International Journal of Electrical and Electronics Research ISSN 2348-6988 (online)
Vol. 3, Issue 2, pp: (305-309), Month: April - June 2015, Available at: www.researchpublish.com

Secured and Privacy Preserving Navigation for VANET

Varun Patil[1], Premala S. Patil[2]

[1] M. Tech Student, [2]Asst. Professor
[1,2] Electronics and Communication, Guru Nanak Dev Engineering College Bidar, Karnataka, India

Abstract: **In this paper a navigation scheme is proposed which dynamically provides the route information with varying speed limits for various countries; also the source information can be authenticated. The privacy for the drivers who issues the query and the query (destination) are guaranteed to be secured (Unlinkable) to any attacker (Hacker) including the trusted authority. The concepts of anonymous credential can be used to achieve this. This scheme fulfills all other necessary security requirements for secured communication along with authentication and maintaining privacy of the vehicle.**

Keywords: **Secured Communication, Navigation using VANET, Privacy Management, anonymous credential, Data Encryption.**

I. INTRODUCTION

Finding a route to the desired location (Destination) is common practice for the driver (User). In VANET, each vehicle is has an on-board unit (OBU) and there is a road-side unit (RSU) installed along a road side. The trusted authority (TA) and application servers are installed in the back end. OBUs and RSUs communicate using a Dedicated Short Range Communications (DSRC) protocol over the wireless channel while the RSUs, TA, and the application servers communicate using a secure fixed Internet Network. In this paper a secure and privacy-preserving navigation application based on VANET is proposed, which uses the collected data to provide navigation service to drivers. Based on the destination and the current location of the driver (the query), this system automatically search for a route that gives minimum travelling time in a distributed manner. Like other communication networks, security issues have been widely addressed in VANETs. Any navigation scheme must also satisfy the following security requirements.

- A user must be authenticated to ensure he is a valid subscriber as the service is not free. Hence the user must be subscribed to the service for subscription charges to apply on user.
- Messages sent in the system must be authenticated and signed to make sure that they were not modified by anyone.

For a VANET-based navigation system, an additional security and privacy requirement also makes the problem nontrivial. Basic confidentiality is another important factor in this scheme. First, a driver may not want nearby vehicles to know destination by eavesdropping the query issued. Second, when the system sends the navigation result back to user, nonsubscribers nearby should not enjoy free navigation service if it is going to the same destination.

A. Related Work:

A similar scheme is proposed in a recent work [6]. However, there are number of differences between their scheme and proposed system. This paper was based on searching a space for parking a vehicle in a congested area or a large parking lot. The major difference is that their scheme was limited to a small parking area compared to the proposed scheme in this paper. Also the number of RSUs used in parking was less and the authors assumed that the RSU were fully trusted as far as security aspects are concerned. Major security issues were addressed [5] using the RSU aided message called RAISE message for authentication of the vehicles. Using this message when an RSU is detected nearby, the vehicle tries to associate with the RSU, and the RSU assigns a unique symmetric secret key and a pseudo ID that could be shared with other vehicles. There are other security related solution are also proposed such as [7], in this work a VANET key management scheme based on Temporary Anonymous Certified Keys (TACKs) were the certificate contains the public keys of all the RSU present in that geographical area as the city was divided into short coverage area which were monitored by regional authorities making the system efficient in providing the navigation service and security. The only disadvantage was that whenever a vehicle enters into the new regional authority it has to authenticate itself and obtain the certificate for communication.

B. Problem Statement:

In older days, a driver usually used to refer a hard copy of the maps, but the current position of the vehicle cannot be known with the map. With the introduction of Global Positioning System (GPS), GPS-based navigation systems become popular where the current position of the vehicle can be known but the real time road condition was not possible to be known. To learn about real-time road conditions, a driver needs another system known as Traffic Message Channel (TMC), which makes use of FM radio. As this uses FM radio for real time road conditions also this service was available in few countries. With the help of VANET the current position of vehicle, the real time road condition and the navigation can be made available in many countries.

