# A SURVEY ON POSITION IDENTIFICATION IN VECHICULAR AD-HOC NETWORKS

[1]Prof.B. Anuradha, [2]D.Gowtham Chakravarthy
[1]Associate Professor,[2]PG Scholar
SNS College of Engineering
Coimbatore – 105



## *Abstract*

VANET is a widely discussed area of wireless communication at present. VANET is a subset of MANET where nodes represent vehicles moving at high pace and vehicle traffic determined regularity. Identifying position of each vehicle when the vehicles are moving from one region to other region is a challenging task in VANET. Verifying the position of vehicles is done through different techniques. Here some position identification techniques are analyzed and compared.


## I INTRODUCTION

Vehicles and beacons on roadsides can form a Vehicular Ad Hoc Network (VANET) using the allocated frequency and service to communicate with each other without central access point. Many consider Vehicular ad hoc networks (VANET) as one of the most prominent technologies for improving the efficiency and safety of modern transportation systems. Vehicular Ad Hoc Network shares some common characteristics with general Mobile Ad Hoc Network (MANET). Both VANET and MANET are characterized by the movement and self-organization of the nodes. They are also different in some ways. MANET can contain many nodes that cannot recharge their power and have uncontrolled moving patterns. Vehicles in VANET can recharge frequently, however can be constrained by the road and traffic pattern.

An overview on position-based routing schemes for MANETs can be found in. For VANETs, mainly greedy routing approaches have been proposed. They have in common that the next hop node of a packet has to be closer to the destination's position than the current node. This implies that a node has to know all its neighbors and their respective positions. To achieve that, all nodes send periodic broadcasts of their own position. By this so-called beaconing, every node can build up a neighbor table and base forwarding decisions on it. Two special cases must be handled with greedy forwarding: there might be more than one suitable next hop or there might be no suitable neighbor. A potential source for such false position data is a malfunction of a node's location sensing system. For example, a GPS receiver may wrongly calculate the position of a node because of bad reception conditions. Whereas malfunctioning nodes may degrade the performance of a system to some extent, malicious nodes may cause even more harm. The intents of an adversary may range from simply disturbing the proper operation of the system to intercepting traffic exchanged by ordinary users, followed by a potential modification and retransmission.

## II MULTIHOP LOCATION VERIFICATION PROTOCOL (MHLVP)

Osama Abumansoor et.al,[1] suggested that the Location verification protocol is to verify a questioned vehicle and its announced location using a cooperative multihop approach whenever direct verification and communication are not possible.

*A. Assumptions*

The protocol is based on the following general assumptions:

1) Each vehicle is capable of determining its own position and mobility information using a data fusion model of existing technologies such as GPS, map matching, a digital compass, and accelerator meters . By using improved GPS technologies such as differential GPS or augmented GPS, accurate position estimation can be achieved (error < 1 m). Position errors tend to affect the position accuracy of all the vehicles in the same area [2], [9]. Hence, relative position computations using GPS coordinates are acceptable.

2) Vehicles are able to verify direct neighbors with direct line of sight using the received radio strength signal (RSS) and calculating the sender's relative distance [12].

3) Communication channels between vehicles are secure. Exchanged messages are digitally signed, and vehicles are able to authenticate the message sender [3], [5]. We assume that an outsider will not be able to inject false information. All protocol messages are sent by legitimate nodes and carry their true position and mobility information. With such an assumption, we focus our work on securing the integrity of the collected position information.

4) Energy consumption and computation resources are not a major concern in VANETs.

*B. Position Verification Computation*

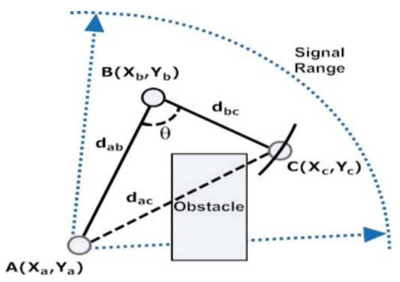


Fig. 1.1 Trilateration Technique

The position computation for the proposed protocol is based on triangulation calculations. In Fig. 1.1, node *A* wants to verify node *C*'s location; however, direct communication is not possible due to the existence of an obstacle. While node *B* can communicate directly with both *A* and *C*, each node knows its GPS position (*x*, *y*) in a two-dimensional plane. Node *A* sends a request to node *B* to verify location *C* with its announced position ($x_c$, $y_c$) and mobility vector. *B* can verify *C*'s location by determining its distance using radio measurements, such as RSSI, and comparing the announced and measured values. If both values are a match, *B* will send a response back to *A* containing the distance $d_{bc}$ and verifying the location of *C*.

