On the Congestion Control within VANET

Mohamed Salah BOUASSIDA and Mohamed SHAWKY
Heudiasyc UMR 6599 CNRS, Université de Technologie de Compiègne

***Abstract*—The basic objective of congestion control is to best exploit the available network resources while preventing sustained overloads of network nodes and links. Appropriate congestion control mechanisms are essential to maintain the efficient operation of a network. Ensuring congestion control within vehicular ad hoc networks address special challenges, due to the characteristic and specificities of such environment (High dynamic and mobility of nodes, high rate of topology changes, high variability in nodes density and neighborhood, broadcast/geocast communication nature . . .). In this context, we present in this paper a congestion control approach, based on the concept of dynamic priorities-based scheduling, to ensure a reliable and safe communications architecture within VANET. Messages priorities are dynamically evaluated according to their types, the network context and the neighborhood.**

I. INTRODUCTION

Congestion control is a challenging issue within vehicular ad hoc networks. Indeed, it should take into account the characteristics of VANET while ensuring the quality of service, required by the applicative level (cf. Figure 1).

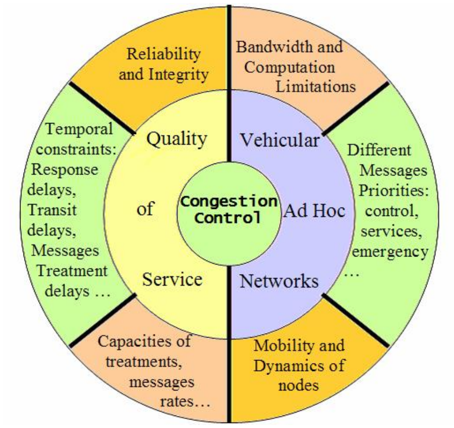

Fig. 1. Congestion control context within VANET.

Vehicular ad hoc networks (VANET) are a form of MANETs used for communication among vehicles and between vehicles and roadside equipment. In addition to the challenging characteristics of MANETs (such as lack of established infrastructure, wireless links, multi-hop broadcast communications), VANET bring new challenges to achieve safe communication architecture within such environment. Indeed, within VANET networks, nodes are characterized by high dynamic and mobility, in addition to the high rate of topology changes and density variability. STIBOR ET AL. [4] evaluate the neighborhood nature of vehicular networks within a four highway lanes context (two lanes for each direction). They carried out simulations and analysis that show that the average number of potential communication neighbors is approximatively four. In addition, in 50% of all occurrences, the maximum potential communication duration is 1 sec ; in 90% of the occurrences, the upper boundary for the communication time is 5 sec. Another important constraint in the multi-hop inter-vehicular communications is the limited bandwidth within a such environment. Indeed, the wireless channel can be occupied by competitive nodes for many reasons (collisions, interferences, insufficient signal strength, duration of the transmission sequence, . . .) [2].

To deal with this environment constraints, and in order to ensure safe and optimized communication architecture (to guarantee required services on a "best effort" network), the establishment of a quality of service policies becomes mandatory, which require the conception of a congestion control approach within VANET. In this context, we propose a new congestion control approach, dedicated to operate within vehicular networks, integrated within the 802.11p underway standard, and based on dynamically scheduling transmitted packets within the network, according to their priorities.

To present our contributions, this paper is structured as follows. Section 2 presents taxonomy of congestion control approaches, within wireless and vehicular networks. In section 3, we present our congestion control approach, based on dynamically scheduling messages according to their priorities. We start by giving an overview on the virtual channelling concept of the 802.11p underway standard. We present then our dynamic priorities assignment and messages transmission scheduling approach. The real applicability of our approach is validated via formal verification, which we present in section 4. Finally, section 5 concludes this paper and presents our future work.

