On the Use of a Cooperative Neighbor Position Verification Scheme to Secure Warning Message Dissemination in VANETs

Manuel Fogue*, Francisco J. Martinez*, Piedad Garrido*, Marco Fiore†,
Carla-Fabiana Chiasserini‡, Claudio Casetti‡, Juan-Carlos Cano§, Carlos T. Calafate§, Pietro Manzoni§

*University of Zaragoza, Spain. E-mail: {mfogue, f.martinez, piedad}@unizar.es
†IEIIT-CNR, Italy and INRIA, France. E-mail: marco.fiore@ieiit.cnr.it
‡Politecnico di Torino, Italy. E-mail: {chiasserini, casetti}@polito.it
§Universitat Politècnica de València, Spain. E-mail: {jucano, calafate, pmanzoni}@disca.upv.es

***Abstract*—Efficient schemes for warning message dissemination in vehicular ad hoc networks (VANETs) use context information collected by vehicles about their neighbor nodes to guide the dissemination process. Based on this information, vehicles autonomously decide whether or not they are the most appropriate forwarding nodes. These schemes maximize their performance when all the vehicles advertise correct information about their positions. Position errors introduced by nodes attacking the system, and other common errors due to malfunction of the localization systems, may drastically reduce the performance of the dissemination process. We present a proactive Cooperative Neighbor Position and Verification (CNPV) protocol that detects nodes advertising false locations and selects optimal forwarders so as to mitigate the impact of adversarial users. We combine our mechanism with two warning dissemination schemes for VANETs, and demonstrate how these algorithms can benefit from the use of our security scheme in the presence of malicious nodes trying to exploit the inherent vulnerabilities of each algorithm.**

***Index Terms*—Neighbor Position Verification, Vehicular Ad Hoc Networks, Warning Message Dissemination, Security.**

I. Introduction

Vehicular ad hoc networks (VANETs) are wireless networks that do not require any fixed infrastructure and are considered essential for cooperative applications among cars on the road. VANETs are usually classified as a subset of Mobile ad hoc networks (MANETs), but they present some distinctive characteristics such as (a) road-constrained high-speed mobility leading to rapidly variable network topologies, (b) challenging RF signal propagation conditions, (c) no significant power constraints, and (d) very large networks scale involving up to hundreds of vehicles.

VANETs have many possible applications, ranging from road safety through cooperative awareness to real-time distributed traffic management via dissemination of information on traffic congestion and road status. In this work we focus on traffic safety and efficient warning message dissemination, where the most critical goal is to reduce the latency while ensuring the accuracy of the information when a dangerous situation occurs. There, any vehicle detecting an abnormal situation (i.e. accident, slippery road, etc.) is deemed to notify the anomaly to nearby vehicles that could face the same problem later on. This is achieved through multi-hop forwarding, being location information about neighboring vehicles the key to decide whether to rebroadcast an incoming warning message or not. Therefore, context information on car positioning is paramount to the correct operation of the system. However, most warning message dissemination schemes assume that all the information shared between vehicles is accurate, thus location errors due to positioning malfunction or attacks can seriously affect performance.

In this paper, we propose a Cooperative Neighbor Position and Verification (CNPV) protocol based on a proactive approach. Our scheme allows securing warning dissemination protocols in adversarial environments where advertised positions are not always accurate. We evaluate the effectiveness of CNPV on the performance of two of the most efficient – yet insecure – dissemination algorithms developed for VANETs. Our mechanism is fully distributed and, combined with dissemination algorithms that require position information from communication neighbors, it avoids that malicious vehicles announcing false positions are considered for the forwarding of critical information. As a result, CNPV improves the performance of the dissemination process in adversarial environments of up to 50% in terms of warning notification time and percentage of uninformed nodes.

The rest of the paper is organized as follows. Section II reviews the related work on neighbor positions localization and verification, as well as about using context information to improve warning message dissemination in VANETs. Section III presents our proactive neighbor position verification algorithm. Section IV details the simulation environment used for the performance evaluation, whose results are presented and discussed in Section V. Finally, Section VI concludes the paper.

II. Related Work

In this Section, we first review existing proposals for the localization and position verification of communication neighbors. We then show how current warning message dissemination schemes make use of context information to maximize their performance.

A. Neighbor Localization and Verification

The collection of neighbor locations in a wireless network is performed by using positioning systems and by verifying the announced positions. Regarding positioning, self-localization can be performed through Global Navigation Satellite Systems (GNSS) [1]. Own position information can then be announced to nearby vehicles using vehicle-to-vehicle Direct Short-Range Communication (DSRC). In addition, different existing methods can be combined to find out the neighbors within communication range. In our case study, we will rely on the Time of Flight (ToF) technique based on the difference between message transmission and reception times [2].

Once a node knows the positions of its neighbors, it must ensure that the advertised positions correspond to the true geographic coordinates, i.e., it must perform a location verification. In the existing literature, we can find several mechanisms for infrastructured or hybrid networks: these provide solutions to secure localization using fixed or mobile nodes connected securely to the certification authority [3], or through multilateration methods based on ranging and Time Difference of Arrival (TDoA) [4].

