

A Robust Congestion Control Scheme for Fast and Reliable Dissemination of Safety Messages in VANETs

S. Djahel, Yacine Ghamri-Doudane

▶ **To cite this version:**

S. Djahel, Yacine Ghamri-Doudane. A Robust Congestion Control Scheme for Fast and Reliable Dissemination of Safety Messages in VANETs. IEEE Wireless Communications and Networking Conference, WCNC'12, 2012, France. pp.2264 - 2269. hal-00794703

HAL Id: hal-00794703
https://hal.science/hal-00794703

Submitted on 7 Mar 2013

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A Robust Congestion Control Scheme for Fast and Reliable Dissemination of Safety Messages in VANETs

Soufiene Djahel and Yacine Ghamri-Doudane
ENSIIE, 1 Square de la Résistance, 91025 Evry Cedex, France
{soufiene.djahel, yacine.ghamri}@ensiie.fr

***Abstract*—In this paper, we address the beacon congestion issue in Vehicular Ad Hoc Networks (VANETs) due to its devastating impact on the performance of ITS applications. The periodic beacon broadcast may consume a large part of the available bandwidth leading to an increasing number of collisions among MAC frames, especially in case of high vehicular density. This will severely affect the performance of the Intelligent Transportation Systems (ITS) safety based applications that require timely and reliable dissemination of the event-driven warning messages. To deal with this problem, we propose an original solution that consists of three phases as follows; priority assignment to the messages to be transmitted /forwarded according to two different metrics, congestion detection phase, and finally transmit power and beacon transmission rate adjustment to facilitate emergency messages spread within VANETs. Our solution outperforms the existing works since it doesn't alter the performance of the running ITS applications unless a VANET congestion state is detected. Moreover, it ensures that the most critical and nearest dangers are advertised prior to the farther and less damaging events. The simulation results show promising results and validate our solution.**

***Keywords* – VANETs, Congestion control, IEEE 802.11P, Beacons, Safety messages.**

I. Introduction

Vehicular Ad Hoc Networks (VANETs)[13] are new paradigm of wireless communications that aim to exploit the recent advances in wireless devices technology to enable intelligent inter-vehicle communication. VANETs are distinguished from other wireless networks by their specific characteristics such as; predictable vehicles movement and high speed, powerful processing units, large storage capacities and new applications scenarios. VANETs may also ensure wide dissemination of data and safety related information due to the large transmission range of vehicles and the specific routing protocols used like GPSR [1], BROADCOMM [2] and GEOCAST routing approach [3]. Moreover, as compared to other wireless networks VANETs are not affected by strict energy constraints since the vehicle's battery can provide a long duration energy supply. Although, VANETs are unable to ensure connectivity between vehicles in certain circumstances like in rural areas where the network density is low. VANETs may also not guarantee timely detection of dangerous road conditions due to the high mobility of vehicles.

The purpose of this work is to design a congestion control mechanism that guarantees reliable and timely dissemination of safety related messages. Currently, most of the existing works propose to reduce the transmit power level as well as the frequency of beacon transmission to release more bandwidth for safety messages transmission, and thus prevent the occurrence of a congestion state. We believe that congestion prevention is not a good idea in VANETs, especially in the context of Hybrid Sensor and Vehicular Networks (HSVNs), as this leads to a severe degradation of ITS applications performance. As one of the main assets of VANETs is the proliferation of ITS applications for both safety and driving comfort purposes, it is not judicious to alter the performance of these applications (i.e, by reducing transmission power and beacon transmission rate) to prevent network congestion. To cope with this problem, we propose three stages based solution in which we first assign different priority levels to the emergency messages according to their contents and the number of hops that they have traveled. Secondly, we apply a congestion detection mechanism to identify any congestion state in VANETs. As a last stage, a vehicle adjusts its transmit power as well as its beacon transmission rate, according to the result of the previous step, to facilitate the dissemination of the emergency messages.

The remainder of the paper is organized as follows. Section II provides a brief description of the of IEEE 802.11P [9] functioning. Next, we present the most significant solutions for beacon congestion control in VANETs and highlight their weaknesses in Section III. In section IV, we introduce our congestion control scheme. In section V, we present and discuss the obtained simulation results. Finally, we conclude in Section VI.

