International Journal on Emerging Technologies (Special Issue on NCRIET-2015) **6**(2): 129-132(2015)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

Secure and Authenticated Navigation System Based on VANET

Udaykumar N Kalyane
Department of Electronics and Communication,
BKIT Bhalki, Karnataka, INDIA

(Corresponding author: Udaykumar N Kalyane)

(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Recent advances in communication sector are enabling implementation of different types of network in various environments. VANET is a subset of MANET.VANET and MANET both are wireless networks which are self configured and autonomous ad-hoc network. The main goal is to generate a navigation scheme that uses the online or real time road information collected by a VANET to guide the drivers to desired destination .In order to integrate vehicular technology into conventional GPS based navigation systems securely, a secure and privacy preserving navigation is required. Addition to authentication and privacy preserving this VSPN scheme fulfills all necessary security requirements. In this scheme the concept of proxy re-encryption scheme and anonymous credentials are used.

Index terms-MANET, VANET, ITS anonymous credentials, proxy re-encryption, GPS,DSRC.

I. INTRODUCTION

Wireless sensors network (WSN) is the collection of homogenous, self organized nodes known as sensor nodes. Ad-hoc networks are also a kind of WSN. Ad-hoc network is a local area network that is built spontaneously as devices connect. Basically ad-hoc network is a temporary network connection created for a specific purpose. VANET is a subset of MANET. Number of vehicles are increasing day by day on roads so peoples are facing a so many problems such as traffic congestion, finding a route to a certain destination, safety applications includes alerting the driver about road conditions, turning directions, traffic light. In GPS[1] system a small hardware device is installed on a vehicle by receiving GPS signals the device can determine its current location and then find a shortest route to a certain destination. Comfort application includes the online information about, petrol stations, map while entering a new city, smart parking [7] lot. It includes toll payment by recharging the OBU installed in every car, while passing the car through toll tax station, the amount of tax can be automatically deducted due to VANET. The fig 1 shows the overview about VANET. In vehicular communication there are mainly two types of communication that is vehicle to vehicle (V to V) and vehicle to infrastructure (V to I).

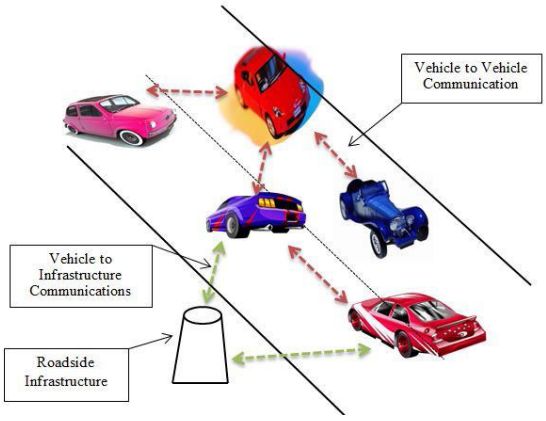

Fig 1. VANET.

In VANET technology the vehicle is mainly equipped with 3 different devices those are OBU(On Board Unit),TPD(Tamper Proof Device),sensors. The RSU (Road Side Unit) is installed along the roads. Communication takes place between OBU and RSU, the information sharing between the cars takes place in multi-hop pattern. Between OBU and RSU dedicated short range communication (DSRC) takes place. DSRC is having IEEE 802.11p standard. The communication range is 1000meter. OBU is a device inside the vehicle .It processes the data collected from various sensors fitted inside the car and give conditions of vehicle.

It is responsible for communicating with outside network that is with other vehicles and infrastructure. Sensors are used for sensing purpose and to measure their own status of the car (fuel consumption of the car). TPD is a safety device installed inside the vehicle. It contains all the vehicles safety information, a battery and watch for synchronization. It involves into all safety operation and it is only reasonable for the authorized person.

II. LITERATURE SURVEY

The idea of real time transportation is not completely new. A similar work is presented in ref [2] but number of differences between there scheme and ours. Their scheme is small scale while ours is large. Our scheme is more authenticated from them. In ref [3] STAP: A Social-Tier-Assisted Packet Forwarding Protocol for Achieving Receiver-Location Privacy Preservation in VANET is explained. In ref [2] an efficient self generated pseudonym mechanism based on Identity-Based Encryption (IBE) was proposed for protecting drivers Privacy [4].

Routing is a process of sending data packets from source node to destination node. Hence routing in a vehicular ad-hoc network is critical issue. The routing protocol should be such that works based on the real-time road vehicle density in order to provide fast and reliable communications so that it adapts to the dynamic vehicular city environment. The routing Protocols are mainly classified into 2 types.