C. Adversary Model:

The attack could happen if the system is not secured from opponent. The opponent can easily trace the identity of the vehicle making the navigation query to obtain easily and change the content of the query also it may linkup the vehicle’s identity with the modified query further colluding between RSU and TA.

D. Security Requirements:

- Message Authentication: The vehicle should be authenticated before sending the query; also the RSU should be able to verify the query without any modification made by attacker.
- Identity preserving: The real vehicle identity must be hidden from RSU, nearby vehicles and the attacker.
- Traceability: The TA must be able to trace the real identity of the vehicle.
- Confidentiality: The content of the query and the navigation result must be kept secret.

II. EXISTING SYSTEM

In existing system proxy re-encryption technique was used where RSUs re-encrypt the most updated master secret key to vehicles and at the same time the RSUs do not know the value of master key. A proxy re-encryption technique is similar to a traditional symmetric or asymmetric encryption technique with the addition of a delegation. The message sender generates a re-encryption key based on their own secret key and the delegated user’s key. A proxy then uses this re-encryption key to translate a cipher text into a special form such that the delegated user can use their private key to decrypt the cipher text to get original message. The authors adopted an asymmetric approach where TA first prepares a re-encryption key for each vehicle then RSUs use this re-encryption key to translate the encrypted master secret key into a form such that the concerned vehicle can decrypt using its private key. In this way, the master secret can be distributed by the RSUs while at the same time and it is kept secret from the RSUs. The geographical distance covered was upto 80 KMs only.

III. PROPOSED SYSTEM

The objective of this paper is to provide a secured navigation system which dynamically shows route information with varying speed as par the transport regulatory of various countries also show to the time required to cover up the distance with average speed under various traffic conditions. Some assumptions are made:

- TA is trusted and is curious.
- TA and OBU on vehicles are assumed to be trusted for the generation and management of anonymous credentials.
- RSUs and TA communicate using a secured Internet.
- For initial vehicle authentication there exists a conventional public key infrastructure.

- RSU broadcasts its public key, same as its real identity with hello messages periodically to vehicles that are traveling within its RSU-Vehicle Communications (RVC) range.
- TA knows the real identity of the vehicle and itself but not by others.
- Each RSU has a local database storing road information in its range (e.g., GPS locations of boundaries, and names of buildings and streets) and how to get to its neighboring RSUs (e.g., distance and direction).
- The vehicle's has a tamper-proof device performs all cryptographic-related functions such as storage of keys, generation of pseudo identities, signing messages, and encryption of messages.
- Finally, it is assumed to have its own clock for generating correct time stamps and be able to run on its own battery. Note that a vehicle can also have a conventional computer device for performing the verification of RSUs' hop information.
- TA, RSUs, and vehicle tamper-proof devices have roughly synchronized clocks. This can be done easily by requiring TA to periodically broadcast the current time to all vehicle tamper-proof devices via RSUs.

A. Basic steps in proposed system:

The steps of this system are adopted from [4] which show how the authentication and forwarding of the navigation query to the neighbouring RSU is done.