II. Overview of IEEE802.11 P

In order to provide an efficient means of communication in VANET and facilitate its integration with other networks, such as WSNs to constitute the so-called Hybrid Sensor and Vehicular Networks (HSVNs), the IEEE 802.11P task group has defined a set of specifications for Wireless Access in Vehicular Environment (WAVE) to fulfill the requirements of such challenging environment. The IEEE802.11P operates in the frequency band of 5.85-5.925 GHZ, within which the DSRC spectrum is divided to 7 channels of 10MHZ each. The control channel (CCH) is exclusively reserved for safety related communications like beacons and event-driven messages whereas up to six service channels (SCHs) are used for non safety data exchange. IEEE802.11P uses the same medium access mechanism of IEEE 802.11e, termed Enhanced Distributed Channel Access (EDCA)[8]. In IEEE802.11P, the channel time is divided into synchronization periods of 100 ms each, consisting of equal-length alternating CCH and SCH intervals. Therefore, the vehicle's devices must switch to the frequency of each channel (i.e, the CCH or one of the SCHs) during its specified interval in order to transmit the type of messages authorized during this period. To make this access scheme more accurate, a period equal to 4ms, called Guard time, is set at the beginning of each interval to account for the radio switching delay and the timing inaccuracies in the devices. Notice that the coordination between channels is achieved through the use of the Coordinated Universal Time (UTC) offered by a global navigation satellite system.

III. related work

We say that the network is congested when the rate of the injected packets exceeds its processing capacity over a continuous period of time leading to an increasing number of packets loss.

Network congestion has been first studied in wired networks and some interesting solutions have been proposed to minimize its impact on network performance. The congestion problem is more severe in wireless networks compared to wired counterpart due to the broadcast nature of the wireless medium. Despite the fact that congestion control in wireless networks has been widely investigated it is still a hot topic that attracts much attention from the research community. In VANET, its specific characteristics, such as highly dynamic environment, frequently changing topology and distributed nature ..., render congestion control more challenging. So, we cannot apply the existing schemes for static wireless networks to this challenging environment.

Most of the proposed solutions to control the congestion in VANETs try to control the transmit power used for broadcasting the beacons to prevent the congestion state or at least alleviate its impact on the performance. This technique may cause, in some situations, an isolation of some vehicles when the network density decreases. This is due to the frequently changing topology of VANETs as the vehicles move very fast and change their directions so often.

Recently, some scholars have focused on designing reliable beacon congestion control mechanisms for VANETs. In what follows, we present the most significant contributions in the literature.

The automotive sector is considered as one of the main areas of concrete applications of Mobile Ad hoc Networks (MANETs). In VANETs, the topology changes within seconds and a congested node used for forwarding a few seconds ago might not be used at all at the point of time when the source reacts to the congestion. To take into account this special feature of VANETs, [6] has proposed a new scheme in which each node locally adapts to the available bandwidth. The contribution of this paper is based on an utility function that calculates for each data packet a value representing the utility of transmitting this data packet at the current point of time. It proposes to assign data rates based on the average utility of data packets transmitted by a vehicle. Thereby, nodes transmitting information with a high utility for the VANET will be allowed to consume a larger part of the available bandwidth. This scheme requires that the nodes share the information that allows to each of them to calculate its own rate (i.e. the proportion of the available bandwidth that should use).

The scheme proposed in [7] highlights the importance of transmit power control to avoid saturated channel conditions and ensure the best use of the channel for safety related purposes. The goal of this work is to design a new transmit power control scheme that ensures distributed fair power adjustment for vehicular environments (D-FPAV) to control the load of periodic messages on the channel. This work seeks to achieve two objectives, as stated below.

- Make the bandwidth available for higher priority data like the dissemination of warning messages.
- Treat the beacons received from different vehicles with equal rights.

