Evaluation of VANET Performance for Anonymous Reporting through Coherent, Automatic Address Resolution (CAAR)

Urquiza Luis[1]; Rodríguez Ana[2]; Tripp Carolina[3]; Aguilar Mónica[1]

[1]Universitat Politècnica de Catalunya (UPC), Departamento de Ingeniería Telemática, Barcelona, Spain
[2]Escuela Politécnica Nacional, Facultad de Ingeniería Eléctrica y Electrónica, Quito, Ecuador
[3]Universidad Autónoma de Sinaloa (UAS), Falcultad de Informática, Mazatlán, México

Abstract: Due to the unpredictable trajectory of its moving nodes, a VANET is a demanding communication environment. For such dynamic communication infrastructures, when certain requirements neet to be coped, the performance is a critical parameter. In this paper, we evaluate the VANET performance when an anonymous reporting service is deployed. In order to pay off the overhead generated by the anonymity service (based on the Crowds mechanism), we tune the layer-two address resolution protocol (ARP) so that it can be performed at the routing level. The tests are done with different VANET routing protocols and vehicle densities by means of simulations of a realistic scenario where the parameters of the anonymity service are also modified to determine their impact on the overall performance of the vehicular network. We found that, despite the more demanding environment generated by the deployment of the anonymity service, the VANET has a good performance in terms of packet losses, delay, and neighboring behavior, thanks to the implementation of a more efficient layer-two address resolution mechanism.

Keywords: VANETs, vehicular networks, crowds, anonymity service, address resolution protocol.

Evaluación del Rendimiento de VANETs para Envío de Reportes Anónimos usando Resolución Automática Coherente de Direcciones

Resumen: Por sí misma, una VANET es un entorno de comunicaciones muy demandante debido a sus nodos móviles cuya trayectoria es, en general, desconocida. Por ello, el rendimiento de las redes vehiculares es un parámetro crítico de estas infraestructuras dinámicas de comunicaciones, especialmente cuando se requiere desplegar sobre ellas servicios de red con distintos requisitos. En este artículo se evalúa el rendimiento de una VANET cuando un servicio anónimo de reporteo es desplegado. Con el fin de compensar la carga generada por el servicio de anonimidad, se afina el protocolo de resolución de direcciones en capa dos (ARP) de manera que éste se realice en capa de enrutamiento. Las pruebas se realizan con diferentes protocolos de enrutamiento y densidades de vehículos, por medio de simulaciones de un escenario realista en el que los parámetros del servicio de anonimidad son también modificados para determinar su impacto en la red vehicular. Encontramos que, a pesar del entorno más demandante que se obtiene por el despliegue del servicio de anonimidad, la VANET tiene un buen rendimiento en términos de pérdida de paquetes, retardo y establecimiento de vecinos, gracias a la implementación de un mecanismo de resolución de nombres más eficiente.

Palabras clave: VANETs, redes vehiculares, crowds, servicio de anonimidad, protocolo de resolución de direcciones.

1. INTRODUCTION

VANETs or Vehicular ad hoc networks (Hartenstein et al, 2010) are network infrastructures built of moving vehicles that interchange data in order to maintain communication routes among them and with other static devices in the road. This kind of networks could be able to support the transmission of very useful information about variables in the road (traffic, weather, accidents, etc.), which may help to implement road safety applications.

Although many other services may arise supported by vehicle ad hoc networks, reporting the state of the elements of a vehicular traffic system is one of the main research areas derived from VANETs. This reporting service consists of

luis.urquiza@entel.upc.edu

sending sensed data from vehicles so that this information can be used to make decisions in a road system.

However, VANETs are built of nodes whose position and speed are prone to change dynamically over time. In order for vehicles to be aware of the routes over such a changing topology, a great deal of information needs to be sent among them through broadcast communications.

If other services different from reporting are deployed over vehicular networks, the amount of data to be transmitted significantly increases.

Additionally, the data generated from the moving nodes may contain identifying information of a vehicle, which is a threat to privacy since such information could be "seen" by many other entities and not only by the destination (Dötzer, 2006). Some anonymity mechanisms (Chaum, 1988) have been proposed to reduce the privacy risks for users in communication networks but very few of them are tailored to meet the specific parameters of vehicular networks. In fact, some of such contributions are based on obfuscating the user information by combining it with forged data, or by randomizing (and commonly lengthening) the path through which information is carried.

In a couple of previous works we have addressed some of the aforementioned issues about VANETs. On the one hand, a collaborative protocol was proposed by Tripp et al (2013) for anonymous reporting based on Crowds (Reiter, 2008), which is a mechanism aware of its impact on vehicular networks performance. On the other hand, Urquiza et al (2014) presented a mechanism to improve the performance of address resolution (ARP/Neighbor Discovery) for vehicular ad hoc networks where the ARP information is sent through the routing messages used in VANETs. By combining these two contributions, the main purpose of this work is to evaluate the performance on VANETs in terms of anonymity level and packet losses obtained with the application of the Coherent Automatic Address Resolution when an anonymous reporting service (also tailored for vehicular communication) is being provided to enable privacy protection among vehicles.