II. RELATED WORK

During the last years, several congestion control approaches have been presented, dedicated to operate within wireless networks. In this section, we cannot claim to present an exhaustive study of these approaches. However, we distinguish two congestion control schemes for wireless networks: end-to-end and hop-by-hop families. End-to-end protocols aim to ensure flows fluidity between senders and receivers, without worrying about the internal relay nodes, whereas hop-by-hop congestion control methods take into account the capacities of the internal links. We present in the following one protocol belonging to these two approaches.

In the proposal of SAHOO ET AL. [3], an end to end congestion control technique is presented, carried out by TCP and physical layers. The adaptive windows based congestion control mechanism used by TCP for wired network may not be appropriate for wireless network. This is due to the time varying nature of a wireless channel and interference from other nodes causing packets loss, which is different from packets loss due to congestion. But, TCP's congestion control mechanism does not discriminate packets loss due to congestion and that due to bad channel or interferences ; it rather applies the same congestion control mechanism for both. For this reason, within the proposed cross layer approach, the MAC layer changes transmission power as per the channel condition and interference received from the neighboring nodes, whereas the TCP layer controls congestion using Reno-2 windowing flow control.

The congestion control approach proposed in [5], dedicated to operate within vehicular ad hoc networks, consists of adapting transmissions to the available bandwidth in a hop-by-hop manner. Thus, nodes transmitting information with a high utility for VANET will be allowed to consume a larger share of the available bandwidth. A priority is evaluated for each packet, depending on its utility and size. Then, an instantaneous data rate is determined, according to the computed priority. This approach requires context exchange between neighbor nodes, which generates a communication overhead.

On the one hand, as argued in [6], end-to-end congestion control approaches are not suitable for vehicular ad hoc networks. Indeed, within these approaches, relay nodes context are not considered, and thus, interferences, collisions and transmission problems are not taken into account. However, the required quality of service of a transmission can be defined by the sender with end-to-end congestion control approaches.

On the other hand, hop-by-hop approaches suffer from lack of scalability, when the number of transmitted flows increases within the network. However, it is known that the size of the transmitted data within VANET is not considerable, due to the dynamic nature of this environment, and to the nodes limitations in terms of storage and computation capacities. It is thus proved that hop-by-hop congestion control approaches are the most suitable for VANET, while taking into account the required quality of service of the transmitted data, as for the end-to-end approaches. Hop-by-hop congestion control approaches, described above, present some lacks (generation of communication and computation overheads, reactive congestion control techniques, idealistic verification frameworks . . .).

We propose in the next section a congestion control approach, considering these drawbacks, whose design should ensure the following objectives:

- Adaptive congestion control approach: approach dynamically adaptable to the context of VANET, while taking into account the required QoS metrics (in terms of reliability and delays).
- Hop-by-hop approach, to take into account relay nodes, while considering the required quality of service as for the end-to-end congestion control approaches.

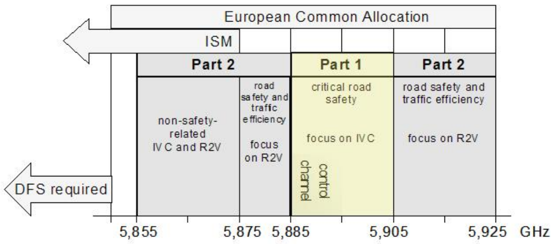

Fig. 2. 802.11p Channeling.

- Cross layered approach, while remaining adapted to the IEEE 802.11p underway standard.
- Applicative layer congestion control approach, in order to define packets priorities according to their application and their utilities in the network.
- Definition of policies and directives to fix a maximum duration of a transmission per VANET node and a maximum number of transmissions per time interval.
- An efficient compromise between proactive nature (to treat high priority safety and emergency messages without delays) and low energy and computation consumption overheads. No additional equipments could be required, or bandwidth consumption due to communication overhead should be generated.

