Fogue, M.; Martinez, FJ.; Garrido, P.; Fiore, M.; Chiasserini, C.; Casetti, C.; Cano Escribá, JC.... (2015). Securing Warning Message Dissemination in VANETs using Cooperative Neighbor Position Verification. IEEE Transactions on Vehicular Technology. 64(6):2538-2550. doi:10.1109/TVT.2014.2344633.

Securing Warning Message Dissemination in VANETs using Cooperative Neighbor Position Verification

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 network scales 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, where location information about neighboring vehicles is 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 [1], [2].

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 allows detecting malicious vehicles announcing false positions, which should not be 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 schemes for warning message dissemination make use of context information to maximize their performance.

A. Neighbor Localization and Verification

As detailed in [3], determining neighbor location in a wireless network is performed using positioning and verification of the position. The positioning process allows computing the position of a neighbor after collecting the information sent by other nodes. The verification of the position determines if the computed location corresponds to the true position of the node.

Regarding positioning, self-localization can be performed through Global Navigation Satellite Systems (GNSS) [4]. Own position information can then be announced to nearby vehicles using vehicle-to-vehicle Dedicated Short-Range Communication (DSRC). In addition, different existing methods can be combined to find out the neighbors within communication range. A technique called “distance bounding” is described in [5], which leverages the fact that each node has a limited communication range in wireless environments. In our case study,

we will rely on the Time of Flight (ToF) technique based on the difference between message transmission and reception times [6], for which off-the-shelf hardware is becoming available [7].

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 [8], or through multilateration methods based on ranging and Time Difference of Arrival (TDoA) [9]. The multilateration is based on the difference of the reception time of a message among a plurality of nodes. Indeed, if a source sends a message, the neighbors will receive it at different times depending on their distance from the transmitter. By sharing information, we can deduce the location of the transmitter. Multilateration systems are widespread nowadays, and they are used by GPS and even airports in order to check the positions of the planes [10].

As far as ad hoc-oriented location verfication protocols are concerned, secure position verification systems for VANETs is presented in [11], [6], [12]. In particular, [11] presents a complete taxonomy of position verification techniques and compares them via simulation under a simple, non-colluder attacker model. The work in [6] applies a simple multilateration involving two nodes only, thus it is not resistant to colluding and Sybil attacks. Our proposal instead can counter such attacks since it exploits the cooperation of all available neighbors through the cross-simmetry test and a more robust multilateration. In [12], 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. If all the nodes forwarding warning messages start this process upon reception of a warning message, the accumulated delay may be very significant, and the efficiency of the dissemination process would decrease. 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) [13] and the *Urban Vehicular broadCAST* (UV-CAST) [14]. 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.

The main objective of the eMDR scheme consists in using the information about the road layout and the position of the vehicles to select the most suitable vehicle to forward a message, in order to reach as many vehicles as possible in the shortest time. In eMDR, a vehicle must decide if it should rebroadcast a received message depending on two factors: (i) distance between sender and receiver, a vehicle will forward the message if it is far enough from the source of the message so as to provide additional coverage area, and (ii) position of the vehicles in the roadmap, due to the effect of buildings and other urban obstacles on radio signal at the

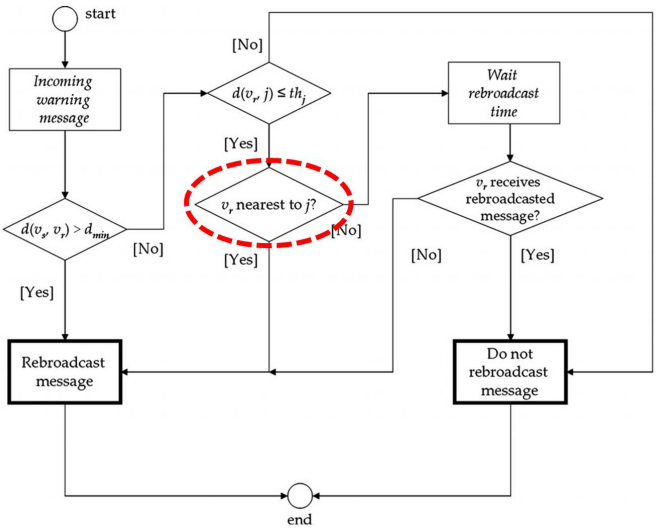
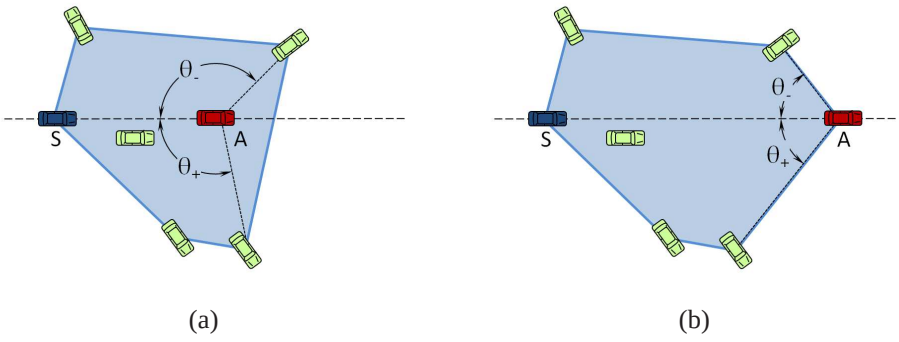


Fig. 1. Use of neighbor information to select forwarding nodes in the eMDR algorithm.



(a) (b)

Fig. 2. Two examples of the distributed gift-wrapping algorithm used in UV-CAST.

frequency of 5.9 GHz used by the IEEE 802.11p standard for VANETs [15]. In order to reduce the number of produced messages, only the vehicle closest to the geographic center of the junction, obtained from integrated GPS maps, is allowed to forward the message. Figure 1 shows the flowchart executed in each vehicle to determine whether to rebroadcast an incoming message or not, where $d(v_x, v_y)$ represents the Euclidean distance between two vehicles, $d(v_x, j)$ represents the Euclidean distance between a vehicles and a junction, d_{min} indicates the minimum distance to allow rebroadcasting messages, and th_j is the threshold used to determine when a vehicle is close enough to a junction. The highlighted operation represents the step of the algorithm where the information collected from the neighbors is used.

The UV-CAST algorithm selects different mechanisms for message dissemination in VANETs differentiating between well-connected and disconnected network regimes, depending in the density of vehicles in the vicinity. Each vehicle uses only local information to decide the network regime it belongs to. Vehicles in well-connected regime rebroadcast incoming messages after a wait time if no redundant messages are received. Vehicles in 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 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. The boundary polygon can be defined as the convex hull including the points representing the positions of the vehicles in communication range from the sender; hence, the boundary vehicles will be those located in the vertices of this convex hull, represented as shadowed polygons in Figure 2. The angles between the receiver vehicles, the source of the message, and each of the neighbors is computed, and the highest and lowest values are used to determine if the vehicle is boundary by means of the *gift-wrapping* algorithm. As shown in Figure 2, after the vehicle A receives a message from the sender S, it obtains the highest and lowest angle values with respect to its neighbors (θ_+ and $\theta\_$, respectively). Since $|\theta_+| + |\theta\_| > \pi$ in Figure 2(a), A is not selected for the SCF task, whereas in Figure 2(b) it detects as a boundary vehicle and it will perform the SCF procedure.

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 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. To retrieve the exact transmission and reception time instants, avoiding the unpredictable latencies introduced by interrupts triggered at the driver level of RF interfaces, a solution such as that implemented in [16] should be adopted. This implies a timing precision of about 23 ns, i.e., an average error of 6.8 meters, determined by the 44 MHz clock of standard 802.11a/b/g cards. Furthermore, the GPS receiver should be integrated in the 802.11 cards; software defined radio solutions integrating GPS in 802.11 are proposed, among others, in [17], [18]. An example of a successful case of RF interface used for ranging can be found in [7].

Each vehicle X has a unique identifier, as well as a long-term private key k_X and a long-term public key K_X, to encrypt and decrypt data [19]. The node identity can be a permanent identifier or a temporary pseudonym, so as to ensure user privacy [20], [21]. 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 exploiting the presence of a public key infrastructure (i.e., certification authority) [22].

