Providing VANET Security through Position Verification

Master's Project Final Report

Author: Gyanesh Kumar Choudhary

Email: gchoudha@cs.odu.edu

Project Advisor: Dr. Michele Weigle

Email: mweigle@cs.odu.edu

Project Presentation Date: September 14, 2007

Department of Computer Science

Old Dominion University

Index

Acknowledgements

I would like to express my appreciation and sincere thanks to my project advisor **Dr. Michele Weigle,** Assistant Professor, Department of Computer Science, Old Dominion University for her guidance, encouragement and patience throughout the duration of this project. I am extremely grateful to her for her valuable time and vast experience which has been most critical in making this project meaningful and successful.

I like to convey my special thanks to **Dr. Stephan Olariu,** Professor, Computer Science, Old Dominion University for his advice and support. He always made me realize my hidden potentials and been a mentor.

My sincere thanks also go to my colleague **Mr. Gongjun Yan,** Ph.D Candidate, Old Dominion University, for providing valuable advice and support throughout the duration of the project.

1. Abstract

This project investigates security aspects of vehicle-to-vehicle communication using GPS and radar. Position is a key piece of information in vehicular ad-hoc networks (VANETs), and the use of radar will substantially augment the amount of trust that can be given to the received position information. The goal is to achieve local security by using onboard radar to detect neighbors and to confirm their announced GPS coordinates. Our solution is based on simple principle: “Believe what you see, verify what you hear”. By comparing what is “seen”, *i.e.*, detected by radar, to what has been reported over the network, a vehicle can corroborate the real position of neighbors and detect malicious vehicles, thus achieving local security. Due to the inherent limitations of radar spatial penetration, we cannot directly use this process to achieve global security, but use local security as a basis for achieving global security. We use preset position-based cells (through which we achieve local security) to create a communication network. Global security is achieved by exchanging packets among cell members and verifying neighboring vehicles’ positions using oncoming traffic. Each vehicle generates information about the state of the traffic based on both what is seen and what is received from other vehicles in the system. This technique will improve security in VANETs by preventing malicious users from falsifying their position information.

2. Introduction

A Vehicular Ad-Hoc Network (VANET) facilitates communication between vehicles and between vehicles and infrastructure. The study of VANETs has recently become an increasingly popular research topic in the area of wireless networking as well as the automotive industries. The goal of VANET research is to develop a vehicular communication system to enable quick and cost-efficient distribution of data for the benefit of passengers' safety or comfort.

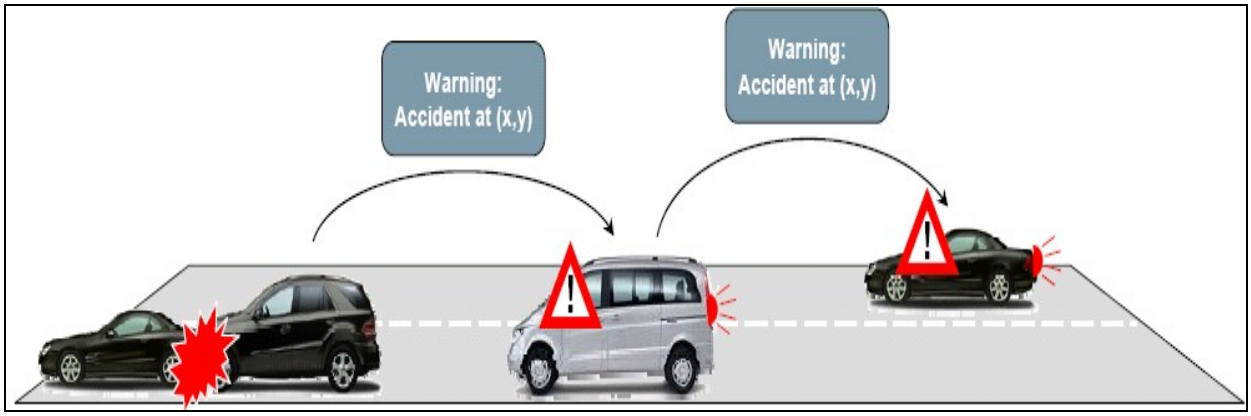

Figure 1 [20] Message generated by vehicle involved in accident to inform approaching vehicles

Figure 1 demonstrates the usefulness of VANET in real road scenario. If an accident warning can be sent to cars approaching the accident region, it would allow the drivers to take preventive measures and avoid disaster. A good real time feedback of the traffic condition would surely decrease the number of accidents and persons killed every year in road accidents. Figure 2 shows the accident figures in Germany since 1970. The figure depicts that with the increase in traffic density, the number of accidents increased as well. The bottom line

indicates that with an increase in safety features like safety belt, air bag, etc., the number of persons killed every year has gone down substantially. This graph provides the motivation for researchers that with the inception of VANET applications, we can further bring down this number.

VANET applications [1, 2] usually require security and can be divided into two categories:

1. *Non-position related applications*, such as online payment services, online shopping, internet access (infotainment). These applications focus on the network access, for example from Ad Hoc wireless network to the Internet.

