

A MULTI-LAYER COOPERATION FRAMEWORK FOR QOS-AWARE INTERNET ACCESS IN VANETS

Antonio Iera, Antonella Molinaro, Sergio Polito, Giuseppe Ruggeri
University Mediterranea of Reggio Calabria, Italy
{name.surname}@unirc.it

ABSTRACT

A VANET is composed of vehicles, equipped with short range wireless communication capabilities, which cooperate to form a temporary distributed network enabling communications with other vehicles or road infrastructure nodes, located in line of sight or even out of the radio range (if a multihop network is built among vehicles). It is clear that granting to vehicles continuous and high-quality connections to the Internet is a very challenging objective, due to the dynamicity of vehicular networks. In this paper, we discuss some inter-layer cooperation principles that could drive the augmentation of widely deployed protocols, at the application and network layers, to provide vehicular users with the best available Internet access.

Keywords: VANET, QoS, Internet connectivity, gateway, AODV, SIP.

1 INTRODUCTION

Vehicle-to-vehicle and vehicle-to-infrastructure communications have turned into an important research area over the last few years. The growing importance of this area has been recognized by governments, corporations, and the academic community [1]. As a result, spectrum has been allocated for inter-vehicular communications (in the 5GHz frequency band), and many research projects and partnerships in this area have been recently started.

Vehicles on the roads dynamically form continuously changing topology networks, which are referred to as Vehicular Ad-hoc Networks (VANETs). Studies in [2] have demonstrated that communications among vehicles can exploit the short-range IEEE 802.11-based radio interface technology. Currently, the IEEE working group 802.11p is specifying a new physical layer and MAC (medium access control) enhancement for inter-vehicular communications in the 5GHz frequency band [3]. In terms of MAC operations, the new standard will be based on the Enhanced Distributed Channel Access (EDCA) of IEEE 802.11e.

Numerous applications are emerging as unique to the vehicular environment. They include both safety and non-safety applications. Safety applications aim at providing drivers information about critical situations in order to prevent accidents and make driving safer. Non-safety applications (e.g., gaming, mobile commerce, multimedia streaming) aim at entertaining the users and improving driving comfort and efficiency of transportation system. These applications are typically bandwidth-demanding, have real time

delivery requirements, and ask for the network capability to offer continuous access to the Internet together with a controlled Quality of Service (QoS). The capability to satisfy these requirements will prove to be a great value-added service and will be a critical factor to the success of vehicular networks.

In spite of these strong requirements, providing QoS-aware on-board Internet connectivity is a very challenging objective, due to the intermittent nature of wireless links in the high mobile and high dynamic vehicular environment.

It is only recently that the research community has focused on the task of providing Internet connectivity to vehicles [4-8]. Their approach is to exploit the presence of *gateway* nodes in the VANET. Gateways can either be *stationary* (or *roadside*) units placed at fixed positions alongside roads, or *mobile* (or *on-board*) units traveling on some vehicles and acting as mobile gateway for other vehicles with just a short-range radio interface. Vehicle to gateway communications can exploit inexpensive IEEE 802.11 equipments; gateways to Internet (or to infrastructure) communications exploit longer range technologies, as cellular radio links or wired links.

Given that vehicles do not necessarily know the position and availability of all gateways in their neighborhood, the effectiveness of procedures for discovery and selection of the "best" gateway, which users' traffic has to be delivered through, turns to be a factor of utmost importance.

The gateway selection may depend on a multiplicity of factors, involving user and application requirements, network availability and features, agreements with service providers, location of the gateway, quality and stability of the (multihop) path to the candidate gateway in the VANET. Above

reported considerations clearly define the choice of the right gateway as a *multi-layer* issue that implies cooperation among protocol layers. In fact, service subscription and pricing usually pertain to the user/application level; setting up a QoS-demanding 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 *MAC/Physical* layer functions.

In this paper, we propose a QoS framework, which provides cooperation among augmented versions of some popular protocols: Session Description Protocol (SDP), with extensions to capability negotiation as proposed in [9] that can be used for SIP-initiated multimedia session description, Ad hoc On-Demand Distance Vector (AODV) [10] routing protocol used to set-up multihop path to the gateway in the VANET, and IEEE 802.11e [11] MAC/Physical interaction to rule channel access and choose the most reliable path to the gateway.

This paper is organized as follows. Section 2 summarizes main achievements in current literature for Internet gateway discovery in vehicular networks. Section 3 gives details of our cooperative multi-layer framework to provide passengers in vehicles with QoS-aware on-board Internet access. Main simulation results are reported and discussed in Section 4, and conclusions are summarized in Section 5.

2 RELATED WORK

Methods for enabling nodes within a mobile ad hoc network (MANET) to obtain Internet connectivity through fixed or mobile gateways have been proposed in literature [10, 12, 13]. In most of these works, gateway discovery is considered as an extension of the routing protocol, this means that the routing protocol is augmented with gateway discovery capabilities. For example, in [10], the authors augment AODV with a new control message, called RREP_I, used as a route reply from the gateway on receiving a route request (RREQ) message to a destination outside the ad hoc network. The source node uses the RREP_I message to identify the gateway and select the best one, e.g. the nearest one.

Only recently the research community has focused on the task of providing Internet connectivity while on the road [4-8]. In this case, vehicles with only short-range radios can use other vehicles (or roadside units), that have both short-range and long-range connections, as mobile (or fixed) gateways to gain on board Internet access. Vehicular settings create more demanding requirements compared to the MANET environment; the most difficult challenge in the VANET scenario is to deal with frequent route interruptions due to

dynamic mobility of vehicles on the road. The frequent route failures can result in a significant amount of time (and signaling overhead) needed for repairing routes or searching for new ones.