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:

- *Verified*: the advertised position corresponds to the true geographic position of the neighbor;
- *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

The proactive verification process uses a message exchange mechanism that takes place in two rounds with the same duration T_{round}:

- ***Round 1***: In the first round, each node X participating in the protocol chooses a random time t_X (not exceeding the round interval). At t_X, the node sends an anonymous HELLO message, using a freshly-generated MAC address and including (i) the node public one-time use key K'_X and (ii) a pair of values

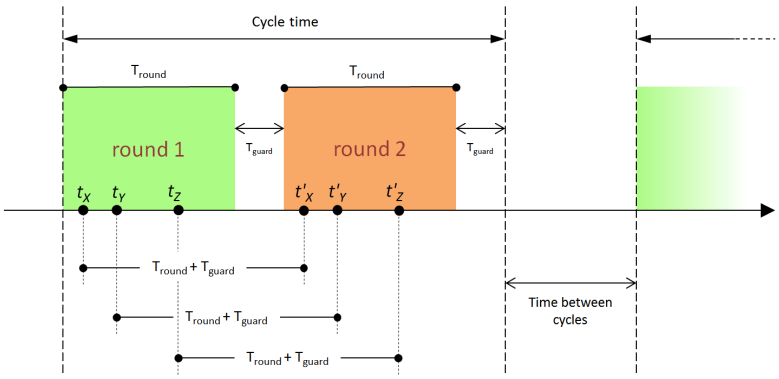


Fig. 3. Temporal detail of the proactive neighbor position verification algorithm.

for each neighbor from which X has received an HELLO in this round. Specifically, the pair of values referring to neighbor Y contains Y's public one-time use key K'_Y and the time instant at which X received Y's HELLO (denoted by t_{YX}). The HELLO message is received by all the neighbors of X, possibly at a different time instant for each node.

- ***Round 2***: Ater a constant *guard time* denoted by T_{guard}, nodes execute the second round of the protocol. Each node X sends a new message, named DISCLOSURE, at time t'_X. DISCLOSURE messages are sent following the same order at which the HELLOs were transmitted by the nodes, i.e., for each node X, $t'_X = t_X + T_{round} + T_{guard}$. The DISCLOSURE message sent by the generic node X contains:
  - (i) the identity of the sender, ID_X;
  - (ii) its announced position, p_x;
  - (iii) the time at which it sent the HELLO message, t_X;
  - (iv) a pair of values (K'_Y, t_{XY}) for each neighbor Y whose HELLO was received by X after t_X;
  - (v) the information needed to make the correspondence with the HELLO message that X sent anonymously during the first round. Such information consists of the public one-time use key X transmitted in the first round, K'_X, and of this same value encrypted with X's private one-time use key k'_X (i.e., $E_{k'_X}(K'_X)$). Note that K'_X allows X's neighbors to decrypt $E_{k'_X}(K'_X)$, while the latter lets X prove to its neighbors that it is the sender of both the HELLO and the DISCLOSURE messages it transmitted;
  - (vi) X's long-term public key K_X;
  - (vii) the digital signature of the DISCLOSURE message generated using X's long-term private key, Sig_X.

The protocol and the message exchange routine are presented in Figure 3 and Algorithm 1. Note that, in Algorithm 1, $\mathbb{N}_X$ denotes the set of neighbors of node X. Furthermore, we remark that during Round 1, a node X keeps recording the pair of values c_Y for all neighbors from which it receives a HELLO message, even after having sent its own HELLO.

After the message exchange routine is complete, each node can create the correspondences between the messages sent in the first round and the neighbors that have revealed their identity (or pseudoidentity) in Round 2. Moreover, each node retrieves from the DISCLOSURE messages the transmission times (t_X) of the HELLOs for each of its neighbors. Such information, together with the locally stored reception times of the HELLOs,

Algorithm 1: Message exchange routine ($\mathbb{N}_X$ denotes the set of neighbors of node X)

```
1  node X do
2      if round == 1 then
3          X : t_X = random ∈ [now, now + t_round]
4          when t_x do
5              forall node Y ∈ N_X do
6                  X : c_y = {(K'_Y, t_YX)}
7              X → * : ⟨HELLO, K'_X, {c_y}_y⟩
8      else if round == 2 then
9          X : t'_X = t_X + T_round + T_guard
10         when t'_x do
11             X → * : ⟨DISCLOSURE, ID_X, p_X, t_X, K'_X, E_k'X(K'_X), {c_y}_y, K_X, Sig_X⟩
```

allows each node to use ToF-based RF ranging to calculate the distance that separates them from their neighbors. Packets received during the second round without a reference from the first round cannot be verified, hence they are ignored until a complete packet interchange is performed.

For example, let us consider the case of a node Y receiving a message from X. Y retrieves t_X, the transmission time of HELLO sent by X, from X's DISCLOSURE message. Y has locally stored t_{XY}, i.e., the time at which it received the same message. Using this information Y can determine the distance that separates it from X.

Finally, we remark that the HELLO message in Round 1 needs to be anonymous, so as to make the protocol robust to attacks. Indeed, if an adversary knew the postion of the nodes taking part in Round 1, it could use this information to adjust the timing data it includes in its own HELLO in Round 1. In order to make the HELLO in Round 1 anonymous, such message (i) is transmitted employing a fresh, software-generated MAC address, and (ii) contains a public key K'_X taken from X's pool of anonymous one-time use keys that do not allow neighbors to map the key onto a specific node. Since a source address has to be included in the MAC-layer header of the message, a fresh, software-generated MAC address is needed; note that this is considered a part of emerging cooperative systems [20]. Including a one-time key in the HELLO also ensures that the message is fresh (i.e., the key acts as a nonce).

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, as well as a mathematical analysis laying the foundations of the secure positioning scheme of CNPV, are available in [12].

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 to the information collected from each of its neighbors. This test does not use the cooperative approach of the protocol. During this test, two sub-tests 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 set to 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 neglected 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 hyperbolas. 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 4(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 Castellana in the city of Madrid (Spain), shown in Figure 4(b), is an example of European city with a more irregular layout. The scenarios were obtained from OpenStreetMap [23], 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

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

(a) (b)

Fig. 4. 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).

from OpenStreetMap and is based on SUMO [24], 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 [25]. 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 [26] to determine such points of attraction in the roadmaps and to derive the macroscopic traffic flows. The effect of traffic flow changes on the performance is negligible, since the dissemination time obtained in our simulations is too short to appreciate noticeable changes due to these changes that could modify the dynamic behavior of the simulation.

Simulations were carried out using the ns-2 simulator [27], modified to include the IEEE 802.11p [15] 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 [28], 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. The RAV model is based on real-world measurements and accounts for attenuation and fading due to radio obstacles.

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. In a urban environment where the maximum speed should not exceed 50 km/^{2}, the maximum distance traveled by vehicles is about 14 meters, and thus it is a reasonable assumption to generate

verification messages at this rate to avoid saturation of the wireless channel. However, the scheme could be easily adapted to comply with standards like the ETSI TS 102 637-2 [29], in which the beacons are sent dynamically with frequencies between 1 Hz and 10 Hz in dependence of the mobility of the sender vehicle. In this case, the CNPV information could be broadcast once per second, while the rest of the beacons would contain only the information required in each situation, making the verification mechanism compatible with these standards.

As for the time required by the operations of signing and verification that are part of the secure protocol, we took them into account. We set the time required for signing a DISCLOSURE message to 3 ms and that required for signature verification to 12 μs, assuming that an Intel Core i7-2670QM 2.2Ghz processor is used [30], [31]. Note that only one signature per cycle time has to be generated by each node, and that every cycle time one signature verification per neighbor has to be carried out.

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, and the effect of different levels of ranging errors on the performance of the mechanism. All results represent the average of multiple executions with different random seeds, and fall within a 95% confidence interval. Table I summarizes the parameter values used in our simulations.

A. Adversary model

Simulations account for different percentages of adversarial vehicles, namely 3%, 6%, and 9% of the total number of vehicles. This relatively high values are selected since we are interested in worst case scenarios where the number of adversaries could threaten the performance of the Warning Message Dissemination system. The nodes only have knowledge about their communication neighbors, they do not have global knowledge of the network, and a high percentage of adversaries is necessary to cover all the attacked area.

