

A Cross-Layer Framework for Best Internet Access in Vehicular Networks

G. Ruggeri, S. Polito, A. Molinaro, A. Iera

Università "Mediterranea" di Reggio Calabria- D.I.M.E.T.

Via Graziella, Località Feo di Vito, 89060 Reggio Calabria Italy.

E-mail (giuseppe.ruggeri, sergio.polito, antonella.molinaro, antonio.iera)@unirc.it

Abstract—From the analysis of feasible applications in the field of vehicular networks it clearly emerges that a key factor for their success will be granting vehicles a constant connection to the Internet, able to provide QoS support. Unfortunately, in spite of these strong requirements, gaining Internet connectivity in a VANET is a very challenging objective. In this paper, we discuss some cross-layer principles that could drive the augmentation of widely accepted and deployed protocols, such as SIP at the application level and AODV at the network level, to provide vehicular users with the best available Internet access.

I. INTRODUCTION

Design and deployment of vehicular networks is a recent innovation in the wireless communications scenario. In such networks a vehicle, equipped with a wireless radio interface, directly transmits information to other vehicles without the use of either a previously deployed infrastructure or a centralized control. Such inter-vehicular networks, in which vehicles on the roads dynamically form continuously changing topologies, are often referred to as Vehicular Ad-hoc Networks (VANET). Studies have demonstrated that moving vehicles in a VANET can exploit high-bandwidth, short-range communication technologies, such as the IEEE 802.11-based standards [1].

When analysing likely applications for vehicular networks, the most relevant categories undoubtedly result to be computer-aided driving and passenger entertainment. In both cases, a common requirement is the ability of the network to offer a constant access to the Internet together with a controlled Quality of Service (QoS) to the users. These latter will likely be critical factors to the success of vehicular networks. Unfortunately, in spite of these strong requirements gaining Internet connectivity in a VANET is a very challenging objective that requires the presence of suitable nodes, called *gateways*, which provide connectivity towards external networks. They can either be *stationary*, i.e. placed at fixed positions along the roadside, or "travel" on board some vehicles and act as *mobile* gateways. An ad-hoc network allows vehicles in a VANET to communicate to both roadside and on-board Internet gateways. It is obvious to suppose that the vehicles do not know a priori which gateway will be available in their neighborhood, and it is likely that the same area can be covered by more than one gateway. Therefore, in such a scenario, the method to discover and select the "right" gateway, which users' traffic has to be delivered through, turns to be a factor of utmost importance. Obviously, the choice of the right

gateway is likely to differ from application to application, this complicating the scenario. In fact, gateways available in a certain area can be owned by different providers, each offering their specific pricing, QoS, and administrative policies to registered users. As an example, let us suppose that a user signed an agreement with two service providers, let's say *SPA* and *SPB*. *SPA* offers a cheap fare and best effort traffic delivery; *SPB* allows for stringent QoS support at a higher fare. The user will likely transmit best effort traffic through a gateway belonging to *SPA*, and QoS demanding flows through a gateway belonging to *SPB*. Unfortunately, the gateway selection procedure is not as simple as stated above, since it can be affected also by (i) the *location* of the gateway, and (ii) the *quality of the path* in the VANET from the user to the candidate gateway. In the example above, a user willing to initiate a QoS sensitive session to an external network could discard the *SPB* gateway, when he/she is aware that the path to this gateway through the VANET is unstable or congested.

Above reported considerations clearly define the choice of the right gateway as an inherently *cross-layer* issue. In fact, service subscription and pricing usually pertain to user/application levels; setting up a QoS application is a typical session initiation problem; finding the route to a gateway is usually accomplished through network-layer procedures and, finally, collecting information about the state of a link is fulfilled by Medium Access Control (MAC)/Physical layer functions.

In this paper, we propose a framework based on cross-layer principles, which combines the functionalities of SDPng (Session Description Protocol Next Generation) [2], an IETF application protocol used to describe multimedia sessions, with a popular routing protocol for mobile ad hoc networks, Ad hoc On-Demand Distance Vector (AODV) [3], and with the MAC protocol of 802.11-based Wireless Local Area Networks (WLANs).

