Available online at www.elixirpublishers.com (Elixir International Journal)

Electrical Engineering

Elixir Elec. Engg. 69 (2014) 22965-22968

ISSN: 2229-712X

Security and privacy in places networked car

Masoud Moradi[1] and Hadis Abbasi[2]

[1]Young Researchers and Elite Club, Ilam Branch, Islamic Azad University, Ilam, Iran.

[2]Department of Software Engineering, Qazvin Branch, Islamic Azad University of Qazvin, Iran.

ARTICLE INFO

Article history:

Received: 17 December 2013;

Received in revised form:

20 March 2014;

Accepted: 3 April 2014;

Keywords

Locating,
GPS,
Security,
Location based services,
Privacy.

ABSTRACT

Positioning of nodes in ad hoc networks of vehicles in recent years is an interesting subject for research, helps to build the topologic map for car. It also provides information about places close to the car. For the open wireless communication and mobility with high -speed for a large number of vehicles, in inter- vehicle communication, authentication message, integrity and privacy of the car have been identified as the main security requirements. In this study, methods for vehicle location privacy is proposed, which include: define a switch pair and a number alias for vehicles, vehicle grouping,, select the leader for groups and finally use of several RSUs. At the end of the study, the proposed method is simulated using NS2 software, and some critical parameters of the network, are examined to see the effect of the proposed method on the network.

Introduction

Large-scale and frequent use of cars, have increased car traffic requirements and improve car safety regulations for Highways and streets. Security for passengers, reduced road accidents, rapid assistance accident to victims, distributed intelligent navigation and traffic congestion, infrastructure and look to the future technology are needed; thus, for the detection of increased safety and other economic benefits, which can result in enabling communication between vehicles and vehicle feedback for ad hoc networks, have had continuous coordinated effort to intelligent network vehicles. Vehicular Ad-hoc Network (VANET) is an important component of intelligent systems for car. The main advantage of vehicle connection is the activated immune system. These systems are aimed at increasing the safety of passengers and warning messages exchanged between the vehicles. Also there are other applications personal services for travelers to reduce costs and develop vehicle temporary network. Global Positioning System is a satellite navigation system includes a network of 24 satellites in orbit in six different orbits around the earth. Satellites in this system, are located in the circuits to the height of Km20.200 from Earth, revolve around the earth twice a day and take the information back to Earth. The area of Earth is seen by at least four satellites.GPS receivers use technique of arrival (TOA) to estimate the distance to four known satellites, and use Trilateration [1] techniques to calculate the position. When these procedures are performed, the recipient will be able to identify the length, width and height of the sea surface. The main solution for VANET locating is to equip automobiles with GPS receiver. The advantage of this method is that the receiver can easily be installed in vehicles, but vehicles are often moving in environments where GPS is not available. The main problem is that GPS cannot receive indoors, or underground or tunnels signals; also, vehicles are not necessary equipped with GPS, and even cannot get purpose access line of satellites, particularly when they enter tunnels [2]. VANET networks, which have been investigated as a subset of mobile ad hoc networks (MANET),are a promising approach in the future for intelligent transport systems.

Figure 1 : View of the Global Positioning System

In these networks, nodes which are in fact the vehicles can move with high speed, and communicate with each other through inter-vehicular communication (IVC) orin major road infrastructure, through road vehicular communication(RVC) [3] and activate critical functions; such as cooperative driving, and vehicle tracking data, which increases vehicle safety and reduces traffic congestion, and offers access to a service-based applications [4].However, several challenges in network services, such as having the right to VANET security and privacy issues remain. Vehicle positioning and locating car detached neighbors is very important for the safety of road users. When moving between vehicles and the outside world, was the old dream of human, the first attempts to realize this dream and history goes back more than forty years. The installation of an antenna on certain vehicles such as police cars or emergency and setting antennas on a single frequency within a geographic area, tried to establish a correlation between the radio and the telephone network. From late 1990, with production of low cost GPS receiver and transmitter devices - wirelessly Wireless LAN (WLAN),The car was a significant acceleration in research conversations. Finally, the basic idea of VANET networks for the first time in 1998 by a group called the Delphi Delco Electronics Systems Engineering was proposed partnership with IBM. The main discussion networks VANET is the issue of security, as if these demands are not met, the Nets will be virtually worthless, and attackers can easily