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

TABLE I

PARAMETER VALUES USED FOR THE SIMULATIONS

Parameter	**Value**
number of vehicles	$100, 200, 300, 400$
simulated area	$2000m \times 2000m$
mobility generator	C4R
mobility models	Krauss [25] and Downtown model [32]
maximum speed of vehicles	$23\ m/s\ \approx\ 83\ km/h$
maximum acceleration of vehicles	$1.4\ m/s^2$
maximum deceleration of vehicles	$2.0\ m/s^2$
driver reaction time (τ)	$1\ s$
number of warning mode vehicles	3
warning message size	$512B$
warning packet rate	$1\ per\ second$
warning message priority	$AC3$
HELLO message size	$40B(CNPV) + 512B(key + sign.)$
HELLO packet rate	$1\ per\ second$
HELLO message priority	$AC1$
MAC/PHY	802.11p
maximum transmission range	$400m$
CNPV ϵ_r	$10m$
CNPV ϵ_p	$10m$
CNPV T_{round}	$0.75\ seconds$
CNPV T_{guard}	$0.25\ seconds$

assigned the data carrying task, reducing the chances that the warning message reaches new areas of the urban scenario.

V. SIMULATION RESULTS

In this section, the performance of the CNPV protocol is evaluated. We rely on simulation since an accurate representation of both (i) vehicular mobility, and (ii) CNPV protocol operation, are required. Unfortunately, those two aspects are nearly impossible to abstract into an analytical model without oversimplifying the system – which would yield results of little significance, as shown, e.g., in [33]. For instance, previous works presenting analytical models of nodes mobility and vehicle-to-vehicle connectivity [34], [35], or message dissemination [36], [37] have limited their scope to extremely simplified scenarios (a highway road section, or a regular grid) and to dynamics over very short time intervals, besides making unrealistic assumptions on car movement (e.g., each road lane corresponds to a fixed speed and lane changes occur with known probabilities). However, the performance of the message dissemination scheme and the secure positioning techniques of CNPV are strongly dependent on the underlying node mobility, which should thus be represented in a very realistic way, too complex to be mathematically tractable via, e.g., Markovian analysis.

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, and the effect of different levels of

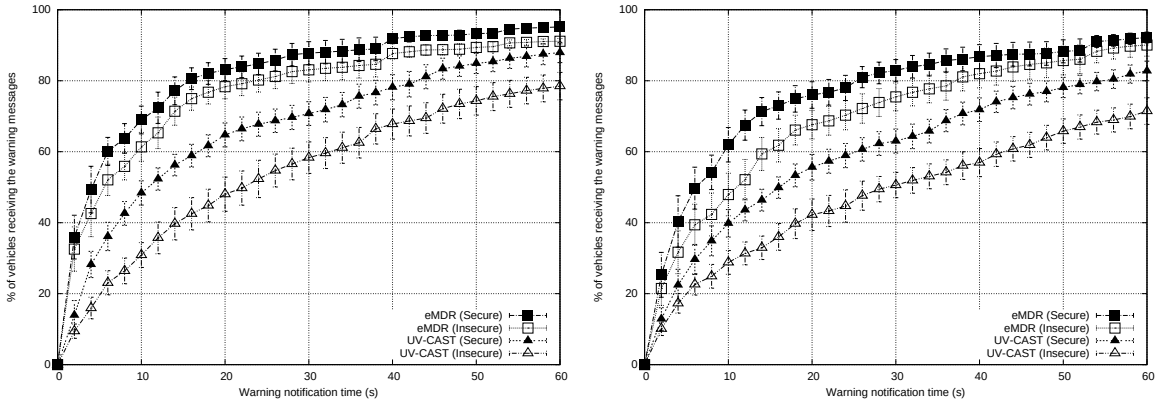


Fig. 5. Warning notification time in Madrid with 200 vehicles varying the percentage of adversaries: (a) 3%, and (b) 9%.

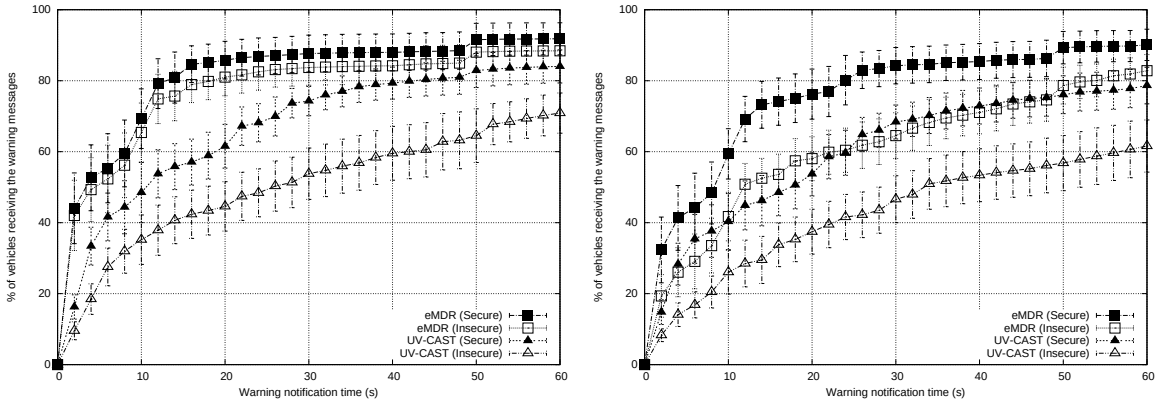


Fig. 6. Warning notification time in Madrid with 400 vehicles varying the percentage of adversaries: (a) 3%, and (b) 9%.

ranging error on the performance of the proposed CNPV protocol to secure warning message dissemination. Finally, we study the influence of high vehicle densities in urban scenarios.

A. Securing Warning Message Dissemination

Figures 5 and 6 show the percentage of vehicles reached by the warning message over 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 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.

