VANET BASED SECURE AND EFFICIENT TRANSPORTATION SYSTEM

Pooja R K[1], Uday Kumar.N. Kalyane[2]

[1]*Department of Electronics and Communication Engineering, BKIT Bhalki, India*
[2]*Department of Electronics and Communication Engineering, BKIT Bhalki, India*

Abstract

This paper presents a recent advance of vehicular technology (VANET) offers many opportunities for developing new navigation systems to avoid the problem of GPS (Global positioning system) based navigation systems. The proposed system is uses VSPN scheme for to know the real time road information. This scheme advice the drivers to reach to the destination. In order to integrate vehicular technology into conventional GPS based navigation systems securely, a secure and privacy preserving navigation is required. This VSPN scheme provides security and authentication to the system and it also helps in preserving privacy of the system. In this proposed system the concept of proxy re-encryption scheme and anonymous credentials are used.

Keywords-*Vehicular ad-hoc network, proxy re-encryption, anonymous credentials, GPS*

----------***----------

1. INTRODUCTION

Vehicles have become an important part of human daily life. In ancient days drivers using the hardcopy of the atlas to get the information about the road to reach to a particular destination but it has some disadvantages. After some days a GPS (Global Positioning System) based navigation system came into existence [1]. GPS is a system which provides information of time and location on the earth.

In the navigation system the vehicle is equipped or having some hardware device and this device is capable of receiving GPS signals then it determines the present location then find shortest path to destination. Depending on the local map data base the searching procedure to a certain route is applied but the local map database is not consider in real time. Later they used the concept of traffic message channel to know the real time information. Vehicular ad-hoc network presents a challenging class of MANET (mobile ad-hoc network). Ad-hoc network establishes whenever two devices connect to each other. It is nothing but a LAN (Local Area Network). Ad-hoc network is a temporary network connection established for particular purpose (application). MANET can change locations and continuously configure itself. VANETs are recognized as one of the most prominent technologies for improving the efficiency and safety of modern transportation system.

With the help of VANET vehicles can communicate with other vehicles and road side infrastructure. In this communication nodes are mainly vehicles. Vehicular ad-hoc Networks collects the information of traffic and with low cost and high accuracy it is able to sense the physical quantities on the path. The main objective of VANET is to provide safety to vehicles such as collision alert, road surrounding warnings, vehicle speed etc. Now a day's VANET technology is used in many countries. VANET is an important part in ITS.

The vehicular communication system is made over this robust and strong IT system. It helps vehicle's driver for co-operative driving, information sharing and other value added services which makes the driving more efficient and convenient and safe on roads. The communication between vehicles is ad-hoc in nature where communications are done between various infrastructure and cars.

Today's vehicles are become a smart car with assistance from wireless communication technology. Smart cars are fully controlled software devices. In a typical VANET **vehicles** are equipped with 3 different devices namely On Board Unit (OBU), Sensors, Tamper proof device (TPD).

On board unit is a one device which is fitted inside the car. This OBU is capable of communicating with other vehicles and road side 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 put in the vehicle. It includes much information of the vehicles such as battery life, watch synchronization. It gets on only by the original owner. Road side units deployed beside the roads. Road side unit and on board unit are continuously communicating with each other using dedicated short range communication protocol.

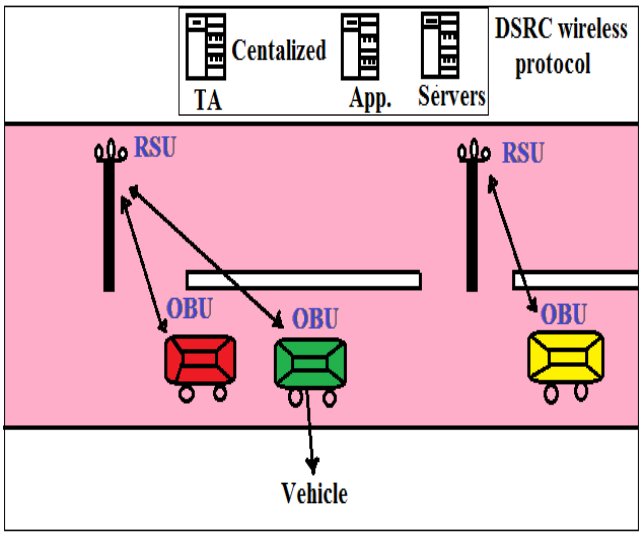

Fig 1: Overview of VANET

The overview of VANET is shown in the fig 1. Here the RSU and OBU communicate using DSRC protocol which uses 5.85 to 5.92GHZ.Its approximate range is 1000 meter.