II POSITION VERIFICATION APPROACH

Tim et al,[6] suggested that, the concept of a "Position Cheating Detection System" similar to intrusion detection systems to detect, for example, selfish nodes in MANETs [10]. In these systems each node uses multiple sensors to detect malicious or selfish behavior of nodes in the network. Based on the sensors' observations, each node calculates a trust value that determines whether nodes are trustworthy or should e.g., be excluded from further routing decisions. Such a system can predict the trustworthiness of other nodes even when single sensors do not work reliably to hundred percent.

- *Verification Sensors*

The accumulation of observations over time and sensors is required to provide the decision of whether a node is to be regarded as being malicious or not. Also knowing that observations from some sensors are more reliable than observations from other ones, we use a trust model that provides the capabilities to consider observations from differently weighted sensors during a certain period of time. The mathematical model mainly derives from the one presented in [11].

When we denote the *n*th observation of sensor *s* by $\sigma^s_n$, the trust model can be described as follows:

• All nodes store trust values $r \in [-1; 1]$ for all direct neighbors. $r = 0$ is equivalent to neutral trust, $r \in (0; 1]$ means a node is trustworthy, and $r \in [-1; 0)$ means no trust. Every observation $\sigma^s_n$ is stored with timestamp $t^s_n$ .

• On the arrival of a new observation, the trust value for a neighboring node is recalculated according to the collected observations for this node.

• All observations are stored for a maximum time *T* and discarded afterwards. weight factor $w^s$ of an observation $\sigma^s_n$

is chosen according to the reliability of the providing sensor, for example, observations from a more reliable sensor like ART can be regarded as more valuable than observations from a less reliable one like Mobility Grade Threshold (MGT) sensor (see the next section for a description of sensors). Besides, observations may also be weighted dynamically (e.g., if a sensor delivers observations different reliability each).

The timestamp $t^s_n$ of an observation $\sigma^s_n$ is used to calculate the observation's time factor $w_t(t, t^s_n)$

The trust value $r_t$ of a neighbor node at a time $t$ is calculated by multiplying the available observations by their weight factor and their time factor, then summarizing the results and at the end normalizing to [–1; 1]. Detected violations are weighted higher than observations of normal behavior; thus, once falsified position information is detected, it takes several correct beacon messages to compensate the trust level. In the routing protocol, location information is distributed between nodes by means of position beacons. In order to prevent abuse of the verification system, beacons need to be authenticated and timestamped by their sender. When a node receives a position beacon from another node, claiming to be at a certain position, the sensors become active in order to verify if this claim is likely to be correct or not.

## III POSITION IDENTIFICATION WITH NEIGHBORS

Ren *et al,* [7] used two directional antennas ( f-antenna and b-antenna ) to process a position verification algorithm that computes the relative position with respect to neighbors. The node constructs front and back group bit vectors and periodically sends group information to neighbors .The Inter-vehicle communication among has great deals and vehicles plays an important role in providing a high level of safety and convenience to drivers. Geographic routing protocol has been identified to be suited as a result of the special nature of vehicular ad hoc networks (VANETs), such as high dynamic mobility and large network size. Although there is considerable functional research about geographic routing, the security aspects have not been vastly concentrated on so far.

The vehicular wireless network on the highway scenario, assume there are two directional antennas on every vehicle. The benefit of using directional antenna includes longer ranges as well as the reduced co-channel interference. The malicious nodes are randomly deployed in the networks. Geographic routing, e.g. GPSR, is a stateless protocol which makes localized optimal choice of next hop and achieves the global optimal routing path. Particularly, at every intermediate node, the farthest neighbor closest to the destination will be chosen as the next hop. Therefore, to affect the network performance, a malicious node could fake its position as the farthest one. Due to the nature of geographic routing, if the node selection of one hop is guaranteed to be safe, all nodes along the routing path can be trusted. Therefore, consider the detection of malicious nodes within one-hop neighbors instead of the entire networks.

## IV SECURE LOCATION VERIFICATION (SLV) SCHEME

Song *et al.* [6] proposed an infrastructureless cooperative protocol to detect false position announcements by measuring the ToF to evaluate the subject node against distance reduction.

