2014 International Joint Conference on Neural Networks (IJCNN)
July 6-11, 2014, Beijing, China

Evaluation of Active Position Detection in Vehicular Ad Hoc Networks

Kiran Penna, Venkatesh Yalavarthi, Huirong Fu
Oakland University, Michigan, USA
{kvpenna, vyalavar, fu}@oakland.edu

Ye Zhu
y.zhu61@csuohio.edu
Cleveland State University, Ohio, USA

Abstract— Vehicular Ad Hoc Network (VANET) is a promising technology in which vehicle-to-vehicle and vehicle-to-roadside infrastructure wireless communications can be achieved. This is important to obtain road safety for vehicles and drivers and collision avoidance. A falsified position by malicious users is one of the important issues in VANETs. Vehicle position identification is one of the important aspects in establishing authentication and security between inter vehicular communication exchange. Deepa et al presented two approaches for verifying sender's position in a multi-hop network. Their first proposed algorithm relies on signal propagation time for verifying the position. Their second proposed algorithm verifies the position information with the help of base stations located in the coverage area of the vehicular network. The main contribution of our work is validating their approach by running an ns2 simulation with dynamic number of nodes in various mobility scenarios such as urban, rural, Manhattan. We have also generated different scenarios with variable velocity ranges and simulated the VANET. We have also considered the effect of delay, jitter in our simulation and observed that the proposed approach is robust and a feasible solution to the problem of Active Position detection.

I. INTRODUCTION

Recently, car manufacturers and telecommunication companies have been gearing up to equip each car with technology that allows drivers and passengers to communicate with each other as well as with the roadside infrastructure that may be located in some critical sections of the road, such as at every traffic light or any intersection or stop sign, in order to improve the driving experience and make driving safer. **V**ehicular **A**d Hoc **Net**work (VANET) is a promising approach to facilitating road safety, traffic management, and infotainment dissemination for drivers and passengers. Vehicular Ad Hoc Networks are receiving a lot of attention due to the wide variety of services they can provide. Their applications range from safety and crash avoidance to Internet access and multimedia. A lot of work and research around the globe is being conducted to define the standards for them.

One of the ultimate goals in the design of such networking is to achieve vehicle-to-vehicle and vehicle-to-roadside unit wireless communication. Using such equipped communication devices, also known as On Board Units (OBUs), vehicles can communicate with each other as well as with the Road Side

Units (RSUs) located at critical points on the road. A self-organized network can be formed by connecting the vehicles and RSUs, called a vehicular ad hoc network (VANET), and the RSUs are further connected to the backbone network. Different VANETs can enable vehicles to communicate with each other so that drivers can have better awareness of what is going on in their driving environment and take early action to respond to abnormal or unexpected situations like crash, traffic jam, detour, road construction etc.

The pictorial representation of VANET is shown in figure 1 below.

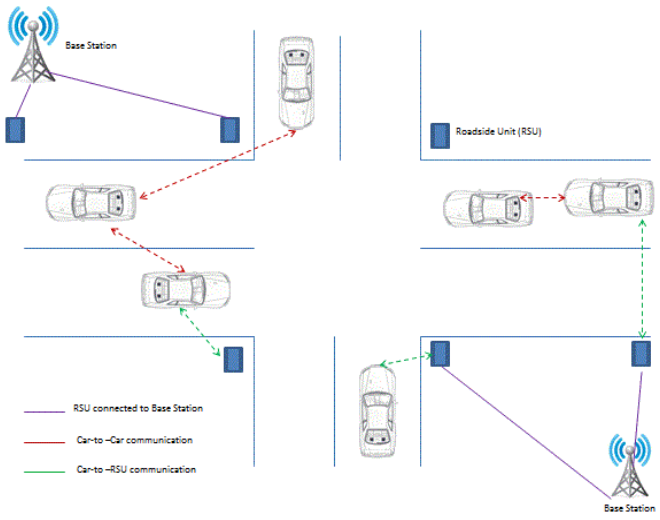


Fig. 1: VANET

The main challenge about VANETs is that they are subject to many security and privacy threats. Hackers or malicious attackers can steal and misuse the confidential user information like driver's name, license plate, speed, position, travelling routes etc. Security becomes more challenging due to the unique features of networks, such as the high-speed mobility of the network entity (or vehicles), extremely large