Successful prediction of route lifetimes can significantly reduce the number of route failures; in fact, predicted route lifetimes can be used to preemptively create new routes before existing ones fail. Approaches to predict route lifetimes have been used in the general context of MANETs [14, 15]; only very recently they have been proposed for vehicular ad hoc networks [8, 16], where they can rely on availability of location and velocity information to each node, which is assumed to be equipped with a global positioning system or other navigational instruments.

In [8] a prediction-based routing protocol is specifically tailored to the mobile gateway scenario; it takes advantage of the knowledge of vehicles position and velocity, and of predictable vehicles mobility pattern on highways, to forecast how long a route will last between a vehicle and the Internet gateway. The analysis in [8] concerns the routing protocol performance, but it does not make any assumption on the MAC layer; this means that packets are sent without any interference from another node, and without accounting for dropping due to contention at the MAC layer.

The main novelty of our proposal compared to previous approaches in literature is the attempt to create a unified framework to provide passengers in vehicles with QoS-enabled Internet connectivity. This requires (i) close cooperation among protocol layers in each “node” vehicle; (ii) augmentation of routing and MAC protocols in the VANET; (iii) enhancement of Internet gateway with QoS-aware functionality.

3 INTER-LAYER COOPERATION FOR BEST GATEWAY SELECTION

In this section, we discuss the main procedures, and the novel features of the proposed cooperative multi-layer framework.

The reference scenario is reported in Figure 1.

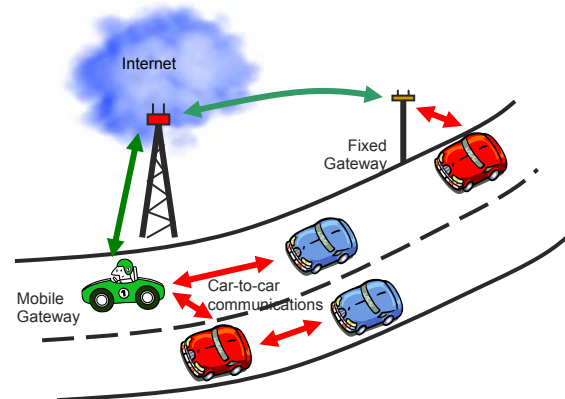


Figure 1: The reference scenario

Vehicles equipped with IEEE 802.11 radios can use other vehicles (or roadside units) that have both 802.11 and long-range connections (e.g., cellular radio links or wired links) respectively as mobile (or fixed) gateways to gain on board Internet access.

The focus is on non-safety applications with real time nature (such as audio or video streaming, or gaming), which can offer entertainment services to passengers on the road.

3.1 Basic Operation

The basic operation of proposed framework and the main roles of all involved nodes are reported in Figure 2. It will be described in details in the following subsections.

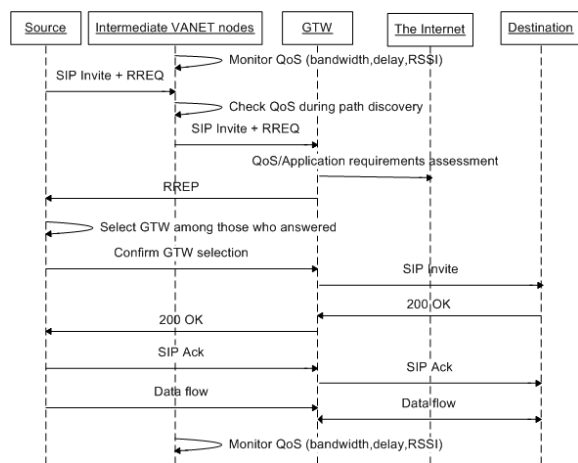


Figure 2: Basic operation of the proposed framework

In the proposed architecture the gateway has a central role. It must assess the ability of both the external network and the vehicular network to match user preferences and QoS requirements. To this aim, it must be provided with capability of interpreting both high layer parameters (such as session description parameters, user preferences, and requirements) and low-level parameters (such as achievable throughput, delay, and estimated path lifetime). Furthermore, the gateway has to be provided with communication and negotiation capability towards the external network and also the VANET nodes.

The main novelties of the proposed multi-layer cooperative approach are here listed and then explained in the following subsections:

- include high layer parameters (and not only network parameters) in the gateway selection process;
- relate gateway selection to both the VANET and the external network status and capabilities;

- use MAC and physical layers interaction to learn about QoS-enabled and reliable paths in the VANET;
- provide the gateways with enhanced capabilities to learn about or to negotiate QoS potential of connected networks.

3.2 Multimedia Session Set up and Description

Multimedia sessions can be initiated by passengers on cars using the Session Initiation Protocol (SIP) [17]. SIP is an application-layer control protocol, developed by the Internet Engineering Task Force (IETF), to establish, modify and terminate multimedia sessions or calls.

Normally, at the session initiation, a SIP INVITE message is issued by the source node (the calling party) to the intended destination (the called party) through one or more SIP servers. The INVITE request contains the details of the type of session. A 200OK response is sent back by the called party when it decides to accept the call, finally an ACK message is sent for confirmation by the source, and the media session is established.

In the reference scenario, illustrated in Figure 3, we assume that the source node is in the VANET and the destination node is outside the VANET.

