A cooperative infrastructure discovery protocol for vehicle to Internet opportunistic communications

Naourez Mejri*, Fethi Filali†, Farouk Kamoun*‡

*CRISTAL Lab., ENSI, Campus Univ. Manouba, Tunisia.
Email: mejri.naourez@cristal.rnu.tn, Telephone: (216) 71 600 444.
† Mobile Communications Department, EURECOM, Sophia-Antipolis, France.
‡ESPRIT, School of engineering, El Ghazala Technopole, Ariana, Tunisia.

***Abstract*—Nowadays, wireless 802.11 access points (APs) are increasingly widespread in urban and sub-urban areas. Besides part of them offer free access, hence such infrastructure can provide intermittent Internet access to vehicles for opportunistic applications like software or digital maps updates, vehicle diagnostic reporting, and certificates/pseudonyms renewing.**
In this paper, we propose a Cooperative Infrastructure Discovery Protocol, called CIDP, which aims at collecting information about discovered APs and stores it in each vehicle's Wireless Infrastructure Database. This database is filled with data gathered through direct communications with the infrastructure (I2V/V2I (Infrastructure to Vehicle/Vehicle to Infrasctructure) communications) or gratuitously obtained from other vehicles. CIDP introduces specific messages for opportunistically exchanging the wireless infrastructure information between vehicles in both solicited and unsolicited manners.
Extensive simulation study of CIDP shows that it improves the discovery process of APs thanks to the dissemination of the infrastructure information cooperatively between equipped vehicles through V2V (Vehicle to Vehicle) communications. However, it is shown that the judicious configuration of its parameters such as the broadcast periodicity helps to keep its overhead low for various configurations with different vehicles' density, speed, and movement pattern.
We consider CIDP as a promising avenue of development for Vehicle-to-Internet communications, and so an additional motivation for this work is to lay a sound basis for further development of opportunistic V2X (Vehicle to Infrasctructure/Vehicle) communications.

***Keywords*-Infrastructure discovery; opportunistic communications; V2V2I communications**

I. Introduction

During the last few years, wireless technologies had spread widely. Among these technologies, deployed 802.11 infrastructure can be found at homes, coffee shops or larger areas such as campuses, industrial zones, shopping malls and airports. These access points (APs) are mainly deployed in a spontaneous manner by individuals or independent organizations. Besides, some of them offer free anonymous access with no security protection. Moreover, market estimates show that Wi-Fi equipments sales are and will considerably increase in years to come [6]. Thus, such pre-existing infrastructure can be very handy for public use since it provides ubiquitous wireless connectivity and hence allows Internet access on the fly.
In this work, we aim at taking advantage of unplanned 802.11-based wireless infrastructure to sustain Internet access to in-vehicles communication devices. Indeed, there is a wide range of applications for which the paradigm of opportunistic Vehicle to Internet communications works well such as driver assistance, some e-safety applications [9], vehicular sensor networks (VSNs) [2], software or digital maps updates, vehicle diagnostic reporting, and asynchronous mail transfer.
However, using pre-existing WIFI unplanned infrastructure comes with at least two main challenges. First, vehicles' speed impacts the connectivity time with the 802.11 APs. Second, when discovering more than one AP at the same time, a considerable fraction of their visibility time is spent in access point selection and association establishment phases. Consequently, the effective time used for data transmission will be severely reduced. Intuitively, we expect that knowing the wireless infrastructure in advance has lot of merits for the design of "intelligent" opportunistic communication architecture for Vehicle to Internet (or Internet to Vehicle) communications.
In this paper, we propose a cooperative wireless infrastructure discovery protocol which allows vehicles to spread the information collected from encountered APs to neighboring vehicles. Consequently, each vehicle will have an up-to-date knowledge about the deployed infrastructure even in not yet visited regions. Hence, when a vehicle has data to transmit to the Internet, it will first check on its own Wireless Infrastructure Database (WID) to determine the best relay (an AP or a neighbor vehicle)[1] for its data "on the fly" (without scanning the envrionment). It is worth mentioning that CIDP protocol can be used for the discovery of communication units integrating V2X communication technologies under development in several standardization bodies, initiatives, and projects. In particular, it will be possible to deploy CIDP as a complementary module in the architecture proposed by IEEE (WAVE - Wireless Access in Vehicular Environment) to discover Road-Side Units (RSU) or in those suggested by ETSI ITS technical committee and ISO CALM working group to discover deployed ITS roadside stations. In the context of the ETSI ITS communication architecture, CIDP can be one of the modules of the facilities layer and contribute on the

[1]A relay selection procedure based on CIDP is one of our on-going works.

building of the Local Dynamic Map (LDM) by adding the APs information in the digital map. In the context of the under-development V2X communication architectures, CIDP would use one of the available Service Channels (SCH) and not the Control Channel (CCH) reserved for critical safety V2X applications.

The remainder of this paper is organized as follows. Section II gives an overview of existing research works in the context of vehicle-to-Internet communications and shows how CIDP is different and/or complementary to these efforts. We give the details of CIDP protocol in Section III where the different transmission modes and suggested messages formats are described. Section IV presents the simulation scenarios and discusses the obtained results. Finally, Section V concludes this paper and outlines future works.

