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. These schemes maximize their performance when all the vehicles advertise correct information about their positions, and hence position errors 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 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. One of the main applications of VANETs consists in improving traffic safety by means of efficient warning message dissemination. There, any vehicle detecting a dangerous situation is deemed to notify the anomaly to nearby vehicles that could face the same problem later on. This is achieved through multihop 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.

Regarding dissemination schemes for critical applications, among the existing mechanisms to improve warning message dissemination in VANETs by making use of information about neighbor vehicle positions, two of the most recent and effective algorithms are the *enhanced Message Dissemination based on Roadmaps* (eMDR) [1] and the *Urban Vehicular broadCAST* (UV-CAST) [2]. In eMDR, the receiver vehicle is allowed to forward the message if sender and receiver are located in different streets, or the receiver vehicle is the closest to the geographic center of a junction, obtained from integrated GPS maps. The UV-CAST algorithm assigns a Store-Carry-Forward (SCF) task to those vehicles in disconnected regimes that have a small expected time before they see new neighbors, obtained as the boundary vehicles of the neighbors in communication range. Both eMDR and UV-CAST are designed to blindly trust the information provided by other vehicles. Hence, location errors due to positioning malfunction or attacks can seriously affect performance.

A distributed neighbor position verification mechanism for wireless networks is proposed in [3]. 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, there can be an important delay between the beginning of the process and the verification of neighbor positions, making it unsuitable for urgent warning messages dissemination.

In this paper, we propose a Cooperative Neighbor Position and Verification (CNPV) protocol based on a proactive approach. Our scheme is fully distributed and 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. 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 informed nodes.

The rest of the paper is organized as follows. Section II presents our proactive neighbor position verification algorithm. Section III details the simulation environment used for the performance evaluation, whose results are presented and discussed in Section IV. Finally, Section V concludes the paper.

II. The CNPV protocol

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

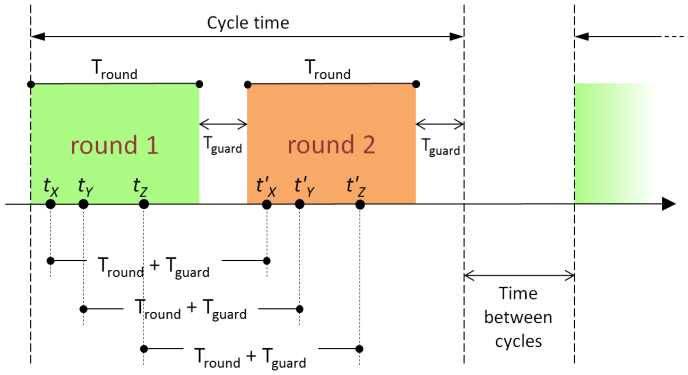

Fig. 1. Temporal detail of the proactive neighbor position verification algorithm.

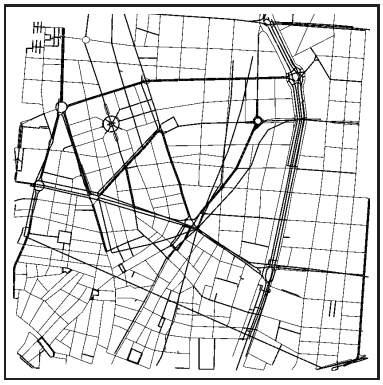

Fig. 2. Scenario of Madrid (Spain) used in our simulations as street graph in SUMO.

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 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 can be fulfilled by equipping vehicles with GPS receivers. In addition, vehicles are capable of performing Time of Flight (ToF)-based Radio Frequency (RF) ranging [4] with a maximum error equal to ϵ_r. This technique is used to calculate distances between the sender and the receiver of a given message. As discussed in [5], this is a reasonable assumption, although it requires modifications to off-the-shelf radio interfaces.

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.

A. CNPV Protocol Message Exchange

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***: 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, 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 anonymous message.

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.

B. 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 [3].

- *Direct Symmetry (DS) Test*: If the distance calculated using the time of flight of radio signal is less than the maximum range of the Radio Frequency (RF), a coherence test is performed between the calculated distance and the position announced by the neighbor.
- *Cross-Symmetry (CS) Test*: Pairs of nodes, such that the two nodes and the verifier node are within communication range, are compared using the same criteria as in the DS test.
- *Multilateration (ML) Test*: Used to detect suspicious situations where nodes have deliberately ignored to announce the links they have with other nodes.