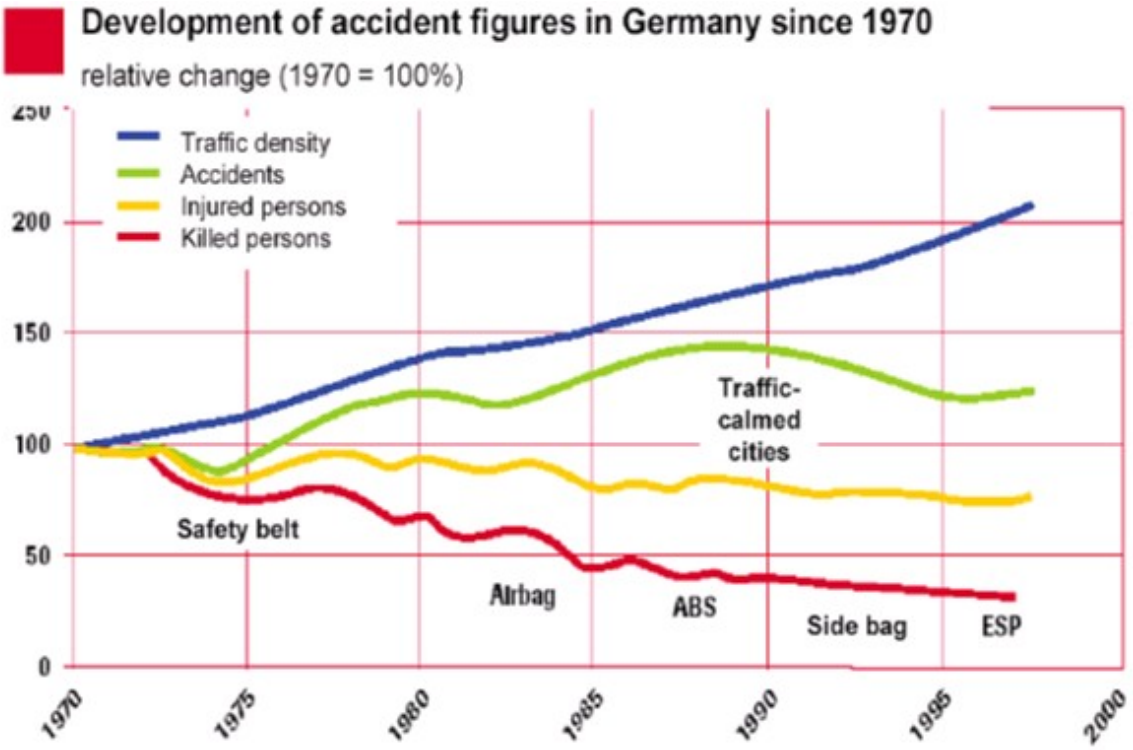

Figure 2 [20].Accident figures in Germany since 1970

2. *Position-related applications*: such as Traffic condition report, collision avoidance, emergency alert, driving suggestion or cooperative driving; traffic optimization, resource service (for example, finding the closest gas

station). The most important thing in second category is position. If position information is not protected, this type of applications can not work at all.

In this project, we address a method that will ensure the validity of position information.

Since position information is very important [3], adversaries could harm a VANET system by doing the following [3, 4, 5, 6, 7 and 8]:

Drop packets, selective dropping or nonselective dropping packets: break routing path, consume bandwidth; for example, a smart malicious attacker may create an accident and drop all the alert packets by creating an illusion position of a vehicle as a router to prevent appropriate deceleration alerts from reaching other vehicles.

Modify exist packets or insert bogus packets: change the topology, break routing. For example, a prankster may insert packets to create a traffic jam illusion before selecting an alternate route to his advantage.

Replay packets: for example, pretend to be someone else whose real position has moved far away at an old position to create an illusion of a vehicle.

Figure 3 illustrates how the car marked with circle launches a Sibyl attack [7]. The circles depict the false position as claimed by malicious vehicle under different IDs.

Figure 3 Launch of position based attack

In this project, we propose a new solution to secure the position information. The goal of our work is to provide a secure topology for a VANET and to build a secure network for applications. The basic idea is the famous saying: “seeing is believing”. We use radar as a virtual “eye” of a vehicle. Although the “eyesight” is limited due to limitation of radar transmission range, a vehicle can “see” surrounding vehicles and hear reports of their GPS coordinate. By comparing what is heard and seen, a vehicle can determine out the real position of the neighbors and isolate liars (Sybil attackers) to achieve local security. Due to the limitation of radar visibility range, we need to combine local security to achieve global security. We present preset position-based cells (where we achieve local security) to create a communication network by securely exchanging packets among cells. Besides, we propose a method to challenge and confirm position of a vehicle in a remote cell. In this way, we achieve global security.

3. Project Details

3.1 System Model

In the near future, new vehicles may have computer network devices, computing devices, storage devices, and even an Event Data Recorder (EDR). Specifically, vehicles in this research are assumed to be endowed with the following features:

A GPS navigation system, such as a GPS receiver, GPS maps;

Microwave radar that can detect objects at distance as far as 200 meters. Some cruise control systems use this kind of radar [14]; in this project, we assume that the radar is Omni directional which does not exist right now, but in the near future it will come true.

A computer center, which will provide data processing, computing and storage;

A wireless transceiver, such as DSRC which provide fast communication for VANET;

A unique ID, such as an electronic license plate [12] which is given by registration authorities or is stored in EDR. We only discuss security in this report.

The radar detects any obstacles ahead. GPS navigation system, specifically the GPS receiver and maps, provides the coordinates and localization. To

simplify the hardware security, we assume that all the devices are tamper-proof, like an EDR. Figure 4 shows the arrangement of devices in a vehicle.