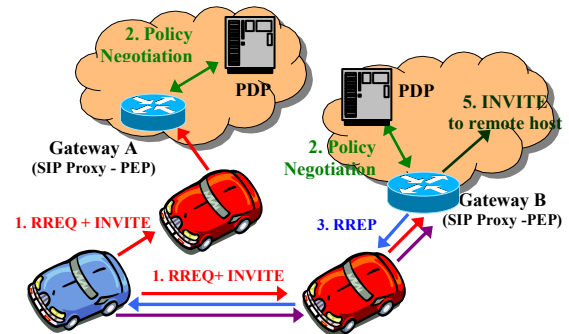


Figure 3: Session set up in the proposed framework

SIP signaling messages have to flow through the Internet gateway to the external network. The proposed approach is that the gateway can exploit session information carried by SIP signaling to carry out mechanisms to negotiate QoS in the external network. In other words, the Internet gateway is proposed to act as a SIP proxy, and to implement functionality of a Policy Enforcement Point (PEP). It intercepts the INVITE message from the source vehicle (message 1 in Figure 3) and translates session description parameters into QoS requirements; then it starts a QoS negotiation phase with the Policy Decision Point (PDP) in the external network (message 2 in Figure 3). Signalling exchange between PEP and PDP can use standard protocols, such as COPS [18] as proposed in [19]. If enough resources are available in the external network and the user has the required privileges, then the policy negotiation succeeds, the gateway informs

the source node (message 3 in Figure 3) and, after the source confirmation (message 4 in Figure 3), it forwards the INVITE packet to the intended destination (message 5 in Figure 3); otherwise the session ends.

To augment SIP semantical expressiveness in describing a session (SIP session description only consists of codec parameters and requested bit-rates), we propose to use the extension of SDP (Session Description Protocol) to handle Capability Negotiation [9]. This working draft allows to enrich media/session description and negotiation capabilities for SIP-initiated multimedia sessions, and yet to maintain them simple enough to allow easy implementation and almost completely backward compatibility with the current SDP standard (RFC 2327).

Besides classic session description parameter (such as IP-address and port, type of media stream, transport protocol), SDP Capability Negotiation allows for new capability attributes to be defined for a session, through suitable *extension capability attributes*. We propose to use these attributes to include high-layer user/application preferences to be interpreted by the gateway before checking QoS capability of the external network. As a simple example of additional session attributes we can consider: (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, and so on.

3.3 The Central Role of Gateway

The protocol's basic operation of creating routes to the gateway in the VANET is similar to that of a reactive protocol, like AODV in [10]. When a vehicle needs to communicate to a location on the Internet, it checks its routing table for a route. If none exists, it broadcasts a route request (RREQ) packet.

When the RREQ packet reaches a gateway with the desired route to the destination, the gateway has to process the request, and check QoS capability of both external and vehicular networks before generating the route reply (RREP) packet and send it back to the source node (message 3 in Figure 3).

Gateways can perform this task because we suggest that route discovery packets embed all the information needed to check end-to-end QoS capability.

The first main difference compared to previous routing approaches is that we propose the SIP INVITE message with SDP Capability Negotiation description to be embedded into the RREQ packets (message 1 in Figure 3) at session set up.

The second difference is that RREQ packets also

carry information on the capability of the VANET to provide a QoS path from the source to the gateway. These low-layer parameters are collected while packets cross the VANET through cooperation of network, MAC, and physical layers (which is explained later in this paper), and give information on achievable throughput, delay, and expected route lifetime.

Therefore, the RREQ packet contains a sequence number, source identification (ID), destination ID, some *route parameters*, and *SDP capability negotiation parameters* embedded in the payload. The gateway is enabled with capability to interpret all embedded information.

The gateway, as a SIP proxy, interprets SDP data, and is aware of end-to-end QoS session requirements and user preferences. It also knows of the QoS capability of the VANET through route parameters, thereby it checks whether the external network can provide residual QoS, i.e., it can provide the minimum throughput and the maximum delay allowed in the external path to the destination.

Therefore, the gateway starts a negotiation phase with the external network to assess both *QoS constraints* towards destination and *application/user preferences*. Only a gateway that successfully passes through the negotiation phase can inform the source node by sending back a RREP packet (message 3 in Figure 3).

If multiple gateways reply, the source node chooses the gateway that is nearest in terms of hops. If the source gets multiple routes for the same gateway, it uses the route that has the maximum predicted route lifetime, as will be described later in the paper.

To manage this, differently from legacy AODV [20], we introduce a control message, called *Route Confirmation Message* (CONFIRM), that is issued by the source towards the selected gateway (message 4 in Figure 3). Upon receiving a CONFIRM message, the gateway forwards the SIP INVITE to the external destination (message 5 in Figure 3). Candidate gateways, which do not receive a CONFIRM message before the expiration of a given timer, reset the current session initiation procedure.

3.4 Routing and MAC Protocols Cooperation

In our reference framework, to improve QoS capability in the VANET, routing choices at the network layer are undertaken through cooperation with the MAC layer. To carry out inter-layer cooperation we propose:

- the MAC protocol to provide estimation of expected delay (and throughput) achievable on the selected route;
- the routing protocol to select the route based on information from the MAC layer.

Access control at the MAC layer is ruled by the

EDCA contention function of IEEE 802.11e standard [11]. This choice is in agreement with studies carried out within the IEEE task group 11p that is standardizing a MAC protocol for VANET [3]. With EDCA, traffic flows have one of four access categories assigned that have different channel transmission priority; voice gets the highest priority, followed by video, and finally background and best effort traffic.

Each wireless node in the VANET manages four queues, one for each 802.11e access category i ($i=0...3$). In each node, when a packet is ready for transmission and enters the Logical Link Control (LLC) layer, it is first buffered in one of the queues, waiting for being processed by the MAC layer and then transmitted on the air interface.

