Journal of Recent Research in Engineering and Technology
ISSN (Online): 2349 –2252, ISSN (Print):2349 –2260 Volume 2 Issue 2 Feb 2015

VANET-Based Secure Online Road Navigation

[1]C. Prabakaran, [2]L.Priyadharshini.

[1]PG Scholar M.E Computer Science And Engineering,Karpagam University, Coimbatore.
[2]Assistant Professor, Computer Science And Engineering,Karpagam University, Coimbatore.

Abstract

Online road information is collected by a vehicular ad hoc network (VANET) to direct the drivers to the desired target locations in both real- time and distributed manner. A VANET-based secure and privacy preserving online road navigation scheme is implemented, the advantage of utilizing this scheme is to compute a better road map (route) by giving the appropriate source information. To ensure the protection of the drivers, the query (about target location) and the user (driver) who issues the query messages are ensured to be un-sinkable to any client, including the trusted authority or the third party. We make utilization of the ideas and methods of anonymous credential to accomplish this objective. Our scheme satisfies all other necessary security issues, in addition to the authentication and privacy preserving.

Keywords- Navigation scheme, secure vehicular network, signature certification, pseudo identity, anonymous credential.

I. INTRODUCTION

The application of VANET is to provide the safety messages to the vehicles like its speed, direction, traffic information, etc.., likewise it should be able to facilitate the communication between the vehicles (V2V- vehicle-to-vehicle) and to vehicle-to-infrastructure communications (RSU). So the vehicles can able to modify their travelling distances and RSUs may educate the traffic control focus to adjust the traffic lights for avoiding the near traffic congestion. A VANET adopts itself to be the sensor network, because the vehicles can

Collect as many useful information about the road conditions. The traveling routes are analyzed easily by the VANET using Dedicated Short Range Communication (DSRC) protocol, but it also requires the privacy protection and security.

In existing the navigation system, the trusted authority has the ability to reveal the genuine identity of a vehicle. In the event that the navigation system is not precisely outlined, it implies that the genuine identity of a driver and the query issued by him can be effortlessly connected up and examined. While we still need the (Trusted Authority/Party) TA to have the authority to uncover the genuine identity in light of a pseudo identity, we need to guarantee that the TA does not know where the driver needs to go. The disadvantages in this system is the Traffic Message Channel (TMC) makes use of the FM radio data system to broadcast the real-time traffic information
and weather reportings to the drivers. The special equipment is required to filter (decode) the received information and the drivers can receive only the road conditions that are being broadcasted but they cannot get the information of general fluency about a road from TMC.

In order to overcome these disadvantages the proposed VANET-based Navigation scheme

collects many information. Based on the target and current location of the driver's query the system can automatically search for the route maps, which yields to a minimum delay in travelling using the online information about the road condition. In addition, of guidance to the drivers, the navigated results can also be used for any other purposes. We proposed to use the routes for strategic routing multi-media information such as videos and images about a desired scene to vehicles.The Privacy leakage approach is applied to use different authentications but it should not be related to the pseudo identity to communicate with various RSU. By collecting all the shared messages between a vehicle and all of the RSU's cannot link the shared messages to reconstruct the driving routes or it cannot analyze the driving habits of a person. The VANET-based navigation system satisfies the security and privacy issues. This scheme implements some of the security issues in a nontrivial way to provide the security to the navigation service.

The rest of the paper is organized as follows: Section presents the related works and research in specific areas. The proposed approach has been discussed in Section 3. Section 4 presents the simulation results. Section 5 concludes the paper.

II. RELATED WORK

VANET have received tremendous attention to enhance active and protective route information for comfort travelling. Security and privacy are essential in vehicular communications for greater acceptance of such technology. Usually attacks cause deviation to the network functionality. So there is necessity for secure exchange of messages from eavesdropping. For a secure VANET system [1] the authentication scheme-proxy re-encryption is implemented to reduce roaming networks by using the public key that is assigned to each of the delegates and delegator, this will improve the security issues in forwarding the messages with less overheads in transmission of the messages.