978-1-4799-1484-5/14/$31.00 ©2014 IEEE

amount of network entities, highly dynamic topology of the network, large scale networks, random movement pattern of vehicles, hybrid communication pattern, self-organizing nature of the network etc. It has been speculated that security and privacy concerns have formed the major barrier preventing many drivers in using VANETs in real life and thus preventing them to be ubiquitous.

There are several different aspects involved in security. Security problems mainly include message authentication, integrity, confidentiality and non-repudiation, message privacy, false positions by some of the users, false velocity, false direction, network latency problem etc. We cannot deny the case where user makes the mistakes and unintentionally broadcasts wrong information. Out of the mentioned problems, we are mainly focusing on the problem of falsified positions by malicious vehicles in our research.

The main contribution of our work was to run a simulation of the proposed vehicle position detection algorithm based on the signals propagation time. We made use of the NS2 simulator to generate communication messages between vehicular nodes in the VANET using various real world vehicular scenarios. We also studied the effect of jitters, delays and effect of velocity and number of nodes in our simulation to study the robustness of the algorithm.

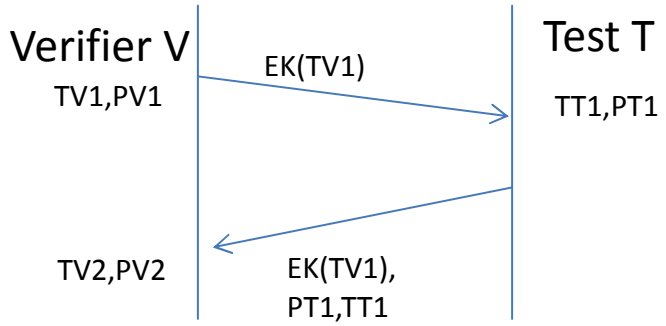
II. POSITION AND VELOCITY VERIFICATION SCHEME

Here we briefly discuss the basic approach proposed by Deepa et al. Following are assumptions and algorithm references to their paper. References are included under the References section in this paper.

A. Assumptions

1. The proposed algorithm is for multi hop networks. Therefore it is assumed that the communicating vehicles are at farther distance apart.
2. The data or information exchanged between the vehicles are highly time sensitive.
3. The algorithm we present is to authenticate that the message was sent from a vehicle at the claimed position. This verification implies that the position information is not modified by a man in the middle.
4. The vehicle knows its own position. This is assumed through the use of GPS.
5. Intermediate vehicles are trusting and will forward messages upon arrival without any malicious intent

B. Algorithm



The algorithm follows the following steps.

Step 1: The verifier vehicle, V, broadcasts a token message out at random time, TV1

Step 2: Once the test vehicle, receives this token message, it immediately replies with its position, PT1, which it determines from its GPS.

Step 3: Upon getting this message at time, TV2, the verifier V, Measures the round trip time

$$RTTm = TV1 - TV2. \quad (1)$$

Step 4: Verifier vehicle then calculates

$$D = (PV1\text{-}PT1) + (PT1\text{-}PV2) \quad (2)$$

D the distance between the positions of the verifier, PV1 and the claimed position of the test vehicle at the time it received the token, PT1. Based on D and the speed of signal propagation, the round trip time can be calculated as,

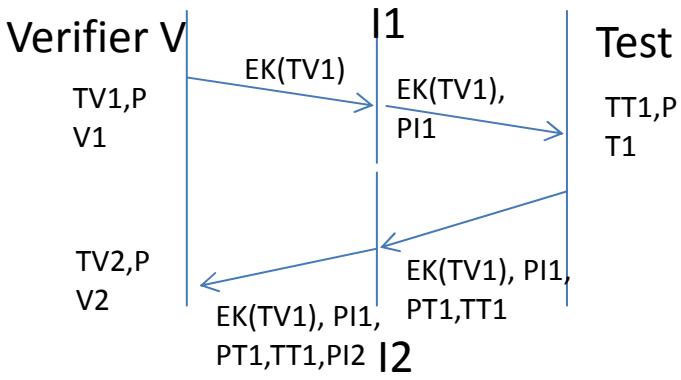
$$RTTc = D/C \quad (3)$$

where C is the speed of light.

