Position Verification for Vehicular Networks via Analyzing Two-hop Neighbors Information

Mervat Abu-Elkheir[1] Sherin Abdel Hamid[1] Hossam S. Hassanein[1] Ibrahim M. Elhenawy[2] Samir Elmougy[3]

[1] School of Computing, Queen's University, Kingston, ON, Canada
[2] Computer and Information Sciences, Zagazig University, Zagazig, Egypt
[3] Computer and Information Sciences, Mansoura University, Mansoura, Egypt
{mfahmy, sherin, hossam}@cs.queensu.ca henawy2000@yahoo.com mougy@mans.edu.eg

Abstract— **Vehicular networks will enable vehicles on the road to utilize wireless communication to exchange safety information; enhancing traffic flow and minimizing accidents. With vehicle positions being the most frequently exchanged information in vehicular networks; it becomes imperative to establish a strong level of trust in the announced positions before a vehicle may take action in response. This paper proposes a position verification scheme that involves the collaborative exchange of one-hop neighbor information in order to help a vehicle make better judgments of position announcements. Vehicles can assess neighborhood connectivity and use the logical traffic flow to form a verdict on trusting a position announcement, thus enabling the detection of possible position falsifications. The scheme analyzes accumulated 2-hop neighbors' information in order to define a plausibility area within which a vehicle should exist in order for its position to be considered "correct". In very sparse traffic scenarios, a vehicle will depend on measuring the consistency of a vehicle's Received Signal Strength (RSS) with its announced position. Performance evaluation was carried out via simulation, and results show that defining this plausibility area yields accurate detection of position falsifications with low false positives.**

Keywords-component; vehicular networks; position verification; security; VANETs

I. INTRODUCTION

Vehicular networks will enable vehicles on the road to use wireless communication to exchange safety information, which is expected to help enhance traffic flow efficiency and minimize accidents. A vehicular network will consist of vehicles, equipped with sensors (GPS, Radar, speedometers, etc.) and communication equipment. Vehicles will be able to communicate with each other as well as with infrastructure Road Side Units (RSUs), which can provide vehicles with a multitude of services, such as downloading updated digital road maps. RSUs will typically exist at intersections and along high-profile highways at the beginning of deployment, so a system design should not depend solely on RSUs in its functionality, hence the term Vehicular Ad hoc Network (VANET) is commonly used to refer to vehicular networks that function in an ad hoc mode and do not depend solely on infrastructure in their operation.

Most of the envisioned applications of vehicular networks assume the knowledge of vehicles' locations, which is realized via the exchange of periodic position information among vehicles. The required level of accuracy of such information is usually high for safety applications [1], [2]. Therefore, it becomes imperative to ensure the integrity of position information. This involves ensuring that the location information received is actually from the original sender and the location information is correct; not forged nor modified. Incorrect position announcements can be the result of temporary sensory malfunctions, or the deliberate efforts by some drivers to abuse the vehicular network in order to enhance their own traffic conditions, or even worse, disrupt the functionality of the network and perhaps cause accidents. The IEEE 1609.2 Wireless Access in Vehicular Environments (WAVE) standard for security services in vehicular networks [3] addresses authentication and some privacy issues, but it only provides entity authentication (via proper vehicle identification) and message integrity (via encryption). The standard does not provide means for a receiving vehicle to verify the contents of a message sent by an authenticated vehicle before action may be taken based on that content. This calls for the need to develop misbehavior detection mechanisms that will enable the verification of falsified information that could potentially exist in received messages.

The requirements of accurate position information, together with the intermittent availability of an infrastructure that would reliably support such information accuracy, establish the need to have cooperative mechanisms that utilize the communication capabilities of vehicular networks to provide accurate localization of vehicles. There is a need for ad hoc and distributed verification and misbehavior detection schemes that achieve these high-accuracy requirements for position information. The primary goal of misbehavior detection in vehicular networks would be the verification of information in order to help prevent system misuse, rather than the identification and tracking of individuals sending such information. This is mainly because of the limitations on instant identification that could be imposed by the realization of privacy protection measures, something that is of high priority in vehicular networks.

This paper proposes a position verification scheme that relies on the exchange of one-hop neighbors' information among vehicles. Exchanging one-hop neighbor information would extend the local view of a vehicle node and enable it to