Using another neighbor, the vehicle can then verify the location of a node for distance enlargement using ellipse computation with foci located on the vehicle and its assisting neighbor's position. The position of the assisting neighbor, with respect to the verifier and the questioned node, has an impact on the computation's results

SLV scheme uses three main steps to verify the location of the prover,

- RF-based distance bounding technique is used to bound the minimum distance between verifier *V* and prover *P*. Since RF signals travel at the speed-of-light *C*, *V* can prevent an attacker from reducing the measured distance by measuring the Time of Fight (ToF) of challenge response messages between *V* and *P*. Since *P* can only cheat on its response message by appearing further from *V* than its actual location, any attempt to reduce the distance will be detected by *V*. When *V* estimates the distance to *P*, *V* also considers the non-zero processing delay $\delta$ of *V*.

- After receiving a response message from *P*, *V* executes the following plausibility check in sequence to verify the claimed location *P*. To include a roadway map is to verify the vehicle's location.

*Acceptable transmission range*: Since there is a maximum transmission limit in each wireless communication device, *P* cannot claim to be located further away than the maximum transmission range of *V*.

*Acceptable speed limit*: Since the speed of vehicles cannot exceed either the mechanical or lawful limit, no vehicle can move farther away than the maximum feasible distance during two consecutive beacon messages.

*Roadway map*: After receiving a response message from *P*, *V* can refer to its roadway map to verify whether the claimed location *P* is on the roadway or not.

- If the claimed location *P* passed all plausibility checks, *V* chooses a common neighbor *B* of both *V* and *P*. Then, *B* gives an estimated location of *P* to the ellipse with foci at both *V* and *B*, and the map of roadway. If the estimated location of *P* is not within a certain error distance of the ellipse, *B* can detect the distance enlargement of *P*. *P* can be detected when *V* estimates the distance to *P*. *V* also considers the non-zero processing delay $\delta$ of *V* .

## V PROVIDING VANET POSITION INTEGRITY THROUGH FILTERING

Yan *et al.* [8] proposed a filtering method to provide position integrity using box counting over a grid plane. By plotting the gathered position information, the grid with the largest amount of information is selected and used to compute the position .The Filtering method is used to provide position integrity using box counting over a grid plane. By plotting the gathered position information, the grid with the largest amount of information is elected and used to compute the position. Position Integrity through Filtering is the efficient method for positioning a vehicle in a noisy environment including malicious attackers and measurement errors. By assuming the majority vehicles are honest and report the detection of position of other vehicles to provide vehicle position integrity in Vehicular Ad hoc Network (VANET). The noise input includes bogus position information and position with measurement errors in VANET.

Given such noisy input, the algorithm estimates the high resolution location of a vehicle by filtering the malicious location input and by refining low resolution location input. Neighborhood awareness allows a vehicle to know about the presence, location and even speed of neighboring vehicles. Today, new vehicles may have network devices, computing devices, and storage devices. Specifically, vehicles represented in this proposal are assumed to be endowed with the following features:

- A GPS receiver. The GPS receiver is going to provide the position information which is the location input in a two dimensional plane. The location input includes measure errors and can be modified by malicious attackers as well. Therefore the location input received by the observer is contaminated.
- A wireless transceiver, using Dedicated Short Range Communications (DSRC) for fast communications, that the data can be changed here by attackers for position attacks.
- A computer center, which will provide data processing, computing and storage.
- A unique ID, like electronic vehicle plates which is a infrared device and is issued by a registration authority annually. This device can periodically broadcast its ID to neighboring vehicles.

Position information is fundamental and important in vehicular wireless networks, adversaries, such as pranksters and malicious attackers, can perpetrate the following position related attacks:

*Fabrication Attacks*: Create a bogus message or lie about congestion position.

*Alteration Attacks*: Modify the position in the message.

*Replay*: The attacker re-injects previously received packets into the network. For example, the attacker can poison a node's location information by replaying beacons.

| Authors | Verification | Detection | Filtering | Infrastructure |
|---|---|---|---|---|
| Osam et.al | Trilateration | __ | __ | Yes |
| Tim Leinmuller et.al | __ | Sensors | __ | No |
| Song et.al | Signal analysis | Distance enlargement | __ | No |
| Ren et.al | Directional antenna | Detection Rule I & II | __ | No |
| Yen et.al | Filtered data | __ | Grid map | No |

Table No. 1 Comparisons of various Position Identification Techniques

- Filtering Malicious Data

The basic idea of filtering the malicious data from the collected data is by a method called box counting. The data is placed on a panel. For one dimensional data, the panel is on a straight line. For two dimensional data, the panel is on an area with x-y axis. The location data is the GPS coordinates in a two-dimensional scenario. The panel is partitioned into grids. For each grid/multi-grid count the number of positions. Since the majority vehicles are honest, to select the grid with highest number of vehicles. Inside this grid, then can partition it into more refined grids and repeat the filtering process until the malicious positions are removed.