II. BACKGROUND

Many aspects of the gateway selection, such as *gateway discovery* and *end-to-end QoS signaling*, have been widely addressed in the scientific literature, mainly as individual topics. A good reference for what we call a *network-level* approach (when gateway discovery is considered as an extension of the routing procedure) is [3]. The authors augment AODV with gateway discovery capabilities to provide Internet connectivity to nodes in a mobile ad hoc network.

The extended version of the protocol, named AODV+, uses a new control message, called RREP_I, which is sent back by the gateway after receiving a route request (RREQ) message for an intended destination located outside the ad-hoc network. The source node uses the RREP_I message to select one of the responding gateways, e.g. the nearest one. The authors of [4] propose an extension of [3] which takes into account the life-time of the paths to the candidate gateways to choose the best one to access the Internet. The life-time of a link is predicted by supposing that each vehicle knows its own position, speed and direction and those of all its corresponding nodes, and by assuming a free space propagation model evaluated only once, during the route discovery phase. Path life-time is utilized to (i) select, among available paths, the one with the longest life-time, (ii) and to trigger a new route discovery procedure before the old one actually crashes. The obtained performance is better than the one obtained through the basic protocol presented in [3]. However, it still suffers from some inefficiencies mainly related to the simple way path-lifetime is computed and to the choice of estimating the path-lifetime only once, during the route set-up phase. A single estimation, in fact, does not allow to take into account the frequent topology changes occurring in a VANET. The approach we introduce in the present paper is based on a constant monitoring of the channel quality; thus, it is expected that weaknesses highlighted in [4] can be overcome. As for the QoS management issue, reference [5] provides a mechanism for end-to-end QoS provisioning in complex heterogeneous networks through a policy-based management of the IP backbone. Users in a wired access network are connected to the backbone via a special gateway device acting as both a Policy Enforcement Point (PEP) [6] and a Session Initiation Protocol (SIP) [7] proxy. Each time a user wants to start a QoS session, he/she issues a SIP INVITE message to the gateway. This latter translates SIP parameters into QoS requirements and starts a policy negotiation process with the Policy Decision Point (PDP) [6]. If enough resources are available in the IP backbone and the user has sufficient privileges, then the policy negotiation succeeds and the gateway forwards the SIP INVITE message; otherwise the session ends. A limit of SIP-based QoS lies in its restricted parameter set, consisting of codecs and requested bit-rates. This set does not allow the user to express more complex expectations about the QoS levels for the requested services. In this paper, we somehow exploit both approaches in [3] and [5] together with throughput and delay estimation presented in [8] by proposing a cross-layer framework to allow a mobile host in the VANET selecting "the best" gateway to the external network. Selection takes into account, at the same time, both low-level parameters (such as, desired throughput and delay) monitored by the routing-MAC layers and higher level ones (such as cost, service level agreements, operator), controlled at the application layer.

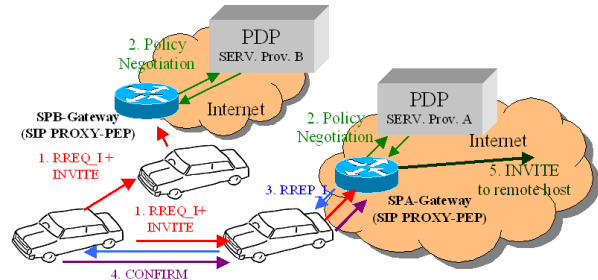


Fig. 1. Network scenario and Signaling flows

III. THE PROPOSED "CROSS-LAYER" FRAMEWORK FOR BEST GATEWAY SELECTION

In this section we summarize the reference scenario (sketched in Fig. 1), the main procedures, and the novel features of our approach. Since our main focus is on QoS provisioning to multimedia services, we suppose that mobile nodes support SIP protocol and use it to start their multimedia sessions. Like in [5], we also assume that it is possible to gather indications on the QoS levels required by the users from session description parameters. SIP expressiveness is augmented in our proposal by using an enhanced session descriptor protocol, namely SDPng [2].

