International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Secure and Privacy Preserving Navigation in VANET

Sudarshana A. Abbad[1], S. P. Godse[2]

Computer Engineering Department, Sinhgad Academy of Engineering, Pune, Maharashtra, India

Abstract: ***In today's communication world technologies reformed human's lifestyles by providing the best effective and beneficial personal and public communication applications with the help of internet services. Recently, in vehicle manufacturers and telecommunication industries gear up to equip each vehicles and cars with the facility that allows the vehicle to vehicle communication with each other as well as with the RSU, which is located near the road, such as at every traffic signal or any important location which exist on fixed distance, in order to good driving experience, facilitate secure driving, and enhance people safety and security. In this research paper, we propose a navigation method that utilizes the road information collected by a vehicular ad hoc network (VANET) which helps to guide the drivers to reach desired destinations in a real-time. The proposed scheme provides the advantage of get real-time road conditions to analyse a better route and simultaneously, the providing information source can be properly authenticated. To protect the real identity of the drivers, the submitted query (destination) and the driver or user who submit the query are must guaranteed to be not linkable to any party including the trusted authority(CA). We make use of the idea of anonymous credential (dummy and not original) to achieve this goal. In addition to message authentication and privacy preserving, our scheme also provide other necessary security requirements. Using the real maps scenario of New York and California, we performed a simulation study on our proposed scheme showing that it is effective and efficient in terms of processing delay and providing proper routes of shorter traveling time.***

Keywords: Privacy preservation; Vehicle ad hoc network; Certificate authority; Navigation; anonymous certificate

1. Introduction

Today, vehicular ad hoc network (VANET) is popular in many countries. It is new and important element of the Intelligent Transportation System (ITS). A vehicular ad hoc network (VANET) can easily achieve driving safety through vehicle-vehicle communications or communications with road-side units. Basically, Vehicular ad hoc networks (VANETs), is a subpart of Mobile Ad hoc networks (MANETs), in that vehicles can communicate among one another or with Road Side unit (RSU) based on wireless Local Area Network (LAN). The primary issue in VANET is to allow vehicles to send important and traffic related messages that contain essential information for ex vehicle speed, turning directions of vehicle, road accident information etc. to other and nearby all vehicles. It is called as vehicle to vehicle or V2V communications.

Every time while travelling driver find a route of a destination in an unknown or known region or to predict the fastest route in a particular area. Recently, global positioning system (GPS) technology providing facility of navigation and many vehicles have started to install GPS system for navigation and to select better and time saving driving paths in terms of the physically shortest and low traffic [1]. However, effective route finding process of these systems is based on local map information. If the local map information is outdated, or if another event (e.g., road accident or disaster) occurs, the GPS navigation system may give erroneous route for destination. We provide efficient path by using shortest path algorithm which analyses accident path and direct user to efficient path. In the meantime, vehicular technology has improved massively in the last decade, especially in driving safety and privacy preserving of vehicle. Hence, today's vehicle becomes a smart vehicle with inclusion of wire- less communication technology. In VANET systems, vehicles are equipped with on board units (OBUs) to save driver related information and communicate with road side units (RSUs) installed along the roads. The vehicles and road side units can communicate by the dedicated short range communications (DSRC) [2].

The proposed method i.e. VANET- based secure and privacy-preserving navigation (VSPN), which use the collected data to provide navigation directions to drivers. According to the destination and the current location of the drivers vehicle (the query), the system can automatically find a route that minimize traveling delay using the online collected information of the road condition and traffic incidents. In addition with driving path information, the navigation results can also be used for many other important purposes. For ex, a recent research work [6] proposed to use information of returned routes for routing information such as images and videos about desired scenes to on route vehicles.