2. BACKGROUND

2.1 Routing Protocols in VANETs

Routing protocols in VANETs are responsible for finding a path from a source device to a destination one, through a very dynamic topology build of moving vehicles and temporal communicating links. Such changes may depend on several conditions derived from the road state or even the number of vehicles during a period of time (traffic). According to these conditions of VANETs, some routing protocols may perform better than others. AODV, GPSR and GBSR are some of those routing protocols.

Perkins et al (2003) describe AODV as a reactive protocol proposal which combines some proactive routing features. It sets up routes on-demand (route discovery) that are maintained (route maintenance) as they are needed. For route discovery, Route Request and Route Reply messages are used. For route maintenance, Hello messages and Router Error messages are employed to indicate whether a route is alive or not available, respectively. Suitable for intermediate and slightly high vehicle density areas with very low number of active connections, AODV is still an interesting option for VANETs.

Karp et al (2000) depict GBSR as a derivation of GPSR, a responsive routing protocol that uses the node position as a parameter to make forwarding decisions. GPSR forwards packets to nodes that are closer to the destination (greedy forwarding).

When such behavior is not possible, an approach called perimeter forwarding is used, which is not so efficient as probed by Tripp et al (2013). Thus GBSR outperforms GPSR in terms of packet losses (packet delay is slightly increased) by replacing perimeter forwarding with the use of a buffer. This means that when no closer neighbor is found, the vehicle carries the packet until a closer node to destination appears. Additionally, GBSR makes a more precise forwarding decision based on a map aware process that estimates position more accurately.

2.2 Anonymous Communications

Since a lot of information in VANETs is sent through the free space, privacy becomes an issue for the data transmitted in such environment. Data transmitted through VANETs might be very critical if coupled with the position or state of a node, or if it has to do with commands to regulate vehicle traffic. Thus, in some cases, mechanisms to protect such information will be necessary. One of such mechanisms is anonymity which hides the identity of the entities participating in communication. Anonymity is a service that needs to be implemented in communication networks in order to protect the private information that users interchange. The aim of anonymous communications is to ensure that the identities of the participants cannot be individuated by an attacker (which may bring identification).

Some anonymizing methods (Reed, 1998, and Scarlata, 2001) have been proposed to protect the privacy of users in information networks and also at the application level (e.g. when users send search queries to Google). Many of such mechanisms (such as the tool evaluated by Estrada et al. (2014) rely on forging information and dramatically changing the common communication algorithms. Although most of these anonymity mechanisms yield promising levels of privacy for users, the price is very high in terms of communications efficiency. In order to reach anonymity, a network has to do extra work that may not be affordable for some environments with very dynamic behaviors, such as VANETs.

A very popular mechanism that provides with an anonymity service is Crowds (Reiter et al, 1998), which has previously been integrated to VANET scenarios.

Crowds has been proposed in the literature to protect the nodes of a network from being identified by an attacker.
This anonymity algorithm tries to "hide" the identity of the original sender of a message within the identities of the rest of the nodes. Collaboration among nodes is the base of Crowds, which enables a node to not always send a message directly to its destination, but to sometimes send it randomly to any other node. When Crowds is used, a node sends a message directly to its destination with a probability *p* or randomly to any other node with a probability *1 - p*.

2.3 *ARP and VANETs*

ARP or Address Resolution Protocol (Plummer, 1982) is a common mechanism used to find the physical MAC address of a device whose IP address is already known, in order to initiate communication. This process is essential to perform link layer communications since, from upper layers, messages are directed towards IP addresses. As reviewed by Carter et al (2003), some malfunctions of ARP have been reported, especially when working over unconventional network infrastructures.

The issues derived from such inefficiencies (packet losses, delay, etc.) could significantly reduce the quality of communications in complex networks such as VANETs. Since most of the basic network protocols were not designed to support the so demanding services (in terms of delay, mobility, processing, etc.) that are promoted currently, there is a wide research field in the optimization of these protocols.

3. APPLYING CAAR TO ANONYMOUS REPORTING IN VANETs

3.1 VANET Reporting Services

Many applications are forecasted to be provided under the infrastructure that VANETs may offer. One of such applications is, undoubtedly, reporting information about the network environment. Reporting services imply the use of vehicular networks to transport informative messages that nodes or their drivers generate about the road or traffic conditions or misbehaviors of other drives. This information may be critical to get feedback from the moving nodes, so that the vehicle infrastructure can be adapted (traffic lights, warnings on the road, etc.) to such conditions (emergencies, heavy traffic, weather, etc.). The evaluation we do in this work is focused on this kind of services which depends on the communication from the vehicles to the network infrastructure (static devices in the road that collects the information from vehicles). This clarification is relevant since other more demanding services (such as audio or video broadcasting in real time) will have to receive a very different treatment in such a dynamic environment as a VANET.

3.2 Anonymity in VANETs

Since the infrastructure of a VANET is built of nodes that are not entirely trusted, privacy issues appear when information about users (such as position and routes) has to be transmitted through such multi-hop network. Several sources of attack on privacy may arise, but the network infrastructure itself is the first one.