Tele:
E-mail addresses: MasoudMoradi1362@yahoo.com

disrupt the integrity of their networks. Because of the mobility of wireless communications and high -speed vehicles, a large number of communication vehicles, message authentication, integrity and privacy as well as safety requirements have been identified; since these networks to security threats, physical and intellectual, more vulnerable than wired networks. VANET network is a new technology that has recently attention has been focused on the industrial and academic sectors. Vehicles communicate with each other, the core of which includes a number of research intended to improve the safety and security of transportation systems by providing the appropriate application systems, such as alarms when exposed to environmental hazards (such as freezing road surface), traffic and road conditions (such as emergency braking, congestion, or construction areas) and local information are derived. Hubaux and colleagues from EPFL [5] and [6], a framework for analyzing security risks and challenges to security and privacy in VANET are proposed. They have several interesting solution for VANET security as an electronic certificate belt (ELP). Lies in the unique approval number of the vehicle liability certificate with additional straps are VANET. Dötzer and research colleagues from BMW, as well as secure V2I, for communication between vehicles and traffic light units, separate their addresses secret.

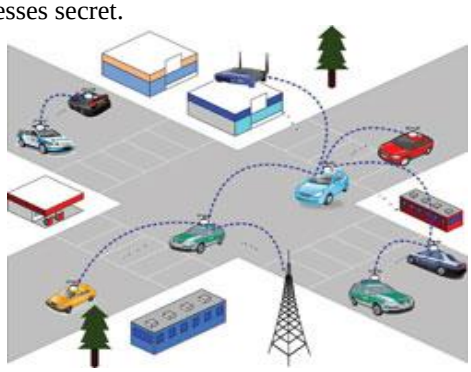

Figure 2: overview of VANET

The probabilistic approach is a promising technique for the switch management is Adhoc networks [7].Zhu et al, probabilistic method for creating a two- way switch between network nodes have been used. Then one of the protocols have been introduced GKMPAN complete tasks within Adhocs witch management for networks is considered. GKMPAN adopts a probabilistic approach to switch distribution based on symmetric keys already expanded.

GKMPAN for mobile wireless networks is efficient and scalable, because of node mobility on the condition lasts. Furthermore, GKMPAN not related to network topology and node locations. A special feature is GKMPAN poker in which a node, two switch groups of a certain number of processes is lost; it can calculate the new group key. However, it cannot update the canceled responsible switches for maintaining the processes lost keys. As the number of revoked keys is not updated increases, it may be necessary to tie the Switch Distribution Center (KDC) to reload a new set of keys to interact[8].Although it has many attractive features GKMPAN protocol, does not consider the latency nodes. At some point during the process group may be transmitted to a node ID, it is clearly necessary. In this way, the attacker can easily trace a particular node which is considered a serious violation of privacy of the drivers. Wasef & Associates, an efficient certificate management for vehicle Adhoc networks (ECMV) based on public switch (PKI) have proposed. In ECMV, each node has a short lifetime certificates that can be updated for each RSU. It depends on frequent updates to keep certification is valid latency. In this study, we decline to address and track the vehicles using an encryption method that involves the following steps have to be.

Working procedures for proposed method

Working procedures for proposed method include:

1 - Assigning aliases and a pair of keys to each node

2 - Group classification of vehicles

3 - Select the group leader

4 –Using a number of RSUs

Assigning a number of aliases and a pair of keys to each node

One of the ways that the improve security and privacy of the vehicles in the VANET network, is that prior to joining the network, each vehicle is to be registered with a reliable source register obtain and a set of a pair of aliases and Public / Private Keys for each alias. Normally, cars readily are being attacked by attacker cars available on the network. With this, attacker vehicles cannot easily obtain information on other vehicles; because the public switch associated with the desired car will be need. As RSUs are semi-reliable, an attacker vehicle can disguise itself to an RSU, to connect with vehicles and acquire their information. What can be done to fix this problem? To prevent these attacks, the RSU can also be equipped with a pair of Public / Private Switch. In this way, the attacker cars that are going to take place in the network as an RSU can be largely countered.

Group classification of vehicles

Grouping method is one of the most important approaches is seen in most modern methods. Increase the efficiency and reduce the network traffic is grouped vehicles. The number of vehicles in the project scenario is 100. The number of nodes was divided into 4 groups of 25 members.

Selecting the leader of the group

If all vehicles have a direct connection with the RSU, network traffic increases, and it is possible that when answering the demand of cars, the vehicle may be removed from the network so generated packet is dropped. This increase drop packets and decrease the network performance. So it is better to define a leader for each group. In the project scenario, nodes 1, 26, 51 and 76 were chosen as the group leaders.

