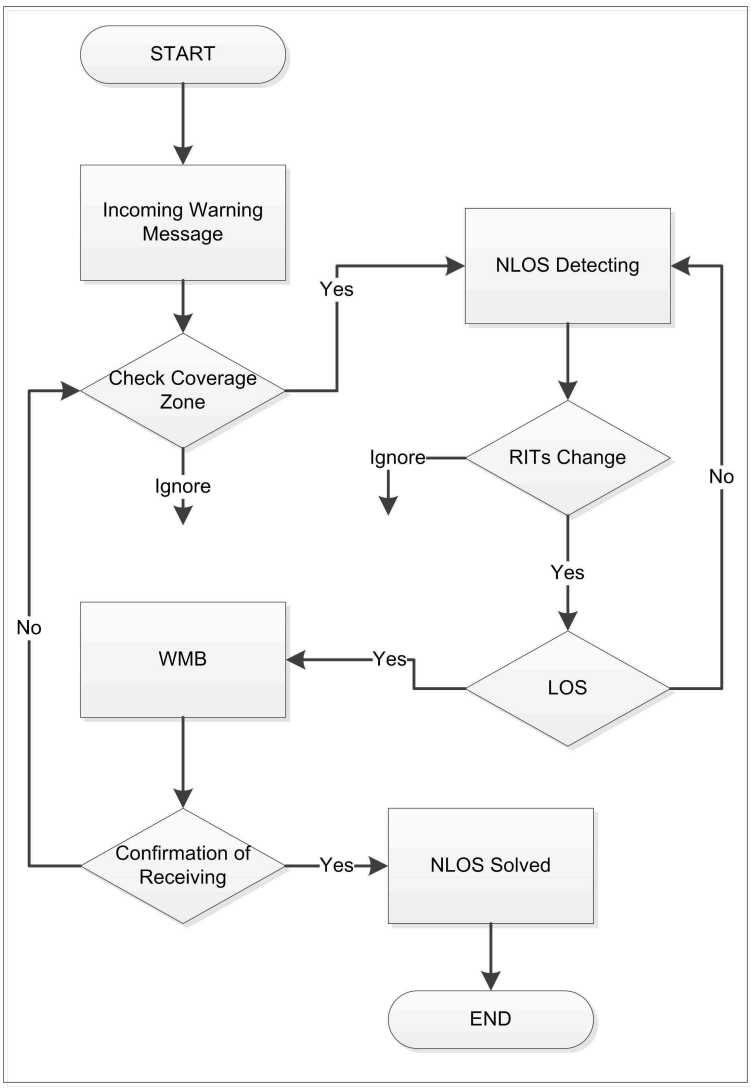

Figure 5: NLOS Detection process

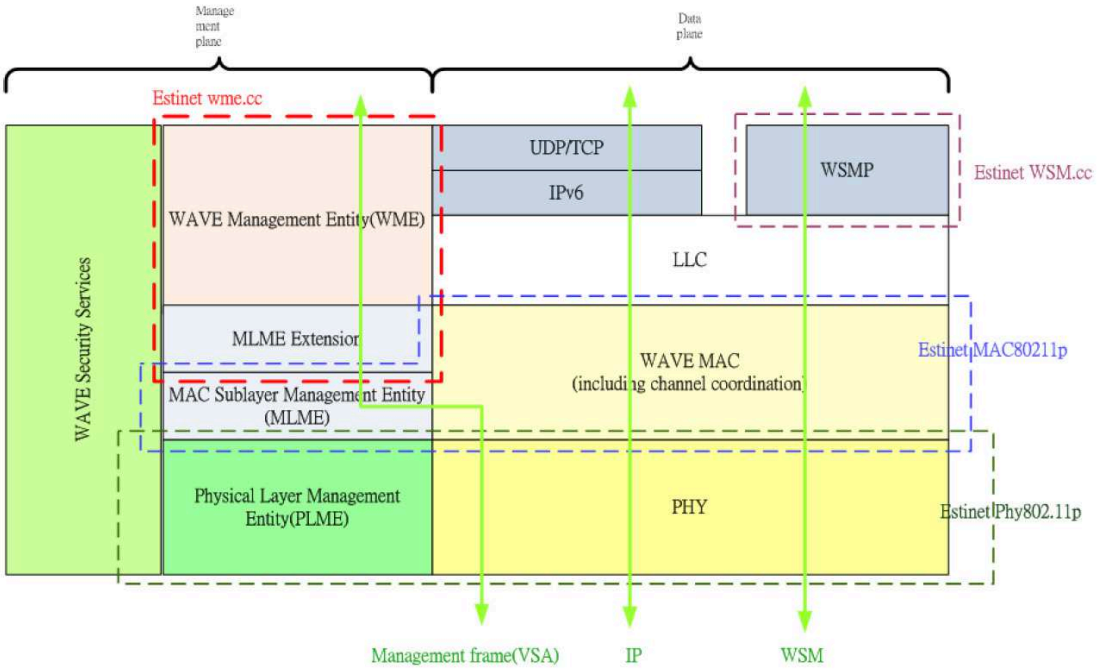

Figure 6: Integration of IEEE 802.11p/1609 and EstiNet module frameworks or planes

on the left of the management plane, mainly processes the four service settings (i.e., provider, user, WSM, and CCH service settings). According to the service setting elements provided by the higher layer, a WME module communicates with the lower layer to determine the correct Service Channel (SCH) that the medium access control/physical layer (MAC/PHY) should switch to, or notifies the lower layer to send the WSAs (or the VSAs in the MAC layer) [19].

In this paper, we use the EstiNet network simulator in order to evaluate the performance of this protocol, by using the performance metrics defined in subsequent subsection. The results of CVP were compared with those of GRANT which is considered to be a standard routing protocol in VANET and ad hoc networks. GRANT was simulated under the same conditions and scenarios as were used to simulate the CVP in order to obtain a justifiable comparison. The performance of GRANT has been selected for comparison with that of the proposed CVP, because both GRANT and proposed CVP share similarity in aims and mechanism. It is used for the detection of obstacles in urban area, and the proposed CVP also aims to detect NLOS situations in urban areas. Both protocols use the extended greedy mechanism for forwarding the messages from source vehicle to the target vehicle. Both routing protocols works in Non-DTN environment, therefore, the comparison of performance of the proposed CVP with GRANT can show the extent to which the latter can perform better than the former in terms decreasing delay in warning messages and other performance parameters evaluated in succeeding sections

5.1. Simulation Metrics