As far as ad hoc-oriented location verfication protocols are concerned, a secure position verification system for VANETs is presented in [2]. Although effective, the proposed solution requires a minimum fixed infrastructure, which does not meet our criteria for pure VANETs. In [5], the authors proposed a distributed neighbor position verification mechanism for wireless networks. This protocol is designed to be reactive, i.e., a node called *verifier* must start the process at a given time to discover and verify the position of its communication neighbors. However, a high number of messages are required by this reactive protocol, thereby imposing a high channel overhead. In addition, there can be an important delay between the beginning of the process and the verification of neighbor positions. Hence, using reactive approaches is not appropriate for networks where nodes need to be constantly aware of the position of their neighbors.

B. Warning Message Dissemination

Dissemination schemes are commonly used in VANETs for critical applications. Among the existing mechanisms to improve warning message dissemination in VANETs, two of the most recent and effective algorithms are the *enhanced Message Dissemination based on Roadmaps* (eMDR) [6] and the *Urban Vehicular broadCAST* (UV-CAST) [7]. These protocols make use of information about neighbor vehicle positions to decide whether to rebroadcast the message or not, and to determine if the vehicle is the most appropriate one to store the message for future forwarding.

In eMDR, vehicles decide whether to rebroadcast a received message depending on the position of the sender and of the receiver. If they are located in different streets, or the receiver vehicle is close to a junction giving access to new streets, the receiver vehicle is allowed to forward the message. In particular, only the vehicle closest to the geographic center of the junction, obtained from integrated GPS maps, is allowed to forward the message. This strategy aims at reducing the number of broadcasted messages.

The UV-CAST algorithm selects different mechanisms for message dissemination in VANETs. Vehicles in a well-connected regime rebroadcast incoming messages after a wait time if no redundant messages are received. Vehicles in a disconnected regime must decide if they are suitable for the Store-Carry-Forward (SCF) task, forwarding the message whenever they meet new neighbors. The SCF task is assigned to vehicles that have a small expected time before they see new neighbors, obtained as the boundary vehicles of the neighbors in communication range, i.e., located on the vertices of the boundary polygon.

Both eMDR and UV-CAST are designed to blindly trust the information provided by other vehicles. Vehicles may announce incorrect positions due to several factors: unintentional inaccuracies, e.g., GPS errors in poorly covered areas; however, malicious vehicles can also advertise an incorrect position to decrease the performance of a system, or to gain advantage among peers, for example by attracting traffic to a specific area. Hence, the information provided by other vehicles should be verified before being trusted and used as an input to dissemination algorithms. To this end, we design CNPV, a protocol that proactively determines which neighbors are advertising false information about their positions.

III. The CNPV protocol

We first introduce the communication environment we will consider in the rest of the paper, and then detail the CNPV protocol we propose.

A. System Model

We consider a vehicular ad hoc network where the communication neighbors of a vehicle are all the nodes that it can reach directly when transmitting. All the vehicles are synchronized to a common time reference, and we assume that each node is able to determine its own geographical position with a maximum error ϵ_p. Both criteria regarding timing and geographical position can be fulfilled by equipping vehicles with GPS receivers, a plausible assumption nowadays since this technology is experiencing a fast introduction in the automotive industry.

In addition, vehicles are capable of performing Time of Flight (ToF)-based Radio Frequency (RF) ranging with a maximum error equal to ϵ_r. Typically, the RF interfaces have a frequency of operation of 44MHz, obtaining an average error of $6.8m$ when transmitting the signal at the speed of light, $3 \cdot 10^8 m/s$. This technique is used to calculate distances between the sender and the receiver of a given message. As discussed in [8], this is a reasonable assumption, although it requires modifications to off-the-shelf radio interfaces. An

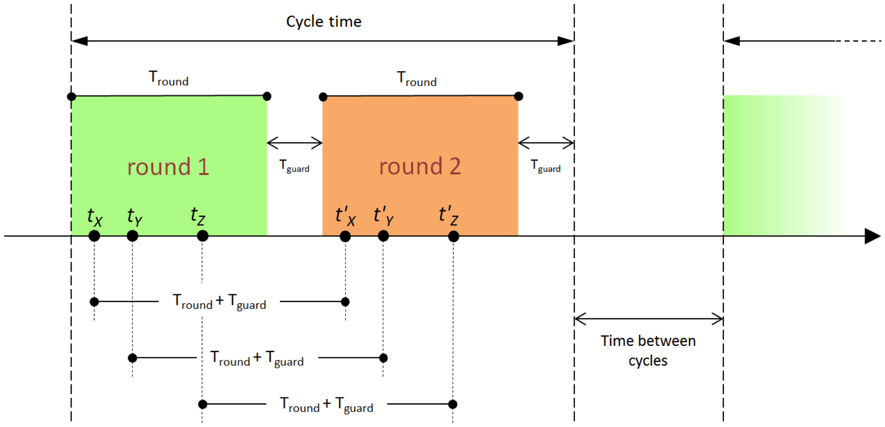


Fig. 1. Temporal detail of the proactive neighbor position verification algorithm.

example of a successful case of RF interface used for ranging can be found in [9].

Each vehicle X has a unique identifier, as well as a private key k_X and a public key K_X, to encrypt and decrypt data. Additionally, vehicles have a set of one-time use keys available $\{k'_X, K'_X\}$, and they can produce digital signatures $(SigX)$ with their private key. We assume that the correspondence between X and K_X can be validated by any node, as in state-of-the-art secure communication architectures [10].

