International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 4, Issue 1, January-February 2015 ISSN 2278-6856

A Survey on Providing Privacy of Navigation In Vehicular Ad Hoc Networks (VANETs)

[1] Ms Rupa Rani , [2]Prof. Sapna Khapre ,[3]Prof. Nishant M. Borkar

[1]Department of computer science engineering, Nagpur University, Maharashtra, India,

[2]Department of computer science engineering, Nagpur University, Maharashtra, India

Abstract

In this paper, we are providing privacy of navigation in vehicular Adhoc network (VANET). This VANET require a mechanism to authenticate message, identify valid vehicles and remove malevolent vehicles. Any query asked by the vehicles from the server or system should be properly authenticated. In this we are using RC6 encryption and decryption algorithm for providing security of the message and Adhoc on demand distance vector (AODV) routing protocol to exchange the message. The advantage of this is that by using real tine road condition to compute the better route and at the same time, prevents from the traffic congestions

Keywords: Navigation, privacy preservation, RC6 encryption, Vehicular Ad Hoc Networks, secure navigation protocol and AODV routing protocol.

1. INTRODUCTION

In a certain destination route finding is a common experience for all among the drivers. Roads have always been dangerous, and a lot of efforts have been undertaken to improve their safety. In old days the hard copy of atlas is used by most of the drivers. But it was very time consuming. After that Global positioning system (GPS) has introduced [1]. Global positioning system (GPS) with navigation has introduced in [2]. Most of the driver has installed GPS on their vehicle for the better driving path. In this, based on local map data base route searching procedure is done but real time road conditions are not mentioned there. After that vehicular Adhoc network becomes very popular among all over the world. It is an important element of the Intelligent Transportation Systems (ITSs) [3]. In VANET, there are various elements. On Board Unit (OBU) is installed in the vehicles, Road Side Unit (RSU) is installed along the road and Trusted authority (TA) and some other informatics server are installed at the back end. The OBU and RSU communicate using the Dedicated Short Range Communications (DSRC) protocol [4]. The main function of VANET is to give a safety message that means turning direction, any accidental information etc. to drivers or any nearby vehicles. VANETs broadcasts the safety messages to vehicle to vehicle(V2V) and vehicle to infrastructure(V2I) or road side unit(V2R).In [5] A new VANET-based smart parking scheme for large parking lots has proposed. In this, to find a vacant parking space in a parking lot, various RSUs provide the navigation scheme to drivers. In [6], real-time traffic information from distributed sensor nodes (vehicle) is performed through the WiMAX interface. Various aspects and research work has given in [7],[8],[9],[10]. Recently, Chim et al [11] proposed a VANET-based secure and privacy-preserving navigation protocol (VSPN). In this, there is a anonymous credentials to provide secure navigation services to drivers. Samara et al. [12], have recently been summarized the Security issues and challenges of VANETs. AMOEBA at [13], was proposed to provide location privacy based on the concept of vehicle group navigation. Different security issues in VANETs has addressed in [14],[15]. Security and privacy-enhancing communications schemes were addressed in [16]. Pseudonym update to sustain privacy has addressed in [17]. For protecting drivers ‘privacy Identity-Based Encryption (IBE) was proposed in [18]. An efficient social-tier-assisted packet forwarding protocol STAP for achieving receiver-location privacy preservation in VANETs was proposed [19]. In this paper, we propose a navigation scheme for privacy preserving system in VANETs. In this, we concentrate on the communication between the vehicle and the infrastructure or two nodes must be more secure. At the same time we are also focus on the routing protocol that we are using is selects better route and prevents from the traffic congestion. The rest of the paper is organized as follow. In section 2, system model and security objectives are given. In section 3, the proposed protocol and algorithms are described for navigation scheme for privacy preserving system in VANETs, and conclude the paper in section 4.

2. SYSTEM MODEL

2.1 Architecture

In this architecture, there are vehicles, RSUs that are installed along the road and trusted authority.

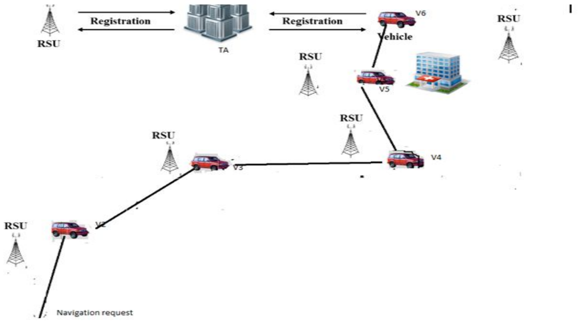

Figure 1: System Architecture

Inside the vehicle, there is a On board unit (OBU) or temper proof device are installed. The Road side units (RSU) are installed along the road and trusted authority (TA) are situated at backside of the road. Each and every RSU have large amount of memory capacity. It stores the real time map information, weather information, accidentals information, traffic information and many more. When the vehicular come in the range and they want navigation then they first have to send real identity to the TA. After that the vehicle will send a authentication request to the RSU through the temper proof device. RSU authenticate the vehicle and send the master key to the vehicle. Then vehicle and RSU starts communication using AODV routing protocol.