The verifier then compares RTTm and RTTc. If they match, then the claimed position is correct and the message is authenticated.

The above calculation holds valid as it is not possible for sender to estimate positions PV1 and velocity of receiver and hence difficult to give out a false position.

This paper also validates the above algorithm over a multi hop network where messages will be passed on by intermediate vehicles between Verifier and Test vehicles.



In a multi hop scenario each vehicle in between the Verifier and the Test vehicle will upon arrival of message forward it on the next vehicle including its sending time and position. Verifier after receiving reply from test vehicle will consider individual distances and times of all vehicles involved in the communication and the calculate measured distance against calculate distance as shown in the algorithm.

$$D = (PV1-PI1) + (PI1-PT1) + (PT1-PI2) + (PI2-PV2) \quad (4)$$

Again here the approach is validated as it is not possible for Test vehicle to predict Verifier's initial position, velocity and time at which message was initiated and hence cannot fake its own position and time.

Here the assumption is that majority of the vehicles in the network are honest and will give out their correct locations and times and hence algorithm can accurately validate test vehicle position based on signal propagation approach.

The algorithm also considers the effect of delay and theoretically shows that test vehicles position can be accurately estimated.

III. PROTOCOL IMPLEMENTATION

We have taken the RBC protocol in our NS2 simulation for vehicular ad hoc networks. We have used the VANETRBC agent as an agent on the simulation nodes. This agent independently acts upon the MAC layer.

IV. SIMULATION

We have used different number of nodes in our simulations they are positioned at the starting of the simulation. These move during the simulation this is achieved by the distances in the scenario file. Each node sends out packets at random intervals of time. This is a broadcast so every node in the communication range will be able to receive the packets. In the packet header we included the timestamp at which the packet is being sent. When a node receives the packet it then calculates the trip time based on the difference between the timestamps in the received packet header.

We have used two sets of scenario files. We generated one set of scenario files using the SETDEST utility in ns2.Using this utility we generated multiple scenarios of a 50 node network with vehicles moving in different sets of velocity ranges. Each scenario was generated using a minimum and maximum speed limit for the mobile nodes in the network. Simulation setup consisted of 50 node network in an area of 500m x 500m. We had to modify version to 2 and other changes in the setdest.cc and compile changes to generate scenario files in a format that was needed for the simulation setup.

The second was derived from the generic mobility simulation framework (GMSF). This framework generates realistic vehicular mobility models that represent real world behavior determined by road maps from a geographic information system. These models use real world maps, realistic speed limits and road topology. Different scenario files generated using different number of nodes were used in simulating VANET. Message communication between nodes simulated for variable lengths of time. Simulation setup consisted of variable nodes network in an area of 4000m x 4000m.

The proposed algorithm depends heaving on GPS system. Real world situations involve delays intentional or non-intentional and other errors. Hence we further analyzed the robustness of the approach by running simulations by introducing signal delays and jitters in the network. We tried simulations with jitter factor 0.0001 - 0.0009 and delay factor of 0.0184 and generated the trace files for analysis.

To get the coordinates in the trace file we had to set the trace format to new trace. Once this was turned on the trace file included the coordinates of the node which received or sent a packet. This is important as we calculate the distance between the nodes based on these values. We developed awk script files to parse through the trace file to find out node that is sending the packet and the node that is receiving the packet and then collect details such as coordinates of the sender and receiver nodes and message sent times.

Simulation properties included Two Ray Ground radio propagation model, 802_11 MAC layer, AODV routing protocol, drop tail queue type, interface queue length of 50. Each simulation was run for 500 secs.