In our reference scenario, gateways behave as SIP proxies, able to check users' Service Level Agreements (SLAs) and to assess the network resources that can be assigned to them. For instance, in a policy-based core network, gateways can implement Policy Enforcement Points (PEPs) and use COPS protocol to interact with Policy Decision Points (PDPs), which in turn manage the core network they belong to [6]. QoS management techniques used across the backbone network fall out of the scope of this paper, the focus being on the access network.

A. Gateway Selection

This phase requires cooperation between application (SDPng) and network (AODV) layers. When a user wants to start a multimedia session (see fig. 1) he/she declares (1) user and application requirements within the SIP INVITE message, by using SDPng [2] session description protocol. We propose the SIP INVITE message *to be embedded into the payload of routing discovery packets (RREQ)*. Gateways must assess the ability of the external networks, along the path to destination, to match user end-to-end QoS requirements. To this aim, they also use information, coming from MAC and Physical layers, about the achievable QoS levels within the VANET segment, collected while routing requests cross the VANET. Parameters taken into account are maximum achievable throughput, minimum delay, and estimated path life-time. Gateways compare (2) the user's requirements with their own capabilities and with those of the external networks they are connected to. Only gateways which are able to offer the required QoS levels and application features respond (3) with a *route reply* message. The user chooses a gateway, among those

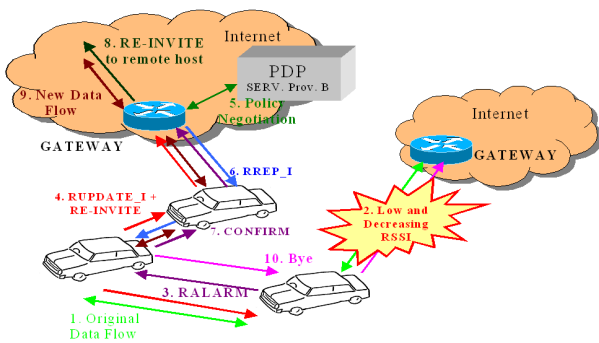


Fig. 2. Signaling Flow during Handover

which replied to the route request message, i.e. the one with the longest path life-time, and issues (4) a confirmation message to that gateway. Finally, upon receiving the confirmation message, the gateway forwards (5) to the final destination the SIP INVITE message received during step 2.

B. Route to the Gateway Maintenance

This phase requires the network layer (AODV) to receive values of monitored parameters at the Physical layer. By referring to Fig. 2, when a path is set up (1) all the nodes continuously monitor the *RSSI* (Received Signal Strength Indication) from their neighbors. When one of them realizes (2) that the link is rapidly deteriorating (please refer to section IV for details), then it labels the route as “*expiring*” and “*critical*”. The label “*expiring*” means that a route is going to be updated, while the label “*critical*” means that the link to the next hop is rapidly going to break. Once the host has labeled its routing table, it issues (3) a “*Route-Alert*” Message upstream to the Sender. Each node in the route modifies its routing table entry, by labeling the route as “*expiring*”, and keeps on forwarding the alarm message upstream to the Sender. However, all the nodes continue to use the existing route to forward the data packets. The source, upon the reception of the “*Route-Alert*” Message, assembles (4) a SIP *re-invite* message including the description of its requirements by using SDPng [2], as we will describe later. The *re-invite* message is embedded into a “*Route-Update*” Message. Once again, we have cross-layer cooperation between application and network layers. When a host receives the “*Route-Update*” Message, it performs the same operations as in case of a “*Route-Request*” Message, with the exception that it avoids to reuse cached routes to the destination; rather it performs next-hop discovery. We suppose a route may overlap with another one already existing, but we do not allow it to include links labeled as “*critical*”.