978-1-61284-928-7/11/$26.00 ©2011 IEEE

better assess the situation in its local neighborhood. The main motivation for this approach is that the limited ability of a vehicle to autonomously verify the position information sent by other vehicles would necessitate a form of consolidation of information in order to establish a higher confidence in the location information sent within the vehicle's local neighborhood. The proposed verification scheme is designed to be efficient and lightweight so that a vehicle would be able to verify a sender in real-time with no reliance on global knowledge of the network. A vehicle will perform a series of logical assessments in order to determine if it should trust the position information announced by other vehicles in its communication range. These assessments are derived from the geographical characteristics of traffic directions and assumptions made about the vehicular environment. It has been shown that data delivery would be highly affected by vehicles themselves being obstacles to radio propagation, leading to a vehicle's connectivity being limited to nearer neighbors [4]. In addition, the transmission range in vehicular networks is expected to degrade to as little as 100m in dense scenarios [5]. The proposed verification procedure would benefit from these observations to detect potential position falsification attempts. It is reasonable to assume that, given the nature of traffic flow, a vehicle's transmission would be received by the neighbors who are physically close to it, typically in a linear fashion. That is, most of the time, vehicles can assume a linear chain of "transmission"; a vehicle will be able to hear immediate neighbors' transmissions and verify them based on road characteristics and radio measurements, and then use those neighbors' information to verify future position announcements by other vehicles. In order to support verification in situations without neighbors' information to help a vehicle form a decision, our scheme will resort to measuring the Received Signal Strength (RSS) from a sending vehicle and compare its measurements with the hypothetical measurements that should have been detected given the sending vehicle's announced position, while allowing a certain margin of error to account for the unstable nature of RSS measurements. Although RSS cannot be fully depended upon to reliably estimate the distance between two vehicles, RSS is in general inversely proportional to the actual distance, so it will provide an initial estimate of the relative position of a sender until further information is available to the vehicle.

The rest of the paper is organized as follows. Section II describes the related work that has been done in position verification for vehicular networks. In Section III, the proposed position verification scheme is introduced and its functionality is explained. Section IV includes a description of simulation and results. Finally, Section V concludes the paper.

II. Related Work

Position verification approaches can be grouped under three main categories: hardware-assisted, parameter-based, and model-based approaches.

In *hardware-assisted solutions*, a vehicle would utilize special hardware installed on board or dedicated infrastructure to verify other vehicles. Hubaux et al. [6] propose the use of infrastructure to perform verifiable multilateration. The basic idea is having three or more Road Side Units (RSUs) to send a synchronized challenge-response message to a vehicle and verify its position based on the consistency in response time calculations. This approach depends heavily on infrastructure that is dedicated to vehicular networks and involves tight synchronization requirements. Radar and GPS were proposed to be used for position verification in [7], where a vehicle's announced location is verified using both radar and GPS readings. The vehicle is assumed to have GPS navigation system and front and rear radars. A history of movements is built for observed vehicles based on the vehicle's own radar readings of neighbor vehicles and the readings sent by other vehicles from oncoming traffic, and this history is used to screen forged data. In [8], the proposed solution depends on two directional antennas to exchange messages between vehicles and two groups of neighbors; those in front of the vehicle and those in the back. Each vehicle periodically sends a message containing its location together with its own two lists of front and back neighbors. A vehicle will decide on the relative positions of its one-hop neighbors based on the messages it receives. The directional antennas approach handles location verification in highway scenarios, and is not expected to be extendable efficiently for urban scenarios where there are intersections.

In parameter-based solutions, network-specific parameters are measured in order to assess whether they are consistent with the expected behavior of the network. The concept of plausibility checks was proposed in [9], where vehicles autonomously check whether an announced node's position is within a degree of accuracy from the actual node's position, based on acceptable values of some network and traffic parameters, such as packet's timestamp's consistency with current time; acceptance range, which assumes that no neighbor is further than the maximum transmission range; and velocity, which builds upon the reasoning that a claimed position update should be within a predicted space window calculated using the vehicle's previous position and the maximum physical velocity allowed. This approach assumes that the transmission range is fixed and does not account for more sophisticated traffic scenarios. Distance bounding and logical evaluation of vehicles positions was proposed in [10]. The basic proposal involves an infrastructureless, verifier-prover solution that is based on cooperative evaluation of vehicles positions, mainly to detect distance enlarging fabrication. The solution extends the plausibility checks notion to being performed by the receiver and the common neighbors between the verifier and the sender. This is done by choosing a common neighbor that will give an estimated location of the prover. If that estimated location is not within a certain error distance of both verifier and neighbor, the prover is considered to be lying about his location. The solution depends on the assumption that a prover can provide an upper bound on its processing delay and this upper bound is fixed and known to other vehicles. Round trip propagation time and time-of-flight are used in [11] with three-way exchange of token beacons between sender and receiver, with no reliance on neighbors feedback.

In model-based solutions, a model of the normal behavior of the system is built, and subsequent actions taking place within the system are compared to that normal profile to identify any abnormalities that could indicate malicious behavior. In vehicular networks, this model can be either of the network itself (i.e. the vehicles' relative positions) or the individual trajectories of vehicles as they move. The approach in [12] depends on each node maintaining a model of the VANET with all the knowledge the node has of the network. A vehicle would depend on its local sensors to determine how many neighbors are currently present and uses this information to build a model of the network, and then it builds possible explanations of any subsequent inconsistent data against that model based on the possible presence of malicious nodes. In [13], Nodes maintain and periodically broadcast private databases that contain information about detected and observing nodes. When a broadcast is received, the contents are merged into the receiving node's database. A node periodically attempts to explain the events in its database; it tries to find the scenario with the least number of malicious nodes. Performance complexity of this scheme is not good due to having to examine a big search space of all possible explanations in a certain scenario.

There are solutions that carry a mix of both parameter and model based approaches. The works in [14], [15] use multiple sensors to monitor and calculate trust values for position information. Autonomous sensors work individually and each result contributes to the node's overall local trust rating of neighbors. These sensors are used mainly in sparse scenarios. Example sensors that will fit this category are the acceptance range threshold, accepted mobility threshold, maximum density threshold, and map verification. Cooperating sensors are used in dense scenarios and depend on information exchange between neighbors to verify positions.