II. Related work

Previous research works already dealt with 802.11 access point mapping. In fact, there are several websites that provide maps of WiFi access points. Some popular examples are WiFiMaps [18], JIwire.com [14] and FON Maps [12]. These websites give the location and characteristics of the encountered APs. However, they are limited to specific regions (WiFiMaps for zones in the US) or for specific hardware (FON Maps only locates FON APs). Besides, in such solutions, data is constructed through war-driving results uploaded by independent users which impacts the accuracy of the collected data and also the frequency of update. Hence, the showed maps can become outdated quickly by the time the driver consults them.

The same problem of accurate data and update frequency arises in the case of research studies such in Intel Place Lab projects [13] where a database of up to 30000 802.11b APs in different US cities is stored and maintained.

Other works also considered the issue of selecting the best access point among a set of available ones. Some of these techniques are based on passive scan for beacon signals the AP willingly broadcasts. It then chooses the non encrypted one with the strongest signal strength. However, conducted studies in [3] showed that the signal strength is an insufficient predictor of AP quality. In fact, the selected AP can belong to a payed service with required subscription. Besides, "open" access APs may also be using a controlled access list by MAC address filtering. Moreover, it can refuse granting a valid IP address through DHCP to allow Internet access thus blocking traffic from not allowed terminals.

In Virgil [4], the authors consider these factors. They launch a set of tests to determine the APs characteristics and even collect information that can be later used for QoS requirements. However, the authors consider that the subject trying to connect to the candidate APs has limited or no mobility meanwhile these tests which is not an accurate assumption in the case of vehicular networks.

To analyse APs scanning and cope with vehicles' mobilities, other works such as [8] and [7] investigated through real experimentations to which level such hazardous encounters between vehicles and APs can offer reliable services to potentiels clients. In Cabernet [7], the authors enhanced Wifi and TCP to use encountered open 802.11 APs for a one-hop delivering data. Authors in [8] also suggested that using APs caching can improve spent time to associate with an existent AP. The results and improvements proposed in these works can be used in conjunction with our proposal CIDP in order to increase the connectivity between vehicles and existent infrastructure.

Our focus in this paper is the development of a cooperative protocol which allows the exchange of infrastructure information between vehicles. This exchange allows vehicles to know if the AP offers free anonymous access (i.e whether the vehicle could obtain an IPv4 address from the access point DHCP server and then get an intermittent Internet connection) so that it can be considered as a data relay candidate. This task is achieved in a distributed manner between vehicles entering and leaving the network. It is also done in a transparent way to the driver and to his driving habits in opposite with required wardriving for previously mentionned works. Moreover, CIDP enables frequent data updates in order to keep accurate fresh information in the AP wireless infrastructure databases (WIDs) since they will be updated each time new APs are detected or when new information are received from other vehicles.

III. Cooperative Infrastructure Discovery Protocol (CIDP)

A. Assumptions and short overview of CIDP

The proposed infrastructure discovery protocol requires vehicles to be equipped with GPS receivers to determine their location at any time. Such assumption is a realistic one since many of the new cars are already equipped with built-in GPS. Furthermore, with their considerably decreasing cost, we presume that in the near future most of the vehicles will be equipped with external or built-in GPS devices. Additionally, we assume that each vehicle has an embedded router with at least one WLAN card which will be used to connect to the Internet. Finally, we consider that there are no storage constraints as the cost of storage disks is decreasing over months.

Passive AP scanning provides each vehicle with a restricted sight limited to the crossed streets. It can not then forecast the presence of APs in its path toward the desired destination.[2] Thanks to CIDP, the vehicles would have a wider knowledge of the APs estimated locations[3] and characteristics. Hence, vehicles will exchange the AP data (or part of it) stored in their local databases. The possible alternatives for exchanging wireless infrastructure information are investigated in Subsection III-C. This exchange will help each vehicle locate the available wireless infrastructure even in regions which have

[2]Although our solution focuses on AP information exchange, it can easily be generalized to spread information about any wireless equipment available among vehicles.

[3]It has to be noted that the knowledge of the GPS coordinates of the APs is not necessary for CIDP operations since what would be important is the visibility area of these APs in the streets which can be estimated by knowing the positions of vehicles at the time when they discovered these APs.

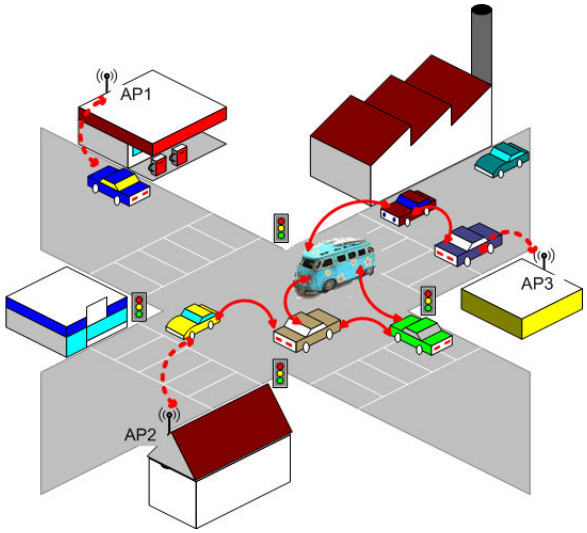

Fig. 1. Scenario of vehicle cooperative communication: By consulting its WID and knowing its heading, the bus can decide whether it should keep its data (it will encounter an "open" AP soon) or forward it to a neighboring vehicles (no immediate APs in its path).

not been visited. It will then reduce the time required to scan the APs and select the optimal one to which each vehicle has to connect (as described in Figure 1).