III. Dynamic Message Scheduling Approach within VANET

In this section, we present a congestion control approach dedicated to operate within VANET. The basic idea of this applicative-layer approach is to define congestion control policies, based on dynamically scheduled messages transmission in the network. Messages scheduling is carried out according to priorities, evaluated as a function of the utility of the concerned messages, the sender application and the neighborhood context. To present our contributions, we describe first the 802.11p underway standard environment, and its influence on the congestion control policies. We then present the principle steps of the approach: dynamic priority assignment, messages scheduling and messages transmission. Finally, we summarize these steps within an algorithm.

A. 802.11p Multi-Channeling

VANET architecture is dealing with a single media based on the European version of IEEE 802.11p (together with IEEE 1609.x). This media is currently under standardization. The multi-channel operation, as specified in the C2C CC decision (cf. Figure 2), implies that a simultaneous reception on two channels should be possible, in case that the incoming signals levels do not differ by more than the adjacent channel rejection value (37 dB). Transmitting on both channels simultaneously will not be required. To ensure compatibility with 802.11a, the system might be emulated using IEEE 802.11a or single receiver IEEE 802.11p".

The two VANET wireless channels (control and service channels) are used for different traffic as such further congestion control mechanisms will differ slightly.

1) Control Channel (CCH): The control channel is primarily used for the transmission of beacons and high / first hop priority traffic. All messages that are necessary to maintain the VANET are transmitted on this channel, especially the network layer beacons. Furthermore high priority messages (emergency notifications) are sent on this channel. Normally, such messages occur on an event basis. With multihop communications, only the first hop will require high priority. JIANG ET AL. define the basic link layer behavior of safety communications in the control channel as single-hop (direct communication among vehicles, within range of one another), uncoordinated (distributed communications without coordinator), broadcast messaging (self-contained short messages) in an unbounded system, consisting of all neighboring equipped vehicles in a dedicated channel [1].

2) Service Channel (SCH1): This channel is available for safety applications with lower priority. Here periodic messages could be sent. This channel should also be used by forwarders of multihop and geocast messages. A second service channel (SCH2) is dedicated to short distance peer to peer VANET communications, with reduced power level. However, this service channel is currently unused.

B. Priority Assignment

Packets will be assigned a priority by the messages generators, when they are created. The relative time of transmission of each priority level will however vary as network density increases, with medium and low priority packets, being delayed more to allow high priority packets to be sent without excessive delays. The priority of a packet is composed of 2 fields: the first is static, deduced from the application type and the second is dynamic, obtained from the specific context of the VANET and determined by the congestion control module. The dynamic and the static fields are combined to obtain the overall priority indicator.

Lets $Pri_{message}$ indicates the priority of a message. $Pri_{message}$ is evaluated as follows:

$$Pri_{message} = Dynamic\_factor \times Stat\_Pri_{message}/Msg\_size \tag{1}$$

Where $Stat\_Pri_{message}$ denotes the static priority of the message, $Dynamic\_factor$ denotes the dynamic factor of the priority to take into account network context and Msg_size denotes the size of the message.

1) Static Factor from Application Class: The static priority factor is defined according to the sender application, and the content of the message. We adopt five priority levels: $PRI_{Emergency}$ is the priority affected to single hop emergency messages to notify an important event without delay, PRI_{VANET} is the priority affected to the network layer beacons, PRI_{HIGH} is the priority affected to high priority safety applications, PRI_{MID} is the priority affected to normal safety applications and PRI_{LOW} is the priority affected to low priority safety applications.

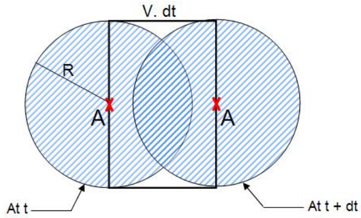

Fig. 3. Node speed consideration.

Regarding Multihop and Geocast communication it is assumed that only the first hop can have the priority $PRI_{Emergency}$. It is assumed that these priority levels are associated with the application classes, but when communicating in geocast or multihop modes, this describes only the communication priority on the first hop.