1.1 Basic Components of VANET

Fig 2 shows the basic components used in the VSPN scheme. Those are road side unit (RSU), on board unit (OBU), Tamper proof device (TPD) and sensors. During the registration of each vehicle trusted authority (TA) assigns a real identity and tamper proof device activation password also provide a license plate number to all vehicles. When vehicle starts the driver enters the real identity and password into tamperproof device to activate it. If the identity and password are incorrect the tamperproof device refuses to perform further operation.

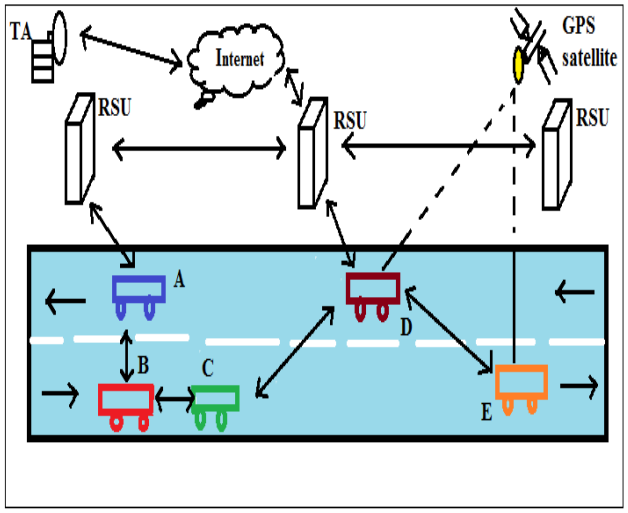

Fig 2: Basic components of VANET

1. The communication between vehicles and other communicating devices uses 802.11p wireless standard for supporting Dedicated Short Range Communication (DSRC) protocols.
2. Vehicles A, B, C, D and E in fig 2 communicate with each other using DSRC protocol. But vehicle C cannot communicate directly with vehicle E as the range of the DSRC 802.11p is limited to approx.1000m.Vehicle c can receive the messages from E through the D. Here multi hop communication takes place
3. OBU is responsible for communicating with other vehicles and infrastructure. Communication between vehicle-vehicle and vehicle-infrastructure are taking place in ad-hoc manner.
4. RSU is a infrastructure component that communicates with the vehicles and other roadside stations for sharing and collecting data from various vehicles. Additionally, it helps in sharing and receiving various information between vehicles and process data information.

1.2 Problem Statement

Every vehicle has a Tamper proof devices and each device will be navigated to Road Side Units (RSU) since there will be multiple RSU and which are interlinked to each other. Hence if 1 RSU compromises the whole network gets attacked since general encryption algorithms are not completely available for providing good security module.

1.3 Adversary (Attacker) Module

1. The malicious users can trace or achieve the real identity of a vehicle and there is no privacy of driver maintains and can trace a vehicle's real identity by knowing multiple messages sent by it.
2. Trough the eavesdropping the malicious user can obtain the information of any navigation query and navigation result.
3. By colluding road side unit and trusted authority malicious users can link up a vehicle's query with its real identity.

1.4 Objective of VANET

- Improve safety transportation and co-operative driving.
- Minimize traffic problems such as crashing of vehicles and accidents.
- Information about traffic regularly
- Collision aware
- Local danger alert
- Information about weather

1.5 Security Requirements

1. Message integrity: The messages which are transferring from source node to destination nodes are not safe they can be altered or changed by the malicious users and inject the false information. [2].
2. Authentication: Without authentication [3] hackers are try to spoil our message by including false information into it and create confusion to others
3. Identity privacy preserving: To protect from the malicious users it is necessary to preserve the privacy.