B. Wireless Infrastructure Database

Each vehicle stores received information about APs (directly or through V2V communication) in a specific database called the Wireless Infrastructure Database (WID). Each AP entry of this database is composed of two parts: a part reserved to the AP properties and a second one reserved to store information about the vehicle that detected the access point. Once a vehicle gets information about an AP, it adds a new entry to the WID if this is the first time it heard about it. When the AP is already stored in the WID, it updates the information accordingly. Consequently, CIDP allows to keep an up-to-date WID in each vehicle.

Among the fields stored in the first part of an AP entry in the WID database, we can list the BSSID, the ESSID, and the AP-related security information. We also have the frequency channel number field (which depends on the AP supported 802.11 variant: a/b/g/p) indicating on which channel the AP is operating and whether the Dynamic Frequency Selection (DFS) option is enabled or not. Note that if DFS is not enabled, when data is to be transmitted, the vehicle will not have to scan again all the channels. Another field is reserved to the AP estimated position which can be approximated with triangulation methods [5] using at least the positions and signal strength information of three of the vehicles that detected it. Initially, this field is left empty but later with more received information, the vehicle would be able to compute an approximated value of it. As far as the position field is concerned it consists of the latitude, the longitude, and the elevation (altitude) of the access point. Additionally, a field named `DiscoveryTimestamp` stores the time when the AP entry has been discovered (i.e scanned). In order to remove obsolete entries from the WID, we use an expiration time field indicating the time after which the entry will be removed if not updated. Other values such as signal level, noise level and quality of the signal (computed with both signal and noise levels values) are also stored to depict the quality of the signal being received from the AP. Finally, a set of extra fields is added according to the AP security information. It contains information about the IP, the default gateway, and the DNS address(es) obtained whenever a vehicle successfully assocciate with an AP using DHCP. Otherwise, it will be filled with information about the AP's adopted security mechanism. We beleive that storing this information can help reducing association time. Experimental results showing improvements obtained thanks to IP caching can be found in [8].

The second part of the AP entry in the WID stores information about the vehicle that originally detected the AP (not necessarily the one from which the corresponding properties have been received). These fields include the identity of the vehicle that detected the AP, its velocity and its position(a tuple consisting of the latitude, the longitude, and the vehicle elevation since it can be on top of a bridge or inside a tunnel)when the AP has been discovered for the first time.

Entries in the WID are filled upon reception of messages either directly from scanned APs or from neighboring vehicles through V2X communications. In the next section, we explain how vehicles can announce the information they gathered about the infrastructure to other surrounding vehicles and how they can request missed information from them.

C. Announcing access points

One of the design goals of CIDP is to ensure the sharing of wireless infrastructure knowledge among vehicles. This is achieved through the exchange of specific messages opportunistically between neighboring vehicles. To increase the efficiency of CIDP, two types of infrastructure announcement messages have been introduced: unsolicited and solicited. These two categories are detailed in the following subsections.

1) CIDP unsolicited announcements: Unsolicited announcements designate periodic broadcast messages sent by vehicles to cooperatively help each other update their WID databases with fresh and new information about available APs. We defined three different kinds of unsolicited announcements namely position, time and type-based broadcasts which can be used by applications looking for a temporary (limited) Internet connectivity. In the first type, the vehicle will broadcast the information about only the APs located in a specific zone. The second one serves to limit broadcasted data to that inserted/updated after a specific time. This type can be used to increase the freshness degree of the WID data since only new infrastructure information will be circulating in the network. Finally, the type-based broadcast restricts the broadcasted information to only APs that for instance offer free access without security protection. CIDP also provides the possibility to combine two or all these types in unsolicited announcements.

Obviously, the efficiency of CIDP thanks to unsolicited announcements broadcasting is highly correlated with different factors such as the movement pattern and density of the vehicles. Moreover, the broadcast interval, which defines the duration between two successive broadcasts of unsolicited announcements, has to tuned effectively since it would impact the frequency and quality of updates of WID's entries.
The effect of these factors will be investigated through extensive simulations in Section IV.