III. Two-Hop-based Position Verification

A. Problem Statement

Location information is expected to be exchanged among vehicles either in the form of periodic beacons for traffic flow enhancement purposes; or as event-based alerts of sudden incidents or abnormal road conditions, also with location information – both about the vehicle and the alert – together with a description of the alert [16]. Beacons are received by one-hop locally bounded neighboring vehicles, and alert messages are relayed from the vehicle(s) detecting the event to all the vehicles within a zone of relevance. Both types of messages are assumed to be authenticated at the receiver using the public/private key pair-based digital signature verification.

The focus of the proposed scheme will be on the verification of position information included in periodic beacons. Periodic beacons are assumed to carry a vehicle's ID, position, speed and general heading (direction), typically recorded from GPS devices.

The problem then can be represented as a question: Given a vehicle V which has a set of neighbors N that it receives beacons from, how can V verify the position information sent by all of N? In the following subsection, a description of the nature of information that would be available to a vehicle at a certain point in time is given, together with the proposed scheme to verify a position announcement based on this information. The following conditions are assumed in a vehicular environment:

- *Self-trust*: A vehicle trusts the information it collects via its own sensors.
- *Honest majority*: The majority of vehicles on the road are honest.
- *Temporal behavior consistency*: There is no guarantee that previously honest nodes will not become malicious, but vehicles –while on the move during a trip lifetime- will maintain temporal honest or malicious behavior. Judgments are made on a per announcement basis, with only the most recent observations of a vehicle taken in account.
- *Knowledgeable and mobile attacker*: Attacker knows communication protocols and message formats, and his movement is restricted to the road network. Attackers generate position announcements abiding by the road network.

B. Verification Scheme

A typical road scenario is shown in Fig. 1, where a node V_1 is sending a falsified position announcing that it is at $V_1^{'}$. If the transmission range of vehicles is not fixed – as is expected by the studies of vehicle networks propagation characteristics – it would be difficult for a vehicle to depend on a sharp cutout of communication range in order to rule out implausible position announcements. Instead of depending on hard thresholds, the proposed verification scheme depends on logical evaluation of a vehicle's neighborhood via the exchange of one-hop neighborhood information between neighbor vehicles in order to build 2-hop neighborhood connectivity. This connectivity information will allow a vehicle to obtain information about other vehicles positions history and whether there are verdicts against them by the vehicle's neighbors.

A vehicle's neighborhood can be characterized by the existence of closely nearby vehicles from which direct transmissions can be heard, and further vehicles whose transmissions will be obstructed by those direct in-between vehicles and other road obstacles, as concluded from the observations made in [4]. Assuming that direct neighbors are physically closer to a vehicle and indirect neighbors are further and only "seen" by direct neighbors, then we can define a "plausible area" within which a sender is expected to exist. This plausible area will be defined using the information a vehicle collects from its direct neighbors, both about the most recent encounters with the sender if they exist and about the two-hop neighbors that are not directly connected with the receiver. In order for a vehicle to obtain this information about prior observations of a sender and potential two-hop neighbors for verification purposes, vehicles need to periodically exchange their position information as well as the position information of their direct neighbors. The proposed verification beacon structure is abstracted in Fig. 2, where a vehicle would include its own position information (i.e. *xy* coordinates, speed, and heading) as well as a list of its direct neighbors with the vehicle's verdict regarding their behavior.