In our framework, every node monitors two parameters for each queue i , namely $D_{LLC,i}$ and $D_{MAC,i}$. The first one represents the time spent by a packet in a node, from the instant it enters the queue to the instant it is transmitted over the radio channel. $D_{MAC,i}$ is the fraction of the $D_{LLC,i}$ period that accounts for the delay due to the MAC protocol rules; it starts from the instant the packet reaches the head of the line and ends when it is transmitted on air. The $D_{MAC,i}$ delay contribution depends on many factors, such as physical transmission rate, random back-off interval, retransmissions attempts, and EDCA priority i . Furthermore, $D_{MAC,i}$ is related to the maximum throughput ($MaxTh_i$) achievable by a station transmitting at priority i through the equation $MaxTh_i = \frac{PktSize}{D_{MAC,i}}$, where $PktSize$ is the packet

length. For the sake of simplicity we assume a fixed packet size in this paper.

Therefore, whenever a frame is scheduled for transmission from the i -th queue, the time intervals $D_{MAC,i}$ and $D_{LLC,i}$ are evaluated. The samples contribute to update the average values $\overline{E\{D_{MAC,i}\}}$ and $\overline{E\{D_{LLC,i}\}}$ through an exponential weighted moving average with a smoothing factor α set to 0.4 after a wide tuning campaign. More details about MAC parameters estimation can be found in [21].

The computed average values $\overline{E\{D_{Mac,i}\}}$ and $\overline{E\{D_{LLC,i}\}}$ will be used by the routing protocol to update route parameters and to choose the best route to the gateway, as detailed in the next subsection.

3.5 QoS-Aware Routing Toward the Gateway

To carry out QoS-aware route set up and maintenance in the VANET, we propose adding some low-layers *route parameters* in the RREQ packets. Two of them, namely $MinTh$ and

$Maxe2eDelay$, respectively carry the minimum throughput and the maximum delay that can be offered by the route. These values are hop-by-hop updated by nodes processing the RREQ packet.

To include QoS parameters in the AODV routing protocol has been first suggested in [20], in this paper we propose a practical way to estimate the delay and the available throughput along the path.

When the source node issues a RREQ packet, it initializes $MinTh$ and $Maxe2eDelay$ to the desired values specified by the user at session set up. Then, it also adds its traffic priority i and the packet length $PktSize$.

Each node along the path reads and/or updates these fields through cooperation with the MAC layer: the $Maxe2eDelay$ field is subtracted by the estimated $D_{LLC,i}$ value to account for time already spent in the path, and the achievable throughput is computed as $\frac{PktSize}{D_{MAC,i}}$ and compared with the value

stored in $MinTh$. Before forwarding the RREQ packet, each node checks whether the residual time is lower than the maximum delay tolerated and the achievable throughput on the current hop is higher than the minimum value specified by the user, according to equation (1):

$$\begin{cases} MinTh \geq \frac{PktSize}{D_{MAC,i}} \\ Maxe2eDelay \geq 0 \end{cases} \quad (1)$$

Only if both the conditions are true, then the RREQ message is forwarded, otherwise it will be discarded.

When the gateway finally receives RREQ packets, it can have information on the QoS capability of the VANET. Specifically, the $MinTh$ and $Maxe2eDelay$ fields contain, respectively, the minimum bit rate requirement and the residual delay allowed to be spent in the remaining path to the destination. Upon receiving this information, the gateway is able to start QoS negotiation with the external network, and reply back to the source, as described in section 3.3.

3.6 Route to the Gateway Maintenance

The proposed routing protocol also differs from reactive protocols like AODV in the way that it proactively creates new routes before they break.

Once the route is set up and the session is established, the routing layer of each VANET node continuously cooperate with DLC and Physical (PHY) layers to get information about the QoS performance of the route and about its reliability. Monitored parameters at the PHY layer of each node, in conjunction with the prediction algorithm (which

is explained later in next subsection), are used to give the node a predicted lifetime for the route.

If either QoS performance can no longer be met over the path or the predicted route lifetime is going to expire, then every node tries to preempt route failure and proactively seeks possibly better routes.

By referring to Figure 4, after a route to the gateway is set up in the VANET, every node continuously monitors the RSSI (Received Signal Strength Indication) from its neighbors and computes the predicted route lifetime. When a node realizes that a link is rapidly deteriorating, then it labels the route as *expiring* and the link as *critical* in its routing table. The label *expiring* means that a route is going to be updated, while the label *critical* means that the link to the adjacent node is rapidly going to break.

Then the node issues a *Route-Alert* packet upstream to the sender (message 3 in Figure 4) to trigger a *Route Update* procedure. 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 node, upon receiving the *Route-Alert* packet, issues a SIP RE-INVITE message (with the same information of the original INVITE plus SDP description) and sends it embedded in a *Route Update* packet (message 4 in Figure 4).

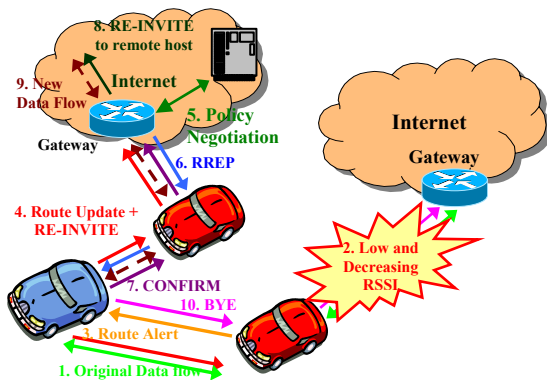


Figure 4: Route maintenance signaling flows

Intermediate nodes process *Route Update* packets like they do with RREQ packets, with the exception that they are not allowed to use cached routes to the destination. Therefore, intermediate nodes do not reply back to the source even if they have a route to the gateway, but they rather perform next-hop discovery if necessary. When searching for the new route, each node will discard routes that include links labeled as *critical*.