On the basis of vehicle's OBU will continuously make communication with RSUs, the driving method of a driver as well as the efficient traveling routes can be easily analyzed. The privacy protection issue is another important and basic. Requirement in VANET. One mostly used approach to resolve this problem is to use a different and unrelated pseudo identity to communicate with a different RSU on road which authenticate user. Thus, collecting all information and messages between communication of vehicle and all RSUs cannot generate messages together to reconstruct the driving routes followed by driver or analyze the different driving habit of a driver. However there are also other attacks for example, if a any node in network performing a denial-of-service attack to the system by sending no of messages to an RSU at one time, the system admin should be able to find that user and to block and deny its further access to the system. Therefore, though pseudonymous certificate is used, a trusted party (e.g., TA)

must be able to obtain a user's real identity if it required for further investigation. Therefore, the real identity of a vehicle kept anonymous from all other vehicles in network and RSUs But the authorized trusted party (TA) can retrieve the real identity of the vehicle if needed by using its pseudo identity.

We provide privacy to each vehicle by using bi-linear algorithm and message encryption done by RSA algorithm. We sent these messages by setting priority to each message header so it reaches to high priority user firstly.

In our proposed system, the trusted authority can easily reveal the real identity of a vehicle. If the navigation system is not strongly protected, it can possible that the real identity of a driver and the query submitted by him can be linked up and it help in analyze the route of vehicle. Here we want that TA can reveal the real identity by using a pseudo identity, but we want that TA should not know where driver wants to go.

Also driver not want vehicles nearby to him know his destination by eavesdropping his query submitted. Second, when the navigation system sends the navigation information back to driver, nonsubscribers nearby to him not enjoy free navigation service in case if it is charged to real user.

Moreover, navigation information (for ex. locations and road conditions)is got from more than one RSU's and most of the RSUs are left unattended hence proper authentication of information is critical. Hence the authentication must be efficient, otherwise, querying duration become long which is unacceptable. Our scheme can save up to 55 percent traveling time when compared with other offline route searching method.

2. Related Work

The idea of real-time navigation using VANET is not totally new. A similar scheme is proposed in a recent work [8]. However, there are a number of differences between their scheme and ours. First, their scheme is of a small scale that covers a car park, while ours is large scale to cover the whole city and beyond. Second, in their scheme a car park is monitored by three RSUs that take up the roles of determining a vehicle's location, searching for a vacant parking space, and providing navigation service to guide the vehicle to go from the car park entrance to the selected parking space. In our scheme, the road system in the city is monitored by a large number of RSUs that take up the navigation task in a distributed manner. Third, in terms of security functions, their scheme assumes RSUs to be fully trusted. This makes sense because the three RSUs are installed indoors and can be monitored by security guards. However, such an assumption is no longer valid in our outdoor setting. It is impossible to have security guards monitor all RSUs across the city. Thus, unlike their scheme, authentication of RSUs becomes a vital component in ours. Fourth, our scheme allows one's identity and navigation query to be delinked. This feature is only interesting for wide area navigation like ours. Thus, the scheme provided in [8] cannot be used to solve the navigation problem discussed in this paper. Besides, an application of real-time navigation is proposed in another recent work [6]. In addition to driving guidance, the returned routes are used for opportunistically routing multimedia information such as images and videos of a desired scene to vehicles. Our scheme is based on the idea of indistinguishable (anonymous) credential. Such a credential system was introduced by Chaum [9]. The system allows a user to obtain a credential from one organization and later show the possession of the credential to another organization, while the transactions at the two organizations are not linkable.

The idea of anonymous credential has been adopted in different applications. For example, [10] proposes a credential-based privacy-preserving e-learning system under which a student can show his/her progress in e-learning without leaking his/her identity information. In fact, VANET security is a hot research topic. Security issues and challenges of VANETs have recently been summarized by Samara et al. [11]. As early as 2007, a scheme called AMOEBA [12] was proposed to provide location privacy based on the concept of vehicle group navigation. In 2008, a number of works including [7], [13], and [14] were published to address different security issues in VANETs. In [7], a batch verification scheme known as IBV was proposed for an RSU to verify a large number of signatures at the same time using only three pairing operations. The scheme relies on a tamper-proof device to store an unchangeable master secret key. However, it can be expected that such a tamper-proof device will be compromised eventually (e.g., Infineon Trusted Platform Modules (TPMs) were compromised a few months ago [15]). And once one tamper-proof device is compromised, the whole system will be compromised. Thus, in our VSPN scheme, we enable the master secret key to be updated regularly via RSUs, yet the RSUs still have no knowledge of it by means of the property of proxy re-encryption. In [13], an RSU aided intervehicle communications scheme was proposed. A vehicle relies on an RSU to verify the signature of another vehicle. In [14], group communications in VANETs are considered and a group key update protocol was proposed. In 2009, some security and privacy-enhancing communications schemes were proposed in [16]. Of particular interest, a group communications protocol was defined. After a simple handshaking with any RSU, a group of known vehicles can verify the signature of each other without any further support from RSUs.