At the end of the discovery phase, all the gateways able to handle the user traffic respond (5-6) with a “*Route-Reply*” Message. Similarly to the set-up case, the user chooses a gateway, among those which replied to the “*Route-Update*” Message, and sends (7) to it a “*Confirm Message*”. When a router receives a “*Confirm Message*” there are two possi-

bilities: (i) it is the same gateway which was already forwarding the user traffic (the route in the ad-hoc has been repaired and the gateway is unchanged), or (ii) it is a new gateway. In the former case, it continues to do its job as before; in the latter case, it forwards (8) the re-invite message to the remote destination, and the communication flow can continue between sender and receiver through the new gateway (9). As soon as the user receives data from the new gateway, it sends a *bye* message to erase all routing entries labeled as “*expiring*” (10).

IV. ESTIMATING THE PATH-LIFETIME

Each nodes continuously evaluates the *RSSI* of each link connecting to its neighbors. These values from Physical layer are processed by the routing protocol at the Network layer.

Each time a node receives a frame, it measures the received *RSSI* and computes the variation with respect to the former measure, according the following equation:

$$\Delta RSSI(t_{actual}) = \frac{RSSI(t_{actual}) - RSSI(t_{former})}{(t_{actual} - t_{former})} \quad (1)$$

where t_{actual} and t_{former} represents the time instants of the current measure and the former measure, respectively. To filter out fluctuations in equation (1), we consider an averaged measure $\overline{\Delta RSSI(t_{actual})}$, which is obtained from $\Delta RSSI(t_{actual})$ through an Exponential Weighted Moving Averaged (EWMA) with a suitably chosen smoothing factor α_{RSSI} .

If $\overline{\Delta RSSI(t_{actual})}$ is greater than, or equal to, zero, the path is assumed to be not in critical phase, and *path-lifetime* is set to infinity; otherwise, it is supposed that *RSSI* will decrease in the next future with a constant trend. Therefore, the *path-lifetime* (*plt*) is related to $RSSI_{t_{actual}}$ and to the receiver sensitivity (S) (i.e. the *RSSI* value, below which the receiver is not able to work properly) through the following equation:

$$[RSSI(t_{actual}) - S] + \overline{\Delta RSSI(t_{actual})} \cdot plt \geq 0 \rightarrow \quad (2)$$

$$plt \leq \frac{(S - RSSI_{t_{actual}})}{\overline{\Delta RSSI(t_{actual})}}$$

Each node, during the data exchange phase, continuously estimates the *path-lifetime*. If the estimated *plt* becomes shorter than a given time interval HO_time , the node triggers a “*Route update*” procedure, as described in section III. The time HO_time is chosen to minimize unnecessary “*Route update*” procedures and, at the same time, to maximize the probability that, when triggered, they are completed before the old route definitively breaks. After a thorough simulation campaign we have chosen to set $HO_time = 1.5sec$.

V. MAC LEVEL QoS MONITORING

In our reference framework QoS routing choices at the network layer are accomplished through cooperation with the MAC layer. QoS control at the MAC layer is achieved through the IEEE 802.11e standard [9]. More specifically,

QoS is managed, through the Enhanced Distributed Channel Access (EDCA), by applying traffic prioritization to MAC frames of four different classes, based on traffic requirements. Delay sensitive voice traffic is handled at the highest priority; video traffic gets the subsequent priority level; finally, flows marked as best effort and background are managed by decreasing classes of priority. A packet coming from the network layer is first queued at the Logical Link Control (LLC) layer until it is transmitted by the MAC protocol. The time required by this latter to transmit a packet ($D_{MAC,i}$) depends on many factors, such as: the physical transmission rate (dynamically adapted by the station), a random back-off interval before transmission, the possible retransmissions due to collisions with other frames, and its EDCA priority i . $D_{MAC,i}$ is related to the maximum throughput ($MaxTh_i$) achievable by a station at the EDCA priority i through $MaxTh_i = \frac{PktSize}{D_{MAC,i}}$, $i = 0, \dots, 3$, where $PktSize$ is the packet length [8]. Thus, the total time spent by a packet in the data link layer (DLL) ($D_{DLL,i}$), consisting of both LLC and MAC layers, is given by the sum of $D_{MAC,i}$ and the time spent in the queue. In our framework, a station measures both $D_{DLL,i}$ and $D_{MAC,i}$ for each sent packet and averages them through an Exponential Weighted Moving Average (EWMA) technique with a smoothing factor set to 0.4 according to [8]. For each station, QoS routing relies on such cross-layer cooperation with MAC and LLC layers to estimate achievable delays and throughput. More details on this issue are available in [8].