2) CIDP solicited announcements: Sometimes, a vehicle can require a precise information about the wireless infrastructure in a specific zone (for example, a tourist's vehicle can demand the full list of APs located in a first-time visited city). In this case, unsolicited announcements can not be sufficient for rapidly handling this request. Hence, CIDP allows a vehicle to send an explicit infrastructure broadcast request to its neighbors. In return, only vehicles which have the data matching this request have to answer. Although these replies can be unicasted to the originator vehicle, we prefer broadcasting them in order to allow vehicles in the neighborhood to graciously update their own WIDs. The replies issued to answer CIDP request messages are called solicited announcements. It is clear that one CIDP infrastructure information request may result in more than one solicited announcement as the replies generated from different vehicles may not contain the same content. Vehicles overhearing at least one solicited announcements containing similar information they are willing to send have to cancel their sending process. A distance-based congestion control mechanism, where a backoff-time inversely proportional to the distance from the originator vehicle is used. This mechanism would contribute on the increase of the efficiency of CIDP by avoiding collisions between solicited announcements. For solicited announcements with different content, the originator vehicle has to merge the gathered wireless infrastructure information.
Similarly to unsolicited announcements, solicited announcements can also be position-based, time-based, or type-based according to the information the user applications require to have at the time of generating the request.
Figure 2 shows how each of these described CIDP messages is processed. Upon receiving either solicited or unsolicited announcements, a vehicle has to check the possible updates of its WID. This operation can be achieved either by adding entries of new announced APs or by updating the content of one or more fields (among those described in Subsection III-B) of an existing AP. Besides, in the case when a vehicle is preparing a solicited announcement while it receives an unsolicited announcement, it has to consider fresher announced information of its solicited announcement message. Furthermore, when a request message is received, a vehicle will check if it has some request-matching entries and prepare a solicited announcement to be broadcasted.
The next section describes the fields included in each CIDP message.

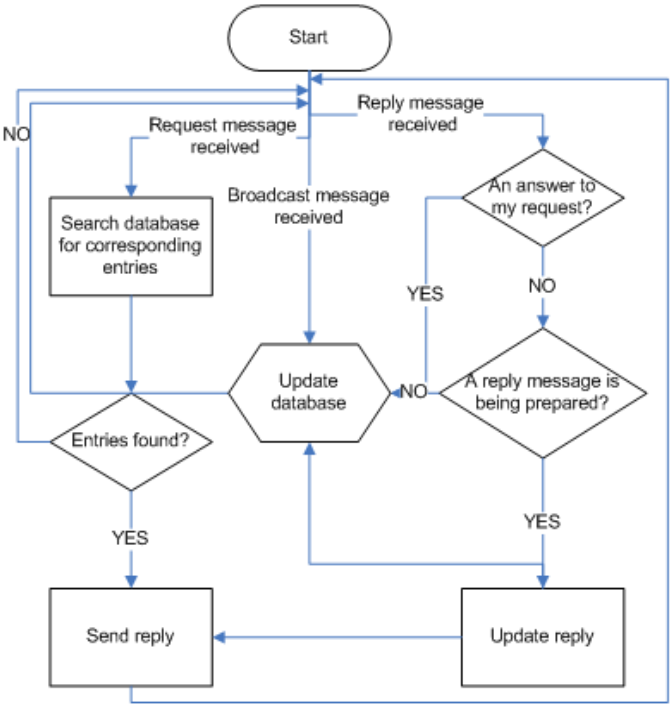

Fig. 2. The global CIDP flowchart.

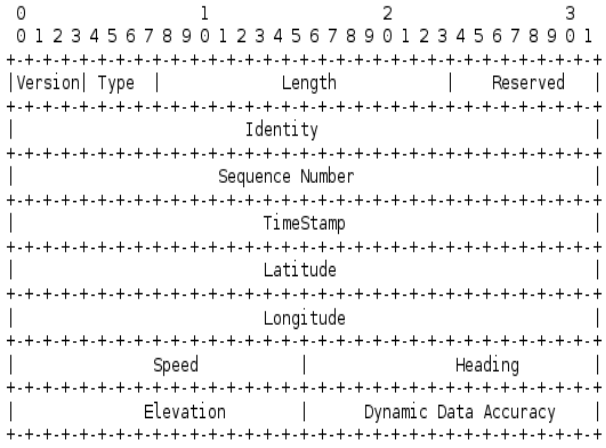

Fig. 3. Format of the generic part of CIDP messages.

D. Structure of CIDP messages

In this subsection, we describe the format of CIDP messages exchanged between vehicles. Each field is explained and justified. However, common fields to more than one type of messages are discussed just once.
Each message in CIDP is divided in two parts: a generic part, which is always present for all messages, followed by an optional part which content depends on the message type. Thus, this part will be detailed separately for each message type.

1) CIDP Packet: Generic Part: The format of the generic part is depicted in Figure 3 as an ASCII representation in network byte order. The content of some of these fields has been

derived from those used in the system architecture defined in [11] in order to guarantee the easy integration of CIDP in ITS communications architectures under development.

This part is common for all types of CIDP messages. It includes the following fields:

Version (Protocol Version) 4-bit selector. Identifies the version of the CIDP protocol.

Type 4-bit selector. Indicates the type of the exchanged message. Three types are used: unsolicited announcements (0x0), infrastructure information requests (0x01) and solicited announcements (replies) (0x02).

Length 16-bit unsigned integer. Length of the message in bytes of data related to the APs being sent in this message.

Reserved 8-bit. The content of the field Reserved changes according the type of the message to be sent thus we will detail it separately in each of the different messages types.

Identity 32-bit identifier. Identity of the vehicle.