Vehicles are *correct* if they comply with the verification protocol, or *adversarial* if they deviate from it. Adversaries can be considered either internal or external to the network, depending on whether they have a set of recognized cryptographic keys or not. External adversaries have fewer opportunities to thwart the system; in fact, they can only serve as relay nodes since messages with unrecognized signatures will be immediately rejected by the rest of nodes. Hence, we only consider the more challenging case of internal network adversaries.

B. CNPV Protocol Objectives

The CNPV protocol is proactive, as each node participating in the system periodically sends its location and the information necessary to the protocol operation. Hence, our approach is proactive in the sense that node messages are not the result of explicit queries.

The proposed protocol is designed to attain two main objectives in a mobile environment: (i) acquiring the positions of the neighbors, and (ii) verifying the correctness of these positions. The system is designed so as to allow each node to decide whether the positions advertised by its neighbors are accurate or not. Thus, a node assigns one of three possible states to each of its neighboring nodes:

- Correct (*verified*): the advertised position corresponds to the true geographic position of the neighbor;
- Incorrect (*faulty*): the advertised position does not correspond to the true position of the neighbor, tagged as an attacker;
- Unverifiable: the information collected so far is not enough to determine the correctness of the advertised position.

The CNPV protocol is based on a cooperative approach that takes advantage of the broadcast nature of the wireless medium, and allows each node to verify the positions of its communication neighbors through the messages it receives. We remark that the position validation is run by each node independently, and that CNPV does not require any exchange of the resulting neighbor states among nodes. Thus, the protocol does not require nodes to have a global knowledge of the network, nor to find a global consensus on the verification of claimed positions.

C. CNPV Protocol Message Exchange

We will use the following notation to describe the neighbor position verification process:

- t_X: transmission time of the message for node X.
- t_{XY}: reception time of the message sent by X and received by Y.
- $\mathbb{N}_X$: set of neighbors of node X.
- p_X: position of node X.

As show in Figure 1, the proactive verification process uses a message exchange mechanism that takes place in two rounds with the same duration:

- ***Round 1***: In the first round, each node X participating in the protocol chooses a random time t_X in the interval corresponding to the first round (at the application layer). Once this time is reached, the node sends its HELLO message at time t_X over the transmission channel. This message is initially anonymous because it is signed by a one-time use key. The message is received by all the neighbors at a specific time for each node, named t_{XY} for node Y.
- ***Round 2***: Once all HELLO messages are sent, nodes execute the second round of the protocol. Each node X sends a new message at time t'_X corresponding to the duration of the first round plus a constant time, called

guard time. Therefore, all the nodes will transmit their messages in the same order in the second round. The HELLO message sent in the second round contains the identity of the sender, as well as the information needed to make the correspondence with the first message, sent anonymously during the first round.

Algorithm 1: Message exchange routine

```
node $X$ do
    if round == 1 then
        $X : t_X$ = random $\in \left[t_{Round1Begin}, t_{Round1End}\right]$
    else if round == 2 then
        $X : t_X = t_X + T_{round} + T_{guard}$
    when $t_x$ do
        if round == 1 then
            forall node $i \in \mathbb{N}_X \left\{\left(K'_i, t_{iX}\right)\right\}$ do
                $X : time\_info = \left\{\left(K'_i, t_{iX}\right)\right\}$
                $X \rightarrow * : \langle HELLO, K'_X, \left\{\left(K'_i, t_{iX}\right)\right\}\rangle$
        else if round == 2 then
            forall node $i \in \mathbb{N}_X \left\{\left(K'_i, t_{iX}\right)\right\}$ do
                $X \rightarrow * : \langle HELLO, ID_X, p_X, t_X, K'_X,$
                $\left\{\left(K'_i, t_{iX}\right)\right\}, K_X, Sig_X\rangle$
```

After the message exchange routine is complete, each node can create the correspondences between the messages sent in the first round and the announced neighbors. Moreover, each nodes retrieves from the second-round messages the transmission times of the first-round HELLO message for each of its neighbors. Such information, together with the locally stored reception times of first-round messages, allows each node to use ToF-based RF ranging to calculate the distance that separates them from their neighbors.

For example, let us consider the case of a node S receiving a message from X. S retrieves t_X, the transmission time of the message sent by X, from the second-round message by X; moreover, S has locally stored t_{XS}, i.e., the time at which it received the same message. Using this information S can determine the distance that separates it from X.

D. CNPV Protocol Verification Algorithm

Once the message exchange is finished, it is time for the participating nodes to verify the positions advertised by their neighbors. To this end, three tests are subsequently carried out by each of the nodes, allowing them to determine if the positions advertised are accurate or not. A more detailed description of such tests is available in [5].

Three tests are performed for position verification: the *Direct Symmetry* test, the *Cross-Symmetry* test, and the *Multilateration* test. After running the three tests for each communication neighbor, each vehicle is able to determine if the interchanged information is trustworthy, hence the neighbor may be considered as a potential forwarding node; or it may be considered malicious, in which case, the neighbor is considered as faulty and not suitable to rebroadcast the message. Next, we present the three different tests.