2) Dynamic Factor from Network Context: We present in the following the basic policies of our congestion control approach within VANET, to evaluate the dynamic priority factor of sent messages[1]:

- **Node Speed Consideration**
  The Dynamic factor takes into account of the node speed, according to the covered zone at each dt, as illustrated in Figure 3. The priority of a messages increases when the speed of the sender increases. Thus, at each dt, the dynamic factor is re evaluated as follows:

$$Dynamic\_factor = \frac{\pi R^2 + 2RV.dt}{\pi.R^2} \tag{2}$$

  Where R: communication range, V: mean speed.
- **Message Utility Consideration**
  The dynamic factor takes also account of the utility of the sent message, according to the number of its retransmissions by the neighborhood, in case of periodic or geocast messages. Thus, when a node A has to send a periodic or geocast message M, and receives the same message M, sent by another node B (cf. Figure 4), it should calibrate the dynamic factor of the message M, in order to take into account the zone covered by the node B, compared to its communication range zone ($= \pi.R^2$ with R is the communication range). The smaller is the covered zone, the higher is the priority to send the message. The dynamic factor is thus equal to the ratio between the total zone covered by the receiver and the already covered zone (CZ):

$$Dynamic\_factor = \frac{Total\_Zone}{Covered\_Zone} = \frac{\Pi R^2}{CZ} \tag{3}$$

  To evaluate the covered zone CZ by the node B (doubly hatched in Figure 4) at the side of the node A, we carried out the following operations (we note d the distance between A and B, and R the range of A and B):

$$CZ = 4 \times surface\_ODC = 4 \times (surface\_ADC - surface\_AOD) \tag{4}$$

[1]A part of this work has been carried out jointly with the VANET research group in the HEUDIASYC laboratory

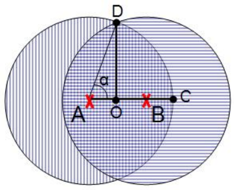

Fig. 4. Message utility consideration.

$$surface\_ADC = \frac{\alpha \Pi R^2}{2\Pi} = \frac{\alpha R^2}{2} \quad (5)$$

$$d(O,D) = \sqrt{R^2 - (\frac{d}{2})^2} \Rightarrow surface\_AOD = \frac{d}{2} \times \sqrt{R^2 - (\frac{d}{2})^2} \quad (6)$$

$$\cos(\alpha) = \frac{d(A,O)}{d(A,D)} = \frac{d}{2R} \quad (7)$$

(4) & (5) & (6) & (7) $\Rightarrow$

$$CZ = 4 \times \left(\arccos\left(\frac{d}{2R}\right) \times \frac{R^2}{2} - \frac{d}{2} \times \sqrt{R^2 - (\frac{d}{2})^2} \right) \quad (8)$$

(3) & (8) $\Rightarrow$

$$Dynamic\_factor = \frac{\Pi R^2}{4 \times \left(\arccos\left(\frac{d}{2R}\right) \times \frac{R^2}{2} - \frac{d}{2} \times \sqrt{R^2 - (\frac{d}{2})^2} \right)} \quad (9)$$

- **Message Validity Consideration**
  The dynamic factor takes into account the message validity (maximum duration of the message). As for the EDF scheduling approach (Earliest Deadline First), the message whose deadline is earliest, holds the highest priority. The dynamic factor is thus computed as follows:

  if remaining_time_to_deadline $\neq 0$
  Dynamic_factor = 1 / remaining_time_to_deadline
  else Dynamic_factor = 1
  end if

C. Messages Scheduling

Each node schedules its messages according to their priorities. We divide the scheduling process into two types: static and dynamic, presented hereafter:

1) Static Scheduling: The static scheduling process consists of affecting messages according to their priorities, into the suitable communication channel queues. $Pri_{Emergency}$, PRI_{VANET} and PRI_{HIGH} priority messages are affected to the control communication channel queue, whereas PRI_{MID} and PRI_{LOW} priority messages are affected to the service queue one.