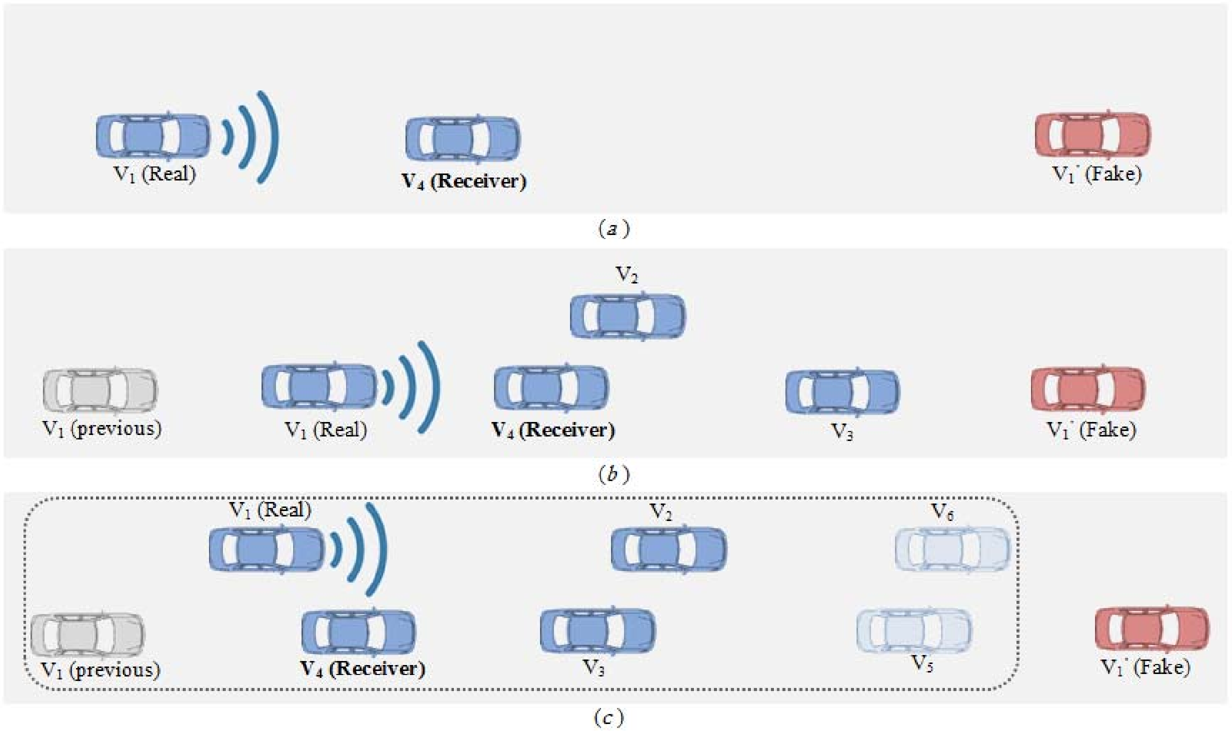

Figure 1: Position falsification scenario in different neighborhood conditions and how it would be detected. In scenario (*a*), V_4 has no neighbor information to rely on when it receives a position announcement from V_1 claiming to be at V_1', so it will compare the RSS of V_1's transmission with the measurement that should exist given the announced position. It will report its findings to later neighbors so they take them into consideration when forming their verdict regarding V_1. In scenario (*b*), as vehicle V_4 begins accumulating information about V_1, it does not have 2-hop neighbor information yet to set a boundary on the plausible area V_1 should exist within. However, it can form its verdict based on the available direct neighbors' information. Vehicle V_4, upon receiving neighbor information from V_2 and V_3, will check what they say about V_1 and will take a majority vote. In scenario (*c*), as V_4 starts accumulating direct and 2-hop neighbor information, it can now define a plausibility area within which the sender V_1 should exist. The area extends from V_1's previous position to the furthest 2-hop neighbor (V_6 in this case). If a vehicle still manages to fake its position to coincide with this plausibility area, then simple majority voting is made.

Vehicle ID				
X position			Y position	
Speed			Heading	
VID	X	Y	Flag	Timestamp
…				

Figure 2: Verification beacon structure

As illustrated in Fig. 1c, vehicle V_4, upon receiving a periodic position information beacon from V_1, will check the information it currently has from its direct neighbors; V_2 and V_3, which have attached the position information about their own direct neighbors; V_5 and V_6. This way, V_4 can use the most recent observation of V_1 together with the position information of its own two-hop neighbors V_5 and V_6 to define the plausible area within which V_1 should exist to be from V_1's previous position and the farthest two-hop neighbor; in this case V_6. The rationale behind using the farthest two-hop neighbor to bound the plausible area is that if V_4 cannot hear the farthest two-hop neighbor, then it would not be able to hear vehicles which are further than that. If a vehicle does not have information about its two-hop neighbors, then it would simply check what its direct neighbors report about the sending vehicle from their prior observations and will take a majority vote as to whether or not to trust the sender based on its previous behavior.

If a vehicle has no neighbor information to rely upon in order to define this plausible area, it will measure the RSS with which the beacon message was transmitted. Since the RSS is in general inversely proportional to the distance between a sender and a receiver, it would give a reasonable indication of the distance that exists between the receiving vehicle and the real position of the sender. The receiving vehicle can then compare this distance with the distance based on the announced position of the sender, subject to an error margin that incorporates the instability in RSS measurements. The use of RSS measurements is not a safe practice that can be followed continuously, due to the signal's vulnerability to obstacles and surroundings and the probability of propagating verdict errors that may result from errors in distance estimation.

Upon reaching a decision of whether or not the sender can be trusted, this piece of information can be relayed periodically so that neighbors within the vehicle's transmission range can receive it and use it to form their own decisions. Each vehicle would send information about its direct neighbors, together with its verdict as to their behavior within a predefined "freshness" window to guarantee that only the most recent observations of a sender are used to make a decision about its position authenticity. The general procedure of the verification scheme can be summarized in the following **Position Verification Procedure**.

Position Verification Procedure:

```
if Receiver has direct and 2-hop neighbors
    – get last observation of Sender by direct neighbors
    – set the lower bound of plausibility area
    – find the farthest 2-hop neighbor along the direction of Sender
    – use its location to set the upper bound of the plausibility area
    if Sender is beyond plausibility area
        flag as suspicious
    else
        collect neighbor votes based on their observations and flag if
          majority voting indicates fake position
    end if
else
    measure RSS and compare relative distance to distance based on
    announced position
end if
```

The proposed scheme does not use neighbors' votes first hand, so it is not strongly dependent on neighbors' observations history. Only the most recent observation – within a time window that takes into account not including neighbors that were not observed by direct neighbors for more than two beaconing intervals – are used to define the plausible area and pull votes. This way, even if vehicles would use pseudo identifiers for privacy purposes, their most recent behavior would still count if it was malicious.