Using multiple RSUs

The most valuable purpose in every network is successful delivery of packets to the destination. Full prevent of attackers from attacking cars available on the network, is unrealizable. Therefore, to reduce the impact of attacks on the network various ways should be used. One of the effects of attacker vehicles in the network is that packet loss rate is increased and the rate of successful delivery of packages has been discarded. If there is only one RSU network, at the same time, various groups may be sending data to or from the RSU, which increase network traffic, and reduce output, and the number of discarded packets and end to end delay is increased. So it is better to use multiple RSUs in the network. In doing so, each group can communicate with the nearest RSU and the percentage of packets successfully delivered in most cases will be increased.

Simulation and its results

At this stage, the outputs of the proposed program are displayed in NS2 software. To evaluate the effectiveness of the proposed methods in VANET networks, we examine some important parameters. The first parameter is discarded information packets, the second parameter is the network output, the third parameter is the successful delivery rate, and the fourth parameter is packet end -to-end delay, and finally, the last parameter, is the maximum tracking nodes in the network. For each of these parameters, a graph is presented. Figure 1 graph shows the number of packets discarded by the network nodes.

The horizontal axis represents the number of network nodes, the number of nodes is 100, and the vertical axis represents the amount of discarded packets at the network level by the attacker nodes in terms of bits per second. As shown in the diagram, we have two curves. Red curve shows the case where the attacker nodes may exist in the network, and the green curve shows the proposed method. It is clear that increasing the number of nodes in the initial state, the number of packets discarded by the network is increased, since the more nodes are trying to send different packets to different nodes. This makes more packets to be trapped by attacker nodes, and be discarded. Comparing the two graphs, we can understand that the proposed method is able to maintain the security of the nodes against attacks by the attacker node; since in this case, fewer packets are discarded.

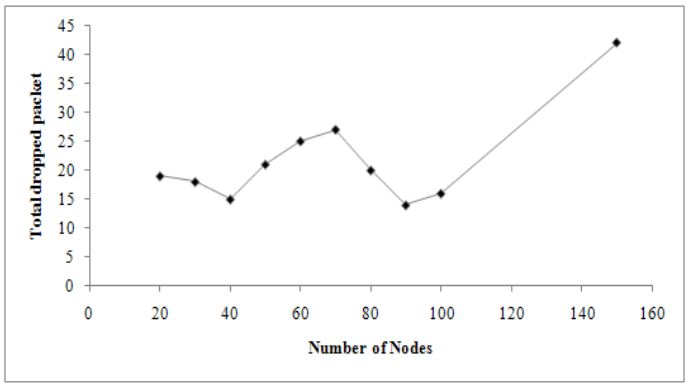

Figure 1: Diagram of data packets discarded by the number of network nodes

Figure 2 shows the output power of the network. The network output power is defined by the number of packets per second that have been delivered to the destination. Since the vehicles should be registered before they are communicating with a source register, and obtain a switch pair, we can conclude that the network output power is reduced compared to when the vehicle enters the network directly and sent the packet to the destination. The output power of the proposed method is slightly different than the first case. In the proposed case, increasing the number of nodes, Throughput is reduced.

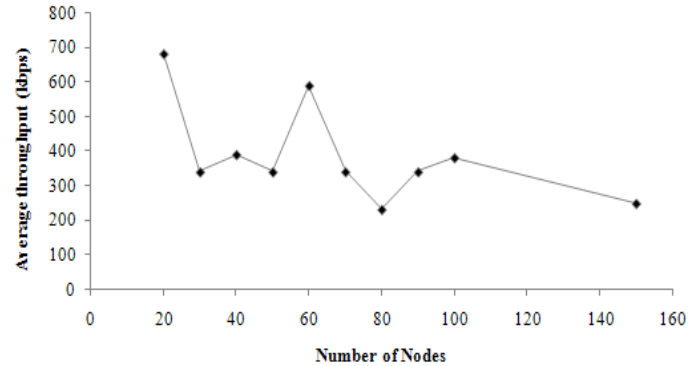

Figure 2 :Throughput Graph versus number of network nodes

The next parameter which is evaluated is the rate of successful delivery of packets. This parameters of the network is important. As shown in Figure 3,we have two curves. The red curve represents the initial state in which nodes have no alias and switches. Green curve shows the proposed method. The vertical axis of this graph shows the percentage of packets successfully delivered, and the horizontal axis shows the nodes participating in a communication for a packet to be delivered. Normally, when the number of nodes participating in the simulation is high, the probability to have attacker nodes is increased, and this means reducing the pdf, which is shown in both graphs. But as shown in the graph, pdf offered in proposed method is more than normal; this means in the normal case, fewer packets will reach the destination.