4. Traceability: The trusted authority is only responsible for tracing the real identity of a vehicle. Trusted authority is only the one who knows about the vehicles details and about its owner.
5. Confidentiality: Always the navigation results an query's are kept confidential.

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

Proxy re-encryption schemes are similar to cryptosystems. Proxy re en-encryption schemes are mainly used to provide more authentication to the system. Simple encryption method is not sufficient.

The users can able to generate or develop a proxy re-encryption scheme depending on their requirement. A proxy can then use this re-encryption key to change a ciphertext into a special form such that the user can use his/her private key to decrypt the ciphertext.

2. OUR SOLUTIONS-VSPN

VSPN is a VANET based secure and privacy preserving navigation (VANET) scheme. Basic steps of VSPN scheme is shown in figure 3.

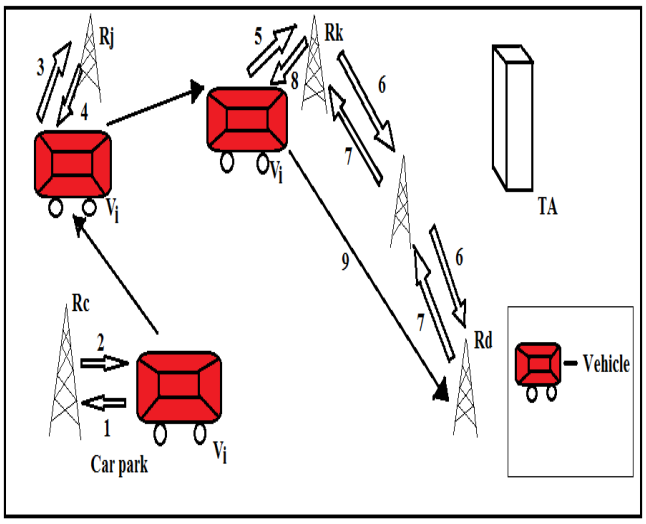

Fig 3: Basic steps in VSPN

1. Parameters and anonymous (unknown) credentials are generated by the trusted authority (TA).
2. There is one Tamper proof device installed in a vehicle Vi which requests the master secret from the RSU Rc.
3. TPD in the vehicle Vi requests RSU Rj to provide navigation credential.
4. Vi's identity is verified by road side unit and Sends an anonymous credential to the TPD of vehicle Vi.
5. After traveling for a random distance, RSU Rk receives the navigation request from TPD of vehicle Vi.
6. RSU Rk transfers the navigation request to its neighbors. This process repeats till the request reaches RSU Rd.
7. RSU Rd sends the reply message and sends it along the reverse path. Here Multi-hop communication takes place.
8. RSU Rk transfers the navigation reply message to TPD of vehicle which then verifies the message from all RSUs along the route in a batch.
9. Each RSU along the route guides Vehicle to reach the next RSU closer to the destination.

3. NETWORK ARCHITECTURE

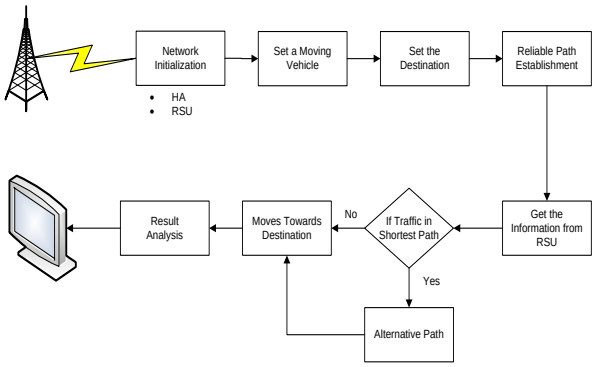

Fig 4: Architecture

Network is initiated by deploying the number of nodes randomly on a geographical area. Here we deployed 20 nodes in a 100X100 m^2 area. Then set a moving vehicle and its destination. Then find the reliable path depending upon number of hopes, energy and distance. The RSU provides the information about the shortest path of our destination. If there is a traffic in a shortest path [6] then moves through the alternative path towards the destination then the result will be analyzed.

