International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 5 040 – 043

Security and Privacy of Navigation in VANETs

Rupa Rani
Department of Computer Science and Engineering
G.H Raisoni Institute of Engineering and Technology for Women
Nagpur, Maharashtra, India
rupa_singh1986@yahoo.in

Prof. Priyanka Fulare, Sapna Khapre
Department of Computer Science and Engineering
G.H Raisoni Institute of Engineering and Technology for Women
Nagpur, Maharashtra, India
Priyanka.fulare@raisoni.net, sapnakhapre27@gmail.com

Abstract:- In this paper we are providing a secure and privacy preserving navigation in vehicular Adhoc network (VANETs). These VANETs require a technique to authenticate message, identify valid vehicles and remove malevolent vehicles. This proposed scheme has the advantage to compute better route by using real time road conditions and at the same time message can be properly authenticated. In this we are using ideas of anonymous credential to protect the privacy of drivers and the driver who issue the query are guaranteed to be unlikable to any and any party including the trusted authority. In this we are using RC6 algorithm to provide security of message and AODV routing protocol to exchange the message.

Index Terms *- Navigation, privacy preservation, RC6, Vehicular Ad Hoc Networks, secure navigation and AODV routing protocol, network simulator-2 (NS2).*

*****

I. INTRODUCTION

It is a very common experience for all drivers to find route to a certain destination. In old days drivers usually refers to the hard copy of atlas.After that global positioning system(GPS) has introduced[1]. Recently GPS based navigation system becomes very popular[2]. In this system a small hardware device is installed on the vehicle to compute better and shortest route.However on the basis of local map data base route searching procedure is done but real time road conditions are not taken into account. After that Traffic Message Channel(TMC)[3]become popular and also fullfill these requrements. This TMC uses FM radio data system to broadcast real time traffic and weather information to drivers.But the driver cannot obtain lattest and current message from the TMC. Recently ,Vehicular Adhoc Network (VANET) becomes very popular among all over contries.It is an important element of intelligent transportation system(ITS)[4].In VANET every vehicle have an on board unit(OBU) and road side unit(RSU).The OBU , installed on the vehicle and RSU installed along the road. At the back end ,trusted authority(TA) and some other server are installed. The OBUs and RSUs uses Dedicated Short Range Communications (DSRC)[5] protocol to exchange the message over the wireless channel and RSU , TA and some other important server exchange the message using internate. The communication from the VANETs are devided into two parts. First one is the vehicle to vehicle(V2V) communication and second one is vehicle to infrastructure communication(V2I). The main function of VANET is to broadcast safety messages that means accident information, turning direction, weather information,traffic congestion to other nearby vehicles. Althow many advantages of VANETs are descrived in the literature.In last few years, many research work have done on the VANET to provide security and privacy of the message[6],[7],[8],[9].

In this paper, we propose a new VANET based navigation scheme for privacy preserving system in VANETs, which make use of collected data to provide navigation service to drivers. In this, we make use of AODV routing protocol to find out the shortest route to the destination.

For a VANET-based navigation system, there is a additional requirements of security and privacy that makes the problems non-trival. In a basic VANET system, the real identity of vehicles can be easily revealed by the trusted authority (TA). If the navigation system is not carefully designed, it means that the real identity of a driver and the query issued by him can be easily linked up and analyzed. While we still want the TA to have the authority to reveal the real identity based on a pseudo identity, we want to ensure that the TA does not know where the driver wants to go.

In navigation system, basic confidentiality is another important factor. In this the vehicular may not want to any nearby vehicle to his/her destination by eavesdropping to the query. And also when the system sends the navigation result to the driver, then the driver may not want that the nonsubscribers nearby to enjoy free navigation service to follow the same destination.

Our scheme that means navigation scheme for privacy preserving system in VANETs provides the various security features:- (1) The vehicle should be properly authenticated when using the navigation service.(2)The real identity of vehicle and navigation query issued by the driver are properly delinked using the ideas of anonymous

credential.(3)Information provided by the RSU to the driver should not been interrupted by the any one or any party.

The rest of the paper is organized as follows. The related work is outlined in section II, in which system model and security objectives are outlined for motivation of the paper. Proposed algorithm and protocol for secure and privacy preserving service in VANETs contains in section III. IV describes the implementation of the proposed system. Last section i.e. section V presents the conclusion.