III. ROUTING PROTOCOLS IN VANETS

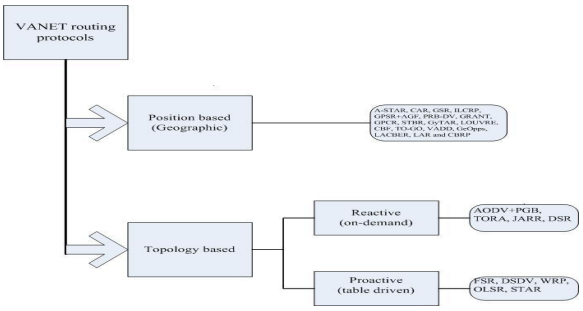

Fig. 2. Routing protocols.

Fig. 2 shows the routing protocols. Based on routing information, routing protocols are broadly classified as topology-based and position-based routing protocols. In topology-based routing mechanism, we deal with the network layout/architecture of the nodes such that packet forwarding is possible using the information that is available about the nodes and links within the network.

1. Topology-based Routing Protocols

This type of routing considers the selection of route for sending the information between sender and receiver. It can be further divided into proactive and reactive routing.

a. Proactive Routing Protocol

Proactive routing protocols also known as table-driven protocols. It maintains current list of destinations and their routes by periodically sharing the routing tables.

b. Reactive Routing protocols

It maintains only the routes that are currently in use, thereby reducing the bandwidth consumption problem as in case of proactive routing.

2. Position based Routing protocols

Determination of routing in all nodes is based on the destination's location included in their packets and the location of the neighbors of forwarding nodes. Examples of position based protocols include,

A-STAR (Anchor-based Street and Traffic Aware Routing) was a protocol for a urban IVC condition. This protocol is based on buses route for recognizing anchor based routing to sending or receiving packets.

CAR (Connectivity-Aware Routing) main property of CAR is its capability to maintain a cache of achieved routes between sources and destinations.

GSR (Geographic Source Routing) proposed for VANET in city environment. It joins position-based routing protocol with topological information by calculating the junctions arrangement that must be passed over by packets to reach their destination;

IV. OUR SOLUTIONS-VSPN

This section presents our VANET based secure and privacy preserving navigation (VANET) scheme. We summarize our scheme into some basic steps as shown in below fig 3.

Fig. 3. Basic steps in VSPN.

1. Trusted authority (TA) sets up parameters and generates anonymous (unknown) credentials.
2. Vehicle Vi's Tamper Proof Device (TPD) starts up and request for the master secret s from RSU Rc.
3. Vehicle Vi's TPD requests for a navigation cre4. RSU Rj verifies Vi's identity and sends its TPD an anonymous credential.
5. After traveling for a random distance, Vi's TPD sends out its navigation request to RSU Rk.
6. RSU Rk transfers the navigation request to its neighbors. This process repeats till the request reaches RSU Rd covering the destination.
7. RSU Rd constructs the navigation reply message and sends it along the reverse path. Multi-hop communication takes place.
8. RSU Rk transfers rhe navigation reply message to Vi's TPD which then verifies the message from all RSUs along the route in a batch.
9. Each RSU along the route guides Vi to reach the next RSU closer to the destination.
10. Based on Vi's pseudo identity received from RSU Rj, TA reveal Vi's real identity for billing purpose. dential from RSU Rj.

V. APPLICATIONS

1. Traffic Signal: communication from the traffic light can be created with the help of VANET technology.
2. Weather conditions: for the convenience of the vehicle VANET is used to avoid traffic jam and to avoid accident by knowing all weather conditions.
3. Vision enhancement: Drivers are given a clear view of vehicles and obstacles in heavy fog conditions and can learn about the existence of vehicles hidden by the obstacles, buildings and by other vehicles
4. Driver assistance: It is mainly helpful to the drivers in driving and privacy of the driver can be preserved
5. Automatic parking: vehicles can park itself without the need for driver intervention [9].
6. Safety: safety applications include collision warning, information sharing, comfort driving, other value added services like transpotation, internet access etc.
7. Searching roadside locations and vehicles direction: For unknown passengers helps to find the gas stations, hotels, shopping centre etc [10].
8. Entertainment: It helps to passengers to play a game, use other internet applications within the vehicle.

Authentication[6]

Proxy re-encryption scheme: A proxy re-encryption scheme [5] is similar to a traditional symmetric or asymmetric encryption scheme with the addition of a delegation function.

Proxy re-encryption schemes are same as cryptosystems which allow third parties to alter a ciphertext which has been encrypted for one party, so that it may be decrypted by another .

The message sender can generate a re-encryption key based on his/her own secret key and the delegated user's key. A proxy can then use this re-encryption key to translate a ciphertext into a special form such that the delegated user can use his/her private key to decrypt the cipherte.

VI. SIMULATION RESULTS

We are using the MATLAB software for simulation.fig 5 shows the processing time V/S distance. Performance of VSPN scheme is measured in terms of processing time and route blocking rate. In this graph proposed method consuming less processing time as compared to existing system because VSPN scheme is online map data searching process.fig 6 shows the route blocking rate V/S distance. Our existing method has much higher blocking rate than our VSPN scheme.

