A Survey on Privacy Preserving Schemes in Vehicular Ad-hoc Networks

Er. Sandhya, Dr.Ravinder Khanna

Abstract-**The security & privacy issues in Vehicular ad-hoc networks (VANET) are very challenging and must be addressed before they are implemented. VANET is providing various secure services and applications thereby helping the drivers for safe journey and plays an important role in creating Intelligent Transportation system (ITS). In this paper a comprehensive survey is done on various privacy preserving schemes in VANET and a comparison is done on certain parameters to find an efficient privacy preserving scheme.**

I. INTRODUCTION

Vehicular Ad hoc Networks (VANET) are categorized as an application of mobile ad hoc networks (MANET)that has the potential [1] in improving road safety and in providing travelers comfort. VANET provides a wireless communication between moving vehicles using a dedicated short range communication (DSRC).DSRC is IEEE 802.11a amended for low overhead operation to 802.11p. The IEEE then standardizes the whole communication stack by the 1609 family of standards referring to wireless access in vehicular environment (Wave). VANET is a special [2] form of MANET in which vehicles act as a mobile nodes that aims to provide communication among nearby vehicles also known as inter vehicular communication (V2V or IVC) and between vehicles and nearby road units (RSU's) referred as vehicle to infrastructure communication (V2I or RUC). There is a hybrid communication including V2V & V2I.

In VANETs, a number of vehicles [5] that are located within a certain area form a group. Each group has a dedicated RSU. Once a group is set up, members of the group can communicate with each other and with the group's RSU. Intergroup communication is also possible between vehicles belonging to adjacent groups. Another type of groups that is formed by VANETs is logical groups. Vehicles that share the same interest or belong to the same organization can form a group where they communicate with each other and exchange information, which introduces another interesting application of VANETs

Manuscript received March 23, 2014.

Er. Sandhya, Department of Computer Applications, CGC, Landran, Mohali, India, (e-mail: ersimranpreet1@gmail.com).
Dr. Ravinder Khanna, Dean R & D, MM University, Sadopur, Ambala, (e-mail: ravikh_2006@yahoo.com)

II. VANET CHARACTERSTICS

The ultimate goal of VANET is to enhance the driving experience and increase the level of safety for drivers. VANET has its own unique characteristics when compared with other type of MANET, the unique characteristics of VANET include:-

A.*Nature of Communication:*

VANET are based on short-ranged wireless ad-hoc communication, where nodes [5] establish connections with each other to exchange information. This topology is called Ad-hoc network.

B.*Predictable Mobility*

In VANET nodes are constantly changing their locations [5] with different speeds and directions, which make the network very dynamic in nature. A group can change its structure if a node leaves or joins another group. So establishing a security protocols guarantee successful communication.

C.*Real Time Processing*

Due to the extremely [5] dynamic nature of nodes in VANET information should be processed in real time to benefit from it. Safety applications such as collision prevention need real time alerts.

D.*No power constraints:*

The power in VANET is not a critical challenge [1] because vehicles have the ability to provide a continuous power to On Board Units (OBU) via the long life battery.

E.*Variable Network density:*

The network [1] density in VANET varies depending on the traffic density, which can be very high in the traffic jam or very low in suburban traffic.

F.*Rapid changes in Network Topology:*

High speed of the vehicles leads to rapid changes in the network topology. The life time of the link between vehicles [1] is affected by the radio communication range and direction of vehicles. VANET can provide communication over 5 to 10 Km, this requires data to be processed and exchanges rapidly.

G. *Position Detection:*

Vehicle position is one of the most valuable pieces of information in VANET. Vehicle [5] safety applications necessitate that each network device periodically broadcast position report. A malicious inside attacker generating false reports whose digital signature is verifiable can cause serious accidents and loss of life.