II. RELATED WORK

The ideas of navigation in VANET are taken from the work [10]. Chaum at [11] described the anonymous credential in the navigation scheme. By Samara et al[12]security issues and challenges have been described. We also refer [13]-[25] for my work.

A. *System Model*

In this section, we describe our system model in which nodes may the vehicle, RSU or TA as shown in figure 1.

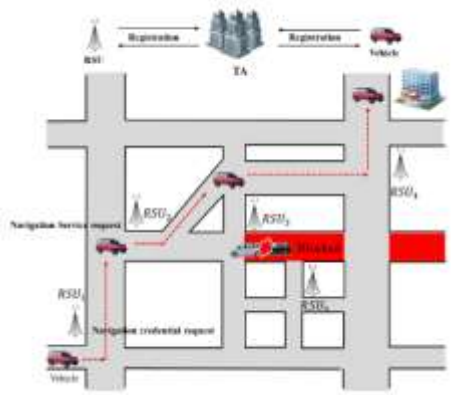

Figure 1: System Architechure

From the figure, each vehicle is assumed to have an OBU and RSU installed along the road. The TA and some important servers are installed along the road.

1. Trusted Authority (TA) performs cryptographic operations like key generation but it is very curious about the vehicular privacy.
2. For the management of Anonymous credential, TA and Tamperproof device on vehicles are assumed to be trusted.
3. RSU are situated along the road and it is not trusted like the TA.
4. The communication between the RSU and TA is done by the fixed network called as internet.
5. Each vehicle has its own real identity and their real identity is known by only by the TA not by the other.
6. Each RSU storing a local data map storing information in its range like GPS location of boundaries, name of building streets, distance and direction to get to its neighboring.
7. Temper proof device is mounted on every vehicle and this device is responsible for all cryptographic operations such as key storing function, pseudo identity generation, signing of message and encryption and decryption of message.
8. RSUs, TA and temper proof device have a synchronized clock and by using this clock TA broadcast current time periodically to all tamperproof device and RSUs.

B. *Security objectives:-*

Requirements of security objectives to provide secure and privacy preserving in VANETs are as follow..

1. ***Message integrity and authentication***. Before issue the navigation query the vehicles should be properly authenticated. RSU and vehicle should also be ensure that the message or query signed by certain RSU and vehicle should not be modified by anyone.
2. ***Identity privacy preserving***. The real identity of vehicle should not be attacked by any third party.
3. ***Traceability***. The real identity of vehicles should be hidden from by the neighbourhood vehicles and RSUs. Only TA has the ability to obtain the real identity of vehicles so that the TA authority can be charged him according to their navigation query.
4. ***Confidentiality.*** All the navigation query should be kept confidential from the third party.
5. ***Unlinkability.*** *When the RSU and TA come together the TA should not be link the real identity of vehicle.*

III. PROPOSED SYSTEM

In this section, we are using RC6 algorithm for secure transmission of data and AODV routing protocol for shortest route to the destination. We have divided the work in four different parts.1.Development of vehicular network 2. Integration of navigation module 3.Development of a secure navigation protocol 4. Development of a privacy preserving navigation protocol.

From the first part i.e development of a vehicular network, there is a network formation between the vehicle to vehicle, vehicle to infrastructure or vehicle to RSU. Nodes do not connect directly to each other.NS2 connect the nodes with the help of agent. In this there are two agents, source agents and destination agents. Source agent is called as UDP agent and destination agent is called as null agent. The communication between these agents or nodes is done by the constant bit rate (CBR) traffic. The main function of CBR is to inform which packet we to send, which packet we to receive, what is the time of packet that is to be send or receive. The snapshot of this part is as follow:-