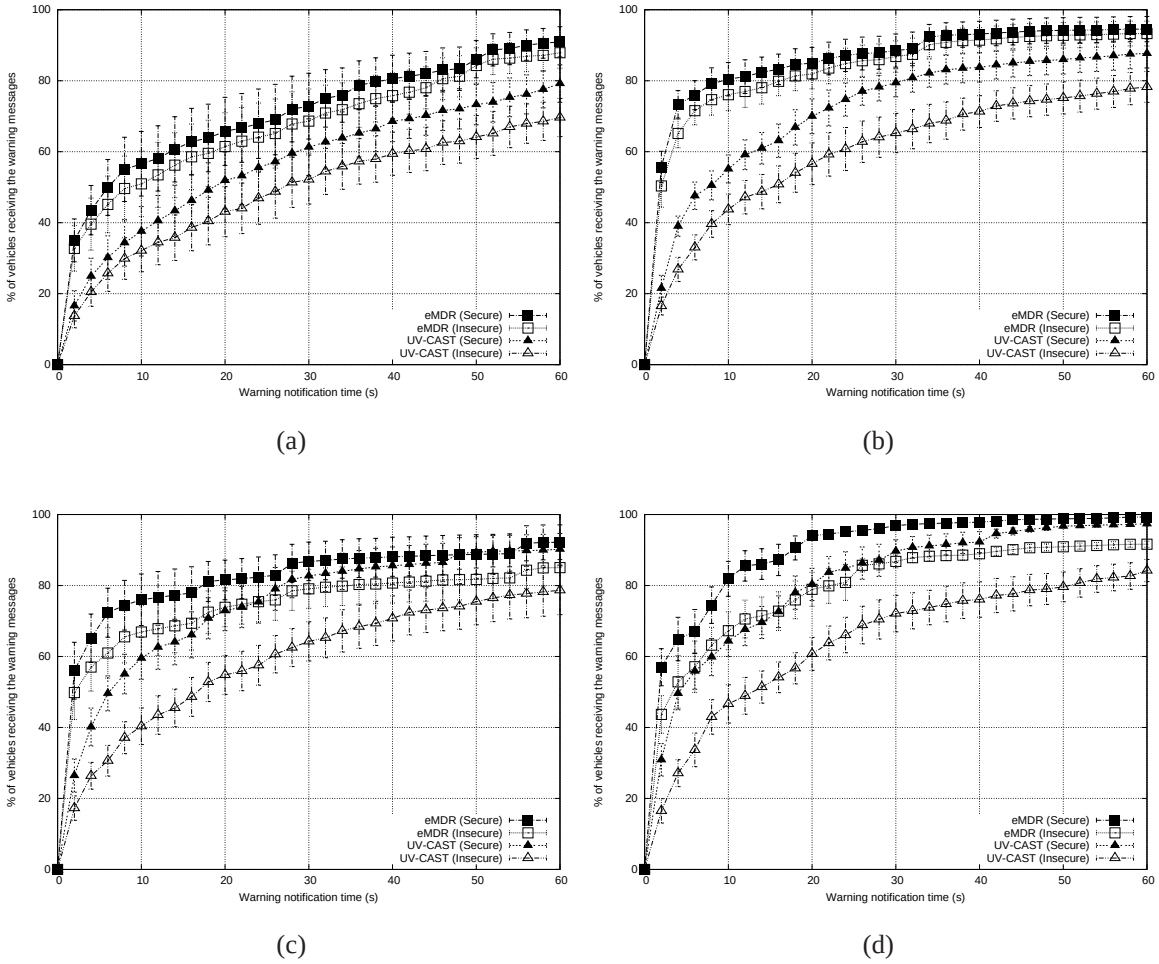


Fig. 7. Warning notification time in Los Angeles with 6% adversaries per warning node and varying the density of vehicles: (a) 100 vehicles, (b) 200 vehicles, (c) 300 vehicles, and (d) 400 vehicles.

The eMDR algorithm is more resistant, in general, to adversaries trying to thwart it. As shown in Figure 5, 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 the area occupied by vehicles is larger. This effect is more evident in Figure 6(b), where we can see an important performance decrease when the security mechanism is not enabled.

To better understand the impact of vehicle density, Figure 7 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

TABLE II

AVERAGE SIMULATION RESULTS IN THE MADRID SCENARIO USING THE EMDR ALGORITHM.

Veh. Density	% Adv.	Security	% Blind veh.	WNT (50%)	WNT (75%)
100 vehicles (25 veh./km^2)	3%	OFF	21.7%	29.10 s	96.11 s
		ON	21.0% (*-3.2%*)	26.63 s (*-8.5%*)	86.09 s (*-10.4%*)
	6%	OFF	28.3%	33.33 s	–
		ON	23.6% (*-16.6%*)	31.34 s (*-6.0%*)	89.63 s
	9%	OFF	32.0%	41.09 s	–
		ON	28.0% (*-12.5%*)	35.10 s (*-14.6%*)	–
200 vehicles (50 veh./km^2)	3%	OFF	3.4%	4.44 s	15.42 s
		ON	2.8% (*-17.6%*)	4.12 s (*-7.2%*)	12.85 s (*-16.7%*)
	6%	OFF	4.9%	6.42 s	20.55 s
		ON	3.9% (*-20.4%*)	4.41 s (*-31.3%*)	14.45 s (*-29.7%*)
	9%	OFF	8.5%	9.42 s	34.44 s
		ON	5.0% (*-41.2%*)	6.11 s (*-35.1%*)	18.44 s (*-46.5%*)
300 vehicles (75 veh./km^2)	3%	OFF	1.3%	1.04 s	8.15 s
		ON	1.2% (*-7.7%*)	0.84 s (*-19.2%*)	6.84 s (*-16.1%*)
	6%	OFF	1.7%	2.13 s	12.83 s
		ON	1.5% (*-11.7%*)	1.67 s (*-21.6%*)	8.67 s (*-32.4%*)
	9%	OFF	2.3%	4.13 s	21.15 s
		ON	1.7% (*-26.1%*)	2.66 s (*-35.6%*)	9.15 s (*-56.7%*)
400 vehicles (100 veh./km^2)	3%	OFF	2.1%	3.73 s	11.89 s
		ON	1.0% (*-52.3%*)	3.19 s (*-14.5%*)	9.73 s (*-18.2%*)
	6%	OFF	3.5%	6.86 s	15.74 s
		ON	2.2% (*-37.1%*)	4.73 s (*-31.0%*)	10.91 s (*-30.7%*)
	9%	OFF	8.2%	13.70 s	48.19 s
		ON	5.1% (*-37.8%*)	8.19 s (*-40.2%*)	18.72 s (*-61.1%*)

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 proximity of the junction. As the number of adversaries rises, the number of occupied junctions increases, and the selection of forwarding vehicles is not optimal.

We already proved how the UV-CAST algorithm is greatly affected by the presence of even a low percentage of adversary nodes. It would be more interesting to study how the eMDR algorithm is affected in a wider variety of scenario. Table II contains the average simulation results for the eMDR scheme in all the configurations tested in the Madrid scenario, for the metrics of blind vehicles not receiving warning messages after 120 seconds, and the time required to inform at least 50% and 75% of the vehicles in the scenario, also called Warning Notification Time (WNT). It is noticeable that, when the security scheme for neighbor position verification is enabled, we achieve better results in all the tested scenarios and for all the metrics selected: the gain in the values of some of the metrics is higher than 60%. In general, we observe how, by increasing the percentage of adversary vehicles per warning vehicle (column *"% Adv."*), the scheme reduces considerably its performance, especially for high vehicle densities. Furthermore, under high vehicle density, the scheme reduces the percentage of blind vehicles (by up to 50%) as well as the time needed to inform 75% of the vehicles. The latter improves from 10.4% when simulating 100 vehicles, to 61.1% for 400 vehicles in the best case. This confirms the tendency observed

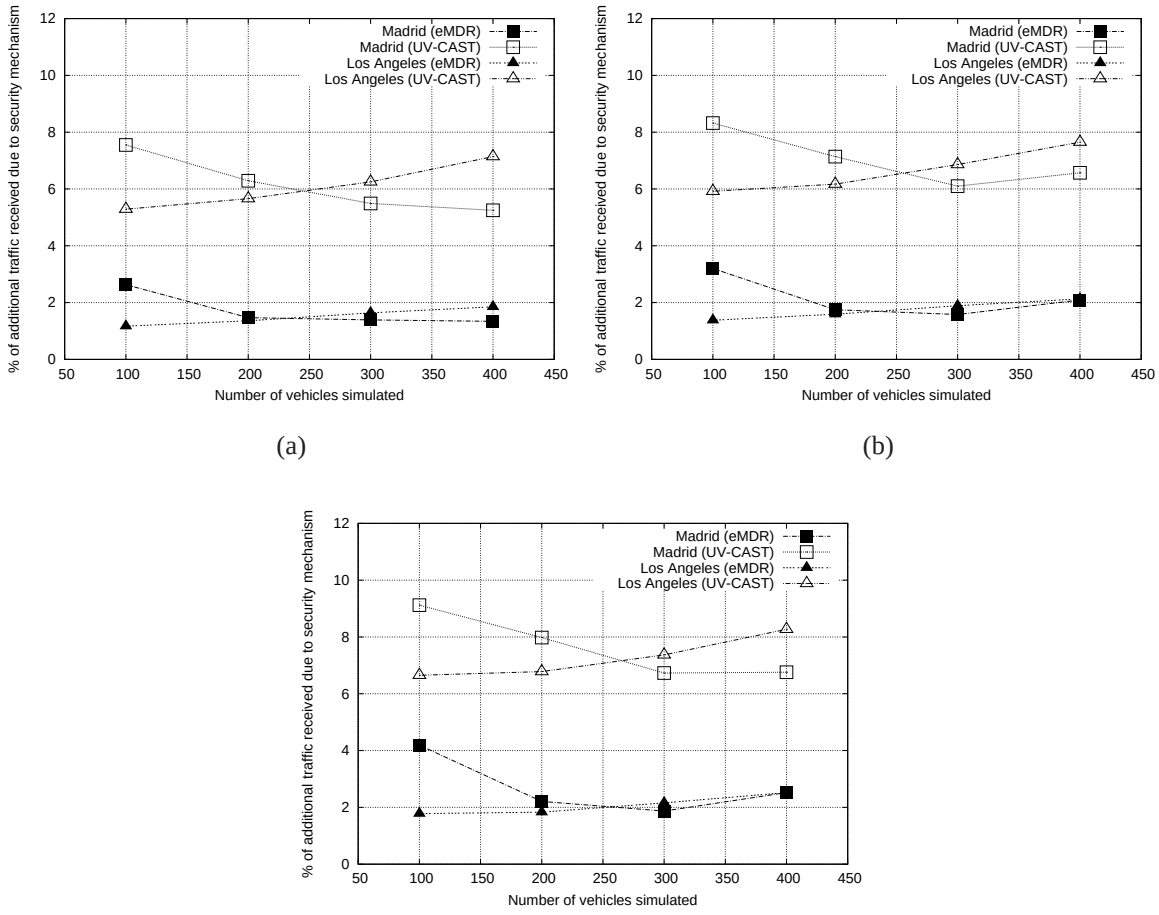


Fig. 8. Average overhead due to the security mechanism with (a) 3%, (b) 6%, and (c) 9% of adversaries.

for the eMDR algorithm in the rest of tested scenarios.