III. 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

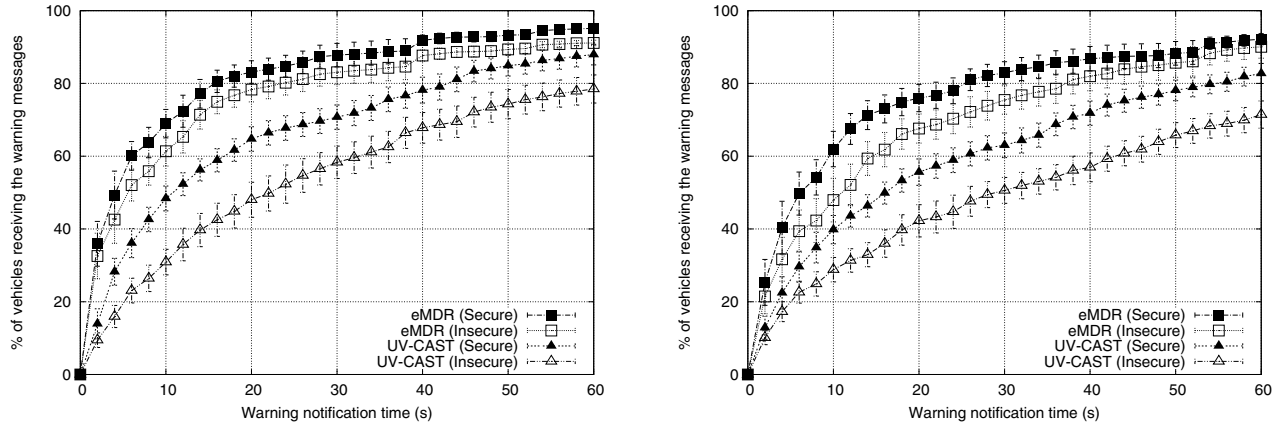

Fig. 3. Warning notification time in Madrid with 200 vehicles varying the percentage of adversaries: (a) 3%, and (b) 9%.

actual implementation. The scenario selected corresponds to the street map around Paseo de la Castellana in the city of Madrid (Spain), shown in Figure 2, which is an example of European city with irregular layout different from synthetic Manhattan-grid scenarios. The road layout was obtained from OpenStreetMap [6], representing a 4-km^2 square area.

Vehicular mobility is generated with the CityMob for Roadmaps (C4R) tool[1], based on SUMO [7] but incorporating the Downtown Model [8] to represent traffic not uniformly distributed, being driven by points of interest that attract vehicles. Network simulations were carried out using the ns-2 simulator [9], modified to include the IEEE 802.11p [10] standard so as to closely follow the upcoming WAVE standard. The simulator was also modified to make use of the Real Attenuation and Visibility (RAV) propagation model [11], 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. 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%, 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.

In the case of the eMDR algorithm, vehicles closer to roadmap junctions have an advantage over their neighbors. Hence, a simple attack against this algorithm consists in announcing bogus positions very close to the junction coordinates. Detecting a neighbor in a more appropriate location, nearby vehicles will refrain from forwarding the message.

Regarding the UV-CAST protocol, the Store-Carry-Forward task is performed by boundary vehicles. 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 scenario.

IV. Simulation Results

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.

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

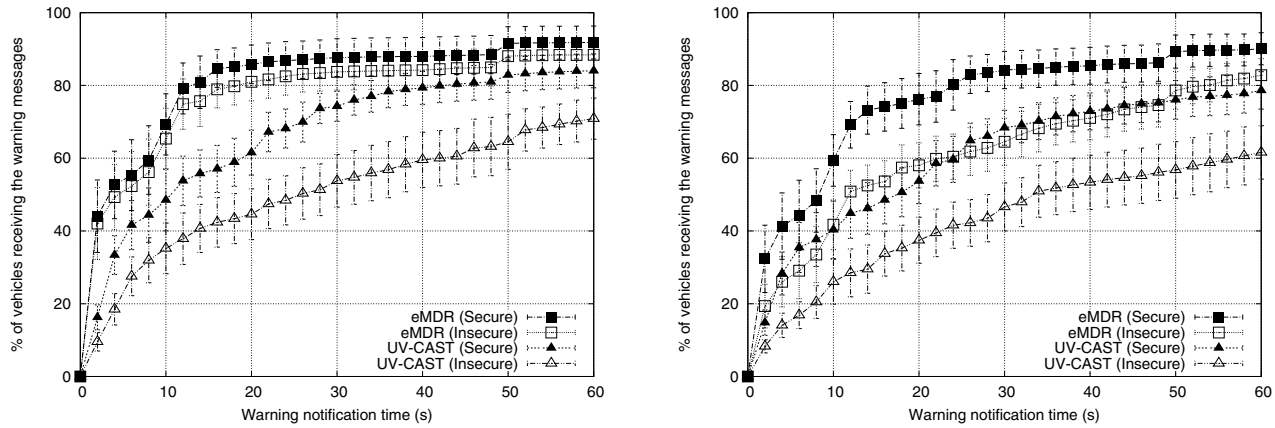

Fig. 4. Warning notification time in Madrid with 400 vehicles varying the percentage of adversaries: (a) 3%, and (b) 9%.

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.

V. 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, specially in schemes like UV-CAST that are especially sensitive to vehicles announcing false positions. 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 informed 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 by the *Diputación General de Aragón* and the European Social Fund (T91 Research Group).

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

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

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.