2) Dynamic Scheduling: Periodically, each node triggers a rescheduling process, consisting of scanning the messages queues, and computing the overall priority indicator for each message (taking into account the dynamic factor of each priority, presented above). The rescheduling process then reorders the messages according to their new computed priorities.

Considering that the number of messages sent within the control channel is smaller than the number of messages sent within the service one, we adopt the following policy: when the service channel is overloaded and the control channel is free, messages within the service queue are switched to the control one, and considered as high priority messages. We consider that the service channel is overloaded if the number of messages in the queue exceeds a defined threshold, called ”Service Channel Congestion Threshold”.

D. Messages Transmission

Messages transmission process sends the highest priority message within the corresponding channel, whenever it is free. However, sending high priority packets via the control channel is preemptive, comparing to packets sent via service channel. Indeed, in order to send high priority packets with the minimum delays, lower priority packets sending is freezed, even if their corresponding channel is free. In addition, when a node receives messages of higher priority than messages that it will send (the first messages in its queues), it freezes its sending.

Concerning the dynamic use of the bandwidth within VANET, the IEEE 802.11p underway standard supports three mandatory user data rates 3 Mbit/s, 6 Mbit/s and 12 Mbit/s within a 10 Mhz channel, and some optional data rates up to 27 Mbit/s. Obviously, the most robust data rate is the 3 Mbit/s one. This rate must be shared among all applications and vehicles inside the interference range. Note that the interference range is a multiple of the communication range. In order not to saturate the provided bandwidth and to allow a reliable transmission of the emergency messages, the bandwidth offered to VANET application per 10Mhz is equal to the half of the total bandwidth. We present hereafter how a vehicle i can compute the effective bandwidth it can use.

Let n denotes the number of neighbors of the node i, a denotes the average number of applications per node, defined at the bootstrap. The number of all the applications N_A within an interference range, reaching the bandwidth, is thus equal to:

$$N_A = 2a.(n+1) \quad (10)$$

The effective bandwidth that an application can use within the vehicular network is thus computed as:

$$Effective\_Bandwidth = \frac{Selected\_Bandwidth}{2a.(n+1)} \quad (11)$$

Note that the effective bandwidth computed at the side of a node is equal to the selected bandwidth multiplied by the percentage of the active sending time:

$$Effective\_Bandwidth = Selected\_Bandwidth \times Active\_Time \quad (12)$$

The percentage of the active sending time, in which a node can offer the bandwidth to an application is thus:

$$Active\_Time = \frac{100}{2a.(n+1)}\% \quad (13)$$

As an example, if the number of vehicles within a neighborhood is equal to 10, with 5 running applications in each vehicle, the active time is equal to 1%. The effective bandwidth for each application is equal to 15 Kbit/s.

The two parameters defining the active sending time are the maximum data transmission duration and the minimum interval between data transmissions, as follows:

$$Active\_Time = \frac{Maximum\_Data\_Transmission\_Duration}{Minimum\_Interval\_Between\_Data\_Transmissions} \quad (14)$$

To continue with the same numerical example presented above (effective bandwidth = 15 Kbit/s) and if we define the minimum interval between data transmissions equal to 1 sec, the maximum data transmission duration is evaluated at 5 ms.

IV. Analysis and Validation

In order to verify and validate our congestion control technique, we propose to specify it using temporized automata, through the Uppaal[2] integrated tool environment for modelling, validation and verification of real-time systems. Uppaal is developed in collaboration between the Department of Information Technology at Uppsala University, Sweden and the Department of Computer Science at Aalborg University in Denmark.