Beacon messages may contain the vehicle speed, its direction and its current position (if it is equipped with a GPS). A high load of beacon messages on the channel leads to huge increase of packets collision in CSMA/CA based MAC protocols. In this case, beacon messages will not be successfully decoded and warning messages will show a slow unreliable spread within VANET. The authors propose to use per packet -level interference management based on per packet transmit power control to give packets "relative" weights that control the introduced interferences and, implicitly, the ability to capture packets. They suggest to carefully controlling the load of beacon messages to prevent deterioration of the quality of reception of safety related information.

Other researchers have applied formal verification techniques to assess the effectiveness of their congestion control schemes rather than using the conventional simulation tools. A recent and interesting work was introduced in [10], in which the authors have used the model checking technique to investigate the efficiency of the congestion control scheme proposed in [12]. This scheme is based on a combined static and dynamic priority assignment schemes. The former scheme defines a message priority as a function of its content and the source application type. In another hand, the latter scheme uses some parameters regarding VANET context such as, surrounding vehicles density, vehicle speed and message utility. Using these priorities, each message is transmitted over an appropriate channel. To allow fast transmission of high priority messages, neighboring vehicles exchange information about the priority of the messages they sent. Thereby, transmission of low priority messages is delayed to prevent congestion. We conclude from the above description that the exchange of messages' priority information may quickly lead to congestion especially in highly dense VANETs such as in traffic jam scenarios.

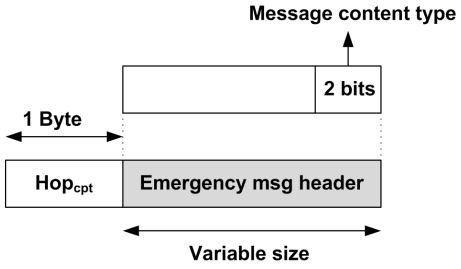


Figure 1: The safety messages' header

IV. The proposed congestion control scheme

In this section, we present the key principal and the different steps of our congestion control scheme. Figure. 2 gives a global overview of this scheme.

A. Priority assignment and messages scheduling

When a vehicle receives more than one event driven messages broadcasted by the Road-Side Units (RSUs), WSN gateways in case of HSVNs or sent by a neighbor vehicle as a result of collision, emergency braking ..., the MAC layer assigns to these messages different levels of priority according to their degree of importance and danger to set up a transmission order among them, especially in case of congestion.

The first metric used for safety messages scheduling is their content type. So, we can distinguish three types of safety message contents, as stated below.

- Immediate danger notification (emergency message): this type of messages is sent in case of accidents, very bad weather condition such as snow, fog etc. It is assigned the Higher Level (HL) priority.
- Warning message: sent to advertise an important event on the road but not an immediate (critical) danger. It is assigned an intermediate or Medium Level (ML) priority.
- Driving information announcement: such as information about traffic jams in some road segments to direct the driver to the fastest and least congested road. It is assigned the Lowest Level (LL) priority.

In our congestion control scheme, a vehicle that has more than one safety related messages waiting for transmission must first assign a priority to each message according to its content type as described above. In case of receiving many messages of the same content type a second metric is then used to determine the priority level of a given message. To take into account this metric, we add a field dubbed

Hop_{cpt} to the safety message packet header [1] as shown in Figure. 1. The value of this field is used to update the priority level of each safety related message. The priority level of a safety message decreases as the Hop_{cpt} value increases. An emergency message is assigned the highest priority when its Hop_{cpt} is equal to 1, which means that it is being transmitted from a direct neighbor vehicle, RSU or WSN Gateway. Therefore, it should be spread towards VANET as soon as the medium becomes free.

The primary purpose of this slight modification of the message header is to speed up the transmission of the fresh emergency messages at the expense of the old messages or those advertising a farther danger. This choice is due to the following reasons:

- A lower Hop_{cpt}value means that the danger is very close to the receiver vehicle. Thus, this message needs to be transmitted very fast towards its neighbors to prevent more damage.
- A larger Hop_{cpt} value indicates that the danger is relatively far from the receiver vehicle. Therefore, delaying its transmission is less harmful than the previous type of messages.