Five different performance metrics, briefly described below, were used to evaluate the performance of CVP:

Warning Messages delivery success rate: This metric represents the total number of packets delivered to the destination node successfully, including the packets forwarded among the nodes to reach the destination node. The goal of using this metric is to determine the efficiency of the routing protocol in terms of successful delivery of packets.

End-to-End Delay: This metric is used to measure the time delay required to forward the data packet from the source node to the destination node; and this includes the time taken to process the data during the retransmission and buffering operations.

Neighbour Awareness and Location Verification: This metric is useful in NLOS situations in which packets delivery fails to those vehicles behind obstacles, and measures the capability of the proposed routing protocol to detect the NLOS situation in the network successfully. The goal of using this metric is to evaluate the performance of the CVP to detect the vehicle under NLOS and verify the location using the cooperative approach. When the source detects the number vehicles in surroundings matching those within its communication range, the neighbour awareness rate is said to be 100%.

Channel Utilisation: This metric measures the performance of the routing protocol in terms of generating the number of messages and the channel capacity occupied by them. The goal of this object is to evaluate the CVP scalability and efficiency of the cooperative approach used to transmit the packets to the destination.

Request Processing and Response Time: Average processing time is the time taken from the generation of request from the sender to the receipt of reply from the other vehicle in the network.

5.2. Parameters and Values

The parameters and their values used are given in Table 7.