Having assumed the attacker, we can adopt a criteria about the attacker strategy to break the user privacy. In accordance to the work done by Haklay et al (2008), we suppose that the network would try to identify the origin of a message. In order to prevent the network from detecting the original sender of a reporting message, an anonymity service inspired in Crowds can be adapted to mobile multi-hop networks. Some modifications have to be implemented to adjust the original Crowds proposal to the dynamic environment of VANETs.

This version of Crowds enables mobile nodes to forward messages towards its destination, not only based on the underlying routing protocol (which sends a message through the best path to its destination), but also based on the attempt to hide the original sender of the message. With the purpose of anonymizing the communication (but at the expense of the efficiency of communication), a node could forward a message to a node different from the one suggested by the routing protocol. The process is repeated on each node until the message reaches its destination.

Crowds was somehow adapted by Urquiza et al (2014) to work in VANETs, but no other variants have been included in the scenario. If, for example, the destination node tries to guess the identity of the node originator of a message, it will be able to realize the last forwarding node only, so that the original sender's identity will be maintained private.

In this work, we evaluate an address resolution scheme we called CAAR, when an anonymity service (inspired in Crowds) is implemented in a VANET. Crowds was adapted to avoid the first mandatory step (an initial random hop), allowing the original senders to directly forward a message to the destination with some probability *p*. This change considerably reduces the number of hops that messages need to reach their destination, but slightly increases the probability that the source node of a message is identified. As can be expected, anonymity services based on collaboration (such as Crowds) generate more traffic through networks, which is especially negative in dynamic infrastructures such as VANETs. Thus, it may be useful to lose some anonymity in order to reduce the packet loses provoked by excessive traffic in VANETs. There is clearly a tradeoff between packet loses (amount of traffic) and anonymity, but it is possible to get low packet loses and still an adequate anonymity level. Additionally, it is worth noting that more transactions will be generated in the reporting service we use to build our test scenario, than the ones in classical unicast traffic applications.

3.3 CAAR implementation

Due to the dynamic topologies of VANETs, issues appear with some established and basic communication protocols. This is the case of ARP, which is an essential mechanism for network devices to find the hardware address corresponding to a given IP address. According to Urquiza et al. (2014), the

layer-two address resolution process in VANETs can be integrated into the routing layer in order to avoid the negative effects (in terms of packet losses) produced by the incompatibility of ARP and on-demand MANET routing protocols. Such incompatibility becomes evident in the aforementioned research works that show that ARP may hinder the neighbor or the route updating process due to its poor performance on dynamic topologies. However, as shown by Urquiza et al (2014), coupling the address resolution mechanism into the neighbor discovery process (part of the routing protocol), and thus avoiding the use of ARP, helps to improve the communication performance, since the link layer information becomes automatically available at the routing layer.

As stated by Urquiza et al (2014), CAAR is an alternative to ARP for IP multi-hop vehicular networks and inspired in previous research about automatic address resolution. It eliminates the interactions between routing and link layers during the address resolution process (stops using conventional ARP). CAAR is an extension of the Automatic Address Resolution (AAR) mechanism for MANETs as depicted by Carter et al (2003). It consists of building routing signaling messages with a new field that includes the MAC address information of the node generating the routing message. When a node receives the routing message, the routing daemon extracts the IP and MAC addresses. Finally, our address resolution process receives this information and updates the ARP table.

No ARP signaling is used, and minimal extra work is added to the routing process when the CAAR mechanism is deployed. CAAR works as follows: when a routing signaling packet arrives to a node, it is processed by the routing daemon which extracts the source IP and MAC addresses from the IP header and the signaling message, respectively. Such IP packets, as depicted in Figure 1, contain both IP and MAC addresses at the same communication layer. Next, the pair of IP and MAC addresses is sent to the Address Resolution process, which adds or updates an entry to the AR table. It is worth noting that the IP address field of the routing signaling message carries the destination of the route (either an IP or network address) while the IP address field within the IP header transports the destination IP address of the packet.

4. PERFORMANCE ANALYSIS

4.1 General proposed scenario

In brief, the scenario we propose includes moving nodes that are not always able to directly communicate with the infrastructure of the network, so the scenario requires multi-hop mechanisms to transport a message through different nodes until it reaches the devices collecting information in the road. Vehicles receive their network configuration from static devices in the road but, in order to initiate the communication among vehicles, address resolution has to be performed. Provided that this scenario is going to be tested with an anonymity service derived from Crowds, any improvement in the address resolution (AR) process, will feasibly enhance the overall performance of the communications in a VANET. This is because the implemented anonymity service requires AR transactions very often due to random behavior and higher number of hops performed by the service. Hence, in this work we evaluate if the performance of an anonymous reporting service over a VANET can be improved when it uses more suitable AR schemes. Specifically, we test this service with CAAR, but also with ARP+, a modified configuration of ARP devised for wireless environments.