IV. Performance Evaluation

In this section, the simulation setup and environment used for implementing the verification scheme are detailed.

A. Simulation Setup

The proposed scheme was implemented using the NS-2 network simulator [17]. A verification agent was developed to handle sending and receiving periodic beacon packets and perform the position verification scheme. The NS-2 simulation parameters and network configurations are shown in Table I. Simulations are conducted for a period of 1000 seconds.

To reflect the effect of outdoor environments on the signal strength and propagation, noise is introduced randomly at some nodes, which in turn causes some alterations for these nodes' RSS.

Experiments were performed over six different scenarios with different number of nodes; 50, 100, 150, 200, 250, and 300 nodes to represent various levels of node density and simulate three different environments: sparse, semi-dense, and dense environments. To generate realistic vehicular topology and movements, we used MOVE (MObility model generator for VEhicular networks) [18], on top of the SUMO (Simulation of Urban MObility) [19] vehicular simulator. SUMO is a microscopic road traffic simulator that can be used to generate a vehicular topology and map, define junctions/intersections and roads for this map, determine routes and flows for vehicles in a microscopic fashion, and visualize the generated traffic model. SUMO works in isolation of the network simulators. To introduce the topology and movements generated by SUMO to network simulators like NS-2 and Qualnet and provide that linkage, MOVE has been built on top of SUMO to generate realistic movement traces to be used by NS-2 and Qualnet network simulators. In the simulations, SUMO and MOVE are used to define our vehicular topology and generate mobility models that are introduced to the NS-2 simulations. Fig. 3 shows a snapshot of the simulated vehicular topology and vehicles movements visualized by SUMO GUI. Vehicles have two optional routes to follow. The vehicles' injection point is point A. They get separated at point B (intersection); some of them go to a destination at point C and the others have their destination at point D. Traffic lights are deployed at each intersection to provide more realism to the topology.

In the simulation, about 10% of the nodes for each scenario would fake their positions at various times during the simulation, and the falsified positions are chosen by each malicious vehicle to be at random points on the roads defined by the topology. The simulation was run five times per scenario with different seeds, and the averages of the performance measures were taken. Two performance measures were used to evaluate the performance of the proposed verification scheme: Detection rate and false alarms rate. *Detection rate* refers to the percentage of the correctly detected nodes that falsify their positions. *False positives rate* refers to the percentage of the incorrectly flagged nodes that did not falsify their position information. The ultimate goal of any position verification scheme is to target a high detection rate while keeping the false positives rate at a minimum. The threshold for the majority votes was set so that a verdict will be made that a vehicle is faking its position if more than 70% of direct neighbors report the vehicle as malicious. To take into account only the most recent observations of a sending vehicle and of two-hop neighbors, when a vehicle is verifying a position announcement it will consider only the observations that were reported in the last 20 seconds.

TABLE I: SIMULATION PARAMETERS AND CONFIGURATIONS

Simulation Parameter/Configuration	Value
Number of nodes	50, 100, 150, 200, 250, 300
Max. Node Velocity (Km/h)	40
Average Road Length (m)	300
Number of Lanes/Road	2
Beaconing Interval	4sec
Beacon Size	64Bytes
Antenna Type	Omni-Antenna
Propagation Model	Two-ray Ground
Link-/MAC Layer	802.11
Topography Dimensions	652 X 307