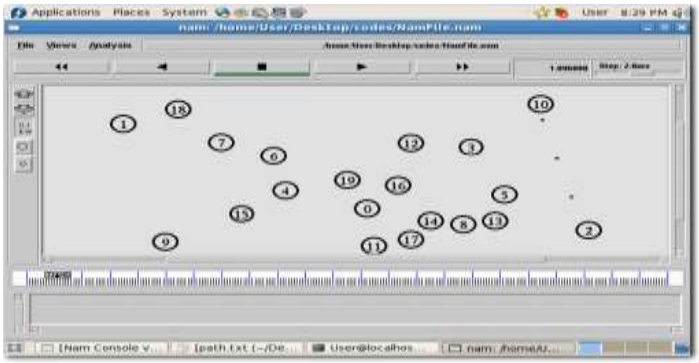

Figure2: Snapshot of node communication

Our second part is integration of navigation module. In this module, we will find out the latitude and magnitude of the nodes that means actual position of the nodes. When the two nodes come in between the 10 m area of range, then the system will send the alert message to the both nodes that you might be collies with each other and you can change the path or the direction. The snapshot of this part is as follow:-

Figure3: Snapshot of nodes colliding

From the third part i.e. Development of secure navigation protocol. In this we are using RC6 secure algorithm to provide the security on the navigation query.RC6 is designed by Ron Rivest in 1998.It uses the block size of 128 bits and key size of 128,192 and 256 bits and takes 20 number round to complete the encryption and decryption of data. The main aim of this part is to provide security to the navigation query which is issued by the driver. The snapshot of module 3 is as follow:-

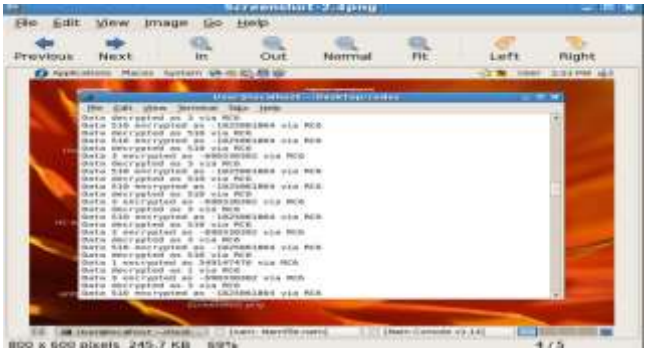

Figure4: Snapshot of Encryption and Decryption of data

IV. IMPLEMENTATION

NS2 is the simulation environment that is used to analyze the proposed system. Network Simulator-2 (NS2) is an event-driven simulation tool that is used to study the dynamic nature of communication network. Simulation of wired as well as wireless network functions and protocols can be performed in NS2. NS2 provides users with a way of specifying network protocols and simulating their corresponding behaviors. C++ and Object-oriented Tool Command Language (OTcl) are two key languages in NS2. NS2 outputs text-based simulation results after simulation. There are tools such as NAM (Network AniMator) and XGraph to interpret these results graphically and interactively.

V. CONCLUSION

In this paper, we have proposed new secure and privacy preserving navigation protocol that overcome the problem of [19]. The proposed protocol provide better route in less and also prevents from the traffic congestion and will provide more secure and privacy preserving system in VANETs

REFERENCES

[1] Global Positioning System Standard Positioning Service Signal Specification. Navtech GPS Supply, 1995.

[2] Papago! Z-Series Navigation System," http://www.papago.com.hk/, 2009.

[3] B.-J. Chang, B.-J. Huang, and Y.-H. Liang, "Wireless sensor network-based adaptive vehicle navigation in multihop-relay wimax networks,"in Proc. of the 22nd International Conference on Advanced InformationNetworking and Applications (AINA'08), Okinawa, Japan. IEEE,March 2008, pp. 56–63.

[4] F. Wang, D. Zeng, and L. Yang, "Smart Cars on Smart Roads: An IEEE Intelligent Transportation Systems Society Update," IEEE Pervasive Computing, vol. 5, no. 4, pp. 68-69, Oct.-Dec. 2006.

[5] H. Oh, C. Yae, D. Ahn, and H. Cho, "5.8 GHz DSRC Packet Communication System for ITS Services," Proc. IEEE VTS 50th Vehicular Technology Conf. (VTC '99), pp. 2223-2227, Sept. 1999.

[6] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "Gsis: A secure and privacy preserving protocol for vehicular communications," IEEE Transactions on Vehicular Technology, vol. 56, no. 6, pp. 3442–3456, November 2007.

[7] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications," in Proc. of the 28th IEEE International Conference on Computer Communications (INFOCOM'08), Phoenix, USA. IEEE, April 2008, pp. 1229–1237.