Sequence number 32-bit unsigned integer. Indicates to receiving vehicles whether broadcasted data has been updated to process or not to ignore it.

Timestamp 32-bit unsigned integer. Expresses the time in milliseconds at which latitude and longitude of the vehicle have been acquired.

Latitude 32-bit signed integer. Latitude of the vehicle expressed in signed units of 1 meter.

Longitude 32-bit signed integer. Longitude of the vehicle expressed in signed units of 1 meter.

Speed 16-bit signed integer. Speed of the vehicle expressed in signed units of 0.01 meters per second.

Heading 16-bit unsigned integer. Heading of the vehicle expressed in signed units of 0.005493247 degrees from North.

Elevation 16-bit signed integer. Elevation of the vehicle expressed in signed units of 1 meter.

Dynamic Position Accuracy Indicators of the accuracy of the position, speed and heading information. This field may be used in the future to increase the accuracy of the position information using distributed position computing mechanisms which are out of the scope of this work.

As an example, infrastructure request messages contain only the CIDP generic part. More details about the content of each message will be given in Subsection III-E.

2) CIDP Packet: Optional Part: In this section, we detail the content of the CIDP optional part eventually added to the generic part according to the type of message.

One of the important data which is present in both unsolicited and solicited announcements is AP information. An AP data frame contains the data related to one of the APs to be announced. Hence, there are as many frames as there are APs being announced. In Figure 4, we provide the content of an AP Information Element (AP-IE). The fields in the AP IE are as follows:

Discovery Timestamp 32-bit unsigned integer. Expresses the time in milliseconds at which the AP was scanned by the vehicle.

Discoverer Latitude 32-bit signed integer. Latitude of the vehicle that actually scanned the AP expressed in signed units of 1 meter.

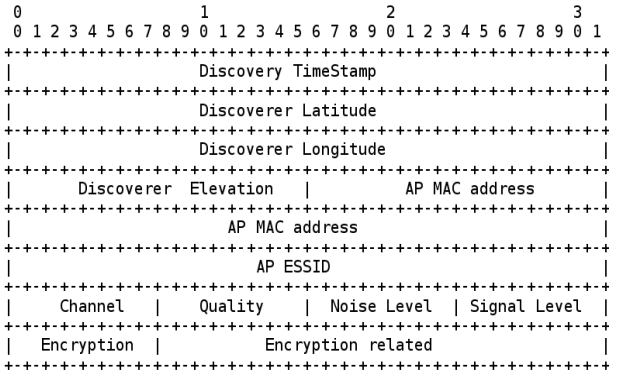

Fig. 4. Format of AP Information Element (AP-IE) announced in one of the CIDP messages.

Discoverer Longitude 32-bit signed integer. Longitude of the vehicle that actually scanned the AP expressed in signed units of 1 meter.

Discoverer Elevation 16-bit signed integer. Elevation of the vehicle that actually scanned the AP expressed in signed units of 1 meter.

AP MAC Address 48-bit address. The MAC Address of the access point.

AP ESSID 32-bit characters. The name of the access point.

Channel 8-bit signed integer. The frequent channel number on which the access point is operating.

Quality 8-bit signed integer. Quality of the received signal, computed using both the noise and the signal levels.

Noise Level 8-bit signed integer. Power of the noise received with the signal expressed in dB.

Signal Level 8-bit unsigned integer. Power of the received signal expressed in dB.

Encryption 8-bit signed integer. The 2 first bits (n°0 and n°1) describe whether the AP has a secured access or not. When set to 00, they indicate that no security mechanism is used by the AP. In this case, the last 4 bits of the same field will be used as flags indicating whether the vehicle got an IP address (bit n°7), a default gateway address (bit n°6) and one or more DNS server addresses (bits n°5 and 4). Consequently, the required fields for non-secured AP as given in Figure 5 should be added to the AP Information Element shown in Figure 4.

IP address 32-bit address The assigned address to the vehicle by DHCP. This field is added if the bit n°7 is set to 1.

DNS address(es) 32-bit address. The address(es) of DNS server(s) to use when connected to this AP. According to the value set in the bits n°5 and n°4 of the encryption field, there will be an address of 0 to 3 DNS servers indicated.

Gateway address 32-bit address. The address of default gateway to use when connected to this AP. This field is added if the bit n°6 is set to 1.

If bits(0,1) = 0x01, 0x10, or 0x11 this indicates whether WEP, WPA or WPA2 are used as the encryption mechanism,

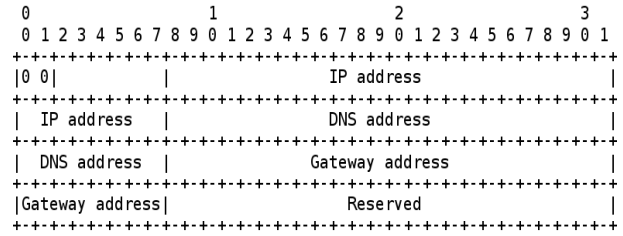

Fig. 5. Information fields of a non-secured AP which provides to vehicles Internet connectivity.

respectively.