1) Direct Symmetry (DS) Test: During this test, the verifier node compares its own information with the information collected from each of its neighbors. This test does not use the cooperative approach of the protocol. During this test, two subtests are performed: (i) a coherence test, where the distance calculated using the time of flight of radio signal must be coherent with the position announced by the neighbor, and (ii) a signal range test, where the calculated distance must be less than the maximum range of the Radio Frequency (RF) communication system.

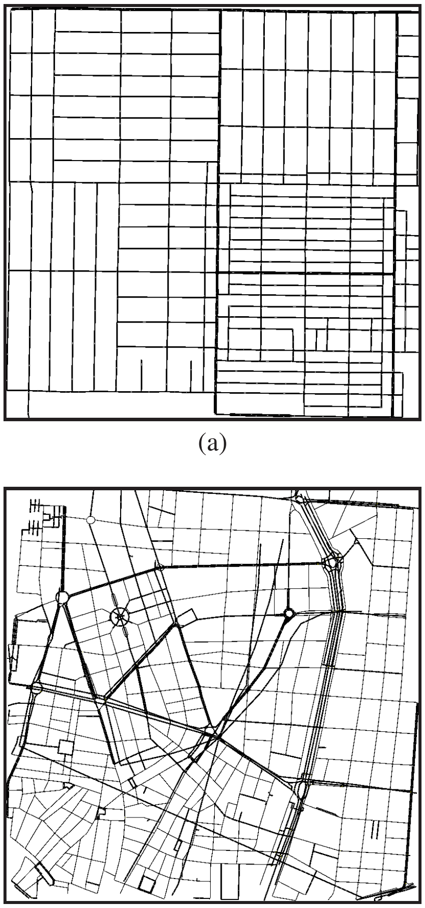
2) Cross-Symmetry (CS) Test: Unlike the DS test, the Cross-Symmetry test exploits the collaborative behavior of our approach by performing cross checks. The purpose is to verify the collected information from the neighbors which are mutually interconnected. The CS test ignores the nodes already considered incorrect by the DS test, and compares pairs of nodes such that the two nodes and the verifier node are within communication range. When nodes meet these conditions, they are tested using the same criteria as in the DS test. The algorithm works by counting the number of links considered correct and the number of links considered incorrect. The ratio of invalid links with respect to the total number of links for a given node allows determining if its advertised position is trustworthy. With a ratio limit δ set as 50%, the majority value is considered. A smaller ratio limit will provide greater security, but it limits the number of links correctly verified.

3) Multilateration (ML) Test: The last of the three proposed tests is applied to previously verified nodes. We want to detect suspicious situations where nodes have deliberately ignored to announce the links they have with other nodes by counting the number of neighbors who reported a link not announced by the suspicious node. If there are at least two, then we can compute – for each pair of nodes including a verifier S and a neighbor Y – a curve in which node X is present. If we can calculate two or more curves, node X is located at the intersection of these curves, that, due to their geometrical construction, are hyperboles. GPS and ToF-based RF ranging error may lead to curves that do not perfectly intersect in one point. Thus, the centroid of such (closely located) intersections is determined and then compared to the distance advertised by the suspicious node. If the error threshold is exceeded, the node is considered invalid. In our simulations, the error threshold is set to 10 meters.

IV. Simulation Environment

We evaluate the impact of the CNPV protocol on eMDR and UV-CAST, two state-of-the-art warning message dissemination algorithms.

Since deploying and testing VANETs is unpractical due to high economic costs and system complexity, we resort to simulation as a viable alternative to actual implementation. We selected two different road layouts to test our proposal. Figure 2(a) shows the area between Martin Luther King Blvd. and West Slauson Av. in the city of Los Angeles (CA, USA), which has a very regular street layout similar to synthetic Manhattan-grid layouts. The street map around Paseo de la


(a)

(b)

Fig. 2. Scenarios used in our simulations as street graphs in SUMO: (a) section of the city of Los Angeles (USA), and (b) section of the city of Madrid (Spain).

Castellana in the city of Madrid (Spain), shown in Figure 2(b), is an example of European city with a more irregular layout. The scenarios were obtained from OpenStreetMap [11], each one representing a 4-km^2 square area.

Vehicular mobility is generated with the CityMob for Roadmaps (C4R) tool[1], which can import maps from OpenStreetMap and is based on SUMO [12], a realistic open-source traffic simulation package. The microscopic mobility is modeled through the Krauss mobility model with some modifications to allow multi-lane behavior [13]. From a macroscopic viewpoint, our mobility simulations account for areas with different vehicle densities, ranging from 12.5 to 100 vehicles/km^2. Since in a realistic urban environment the traffic is not uniformly distributed, being driven by points of interest that attract vehicles, we adopt the Downtown Model [14] to determine such points of attraction in the roadmaps and to derive the macroscopic traffic flows.

Simulations were carried out using the ns-2 simulator [15], modified to include the IEEE 802.11p [16] standard so as to closely follow the upcoming WAVE standard. In terms of the physical layer, the data rate used for packet broadcasting is of 6 Mbit/s, as this is the maximum rate for broadcasting in 802.11p. At the MAC layer, channel access priorities were implemented: four different Access Categories (ACs) provide different priority to application messages, where AC0 has the lowest and AC3 the highest priority. The simulator was also modified to make use of our Real Attenuation and Visibility (RAV) propagation model [17], which increases the level of realism of the VANET simulations by accounting for real urban roadmaps and obstacles that have a strong influence over the wireless signal propagation.

