International Journal of Emerging Technology and Innovative Engineering
IJETIE
Volume 2, Issue 3, March 2016 (ISSN: 2394 – 6598)

Date of Publication: 30.03.2016

# AN EFFICIENT AND SECURE DISSEMINATION OF WARNING MESSAGE IN VANET

P.CHITRA[1], G.ISWARYADEVI[2], P.KARPAGACHITRA[3], M.ANGELIN NITHYA DEVI[4]
Chitraparasuram95@gmail.com,g.iswaryadevi1995@gmail.com
[1,2,3] Student, [4].Asst.Professor
[1, 2, 3,4],PSR RENGASAMY COLLEGE OF ENGINEERING FOR WOMEN

**ABSTRACT**

Vehicular ad-hoc networks (VANETs) provide the communication framework for the dissemination of warning messages to know the position of a vehicle by collecting context information about its neighbor nodes in order to lead the dissemination process. Based on such information, a decision is autonomously taken by the vehicle whether they are the most suitable forwarding nodes. This scheme can provide better performance while all the vehicles promote correct information about their location. At the same time position errors may occur which can degrade the performance of the warning message dissemination process. For that a proactive Cooperative Neighbor Position Verification (CNPV) protocol is proposed that observes advertisement of node's false location and chooses optimal network forwarders reduce the condition of adversarial users. Here the proposed mechanism is combined with two warning message dissemination approaches to demonstrate how the proposed scheme works in the presence of malicious nodes attempting to feat recognized system vulnerabilities. Experimental results show the performance of the proposed security scheme.

**KEY TERMS:** Vehicular ad-hoc Networks, Cooperative Neighbor Position Verification protocol, multilateration and warning message dissemination.

## 1. INTRODUCTION

In the recent years, wireless communication between vehicles have attracted extensive attention for their promise to contribute to be safer, efficient, and more comfortable driving experience in the foreseeable future. The self-organized network formed by such vehicles is referred to as a Vehicular ad-hoc Network (VANET). Generally VANETs are separated as a subset of Mobile ad-hoc Networks (MANETs). [1]. But VANET posses some typical characteristics like; 1. Frequent topology changes during high speed mobility of vehicular node on the

road, 2. challenging conditions of RF signal propagation, 3. no substantial power constraints, and 4. large network that scales requiring up to thousands/hundreds of vehicles. VANETs hold various applications, ranging from road safety via cooperative vehicle awareness to real-time disseminated traffic management. Each safety application is designed to deal with a particular safety aspect and, has a unique communication paradigm. In some applications, vehicles need to be constantly aware of the events in their surrounding environment to prevent some unsafe situation before it occurs [2].

In this paper, our major aim is to reduce the network latency while assuring the accuracy of the collected information when a serious situation takes place. It also provides traffic safety and efficient warning message dissemination. When the participating vehicular nodes discovers an abnormal conditions like accident, slippery road, etc are considered to reveal anomaly to neighboring vehicles which could experience the same trouble later on. This process is attained via multi-hop forwarding in which position information is the fundamental to determine whether to resend the incoming warning message or not. Thus, the context information on vehicle location is primary to the exact operation of the network. Nevertheless, most of the warning message dissemination approaches assume that all the shared context information among the vehicles is precise. Therefore position errors because of a positioning impairment or attacks can critically impress the network performance [3, 4].

Here, the Cooperative Neighbor Position Verification (CNPV) protocol which based on the proactive approach is presented. The proposed scheme appropriates securing warning dissemination protocols at adversarial network environments in which promoted locations are not accurate forever. The proposed CNPV protocol is completely distributed and aggregated with dissemination algorithms which necessitate location information from its communicating neighbors. It appropriates discovering malicious vehicles declaring false position that might not be thought for the transmission of serious information. Finally, CNPV enhances the performance of the warning message dissemination process in adversarial network environments of more than 60% in terms of percentage of uninformed nodes and notification time of warning message.

The rest of this paper is organizes as follows. Section 2 presents the related work on neighbor position localization. Section 3 presents the proposed proactive CNPV algorithm. Section 4 discussed the experimental results and finally, the Section 5 concludes this paper.

## 2. RELATED WORK

Here, we first survey existing localization proposals and location verification of neighbor communication. We then present how current approaches for warning message dissemination utilize context information I order to enhance network performance.