All the gateways contacted, and able to handle the user traffic (message 5 in Figure 4), respond with a RREP packet (message 6 in Figure 4), and procedure goes on like described in section 3.3. When a gateway receives a CONFIRM packet from the source (message 7 in Figure 4), there are two

possibilities: (a) it is the same gateway which was already forwarding the user traffic (the route in the VANET has been repaired and the gateway is unchanged), or (b) it is a new gateway. In case (a), it continues to do its job as before; in case (b), it forwards the RE-INVITE message to the remote destination (message 8 in Figure 4). If procedure concludes successfully, the data traffic can flow between sender and receiver through the new gateway. As soon as the source receives data from the new gateway, it sends a BYE message to the old gateway (message 10 in Figure 4) to erase all routing entries labeled as *expiring*.

3.7 Estimating the Route Lifetime

A critical component of the proposed scheme is determining when path reliability is no longer acceptable (which generates a *Route-Alert* message). The path reliability can incorporate several criteria, such as signal strength, the age of a path, the number of hops, and rate of collisions [15]. In this paper, we restrict the path reliability to be a function of the signal strength (RSSI) of received packets. Since most route breaks can be ascribed to link failures due to node motion in the vehicular scenario, the signal strength offers the most direct estimate of the ability of the nodes to reach each other.

When using RSSI as a path reliability indicator, it is important that signal power fluctuations, due to channel fading and multipath effects, do not generate erroneous warnings causing unnecessary floods of route update requests. Some established mechanisms are used in the cellular telephony field to solve this problem [15]. For example, maintaining an exponential average of the signal power (rather than triggering the mechanism based on a single packet) can be used to verify that the signal power drop was not due to fading or similar temporary disturbances.

This is the approach we follow. All nodes in the VANET continuously measure the RSSI on each active link to their neighbors, and compute the RSSI variation according to equation (2):

$$\Delta RSSI(t_{actual}) = \frac{RSSI(t_{actual}) - RSSI(t_{former})}{t_{actual} - t_{former}} \quad (2)$$

where t_{actual} and t_{former} are the two time instants of current and previous RSSI measures, respectively. To filter out RSSI fluctuations in eq. (2), we consider an average $\overline{\Delta RSSI(t_{actual})}$ measure, which is obtained from $\Delta RSSI(t_{actual})$ through an exponential weighted moving average with smoothing factor α_{RSSI} . If $\overline{\Delta RSSI(t_{actual})}$ is greater than, or equal to, zero, the route is assumed to be reliable, otherwise, the RSSI is expected to have a decreasing trend.

RSSI trend monitoring is used by each node to

predict the route lifetime, according to the prediction algorithm here described. The algorithm exploits another additional field in the RREQ packet, namely *ExpLifetime* that is used to carry information concerning the expected route lifetime.

Initially, the source node sets the *ExpLifetime* field in the RREQ packet header equal to infinite. As the packet traverses the VANET to the gateway, each intermediate node does the following. Based on RSSI measurements from its adjacent nodes, it predicts the lifetime of the link between the two nodes using the prediction algorithm. If this value is smaller than the current lifetime mentioned in the RREQ packet, then the *ExpLifetime* field is changed to this value. Therefore, $ExpLifetime = \min(ExpLifetime, plt)$, where *plt* is the predicted path lifetime. Else, the current value in the packet is left unchanged and forwarded toward the gateway. In this way, when the gateway gets a RREQ packet, the value of the *ExpLifetime* field that is indicated in the packet is the route's predicted lifetime.

The prediction algorithm performs *plt* computation based on both RSSI measurements and the receiver sensitivity *S* (the RSSI value, below which the receiver is not able to work properly), as shown in equation (3):

$$\begin{aligned} [RSSI(t_{actual}) - S] + \overline{\Delta RSSI(t_{actual})} \cdot plt \geq 0 \rightarrow \\ plt \leq \frac{S - RSSI(t_{actual})}{\Delta RSSI(t_{actual})} \end{aligned} \quad (3)$$

The preemptive warning that triggers the *Route update* procedure is generated when the estimated lifetime of a monitored path drops below a threshold. The value of this threshold is critical to the efficiency of the algorithm. If the value is too low, there will not be sufficient time to discover an alternative path before the path breaks. However, if the value is too high, the warning is generated too early with the negative side-effect of unnecessary route updates: if the suspect path never breaks (e.g., the vehicles may change direction) and so the full life of the path currently in use is not exploited. After thorough simulations, the threshold has been set to 1.5 sec.

4 COMPARING LEGACY AND PROPOSED APPROACH

In this section we present a simulation campaign, carried out through ns2 (Network Simulator v2) [22] to assess the performance of the proposed multi-layer cooperative approach. We compare our solution, in the following referred to as *multilayer* approach, with the so-called *legacy* approach, which uses standard AODV routing protocol as in [10], and simply chooses the nearest gateway without any consideration on its capability to satisfy user requirements. The ns2 code used to implement the

legacy algorithm is available on the web [23].