III. VANET APPLICATIONS

V2V and V2I communication allow the development [1] of a large no of applications and provide a wide range of information to drivers and travelers. Vehicle safety communication project [3] classifies the intelligent safety applications in the following two major categories:-

A.*Safety applications*

Safety applications have an essential requirement for the ability to gather information through vehicle sensors from other vehicles or both. Safety applications can be classified as:

i. Public Safety applications:

A public safety application is used to help an emergency [3] team by sending event driven messages. The objective of these applications is to minimize the travel time needed for the emergency team to reach a specific location. The approaching emergency vehicle warning, emergency vehicle signal preemption, SOS services and post crash warning are the examples of public safety applications.

ii. Intersection Collision Avoidance:

Many major accidents [1] have occurred due to intersection collision. Improving intersection collision avoidance system will lead to the avoidance of many road accidents. This system is based on I2V or V2I communication. The sensors at infrastructure gather process and analyze the information from the vehicles moving close to the intersection, depending on the analysis of data. If there is a probability of an accident or a hazardous situation, a warning message is sent to the vehicles in the intersection area to warn them about the possibility of the accident so that they can take appropriate action to avoid it. There are many applications that fall under intersection collision avoidance system they are:-

- Warning about violating traffic signal
- Warning about violating stop sign
- Left turn assistant
- Stop sign movement assistant
- Intersection collision warning
- Warning about blind merge detection
- Pedestrian crossing information designated intersection

iii. Sign Extension:

The main goal of this application is to alert inattentive drivers to signs [1] that are placed on the side of the road while driving in order to prevent accidents. The sign extension applications use a minimum frequency of 1 Hz relying on I2V communication and the use of periodic safety messages with a communication range of 100-500m. Sign extension applications can be of following types:-

- In-vehicle signage
- Curve speed warning
- Low parking structure and bridge warning
- Low bridge warning
- Wrong way driver warning
- Work zone warning
- In-vehicle Amber alert.

iv. Vehicle Diagnostic and Maintenance Application

These kinds of applications [3] are related to vehicles diagnostics and maintenance and sending alert messages to the owner of vehicle. So that the owner is reminded about safety defects of the vehicle and its maintenance schedule. The range of these events driven messages is 400m and it is used in the I2V type of communication. These applications can be of following types:-

- Safety recall notice
- Just-in-time repair notification

v. Information from other vehicle Application:

Short range communications [3] is used for sending and receiving information between a host vehicle and other vehicles. These applications are used in V2V or V2I and in both. Minimum frequency range used is 2 to 50 Hz and communication range of 50m to 400m is used for these periodic event driven messages. Information from other vehicle applications can be classified as:-

- Cooperative forward collision warning
- Vehicle –based road condition warning
- Emergency electronic brake lights
- Lane change warning
- Blind spot warning
- Highway merge assistant
- Visibility enhancer
- Cooperative collision warning
- Cooperative adaptive cruise control
- Road condition warning

B.*Non Safety Applications*

Non safety applications also known as Comfort applications. The roles of non safety applications are to provide comfort to the passengers and improve the traffic system. These applications are related to user's entertainment and these applications should not interfere with safety applications. These applications also provide opportunities for business parties to setup their business near the highway.

IV. SECURITY AND PRIVACY IN VANET

Security plays essential role in VANET communication [4] due to exchange of messages, which has high level of importance in safety applications. The safety threats by the attackers are major problems of VANET .Different researchers have categorized the attacks into diff groups depending upon their nature of attack like Sumra et.al (2011) proposed an assortment of attack, their level threat and priority of attack. They categorized them into five groups like: Monitoring Attack, Social Attack, Timing Attack, Application Attack and Network Attack. Wei et al. (2012) categorized the attacks in VANET into Non-collusion vulnerabilities into six groups include: Jamming, Forgery, Traffic Tampering, Impersonation, Privacy violation and On-board Tampering. For widespread deployment of secure VANET security solution designers should meet some basic and significant requirements. The security framework of VANET should include following parameters:

A.*Authentication/Integrity*

VANET participants need to check [5] the authenticity and integrity. The system must assure that the messages are generated by trusted source and vehicle reaction to events should base on legitimate messages. Authentication/Integrity constraint helps in preventing Sybil attacks and falsifying position information.

B.*Privacy/Confidentiality*

Privacy is the ability to trace the source of misbehaving vehicles. The privacy preservation in VANET should be conditional, where senders are anonymous to receivers while traceable by the authority. With traceability, the authority can reveal the sender's identity of a message once a dispute occurs

C.*Data Consistency*

The legitimacy of messages also encompasses their consistency with similar ones, because sometimes the sender can be legitimate while message contains the false data. This is also known as plausibility.