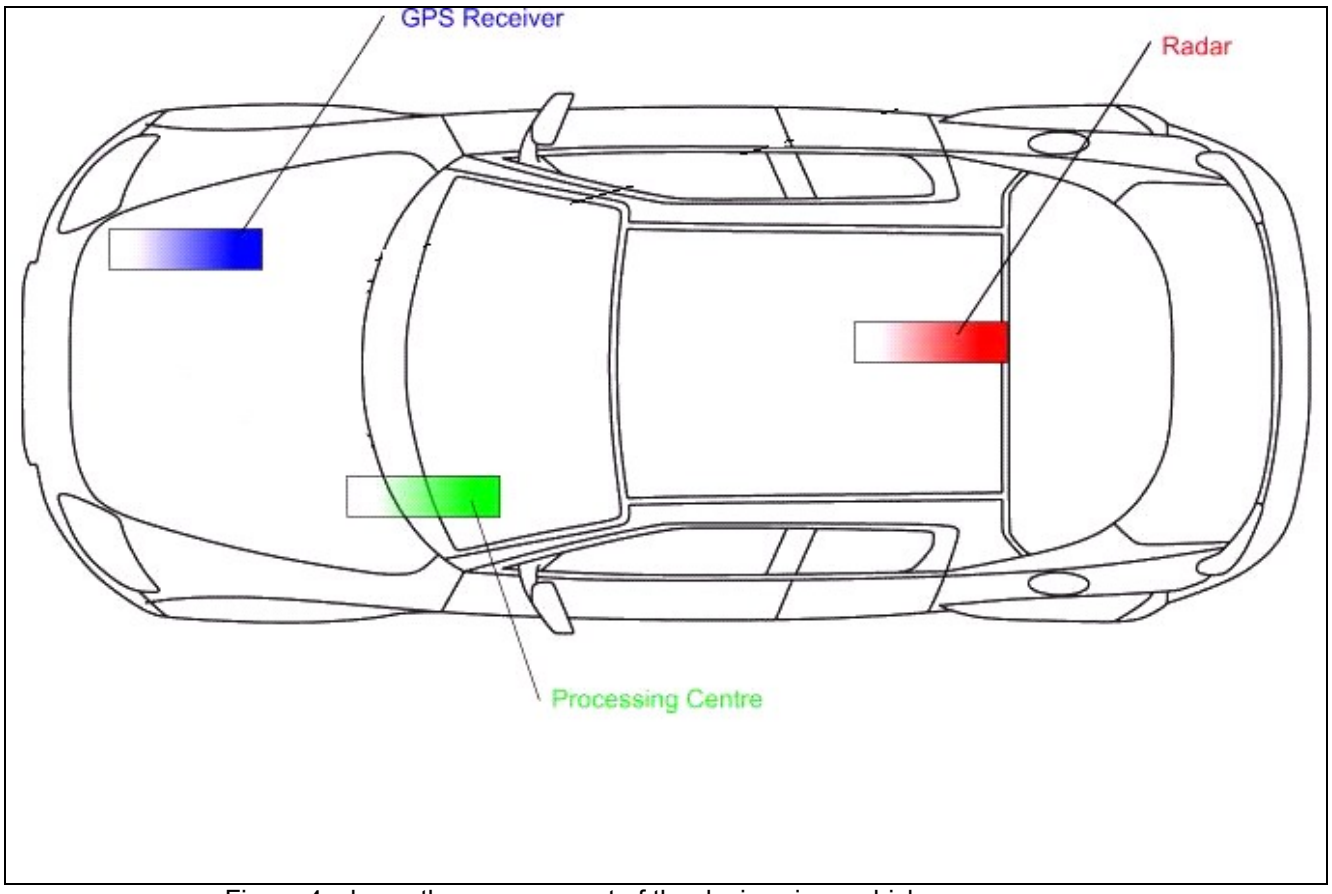

Figure 4, shows the arrangement of the devices in a vehicle.

3.2 Network Model

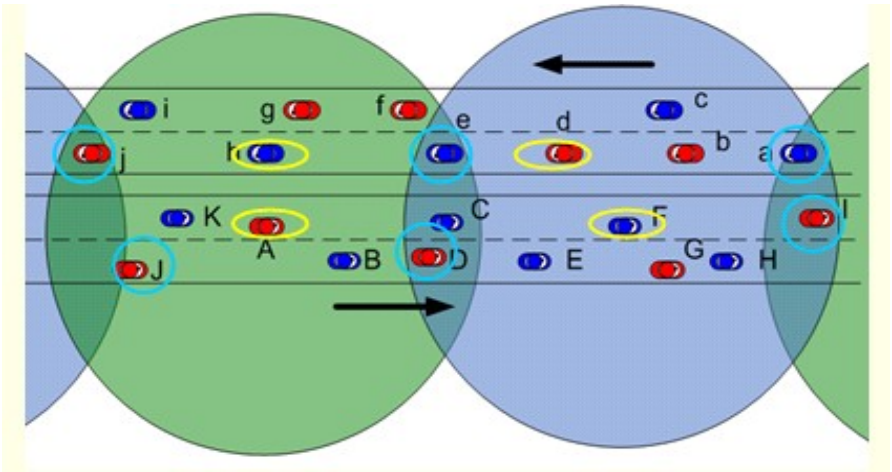

Figure 5. Representation of cell leader and cell routers in a preset map

There are two types of cells [10, 11]: dynamic cells and position-based cells. Although dynamic cells are flexible, they are not efficient. The position-based cells, on the other hand, are created beforehand and vehicles use their GPS coordinates to map to their respective cells. These preset cells avoid the need to undergo the complex process of forming a cell and electing a cell leader. In this project, we use position-based cells to build a communication network. Cells are shown in Figure 5 as shadow areas which are set statically. Vehicles compare their GPS coordinates with these preset cells to identify their host cell.