Delay Tolerant Networks (DTNs) are a class of the network that enables communications with high latency, symmetric transfer of data rates and high data rates. This DTN architecture model has applied in [3] vehicular networks and it is said to be as a Vehicular Delay Tolerant Network (VDTN). In this vehicular network they implement the message relay service method in their mobile and gather the messages from the source node. This method will review the routing protocols in DTN and has the comparative study with the VDTN in terms of route maps, awareness of traffic and traffic data rates.

VANET is the subclass of Ad-hoc network, which has a high amount of potential technology. The major difference between the Mobile Ad hoc Network (MANET) and VANET is the special mobile patterns and rapid growth of changing topologies. [6] Issues in VANET are the mobility predictions and routing protocols to support the smart Intelligent Transportation System (ITS). The performance of prediction technique is necessary for different vehicle users.

Many routing protocols have been proposed and determined to increase the efficiency of VANET. Simulation of the AODV routing protocol is implemented to generate simulators for identifying the [8] routes using mobility models. The simulation results and the performance of the AODV protocol is used to analyze throughputs in sending, receiving and dropping of the query messages, the packet size of those messages. The results are performed with three of the high density networks and achieves the average simulation delay in the networks.

For secure inter and intra vehicles communication the authenticate communication model is utilized. The architecture model makes use of the distributed database concept. In this model each and every driver of the vehicles has to prove his identity to certified authority [9] for

communication rights. In addition to the distributed database storage system the system has to improve the response time of local servers and increase in the throughput of server operation. Using of several protocols and different types of communication patterns to make the VANET communication for secure and safe application.

VANET are themselves to be one of the liable against the attacks which can lead directly to the corruption of the networks by causing big damage and loss in money and the human's lifetime. [13] For strong and secured VANET communication, the secured communication framework is used with powerful routing algorithms for providing the facilities in the detection of malicious vehicles and to reduce them.

III. SECURE VANET-BASED NAVIGATION SYSTEM

For secure navigation service the VANET-based navigation system is utilized to provide security and privacy preservation. The Pseudo identity idea is implemented to achieve the property of security, authentication and privacy preservation, at the same time the vehicle's real identity can also be traced in the case of necessary issues. By using the idea of anonymous credential the system can able to protect the user's navigation queries, responses and the operators information in a confidential manner. The information provided by the vehicle-to-infrastructure (RSU) can also be properly authenticated efficiently.

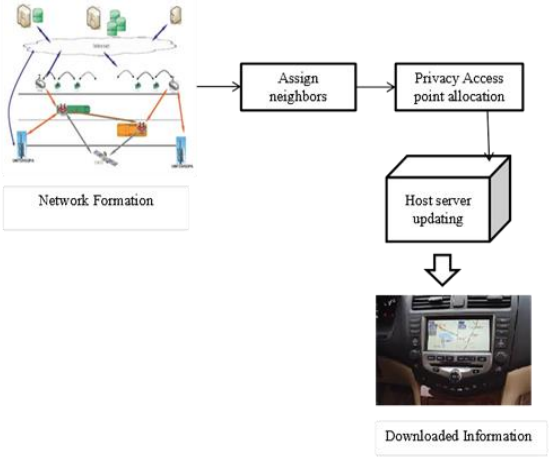

Figure.1 Authenticated navigation information

A. Network formation and assigning neighbors

The Network is formed among the vehicles by analyzing the nearest base station for net accessing to know their vehicle's current location. In Figure.1 The network formation can analyze the different access points of the vehicles that are travelling at different locations. So, that the access points are tracked and characterized by the short-range of coverage areas (i.e. Hundreds of meters), relatively with cheap and easy deployment along with the high data access rate. Within a network the access points of the vehicles vary accordingly with the distance between them. The access point distance of each vehicle and its range can be added up to calculate the maximum value. The coverage areas end access point will be the maximum value. The access point distance which is less than the maximum value will be assigned as the neighbor vehicle, the network itself will assign it.