Y. Zeng et al. [5] have proposed a secure localization and location verification scheme that deciding neighbor position in a remote system by utilizing positioning and verification of the location. The process of positioning permits figuring the position of a neighbor subsequent to gathering the information sent by different nodes. The position verification figures out whether the registered location coordinates the true position of the vehicular node. With respect to, self-restriction can be accomplished by Global Navigation Satellite Systems [6]. Own location information can then be reported to adjacent vehicular nodes by utilizing vehicle-to-vehicle committed short-range communication. Furthermore, distinctive existing strategies can be consolidated to discover the neighbors inside of communication extent.

A distance bounding method is portrayed by N. Sastry et al. [7], which influences the

way that every vehicular node has a restricted remote communication range. For our case study, we will depend on time of flight (ToF) estimations of the contrast between the time warning message transmission and reception [8]. Once a vehicular node knows the location of its neighbor nodes, it must guarantee that the promoted locations relate to the true geographic directions; that is it must execute location verification. In the current literature, we can discover a few mechanisms for base or hybrid networks: These give answers for secure limitation of utilizing fixed or moving vehicular nodes safely associated with the certification authority [9], or via multilateration techniques based on the network ranging and time contrast of arrival [10].

The multilateration depends on the distinction of the reception time of a warning message among a majority of vehicular nodes. To be sure, if a source transmits a message, the neighbor nodes will get it at various times, contingent upon their length from the transmitter. By sharing information, we can find the area of the transmitter. Multilateration frameworks are widespread in recent days, and they are utilized by GPS and even in airports to check the loctions of the planes [11].

## 3. COOPERATIVE NEIGHBOR POSITION VERIFICATION (CNPV) PROTOCOL

### 3.1. SYSTEM MODEL

A consideration is made on VANET where the corresponding neighbor nodes of a vehicle are every the nodes that it can attain its destination directly when forwarding. All vehicular nodes are synchronized to a typical time reference, and we expect that every vehicular node can decide its own particular geological location with a maximum error. Both criteria in involving time and geographical location can be satisfied by vehicles fitted with GPS recipients, which is a conceivable presumption given the fast diffusion of this technology in the automotive business.

Moreover, vehicles are fit for performing ToF-based Radio Frequency (RF) extending with a maximum error. To recover the precise transmission and gathering time instants, keeping away from the capricious latencies presented by interrupts activated at the driver level of RF interfaces. For instance, that executed in [12] ought to be adopted. This suggests a timing exactness of around 23 ns that is an average error of 6.8 m, controlled by the 44-MHz clock of standard 802.11a/b/g cards. Besides, the GPS receiver ought to be integrated in the 802.11 cards; software-defined radio solutions integrating coordinating GPS in 802.11 are presented in [13, 14].

### 3.2. OBJECTIVE

The proposed CNPV protocol is proactive, as every vehicular node actively participating in the network periodically transmits its location and the information vital for the operation of the protocol, like other existing forwarding protocols [15, 16]. Subsequently, our methodology is proactive as in vehicular messages are not the solution of unrestricted queries. The proposed CNPV protocol is intended to accomplish two primary targets in a mobile network environment: 1) securing the positions of the neighbors and 2) confirming the accuracy of these positions. The framework is intended to permit every vehicular node to choose whether the positions promoted by its neighbors are exact or not. In this manner, a node allocates one of three conceivable states to each of its neighboring nodes.

The CNPV protocol depends on a cooperative methodology that exploits the broadcasting nature of the remote medium and permits every node to confirm the positions of its communication neighbor nodes via the messages it obtains. We comment that the location validation is controlled by every node freely and that CNPV does not necessitate any trade of the subsequent neighbor states among nodes.

Along these lines, the protocol does not oblige nodes to have worldwide learning of the network or to locate a worldwide concord on the verification of guaranteed positions.

### 3.3. MESSAGE EXCHANGE

The process of proactive verification utilizes a message interchange mechanism that happens in two rounds with the same time duration as follows.

• Round 1: In the first round, every vehicular node partaking in the protocol selects an arbitrary time. At, the vehicular node transmits an anonymous HELLO message, utilizing a newly produced MAC address and containing 1) the vehicular node public one-time use key and 2) a couple of qualities for every neighbor from which has gotten a HELLO in this round. In particular, the pair of qualities alluding to neighbor contains public onetime use key and the time moment at which got HELLO. The HELLO message is gotten by every neighbors of, perhaps at an alternate time moment for every node.