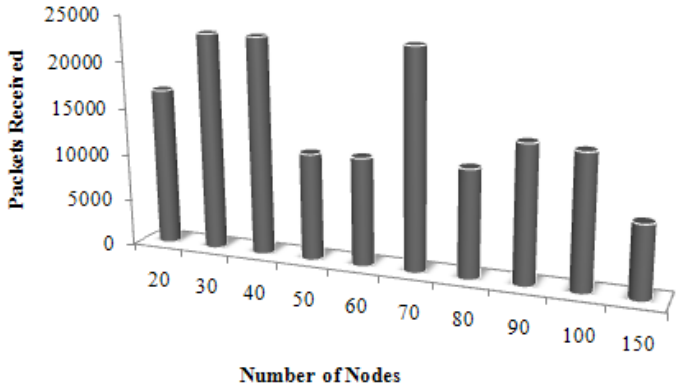

Figure 3: Rate of successful packet delivery ratio compared to the number of jumps

Figure 4 shows the end -to-end delay in terms of number of nodes on the network. In this graph, the red curve represents the normal state of the network and the green curve shows the proposed method. It is clear that increasing the number of nodes in the network will increase the delay between two end nodes. Comparing the two curves, it is observed that in the proposed method packets arrive earlier than normal.

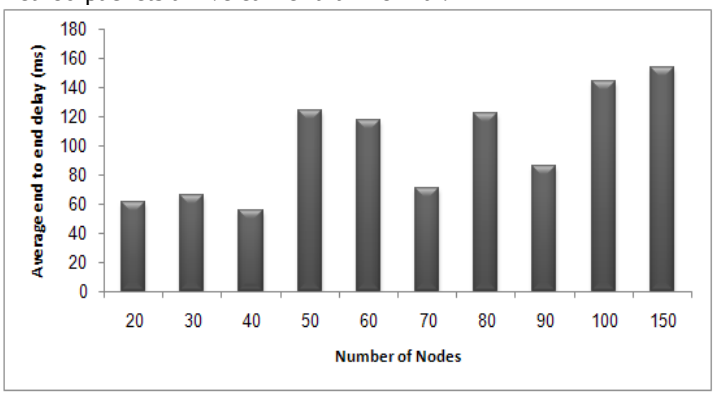

Figure 4: Graph of end -to-end delay compared to the number of nodes on the network

The last parameter studied is the maximum time tracking of nodes in the network. From the Figure 5 we notice that in the proposed method, increase in the number of cars on the network, reduce the time of nodes detection; since updating aliases is increased and the attacker cannot easily identify the desired node.

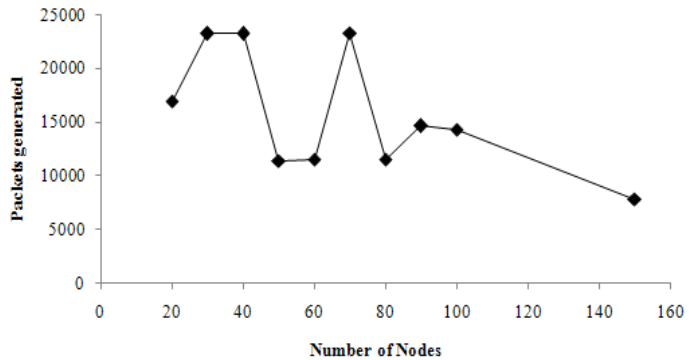

Figure 5: The mean tracking time compared to the nodes number in the network

In this paper, initially, we offered an overview of vehicle networks and the concepts related to it. Then the software used in this study was examined and its benefits and features were mentioned.