VI. QoS-AWARE ROUTING TOWARD GATEWAYS

According to the proposal presented in [10] (which in the following will be referred as AODV-QoS) we extended AODV+ [3] protocol by means of two additional fields in the RREQ message. Those fields, named $MinTh$ and $Maxe2eDelay$, carry respectively the minimum throughput and the maximum end to end delay tolerated by the user. Differently from [10], where the proposal has been done independently of the protocol adopted at MAC layer, in the present work we consider 802.11 based VANET, therefore we have a practical way to estimate the delay spent at every hop and the available throughput along the path (see section V). We further considered another additional field in the RREQ message, namely $ExpLifetime$, which carries information concerning the expected route lifetime, and a new routing message (CONFIRM), needed to confirm the selection of a single gateway.

In our framework, when a host issues a RREQ message, it initialises $MinTh$ and $Maxe2eDelay$ to the values specified by the user, and sets $ExpLifetime$ to infinity. Then, it inserts in the RREQ message the MAC level priority i , chosen to forward the traffic, and the size of the packets intended to be sent. As a first approximation, we assume that fixed-size packets are sent by the source node.

Each node along the path reads the new fields and updates them accordingly with the estimation made with cooperation of MAC and Physical layers. More specifically, it subtracts from $Maxe2eDelay$ the value $D_{DLL,i}$ (see sec-

tion V), and sets $ExpLifetime = \min(ExpLifetime, plt)$ (see section IV).

Before forwarding a RREQ packet, and just after the updating process has been completed, each node checks that:

$$\begin{cases} MinTh \geq \frac{PktSize}{D_{MAC,i}} \\ Maxe2eDelay \geq 0 \end{cases} \quad (3)$$

Only if both the conditions expressed in (3) are true, then the RREQ message is forwarded, otherwise it will be discarded. When a gateway (which acts as a SIP proxy server) receives the RREQ message, it can have a clear description of both the user/application requirements, contained in the encapsulated SIP message, and the QoS degree offered in the VANET. More specifically, the values of $MinTh$ and $Maxe2eDelay$, which have been updated along the path, contain the minimum throughput and the maximum end-to-end delay allowed in the remaining part of the path toward the destination. Therefore, as described in section III, the gateway is able to start a negotiation phase with the core network, to assess two disjoint sets of requirements: (i) *QoS constraints towards destination*, i.e. the ability of the core network to deliver traffic to the destination within the maximum tolerated delay and at the minimum rate desired by the user; (ii) *application/user preferences*, written in the SDPng header of the SIP INVITE message, concerning application-layer features such as pricing and security. In such a way, the gateway is asked to manage low-layer and high-layer aspects at the same time, in a fully cross-layer fashion.

Differently from the legacy protocol [10], we introduce a further unicast routing message, called *Route Confirmation Message* (CONFIRM), that is issued by the user towards one of the gateways (e.g. the nearest one) that answered the Route Request, if any. Upon receiving a CONFIRM message, the selected gateway forwards the original SIP INVITE message to the external network, and the multimedia session establishment can continue. Candidate gateways, which do not receive a CONFIRM message before the expiration of a given timer, reset the current session initiation/routing procedure.