B. Congestion detection mechanism

How vehicles can detect that VANET is congested? To answer to this question, we should first define a set of metrics that represents VANET state at any point of time. After carefully studying VANET environment, we have chosen the following metrics:

- Average Waiting Time (AWT) to access the wireless medium (particularly the CCH) which can be also inferred from the Medium Busy Time (MBT). The MBT represents the time during which the wireless medium (CCH) was busy due to transmissions from the nearby vehicles. This gives an overview on the density of vehicles as well as the packets exchange rate among them.
- Collision Rate (CR): this metric is defined as the ratio of the unsuccessful transmissions from the vehicle to the total number of sent packets over CCH.

$$CR(V) = \frac{Own\ \ unsuccessful\ \ transmissions}{\sum sent\ \ messages\ \ over\ \ CCH} \quad (1)$$

  To detect an unsuccessful transmission of a beacon message over the CCH, we may use one of the nearby vehicles as a collision detector and the sender vehicle carries out handshaking with it before broadcasting any beacon message. Therefore, any lost or collided beacon will be detected.
- Beacon Reception Rate (BRR) that is expressed as the ratio of the number of received beacons, issued from different vehicles, to the total number of received beacons.

$$BRR(V) = \frac{|N_{1hop}(V)|}{\sum Beacons_{received(V)}} \quad (2)$$

  where N_{1hop} (V) denotes the one hop neighbor set of the vehicle V.

Each vehicle collects and updates the information regarding the above three metrics that express the state of VANET in terms of traffic load, at each Congestion Monitoring Interval (CMI). This interval is divided into a set of equal length mini-intervals. During each mini-interval one measurement is taken regarding the above metrics and the corresponding values are stored in a three dimensions vector called Congestion Index Vector (CIV)

$$CIV_i = (AWT_i, CR_i, BRR_i)$$

[1]One can argue that we can use the TTL field as a metric to realize the same task of this new metric, however our congestion control scheme is implemented at MAC layer where TTL value is not available. Moreover, different senders of safety messages may assign different values of TTL which makes the value of this field meaningless for our congestion control scheme.

such that i indicates the i^{th} mini-interval of current CMI. We consider that the sets of normal states (i.e, in which VANET load is normal) are aggregated close in the feature space while those of overloaded (congested) states are considered as a dispersed states that deviate from the cluster of the normal VANET states. According to this description of VANET's states, we perform the following computation to identify a congestion state.
First, we use the set of collected information during a training CMI, that consists of M mini-intervals, to calculate the mean vector $\overline{CIV}$ following the formula given below:

$$\overline{CIV} = \frac{\sum_{i=1}^{M} CIV_i}{M} \quad (3)$$

Subsequently, we calculate the distance between the CIV measured during a given CMI and the $\overline{CIV}$ as follows:

$$Dist(CIV) = \| CIV - \overline{CIV} \|^2 \quad (4)$$

Finally, the congestion is detected if the distance is larger than a certain threshold Thr, as indicated in Equation. 5.

$$\begin{cases} Dist(CIV) > Thr & \text{VANET state is congested} \\ Dist(CIV) \leq Thr & \text{VANET state is normal} \end{cases} \quad (5)$$

The Thr value is updated dynamically based on the information acquired from the messages broadcasted by the RSUs regarding the ahead traffic conditions, the messages received from the WSNs gateways in case of HSVNs (Hybrid Sensor and Vehicular Networks) context, the weather conditions as well as the traversed area (i.e, tunnels, intersections,...). Notice that the CIV values corresponding to a congestion states are discarded whereas those of normal states are used as a training measurement to determine the new $\overline{CIV}$.

C. Adjusting the beacon load

When a vehicle ascertains that the network is congested in its vicinity it adjusts its beacon load in order to preserve some amount of the available bandwidth for transmission of the emergency messages that require low transmission delay. The beacon load can be reduced either through the reduction of the transmit power used to send out these beacons or by decreasing their transmission rate. We note here that usually wireless cards provide limited choices of power transmit levels to be used, and each of them corresponds to a certain transmission range within which any packet transmitted can be correctly decoded with high probability. In what follows, we present a scheme to adjust the transmit power and another one for beacon rate regulation.