Uppaal is a tool box for validation (via graphical simulation) and verification (via automatic model-checking) of real-time systems. It consists of two main parts: a graphical user interface and a model-checker engine. The idea is to model a system using temporized automata, simulate it and then verify properties on it. A real-time system in Uppaal is composed of concurrent processes, each of them modelled as an automaton. The automaton has a set of locations. transitions are used to change location. To control when to fire a transition, it is possible to have a guard and a synchronization. A guard is a condition on the variables and the clocks saying when the transition is enabled. The synchronization mechanism in Uppaal is a hand-shaking synchronization: two processes take a transition at the same time, one will have a **!a**, and the other **a?**, **a** being the synchronization channel. The verification tool provided by Uppaal, checks for the following properties: reachability, safety, liveness and no deadlock.

To simulate, via UPPAAL, our priority-based scheduling mechanism within VANET, we divide our system into four independent sub-systems: message manager, congestion control message enqueueing, congestion control message dequeueing and transmission engine automata. We present hereafter the congestion control message enqueueing automaton (cf. Figure 5).

We randomly simulate all the possible transitions of the four automata. This verification step validates the following results:

- No deadlock in the operation of our messages priorities-based scheduling approach. All states of the modelled automata have successors.
- All states of the modelled automata are eventually reachable.
- All the high priority messages are effectively sent on the control channel. However, some low priority packets can be deleted, due to service channel congestion (bounded service messages queue).
- The sending of high priority messages is preemptive comparing to the emission of low priority messages. Service messages are sent only when there is no any control message in the queue of the control channel.
- In addition, the emission of a high priority message is carried out without delay. All the high priority messages are considered as emergency, requiring thus to freeze the emission of lower priority messages.

[2]www.uppaal.com

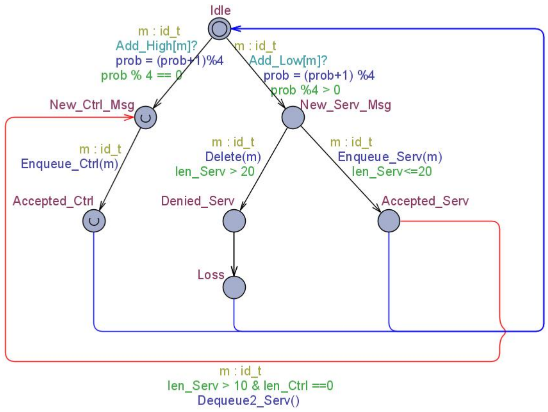

Fig. 5. Congestion Control Message Enqueueing.

V. Conclusions and Future Work

We considered in this paper the congestion control issue within vehicular networks. We summarized in a first step existing research works on this topic, then we presented a congestion control approach, based on dynamic priority scheduling transmissions. This approach takes into account the network load and the neighborhood context to adapt the priorities of the sent messages via the control and service communications channels. The efficiency of this congestion control technique was validated, through formal verification, via the UPPAAL verification tool. As future work, we plane to consider the reliability issue for the transmission of multimedia data within VANETs, while taking into account the specific quality of service required by this kind of transmitted data.

References

[1] D. Jiang, V. Taliwal, A. Meier, and W. Holfelder. Design of 5.9 GHz DSRC-based Vehicular Safety Communication. IEEE Wireless Communications, Vol. 13 No. 5, pages 36-43, October 2006.

[2] E. Minack. Evaluation of the influence of channel conditions on Car2X communications. Dilpoma thesis. Chemnitz University. November 2005.

[3] H.K. Rath and A. Sahoo. Cross layer based congestion control in wireless networks, technical report, April 2006.

[4] L. Stibor, Y. Zang and H.J. Reumerman. Neighborhood evaluation of vehicular ad-hoc network using IEEE 802.11p, In Proceedings of The 8th European Wireless Conference, p. 5, Paris, France. 2007.

[5] L. Wischhof and H. Rohling. Congestion control in vehicular ad hoc networks. In IEEE International Conference on Vehicular Electronics and Safety, 2005. pages 58-63.

[6] Y. Yi and S. Shakkottai. Hop-by-hop congestion control over a wireless multi-hop network. IEEE Transactions Networks, 15(1):133-144, 2007.