4.2 Simulation Settings

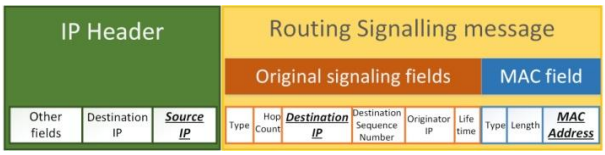


Figure 1. An IP Packet carrying a VANET Routing signaling message

The simulation scenario (see Figure 2) we use in this work is basically the same used by Urquiza et al (2014). The main difference is that now we incorporate an anonymity service (derived from Crowds) in order to evaluate the performance of the vehicular network when using modified versions of address resolution (i.e., ARP+, CAAR) to support this privacy service. The overall proposal is evaluated for both of the aforementioned routing protocols: AODV and GBSR. The realistic VANET scenario was simulated using Estinet (Estinet, 2015) and its mobility generator C4R (Fogue, 2012) which implements the Kraus mobility model. Since obstacles in the form of buildings significantly modify the behavior of the vehicular network, this information was exported from Open Street Maps (Open Street Maps, 2014) to be part of the Estinet scenario. Moreover, three different values of density of vehicles were used to evaluate the impact of the number of nodes on the performance of the network. 1000-byte packets were randomly introduced in the network during 300 seconds and in concordance with the IEEE 802.11p standard to add wireless access in vehicular environments. A summary of the main characteristics can be found in Table 1.

4.3 Simulation results

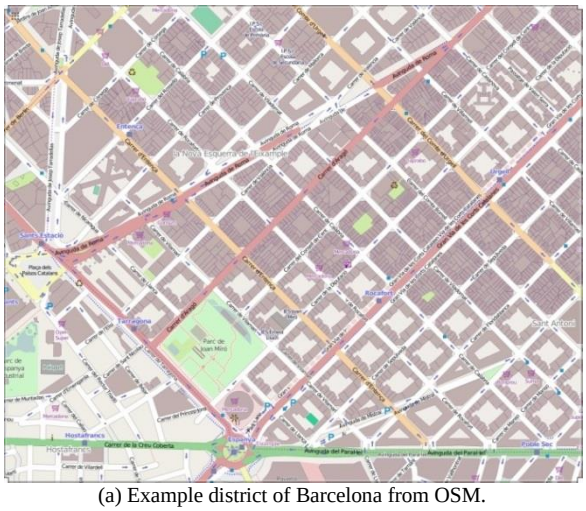
After testing the scenario we described before, we evaluate here the performance of the anonymous reporting service (inspired in Crowds) deployed over a realistic VANET where the link layer address resolution process is accomplished through routing messages (with the aim of efficiency). This performance is measured and shown in the following tables and figures in terms of packet losses, delay, and amount of hops, neighbors, and signaling.

In order to assess the proposed address resolution mechanism, we performed a statistical test (J-T, see Jonckheere (1954)) and tried to find a bias among different address resolution approaches (the alternative hypothesis). If there is such bias, the STS (Standardized Test Statistical) provides a measure of how strong the correlation is among the results obtained and the AR mechanisms evaluated. If this first test does not yield evidence of a trend, another statistical

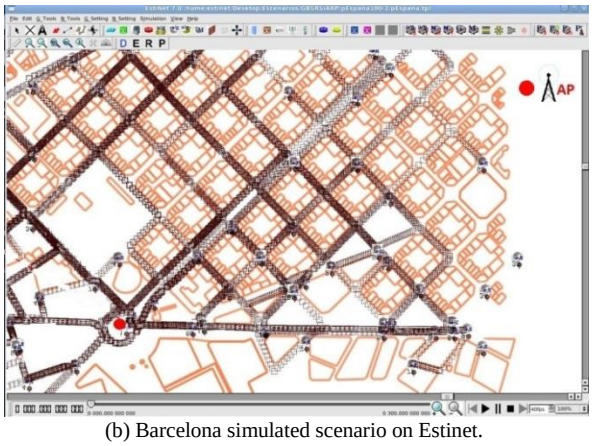
evaluation was done (K-W, Kruskal-Wallis one-way analysis of variance). The results of these statistical tests are depicted in Tables 2 and 3. The address resolution schemes (where the anonymity service is deployed) are pairwise compared, in terms of their performance parameters, in Table 4 when K-W or J-T test show a statistical difference.

Table 1. Simulation settings

Parameter	Value
Number of nodes	100 vehicles
Map zone & Area	Eixample district of Barcelona, 1,5 km x 1 km
Path loss model	Empirical IEEE 802.11p radio shadowing
Fading model	Rician (LOS) and Rayleigh (not in LOS)
Power transmission	23 dbm
Receiving sensing	-82 dbm (400 m in LOS)
Mobility generator	SUMO / C4R
Mobility model	Krauss
Max speed	60 km/h
MAC specification	IEEE 802.11p
QoS access category	BE (Best Effort)
Bandwidth	6 Mbps
Simulation time	300 sec
Maximum packet size	1.000 bytes
Traffic profile	Uniform distributed from 1,3 to 4 Kbps
Routing protocol	AODV, GBSR
GPS precision	10 m



(a) Example district of Barcelona from OSM.



(b) Barcelona simulated scenario on Estinet.