5.3. Simulation Results

Neighbourhood Awareness and Location Verification When vehicles and buildings obstruct the communication channel, the packets cannot be delivered successfully to the vehicles behind the obstacles. Vehicles in NLOS situations cannot be detected by the system. Therefore, neighbour awareness is important and can be achieved by verifying the location of the questioned vehicle. In other words, obstacles have a negative impact on the neighbourhood awareness rate. The simulation was performed to detect the NLOS situation

Table 7: Parameters and values for simulation

Parameters	Values
Simulation area	1500m x 1500m
Routing protocol	CVP, GRANT
Transmission range	200m
MAC layer protocol	IEEE 802.11p
Number of Vehicles	37, 76, 110, 160
Traffic type	Constant Bit Rate (CBR)
Warning packet size	512B
Bandwidth	12 Mbps
Simulation time	270s
Maximum vehicle's speed	30mph, 70mph
Mobility generator	OpenStreetMap

both in highway and intersection scenarios. Data showed that the proposed protocol was able to successfully identify the NLOS situation by increasing the neighbourhood awareness rate. The updates about the neighbour depend on the reception of the forwarded packets, which can be disrupted by the presence of obstacles between the node forwarding the packet and the node in an NLOS situation. In comparison with GRANT, the use of the proposed protocol increased the neighbourhood awareness rate. Simulation data obtained from GRANT was inconsistent as it has some network performance issues that impacted the performance and limited its use. Using CVP increased the neighbourhood awareness rate by up to 89% with the application of the RIT, which was able to verify requests whenever a verification reply was found to be inconsistent. The proposed protocol was able to detect the NLOS situation in the questioned neighbourhood by comparing the number of detected neighbours and number of surrounding vehicles within the packet dissemination range. The RIT is updated if the verification reply is received that a node finds itself in an NLOS situation. The CVP recognised the NLOS situation and continued sending requests to determine whether the target neighbour still existed before deleting the record.

Figure 7, shows the average awareness rate of various densities with 20%

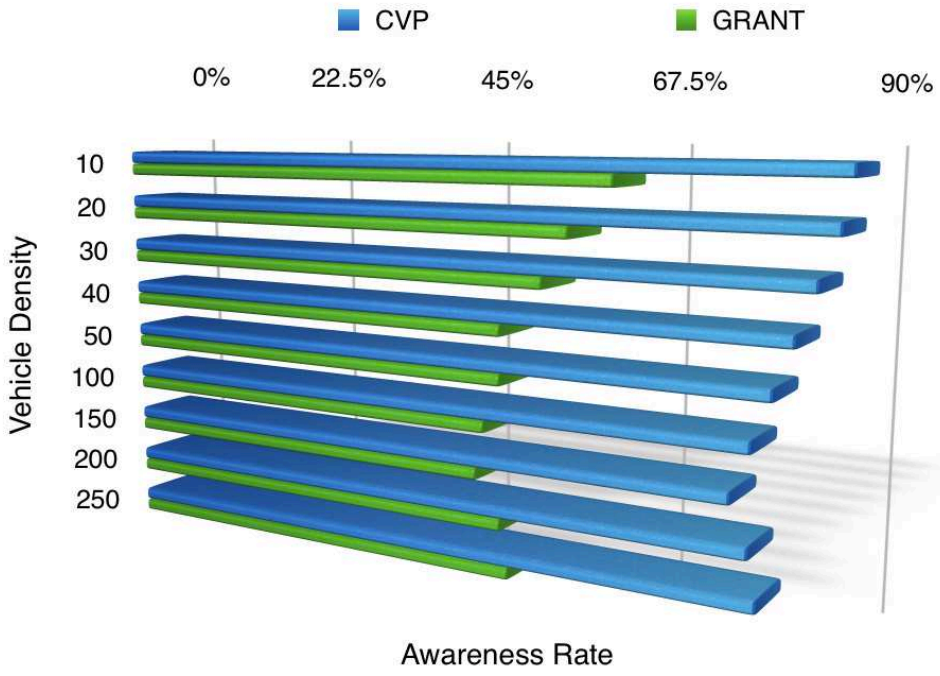

Figure 7: Neighbourhood Awareness

obstacles included in the simulation. The findings reflected that improvement in detection of NLOS was achieved by using the proposed protocol.