*1) **Transmit power adjustment**:* By analyzing the content of the received beacons, each vehicle maintains a neighboring table in which each entry consists of five parameters ($vehicle_{id}$, $speed$, $direction$, $expiration_{time}$, Tx_{pw}), which are described as follows:

- $vehicle_{id}$: identifier of the sender vehicle.
- $speed$: indicates the current speed of $vehicle_{id}$.
- $direction$: determines whether a vehicle ($vehicle_{id}$) is moving in the same or opposite direction of the receiver vehicle.
- $expiration_{time}$: is the duration after which if no new beacon is received from the same vehicle then the entry with the corresponding $vehicle_{id}$ is deleted.
- Tx_{pw}: indicates the transmit power level used to transmit the received beacon.

We assume that the vehicle is aware of (or it selects) the next forwarder of the generated/forwarded emergency message. To calculate an approximate value of the distance separating it to the sender of a beacon message, it uses the beacon Received Signal Strength (RSS) instead of the GPS information since this latter is not always available (e.g, the GPS signal cannot be received inside tunnels,

areas characterized by high buildings ...). To adjust the transmit power for beacons, we calculate the new transmit power based on the minimum power used by the nearby vehicles, including itself, and the distance separating it to the next forwarder of the emergency message. Notice that the vehicle can determine this distance based on m other candidates to be next forwarder under the condition that they belong to the set $N_{1hop} \cap N_{old}$ and m is determined based on the size of N_{1hop}. Here, N_{old} denotes the previous set of one hop neighbors of the vehicle and N_{1hop} is the current set. We calculate the transmit power that the vehicle will use for subsequent transmissions according to the following equation.

$$P = MAX[min(Tx_{pw}(i), Tx_{pw}(own)), P(nf_{dist} + \delta)] \quad (6)$$

where δ represents the difference between the next forwarder distance (nf_{dist}) and the maximum distance (max_{dist}) separating one candidate to the vehicle. If max_{dist} is smaller than nf_{dist} then δ is set to 0. Notice that the value i refers to the $vehicle_{id}$ and $P(nf_{dist} + \delta)$ can be interpreted as the transmit power that ensures a transmission range slightly greater than $nf_{dist} + \delta$.

In order to ensure fast dissemination of the emergency messages through the adaptation of the transmit power value to the change in the neighborhood and the CCH conditions, the P value calculated above is gradually increased or decreased as follows. First, we calculate the increase factor (IF) according to the formula below.

$$IF = \frac{|(N_{1hop} \cup N_{old}) - (N_{1hop} \cap N_{old})|}{|N_{1hop}|} \quad (7)$$

Secondly, we adjust the transmit power P according to the IF value as described the following.

$$P1 = \begin{cases} P & \text{if IF = 0} \\ P(1 + (1 - MIN(IF, BRR))) & \text{if } 0 < \text{IF} \leq 1 \\ & \text{and CR is low} \\ P(1 + (\frac{(IF-1)}{IF} * CR)) & \text{if } 0 < \text{IF} \leq 1 \\ & \text{and CR is high} \\ P(1 + (\frac{(IF-1)}{IF})) & \text{Otherwise} \end{cases} \quad (8)$$

Finally, the transmit power level to be used for transmission is the minimum of the intermediate value $P1$ and the current transmit power.

$$P = MIN[Tx_{pw}(i), P1] \quad (9)$$

If a vehicle has no message in the high priority messages queue it chooses a double backoff [2] value before transmitting its beacons or the lower priority warning messages. So, this vehicle gives more chances to its neighbors holding a high priority emergency messages to transmit them quickly. This extra delay is managed through the following equation.

$$Extra_{backoff} = rand[0, Backoff \times \alpha] \quad (10)$$

Where $Backoff$ is the currently chosen backoff value and α is a multiplicative factor equals to $\frac{1}{|(|N_{old}| - |N_{1hop}|)|}$ if $|(|N_{old}| - |N_{1hop}|)| \neq 0$, otherwise it is set to a default value equals to 1.