We can configure the road with virtual digital cells, for example every 200 meters a cell on the road, i.e., the cells' radius is 100 meters such that all the vehicles inside can directly send or receive packets without any routing. The radius of cells is same with the transmission range of radar such that all the neighbors inside can be directly detected by radar. Overlap, which is intersection area between two cells, must be decided before the cells are formed. The size of overlap depends on the size of cells and the road condition. If the size of cells is very large, the overlap may be small proportion of the cells; if the road is highway, the overlap may be larger to contain more vehicles as potential routers. In this project, we use a highway scenario, and the cells are 100 meter-radiuses, therefore, we select 20-30 meter overlaps. When vehicles are close to the overlap of two cells, they may be chosen as routing vehicles. The need for routers depends on the transmission range. If the transmission range can reach the next cell leader without needing an intermediate hop, then there is no need to have cell routers. The steps to form a network cell are:

By consulting loaded digit map, each vehicle can decide the width of the overlap regions between two cells;

Partition the digital map into cells, for example 100 meter-radius cells, making sure the overlaps;

Vehicles decide its cells based on its GPS coordinates and preset digital maps;

3.2.1 Cell Leader

Cell leader is determined for each direction. A vehicle close to the centre of the cell would be eligible be the cell leader. Since, we are using preset maps; each vehicle would know which cell they belong to and where the center of the cell lies. Each vehicle would get a credit score depending on the distance from the cell. The vehicle with highest credit score would take over as cell leader and announces its new designation. In cases where more than one car is gets the same score, lower ID would get the precedence [10].

Member vehicles periodically (every 100ms) send position information to the cell leader. Not only cell leader would get this information but also other members of the vehicle. We can reduce collisions due to the periodic broadcast by allowing vehicles to not only broadcast their GPS coordinates but also the position of vehicles in their direct line of sight. Distance and position with respect to the cell leader would decide the next transmission time. In this way, neighboring vehicles need not broadcast their coordinates if they agree with

transmitting vehicle. The cell leader and other members of the cell aggregate this information and build the traffic view.

When a new vehicle enters the system, it waits for 200ms during which it hears the information transmitted by other members of the cell and learns the cell leader's ID. The new vehicle also activates its radar to detect its neighbors. At the end of the time slice, it sends its position information as well as position information of its neighbors. If it was not able to detect the cell leader, it sends a query asking the address (ID) of the cell leader. If no response comes, then new vehicle takes over as a cell leader and announces its new role.

3.3 Local Security

A cell is the smallest entity which can be secured from position attacks. Any member of the cell can verify the GPS coordinates received from any other member using the radar. If the broadcasted coordinates match with radar findings, the message is accepted. The cell leader broadcasts information about its cell members every 100ms (keeping collision warning interval in mind) along with its aggregated traffic view. Since other members of the cell would also see the similar traffic situation, malicious cell leader can be detected, assuming most of the vehicles are honest. If a cell leader lies, the neighbors would broadcast the correct information. The message can be picked up by the cell router, cell leader or any member vehicle depending on the transmission range and traffic condition. Member vehicles reset the relay timer when they receive the message. If a vehicle does not hear the relay of the message before its timer expires, it

would relay the received message. The next relay time would depend on the distance from the source of the message.

3.3.1 GPS Position

In GPS, when satellite radio signals are transmitted, they are distorted by the troposphere and especially the ionosphere; therefore GPS coordinates have some tolerance. GPS data normally changes in the range of $\Delta x = \pm 0.25m$; $\Delta y = \pm 0.25m$ [18]. In Figure 6, we assume that Δy and Δx are always equal, marked as $\Delta\alpha = \Delta x = \Delta y$. The shadow region is the set of all possible real vehicle positions.

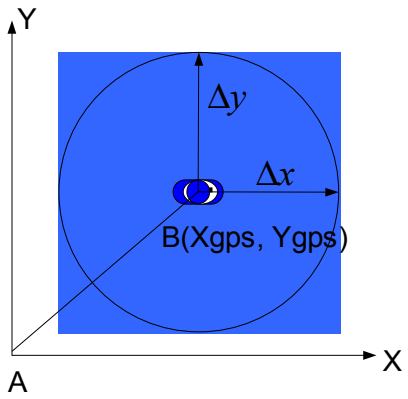

Figure 6, The GPS tolerance causes a set of real GPS position, shown as dark shadow.

We can use formula (1) to describe this region. We use (x, y) to represent the real position of vehicle in the GPS system.

$$(x - x_{gps})^2 + (y - y_{gps})^2 \leq (\Delta\alpha)^2 \qquad (1)$$

3.3.2 Radar Detection

We assume that radar's tolerance includes two parts: angle tolerance $\Delta\theta$ and radius tolerance Δr, marked as ($\Delta\theta$, Δr). In Figure 7, the shadowed region is bounded by *HGQFEP*. We use (x, y) to represent the real position of vehicle in the GPS system and mark the radar readings as (θ, r). We can use formulas (2) and (3) to describe two circles, *circle D* and *circle C* in Figure 7. Without losing generality, we assume the detected vehicle is at the center of the shadow:

$$(x - r \times \cos(\theta - \Delta\theta))^2 + (y - r \times \sin(\theta - \Delta\theta))^2 \le (\Delta r)^2 \qquad (2)$$

$$(x - r \times \cos(\theta + \Delta\theta))^2 + (y - r \times \sin(\theta + \Delta\theta))^2 \le (\Delta r)^2 \qquad (3)$$