B. CNPV Protocol Overhead

We define the overhead as the average ratio of wireless traffic received by a vehicle due to the CNPV protocol, in terms of HELLO and DISCLOSURE messages. More formally, the overhead is computed as:

$$Overhead = \frac{1}{N} \sum_{i=1}^{N} \frac{BytesReceived_{CNPV}(i)}{BytesReceived_{total}(i)} \quad (1)$$

Where $BytesReceived_{CNPV}(i)$ are the bytes of traffic induced by CNPV and received by vehicle i, $BytesReceived_{total}(i)$ are the total bytes received by vehicle i, and N is the total number of vehicles in the system. As shown in Figure 8, the packet overhead is less than 8% of the total traffic in all the tested scenarios when 3% of adversaries are considered, and less than 10% when the simulation accounts for 9% of adversaries. There is a slight increase in the overhead produced by the security mechanism as the percentage of adversarial nodes grows, since there are fewer vehicles forwarding warning messages and the amount of relative traffic due to HELLO messages is higher.

We can observe how the percentage becomes higher when the UV-CAST algorithm is used: 5-10% of traffic for UV-CAST compared to 1-4% 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 and warning messages increases as the vehicle density grows, due to the superlinear increase in the number of one-hop neighbors with respect to the total number of vehicles. Conversely, the overhead does not have a monotonic trend in irregular maps like Madrid, which is characterized by sparser connectivity.

In general, the additional traffic generated by the security scheme is low compared to the warning message dissemination scheme that it gives support to. The small one-hop HELLO messages used by the CNPV mechanism occupy less bandwidth than the large warning message that are not limited to one-hop interactions.

To better understand the efficiency of the dissemination algorithms studied, Figure 9 shows the average percentage of duplicate warning messages received by each vehicle in Madrid, compared to the total number of warning messages received. As we can see, the amount of duplicate messages is higher when using the eMDR algorithm, where 60-80% messages received are duplicated. However, even if this may be considered inefficient compared to the UV-CAST scheme, which achieves 40-50% of duplicates, the results show how eMDR is able to inform more vehicles in less time, making it especially suitable to deliver critical information. UV-CAST could be useful to disseminate non-critical information with decent performance and little resource usage. Finally, if we disable the verification mechanism, the percentage of duplicate messages also decreases. Malicious nodes are able to reduce the overall warning message traffic, thus reducing the amount of informed vehicles and increasing the time required to notify the affected vehicles.

C. Influence of ToF Ranging Errors on CNPV Performance

The localization obtained by means of Time of Flight-based Radio Frequency ranging technique is not completely accurate. Depending on the frequency selected, the specific interfaces, and the environment we may find different levels of ranging errors that could affect the performance of the security mechanism developed.

Lanzisera et al. [38] performed different experiments using several frequency ranges around the 2.4 GHz band, including methods for reducing error from clock offset and multipath propagation implemented on prototype hardware. In this scenario, the maximum localization error found was 24 meters using the frequency of 2405 MHz, whereas for the rest of frequencies the maximum error was under 20 meters, with an average error of 3 meters. The error registered showed a Gaussian distribution, meaning that the probability of error over 10 meters is less than 10%.

Sikora and Groza [39] tested this ranging technique in street scenarios with and without obstacles, such as vehicles, trees, and other urban structures, using commercial equipment working in the 2.4 GHz band. The error registered were about 4-10 meters without obstacles, and 5-15 meters in the presence of obstacles, with typical standard deviations below 0.4 meters.

Using the data from existing works as a reference, we studied the effect of ranging errors on the performance of CNPV mechanism used jointly with the tested warning message dissemination algorithms. We simulated different levels of maximum error: from 10 meters, as used in the previous simulations presented, to 40 meters, representing conditions with extreme error values if we compare with the empirical results using this ranging

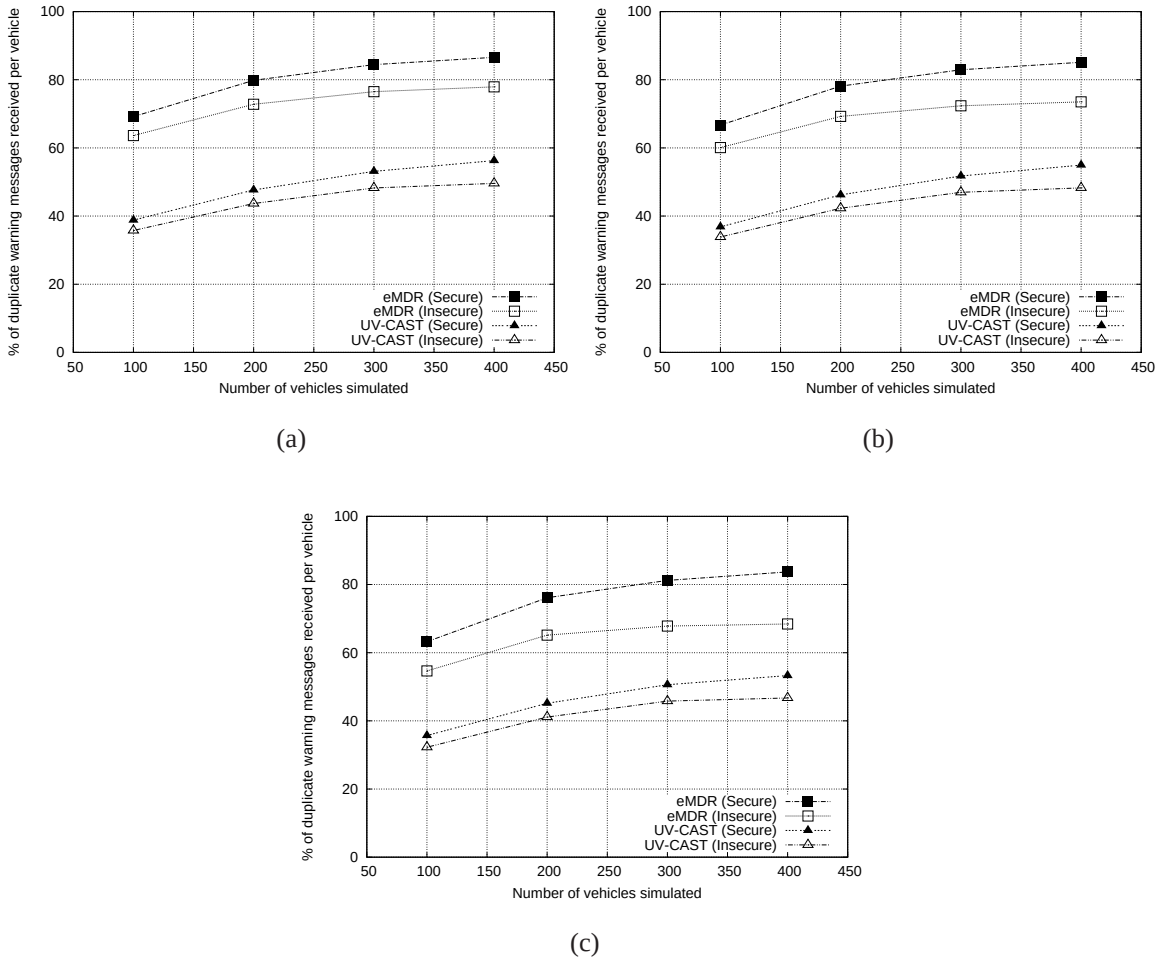


Fig. 9. Average percentage of duplicate warning messages received in the Madrid scenario with (a) 3%, (b) 6%, and (c) 9% of adversaries.

technology. These values correspond to the variable ϵ_r in the CNPV algorithm, representing the precision of the ranging mechanism.