A common group secret is also developed for secure communications among group members. In the same year, a strategy was formulated for pseudonym update to sustain privacy when a vehicle is being observed by an adversary who has different capabilities [17]. Results show that by adopting the pseudonym update strategy, the privacy of a vehicle can be maximized. Recently in 2011, two more related works [18] and [19] were published. In [18], an efficient self generated pseudonym mechanism based on Identity-Based Encryption (IBE) was proposed for protecting drivers' privacy. In [19], an efficient social-tier-assisted packet forwarding protocol STAP for achieving receiver-location privacy preservation in VANETs was proposed.

Sr	Paper	Year	Advantage	Disadvantage
1	VSPN: VANET-Based Secure and Privacy-Preserving Navigation	2014	Privacy preserving navigation Time efficient	Centralized system Not scalable for large cities2
2	An Efficient Approach for Emergency Message Dissemination in VANET	2014	Reduce delay by reducing broadcast message redundancy High resource utilization	Message source not authenticated Replica attack
3	Prioritized Emergency Messaging of a Car Accident in Vehicular Ad-Hoc Network	2014	Collision Avoidance system Priority based emergency message generation	Messages are not authenticated Packets are not categorized in control packet or data packet
4	Request Response Detection Algorithm for Detecting DoS Attack in VANET	2014	Detect DoS attack	Only detection part No malicious node notification part
5	Balancing Safety and Routing Efficiency with VANET Beaconing Messages	2013	Maximize routing and safety efficiency	Deciding data size, transmission frequency, and communications range parameters are very difficult and may be modeled as per need

Figure 2.1: Literature Survey

The authors proposed to deploy storage-rich RSUs at social spots and let them form a virtual social tier. In this way, without knowing the receiver's exact location, a packet for him/her can first be forwarded and disseminated in the social tier concerned. Once the receiver visits one of social spots at a later time, he/she can receive the packet successfully.

Other recent efforts include [20] and [21]. These two works also target at driver privacy preservation but instead of using pseudo identities, the concept of group signature is adopted. The signature of any vehicle can be verified by the same group key but the actual signer can only be traced by a trusted party. Though privacy can be preserved, these schemes are rather complicated and may not be practical.

3. Problem Statement

3.1 System Model:

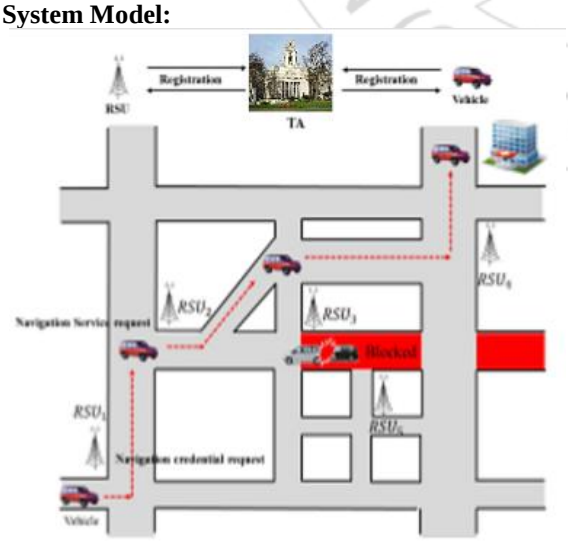

Figure 3.1: System Model

From figure assume each vehicle is having an OBU and RSU installed along the road. The TA and some essential servers are installed along the road.