Figure 2. Simulation scenario. Eixample district of Barcelona with an Access Point (AP). Building from OpenStreetMap are included.

As one might expect, the random forwarding strategy of the Crowds-like mechanism (CAAR) increases the number of hops needed for the communication whe compared with the traditional unicast traffic (Figure 5c). When this anonymity service is deployed, it requires more address resolution queries than the ones required by traditional unicast traffic since the paths followed are not direct. For the tests, we used probabilities of random forwarding of 0,25 and 0,5 for the anonymity mechanism (i.e. two set of simulations where 25 % and 50 % of the packets were randomly sent from the source, respectively).

A higher probability of random forwarding produces an increase in the anonymity level of the communication. However, this randomness may provoke more losses since the routes tend to be longer increasing the probability of packet collisions or errors. In this context, we evaluated if the address resolution process is able to cause any impact in the level of anonymity and loss.

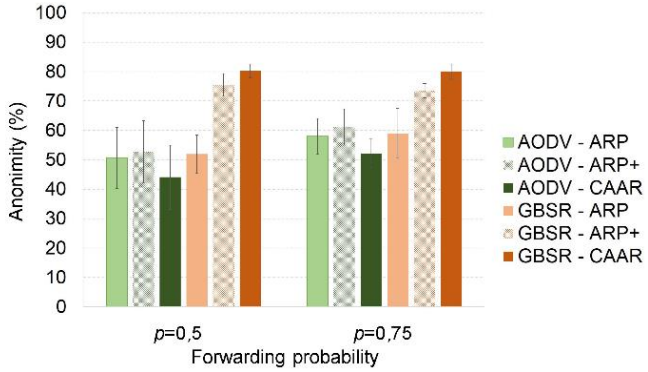
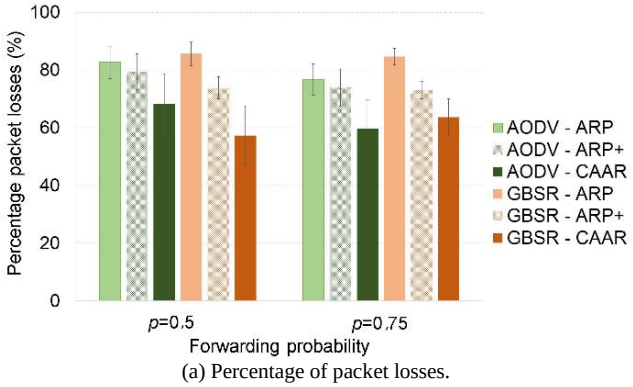


Figure 3. Anonymity level provided by our Crowds-like anonymity service using the three Address Resolution schemes (CI 95 %).

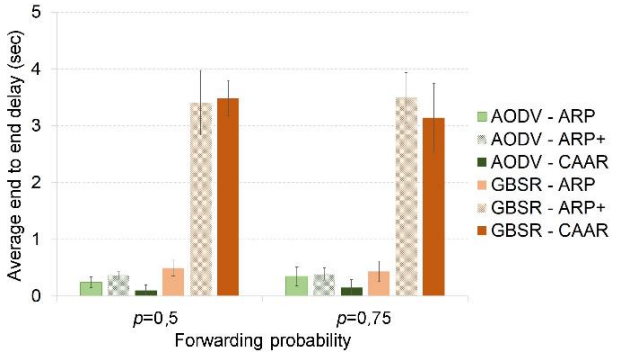
In Figure 3 we illustrate the anonymity level reached when the Crowd-like anonymity service is deployed over the different routing protocols and address resolution mechanisms. It can be appreciated that this anonymity level (percentage of packets whose original source could not be detected by the access point) for AODV did not vary significantly (compared to the original version of Crowds) when the probability of random forwarding was 0,5. Indeed, according to Table 2 (fifth column) there is no statistical difference in the anonymity level of the address resolution schemes when the probability of random forwarding is 0,5. Figure 3 shows, however, a slightly decrease of the anonymity level when AODV protocol and CAAR are used. When the probability of random forwarding is 0,75, the significance values go under 0,05; which means that there is a variation in the anonymity level obtained for AODV when the different address resolution mechanisms are employed.

However, a closer look into Table 4 shows that the proposal AODV CAAR maintains the same anonymity level than AODV-ARP (since the significance value is lower than 0,5). In contrast, as seen in Figure 3, GBSR tends to improve the anonymity level with respect to the address resolution scheme used (it can also be checked in fifth row of Table 3), being CAAR the most suitable mechanism for anonymity purposes.