θ: The detected angle, starting from north 0 degree;

r : The detected radius (distance between vehicle A and vehicle B);

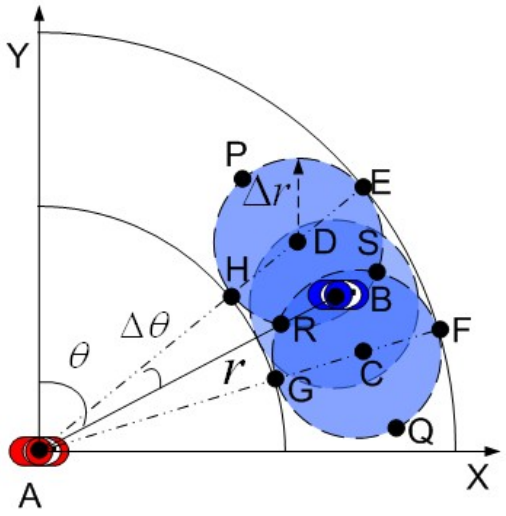

Figure 7. The tolerance ($\Delta\theta$, Δr) of radar system cause a set of real position, shown as light shadow.

We notice that there are two small *regions HRG* and *EBF* where the real position of a vehicle could be that are not described by formula (2) and (3), for

example the *FGHE region* in Figure 7. Therefore we use the formula (4) to describe this region.

$$\begin{cases} r - \Delta r \le x^2 + y^2 \le r + \Delta r \\ \theta - \Delta\theta \le arctg\dfrac{x}{y} \le \theta + \Delta\theta \end{cases} \qquad (4)$$

Although formula (4) includes some region which has been described by formulas (2) and (3), it has no negative effect because we will find an overlap between the GPS position formula and the Radar position formula.

3.3.3 Intersection Region

Without losing generality, we assume that the real vehicle is at the center of GPS position and radar position, shown as the shadowed area in Figure 8. If any of the following combinations has a solution, we can draw the conclusion that the detected vehicle is honest:

Formula (1) and *formula (2)*

Formula (1) and *formula (3)*

Formula (1) and *formula (4)*.

Otherwise, it is determined to be a compromised vehicle. The meaning of these combinations is shown in Figure 8. If the GPS real position is dropping into the radar real position region, i.e. if there is an overlap between the GPS position shadow and radar position shadow, this means the GPS real position is very close the value which is detected by radar system. Therefore we claim that we can accept the GPS position.

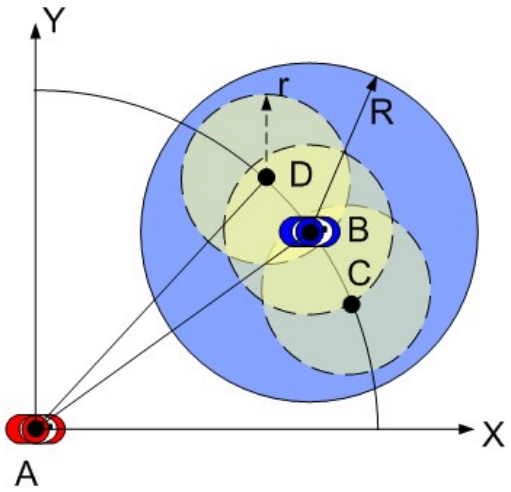

Figure 8. If there has an overlap area between darker shadow (GPS position) and lighter shadow (radar position), we accept the GPS coordinates, otherwise discard it.

3.4 Global Security

Messages broadcasted by the cell leader are picked up by the cell leader of the approaching traffic rather than the one that has already passed that location. A cell leader or any other member of the cell can send a verification request in two ways: proactive [13] and reactive [15, 19]. Proactive means a vehicle can randomly pick a record and request verification. Reactive is when a record is in dispute. Usually a member vehicle waits for the cell leader to send verification request before it sends its own. A vehicle in a nearby cell would more likely to be picked for verification than a vehicle which is far from the cell.

In order to increase the probability of verifying potential malicious vehicles position, we keep track of vehicle movements. Each vehicle in a cell knows the exact position of all the remaining vehicles in a cell by exchanging packets. Vehicles in a cell can query the position of a specified vehicle among the neighbors in the cell. When receiving responses from neighbors and computing

these positions, the requester comes to an agreement about all the neighbors' position. With locally Radar-detected data, oncoming traffic's radar detected data, and trusted neighbors' data in hand; we apply cosine similarity to these data. If the similarity value is above a threshold, we accept the data, otherwise it is dropped. With the accepted data, we build a history of vehicle movements, or a History table. The basic idea is that a vehicle without position history is not trustable, just like a person without credit history can not obtain a loan. When receiving a position announcement, the observer checks the History table to verify the position based on movement consistency. If there is any inconsistency, the particular record is more than likely to be picked up for verification.

A verification request can be sent in two different ways. First, using the vehicles in the same direction and secondly, making the opposite direction vehicles verify the vehicle. The request message travel till it reaches the vehicle which is in direct line of sight of the disputed vehicle. A response message is then sent back to the requester. A positive response would validate the record. The request and response message need not wait for next transmission to happen. They are transmitted as soon as they are received. Because of this the vehicle might receive two confirmations: one from reverse direction vehicles and another from same direction vehicle. Since there is less incentive for reverse direction vehicles to lie, reverse direction confirmation is given more weight.