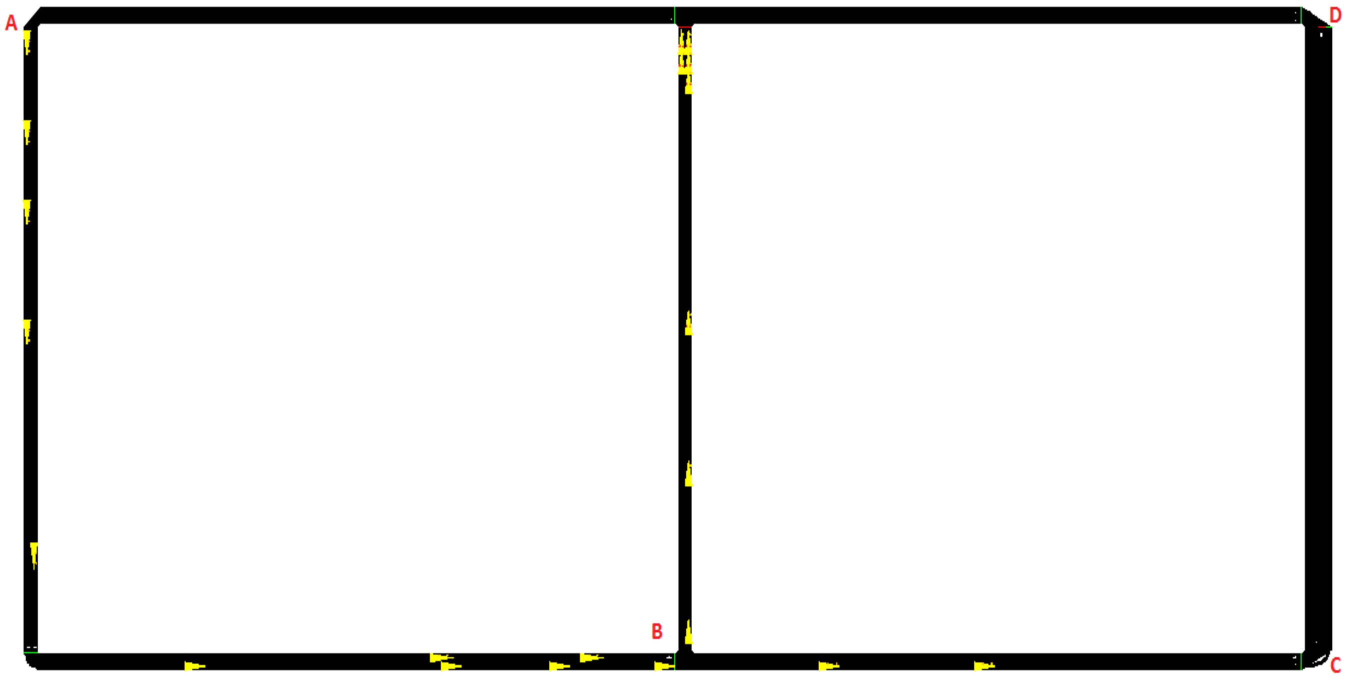

Figure 3: Visualization of Topology and Movement by SUMO

In the following sub-section, performance and simulation results of the proposed position verification scheme are discussed.

B. Simulation results and discussions

As shown in Fig. 4, the detection rate of the proposed position verification is between 84% and 95.2%, excluding the case scenario where the number of nodes equals 50. The 50 nodes case scenario delivers a 100% detection rate because it is considered a sparse scenario, in which each vehicle has at most two direct neighbors and no two hop neighbors, as shown in Table II, which shows the average number of direct neighbors and two-hop neighbors per vehicle in the different scenarios. Vehicles thus will depend solely on RSS measurements to make a verdict about the received position announcements. Introducing the random errors in RSS readings at a vehicle affects the false alarms rate, which is over 22% in the 50 nodes scenario. The detection rate generally goes higher as the number of nodes increases in the other scenarios, with a drop in performance in the 250 nodes scenario. As the environment becomes more dense, the number of neighbors (direct and two-hop) per vehicle increases, and thus the chance is higher that a vehicle will have two-hop neighbors to define a reasonable plausible area for sending vehicles, and more observations of sending vehicles by neighbors will be reported. The drop in performance in the 250 scenario can be contributed to the increase in the number of direct and two-hop neighbors, which will result in defining a larger plausible area, resulting in the possibility of a vehicle faking its position to be within this plausible area if it is big enough. In the 300 nodes scenario, performance starts to get better, mostly due to the fact that a vehicle's decision is mitigated by the majority votes of direct neighbors, which increase with the density.

TABLE II: NEIGHBORHOOD SIZE PER VEHICLE

	50 nodes	**100 nodes**	**150 nodes**	**200 nodes**	**250 nodes**	**300 nodes**
# Direct neighbors	2	6	9	13	16	23
# 2-hop Neighbors	0	4	6	8	11	13

The false alarms rate of the proposed scheme, shown in Fig. 5, ranges from 2.6% to 7.2%, again with the exception of the 50 nodes scenario. The false alarms generated in the 50 nodes scenario are all due to the errors introduced to the RSS measurements at the receiver to account to its potential inconsistency. Since the number of nodes is not big, the false alarms become more pronounced. In general, the performance with regard to the false alarms rate is satisfactory.