2.2 Security Objective

Security objectives are used to provide secure and privacy navigation in VANETs. The main security objectives are as follow:-

1. **Message integrity and authentication:-** Before issue a navigation query the vehicle should be properly authenticated.
2. **Identity privacy preserving:-** The real identity of vehicle should be keep unknown from the other vehicle as well as from the RSUs.
3. **Traceability:-** Although a vehicle's real identity should be unknown from other vehicles and RSUs.
   The TA should have the ability to obtain Vehicle's real identity so that the vehicle can be charged for using the navigation service.
4. **Confidentiality**:- Data packet of query and navigation result should be confidential from the eavesdroppers.
5. **Unlinkability:-** When all RSUs and TA collude, they cannot link up a vehicle's query with its real identity with the RSUs any others.

3. PROPOSED METHOD

In this section, we propose a navigation scheme for privacy preserving system in VANETs. In this we will use the AODV routing protocol for recently search the better route, prevents from the traffic congestion and consume less time to reach the destination. We will also use RC6 algorithm to provide security of navigation in VANETs. We have divided the work in 1.Development of vehicular network. 2. Integration of Navigation module.3.Development of a secure navigation protocol and 4.Development of privacy Preserving Navigation Protocol. In development of vehicular network, network will form between the vehicle, RSUs and TA and all this done by the VANETs. There are various nodes (vehicles and RSUs) and after network formation they may start communication .So, this is the snapshot of two node communication.

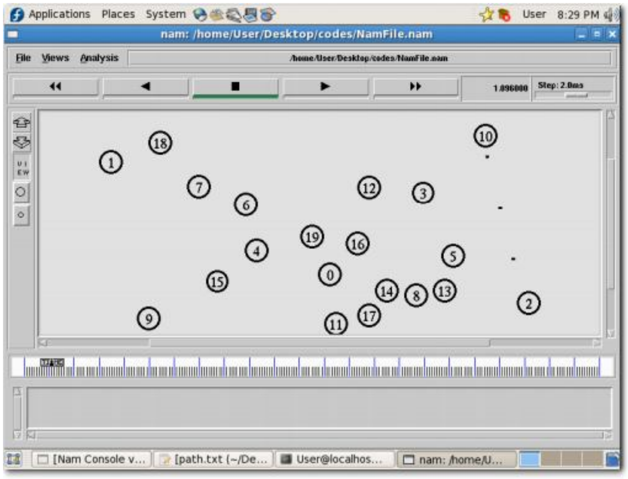

Figure 2: Node communication

In the second part, the nodes will move in up, down, left and right. So we have to find the latitude and magnitude of the nodes. When the nodes come closer or within the range of 10m then the RSUs will send the alert message to the vehicular that you might be collide with each other and you can change the direction. The snap short of this part is as follow.

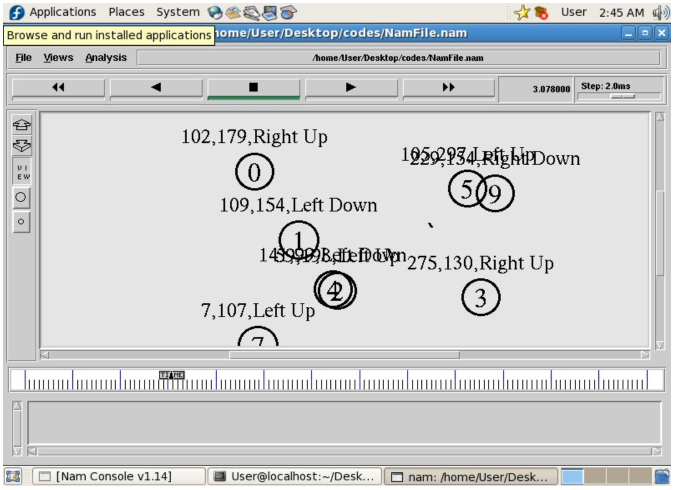

Figure 3: Alert message by RSU to vehicular

4. CONCLUSION

In this paper, we have proposed a new secure and privacy preserving navigation protocol that overcome the problems of [11]. The proposed protocol will select the better route in very less time and prevents from the traffic congestion and will provide more secure and privacy preserving navigation 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] 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.

[4] US Federal Communication Commission, “Dedicated Short Range Communication Report and Order, “December 2003. [Online]. Available: http://fjallfoss.fcc.gov/edocs public/attachmatch/FCC-03-324A1.pdf/

[5] R. Lu, X. Lin, H. Zhu, and X. Shen, “Spark: A new vanet-based smart parking scheme for large parking lots,”in Proc. of the 28th IEEE International Conference on Computer Communications (INFOCOM’09), Rio de Janeiro, Brazil. IEEE, April 2009, pp. 1413–1421.

[6] 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 Information. Networking and Applications (AINA’08), Okinawa, Japan. IEEE, March 2008, pp. 56–63.

[7] 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.

[8] 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.

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

[10] 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.

[11] T. Chim, S. Yiu, L. C. Hui, and V. O. Li, “Vspn: Vanet- based secure and privacy-preserving navigation,” IEEE Transactions on Computers, vol. PP, no. 99, pp. 1–14, August 2012.

[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] 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.

[14] 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.

[15] “Researcher Cracks Trusted Platform Module Security Chip,” http://www.digitaltrends.com/computing/researcher-crackstrusted-platform-module-security-chip/, 2013.

[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] 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.

[20] 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.

[21] 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.

[22] J.P.H.M. Raya, P. Papadimitratos, “Securing Vehicular Communications,” IEEE Wireless Comm., vol. 13, no. 5, pp. 8-15, Oct. 2006.

[23] 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.

[24] A. Menezes, “An Introduction to Pairing-Based Cryptography,” Math. Subject Classification, Primary 94A60, 1991.

[25] 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.