In Figure 9, vehicle A sends a verification request for vehicle I. The request travels in the same direction as well as opposite direction, and a response is generated by vehicle B as well as vehicle F.

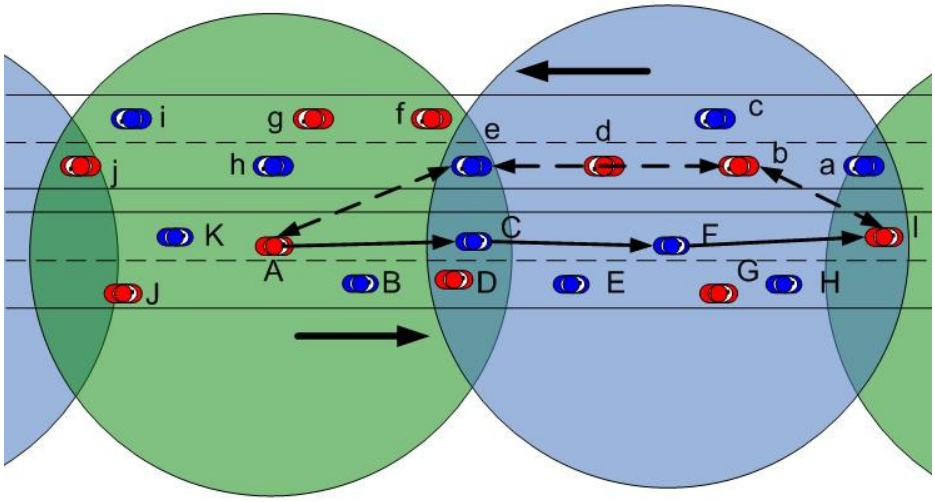

Figure 9. Vehicle A sent a verification request for vehicle I.

4. Simulation

We extended a microscopic traffic simulator based on the microscopic transport simulator from the Dresden University of Technology [16], which features a realistic traffic model. A snapshot is shown in figure 10. Vehicles in our simulator can accelerate if there is reasonable space ahead, decelerate if the space in front is small or forward vehicles suddenly decelerate, completely stop if there is no way to move or change lane or steadily drive and change lanes. In this project, we use a two-direction highway scenario with two lanes in each direction. The total road length is 3 Km, cell radius is 100 meters, traffic arrival rate is 3600 vehicles/ hour, mean velocity is 33.3 m/s, and transmission radius is 100 meters.

Figure 11 shows the comparison of our algorithm with flooding. In flooding each vehicle within transmission range receives the message and broadcasts it to its neighbors' till it reaches the destination vehicle. Our algorithm needs less number of hops compared to flooding.