Channel Utilisation The proposed CVP mechanism is based on the co-operative approach that requires an exchange of warning messages among the neighbouring nodes in the network. The estimation of the volume of message exchanges and the space used by them in the communication channel bears on the efficiency and effectiveness of the model designed to disseminate the warning messages to the target vehicles. The packet payload size used during simulation experiments was 150b, which includes the messages relating to location information and request information about the node under NLOS situation. The findings obtained from the simulation experiments showed that the average

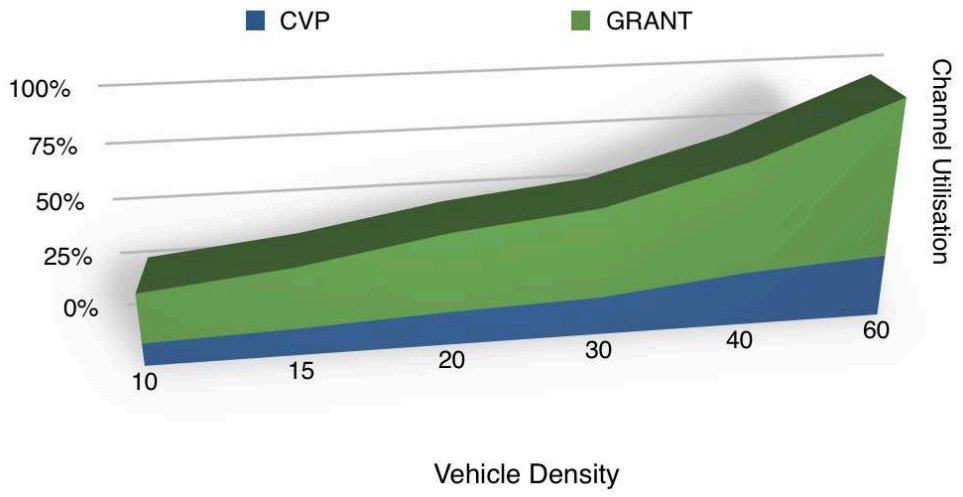

Figure 8: Channel Utilisation

channel utilised by the packets generated during the experiments was found to be less than 9% of the total available channel capacity of 6Mb/s (Figure 8).

In comparison with GRANT, the CVP protocol showed 20% less utilisation of space of communication channels owing to the cooperative approach adopted by CVP. This approach allows the generation of packets from one vehicle to another based on requests from each other; thus, each node does not transmit multiple packets in a given time space, thereby allowing the utilisation of less space within the communication channel. Figure 8, shows the comparison of cooperative and non-cooperative systems, and it can be clearly observed that in the absence of a cooperative approach, the channel bandwidth can be quickly saturated, as each node has to issue its own verification request, particularly in high-density areas.

The Time Delay of Data Delivery The end-to-end delay for the CVP has been simulated and measured for network size. These results were compared with those obtained with the GRANT protocol, which was evaluated using the

same conditions and scenarios. Figure 9 shows the influence of the number of nodes in the network on the time delay of data delivery. It can be seen that with an increase in the number of nodes in the network, the end-to-end delays decreases, which assures the delivery of packets to their destination nodes within as little time as possible. This is because the protocol guarantees the dissemination of packets to the destination through a cooperative approach. In areas containing a high node density, the packets are forwarded quickly due to the availability of more intermediate nodes mediating the forwarding action on the warning messages issued by the source. Furthermore, it can be observed in the figure that the performance of GRANT starts improving before slowing down as the number of nodes increases. This indicates the negative impact of increasing node density on the performance of GRANT, primarily because of the non-cooperative nature of the protocol and selection of the next-hop node based on its position. During the selection of the forwarding node based on location, GRANT attempts to depend on the vehicles on the perimeter (perimeter mode) if nodes in the local neighbourhood become less dense or are unavailable. That is not considered to be efficient in terms of delivering the message successfully to the destination, thereby leading to a loss of packets in switching to perimeter mode. However, in comparison to GRANT, the novel feature of the proposed CVP works more efficiently for both high-density nodes and in low-density areas due to the availability of cooperative nodes assisting in forwarding the warning messages to those nodes in NLOS situations.