In each scenario, three *warning-mode* vehicles generate warning messages at a rate of 1 message/second, while the rest of *normal-mode* vehicles act as relaying nodes for these messages. The vehicles in the simulation also broadcast one-hop HELLO messages at a rate of 1 message/second in order to implement the neighbor position verification algorithm.

We evaluate the following performance metrics of interest: the warning notification time, i.e., the time required by normal vehicles to receive a warning message sent by a warning-mode vehicle, and the percentage of blind vehicles, i.e., the percentage of normal-mode vehicles that do not receive a warning message. We are also interested in assessing the overhead that CNPV induces in the network. All results represent the average of multiple executions with different random seeds, and fall within a 95% confidence interval.

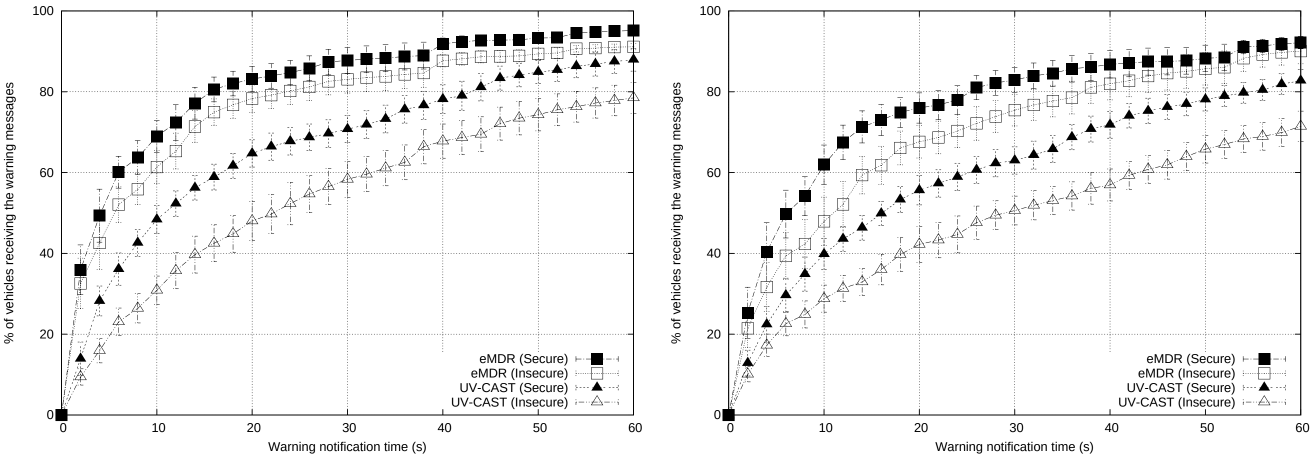
A. Adversary model

Simulations account for different percentages of adversarial vehicles, namely 3%, 6%, and 9% of the total number of vehicles. Attackers aim at reducing the performance of the warning message dissemination process, by attracting the road safety data traffic but not forwarding the warning messages received. To that end, they announce false positions so as to exploit the vulnerabilities of the eMDR and UV-CAST algorithms, as detailed next.

In the case of the eMDR algorithm, vehicles closer to roadmap junctions have an advantage over their neighbors since they have the highest chances of reaching new areas of the topology. Hence, a simple attack that would reduce the performance of warning message dissemination using this algorithm consists in announcing bogus positions very close to the junction coordinates. Detecting a neighbor in a more appropriate location, all other vehicles will refrain from forwarding the message. Some time later, another node might forward the message even though it is in a less favorable position, since the integrity of the system has been compromised.

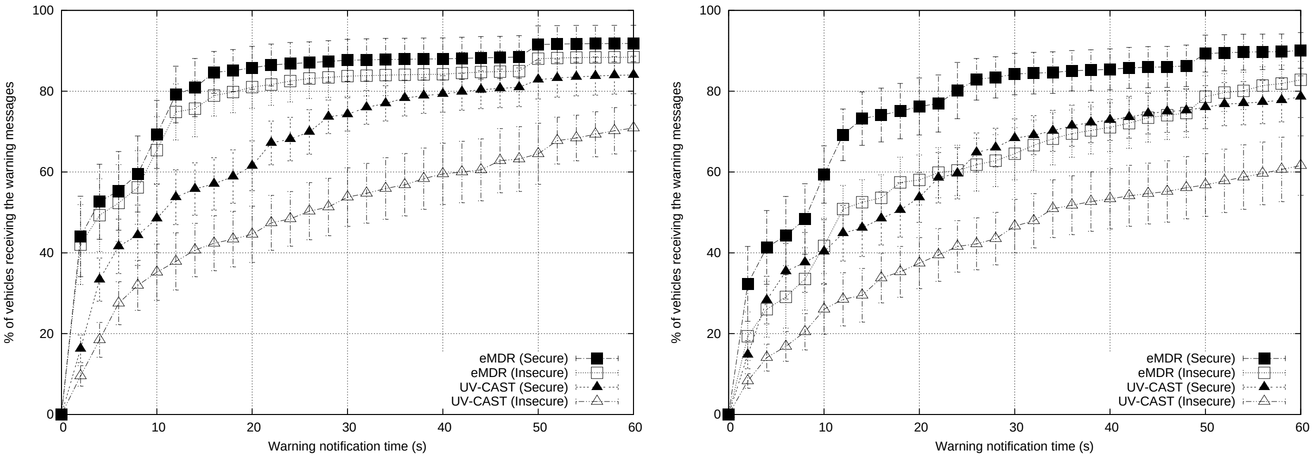
Regarding the UV-CAST protocol, the Store-Carry-Forward task is performed by boundary vehicles, and a vehicle which is not located in the vertices of the boundary polygon will not be assigned this task. Hence, vehicles advertising false positions relatively far from their actual position will obtain advantage over their neighbors, since they will be located with higher probability in the boundary area. Fewer neighbors will be assigned the data carrying task, reducing the chances that the warning message reaches new areas of the urban scenario.