As a sample urban scenario, we considered a 1200m*600m map of the Reggio Calabria's seafront area, illustrated in Figure 5. Vehicles are supposed to travel at piecewise constant speeds, ranging between 5m/s and 12.5 m/s (18 km/h and 45 km/h); changes of velocity and direction can occur at each crossroad in the map, according to the mobility model proposed in [24]. The two-ray ground reflection model provided by ns2 has been used to simulate signal propagation in the channel.

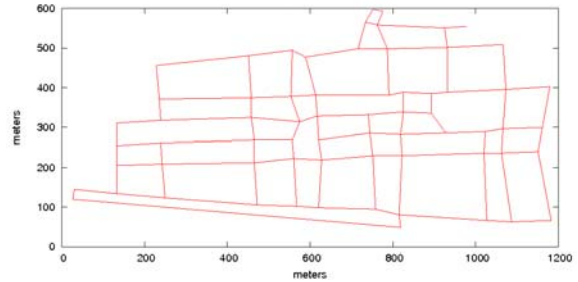


Figure 5: The reference map for urban scenario

Gateways or fixed relays have been placed at each intersection of a grid of 10 columns and 5 rows covering the reference urban area. Ten of the fifty fixed nodes are gateways and are connected to the wired Internet through links of different capacity, while the remaining nodes are only able to forward user traffic to the chosen gateway. The position of the gateways in the grid is randomly chosen and changes at each simulation run.

Three kinds of gateways have been simulated whose main characteristics are reported in Table 1: *Class 1* gateways act as broadband fixed points of presence for high demanding customers; *Class 2* gateways are able to guarantee lower bit-rates but stricter delay constraints; *Class 3* gateways offer more limited network resources. 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. The other parameters in Table 1 account for the high-layer capabilities of the gateways (e.g., monetary cost of the connection, agreement with providers, and security degree). Two of the ten gateways belong to Class 1, two are Class 2 gateways, while the remaining six are Class 3 gateways.

Ten vehicles among those moving in the simulation scenario, originate QoS-sensitive flows (voice and video) directed toward external hosts. QoS requirements of exchanged flows and user preferences are reported in Table 2. Voice traffic is modeled as a 8 Kbps Constant Bit Rate (CBR) flow; video streaming is modeled as a 192 Kbps CBR flow.

The high-level requirements for each traffic class include the preferred provider, the maximum cost the user is available to pay for the connection, and the degree of security required.

Gateway type	External network QoS	Cost	Agreements with providers	Sec. level
Class 1	1.5 Mbps 0.3 s	10	All	1
Class 2	128 Kbps 0.05 s	3	Only providers A and B	1
Class 3	56 Kbps 0.1 s	2	All	1

Table 1. Simulated gateways characteristics

Flow	Max e2e delay	Min. bit-rate	Preferred Provider	Max Cost	Sec. level
Voice	0.125s	8Kbps	Prov. A	5	1
Video	0.5s	192 Kbps	Prov. B	10	1

Table 2. Requirements of the QoS-sensitive flows

All other vehicles in the simulated scenario generate background interfering traffic (with low-priority), which is likewise directed to the Internet. The interfering traffic load varies from 0 to 3 Mbps.

Tables 1 and 2 show that the use of some gateways is prohibited to some traffic flows; for example, video flows can be served only through Class 1 gateways that are the only capable of providing the requested QoS (both Class 2 and Class 3 gateways do not match the bit rate requirement). Analogously, voice calls can pass through Class 2 or 3 gateways.

Traffic flows access the radio channel in the VANET according to the rules of IEEE 802.11e MAC protocol [11]. Voice traffic achieves the highest priority, followed by video and finally by background traffic generated by the interfering vehicles.

Simulations, each one lasting 200 seconds, are repeated 10 times by varying the mobility patterns, the position of available gateways, and the amount of background interfering traffic. Averaged measures are reported together with the relevant 95% confidence intervals.

Figure 6 and 7 show the percentage of voice and video packets that have been delivered “in time” to the destination in the Internet. “In time” means within the committed end-to-end delay. This metric allows us to appreciate the degradation due to both lost packets and late delivered packets. Curves are reported when varying both the average speed of the vehicles and the interfering load. A general deterioration of performance (even if not dramatic) is visible when the vehicles speed increases, given to the higher difficulty of maintaining a route to the

gateway. From the results shown, the proposed multilayer framework outperforms the legacy one in any simulated case for video flows. This is generally true also for voice flows even if, in this case, the gain is sometimes lower than in the video case. In fact, the legacy approach has more chances that the selected gateway to forward voice traffic (i.e., any closest gateway) is also able to satisfy user and QoS requirements (eight of the ten gateways are good ones for voice); while this is not true for video flows whose requirements can be matched only by Class 2 gateways (two of the ten gateways are good ones).

Furthermore, Figures 6 and 7 show that the performance of the multilayer approach when there is no interfering traffic is dramatically higher than the legacy approach in the same traffic condition. This is because of the smart selection operated by the multilayer approach that is able to reach the right gateway through a good and reliable path in the VANET. When the interfering traffic increases, obviously the performance decreases also due to the fact that to find and maintain a good and reliable path to the best gateway is more difficult.

As shown in Figure 8, the multilayer approach chooses longer paths in the VANET compared to the legacy one. This is because the legacy approach can often find a (*any*) gateway at one hop distance, while the multilayer approach searches for the *best* gateway (that is rarely the nearest one).