• Round 2: After a consistent guard time meant by, vehicular nodes execute the second round of the protocol. Every nodebroadcasts another message, called DISCLOSURE, at time. DISCLOSURE messages are transmitted after the same request at which the HELLOs were sent by the vehicular nodes, i.e., for every node ,

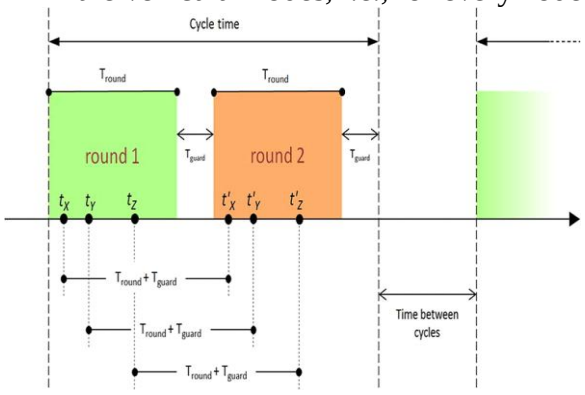


**Figure 1: Timings of the proactive neighbor position verification algorithm**

The CNPV protocol and the message interchange routine are exhibited in Figure 1. Besides, we comment that during Round 1, a vehicular node continues recording the pair of qualities for all neighbor nodes from which it gets a HELLO message, even after getting transmitted its own HELLO. After the message interchange routine is finished, every node can make the communications between the messages sent in the first round and the neighbors that have uncovered their individuality in Round 2.

Besides, every vehicular node recovers from the DISCLOSURE messages the transmission times () of the HELLOs for each of its neighbor nodes. This information, together with the privately stored reception times of the HELLOs, permits every node to utilize ToF-based RF ranging to compute the length that isolates them from their neighbor nodes. Packets got during the second round without a reference from the first round can't be checked; henceforth, they are disregarded until a complete packet exchange is performed.

### 3.4. VERIFICATION ALGORITHM

Once the message interchange is done, it is the ideal opportunity for the node to participate and check the positions promoted by their neighbors. As a result, three tests are later carried out by each of the vehicular nodes, permitting them to figure out whether the positions publicized are exact or not. A more elaborated explanation of these tests, and additionally a mathematical analysis establishing the frameworks of the secure positioning methodology of CNPV, are accessible in [17]. Three tests are conducted for location verification such as: the Direct Symmetry test, the Cross-Symmetry test, and the Multilateration test. In the wake of running the three tests for every communication neighbor, every vehicular node can figure out whether the exchanged information is reliable; subsequently, the neighbor might be took as a potential forwarding node, or it might be viewed as malignant, in which case, the neighbor node is deliberated as faulty and not desirable to rebroadcast the transmitted message.

## 4. EXPERIMENTAL RESULTS

It compares the Warning notification time (s) and % of vehicles receiving the warning messages of e-MDR and UV-CAST algorithms of secure channel. The red line indicates the performance of the e-MDR algorithm and blue line shows the UV-CAST performance. When Warning notification time increases the performance of % of vehicles receiving the warning messages are also increased gradually. Through the comparison graph it is clearly show that e-MDR algorithm provides better performance when compared to UV-CAST algorithm.

## 5. CONCLUSION

Thus, we have exhibited a proactive Cooperative Neighbor Position Verification (CNPV) protocol in which context information exchanged among one-hop neighbor nodes. The proposed CNPV protocol is effectively versatile to various warning message dissemination approaches that make utilization of the neighbor node information to choose the most suitable forwarding methodology in VANETs. CNPV permits verifying the location of the neighbor nodes before choosing the following forwarding vehicle, supporting the dissemination process and constraining the quantity of vehicles that don't obtain the warning messages.

We assessed the performance of the CNPV protocol by pairing it with two dissemination network algorithms such as: eMDR and UVCAST, indicating how 1) the vicinity of adversary vehicular nodes influences the warning message dissemination execution in urban situations and 2) CNPV can decrease the effect of adversarial users in the vehicular system. While applying the proposed technique to deal with the UVCAST approach, we notice that it is especially delicate to vehicles reporting false positions; because the SCF scheme received to achieve new zones in separated regimes is just performed by limit vehicles.