Warning Message Delivery Success Rate The performance of the CVP has been compared with that of GRANT in terms of efficiency of delivering messages to a target under NLOS successfully, to test the influence of variations in the number of vehicles and the vehicular distance on the measurements. Figure 10 depicts the relationship between the number of packets delivered and the number of nodes in the network. Firstly, it can be seen clearly that a considerable increase in the efficiency of the delivery of warning messages occurs when the number of nodes in the network increases. This is because of

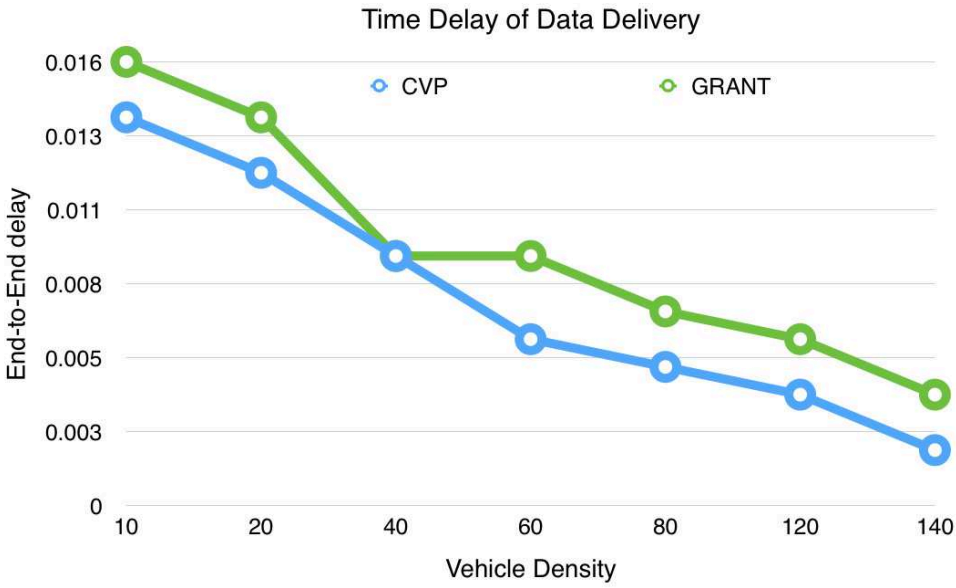

Figure 9: Time Delay of Data Delivery - Vehicle Density

the availability of more volunteer nodes and a reduction in the disconnected areas between the nodes. The existence of more voluntary nodes in the network creates more intermediary nodes that make it possible to transmit the message in an end-to-end fashion to the target destination under NLOS. Hence, the warning message is efficiently delivered to the target destination, thereby avoiding any collision between the source (emergency vehicle) and the vehicle in the NLOS situation.