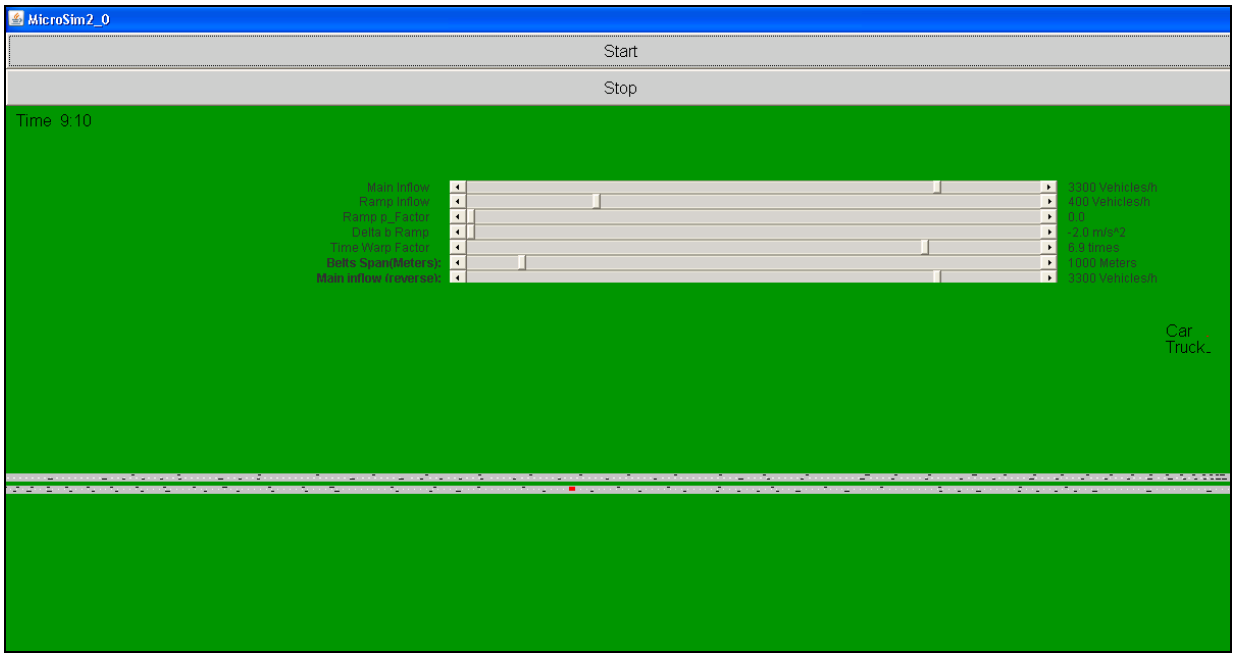

Figure 10. Simulator snapshot

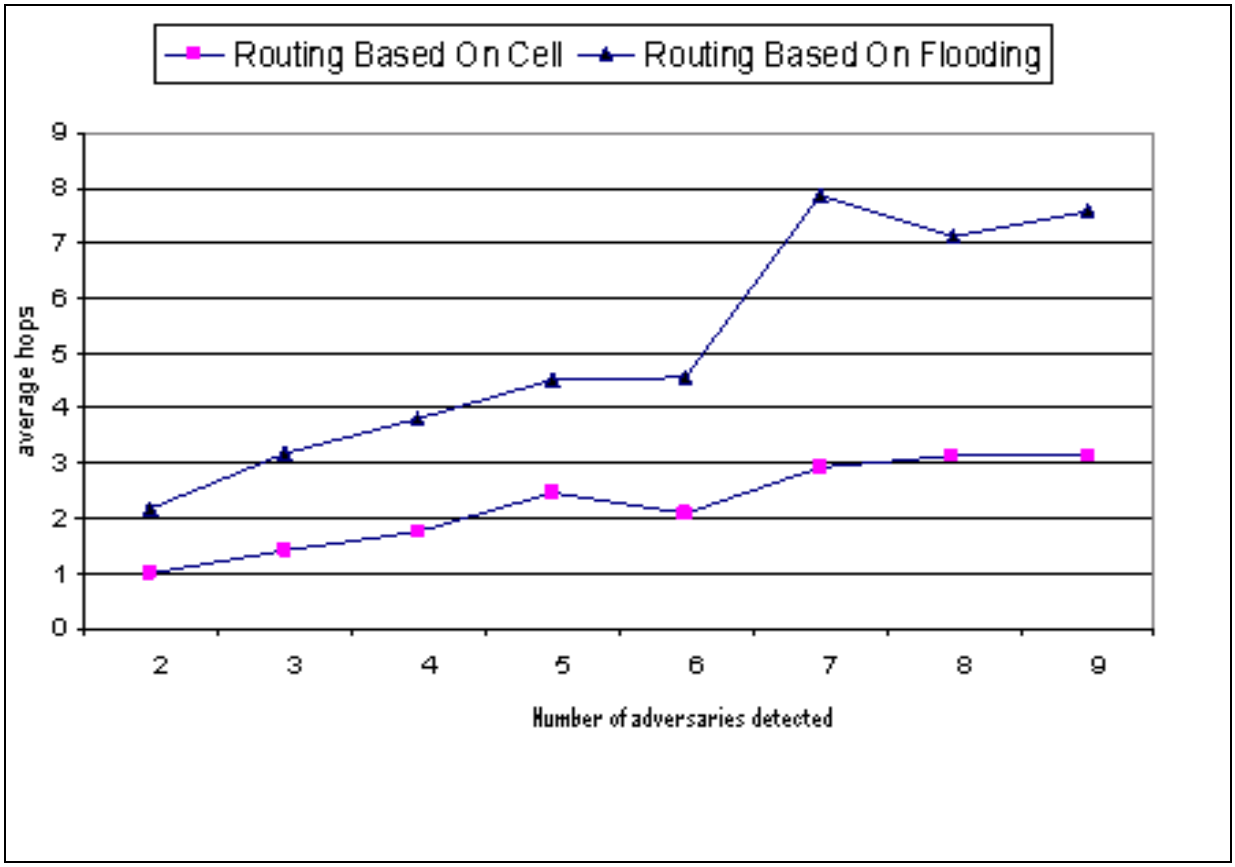

Figure 11. Comparing flooding and our algorithm

The next experiment was run to calculate the time taken to detect the malicious vehicles in the system. The experiment was run for two ranges of transmission: one with a range of 100m and another with a range of 500m. Since the time depends on the number of intermediate hops, the increased range of transmission would certainly decrease the time. However, the increased transmission range would increase the probability of packet collisions. A full network model is needed to evaluate the packet loss. Figure 12 shows the time taken to detect the malicious vehicles with respect to their proximity from the vehicle generating the verification request.