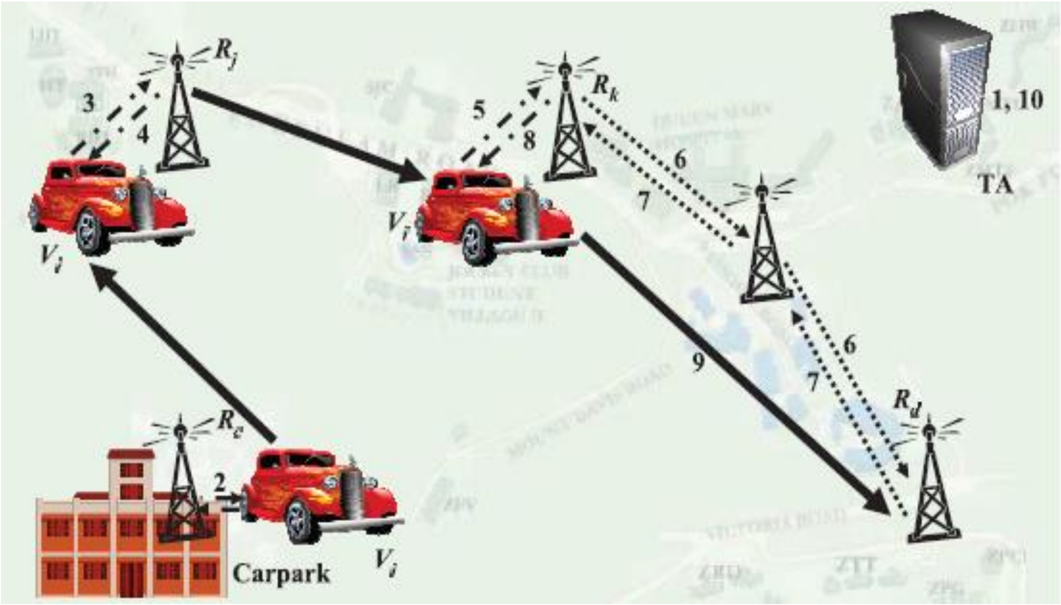

Fig. 1 Basic Steps

1. TA sets up parameters and generates anonymous credentials.
2. Vehicle V_i's tamper-proof device starts up and requests for the key from RSU R_c.
3. Vehicle V_i's tamper-proof device requests for a navigation credential from RSU R_j.
4. RSU R_j verifies V_i's identity and sends its tamperproof device an anonymous credential.
5. After a random delay or after travelling for a random distance, V_i's tamper-proof device sends out its navigation request to RSU R_k.
6. RSU R_k forwards the navigation request to its neighbours.
7. RSU R_d constructs the navigation reply message and sends it along the reverse path.
8. RSU R_k forwards the navigation reply message to V_i's tamper-proof device which then verifies the messages from all RSUs along the route in a batch.

9. By presenting the navigation session number, each RSU along the route guides V_i to reach the next RSU closer to the destination.

10. Based on V_i's pseudo identity received from RSU R_j, TA reveals V_i's real identity for billing purpose.

B. Simulation Model:

In this set of experiment the geographical distance of 50 km with the speed limit of 100 km/h, in general scenario the number of RSU required is are more. For example [11] the authors considered around 8500 units for 14498 roads. The basic concept in VANET relay on the placement of RSU. For this simulation RSU are placed at 500 mtrs apart. More units can be placed along the road side to improve the coverage area depending upon the traffic congestion and the width of the road. TA server is placed and RSUs communicate with each other and with TA via a fixed infrastructure at a bandwidth of 6 and 10 Mb/s, respectively. Regarding processing time, following the experiment on an Intel Core i3 processor at 2.24-GHz computer, assuming each pairing operation taking 4.5 ms and each point multiplication over an elliptic curve takes 0.6 ms. Each conventional asymmetric encryption takes 1.2 ms, while each conventional symmetric encryption takes only 0.6 ms. RSU needs to look up its routing table for forwarding direction. As the experiment starts at about 10 percent of all roads are blocked considering sources and destinations that have roads connected and these roads are not blocked at this time. The vehicle sends out its navigation query once it enters an RSU's range. Since a vehicle can wait for a random delay or travel for a random distance after obtaining a navigation credential before sending out its navigation query.

C. Simulation Results:

As the simulation covers a distance of 50km with speed limit of 100km/h the time taken to cover distance of 20km by the proposed system is 25 minutes as the existing system takes 30 minutes as shown in fig below.