Furthermore, after comparing the efficiency of data packet delivery by CVP, it was found that CVP performs better than GRANT, even in low-density areas of the network. This is due to the fact that CVP is based on the cooperative approach through which volunteers are recruited to deliver the message to the next hop and finally to the destination node, thereby reducing the possibility of packet drop dramatically. The cooperative approach also ensures the reliability of CVP as nodes in LOS and nodes in proximity to nodes in NLOS situations were found to receive the message through intermediary or voluntary nodes

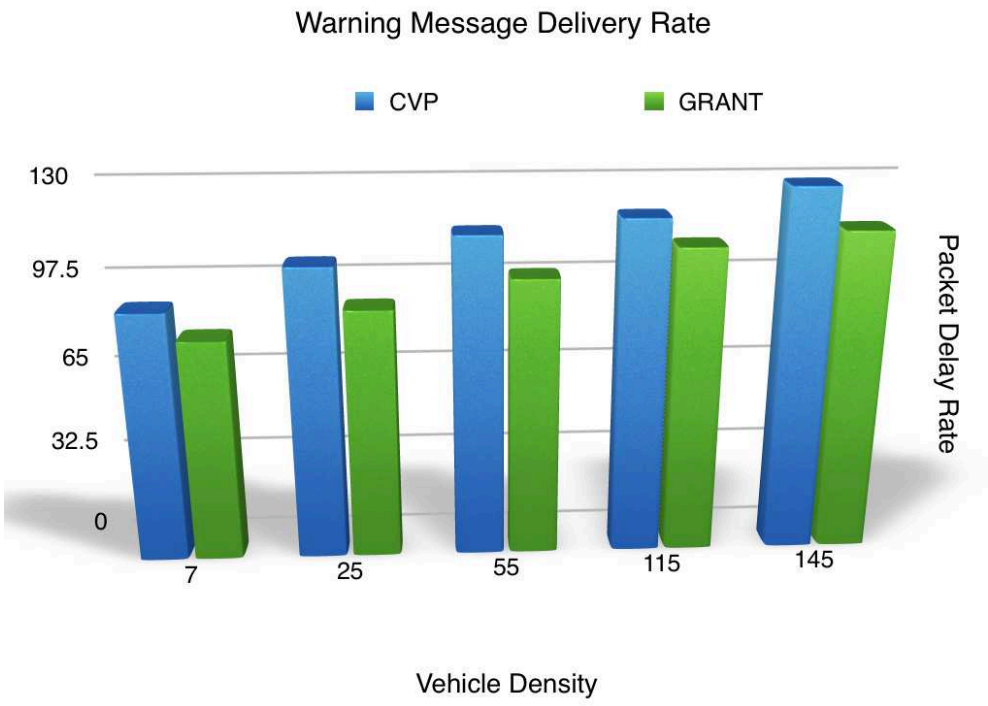

Figure 10: Warning Message Delivery Rate - Vehicle Density

with greater reliability compared to GRANT. Additionally, these data also reflect that CVP is able to promise a greater degree of reliability in terms of delivering the packet to the destination node, even with a low number of nodes prevailing in certain areas, which fits with the designers objective engaged in developing the CVP protocol.

Average Processing Time for Request Verification The average processing time for request verification has been measured for the CVP using a network size scenario. The evaluation of the performance of the CVP was then conducted by comparing it to GRANT under the same evaluation conditions. The average processing time is the time taken from the moment the request is generated by the sender until the moment at which the reply is received from the other vehicle in the network.

The performance of the CVP in comparison with GRANT was evaluated by the nodes in the network. The simulation results are depicted in Figure 11. It shows that the average processing time increases with an increase in the number of network nodes. This increase was more pronounced in GRANT compared to the CVP, showing that the latter is more efficient for processing a request between the sender and receiver vehicles in the network. The increase in the time taken to process the request is attributed to the accumulation of an increased number of processed and queued messages for vehicles in a high-density area. The CVP performed more effectively compared to GRANT because of the cooperative approach, which prevents the message contentions issue to a considerable extent.