A vehicle broadcasting false data can easily turn the boundary vehicle, maintaining a strategic distance from vehicles with a more great location to accept this part. At last, the proposed simulation results indicate how CNPV enhances the performance of the process of dissemination in adversarial network environments by up to 60% in terms of time of warning notification and rate of ignorant nodes.

## 6. REFERENCES

[1] J. A. Dias, J. J. Rodrigues, and L. Zhou, "Cooperation advances on vehicular communications: A survey," Veh. Commun., vol. 1, no. 1, pp. 22–32, Jan. 2014.

[2] J. A. Dias, J. J. Rodrigues, and L. Zhou, "Performance evaluation of cooperative strategies for vehicular delay-tolerant networks," Eur. Trans. Emerging Telecommun. Technol., vol. 25, no. 8, pp. 815–822, Aug. 2014.

[3] E. Schoch, F. Kargl, and T. Leinmüller, "Vulnerabilities of geocast message distribution," in Proc. IEEE Workshop AutoNet Appl., 2007, pp. 1–8.

[4] Q. Xu, T. Mak, J. Ko, and R. Sengupta, "Vehicle-to-vehicle safety mes-saging in DSRC," in Proc. ACM VANET, Oct. 2004, pp. 19–28.

[5] Y. Zeng, J. Cao, J. Hong, and L. Xie, "Secure localization and location verification in wireless sensor networks," in Proc. IEEE 6th Int. Conf. MASS, Oct. 2009, pp. 864–869.

[6] P. Papadimitratos and A. Jovanovic, "GNSS-based positioning: Attacks and countermeasures," in Proc. IEEE MILCOM, San Diego, CA, USA, Nov. 2008, pp. 1–7.

[7] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in Proc. ACM Workshop WiSe, San Diego, CA, USA, Sep. 2003, pp. 1–10.

[8] J.-H. Song, V. Wong, and V. Leung, "Secure location verification for vehicular ad-hoc networks," in Proc. IEEE

GLOBECOM, New Orleans, LA, USA, Dec. 2008, pp. 1–5.
[9] S. Capkun, K. Rasmussen, M. Cagalj, andM. Srivastava, "Secure location verification with hidden and mobile base stations," IEEE Trans. Mobile Comput., vol. 7, no. 4, pp. 470–483, Apr. 2008.
[10] S. Capkun and J.-P. Hubaux, "Securing position and distance verification in wireless networks," Swiss Fed. Inst. Technol. Lausanne, Lausanne, Switzerland, Tech. Rep. EPFL/IC/200443, May 2004.
[11] Multilateration Executive Reference Guide, Creativerge ERA Corp., Prague, Czech Republic, 2013.
[12] M. Ciurana, F. Barcelo-Arroyo, and F. Izquierdo, "A ranging system with IEEE 802.11 data frames," in Proc. IEEE Radio Wireless Symp., Jan. 2007, pp. 133–136.
[13] F. Carpenter, S. Srikanteswara, and A. Brown, "Software defined radio test bed for integrated communications and navigation applications," in Proc. Softw. Defined Radio Tech. Conf., Phoenix, AZ, USA, Nov. 2004, pp. 1–6.
[14] E. D. Re et al., "Software defined radio terminal for assisted localization in emergency situations," in Proc. CTIF Wireless Vitae, May 2009, pp. 554–558.
[15] P. Fazio, F. De Rango, C. Sottile, and A. F. Santamaria, "Routing optimization in vehicular networks: A new approach based on multiobjective metrics and minimum spanning tree," Int. J. Distrib. Sensor Netw., vol. 2013, pp. 598 675-1–598 675-13, 2013.
[16] P. Fazio, F. De Rango, and C. Sottile, "An on demand interference aware routing protocol for VANETS," J. Netw., vol. 7, no. 11, pp. 1728–1738, Nov. 2012.
[17] M. Fiore, C. Casetti, C. Chiasserini, and P. Papadimitratos, "Discovery and verification of neighbor positions in mobile ad-hoc networks," IEEE Trans. Mobile Comput., vol. 12, no. 2, pp. 289–303, Feb. 2013.