B. Privacy access point allocation

The vehicle's access point should be allocated in a privacy manner when the vehicle is moving from one access point to the other access point. The VANET-based navigation scheme is used for providing security and privacy facilities for the vehicles while sharing the messages.

(i) Message integrity and authentication

Before the generation of navigation query the vehicle should be authenticated. At the same time vehicle communicating with the infrastructure (RSU) is able to verify the message (query) sent and signed by the particular RSU without being modified by anyone.

(ii) Identity of privacy preserving

The original identity of the vehicle should be kept secret from knowing it to the other vehicles and RSU. Similarly the third-party (TA) should also cannot be able to reveal the original identity by analyzing the multiple messages or queries that are sent to the RSU. Thus the TA performs two simple operations for privacy preserving. First, TA computes the credential for the current duration as $C = < NC, t, TA_{SK} >$. Where C is represented as the credential, NC denotes Navigation Credential, t represent time and TA_{sk} denotes the secret key of third-party. Then the TA securely sends the encrypted credential message EN (C) to all of the RSU, thus the C does not carry any information about the user and hence it is said to be as the anonymous.

(iii) Tracking

However the original identity is being hidden from other vehicles and RSU, the TA- third party has the ability to obtain the vehicle's original that is the real identity of the vehicle and only because of this the vehicle can be charged for the navigation services. The TA has the major role to maintain the non-reputed message properties and thus it helps to trace the location if any accidents happen on the road.

(iv) Confidentiality

The content of the query message and the navigated result should be kept confidential from the eavesdroppers. This is performed by generating the public key (master key) while sharing the message and response from user to RSU or in vice versa. Tamper- proof is a device used for confidentiality, the device signs the query message request along with the master key (MK_req) before sending it to the RSU. Similarly, on the RSU operator's side the device signs the key (MK-res) along with the navigated result. Thus the queries are shared authentically.

(v) Unsinkable

Even if all the RSU and TA collide with each other they cannot be able to make a link up with the vehicle's query message and its original identity. Because the distributed denial of service (DDoS) attacks are different in the VANET environment.

C. Host Server Updating

According to the user's query like roadside information, traffic information, destination's information, etc, to the RSU. The RSU operators will transfer the secure information to the user's server database and the administrator (the user) can only be able to access the update permissions from the network.

D. Downloaded Information

Whenever the vehicle request to know about the current location the query message is sent to the nearest neighbor access points. The access point will forward the request to the web service (base station RSU). So that the RSU can retrieve the data for the query message from the database and then it updates its responses to the requested access point. Thus the response received access point will forward the information to the requested vehicle. By this VANET-based navigation scheme the vehicles can download the information about the location, accident, traffic, etc.

IV. SIMULATION RESULTS

Simulations are carried out to evaluate the performance of the proposed approach. Here, VANET simulator is used as a simulation

environment to perform simulation. The performance of the proposed approach is analyzed in terms of processing time. Table.1 indicates the simulation parameters

Simulation Parameters	
Channel type	Wireless
Network Interface type	Physical Interface
Routing protocol	Dedicated Short Range Communication (DSRC) protocol
Number of vehicles in a network	7
Processing time	$\frac{Distance}{Travelling\ time}$

Table 1. Simulation parameters

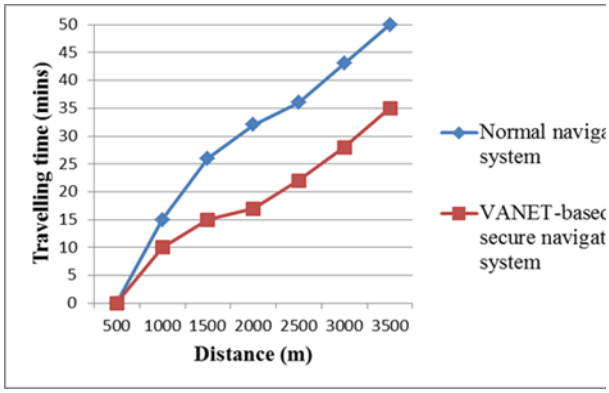

Figure.2 Comparison between a Normal and VANET-based secured Navigation system

Figure.2 shows the comparison of Processing time between the VANET-based secured navigation system and Normal map data searching scheme. Implementation of VANET based secure navigation scheme is used to simulate the results of secure navigation service with reduced processing delay and reduction in the travelling time of sharing the secured and privacy query message and response between the user and RSU operator, when compared to the normal navigation system.