6. CONCLUSION

The main contribution of this work is the presentation of new routing management based on the design of a new routing protocol for the detection of NLOS situations on the road at intersections in urban scenarios. The work involved the dissemination of warning messages broadcast by the source vehicle (emergency vehicle) to a target vehicle facing an NLOS situation. In addition, the

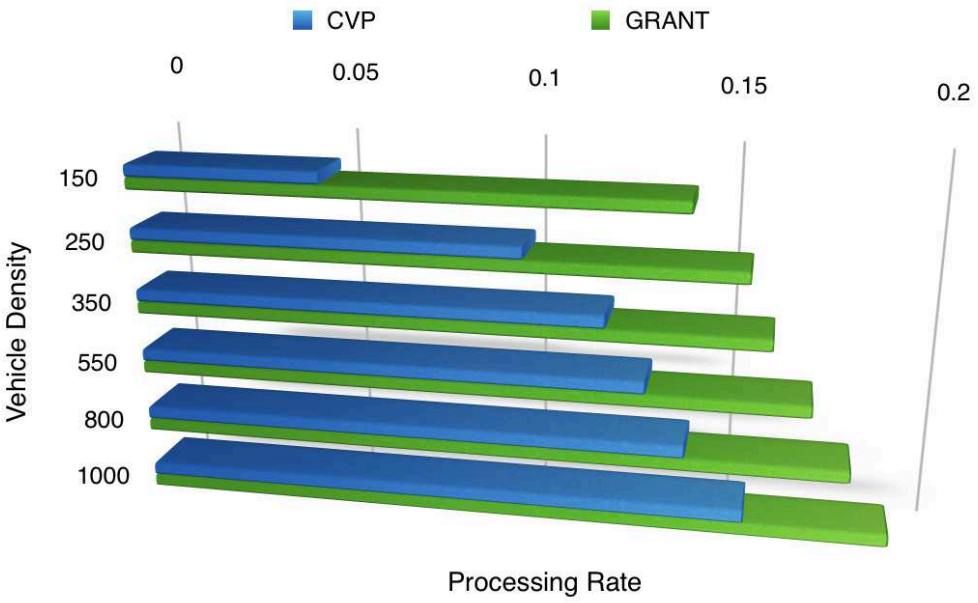

Figure 11: Average Processing Rate for Request Verification - Vehicle density

simulation results demonstrated that CVP achieved the target of the successful dissemination of warning messages to vehicles under NLOS through cooperatively delivering messages to these vehicles, thereby solving the NLOS situation successfully. It has been shown that CVP can operate in two modes: an intersection scenario in which a vehicle is hidden by a bus, truck or building, thereby preventing access to warning messages from the source emergency vehicle to the vehicle hidden by an obstacle; and the highway scenario in which the location of the target node under NLOS is hidden by some other vehicle (bus, truck) or foliage along the highways. CVP effectively detected the NLOS and was triggered to solve the NLOS using the cooperative approach for message delivery to the target vehicle. The CVP proposed in this work was able to outperform GRANT in terms of the ability of CVP to detect NLOS situations by using the RIT data.

Acknowledgment

The authors extend their appreciation to the Deanship of Scientific Research at King Saud University for funding this work through research groups.

References

[1] Road Driver web site. Available on: `http://www.roaddriver.co.uk/safety-tips/what-to-do-when-emergency-vehicles-approach`.

[2] Buchenscheit, A.Schaub, F.Kargl, F.Weber, M.: A vanet-based emergency vehicle warning system: In Proceedings of the IEEE Vehicular Networking Conference (VNC), Oct. 2009, pp. 1–8.

[3] M*ü*ller, D.: Typical hazards when using drives of the emergency services: the Institute for Traffic Law and Traffic Behaviour, vol. 37, 2007, No.3, pp. 120–131 (In German).

[4] Murthy, N.Srinvasa, R.: Development of model for road accidents based on intersection parameters using regression models: International Journal of Scientific and Research Publications, Vol. 5, No. 1, January 2015.

[5] Olariu, S.Weigle, M. C.: Vehicular Networks: From Theory to Practice. Chapman & Hall/CRC, 2009.

[6] C2C-CC, Car to Car Communication Consortium Manifesto: Overview of the C2C-CC System, Car to Car Communication Consortium, Tech. Rep. Version 1.1, 2007.