V. PERFORMANCE EVALUATION AND ANALYSIS

As mentioned in the setup, we are running the simulation for a predetermined time, this time decides the movement in the nodes as specified in the scenario files. All the nodes that receive packets compute the trip time and this is printed out. At the same time the coordinates of the nodes will be noted in the trace files these will be used to find the distance between the nodes. Once we have the distance between the

nodes we can find out the time it took for the packet to travel from the sender to the receiver.

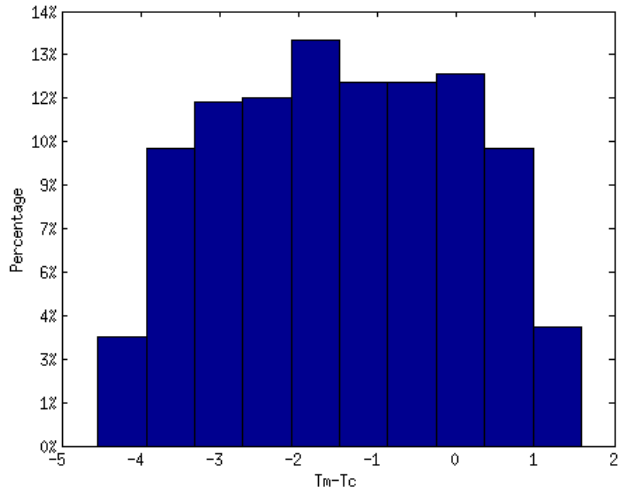


Figure 1

Figure 1 depicts the distribution of the difference between calculated and measured trip times. We can see that the highest distribution is in-between -3 and 0ms. Our main aim is to verify that the signal propagation time can be used to find out the distance between the nodes. This will be true if the distribution is at or around 0ms.We can see the same distribution in the above figure.

We also see similar results for the urban and rural scenarios.

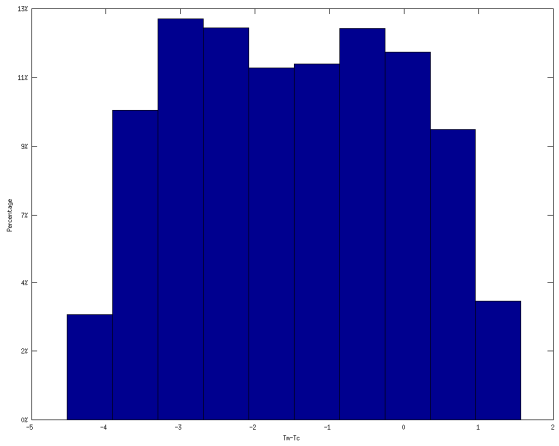


Figure 2

As shown in Figure 2 above, for the rural scenarios the highest distribution of the difference between calculated and measure trip times is seen to be in the range of -3 and 0ms. Above scenario was simulated with 100 nodes.

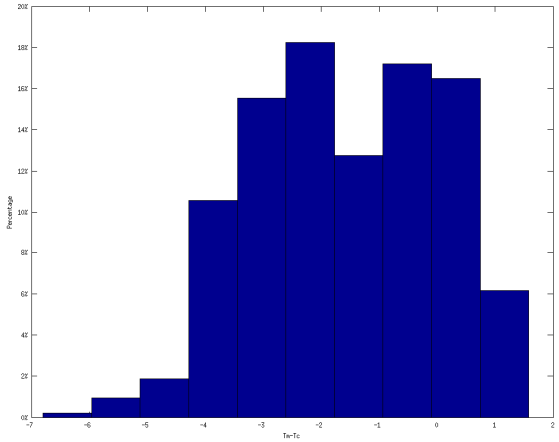


Figure 3

As shown in Figure 3 above, for the urban scenarios the highest distribution of the difference between the calculated and measured trip times is seen to be in the range of -3 and 1ms. Above scenario was simulated with 125 nodes.