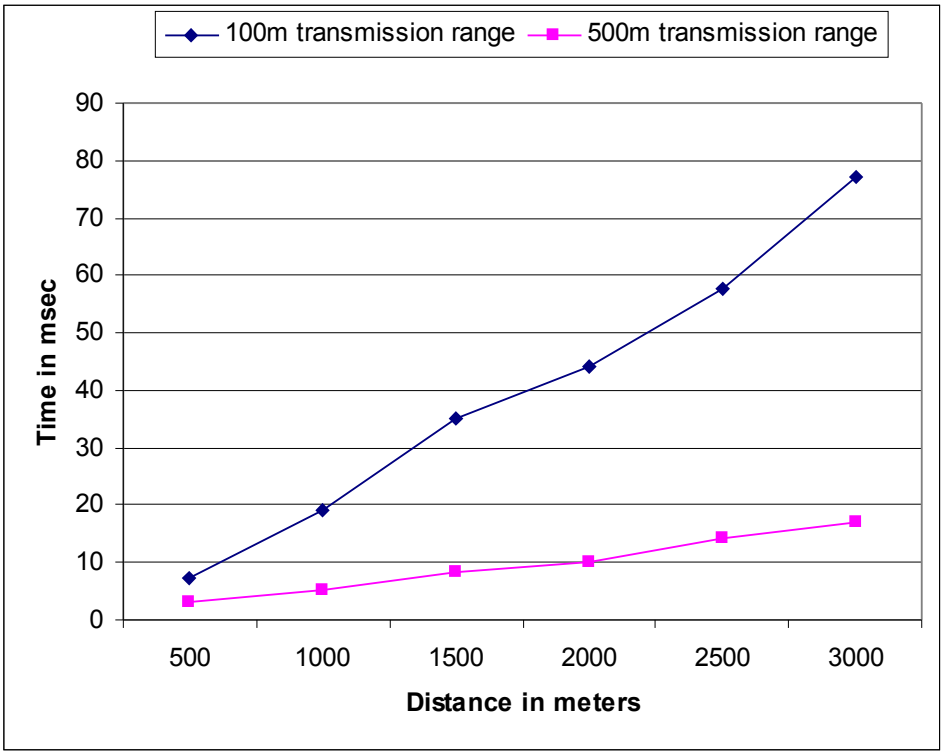

Figure 12. Average time to detect malicious vehicles

5. Conclusion

Detecting false position information and reducing the chances of attack is the key to the success of VANETs. This project focuses on this prime area. Radar acts as the eye of the system and allows a vehicle to trust the information received from the vehicles within its range. The capability to verify record is also available for achieving global security. Our approach is efficient in identifying compromised vehicles and reduces the burden on channel available.

We are working on increasing the precision of our system to detect all compromised vehicles and on simulating the Sybil attack and some combination of Sybil attacks and position attacks.

6. References

[1] Fan Bai, Tamer Elbatt, Gavin Hollan, at el, "Towards Characterizing and Classifying Communication-based Automotive Applications from a Wireless Networking Perspective," AutoNet 2006, December 1, 2006, San Francisco, CA, USA

[2] JoonSang Park, Uichin Lee,Soon Y. Oh, at el, "Emergency Related Video Streaming in VANET using Network Coding," In Proc. 3rd International Workshop on Vehicular Ad Hoc Networks (VANET '06), pages 102-103.

[3] Maxim Raya and Jean-Pierre Hubaux, “The Security of Vehicular Ad Hoc Networks,” SASN'05, November 7, 2005, Alexandria, Virginia, USA.

[4] B. Parno and A. Perrig, "Challenges in securing vehicular networks," Proceedings of the Workshop, on Hot Topics in Networks (HotNets-IV), 2005.

[5] Leinm¨uller, T., and Schoch, E. Greedy routing in highway scenarios: The impact of position faking nodes. In Proceedings of Workshop On Intelligent Transportation (WIT 2006) (Mar. 2006).

[6] Leinm¨uller, T., Schoch, E., Kargl, F., and Maih¨ofer, C. Influence of Falsified Position Data on Geographic Ad-Hoc Routing. In Proceedings of the second European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS 2005) (July 2005).

[7] John R. Douceur, "The Sybil attack, " In First International Workshop on Peer-to-Peer Systems (IPTPS), March 2002.

[8] Philippe Golle, Dan Greene, Jessica Staddon, "Detecting and correcting malicious data in VANETs,"Philadelphia, PA, USA, ,2004,Security in VANET table of contents, Pages: 29 - 37

[9] T. Leinmüller, E. Schoch, F. Kargl, C. Maihöfer, "Improved Security in Geographic Ad hoc Routing through Autonomous Position Verification," VANET'06, September 29, 2006, Los Angeles, California, USA

[10] Maxim Raya, Adel Aziz and Jean-Pierre Hubaux, "Efficient Secure Aggregation in VANETs," VANET'06, September 29, 2006, Los Angeles, California, USA.

[11] M. Raya, P. Papadimitratos, J.-P. Hubaux, "Securing Vehicular Communications," IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, Vol. 13, Nr. 5, pp. 8-15, 2006.

[12] J.-P. Hubaux, S. Capkun, J. Luo, "The Security and Privacy of Smart Vehicles," IEEE Security and Privacy Magazine, 2(3):49-55, May-June 2004.

[13] F. Dai, J. Wu, "MC04-2: Proactive Route Maintenance in Wireless Ad-Hoc Networks," IEEE INTERNATIONAL CONFERENCE ON COMMUNICATIONS, 2005, VOL 2, pages 1236-1240

[14] R. Moebus, A. Joos, and M. Morari, "Multi-Object Adaptive Cruise Control," Proc. Hybrid Systems: Computation and Control, LNCS vol. 2623, Springer Verlag, 2003, pp. 359–376.

[15] Z.J. Hass, "A new routing protocol for the reconfigurable wireless networks," Proceedings, IEEE 6th International Conference on Universal Personal Communications, 1997, pp. 562-566.

[16] M. Treibra, Microsimulation of road traffic, http://www.traffic-simulation.de/,july 2005

[17] IEEE, "DSRC FAQ," http://grouper.ieee.org/groups/scc32/dsrc/faq/.

[18] Lei Tian, Yunshan Zhou, Lie Tang, "Improving GPS positioning precision by using optical encoders," 2000 IEEE Intelligent Transportation Systems, Conference Proceedings, Dearborn (MI), USA Octoberl-3, 2000

[19] M. Käsemann, H. Füßler, H. Hartenstein, and M. Mauve. "A Reactive Location Service for Mobile Ad Hoc Networks. Technical Report TR-02-014, Department of Computer Science," University of Mannheim, November 2002

[20] http://events.ccc.de/congress/2006/Fahrplan /attachments/1216-vanet.pdf