[2]double backoff means that the vehicle chooses twice a random backoff value, then it waits for the sum of both values before trying to transmit a message, if any.

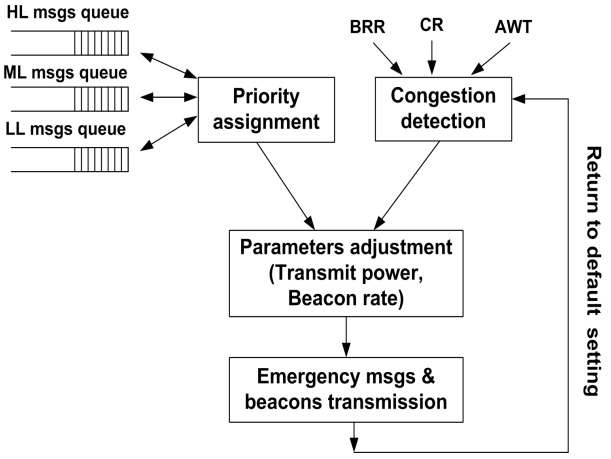


Figure 2: Global overview on our congestion control scheme

Parameters	Values
Road length	10km
Road lane width	3m
Physical layer	OFDM
Frequency band	5.9 GHZ
Channel width	10 MHZ
Transmission range	500 m
Vehicles density	10..60 vehicles /km/lane
Data rate	3 mbps
Beacon transmission rate	10 beacons/s
Beacon size	500 bytes
Emergency messages size	500 bytes
Emergency messages rate	1..3 msgs/s
Simulation time	500 seconds
No. of simulation epochs	10

Table I: Simulation settings

*2) **Beacon rate (B_{rate}) adjustment**:* our beacon rate adjustment scheme is based on two steps, as described below.

- learn the list of vehicles within its carrier sensing range (CS_r): each vehicle analyzes the information contained in the received beacons and control messages of routing protocols to learn the set of vehicles within its CS_r. Next, it extracts the maximal cliques set of the graph representing the topology within its CS_r.
- compute the bandwidth fair share (BF): using the information acquired in the previous step, each vehicle can determine its bandwidth fair share. For the sake of brevity, the details of this step are omitted (the reader may refer to our previous work presented in [11] to get a detailed description of bandwidth fair share estimation).

Based on the calculated BF, the vehicle adjusts its beacon transmission rate as follows:

$$B_{rate} = \frac{BF - B(emergency)}{B_{size}} \quad (11)$$

such that $B(emergency)$ denotes the bandwidth portion reserved for the expected emergency messages. This value varies according to the same parameters used for updating the Thr value, discussed in section IV-B.

V. Simulation setting and results

In this section, we present and discuss the obtained results that evaluates the performance of our congestion control scheme. We have