Figures 10 and 11 show the results obtained using the scenario of Madrid simulating 200 and 400 vehicles, i.e., 50 and 100 vehicles/km^2. As shown, the performance of the warning dissemination process in an adversarial environment is noticeable influenced by the presence of ranging errors, but it is only really remarkable when the error levels are very high (over 30 meters) and when the percentage of attackers exceeds 6%. The tendency in all the situations tested is the same, the warning notification time and the percentage of uninformed nodes are increased as the error level grows, but there are no significant differences when the maximum error is 30 meters or 40 meters.

If we compare the dissemination algorithms, eMDR and UV-CAST, it is also noteworthy that the eMDR scheme outperforms UV-CAST in all the scenarios, even when the ranging error levels are the highest. However, the influence of ranging errors on the performance of UV-CAST are almost independent on the percentage of adversarial nodes, whereas eMDR becomes less efficient as the number of attackers increases. This is especially visible in Figure 11(c), where the performance of eMDR reduces up to 20% comparing between 10 and 50 meters of maximum ranging error.

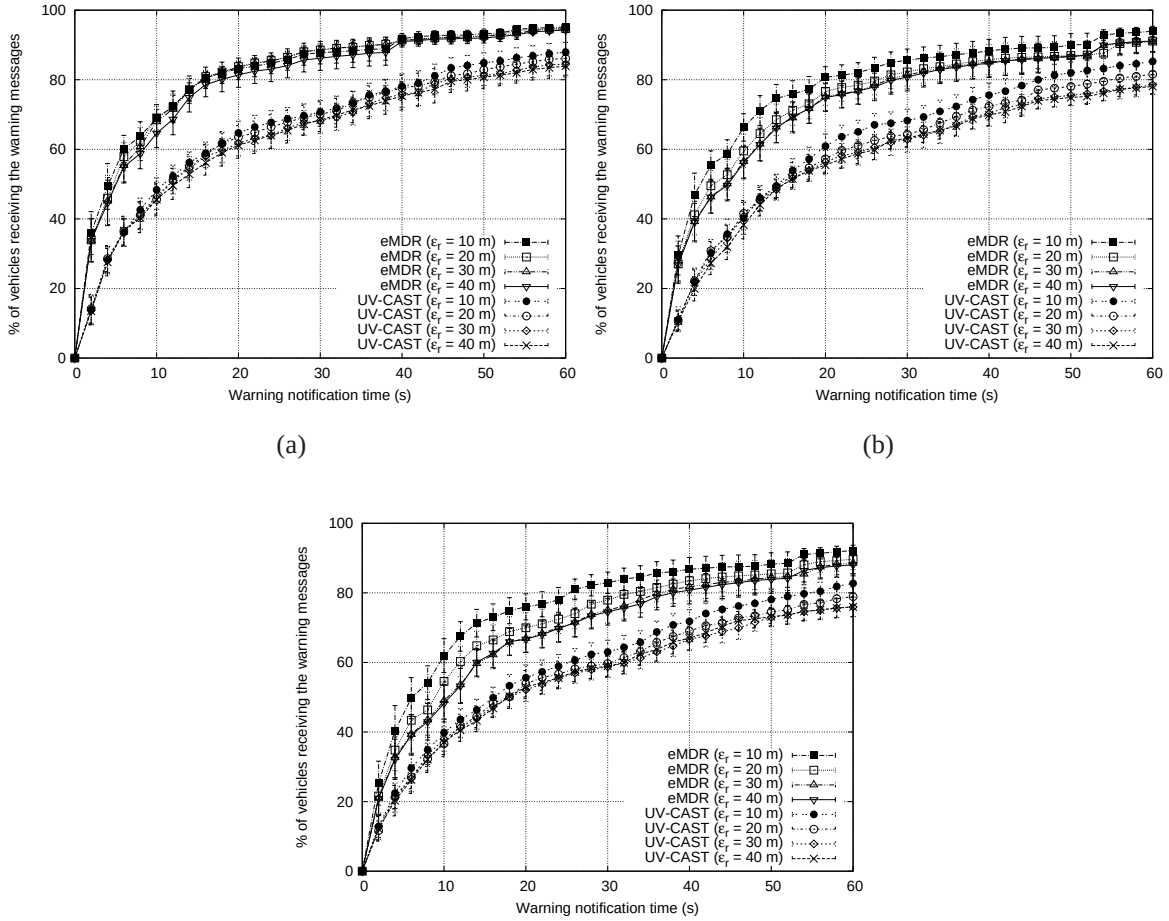


Fig. 10. Warning notification time under different levels of maximum ranging error in Madrid simulating 200 vehicles with (a) 3%, (b) 6%, and (c) 9% of adversaries.

D. Performance under High Vehicle Density

In realistic urban environments, the vehicle density could increase far over the threshold of 100 vehicles/km^2, producing scenarios prone to cause broadcast storms due to the number of vehicles directly connected. The higher probability of packet collisions in the shared channel under these conditions may reduce the effectiveness of the position verification mechanism. Hence, we will study the effects of dense environments on the designed system.

We performed new simulations accounting for higher vehicle densities. Specifically, we tested with 400 vehicles/km^2 and 800 vehicles/km^2, representing traffic jam conditions in dense cities. Due to the limitations of the ns-2 simulator, we obtained a smaller area of the Madrid map covering 1 km^2 were the new simulations could be performed without excessively increasing simulation time. We decided to test new values for the percentage of adversary nodes to observe their effect when combined with higher vehicular densities. In particular, we also obtained the results simulating when 1% of adversaries, as well as the previous tested values. Figures 13 and 14 show the simulation results in this scenario.

As shown, the performance reduction when the verification mechanism is disabled is not as noticeable as it

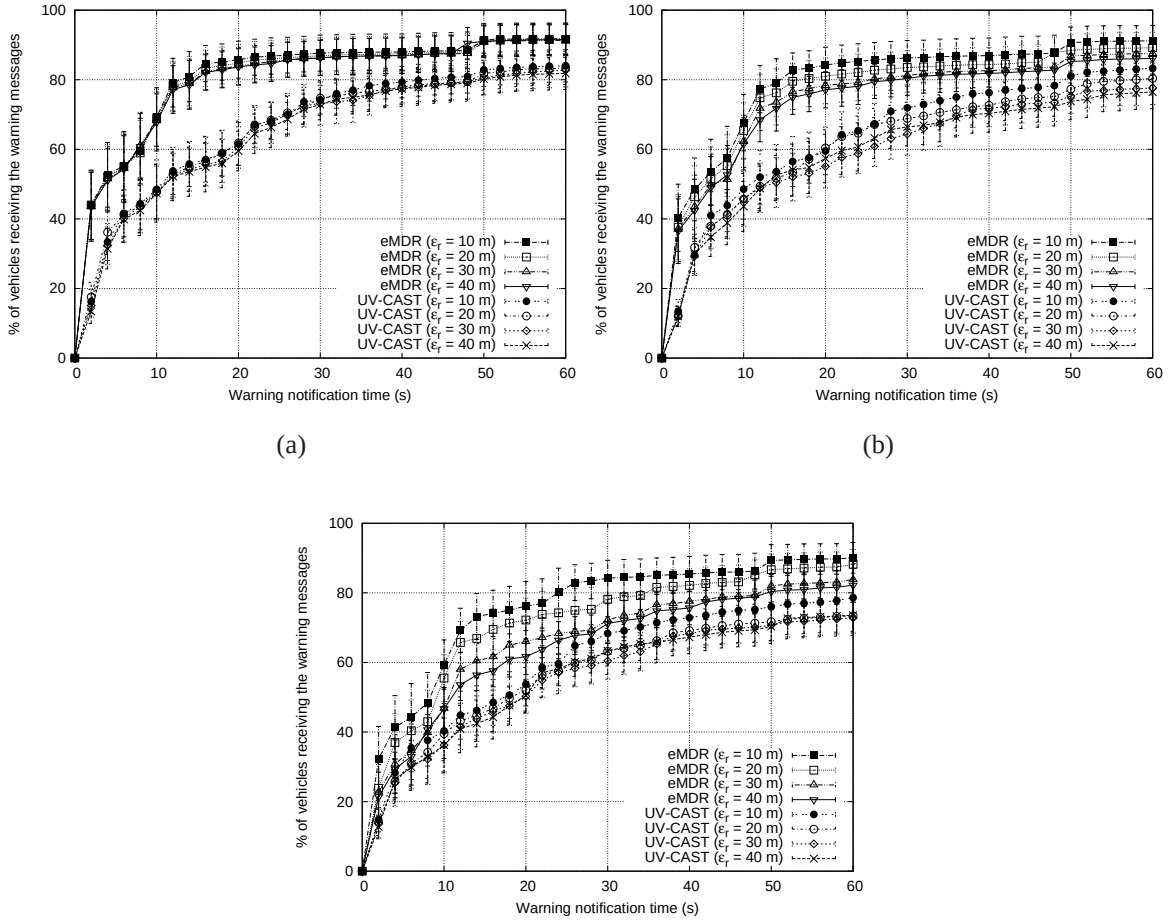


Fig. 11. Warning notification time under different levels of maximum ranging error in Madrid simulating 400 vehicles under (a) 3%, (b) 6%, and (c) 9% of adversaries.