[8] Y. Park, C. Sur, C. D. Jung, and K.-H. Rhee, "An efficient anonymous authentication protocol for secure vehicular communications," Journal of Information Science and Engineering, vol. 26, no. 3, pp. 785–800, May 2010.

[9] C. Sur, Y. Park, K. Sakurai, and K. H. Rhee, "Providing secure location-aware services for cooperative vehicular ad hoc networks," Journal of Internet Technology, vol. 13, no. 4, pp. 631–644, July 2012.

[10] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A New VANET Based Smart Parking Scheme for Large Parking Lots," Proc. IEEE INFOCOM '09, pp. 1413-1421, Apr. 2009.

[11] D. Chaum, "Security without Identification: Transaction Systems to Make Big Brother Obsolete," Comm. ACM, vol. 28, pp. 1030-1044, 1985.
[12] G. Samara, W. Al-Salihy, and R. Sures, "Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)," Proc. IEEE Fourth Int'l Conf. New Trends in Information Science and Service Science (NISS '10), pp. 393-398, May 2010.
[13] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran,"AMOEBA: Robust Location Privacy Scheme for VANET," IEEE J. Selected Areas in Comm., vol. 25, no. 8, pp. 1569-1589, Oct. 2007.
[14] C. Zhang, X. Lin, R. Lu, and P.H. Ho, "RAISE: An Efficient RSUAided Message Authentication Scheme in Vehicular Communication Networks," Proc. IEEE Int'l Conf. Comm. (ICC '08), pp. 1451- 1457, May 2008.
[15] A. Wasef and X. Shen, "PPGCV: Privacy Preserving Group Communications Protocol for Vehicular Ad Hoc Networks," Proc. IEEE Int'l Conf. Comm. (ICC '08), pp. 1458-1463, May 2008.
[16] T. Chim, S. Yiu, L.C. Hui, and V.O. Li, "SPECS: Secure and Privacy Enhancing Communications for VANET," Elsevier Ad Hoc Networks, vol. 9, no. 2, pp. 189-203, Mar. 2010.
[17] B. Chaurasia, S. Verma, G. Tomar, and S. Bhaskar, "Pseudonym Based Mechanism for Sustaining Privacy in VANETs," Proc. IEEE First Int'l Conf. Computational Intelligence, Comm. Systems and Networks (CICSYN '09), pp. 420-425, Sept. 2009.
[18] R. Hwang, Y. Hsiao, and Y. Liu, "Secure Communication Scheme of VANET with Privacy Preserving," Proc. IEEE 17th Int'l Conf. Parallel and Distributed Systems (ICPADS '11), pp. 654-659, Dec. 2011.
[19] T.W. Chim, S.M. Yiu, Lucas C.K. Hui "VSPN: VANET-Based Secure and Privacy-Preserving Navigation"2014,IEEE Transaction on Computers,Vol. 63, No. 2.
[20] X. Lin, R. Lu, X. Liang, and X. Shen, "STAP: A Social-Tier-Assisted Packet Forwarding Protocol for Achieving Receiver-Location Privacy Preservation in VANETs," Proc. IEEE INFOCOM '11, pp. 2147-2155, Apr. 2011.
[21] B.K. Chaurasia, S. Verma, and S.M. Bhasker, "Message Broadcast in VANETs Using Group Signature," Proc. IEEE Fourth Int'l Conf. Wireless Comm. Sensor Networks (WCSN '09), pp. 131-136, Dec. 2008.
[22] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs," Proc. IEEE Sixth Ann. Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON '09), pp. 1-9, June 2009.
[23] J.P.H.M. Raya, P. Papadimitratos, "Securing Vehicular Communications," IEEE Wireless Comm., vol. 13, no. 5, pp. 8-15, Oct. 2006.
[24] Y. Choi, J. Oh, J. Jang, and J. Ryou, "Integrated DDoS Attack Defense Infrastructure for Effective Attack Prevention," Proc. IEEE Second Int'l Conf. Information Technology Convergence and Services (ITCS '10), pp. 1-6, Aug. 2010.
[25] A. Menezes, "An Introduction to Pairing-Based Cryptography," Math. Subject Classification, Primary 94A60, 1991.
[26] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. 12th Ann. Network and Distributed Systems Security Symp. (NDSS), 2005.