[1] C4R is freely available at http://www.grc.upv.es/software/



(a) (b)

Fig. 3. Warning notification time in Madrid with 200 vehicles varying the percentage of adversaries: (a) 3%, and (b) 9%.



(a) (b)

Fig. 4. Warning notification time in Madrid with 400 vehicles varying the percentage of adversaries: (a) 3%, and (b) 9%.

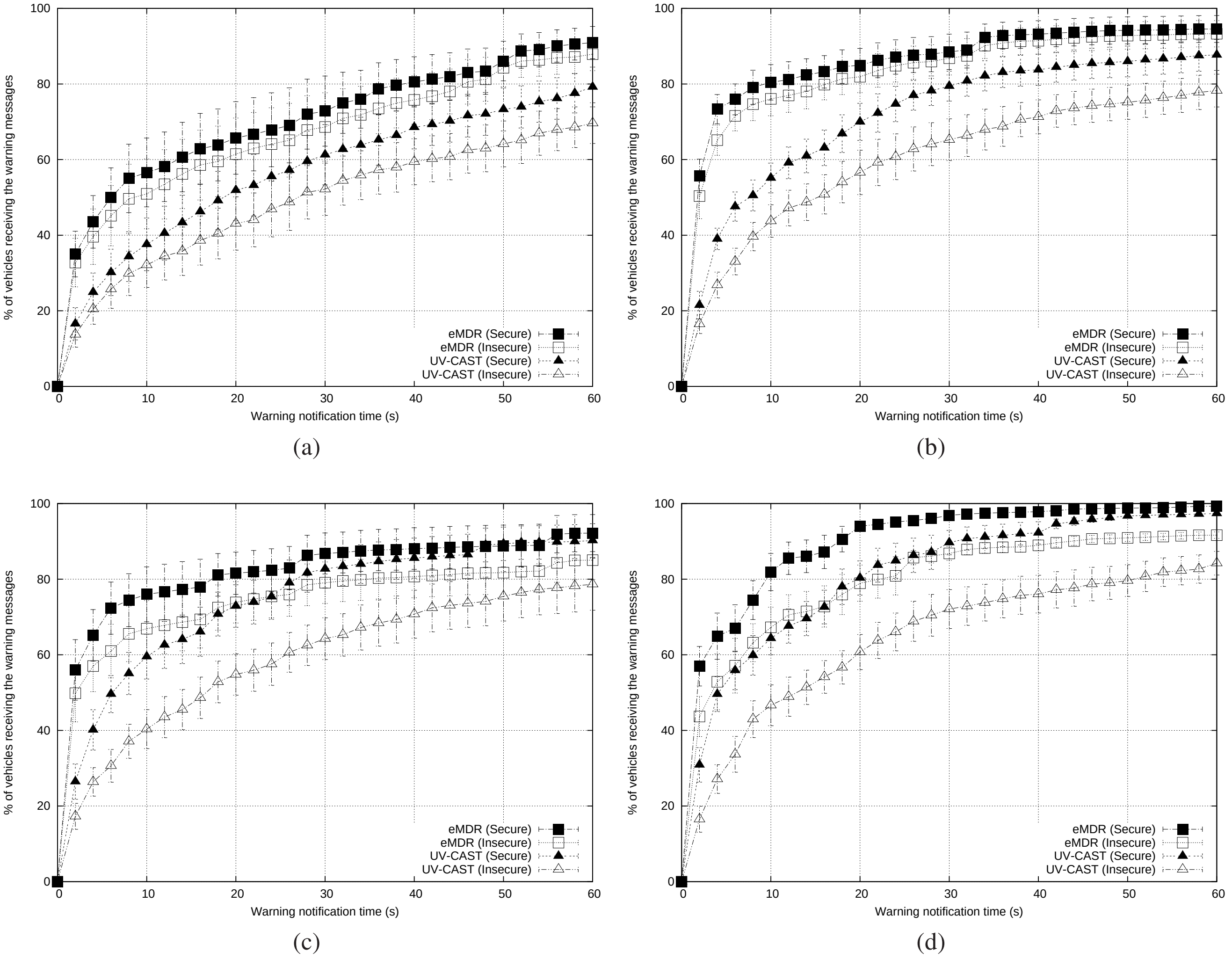
V. Simulation Results

We first study the effect of adversarial nodes on the performance of the dissemination process, when eMDR and UV-CAST are used in their legacy version as well as in combination with the CNPV protocol we propose. Then, we assess the overhead induced by the use of the CNPV protocol.