was under lower densities. The main reason of this effect is that the parts of the algorithm that are inhibited by the actions of the malicious nodes, i.e., rebroadcast in junctions using eMDR and Store-Carry-Forward using UV-CAST, are mainly useful for densities under 100 vehicles/km^2 since they are designed for low-congested urban environments. As vehicle density increases, the importance of theses mechanisms in the notification of additional vehicles is less important, and the other parts of the algorithm become more useful, reducing the negative effect of the adversaries.

Regarding the trend observed in these new results, it remains the same when compared to those obtained under low-medium density. The eMDR algorithm achieves better results than UV-CAST in all the simulations, and it only experiences performance drops under the highest percentages of adversaries. The performance reduction is hardly noticeable for 1% of adversary nodes, increasing as the number of adversaries increases. The performance of the UV-CAST algorithm is reduced by about 5-10% even when the number of adversaries is low, proving that the efficiency of the verification system is maintained even in congested environments.

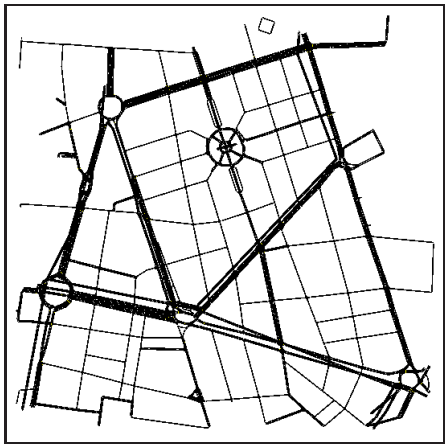


Fig. 12. Scenario of Madrid representing 1 km^2 area.

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, by the Fundación Universitaria Antonio Gargallo and the Obra Social de Ibercaja, under Grant 2013/B010, as well as the Government of Aragón under Grant “subvenciones destinadas a la formación y contratación de personal investigador” and the European Social Fund (T91 Research Group).

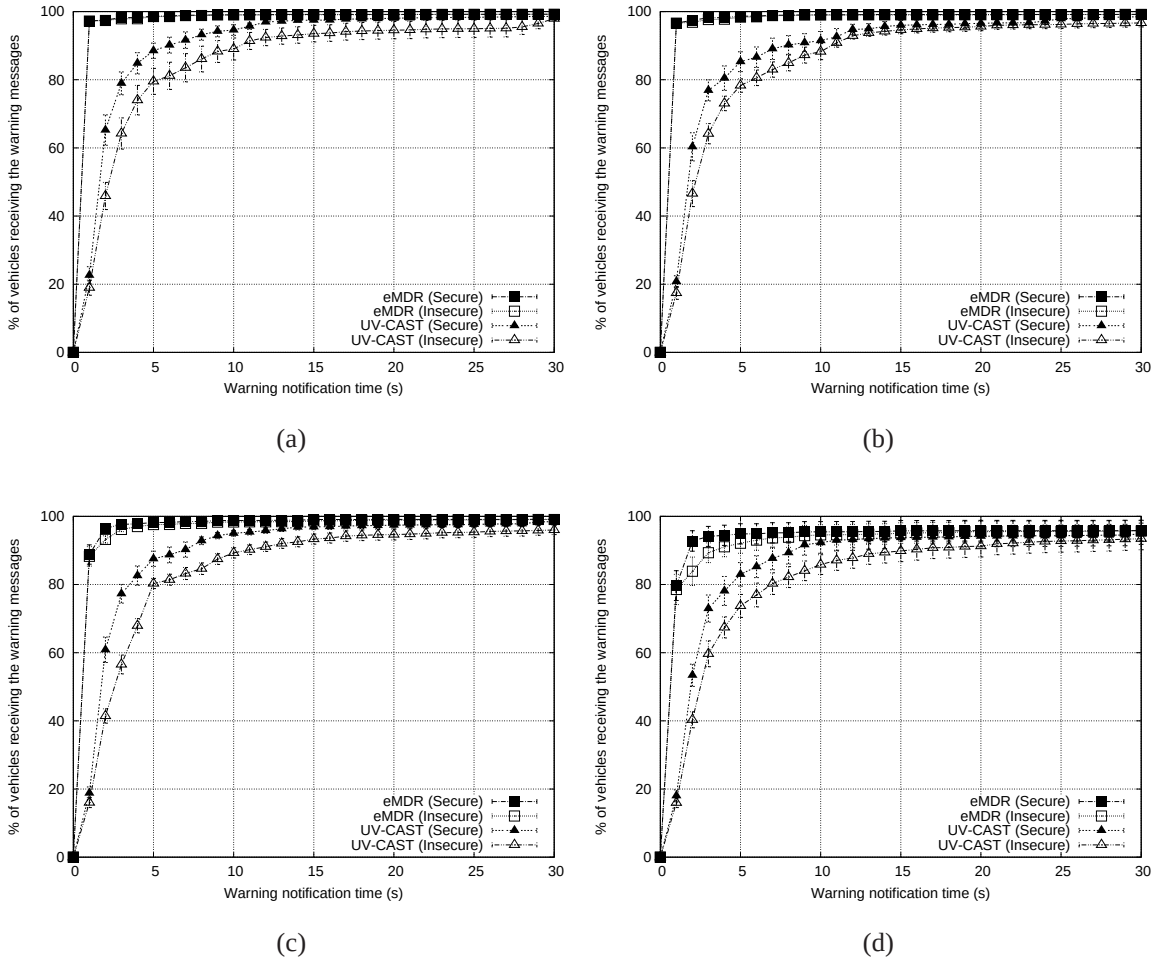


Fig. 13. Warning notification time in Madrid simulating 400 vehicles/km^2 varying the percentage of adversaries: (a) 1%, (b) 3%, (a) 6%, and (b) 9%.

REFERENCES

[1] E. Schoch, F. Kargl, and T. Leinmüller, "Vulnerabilities of geocast message distribution," in *IEEE Workshop on Automotive Networking and Applications (AutoNet)*, 2007.

[2] T. Leinmller and E. Schoch, "Greedy routing in highway scenarios: The impact of position faking nodes," in *Workshop on Intelligent Transportation (WIT)*, 2006.

[3] Y. Zeng, J. Cao, J. Hong, and L. Xie, "Secure localization and location verification in wireless sensor networks," in *IEEE 6th International Conference on Mobile Adhoc and Sensor Systems (MASS '09)*, Oct. 2009, pp. 864–869.

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

[5] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *Proc. of the ACM Workshop on Wireless Security 2003 (WiSe'03)*, San Diego, CA, USA, Sep. 2003, pp. 1–10.

[6] 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.

[7] Nanotron Technologies, "Nano LOC TRX NA5TR1 Facts Sheet," 2013. [Online]. Available: http://www.nanotron.com/EN/pdf/Factsheet_nanoLOC-NA5TR1.pdf

[8] 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.