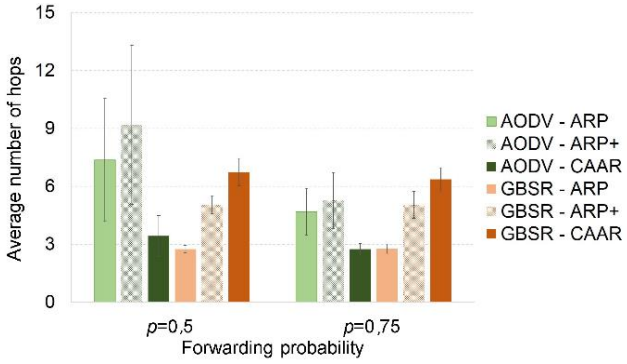
The percentage of packet losses decreases with the address resolution order (i.e., ARP, ARP+ and CAAR) for each routing protocol and for both forwarding probabilities, as depicted in Figure 4a. The reason is that ARP+ requires less



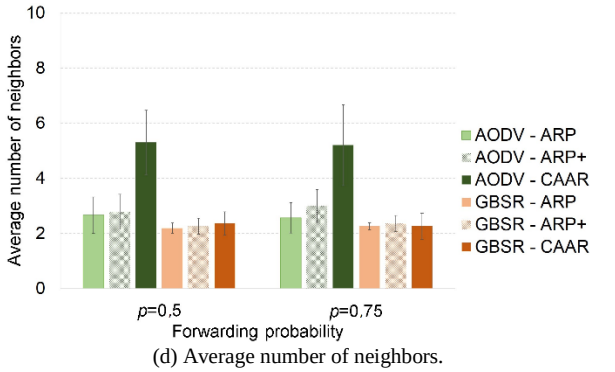
(a) Percentage of packet losses.



(b) Average end-to-end delay.



(c) Average number of hops



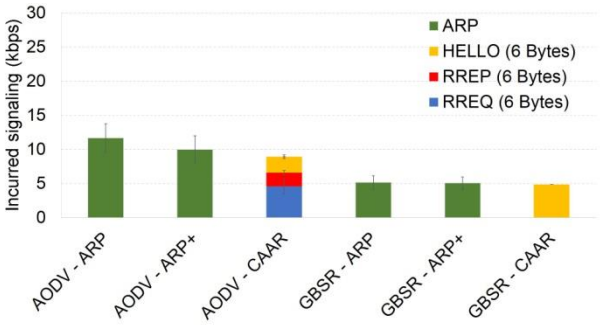
(d) Average number of neighbors.

Figure 4. Evaluation of our Crowds-like anonymity service using the three Address Resolution schemes. (CI 95 %).

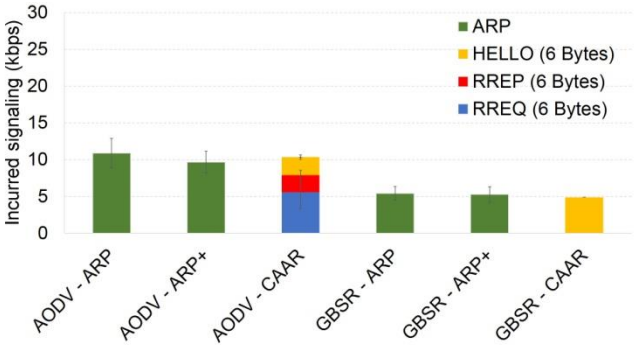
AR transactions than ARP and that CAAR inhibits them, thus alleviating collisions (negative STS values in Tables 2 and 3 reflects a decrease in losses as the address resolution mechanism varies) and this is very important given that our Crowds-like anonymity service will require to perform an address resolution for almost each random hop.

The high demand of AR transactions produces more collisions and especially for AODV the creation of path complicates a lot, as consequence packets will be dropped because no route was found. Regarding the delay (Figure 4b) and the average number of hops (Figure 4c), which are related to each other, note that AODV-CAAR (third column in Figure 4c) produces shorter routes than AODV-ARP or AODV-ARP+ routes (according to third and first and second columns of Figure 4c) for both probabilities.

Consequently, AODV-CAAR offers a shorter delay. GBSR paths, however, suffers longer delays than AODV paths, since GBSR forwarding decision mechanism uses the buffer to save packets from being discarded.



(a) p=0,5



(b) p=0,75

Figure 5. Signaling traffic incurred only by the AR process in our Crowds-like anonymity service scenario using the three Address Resolution schemes (CI 95 %). AR signaling in ARP and ARP+ involves all ARP REQ/REP messages. AR signaling in CAAR only consists of 6 bytes added to each routing message (RREQ, RREP and HELLO in AODV and HELLO in GBSR) to carry the MAC address.

Another parameter we measured in our scenario is the average number of neighbors (see Figure 4d). When using a Crowd-like anonymity service, it is reasonable to expect a reduction in the number of neighbors in a VANET since the extra traffic generated by the random forwarding strategy may cause collisions (which could obscure some neighbors).

In contrast, CAAR helps to reduce these collisions and, consequently, when combined with AODV and the anonymity service, the average number of neighbors is similar to the ones existing when the Crowd-like mechanism is not implemented. In the case of GBSR, the number of neighbors is considerably reduced due to the collisions and losses provoked by the random forwarding strategy.

Finally, Figure 5a and Figure 5b illustrate that no extra traffic is inserted by our AR proposal CAAR (due to address resolution signaling), despite the deployment of the anonymity mechanism, with any of the values of random forwarding probabilities (0,5 and 0,75) as it can be checked in the last row of 2 and 3. In fact, CAAR significantly reduces the signaling traffic associated to the address resolution process for the forwarding probability of 0,5.