[7] Chen, W.Guha, R. K.Kwon, T. J.Lee, J.HSU, I. Y.: A survey and challenges in routing and data dissemination in vehicular ad hoc networks: In Proceedings of the IEEE International Conference on Vehicular Electronics and Safety, pp. 328–333, 2008.

[8] Abdalla, G. M. T.Abu-Rgheff, M. A.Senouci, S. M.: Current trends in vehicular ad hoc networks: In Proceedings of UBIROADS workshop. 2007.

[9] Hartenstein, H.Laberteaux, K. P.: A tutorial survey on vehicular ad hoc networks. IEEE Communications Magazine, Vol. 46, No. 6, pp. 164–171, 2008.

[10] Sastry, N.Shankar, U.Wagner, D.: Secure verification of location claims. In Proceeding ACM Workshop Wireless Security, pp. 1–10, 2009.

[11] Capkun, S.Hubaux, J.: Secure positioning of wireless devices with application to sensor networks. In Proceeding IEEE INFOCOM, vol. 3, pp. 1917–1928, 2005.

[12] Anjum, F.Pandey, S.Agrawal, P.: Secure localization in sensor networks using transmission range variation. In Proceeding IEEE International Mobile Adhoc and Sensor Systems Conference, pp. 195–203, 2005.

[13] Capkun, S.Rasmussen, K.Cagalj, M.Srivastava, M.: Secure location verification with hidden and mobile base stations. IEEE Transactions on Mobile Computing, Vol. 7, No. 4, pp. 470–483, 2008.

[14] Zhang, Y.Liu, W.Lou, W.Fang, Y.: Location-based compromise tolerant security mechanisms for wireless sensor networks. The IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, pp. 247–260, 2006.

[15] Leinmller, T.Maihfer, C.Schoch, E.Kargl, F.: Improved security in geographic ad hoc routing through autonomous position verification: In Proceedings of the 3rd international workshop on Vehicular ad hoc networks (VANET '06). ACM, New York, USA, pp. 57–66. 2006.

[16] Liu, D.Lee, M. C.Wu, D.: A node-to-node location verification method. IEEE Transactions on Industrial Electronics, Vol. 57, No. 5, pp. 1526–1537, 2005.

[17] Al-Bayatti, A. H.Alalwan, N.Alzahrani, A.Alfarraj, O.: Security Management Techniques Designed for Mobile Ad Hoc Network of Networks (MANoN), SENSOR LETTERS, Vol. 13, No. 11, pp. 967–979, 2015.

[18] Wang, S. Y.Lin, C. C.: NCTUns 5.0: A Network Simulator for IEEE 802.11(p) and 1609 Wireless Vehicular Network Researches: In the Tenth International conference on Mobile Data Management: Systems, Services and Middleware. MDM '09. IEEE, Taipei, Taiwan, pp. 375–376, 18-20 May 2009.

[19] Wang, S. Y.Lin, C. C.: NCTUns 6.0: A Simulator for Advanced Wireless Vehicular Network Research: In the Vehicular Technology Conference (VTC 2010-Spring), 2010 IEEE 71st. pp. 1–2, 16-19 May 2010.

[20] Bruno, M. C.Silva, Joel J. P. C.Rodrigues, Neeraj K., Mrio L. Proena Jnior, Guangjie Han, MobiCoop: An Incentive-Based Cooperation Solution for Mobile Applications, ACM Transactions on Multimedia Computing Communications and Applications (TOMM), Vol. 12, No 4, Article 49, August 2016.

[21] Dias, J. A. F. F. Dias, J. J. P. C. Rodrigues, N. Kumar, K. Saleem, Cooperation Strategies for Vehicular Delay-Tolerant Networks, in IEEE Communications Magazine, Vol. 53, No. 12, pp. 88-94, December 2015.

[22] Dias, J. A. F. F., Rodrigues J. J. P. C., Zhou L., Cooperation Advances

on Vehicular Communications: A Survey, in Vehicular Communications, Elsevier, Vol. 1, Issue 1, pp. 22-32, March 2014.