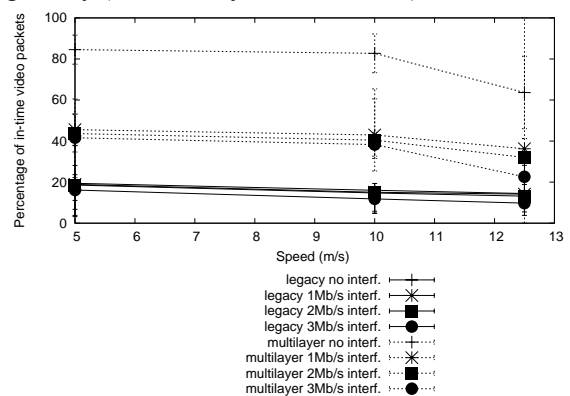


Figure 6. Percentage of video packets in-time delivered to destination

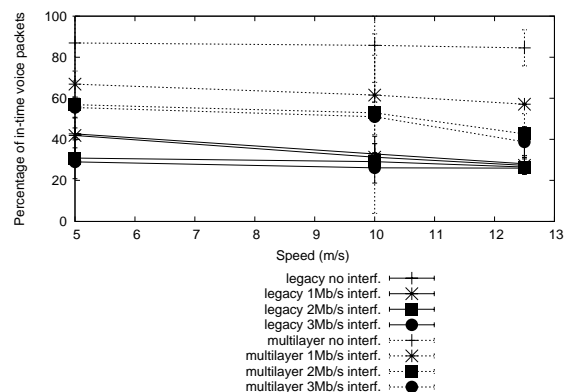


Figure 7. Percentage of voice packets in-time delivered to destination

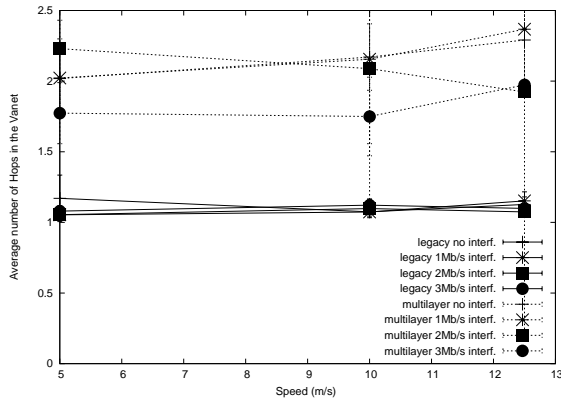


Figure 8. Average number of hops in the VANET

A further evidence of this fact is observable in Figures 9 and 10 that show the percentage of packets which is delivered to a gateway in the VANET. The legacy approach delivers almost all packets to a (any) gateway in the VANET. Unfortunately, a very small percentage of these packets will be delivered to the intended destination within the target end-to-end delay.

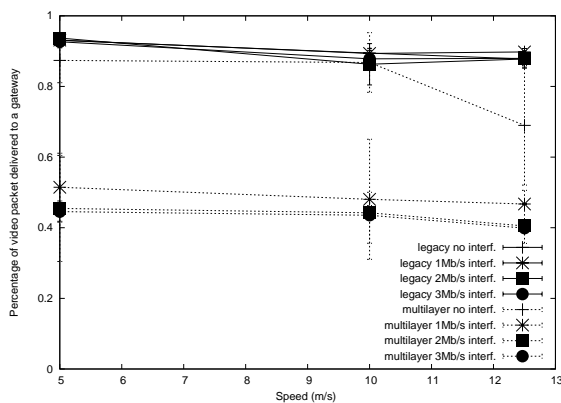


Figure 9. Percentage of video packets delivered to a gateway in the VANET

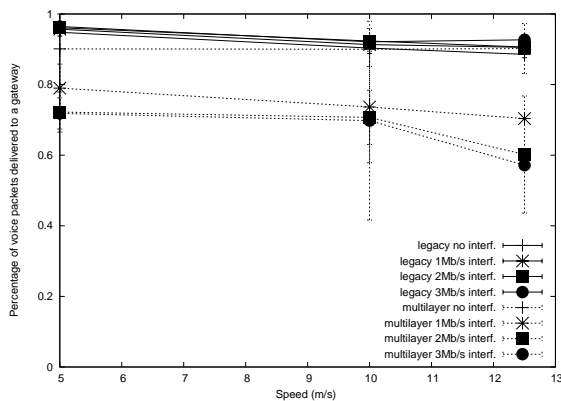


Figure 10. Percentage of voice packets delivered to a gateway in the VANET

Finally let us consider the protocol overhead reported in Figure 11 that shows the fraction of signaling packets over the total number of generated

packets in the VANET. Signaling packets included in the overhead computation are all the packets needed at the network layer to set up and maintain the route to the gateway (RREQ, RREP, RERR, and Route Alert messages).

Both approaches show a general decrease of the overhead when the interfering traffic load increases and a general increase of the overhead when the vehicles speed increases. The former effect is due to the fact that, when the interfering traffic is higher the number of totally generated packets in the VANET increases more rapidly than the number of signaling packets, thus the fraction of overhead is computed over a higher number of totally generated packets. The latter effect is due to a higher route breakage probability when the speed of mobile nodes increases. This effect is however less evident when the interfering traffic increases, because at the increasing of the interfering traffic also increases the number of route breakages due to network congestion rather than to the mobility of the nodes.

The comparison of multilayer and legacy approaches shows that the multilayer approach introduces lower overhead than the legacy approach when no interfering traffic is considered, then when the interfering traffic increases the overhead slightly increases, but it keeps on values that are comparable to the legacy one. The better behavior of multilayer approach compared to the legacy one in the case of zero interferers is because of its choice of more reliable (i.e., with a longer lifetime) paths to the gateway.