4. APPLICATIONS

1. Traffic Signal: Traffic light can be operated with the help of VANET technology..
2. Weather conditions: VANET is used to avoid traffic jam and to avoid accident by knowing all weather conditions.
3. Vision enhancement: VANETs are used to have clear vision in heavy fog conditions and to know about the presence of vehicles hidden by buildings or obstacles
4. Driver assistance: It is mainly helpful to the drivers in driving and privacy of the driver can be preserved
5. Automatic parking: Without the need for driver intervention the car can park itself. [7].
6. Safety: safety applications include collision warning, information sharing, easy driving, accessing of internet.
7. To know the locations of roads and vehicles: For newcomers helps to find the locations like gas stations, hotels, shopping centre etc [8].
8. Entertainment: It helps to passengers to play a game, use other internet applications within the vehicle.

Advantages

- Provides security
- Traffic control
- Traffic congestion avoidance

- information support to passengers
- Comfort
- Information source can be properly authenticated (protected).

5. SIMULATION RESULTS

We are using the MATLAB software for simulation.fig 1 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 2 shows the route blocking rate V/S distance. The proposed scheme has less route blocking rate as compared to existing systems.

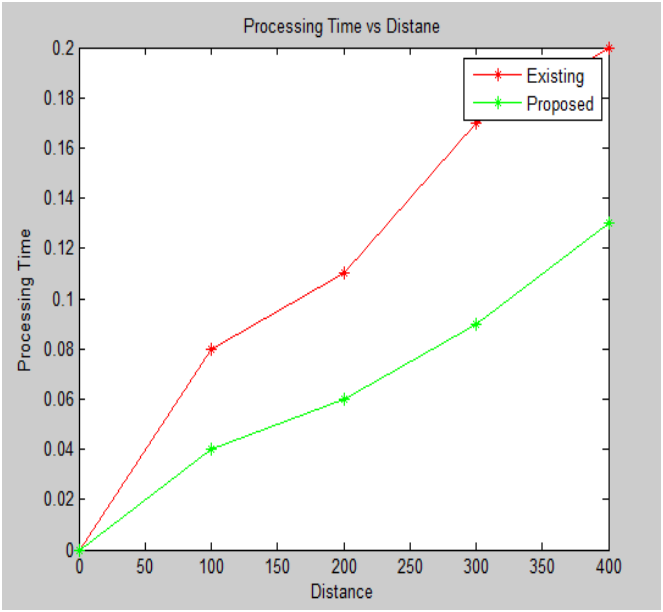

Fig 5: Processing time verses distance

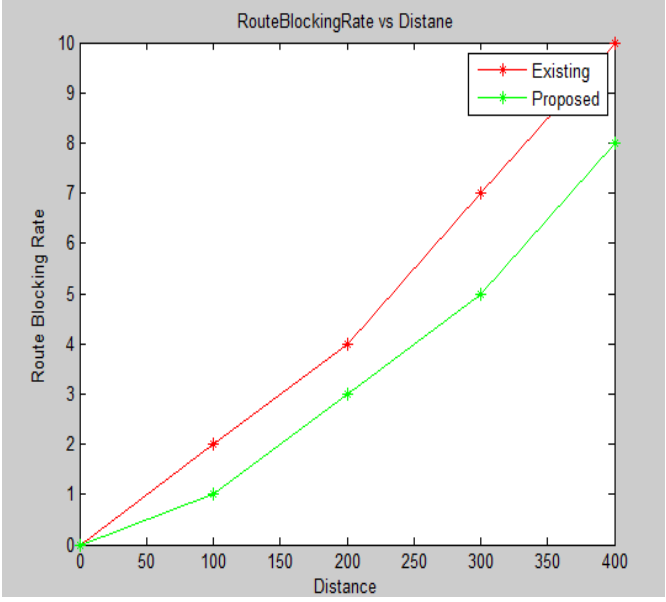

Fig 6: Route Blocking Rate verses distance

6. 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.

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]. 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.

[3]. 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.

[4]. 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.

[5]. 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.

[6]. 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.

[7]. 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.

[8]. 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.