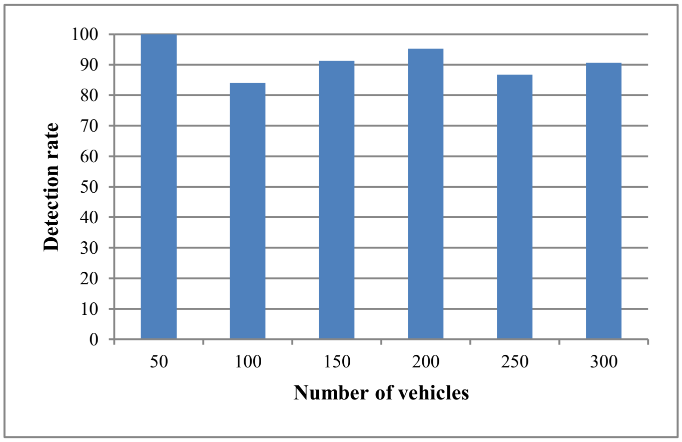

Figure 4: Detection rate of the proposed position verification scheme

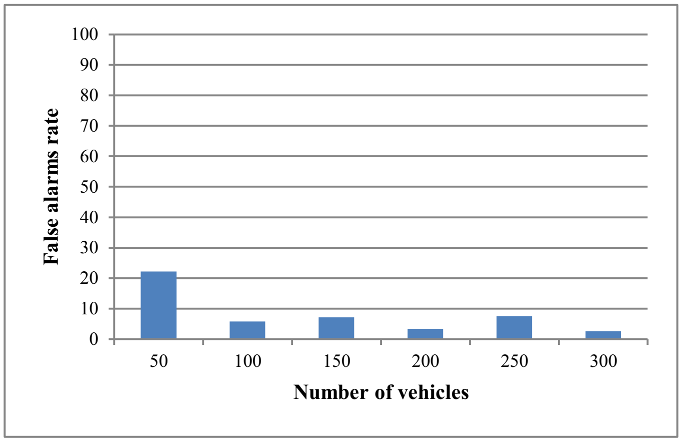

Figure 5: False alarms rate of the proposed position verification scheme

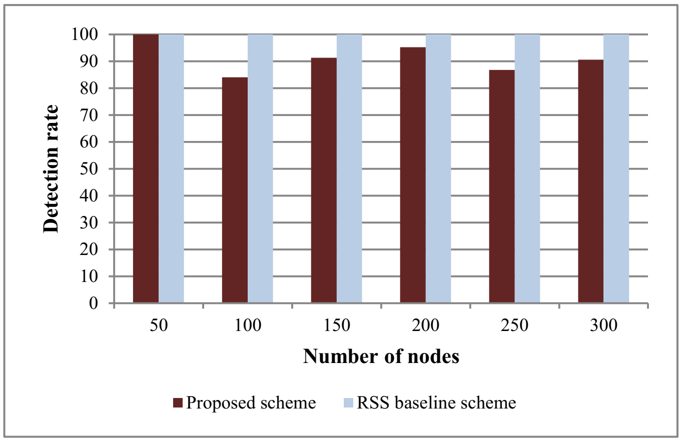

Figure 6: Detection rate of proposed scheme vs. RSS baseline scheme

C. Comparison with baseline RSS-based position verification

We have developed a baseline scheme which depends solely on RSS measurements to verify vehicles positions. The scheme will do the same as the proposed verification scheme when the neighborhood is sparse and there are no direct or two-hop neighbors to rely on in order to form a verdict regarding a sending vehicle. When a vehicle receives a suspicious position announcement, it will not flag it as malicious. Rather, it will report a “medium suspicion” flag to other vehicles. When other vehicles report this medium suspicion flag, they will flag the corresponding vehicle as highly suspicious. Otherwise, if a vehicle later receives neighbors “good” verdicts about the vehicle being verified, the verifying vehicle will set its flag back to normal. This baseline scheme gives a 100% detection rate, as can be seen in Fig. 6. The proposed position verification scheme does reasonably well compared to this baseline scheme, considering that in the proposed scheme, RSS measurements are only used in sparse scenarios and neighborhood information is used later to evaluate positions announcements. The false alarms rate in the baseline scheme are close to the proposed verification scheme in the 50 and 100 nodes scenarios, because the majority of false alarms are caused by the errors of RSS measurements when a vehicle has no neighbors to depend on to make its verdict regarding another vehicle. As the neighborhood size increases, the baseline scheme has no false alarm, because a vehicle now can depend on other neighbors RSS measurements to strengthen its own verdict regarding a position announcement. As can be seen in Fig. 7, the proposed position verification scheme still has percentage of false alarms higher than that of the baseline scheme. A motivation of continuous development of the proposed scheme is to lower the false alarms so that normally behaving vehicles would not be penalized.

V. Conclusions and Future Work

A position verification scheme was proposed which will benefit from 2-hop neighborhood information in order to form verdicts about vehicles announced positions. The proposed scheme performs reasonably well, and performance can be expected to enhance with the addition of more plausibility checks for vehicles speed and existence in physical spaces occupied by other vehicles. This is a work in progress and more logical checks are being investigated in order to increase the rate of detecting falsified positions and reduce the amount of false alarms.

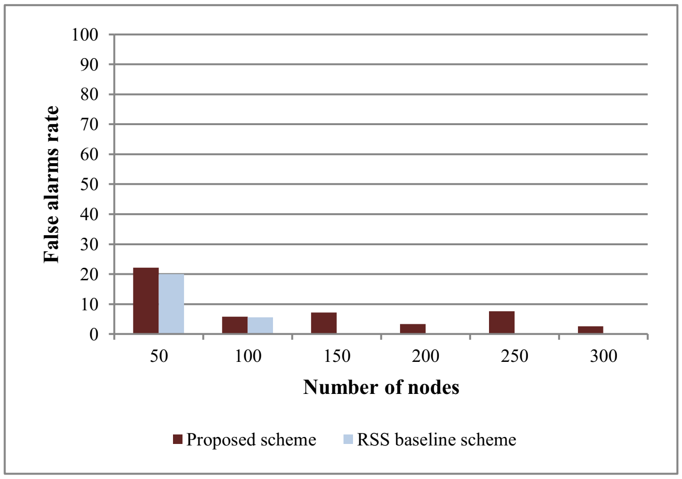

Figure 7: False alarms rate of proposed scheme vs. RSS baseline scheme.

Future work would involve implementing a realistic VANET propagation model, such as the ones proposed in [4] and [20], and investigating its effect on message delivery and the verification procedure. A special case in which the scheme’s performance is still lacking is when a vehicle fakes a position to be within the plausibility area with no information previously recorded of the vehicle. To handle this scenario, it would be essential that a vehicle record physical visuals of the surrounding vehicles to provide more credibility. The integration of Radar [21], Visible Light Communication (VLC) [22], and Laser scanners [23] will be investigated to provide means for vehicles to associate position announcements with physical detection of objects in their environment.