1) Trusted Authority (TA) provides security by performing cryptographic operations for ex. key generation but T.A. IS very curious about the vehicular information privacy about queries.
2) TA and Tamperproof device on vehicles manage the Anonymous credential and are assumed to be trusted in the system privacy to each driver provided by bi-linear algorithm.
3) RSU are situated near by the road on fixed distance and it can't trust like the Trusted Authority.
4) The communication between the various component like Road side unit and Trusted Authority is done by the called as internet. Message encryption done by RSA algorithm. Each user maintains priority and non-priority queue for messages. User send higher priority message first(ex. Unsafe condition like accidents)
5) Each vehicle is having own real identity which should not disclosed and their real identity is known by only Trusted Authority not by the other.
6) Each RSU storing vehicle sent information a local map information in its range which includes GPS location of boundaries, name of buildings, name of streets, distance, direction to get to its neighbors and neighbor location names.
7) Temper proof device is set on every vehicle and this device is get responsibility of all cryptographic operations like store key function, pseudonymous identity generation, signing of message, message authentication and encrypt and decrypt of all messages.
8) TA and RSUs having temper proof device that having synchronized clock and by this clock time TA broadcast current time to all tamperproof device and RSUs after fixed time (periodically).

- TA is trusted authority. For our convenience, transportation authorities or central systems have administrative rights of taking a role as TA. TA is on charge of registration of Road Side Units and all vehicles exist in a VANET and issues of cryptographic materials by initial registration. In addition, TA must be able to trace a each vehicle's real identity for billing purpose of

navigation system or tracing the attacker or subscriber who makes threats for the system.
- RSUs are installed near by the roads on fixed distance and subpart of the TA. Each RSU having its local database to store real time map information (e.g., traffic density, accident events information) about its details. RSU performs the route finding process to provide navigation path for drivers and it also do cryptographic operations for providing security and privacy-preserving navigation information to each vehicle current network i.e. within RSUs' communication range. Also, RSU must not disclose any inner confidential Information without permission or the authorization of the TA.

Each vehicle set OBU to make communication with RSUs and request navigation information by query. In our system architecture, every vehicle is having its own identity and secret key provided by TA at initial phase, is used to perform cryptographic operations of messages for security of messages and privacy-preserving navigation system.

For the more clarity, following assumptions made for the system:
- Vehicles are installed with an embedded computer system, a GPS signal receiver, a wireless network interface to connect with network is having dedicated short range communications (DSRC) [2].
- TA, RSUs, and vehicles have synchronized clocks for generation of time stamp and TA sent valid time of credentials. They can also use GPS information for getting synchronized time [14].
- The adversary can make strong system and can overhear V2V and V2I communications to eavesdropping of messages from vehicles or Road side units to enjoy free navigation services and data in case if it is forwarded to the same destination.

Adversary can modify priority of the forged message which harms the service maintenance.
- The adversary can try to identify vehicles or to trace the traveling routes of a vehicle by packet analysis.
- The TA can inspect all RSUs at high level and maintain the compromised entities list.

3.2 Security Objectives

The concern of our designs is summarized as follows:
- Authentication and Authorization: Only authenticated entities should participate in the VANETs. Except that, messages should be authenticated to protect against the modification and message stealing attacks. Also, an only legitimate user which has access rights of service should get navigation information time to time to maintain the quality of service in VANET applications.
- Confidentiality: System must confirm that to deny access of navigation information service illegally from non-legitimate vehicles who may want access navigation service in free, navigation request query and reply should be kept hidden from eavesdroppers.
- Identity Privacy Preservation: The real identity of every vehicle and driver should keep confidential from other vehicles and RSUs for preserving privacy.
- Traceability: The Trusted Authority should able to get the real identity of a vehicle because issue of service charge of navigation service or non-repudiation of messages.
- Non-transferability of credential: Vehicles also not able to share navigation service information with other vehicles freely. The privacy issue being mostly raised in wireless communications, user hiding user identity has become an important for securing VANET applications. The variety of methods for user anonymity for ex protection of user identity, user intractability and so on [15, 16], and various technologies may be implemented in different application. The issue of anonymity in the protocol is defined for protection from the eavesdropping attackers. Service provider needed to disclose vehicle user's real identity for accounting of information, billing and revocation of user.