This statement can be confirmed in Table 4 when single AODV is compared to AODV-CAAR (fifth row), where the significance level is lower than 0,05, which evidences that both AODV-ARP and AODV-CAAR actually behave differently, provided that signaling traffic is reduced with CAAR (Figure 5a).

Table 2. Hypothesis Test Summary of AODV with anonymity service Crowds-like.

			p = 0,5			p = 0,75	
Parameter Hypothesis	**Test** 50/75	**STS**	**Significance**	**Decision**	**STS**	**Significance**	**Decision**
Packet Losses	J-T/J-T	-2,395	0,017	**Reject**	-2,928	0	**Reject**
End-to-end delay	K-W/K-W		0	**Reject**		0,01	**Reject**
Number of hops	K-W/J-T		0,026	**Reject**	-3,004	0	**Reject**
Neighbors	J-T/J-T	4,118	0	**Reject**	4,343	0	**Reject**
Anonymity level	K-W/K-W		0,165	Retain		0,03	**Reject**
AR Signaling	J-T/K-W	-2,319	0,02	**Reject**		0,5	Retain

J-T = Jonckheere-Terpstra tend test. K-W = Kruskal-Wallis test. STS = Standardized Test Statistic. We performed J-T test for all the performance metrics. When the J-T test retains the null hypothesis, we performed K-W to look for any difference. Null hypothesis: The distribution of the parameter's result is the same across ARP, ARP+ and CAAR. J-T Alternative hypothesis: The distribution of the result follows an order across ARP, ARP+ and CAAR. K-W Alternative hypothesis: There is at least one scheme for which its distribution is different from the other schemes. In all the tests, we rejected the null hypothesis when the significance value is lower than the significance level of 0,05.

Table 3. Hypothesis Test Summary of GBSR with anonymity service Crowds-like.

			p = 0,5			p = 0,75	
Parameter Hypothesis	**Test** 50/75	**STS**	**Significance**	**Decision**	**STS**	**Significance**	**Decision**
Packet Losses	J-T/J-T	5,475	0	**Reject**	-5,095	0	**Reject**
End-to-end delay	J-T/J-T	4,183	0	**Reject**	3,156	0	**Reject**
Number of hops	J-T/J-T	5,513	0	**Reject**	5,209	0	**Reject**
Neighbors	K-W/K-W		0,78	Retain		0,72	Retain
Anonymity level	J-T/J-T	-5,475	0	**Reject**	-5,209	0	**Reject**
AR Signaling	K-W/K-W		0,655	Retain		0,66	Retain

J-T = Jonckheere-Terpstra tend test. K-W = Kruskal-Wallis test. STS = Standardized Test Statistic. We performed J-T test for all the performance metrics. When the J-T test retains the null hypothesis, we performed K-W to look for any difference. Null hypothesis: The distribution of the parameter's result is the same across ARP, ARP+ and CAAR. J-T Alternative hypothesis: The distribution of the result follows an order across ARP, ARP+ and CAAR. K-W Alternative hypothesis: There is at least one scheme for which its distribution is different from the other schemes. In all the tests, we rejected the null hypothesis when the significance value is lower than the significance level of 0,05.

Table 4. Pairwise comparison of performance metrics for anonymity service Crowds-like.

				Adjusted Significance (AS)		
# row	**Probability**	**Protocol**	**Parameter**	**CAAR-ARP**	**CAAR-ARP+**	**ARP-ARP+**
1	50	AODV	Losses	**0,029**	0,144	0,675
2	50	AODV	Delay Hops	0,161	**0**	0,134
3	50	AODV	Neigbors	0.134	**0,031**	1
4	50	AODV	Signaling	**0**	**0**	0,814
5	50	AODV	Losses Delay	**0,019**	0,547	0,34
6	75	AODV	Hops	**0,004**	**0,023**	1
7	75	AODV	Neighbors	0,105	**0,006**	1
8	75	AODV	Anonymity	**0,002**	**0**	1
9	75	AODV	Losses Delay	**0,001**	**0,002**	0,073
10	75	AODV	Hops	0,202	**0,029**	1
11	50	GBSR	Anonymity	**0**	**0**	**0,001**
12	50	GBSR	Losses Delay	**0**	0,675	**0**
13	50	GBSR	Hops	**0**	**0,001**	**0**
14	50	GBSR	Anonymity	**0**	**0,001**	**0**
15	75	GBSR		**0**	**0,012**	**0**
16	75	GBSR		**0**	1	**0**
17	75	GBSR		**0**	**0,008**	**0**
18	75	GBSR		**0**	**0,008**	**0**

The comparisons were performed using the Mann-Whitney test. Null hypothesis: The results of the two AR schemes come from the same distribution. Alternative hypothesis: The distributions of results of the two AR schemes are different. In all the tests, we rejected the null hypothesis when the adjusted significance value is lower than the significance level of 0,05.

5. CONCLUSIONS

Provided the additional paths that have to be created to hide a vehicle in the crowd, the anonymity service incorporated to a realistic VANET scenario is very demanding. Additionally, greater delay and less neighbor relationships are negative consequences of the random forwarding mechanism employed by this Crowd-like mechanism. However, the delay does not increase significantly when the randomness of the forwarding probability gets higher.