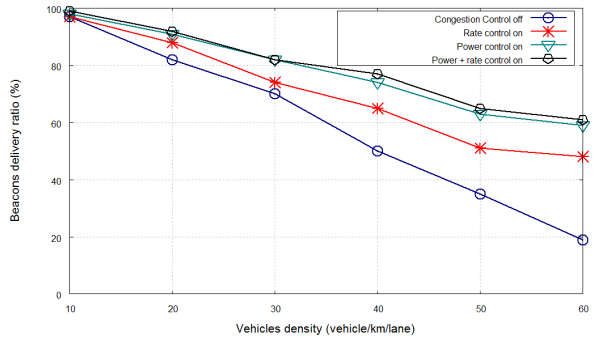


Figure 3: Beacon delivery ratio under varying vehicular densities

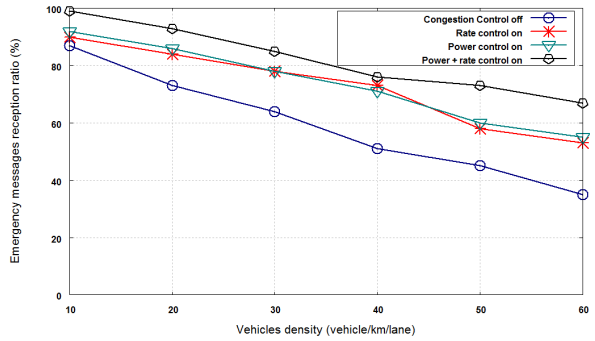


Figure 4: Emergency messages reception ratio under varying vehicular densities

conducted our simulation using OPNET-16.0 [14] which we have extended by adding new functions to the MAC layer component to be compliant with IEEE802.11P specifications. To highlight the effectiveness of our scheme in different VANETs conditions, we perform several simulation scenarios under various levels of vehicles density and emergency messages transmission rates. To run rational simulation scenarios, we have referred to some pioneers studies in the literature regarding VANETs' parameters configuration in real environments. So, we set the beacon transmission rate to 10 packets/s, which is a value that can provide accurate information to the safety components in VANETs as stated in [5]. We have also fixed the beacon size to 500 bytes since it is considered an acceptable value according to the study done in [4]. The setting of the other parameters is summarized in the Table I.

In our simulation, we evaluate vehicular scenarios consisting of 10km bidirectional road section with four lanes. The vehicles move with varying average speed, from 60 km/h to 120 km/h, according to the vehicular density at a given point of time, which corresponds to a real vehicular traffic in many highways. Notice that we have used four traffic density levels (i.e, light, moderate, heavy and jam) to reflect the real situation in different point of time during the day. In our scenario, the RSU broadcasts different types of messages including emergency, warning and information with various rates.

Figures 3 and 4 depict the obtained results in terms of beacons delivery ratio (BDR) and emergency messages reception ratio ($EMRR$), under various traffic density levels. The BDR measures the amount of the broadcasted beacons that have been successfully received by the one hop neighbors of the sender, whereas $EMRR$ refers to the portion of safety related messages that have been successfully advertised to the majority of vehicles. We can clearly observe from the two figures that both of BDR and $EMRR$ are

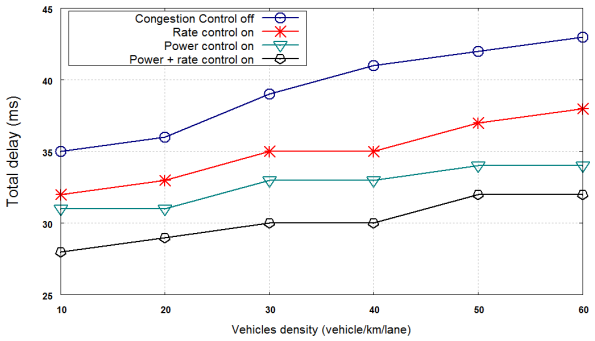


Figure 5: End to end delay of emergency messages transmission under varying vehicular densities

inversely proportional to the vehicles density levels. When the density level is light or moderate (i.e. from 10 to 30 vehicles/km/lane) both of our three schemes (i.e, power control, rate control and joint power and rate control) achieve higher BDR and $EMRR$ compared to the ratio achieved when no congestion control is applied. For heavy vehicles density scenarios (i.e. from 40 to 60 vehicles/km/lane), VANET experiences a sharp decrease of BDR and $EMRR$ when no congestion control is applied. In contrast, our three schemes still achieving acceptable ratios equal to 62% of BDR and 73% of $EMRR$. We remark here that this gain of $EMRR$ is achieved at the detriment of the BDR since the higher priority assigned to the emergency messages and the smart adjustment of the transmit power increase the probability of their successful reception. Additionally, the portion of bandwidth devoted for emergency messages transmission by the rate control scheme will consolidate the previous probability, and meanwhile decreases that of beacons.

As the bandwidth fair share value, defined by our rate control scheme, depends solely on the topology of VANET within the CS_r of the vehicle. So, its value varies whenever any change is occurred in the vicinity of the vehicle. Therefore, the corresponding B_{rate} may be greater than the configured value in the simulation. In this case, our simulator will just transmit 10 beacons, however if it is smaller than 10 then the calculated B_{rate} will be considered rather than the configured value.