E. The CIDP messages

As mentioned in Subsection III-D1, CIDP operations are based on three different types of messages:

- unsolicited announcements: periodic broadcast messages of AP information elements sent by all vehicles.
- infrastructure information requests: broadcast messages sent by a vehicle in order to request for wireless infrastructure information.
- solicited announcements: broadcast replies sent by some vehicles upon receiving infrastructure information requests.

1) CIDP periodic broadcast messages: This message is used to spread the information collected about APs. This message has in its optional part the set of AP Information Elements to broadcast to all surrounding vehicles.
For CIDP periodic broadcast messages, the one byte field *Reserved* of the generic part of Figure 3 is divided into two parts: 2 bits to indicate the broadcast type (*bt*) and the 6 bits set information related to the type selected in the first part (*bt_related*). The possible values of the reserved field are as follows:

- If the whole AP database is being broadcasted, *bt* is set to 00. This kind of AP information broadcast occurs only if the database size is beyond a specific threshold which value is indicated in the *bt_related* field and is expressed in units of bytes.
- When the broadcasting is position-based, *bt* value is 01. In such type of AP information broadcast, we need to mention the boundaries of concerned geographic region. Although several shapes can be used, CIDP adopts the circle shape one which could be much more useful and can be specified in the message with less overhead. The center of the circle can be easily identified by the position of the vehicle sending the broadcast. The circle radius is set in the *bt_related* field and is expressed in units of 100 meters.
- Finally, *bt* is set to 0x10 if a time-based broadcast is chosen. This type of broadcast limits the broadcasted information to only newly detected APs i.e detected after a certain time which value is specified in the *bt_related* field and is expressed in units of minutes.

2) CIDP infrastructure information request: When a vehicle requires specific information which it couldn't obtain neither in its WID nor through broadcasted unsolicited announcements, it can decide to send an infrastructure information request message where it specifies the requested data. As different types of requests can be sent, the value of the *Reserved* field of the generic part of Figure 3 depends on the request type. More precisely, there are three possible request types (or different combinations of these four types). Hence, we used three bits of the *Reserved* field as flags to indicate which request types are used. Bit n°0 indicates whether the request is position-based or not. Bit n°1 is set in the case the request is time-based. When the vehicle wants to request only the set of non-secured APs, bit n°2 will be positioned to 1.
Once the type flags are set, several optional fields will be added according to them. If the flag time is set, an extra field indicating the time expressed in minutes is added (32-bit signed integer). When the vehicle requests data about a specific zone, the added fields are the coordinates of the center node (a two 32-bit signed integer for latitude and longitude) and the circle radius (32-bit signed integer). Finally, no additional fields are required if a request by AP type (secure or not secure) is to be sent.

3) CIDP broadcast replies: A CIDP reply message is sent as a response to a received information request from a neighboring vehicle. This message is only issued if the vehicle has information about the requested APs or about some of them. For this particular type of messages, the field *Reserved* of the generic part of Figure 3 remains unused. In addition to the APs Information Elements, two extra fields which are the Originator Identity and Originator Sequence Number are added.
Originator Identity 32-bit address Identity of the vehicle to which the reply is sent.
Originator Sequence Number 32-bit unsigned integer. The received sequence number in the request being answered. This identifies the vehicle that originated the request being replied. As explained in Section III-C2 , this reply will be broadcast to all neighbors in order to allow them update their WID databases.

IV. CIDP PERFORMANCE ANALYSIS

We implemented the CIDP protocol in NS-2.33 [15]. For simulation purposes, we used random generated mobility traces. These traces were obtained using TraNS [17] which is a GUI tool that integrates traffic and network simulators (NS-2 and SUMO [16]) to generate realistic simulation scenarios.

A. Simulation scenario

We investigated CIDP performances with random mobility traces generated with SUMO.
The network topology consists of a grid map of 10*10 edges. The distance between vertices is set to 300 meters. TraNS is then used to generate random mobility traces of the vehicles. We run simulation for three different densities values: high density with 850 vehicles, medium density with 400 vehicles,

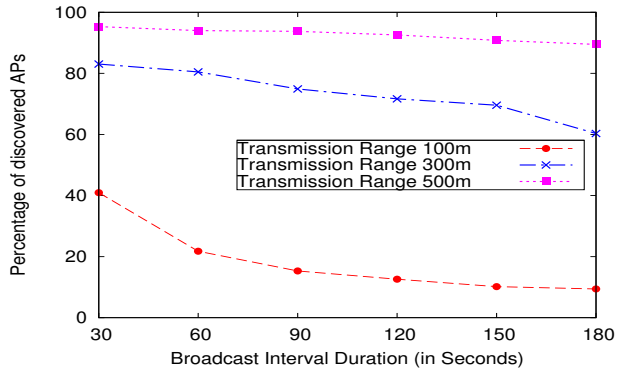

Fig. 6. Impact of variable transmission range of vehicles on CIDP performances in the case of 250 vehicles.