A. Securing Warning Message Dissemination

Figures 3 and 4 show the evolution of the dissemination process through time in the Madrid map, under different vehicle densities and percentages of adversaries. As we can observe, the legacy UV-CAST scheme is noticeably affected even when a low percentage of attackers are present in the environment: when CNPV is used, the number of informed vehicles grows by 15-20% for most warning notification times. The differences observed when CNPV is used or not tend to grow with increasing vehicle densities, which implies that attackers can more easily slow down the overall process in the presence of a dense vehicular network. Regarding the two mechanisms used by the UV-CAST algorithm, the Store-Carry-Forward (SCF) task is mainly inhibited when adversaries announce false positions. Results show that this is a very important mechanism to reach new areas of the roadmap, and hence the UV-CAST algorithm is greatly affected by the presence of adversaries.

The eMDR algorithm is more resistant, in general, to adversaries trying to thwart it. As shown in Figure 3, when the vehicle density remains low, there are not enough vehicles to cover most of the junctions of the topology, and hence the warning message reception probability is only reduced by 10% at each time instant. However, the effect of the adversary nodes is more evident when the vehicle density increases, since there is more area of the map occupied. This effect is mainly noticeable in Figure 4(b), where we can see an important performance decrease when the security mechanism is not enabled.



(a)

(b)

(c)

(d)

Fig. 5. Warning notification time in Los Angeles with 6% adversaries per warning node and varying the density of vehicles: (a) 100 vehicles, (b) 200 vehicles, (c) 300 vehicles, and (d) 400 vehicles,

To better understand the impact of vehicle density, Figure 5 shows the evolution of the warning dissemination process in Los Angeles when the percentage of adversaries is fixed at 6%. Again, we observe a similar tendency for both dissemination schemes with respect to the Madrid scenario. The UV-CAST algorithm is very sensitive to adversaries in the environment, and there is a uniform performance reduction in all the tested scenarios, independently of the chosen vehicle density. However, the eMDR scheme is able to support up to 200 vehicles (50 vehicles/km^2) without a significant performance loss. Whenever the vehicle density exceeds this threshold, the number of adversary vehicles is enough to degrade the dissemination process, making the selection of the optimal forwarding vehicles unfeasible. We must remember that this selection uses the information of the road topology to choose those vehicles with a better line-of-sight with respect to the streets (i.e., the closest to the center of the junctions), and adversary vehicles sending this information will affect all the vehicles in the vicinity of the junction. As the number of adversaries rises, the number of occupied junctions increases, and the selection of forwarding vehicles is not optimal.

B. CNPV Protocol Overhead

As shown in Figure 6, the percentage of packet traffic received by the simulated vehicles and produced by the use of the CNPV protocol is less than 8% of the total traffic in all the tested scenarios when 3% of adversaries are considered. We can observe how the percentage becomes higher when the UV-CAST algorithm is used: 5-8% of traffic for UV-CAST compared to 1-3% for eMDR; notice that this difference is mainly due to the lower number of messages produced by UV-CAST compared to the eMDR scheme. In addition, in regular maps like Los Angeles, the ratio between HELLO messages received and warning messages is increased as the vehicle density grows, since a higher percentage of vehicles are directly connected, whereas the overhead decreases in irregular maps like Madrid, characterized by a sparser connectivity.

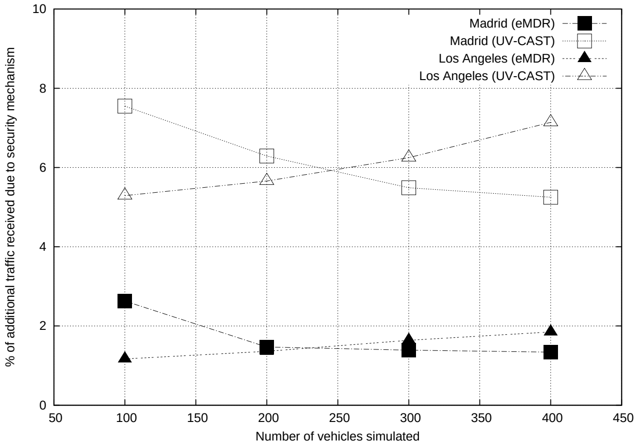


Fig. 6. Overhead produced due to the security mechanism with 3% of adversaries.

VI. Conclusions

In this paper, we presented a proactive, cooperative mechanism for neighbor position verification based on the information interchanged among one-hop neighbors. Our CNPV protocol is easily adaptable to different warning message dissemination schemes that make use of the neighbor information to decide the most appropriate forwarding scheme in VANETs. CNPV allows verifying the position of the neighbors before deciding the next forwarding vehicle, favouring the dissemination process and a limiting the number of vehicles that do not receive the warning messages.

