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

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

1Department of computer science engineering, Nagpur University, Maharashtra, India,
2Department 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 time 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.
Inside the vehicle, there is an 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.

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**