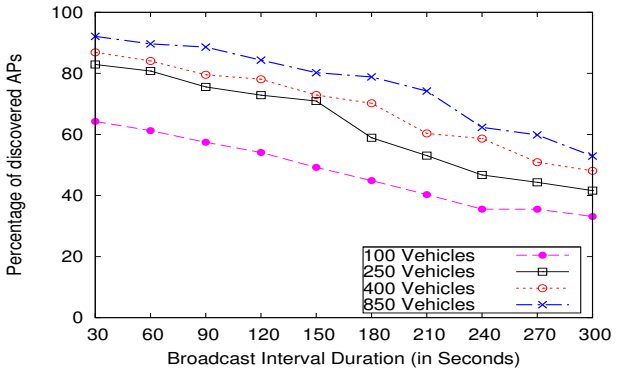

Fig. 7. Impact of the broadcast interval duration on the wireless infrastructure discovery process.

and low density with only 100 vehicles to study the impact of vehicles density variation on the APs' discovery process. The number of deployed APs is set to 20. Simulation ends when all the vehicles have left the network.

B. Simulation results

We describe and discuss the results obtained with CIDP unsolicited announcements broadcast exchange when varying a set of parameters such as transmission range, density and speed.

1) Impact of variable transmission range: We first, study the impact of varying the vehicles' transmission range on CIDP performances. As depicted in Figure 6, with 250 vehicles traveling with their transmissions ranges varying between 100, 300 and 500 meters, we notice that increasing the vehicles' transmission range highly improves CIDP performances even for low densities. In fact, with a transmission range equal to 500m, more than 90% of deployed APs were detected compared to less than 30% when the range is fixed at 100 m with variable broadcast interval duration.

In the following subsections, the vehicles' transmission range will be fixed to 300m.

2) Impact of CIDP broadcasting period: In Figure 7, we observe that decreasing the duration of V2V broadcast allows vehicles to discover a higher percentage of access points. We also notice that with small broadcast interval values, the discovery of APs is mainly accomplished thanks to CIDP V2V communications. As shown in Figure 8, we remark that among the total discovered APs, the higher percentage is discovered with V2V broadcasting especially with small broadcast interval values. In fact, when decreasing the broadcast period, the likelihood of vehicles meeting increases. This enhances the exchange of the information collected about APs between encountered vehicles. Consequently, the number discovered APs increases. However, we observe that when the broadcast interval duration increases, the V2V communications occur less frequently. Hence, the percentage of directly discovered APs increases.

To estimate CIDP cost, we compute the overhead it induces in terms of the number of exchanged bytes between vehicles.

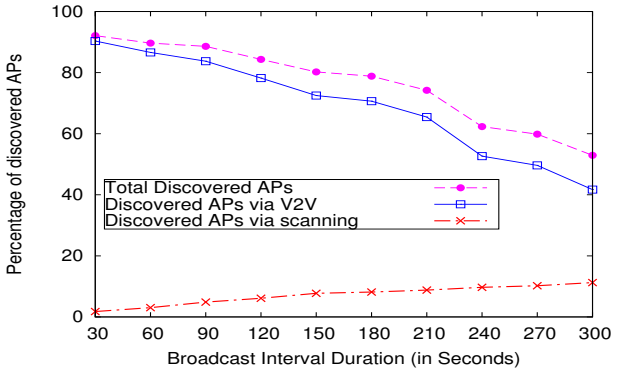

Fig. 8. Impact of V2V communications on the wireless infrastructure discovery process for the case of 850 vehicles.

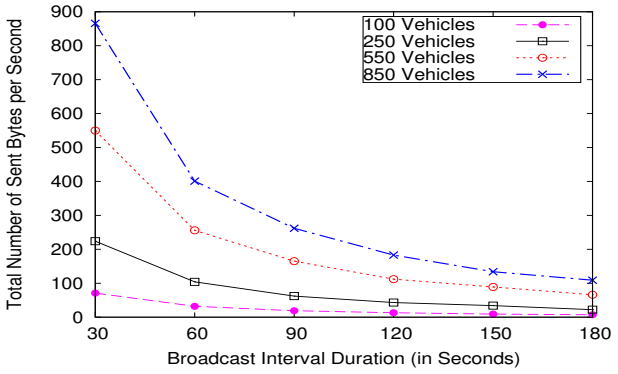

Fig. 9. Overhead due to CIDP broadcasting in number of generated bytes per second.

Figure 9 depicts the number of bytes sent per second during the V2V communication process. Obviously, the overhead increases with the number of vehicles or when the broadcast interval duration decreases. Nevertheless, in order to avoid overloading the network, CIDP would use one of the available Service Channels (SCH) and not the Control Channel (CCH) reserved for critical safety V2X applications.

3) Impact of the vehicles' density: Figure 7 also highlights the impact of density variation. We notice that the higher the

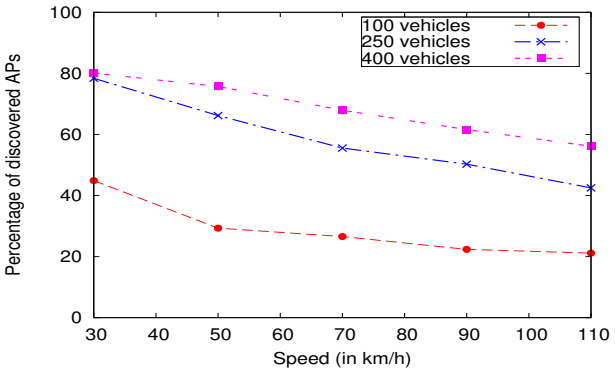

Fig. 10. Impact of the variation of vehicles speed on the AP discovery process.

density is, the higher is the percentage of discovered access points. Also, high density enhances the V2V communication performance. In fact, with more vehicles running in roads, the probability of meeting each other increases and thus the information is exchanged easily and efficiently. Situations with high densities are very frequent in real scenarios (traffic jams, rush hours, highly frequented roads, etc.).