We evaluated the performance of the CNPV protocol by coupling it with two dissemination algorithms, eMDR and UV-CAST, showing how (i) the presence of adversary nodes affects the warning message dissemination performance in urban scenarios, and (ii) CNPV can help to reduce the impact of adversarial users in the vehicular network. When applied in conjunction to the eMDR algorithm, we see how this dissemination scheme supports a high percentage of attackers if the vehicle density is low; however, increasing the number of vehicles in the area allows adversary nodes to occupy the best positions of the road topology, noticeably reducing the performance of the dissemination process. When applying our approach to the UV-CAST scheme, we observe that it is especially sensitive to vehicles announcing false positions, since the store-carry-and-forward approach adopted to reach new areas in disconnected regimes is only performed by boundary vehicles. A vehicle sending false information can easily become the boundary vehicle, avoiding vehicles with a more favorable position to assume this role. Overall, our results show how CNPV improves the performance of the dissemination process in adversarial environments by up to 50% in terms of warning notification time and percentage of uninformed nodes.

Acknowledgments

This work was partially supported by the *Ministerio de Ciencia e Innovación*, Spain, under Grant TIN2011-27543-C03-01, and by the *Diputación General de Aragón*, under Grant “subvenciones destinadas a la formación y contratación de personal investigador”.

References

[1] P. Papadimitratos and A. Jovanovic, “GNSS-based Positioning: Attacks and Countermeasures,” in *IEEE Milcom*, San Diego, CA, USA, Nov. 2008.

[2] J.-H. Song, V. Wong, and V. Leung, “Secure location verification for vehicular ad-hoc networks,” in *IEEE Global Telecommunications Conference (IEEE GLOBECOM)*, New Orleans, LO, USA, Dec. 2008, pp. 1–5.

[3] S. Capkun, K. Rasmussen, M. Cagalj, and M. Srivastava, “Secure location verification with hidden and mobile base stations,” *IEEE Transactions on Mobile Computing*, vol. 7, no. 4, pp. 470–483, Apr. 2008.

[4] S. Capkun and J.-P. Hubaux, “Securing position and distance verification in wireless networks,” Swiss Federal Institute of Technology Lausanne, Lausanne, Switzerland, Technical Report EPFL/IC/200443, Tech. Rep., May 2004.

[5] M. Fiore, C. Casetti, C. Chiasserini, and P. Papadimitratos, “Discovery and verification of neighbor positions in mobile ad hoc networks,” *IEEE Transactions on Mobile Computing*, vol. 12, no. 2, pp. 289–303, Feb. 2013.

[6] M. Fogue, P. Garrido, F. J. Martinez, J.-C. Cano, C. T. Calafate, and P. Manzoni, “Evaluating the impact of a novel message dissemination scheme for vehicular networks using real maps,” *Transportation Research Part C: Emerging Technologies*, vol. 25, pp. 61–80, Dec. 2012.

[7] W. Viriyasitavat, O. Tonguz, and F. Bai, “UV-CAST: an urban vehicular broadcast protocol,” *IEEE Communications Magazine*, vol. 49, no. 11, pp. 116–124, Nov. 2011.

[8] S. Capkun and J.-P. Hubaux, “Secure positioning in wireless networks,” *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 221–232, Feb. 2006.

[9] Nanotron Technologies, “Nano LOC TRX NA5TR1 Facts Sheet,” 2013, available at http://www.nanotron.com/EN/pdf/Factsheet_nanoLOC-NA5TR1.pdf.

[10] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J. P. Hubaux, “Secure vehicular communication systems: Design and architecture,” *IEEE Communications Magazine*, vol. 46, no. 11, pp. 100–109, 2008.

[11] “OpenStreetMap, collaborative project to create a free editable map of the world,” 2013, available at http://www.openstreetmap.org.

[12] D. Krajzewicz and C. Rossel, “Simulation of Urban MObility (SUMO),” Centre for Applied Informatics (ZAIK) and the Institute of Transport Research at the German Aerospace Centre, 2007, available at http://sumo.sourceforge.net/index.shtml.

[13] D. Krajzewicz, G. Hertkorn, C. Rossel, and P. Wagner, “SUMO (Simulation of Urban MObility) - An open-source traffic simulation,” in *Proceedings of the 4th Middle East Symposium on Simulation and Modelling (MESM2002)*, Sharjah, United Arab Emirates, Sept. 2002, pp. 183–187.

[14] F. J. Martinez, J.-C. Cano, C. T. Calafate, and P. Manzoni, “A Performance Evaluation of Warning Message Dissemination in 802.11p based VANETs,” in *IEEE Local Computer Networks Conference (LCN), Zurich, Switzerland*, Oct. 2009, pp. 221–224.

[15] K. Fall and K. Varadhan, “ns notes and documents,” The VINT Project. UC Berkeley, LBL, USC/ISI, and Xerox PARC, February 2000, available at http://www.isi.edu/nsnam/ns/ns-documentation.html.

[16] IEEE 802.11 Working Group, “IEEE Standard for Information Technology – Telecommunications and information exchange between systems – Local and metropolitan area networks –Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Wireless Access in Vehicular Environments,” July 2010.

[17] F. J. Martinez, M. Fogue, C. Toh, J.-C. Cano, C. T. Calafate, and P. Manzoni, “Computer simulations of VANETs using realistic city topologies,” *Wireless Personal Communications*, vol. 69, no. 2, pp. 639–663, 2013.