Once the session is established, the routing layer of each VANET node along the path continuously monitors both the QoS performance parameters exported by the Data Link Layer and the Physical layer parameters. If either QoS performance negotiated during the route setup procedure can no longer be met or a link is rapidly going to break, then it issues a “Route-Alert” message and triggers a “Route-Update” procedure, as described in section III-B. This procedure requires continuous cooperation between Physical, MAC/LLC, and Network layers.

VII. THE DESCRIPTION OF SERVICE REQUIREMENTS

The SDPng protocol [2] has been developed as an extensible framework, based on XML (Extensible Markup Language), aiming at describing multimedia sessions and negotiating end-host capabilities. SDPng session descriptions, usually embedded within session initiation messages, e.g. SIP messages, can be provided with an optional section,

called *Session Information*, reserved to specify additional data about the session.

We propose to fill packets belonging to a SIP session initiation procedure from a VANET node with high-layer user/application preferences declared through SDPng, and then to carry these packets into AODV route discovery packets. Therefore a RREQ messages contains both high and low-layer parameters.

A simple SDPng description could include the following high-layer parameters, which help the gateways to choose an external network to the Internet: (i) *preferred service providers* the user has subscribed an agreement with; (ii) *security and privacy level*, representing the user requirements on data confidentiality; (ii) *maximum cost* the user is willing to pay for the required service, expressed through a suitable metric.

VIII. COMPARING LEGACY AND PROPOSED APPROACHES

In this section we present a simulation campaign, carried out through ns2 (Network Simulator v2) to assess the performance of the proposed route selection approach. We compare our solution, in the following referred to as *HO_prediction*, with two reference algorithms: legacy AODV-based gateway discovery approach, proposed in [3], which does neither implement smart gateway selection nor handover management strategies, called *legacy*; and a simplified version of our solution, that applies gateway selection but does not deal with early handover detection, in the following called *GTW_selection_only*.

Let's consider a sample urban scenario, consisting of 110 roads and 67 intersections, which models a 1200m*600m wide portion of Reggio Calabria's seafront road network. As the propagation model, we use the two-ray ground reflection model provided by ns2. Vehicles are supposed to travel at piecewise constant speeds, ranging between 3 and 7 m/s, according to the mobility model proposed in [11]. We consider that 10 vehicles, randomly chosen among 40 vehicles moving in the simulation scenario, originate QoS sensitive flows directed toward external hosts, when in presence of different gateways. Specifically, we simulate three kinds of gateways (see Table I), installed at fixed locations: *Class 1* gateways act as broadband fixed Points Of Presence (POP) for high demanding customers, e.g. the so-called hot-spots; *Class 2* gateways represent POPs as well, and are able to guarantee lower bit-rates but stricter delay constraints; *Class 3* gateways offer more limited network resources. Other parameters in Table I account for the high-layer capabilities of the gateways (e.g., monetary cost of the connection, agreement with providers, and security degree). For the sake of simplicity, the achievable QoS in external networks is represented with fixed bit rates and delays. This assumption, although not totally realistic, allows us to focus on the main issue of this paper, i.e. how QoS, routing and gateway selection are performed within the access network, rather than investigating how they are accomplished outward.

Characteristics of user/applications and QoS requirements of exchanged flows are reported in Table II. The first class,

Gateway type	QoS performance	Cost	Provider	Security Level
Class 1	1.5Mb/s, 0.3s	10	Agreements with all providers	1
Class 2	384kb/s, 0.05s	5	prov1.com, prov2.com only	1
Class 3	56kb/s, 0.1s	2	Agreements with all providers	1

TABLE I
SIMULATED GATEWAYS CHARACTERISTICS

Flow	Maximum end-to-end delay	Minimum bit-rate	Required provider	Maximum cost	Security Level
voice	0.125s	8kb/s	prov1.com	3	1
video	0.5s	192kb/s	prov2.com	10	1