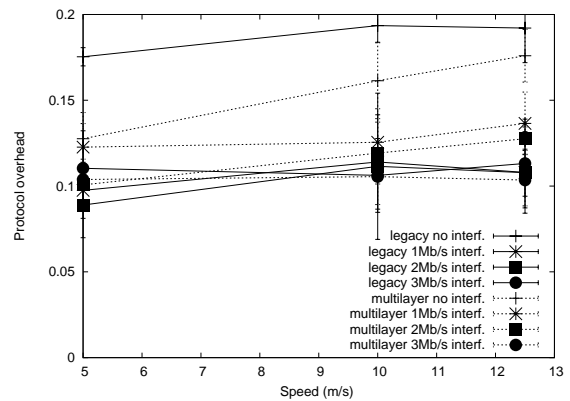


Figure 11: Protocol overhead

5 CONCLUSIONS

The reference scenario analyzed in this paper considers moving vehicles that gain Internet connectivity while on the road, through fixed or mobile gateways in their radio proximity. The proposed framework, which is based on inter-layer cooperation, provides mobile passengers with QoS-enabled on board connectivity for entertainment purposes.

These tasks are performed through (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.

Simulations in urban scenarios showed that the proposed approach achieves improved performance, mainly in terms of effectiveness of procedures of path-to-the-gateway discovery and maintenance, and end-to-end QoS provisioning.

REFERENCES

- [1] K. D. Wong, K. Tepe, W. Chen, M. Gerla: Inter-vehicular communications, *IEEE Wireless Communications*, Vol. 13, No. 5, (2006)
- [2] M. Wellens, B. Westphal, P. Mahonen: Performance evaluation of IEEE 802.11-based WLANs in vehicular scenarios, *Proceedings of IEEE Vehicular Technology Conference, VTC Spring*, (2007)
- [3] Status of Project IEEE 802.11p, http://grouper.ieee.org/groups/802/11/Reports/tg_p_update.htm [Cited on: Sept. 2007], (2007)
- [4] M. Bechler, O. Storz, W. Franz, L. Wolf: Efficient discovery of internet gateways in vehicular communication systems, *Proceedings of IEEE Vehicular Technology Conference, VTC Spring*, (2003)
- [5] J. Ott, T. Kutscher: Drive-thru Internet: IEEE 802.11b for 'Automobile' users, *Proc. IEEE INFOCOM*, (2004)
- [6] A. Iera, A. Molinaro, S. Polito, G. Ruggeri: End-to-end QoS provisioning in 4G with mobile hotspots, *IEEE Network Magazine*, Vol. 19, No. 5, pp. 26-34, (2005)
- [7] V. Bychkovsky, B. Hull, A. K. Miu, H. Balakrishnan, S. Madden: A measurement study of vehicular internet access using in situ Wi-Fi networks, *Proc. ACM MOBICOM* (2006)
- [8] V. Namboodiri, L. Gao: Prediction-based routing for vehicular ad hoc networks, *IEEE Transactions on Vehicular Technology*, Vol. 56, No. 4, pp. 2332-2345, (2007)
- [9] F. Andreassen: SDP capability negotiation, IETF MMUSIC Working Group, Internet draft draft-ietf-mmusic-sdp-capability-negotiation-06.txt, (2007)
- [10] C. E. Perkins, J. T. Malinen, R. Wakikawa, A. Nilsson, A. J. Tuominen: Internet connectivity for mobile ad hoc networks, *Wireless Communications and Mobile Computing*, no. 2, pp. 465-482 (2002)
- [11] IEEE 802, part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: MAC enhancements for quality of service (QoS), *IEEE std 802.11e*, (2005)
- [12] H. Ammari, H. El-Rewini: Integration of mobile ad hoc networks and the Internet using mobile gateways, *Proceedings of International Parallel and Distributed Processing Symposium* (2004)
- [13] M. K. Denko, C. Wei: An architecture for integrating mobile ad hoc networks with the Internet using multiple mobile gateways, *Canadian Conference on Electrical and Computer Engineering*, (2005)
- [14] W. Su, S. Lee, M. Gerla: Mobility prediction and routing in ad hoc wireless networks, *International Journal of Network Management*, Vol. 11, No. 1, pp. 3-30, (2001)
- [15] T. Goff, N. B. Abu-Ghazaleh, D. S. Pathak, R. Kahvecioglu: Preemptive routing in ad hoc networks, *Journal of Parallel and Distributed Computing*, Vol. 63, No. 2, pp. 123-140 (2003)
- [16] M. Mabilia, A. Busson, V. Veque: Inside VANET: hybrid network dimensioning and routing protocol comparison, *Proceedings of IEEE Vehicular Technology Conference, VTC Spring*, (2007)
- [17] J. Rosenberg et al.: SIP: Session Initiation Protocol, *IETF RFC 3261* (2002)
- [18] D. Durham et al.: The COPS (Common Open Policy Service) protocol, *IETF FRC 2748* (2000)
- [19] S. Salsano, L. Veltri: QoS control by means of COPS to support SIP-based applications, *IEEE Network*, Vol. 16, No. 2, pp.27-33 (2002)
- [20] E. M. Belding-Royer, 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, (2003)
- [21] A. Iera, A. Molinaro, G. Ruggeri, D. Tripodi: Dynamic priority assignment in IEEE 802.11e ad-hoc networks, *Proceedings of IEEE Global Telecomm. Conference (GLOBECOM)*, (2005)
- [22] <http://www.isi.edu/nsnam/ns>
- [23] <http://www.telecom.lth.se/Personal/alexh/>
- [24] A. K. Saha, D. B. Johnson: Modeling mobility for vehicular ad-hoc networks, *Proceedings of ACM Workshop on Vehicular Ad hoc networks*, (2004)