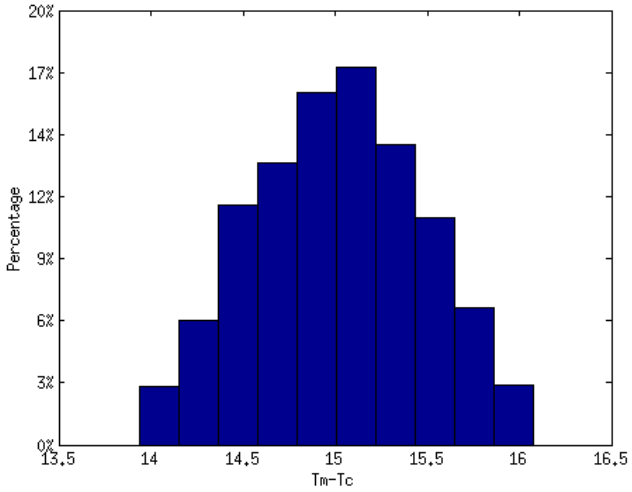


Figure 4

In Figure 4, the distribution of the difference of the trip times is plotted. For this scenario we considered delay factor of 0.018 and a jitter factor of 0.001. As seen in the graph the trip times are centered around 15 ms as this includes the delay caused by the jitter and the calculation delay. The delay has a significant impact on the time difference this is as expected as the calculated value is based on the distance between the nodes and the measured is based on the time stamps. The time stamps will have an increase with respect to the jitter and the delay. This shows that proposed algorithm can identify intentionally introduced position errors. Greater the error greater would be the difference in the calculated and the measured trip times.

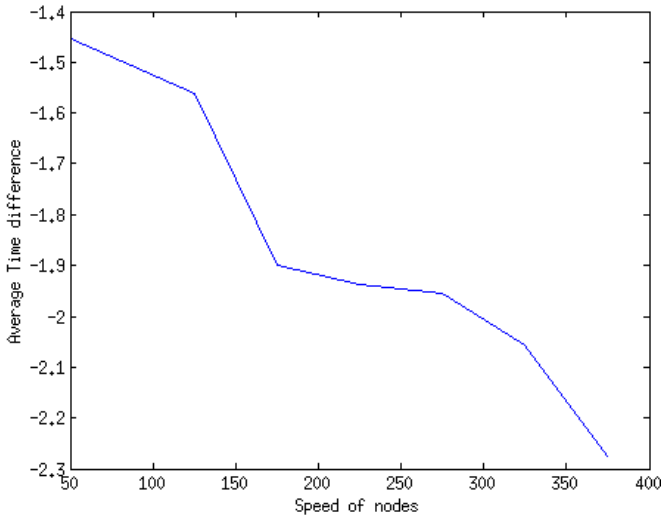


Figure 5

In Figure 5, the numbers of nodes are varied from 50 to 425 and the simulation is run calculating the average difference between the measured and the calculated time. The velocity of the vehicles and the time for the simulation are kept constant for each case. We are focused on the impact of the number of vehicles or nodes on the trip times. From the graph we can see that with the increase in the nodes the average time difference increases. We can see that the number of nodes does increase the average time difference but this is small.

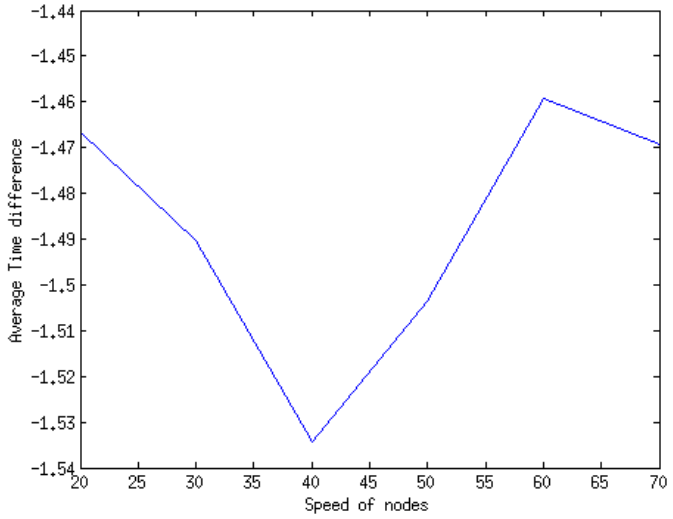


Figure 6

Figure 6 is a graph for the speed of the nodes against the average time difference between the measured and calculated time. In this set of simulations the number of vehicles and the simulation time are kept constant while varying the maximum speed of vehicles from 20 to 70. Here we are focused on the effect of the vehicle velocity on the trip times. We can see that the velocity does have some effect on the trip times but it is very small much less than 1ms.