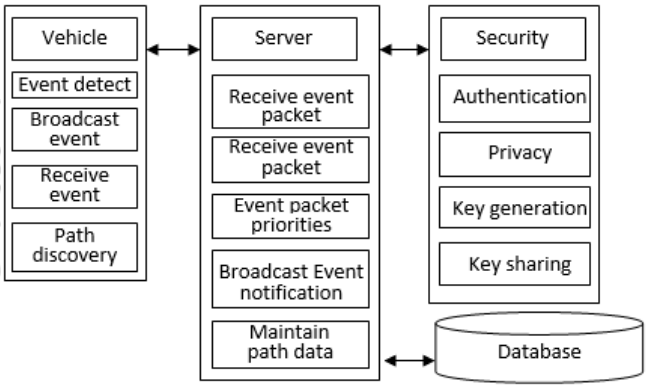

Figure 3.2: Basic Vehicular network Model

Generation of Anonymous Credentials by TA
In this scheme, a navigation credential will expire after a predefined time of expiration period (e.g., a day, a week). Thus, even if attacker breached the system information and obtains credentials, the impact of attack is limited to the system.

Trusted authority generates Anonymous credential which doesn't having driver real data. And when TPD request for credential TA encrypt and send these details and user Decrypt and save these credentials.

Requesting for Anonymous details by Vehicle hardware Device
In this project the anonymous certificate provided to user and it must be changed time to time hence trusted authority change the certificate because if this credentials are theft then its effect remain for shorter period of time

Requesting for Navigation Service by Vehicle hardware Device
Each Vehicle after started journey send request for navigation information to the RSU. TPD generate request by encrypting real messages and attach its credential to RSU.

Navigation Request and Reply Propagation among RSUs
When RSU get request it forward its request to nearer RSU's forwarding continues until doesn't get path of destination. And last RSU bind this destination path in reverse and send to main RSU then RSU send this information to Driver by priority. This priority is set by information from TA.

Urgent Change of Route Initiated by RSU
If the driver changes its route then request for the path then RSU is able to find new path to destination and inform the driver quickly.

4. Conclusion

In this paper we search a VANET-based secure and privacy-preserving navigation scheme. It utilized speed data and road conditions collected by RSUs to guide vehicles to desired destinations in a distributed manner. this scheme adopts some security primitives in a nontrivial way to provide a number of security features: 1) Vehicles are authenticated by means of pseudo identities. 2) Navigation queries and results are protected from eavesdroppers. Besides, with the idea of anonymous credential, no one including TA can link up a vehicle's navigation query and its identity. 3) Information provided by RSUs can be properly authenticated before the route is actually being used. Besides satisfying all security and privacy requirements, our solution is efficient in the sense that a vehicle can complete the whole navigation querying process and receive urgent notification in a very short time. On the other hand, the route returned by our scheme can lead to savings of up to 55 percent of traveling time compared with the offline map data searching approach. This paper also gives lower route blocking rate in practice. this VSPN scheme can apply to the situation where the route searching process is done by a central server, which collects and verifies speed data and road conditions from RSUs. The authentication process at vehicles can be even simpler because a vehicle only needs to check against the central server's signature on the processed result. However, such a centralized approach is not scalable, especially for large cities. We are implementing our VSPN scheme on a test based to further verify its performance

References

[1] G. Eason, B. Noble, and I.N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529-551, April 1955. (*references*)
[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.
[3] I.S. Jacobs and C.P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.
[4] K. Elissa, "Title of paper if known," unpublished.
[5] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.
[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740-741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.