Moreover, CAAR in general provokes less packet losses than ARP, which contributes to counter the demanding environment of the Crowds anonymity service. In any case, GBSR causes higher delay, no matter the parameters (e.g. forwarding probability) used in for the anonymity service. Finally, it is worth noting that CAAR shows high performance when a demanding service (like anonymous reporting) is tested. It is evident that CAAR significantly reduces the amount of signaling for both routing protocols and for both forwarding probabilities used in the Crowds-like service. Future work includes the study of more easy-to-implement modifications to the communication protocol stack in order to offer mechanisms more suitable for dynamic wireless environments such as VANETs.

ACKNOWLEDGMENT

We would like to thank Professor Antoni Miñarro (UB) for a good number of helpful comments in the use of statistical tests.

REFERENCES

Carter, C., Yi, S., & Kravets, R. (2003, March). ARP considered harmful: Manycast transactions in ad hoc networks. *Wireless Communications and Networking, 2003. WCNC 2003*. 2003 IEEE (Vol. 3, pp. 1801-1806). IEEE. http://dx.doi.org/10.1109/WCNC.2003.1200660

Chaum, D. (1988). The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology*, 1(1), 65-75. http://dx.doi.org/10.1007/BF00206326

Dötzer, F. (2005, May). Privacy issues in vehicular ad hoc networks. *Privacy Enhancing Technologies* (pp. 197-209). Springer Berlin Heidelberg. http://dx.doi.org/10.1007/11767831_13

Estinet. (2016). EstiNet Technologies. Retrieved 1 June 2015, from http://www.estinet.com/products.php

Estrada, J. A., & Rodríguez, A. (2014). Evaluación de Protección de Privacidad de una Herramienta de Navegador Web. *Revista Politécnica*, 33(1).

Fogue, M., Garrido, P., Martinez, F. J., Cano, J. C., Calafate, C. T., & Manzoni, P. (2012, March). A realistic simulation framework for vehicular networks. *Proceedings of the 5th International ICST Conference on Simulation Tools and Techniques* (pp. 37-46). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering). http://dx.doi.org/10.4108/icst.simutools.2012.247682

Haklay, M., & Weber, P. (2008). Openstreetmap: User-generated street maps. *Pervasive Computing, IEEE*, 7(4), 12-18.

Hartenstein, H. (2010). VANET: vehicular applications and inter-networking technologies (Vol. 1). *Chichester*, UK: Wiley. http://dx.doi.org/10.1002/9780470740637

Jonckheere, A. R. (1954). A distribution-free k-sample test against ordered alternatives. *Biometrika*, 41(1/2), 133-145. http://dx.doi.org/doi:10.1093/biomet/41.1-2.133

Karp, B., & Kung, H. T. (2000, August). GPSR: Greedy perimeter stateless routing for wireless networks. *Proceedings of the 6th annual international conference on Mobile computing and networking* (pp. 243-254). ACM. http://dx.doi.org/10.1145/345910.345953

Perkins, C., Belding-Royer, E. M., & Das, S. (2003). Request for Comments: 3561. Category: Experimental, Network, Working Group.

Plummer, D. C. (1982). RFC 826-ARP Protocol.

Reed, M. G., Syverson, P. F., & Goldschlag, D. M. (1998). Anonymous connections and onion routing. *Selected Areas in Communications, IEEE Journal on*, 16(4), 482-494. http://dx.doi.org/10.1109/49.668972

Reiter, M. K., & Rubin, A. D. (1998). Crowds: Anonymity for web transactions. *ACM Transactions on Information and System Security* (TISSEC), 1(1), 66-92. http://dx.doi.org/10.1145/290163.290168

Scarlata, V., Levine, B. N., & Shields, C. (2001, November). Responder anonymity and anonymous peer-to-peer file sharing. *Network Protocols, 2001*. Ninth International Conference on (pp. 272-280). IEEE. http://dx.doi.org/10.1109/ICNP.2001.992907

Tripp Barba, C., Urquiza Aguiar, L., & Aguilar Igartua, M. (2013). Design and evaluation of GBSR-B, an improvement of GPSR for VANETs. *Latin America Transactions, IEEE*, 11(4), 1083-1089. http://dx.doi.org/10.1109/TLA.2013.6601753

Tripp Barba, C., Urquiza Aguiar, L., Igartua, M. A., Parra-Arnau, J., Rebollo-Monedero, D., Forné, J., & Pallarès, E. (2013). A collaborative protocol for anonymous reporting in vehicular ad hoc networks. *Computer Standards & Interfaces*, 36(1), 188-197. http://dx.doi.org/10.1016/j.csi.2013.06.001

Urquiza Aguiar, L., Tripp Barba, C., Rebollo Monedero, D., Mezher, A., Aguilar Igartua, M., & Forné Muñoz, J. (2015). Coherent and automatic address resolution for vehicular ad hoc networks. *International journal of Ad Hoc and ubiquitous computing*. http://dx.doi.org/10.3390/s150409039