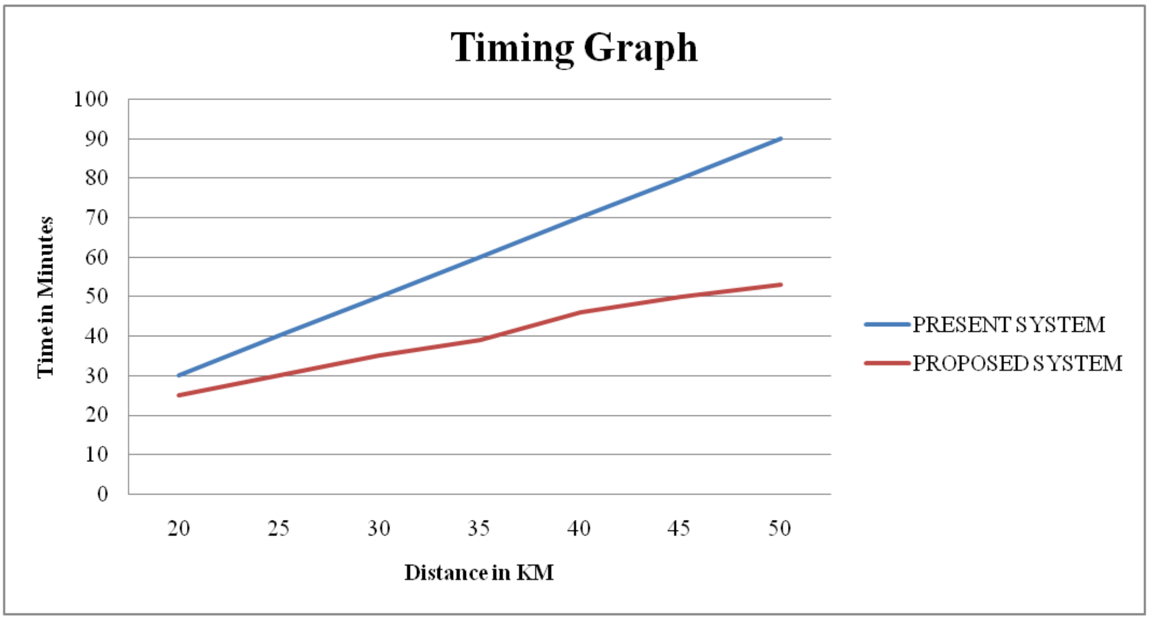

Fig. 2. Time vs. Distance Graph

Comparing the time further, it increases as the distance increases. For all geographical distance ranges, the traveling route returned by proposed scheme gives lower delay than the offline map database checking approach. These similar results can be obtained for various speed limits as pas the regional transport authority of different countries.

IV. CONCLUSION

Using the concepts of VANET in navigation system and utilizing the speed and condition of roads obtained from RSUs to guide the drivers to the desired location in secured and distributed manner. The proposed scheme adopts some security primitives to provide a number of security features i.e. vehicles are properly authenticated with pseudo identities, navigation queries and results are protected from eavesdropping. Besides satisfying all security and privacy requirements the proposed solution is efficient such that the whole navigation querying process completes in very short time. On the other hand the route returned by this system can save upto 55% of travelling time compared to offline map data searching approach.

REFERENCES

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

[2] 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.

[3] M. Green and G. Ateniese, “Identity-Based Proxy Re-encryption,” Proc. Applied Cryptography and Network Security Conf., 2007.

[4] M. Scott, “Efficient Implementation of Cryptographic Pairings,” http://ecrypt-ss07.rhul.ac.uk/Slides/Thursday/ mscottsamos07. pdf, 2007.

[5] Zhang, R. Lu, X. Lin, P.H. Ho, and X. Shen, “An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks,” Proc. IEEE INFOCOM ’08, pp. 816-824, Apr. 2008.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] T.W. Chim, S.M. Yiu, Lucas C.K. Hui and Victor O.K. Li, “VSPN: VANET-Based Secure and Privacy-Preserving Navigation”, IEEE TRANSACTIONS ON COMPUTERS, VOL. 63, NO. 2, FEBRUARY 2014.