4) Impact of the vehicles' speed: To measure the impact of vehicles speed variation, we varied vehicles maximum authorized speed during the simulation time from 30 km/h to 110 km/h. We considered the scenario with different vehicles densities and 20 APs deployed. The broadcast interval was set to 90s and the vehicles range was fixed to 300m. Simulation ends when all vehicles leave simulation. As depicted in Figure 10, we notice that higher speed slightly decreases the performances of CIDP. This is what we expected since the connectivity time between vehicle is reduced.

V. Conclusion and Future Works

In this paper, we proposed a new protocol CIDP (Cooperative Infrastructure Discovery Protocol) for gathering the wireless infrastructure information through vehicular cooperation. It offers the advantage of easy and accurate update of access points database. Different information dissemination capabilities (solicited and unsolicited) have been defined in order to allow vehicles to communicate and exchange their knowledge about the discovered APs. Simulation results showed that the V2V broadcast interval and the vehicles density have an expected impact on the performance of CIDP.

In fact, CIDP's performances are better with a higher density of vehicles since it helps spreading the AP information to all vehicles.

Nevertheless, this condition can be easily met in real daily traffic scenarios. Besides, CIDP still performs well even for lower densities.

Future works would include further simulation experiments of the proposed solution especially tuning the broadcast frequency to the density of vehicles in order to reduce the induced overhead. It will also focus on the use of these databases for Vehicle-Internet opportunistic communications since the wireless infrastructure database can be useful for the AP selection algorithm which can predict future possible connections to the Internet when the vehicle is moving. A preliminary work in this direction has been already presented in [10].

References

[1] A. Akella and G. Judd and P. Steenkiste and S. Seshan, *Self Management in Chaotic Wireless Deployments*, ACM MOBICOM, pp. 185-199, 2005.
[2] P.Bellavista and E. Magistretti and U. Lee and M. Gerla, *Standard Integration of Sensing and Opportunistic Diffusion for Urban Monitoring in Vehicular Sensor Networks: the MobEyes Architecture*, IEEE International Symposium, 2007.
[3] K. Matsuzawa and K. Mase and Y. Hirano and S. Kajita, *Experience Map Creation by Virtual WLAN Location Estimation*, International Symposium on Wearable Computers, ISWC, 2006.
[4] A. Nicholson and Y. Chawathe and M. Chen and B. Noble and D. Wetherall, *Improved access point selection*, MobiSys, 2006.
[5] A. Roxin and J. Gaber and M. Wack and A. Nait-Sidi-Moh, *Survey of Wireless Geolocation Techniques*, IEEE Globecom 2007, IEEE Workshop on Service Discovery and Composition in Ubiquitous and Pervasive Environments (SUPE).
[6] S. Srinivasan, *Opportunities and Challenges in Unlicensed-Band Networks*, Wireless/Mobile Planning Group Workshop.
[7] J. Eriksson and H. Balakrishnan and S. Madden, *Cabernet: vehicular content delivery using WiFi*, ACM MOBICOM, pp. 199-210, 2008.
[8] V. Bychkovsky and B. Hull and A.n Miu and H. Balakrishnan and S. Madden, *A Measurement Study of Vehicular Internet Access Using In Situ Wi-Fi Networks*, ACM MOBICOM, pp. 50-61, 2006.
[9] Y. Qian and N. Moayeri, *Design Secure and Application-Oriented VANETs*, Proc. IEEE Vehicular Technology Conf., pp. 2794-2799, 2008.
[10] I. Amdouni and F. Filali, *Intelligent strategies of access point selection for vehicle to infrastructure opportunistic communication*, Proc. IEEE VNC'2009, 2009.
[11] *COMeSafety: Communication for eSafety*, http://www.comesafety.org. [Accessed: Dec. 24, 2009].
[12] *FON maps*, http://maps.fon.com. [Accessed: Mar. 10, 2009]
[13] *Intel research Seattle, place lab: a privacy-observant location system*, http://placelab.org. [Accessed: Mar. 10, 2009]
[14] *JIWire, Wi-Fi access point locator*, http://jiwire.com. [Accessed: Mar. 10, 2009]
[15] *NS-2 simulator*, http://www.nsnam.isi.edu. [Accessed: Fev. 20, 2009]
[16] *SUMO, Simulation of Urban MObility*, http://sumo.sourceforge.net. [Accessed: Jan. 7, 2010]
[17] *TraNS*, http://www.trans.epfl.ch. [Accessed: Jan. 7, 2010]
[18] *WiFi Maps: War-driving maps and access points locator*, http://www.wifimaps.com. [Accessed: Mar. 10, 2009]