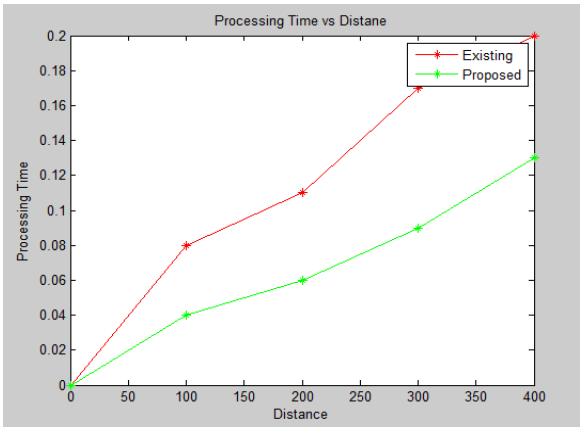

Fig. 5. Processing time v/s distance.

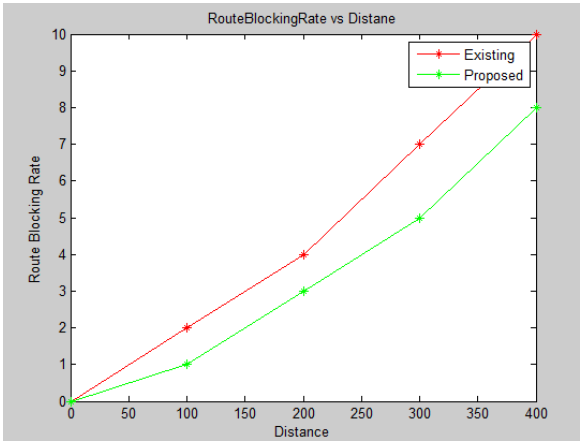

Fig. 6. Route Blocking Rate v/s distance.

VII. CONCLUSION

In this paper, we prepare transportation scheme that uses the online road information in real time by the help of VANET. In addition to information sharing, co-operative driving, finding a shortest route to a certain destination. it provides authentication, privacy and security to the data. VSPN scheme are achieved by using anonymous credential and proxy re-encryption. In these scheme vehicles are authenticated by using pseudo identity. Navigation results and privacy of drivers are protected from malicious users or hackers. It saves the travelling time upto 55 percent compared with the offline map data searching approach. In very short time the whole process will completes. car manufactures like BMW, Mercedes, Fiat, Ford, Toyota, and Nissan, are currently prototyping vehicles equipped with Wi-Fi (802.11a/b/g) and DSRC technologies, which are expected to be on the road within the next 3–5 years. Finally, privacy of the drivers and security of the information are protected by using the sensor infrastructure and encryption/decryption approach

REFERENCES

[1] Sherisha Pullola, Pradeep K. Atrey and Abdulmotaleb El Saddik," Towards An Intelligent GPS- Based Vehicle Navigation System For Finding Street Parking Lots", *2007 IEEE International Conference on Signal Processing and Communications (ICSPC 2007),* 24-27 November 2007, Dubai, United Arab Emirates.

[2] 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.

[3] 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.

[4]. Raya, M. and Hubaux, J., "The Security of Vehicular Ad Hoc Networks", in proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2005), Aleandria , V A, pp1-11.

[5]. H. Song, S. Zhu, and G. Cao, "SVATS: A sensor-network-based Vehicle Anti-Theft System," in Proc. IEEE INFOCOM'08, Phoenix, AZ, USA, April 14-18, 2008.

[6]. C.T. Li, M.S. Hwang, and Y.-P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy perserving for vehicular ad hoc networks," *Comput. Commun.*, vol. **31**, no. 12, pp. 2803–2814, 2008.

[7]. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Advanced proxy re-encryption schemes with applications to secure distributed storage," *ACM Transactions on Information and System Security*, vol. **9**, no. 1, pp. 1–30, February 2006.

[8] M. Jerbi, S.-M. Senouci, T. Rasheed, Y. Ghamri-Doudane, "Towards Efficient Geographic Routing in Urban Vehicular Networks," Vehicular Technology, *IEEE Transactions on Vehicular Technology,* vol. **58**, no. 9, pp. 5048-5059, 2009.

[9]. Rongxing Lu, Xiaodong Lin, Haojin Zhu, and Xuemin (Sherman) Shen, "A New VANET-based Smart Parking Scheme for Large Parking Lots", IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2009 proceedings, 978-1-4244-3513-5/09, 009.

[10] Q.Shengbo, D.Keliang, and L.Qingli, An effective gps/dr device and algorithm used in vehicle positioning system. In IEEE ITS Conference, oct. 2003.