*Gridding:* The granularity of grid is a key issue. If the granularity is big, the malicious position will be included. If the granularity is small, the final position will deviate from the right position.

*Filtering:* After gridding, the panel is partitioned into grids. The collected data is placed on the panel, count the number of positions in each grid. The grid with the largest number of positions will be found. If there is more than one grid with the same largest number of positions, then merging with other grids to find a bigger grid. If these grids are adjacent, these grids will be merged into a bigger grid. For a grid, there are usually 8 neighboring grids (grids at edges of the data panel have at most 5 neighboring grids).

CONCLUSION

In this paper, we compared some of the position identification techniques. These techniques are used to identify the position of moving vehicles, by applying these techniques we can obtain the solutions for identifying the false positioning nodes, malicious nodes, and cheating beacon nodes.

REFERENCES

[1] Osama Abumansoor, Azzedine Boukerche, "A Secure Cooperative Approach for Nonline-of-Sight Location Verification in VANET" *IEEE Trans. on Vehicular Technology*, VOL. 61, NO. 1, Jan 2012.

[2] A. Boukerche, H. Oliveira, E. Nakamura, and A. Loureiro, "Vehicular ad hoc networks: A new challenge for localization-based systems," *Comput. Commun.*, vol. 31, no. 12, pp. 2838–2849, Jul. 2008.

[3] 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 Commun. Mag.*, vol. 46, no. 11, pp. 100–109, Nov. 2008.

[4] T. Leinmüller, E. Schoch, and F. Kargl, "Position verification approaches for vehicular ad hoc networks," *IEEE Wireless Commun.*, vol. 13, no. 5, pp. 16–21, Oct. 2006.

[5] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in vehicular ad hoc networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 88–95, Apr. 2008.

[6] J.-H. Song, V.W. S.Wong, and V. C.M. Leung, “Secure location verification for vehicular ad-hoc networks,” in *Proc. IEEE Global Telecommun. Conf.*, 2008, pp. 1–5.

[7] Z. Ren, W. Li, and Q. Yang, “Location verification for VANETs routing,” in *Proc. IEEE Int. Conf. Wireless Mobile Comput., Netw. Commun.*, 2009, pp. 141–146.

[8] G. Yan, X. Chen, and S. Olariu, “Providing VANET position integrity through filtering,” in *Proc. 12th Int. IEEE Conf. Intell. Transp. Syst.*, St. Louis, MO, 2009, pp. 1–6.

[9] M. Schlingelhof, D. Betaille, P. Bonnifait, and K. Demaseure, “Advanced positioning technologies for co-operative systems,” *IET Intell. Transp. Syst.*, vol. 2, no. 2, pp. 81–91, Jun. 2008.

[10] F. Kargl *et al.*, “Advanced Detection of Selfish or Malicious Nodes in Ad Hoc Networks,” *Proc. 1st European Wksp. Security in Ad-Hoc and* Sensor Networks (ESAS 2004), Sept. 2004, pp. 152–65.

[11] P. Michiardi and R. Molva, “CORE: a Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks,” *Proc. IFIP TC6/TC11 6th Joint Working Conf. Commun and Multimedia Security*, Deventer, The Netherlands, 2002, pp. 107–

[12] R. Parker and S.Valaee, “Vehicular node localization using received signal- strength indicator,” *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3371–3380, Nov. 2007.

## Authors Profile

**Prof. B. Anuradha** obtained her bachelor’s degree in Computer Hardware and Software Engineering from Avinashilingam University and Masters Degree in Embedded systems from Anna University and currently pursuing her Ph.D from Anna University of Technology, Coimbatore. She has more than 10 years of teaching experience and currently, she is working as Associate Professor in Department of Computer Science and Engineering, in SNS College of Engineering, Coimbatore, and Tamil Nadu. Her areas of interest include Embedded System, Operating Systems and Computer Architecture.

**D. Gowtham Chakravarthy** received his B.E., degree in Computer Science & Engineering from Sri Ramakrishana Institute of Technology, Coimbatore, in 2011. Currently pursuing M.E., in Computer Science & Engineering from SNS College of Engineering, coimbatore. His area of interest includes MANET, VANET

 