VI. CONCLUSION

VANET is a highly safety critical system. Flaw in the system security may lead to loss of properties and lives of people. Design and security of VANET has to be fail-safe and non-vulnerable to different types of attacks like false positions.

Simulation and analysis of the signal propagation time algorithm for active position detection of vehicles in a VANET validates the effectiveness of the approach. The simulation results obtained by using the variable set of nodes indicate that the computed and measured trip times between the verifier and the test vehicles are comparable. The distribution of the difference in the trip times as plotted in the graphs show that algorithm can be effectively implemented for position detection.

It is also observed that delay and jitter adversely affect the trip times. Graphs show that the delay has a significant impact on the time with increase in the difference between the calculated and the measured trip times. Thus an intentional positional error can be easily identified.

We also studied the effect of the number of nodes in the network. With increase in the number of the nodes the trip times are slightly increased and similar trend was observed with increase in vehicle velocities.

It can be concluded that proposed algorithm is an effective solution to the problem of active position detection in a VANET and can be implemented and further researched upon.

VII. FUTURE WORK

We intend to further evaluate the effectiveness with increase in the number of simulation runs using different real world traffic scenarios and increase in number of nodes. We will also consider the effect of encryption and decryption of the verifiers start time and see how it would affect the performance of the algorithm. We will further analyze the effect of different variables involved like speed, number of vehicles, distances between the nodes and different traffic behaviors.

REFERENCES

[1] Deepa Susan Rajan Chetan Yeole, Harsha Nakade and Huirong Fu, “Position Verification in Multi-hop Vehicular Networks,” Technical Report.

[2] Hesiri D. Weerasinghe, Raymond Tackett, and Huirong Fu, “Verifying Position and Velocity for Vehicular Ad-Hoc Networks,” Special Issue on

Security and Privacy in Wireless Systems, Security and Communication Networks, vol. 4, no. 7, pp. 785-791, 2011.

[3] Yongzhong He and Huriong Fu, "Trusted Vehicular Ad hoc Network," Technical Report.

[4] Gongjun Yan, Stephan Olariu, and Michele C. Weigle, "Providing VANET security through active position detection, Computer Communications," Volume 31, Issue 12, 30 July 2008, Pages 2883-2897, ISSN 0140-3664, 10.1016/j.comcom.2008.01.009.

[5] Albert Wasef and Xumein Shen, "REP: Location Privacy for VANETs Using Random Encryption Periods,"

[6] Gongjun Yan, "Providing VANET security through Active Position detection,"

[7] Gongjun Yan; S. Olariu, M. Weigle, "Providing location security in vehicular Ad Hoc networks," Wireless Communications, IEEE, vol.16, no.6, pp.48-55, December 2009.

[8] Xiaodong Lin, Rongxing Lu, Chenxi Zhang, Haojin Zhu, Pin-Han Ho, and Xuemin Shen, "Security in vehicular ad hoc networks,' Communications Magazine, IEEE , vol.46, no.4, pp.88-95, April 2008.

[9] N. Alsharif, A. Wasef, and X. Shen, "ESPR: Efficient Security Scheme for Position-Based Routing in Vehicular Ad Hoc Networks," GLOBECOM 2010, 2010 IEEE Global Telecommunications Conference, vol., no., pp.1-5, 6-10 Dec. 2010.

[10] Tim Leinmiller, Elmar Schoch, and Frank Kargi, "Position Verification Approaches for Vehicular Ad Hoc Networks", IEEE Wireless Communication Magazine, October 2006.