Further enhancements to this work would involve looking into methods for the fusion of two-hop neighbors’ information in order to further optimize the format of the location information that is included in the verification message. Fusion of two-hop location information will be investigated to see if it would lead to a more efficient utilization of bandwidth, less processing at the verifying nodes, and an overall faster verification procedure.

REFERENCES

[1] A. Boukerche, H. Oliveira, E.F. Nakamura, and A. Loureiro, "Vehicular Ad Hoc Networks: A New Challenge for Localization-Based Systems," *Computer Communications*, vol. 31, no. 12, pp. 2838-2849, July 2008.

[2] S. E. Shladover and S. K. Tan, "Analysis of vehicle positioning accuracy requirements for communication-based cooperative collision warning," *Journal of Intelligent Transportation Systems*, vol. 10, no. 3, pp. 131-140, 2006.

[3] IEEE, 1609.2: Trial-use standard for wireless access in vehicular environments-security services for applications and management messages, 2006, IEEE Standards.

[4] M. Boban, T.T.V. Vinhoza, M. Ferreira, J. Barros, and O.K. Tonguz, "Impact of Vehicles as Obstacles in Vehicular Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 1, pp. 15-28, January 2011.

[5] R. K. Schmidt, T. Köllmer, T. Leinmüller, B. Böddeker, and G. Schäfer, "Degradation of Transmission Range in VANETs caused by Interference," *PIK - Praxis of information processing and communication*, vol. 32, no. 4, pp. 224–234, October - December 2009.

[6] J.P. Hubaux, S. Capkun, and Jun Luo, "The security and privacy of smart vehicles," *IEEE Security & Privacy*, vol. 2, no. 3, pp. 49-55, May-June 2004.

[7] G. Yan, S. Olariu, and M. C. Weigle, "Providing VANET security through active position detection," *Computer Communications*, vol. 31, no. 12, pp. 2883-2897, July 2008.

[8] Z. Ren, W. Li, and Q. Yang, "Location Verification for VANETs Routing," , 2009, pp. 141-146.

[9] C. Harsch, A. Festag, and P. Papadimitratos, "Secure Position-Based Routing for VANETs," in *IEEE 66th Vehicular Technology Conference*, 2007, pp. 26-30.

[10] Joo-Han Song, V.W.S. Wong, and V.C.M. Leung, "Secure Location Verification for Vehicular Ad-Hoc Networks," in *IEEE Global Telecommunications Conference (GLOBECOM)*, 2008, pp. 1-5.

[11] H. D. Weerasinghe, R. Tackett, and H. Fu, "Verifying position and velocity for vehicular ad-hoc networks," *Security and Communication Networks*, 2011.

[12] P. Golle and J. Staddon, "Detecting and Correcting Malicious Data in VANETs," in *International Conference on Mobile Computing and Networking*, 2004.

[13] J. Van Eenwyk, "Detecting Malicious Data in Vehicular Networks," in *VANET '07*, Montreal, Canada, 2007.

[14] T. Leinmüller, C. Maihöfer, E. Schoch, and F. Kargl, "Improved Security in Geographic Ad hoc Routing through Autonomous Position Verification," in *The 3rd International Workshop on Vehicular Ad hoc Networks*, 2006, pp. 57-66.

[15] T. Leinmüller, E. Schoch, and F. Kargl, "Position Verification Approaches for Vehicular Ad hoc Networks," *IEEE Wireless Communications*, vol. 13, pp. 16-21, October 2006.

[16] F. Bai, T. Elbatt, G. Hollan, H. Krishnan, and V. Sadekar, "Towards characterizing and classifying communication-based automotive appliapplications," in *Proceedings of IEEE Workshop on Automotive Networking and Applications (AutoNet)*, 2006.

[17] (2011, April 24th) The Network Simulator NS-2 homepage. [Online]. http://www.isi.edu/nsnam/ns/

[18] (2011, April 24th) MOVE (Mobility model generator for vehicular networks). [Online]. http://lens1.csie.ncku.edu.tw/wiki/doku.php?id=%E2%80%A7realistic_mobility_generator_for_vehicular_networks

[19] (2011, April 24th) SUMO (Simulation of urban mobility). [Online]. http://sumo.sourceforge.net/

[20] J. Maurer, T. Fugen, T. Schafer, and W. Wiesbeck, "A new inter-vehicle communications (IVC) channel model," in *IEEE 60th Vehicular Technology Conference (VTC2004)*, vol. 1, September 2004, pp. 9-13.

[21] G. Yan, S. Olariu, and Weigle M.C., "Cross-layer Location Verification Enhancement in Vehicular Networks," in *IEEE Intelligent Vehicles Symposium*, San Diego, CA, USA, 2010.

[22] Intel Corporation White Paper. (2011, April 24th) Visible Light Communications and Positioning (VLCP) - The automotive use case - 2010. [Online]. http://www.connectedvehicle.org/VisibleLight.pdf

[23] F. Nashashibi and A. Bargeton, "Laser-based vehicles tracking and classification using occlusion reasoning and confidence estimation," in *IEEE Intelligent Vehicles Symposium*, June 2008, pp. 847–852.