V. CONCLUSION

A VANET-based secure and privacy preserving online road navigation scheme is implemented based on the target location and current location of the driver's query, the system can automatically search for the route maps that yields to a minimum delay in travelling using the online information about the road condition.The Privacy leakage approach is applied to use different authentications but it should not be related to the pseudo identity to communicate with various RSU. By using the idea of anonymous credential the system can able to protect the user's navigation queries, responses and the operators information in a confidential manner. The information provided by the vehicle-to-infrastructure (RSU) can also be properly authenticated efficiently. The performance results of VANET-based secure and privacy preserving navigation scheme produces less travelling time to update the navigated result when compared to the normal navigation system.

REFERENCES

[1] Surabhi Mahajan and Prof. Alka Jindal, "Security and Privacy in VANET to reduce Authentication Overhead for Rapid Roaming Networks**",** International Journal of Computer Applications (0975 – 8887)Volume 1– No.20, February 2010.

[2] Hang Dok, Huirong Fu, Ruben Echevarria, and Hesiri Weerasinghe, "Privacy Issues of Vehicular Ad-Hoc Networks", International Journal of Future Generation Communication and Networking Vol. 3, No. 1, March, 2010.

[3] Ramin Karimi, Norafida Ithnin, Shukor Abd Razak, Sara Najafzadeh**, "**DTN Routing Protocols for VANETs: Issues and Approaches", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011.

[4] A. Sajid, A.H.S Bukhari and A.W. Shaikh, "Privacy issues in VANETs Intelligent Applications",Sindh Univ. Res. Jour. (Sci. Ser.) Vol.43 (1-A) 35- 42 (2011).

[5] Mr. Yugal Kumar, Mr. Pradeep Kumar and Mr. Akash Kadian," A Survey on Routing Mechanism and Techniques in Vehicle to Vehicle Communication (VANET)", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.1, Feb 2011.

[6] Prof. Uma Nagaraj, Amit Bharane Bhushan Chaudhari, Ankit, "Mobility Prediction and Routing in Vehicular Ad hoc Network", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 2,Mar-Apr 2012, pp.1514-1518.

[7] Bijan Paul, Mohammed J. Islam, "Survey over VANET Routing Protocols for Vehicle to Vehicle Communication",IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661, ISBN: 2278-8727 Volume 7, Issue 5 (Nov-Dec. 2012), PP 01-09.

[8] Tajinder Kaur, A. K. Verma," Simulation and Analysis of AODV routing protocol in VANETs", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012.

[9] Ms. Bhagyashree Dharaskar, Dr. R.V. Dharaskar,Dr. V. M. Thakare, "A Novel Architecture for Authentication and Secure Communication in VANET",International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 5- May 2013.

[10] Maria Elsa Mathew and Arun Raj Kumar P,"Threat Analysis and Defence Mechanisms in VANET "International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 1, January 2013.

[11] R.Rajesh kumar, S.Wahida Begum, M.Manikandan," Distance Based Accident Prevention inIntersection Using Vanet", International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Issue 3, March 2014.

[12] Ram Shringar Rao,Sanjay Kumar Soni,Nanhay Singh,and Omprakash Kaiwartya, "A Probabilistic Analysis of Path Duration Using Routing Protocol in VANETs",International Journal of Vehicular Technology Volume 2014.

[13]Vinh Hoa LA, Ana CAVALLI, "SECURITY ATTACKS AND SOLUTIONS IN VEHICULAR AD HOC NETWORKS: A SURVEY",International Journal on AdHoc Networking Systems (IJANS) Vol. 4, No. 2, April 2014.