TABLE II
REQUIREMENTS OF THE QoS SENSITIVE FLOWS

representing a voice call, asks for low end-to-end delay and low bit-rate; it is modeled as a 8kb/s Constant Bit Rate (CBR) flow. The second class, representing a video streaming application, needs a higher bit-rate but tolerates less strict delays, and is modeled through a 192kb/s CBR flow. We further introduce a variable amount of background traffic, exchanged between couples of vehicles in the VANET, modeled as 32kb/s CBR flows, to the purpose of verifying the impact of different network loads on the considered algorithms. For each traffic class, also high-level requirements are considered in Table II; these are the preferred provider, the maximum cost the user is available to pay for the connection, and the degree of security required. Simulations, each one lasting 300 seconds, are repeated 10 times by varying the mobility patterns, the number of available gateways, and the amount of background traffic. Averaged measures are reported together with the relevant 95% confidence intervals. With reference to QoS flows, the average bitrate of packets arrived *within the committed end-to-end delay bounds* is selected as a comprehensive performance metric. It gives information on both throughput and delays. Results are reported in Fig. 3 when varying the amount of background flows, which compete with QoS sensitive traffic in the VANET. As expected, in-time delivery rates of QoS sensitive flows decrease with a growing presence of competing background traffic. However, our solution performs better, with respect to both *legacy* and *GTW_selection_only* ones, with all network loads. We can explain such results by noticing that, according to the considered flow constraints and gateways characteristics, video flows can be adequately served by gateways of *Class 1* only, while voice flows need *Class 2* gateways to accomplish their commitments. *Legacy* approach neither pays attention on QoS paths in VANET nor on the selection of the best gateways among those present, and then distributes QoS traffic evenly among all the available gateways. Thus, it can not offer the requested guarantees. Further, by comparing the proposed handover detection strategy with the *GTW_selection_only* approach, we distinguish that the handover control in the VANET provides

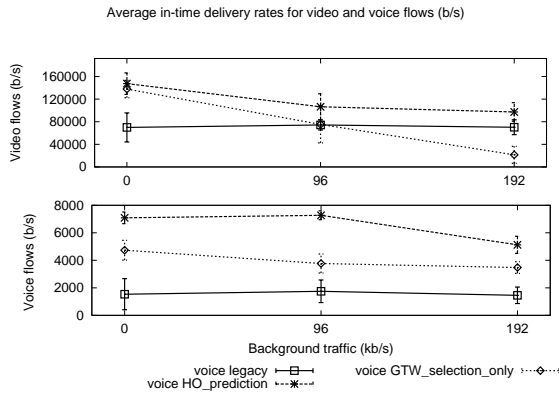


Fig. 3. In-time delivery rates for QoS flows, varying the amount of background traffic

a beneficial effect on the overall performance, even when background traffic increases. Differently, in such conditions the *GTW_selection_only* solution degrades also with respect to *legacy*, since it loses much time in the search for suitable paths after route break events.

In Fig. 4 we analyze how the presence of gateways with different characteristics impacts on the capability to serve QoS flows. While keeping the total number of gateways deployed in the simulation area fixed to 10, we vary the proportion of gateways belonging to the three classes described above (we recall that *Class 1* and *Class 2* gateways offer higher features than *Class 3* ones). On the *x-axis* we report three different configurations, characterized through the number of gateways of each class deployed in the simulation scenario. As we could expect, the performance improves when increasing the number of *Class 1* and *Class 2* gateways, i.e. the most valuable ones. However, irrespective of the presence of gateways with a different nature, the proposed approach outperforms both *legacy* and *GTW_selection_only*. Furthermore, given that our algorithm has gateway selection and QoS routing in the VANET in common to *GTW_selection_only*, the improvement in performance is evidently due to the implemented path selection strategies, that allow for early detection and repair of broken links. We have also evaluated the overhead introduced by each protocol, considering the fraction of the signaling related traffic with respect to the total traffic injected into the network. We can observe that the overhead introduced by our proposal is about 1.5 times the one of the legacy approach, while the *GTW_selection_only* approach introduces about 1.25 times the overhead of legacy, because it saves the signalling exchange related to the early handover detection.