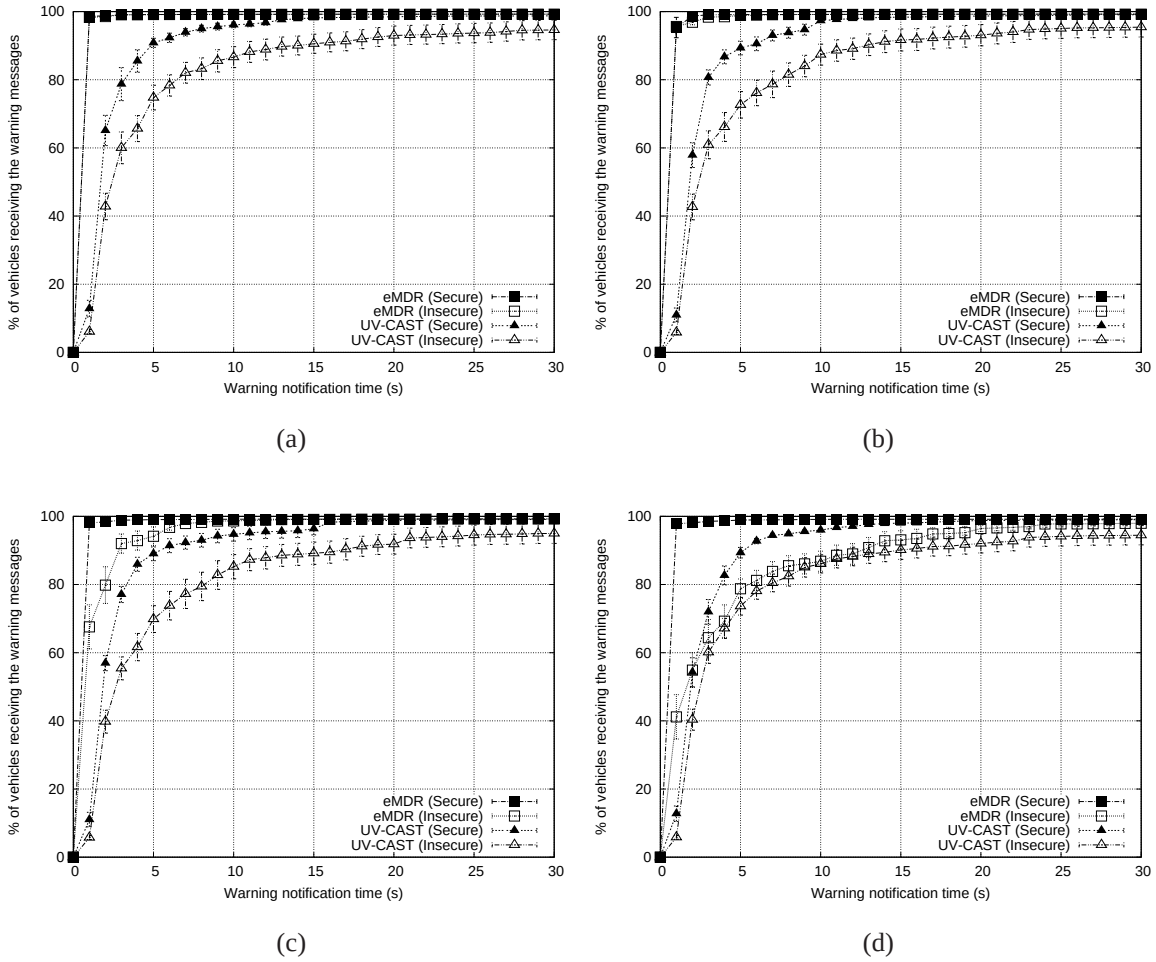


Fig. 14. Warning notification time in Madrid simulating 800 vehicles/km^2 varying the percentage of adversaries: (a) 1%, (b) 3%, (a) 6%, and (b) 9%.

[9] 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.

[10] Creativerge ERA Corporation, "Multilateration Executive Reference Guide," 2013. [Online]. Available: http://multilateration.com/

[11] T. Leinmüller, E. Schoch, F. Kargl, and C. Maihöfer, "Decentralized position verification in geographic ad hoc routing," *Security and Communication Networks*, 2008.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] M. Ciurana, F. Barcelo-Arroyo, and F. Izquierdo, "A ranging system with IEEE 802.11 data frames," in *IEEE Radio and Wireless Symposium*, January 2007.

[17] F. Carpenter, S. Srikanteswara, and A. Brown, "Software defined radio test bed for integrated communications and navigation

applications," in *Software Defined Radio Technical Conference*, November 2004.

[18] E. D. Re, L. S. Ronga, L. Vettori, L. L. Presti, E. Falletti, and M. Pini, "Software defined radio terminal for assisted localization in emergency situations," in *CTIF Wireless Vitae*, May 2009.

[19] "Ieee 1363a 2004, ieee standard specifications for public-key cryptography – amendment 1: Additional techniques," 2004.

[20] "Preciosa: Privacy enabled capability in co-operative systems and safety applications." [Online]. Available: http://www.preciosa-project.org

[21] J. Kenney, "Dedicated short-range communications (dsrc) standards in the united states," *IEEE journal, special issue on vehicular communications*, vol. 99, no. 7, pp. 1162–1182, 2011.

[22] 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.

[23] "OpenStreetMap, collaborative project to create a free editable map of the world," 2013. [Online]. Available: http://www.openstreetmap.org

[24] 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. [Online]. Available: http://sumo.sourceforge.net/index.shtml

[25] 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.

[26] M. Fogue, P. Garrido, F. J. Martinez, J.-C. Cano, C. T. Calafate, and P. Manzoni, "A realistic simulation framework for vehicular networks," in *5th International ICST Conference on Simulation Tools and Techniques (SIMUTools)*, March 2012, pp. 37–46.

[27] K. Fall and K. Varadhan, "ns notes and documents," The VINT Project. UC Berkeley, LBL, USC/ISI, and Xerox PARC, February 2000. [Online]. Available: http://www.isi.edu/nsnam/ns/ns-documentation.html

[28] 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.

[29] European Telecommunications Standards Institute, "ETSI TS 102 637-2: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service"," 2011. [Online]. Available: http://www.etsi.org/deliver/etsi_ts/102600_102699/10263702/01.02.01_60/ts_10263702v010201p.pdf

[30] C. K. Wong and S. Lam, "Digital signatures for flows and multicasts," *IEEE/ACM Transactions on Networking*, vol. 7, no. 4, pp. 502–513, 1999.

[31] "Bitcoin network scalability." [Online]. Available: https://en.bitcoin.it/wiki/Scalability

[32] 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.

[33] A. Kesting, M. Treiber, and D. Helbing, "Connectivity statistics of store-and-forward intervehicle communication," *IEEE Transactions on Intelligent Transportation Systems*, vol. 11, no. 1, pp. 172–181, March 2010.

[34] J. Zhao, T. Arnold, Y. Zhang, and G. Cao, "Extending drive-thru data access by vehicle-to-vehicle relay," in *Proceedings of the Fifth ACM International Workshop on VehiculAr Inter-NETworking*, ser. VANET '08. New York, NY, USA: ACM, 2008, pp. 66–75. [Online]. Available: http://doi.acm.org/10.1145/1410043.1410055

[35] W. Viriyasitavat, O. Tonguz, and F. Bai, "Network connectivity of vanets in urban areas," in *SECON '09. 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2009*, June 2009, pp. 1–9.

[36] E. Baccelli, P. Jacquet, B. Mans, and G. Rodolakis, "Information propagation speed in bidirectional vehicular delay tolerant networks," in *2011 Proceedings IEEE INFOCOM*, April 2011, pp. 436–440.

[37] Y. Fallah, C.-L. Huang, R. Sengupta, and H. Krishnan, "Analysis of information dissemination in vehicular ad-hoc networks with application to cooperative vehicle safety systems," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 1, pp. 233–247, Jan 2011.

[38] S. Lanzisera, D. Lin, and K. Pister, "RF Time of Flight Ranging for Wireless Sensor Network Localization," in *2006 International Workshop on Intelligent Solutions in Embedded Systems*, 2006, pp. 1–12.

[39] A. Sikora and V. Groza, "Fields Tests for Ranging and Localization with Time-of-Flight-Measurements Using Chirp Spread Spectrum RF-devices," in *IEEE Instrumentation and Measurement Technology Conference Proceedings, 2007 (IMTC 2007)*, 2007, pp. 1–6.