We now compare the end to end delay incurred from the transmission of an emergency message to a 8 km faraway vehicle through VANET. As graphed in Figure. 5, the end to end delay varies from 35ms to 43 ms when no congestion control is deployed in VANET. However this delay is gets reduced when we apply our schemes and the highest reduction amount (equals to 20% reduction of the end to end delay) is achieved by the joint power and rate control scheme. We believe that this achievement encourages us to focus our efforts in the future to enhance the efficiency of both of the proposed schemes and find a better way to combine them together since the resulted scheme has shown the highest performance in the herein conducted simulation.

VI. Conclusion

A robust congestion detection and control scheme was introduced in this paper to overcome the drawbacks of the existing works in the literature. In our scheme, we have devised a three complementary stages based scheme that reduces the transmit power or the beacon transmission frequency only in case where congestion is confirmed. Thus, the performance of ITS related applications running on a given vehicle is kept reasonably high since it is altered only for relatively short congestion period. The working principal of our scheme has been evaluated through computer simulation and the obtained results have proven its efficiency.

REFERENCES

[1] B. Karp and H.T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks", *In Proc. of ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), Boston, Massachusetts, Aug. 6-10, 2000.*

[2] M. Durresi, A. Durresi, and L. Barolli, "Emergency broadcast protocol for intervehicle communications", In Proc. of the 11^{th} International Conference on Parallel and Distributed Systems Workshops (ICPADS05), Fukuoka, Japan, Jul. 20-22, 2005.

[3] C. Maihfer, "A survey of geocast routing protocols", *IEEE Communications Surveys & Tutorials, Vol. 6, No. 2, pp. 32-42, 2004.*

[4] M. Raya and J. P. Hubaux, "The security of Vehicular Ad Hoc Networks", In Proc. of the 3^{rd} ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), *Alexandria, VA, USA, Nov. 7, 2005.*

[5] Q. Xu, T. Mak, J. Ko, and R. Sengupta, "Vehicle-to-Vehicle safety messaging in DSRC", In Proc. of the 1^{st} ACM Workshop on Vehicular Ad Hoc Networks (VANET), *Philadelphia, PA, USA, Oct. 1, 2004.*

[6] L. Wischhof and H. Rohling, "Congestion Control in Vehicular Ad Hoc Networks", In Proc. of IEEE International Conference on Vehicular Electronics and safety, *Xi'an, Shaan'xi, China, Oct. 14-16, 2005.*

[7] M. Torrent-Moreno, Jens Mittag, P. Santi and H. Hartenstein, "Vehicle-to-Vehicle Communication: Fair Transmit Power Control for Safety-Critical Information", IEEE Transactions on Vehicular Technologty, *Vol. 58, No. 7, pp. 3684-3703, Sep. 2009.*

[8] Standards Committee, "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: Amendment 8: Medium access control (MAC) quality of services enhancements", 2005.

[9] D. Jiang, L. Delgrossi, "IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environment", In Proc. of the 67^{th} IEEE Vehicular Technology Conference VTC, *Singapore, May 11-14, 2008.*

[10] S. konur and M. Fisher, "Formal Analaysis of a VANET Congestion Control Protocol through Probabilistic Verification", In Proc. of the 73^{rd} IEEE Vehicular Technology Conference (VTC Spring), *Budapest, Hungary, May 15-18, 2011.*

[11] S. Djahel, F. Nat-abdesselam, and D. Turgut, "Characterizing the greedy behavior in wireless ad hoc networks", Security and Communication Networks, Wiley InterScience, *Vol. 4, No. 3, pp. 284-298, Mar. 2011.*

[12] M. Bouassida and M. Shawky, "A Cooperative and Fully-distributed Congestion Control Approach within VANETs", In Proc. of the 9^{th} International Conference on Intelligent Transport systems Telecommunications, (ITST), *Lille, France, 20-22 Oct. 2009.*

[13] E. Hossain, G. Chow, V. Leung, R. McLeod, J. Miic, V. Wong and O. Yang, "Vehicular telematics over heterogeneous wireless networks: A survey", Computer Communications, *Vol. 33, No. 7, pp. 775-793. Elsevier 2010.*

[14] OPNET Technologies, "OPNET Modeler", http://www.opnet.com/.