IX. CONCLUSIONS

The reference scenario reported in this paper considers public transport vehicles and cars travelling along urban and suburban roads; user terminals on board the vehicles can benefit from the presence of either one or multiple gateways in their radio proximity. Gateways can be used to exploit different access technologies provided by ei-

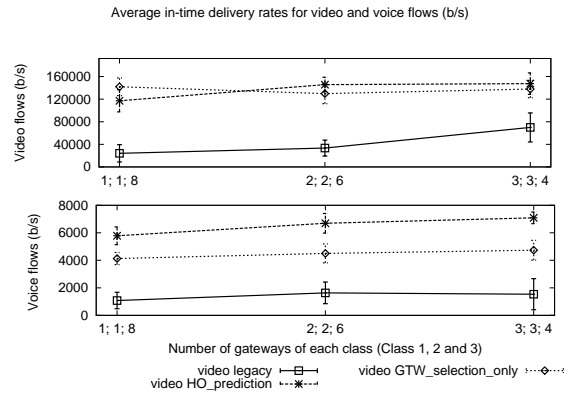


Fig. 4. In-time delivery rates for QoS flows, varying gateways' characteristics

ther the same or different service providers. We proposed a framework based on a cross-layer approach to provide Internet connectivity and end-to-end QoS to the vehicles. These tasks are performed by (i) setting up multimedia sessions from VANET nodes; (ii) reactively building QoS network paths in the VANET; (iii) selecting the best available gateway for outward transmission, according to network resource availability and compliance with user/application requirements, and (iv) constantly maintaining and updating routes to the gateways.

Simulation results in urban scenarios showed that the proposed approach can lead to better overall performance, in terms of throughput and delay, than the legacy one.

REFERENCES

- [1] K. D. Wong, K. Tepe, W. Chen, and M. Gerla Ed., "IEEE Wireless Communications, special issue on Inter-vehicular communications," *IEEE Wireless Communications*, vol. 13, no. 5, October 2006.
- [2] D. Kutscher, J. Ott, and C. Bormann, "Session description and capability negotiation," Tech. Rep., IETF, draft-ietf-mmusic-sdpng-08.txt, Work in Progress.
- [3] C. E. Perkins, J. T. Malinen, R. Wakikawa, A. Nilsson, and A. J. Tuominen, "Internet Connectivity for Mobile Ad Hoc Networks," *Wireless Communications and Mobile Computing*, no. 2, pp. 465-482, 2002.
- [4] V. Namboodiri, M. Agarwal, and L. Gao, "A Study on the Feasibility of Mobile Gateways for Vehicular Ad-hoc Networks," in *In Proc. of VANET04, October 2004, Philadelphia (USA)*.
- [5] S. Salsano and L. Veltri, "QoS Control by Means of COPS to Support SIP-Based Applications," *IEEE Network*, March/April 2002.
- [6] D. Durham et. Alii, "The COPS (Common Open Policy Service) Protocol," IETF RFC 2748, January 2000.
- [7] "Sip: Session initiation protocol," Tech. Rep. RFC 3261, IETF, 2002.
- [8] A. Iera, A. Molinaro, G. Ruggeri, and D. Tripodi, "Dynamic priority assignment in IEEE 802.11e ad-hoc networks," in *In Proc. Of Globecom 05*, November 2005.
- [9] "IEEE 802, part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: MAC Enhancements for Quality of Service (QoS)," Tech. Rep. IEEE std 802.11e, IEEE, 2005.
- [10] E. M. Belding-Royer and C. E. Perkins, "Evolution and future directions of the ad hoc on-demand distance vector routing protocol," *Ad Hoc Networks Journal*, vol. 1, no. 1, pp. 125-150, July 2003.
- [11] A. K. Saha and D. B. Johnson, "Modeling mobility for vehicular ad-hoc networks," in *In Proc. of the first ACM workshop on Vehicular ad hoc networks. Philadelphia, PA, USA, Oct. 2004*.