Table 1: The results of the simulation

Average throughput(kbps)	Average end to end delay(ms)	Total dropped packet	Packet delivery ratio (%)	Received packets	Generated packets	Number of nodes
680.85	61.4786	19	99.6576	16883	16941	20
340.02	65.9238	18	99.8710	23233	23263	30
390.2	55.7434	15	99.8580	23220	23253	40
340.13	124.106	21	99.782	11432	11462	50
589.17	117.468	25	99.4136	11530	11598	60
340.49	71.215	27	99.8757	23314	23343	70
232.04	122.339	20	99.5844	11503	11551	80
340.31	86.4349	14	99.6859	14600	14646	90
381.17	144.535	16	99.5531	14256	14320	100
249.20	153.53	42	99.0079	7784	7862	150

In the following, some examples of the locating techniques were introduced. Then, issues about the security and privacy of the VANET network were discussed and for security in networks, some solutions were presented. Finally, the results of implementation of these networks with NS2 software were showed.

Challenges

We believe that the first and the biggest challenge for the automotive networks is the security and privacy of the location of the car. One can easily imagine that the smallest threat to these networks will result in severe human and financial consequences. Since this is very critical and for the security of networks equipment improvements are needed, one can say that a reason for non implementation of these networks in recent years is this.

Conclusions and Future Works

In this paper, by the application of VANET networks, we argued that vehicles can communicate with each other and with roadside units, and exchange data with each other and avoid some of the possible pitfalls. Vehicle location and extent of the security in these networks is very important. Finally, a simple implementation of security in VANET networks was introduced. In this implementation, for a number of nodes in the simulation, we defined a switch pair and a set of alias, and we showed that the maximum tracking time was decreased and this shows the increased security of nodes in the network. This is just a small introduction to the security in these networks. Other features can be added to the program to push higher level of security. Security is a critical issue in such VANET networks that is one factor for non implementation of these networks in the past few years. Range of solutions based on data encryption between cars, Network isolation, and the use of authentication mechanisms for new cars that want to get into the network, designing validation specific programs such as ELP and VPKI, and using hardware with 99.99 percent reliability, and dozens of other projects, are some work has been done to secure VANET networks. As part of future work, the proposed solutions can be evaluated using simulators based on mobility vehicles like SUMO, MOVE, Glomosim and... Which combine participated behavior for traffic signs and the impact of tangled packed roads with map data and traffic communication models? Future work is conducted towards extensive simulations and generalization of above solutions. The proposed solutions are not limited to VANET but also are applicable in mobile telephone systems locating.

References

[1] A. Boukerche, H.A.B.F. Oliveira, E.F. Nakamura, A.A.Loureiro, "Localization systems for wireless sensor networks", IEEE Wireless Communications – Special Issue on Wireless Sensor Networks vol. 14, 2007, pp. 6–12.

[1] A.Benslimane, « Localization in vehicular Ad-hoc networks », Proceedings of the 2005 Systems Communications (ICW'05).

[3] S. Capkun, M. Hamdi, and J. Hubaux, "GPS-free positioning in mobile ad-hoc networks", in IEEE Proceedings of the 34th Annual Hawaii International Conference on System Sciences, January 2001.

[4] K. Sampigethaya , M. Li , L. Huang and R. Poovendran "AMOEBA: Robust location privacy scheme for VANET", IEEE J. Select Areas Commun., vol. 25, no. 8, 2007, pp.1569 -1589.

[5] T. S. Rappaport, J. H. Reed, and B. D. Woerner, "Position location using wireless communications on highways of the future", IEEE Communications Magazine, vol. 10, no. 1, pp. 33–41, October 1996.

[6] Y. Zhao, "Mobile phone location determination and its impact on intelligent transportation systems", IEEE Trans. on Intelligent Transportation Systems, vol. 1, no. 1, pp. 55–64, March 2000.

[7] M Moradi, A Ahmadi, "Reducing Energy Consumption in Wireless Sensor Networks Using Hash Distribution Table ",J ElectrEng Electron Technol 2, vol. 2,p.2,2013.

[8] M. Raya and J.-P.Hubaux, "Security aspects of inter-vehicle communications", in Proc. of Swiss Transport Research Conference, March 2005.

[9].Sayadi, R., Abbasi, H., Moradi, M and Abbasnejad, A, 2013. Dynamic Selection of Cluster Heads for Increasing Lifetime in Wireless Sensor Networks with Bloom Filter. J. Basic Appl. Sci. Res. 3(11): 157-165

[10] Somayeh Zalani Sofla, Masoud Moradi, Somayeh Mohammad nezhad, Zahra Abbasi Design of a Novel Nano-Sensor for Determination of Acetaminophen.J. Appl. Environ. Biol. Sci., 4(2)51-56, 2014