D.*Information Availability*

A vehicle's data should be available to all other vehicles around, all the time. Some attacks like DOS are very severe that they bring down the network. So availability should be supported by alternative means

E.*Traceability and Revocation*

An authority should be able to trace an OBU that abuses the system. Once a misbehaving OBU has been traced, the authority should be able to revoke it in timely manner. This prevents the misbehaving OBU from causing any further damage.

F.*Efficiency*

OBU's must have resource limited processors to make VANET economically viable. The cryptography used in VANET should incur limited computational overhead.

V.VANET SECURITY AND PRIVACY CHALLENGES

Various security models have been proposed. The most important aspect of security is privacy, the significant research in the field of security and privacy in VANET is discussed below:

a. One of the major challenges of securing VANET is communication security. This aims to provide secure communication between vehicles, which is referred to as Inter-Vehicle Communication (IVC), and between vehicles and Road Side Units (RSU); Vehicle-to-RSU communication (VRC). Any services include: information confidentiality which aims to prevent unauthorized access to information. Also, integrity of exchanged messages must be provided in order to detect and prevent malicious intent such as information alteration.[7]

b. Node authentication is another important issue in security to ensure that all nodes within the network are valid who are claiming to be and hence prevent impersonation. Other services which includes availability of network services for all users at all time and accountability to prevent falls claims or reject true ones.

a. Key management is another challenge in the security of VANET. Traditional methods of key revocation such as certificate revocation list (CRLs) are not suitable for VANET due to large scale network.

b. Detection of malicious nodes and intentions is another most challenging issue in VANET. It is easy to access data in the network and hence data validity is compromised. So it becomes much more difficult to distinguish between valid data and malicious data.

c. Location verification is a great challenge for VANET security. The current methods like GPS Unit or RSU considered as weak security providers as an attacker can easily manipulate the data.

d. Privacy preservation is a very challenging issue in VANET as it is concerned with protecting personal information of drivers within the network.

VI. ATTACKS ON PRIVACY

Privacy attacks in VANET are mainly related to illegally getting sensitive information [8] about vehicles. Privacy attacks are classified into two categories.

a. Identity Revealing: Getting the owner identity of a given vehicles could put its privacy at risk. Usually, a vehicle's owner is also its driver, so it would simplify getting personal data about that person.

b. Location tracking: The location of a vehicle in a given moment, or the path followed along a period of time are considered as personal data. It allows building that vehicle's profile and, therefore, that of its driver.

VII. SECURITY SCHEMES PROPOSED FOR PRESERVING PRIVACY IN VANET:

A.*Electronic License Plate (ELP) and Cryptographic Mechanism*

Hubaux et al. proposed a natural extension of license plates called ELP. This credential is issued by legal authority to make the vehicles authenticated identified. Public key certificates (PKI) are used for creating the balance between authentication and privacy. Liability attribute is required by the legal authority whenever misbehavior is detected. Burmester, M., et al. (2008) proposed cryptographic mechanism to establish a balance between privacy and liability in VANET. Identity based cryptography and pseudonymous short-lived public key certificates have been proposed to strengthen the unlink ability aspects in VANET.

B.*Secure and Efficient communication scheme with authenticated key establishment and privacy preserving in VANET (SECSPP)*

Li, C.-T., et al. (2008) proposed a scheme called SECSPP that provide an efficient and secure key establishment as well as privacy preservation in VANET. SECSPP is secured against eavesdropping and impersonating attacks and maintains data confidentiality of the nodes that are participants in VANET [9].SECSPP maintains and ensure anonymous communication for authorized vehicular users and neither the service provider nor outsiders can describe any session to a particular user when the user accesses the service from service provider. This is one of the first schemes that took care of authentication, key establishment and privacy preservation all at the same time.

C.*Group Signature and Identity-based signature scheme (GSIS)*

Lin et.al proposed GSIS scheme to offer conditional privacy in VANET. This scheme offers desirable security requirements such as authentication, integrity and anonymous user authentication, vehicle anonymity, RSU ID exposure, prevention of RSU replication, vehicle ID traceability and efficiency [10]. Lin et.al. Pointed out that traditional public key encryption scheme cannot be used in signing the safety messages, as the ID information is contained in the public key certificates. Thus, for V2V communication, group signature is employed and messages can be securely and anonymously be signed by the senders, while the road authorities can reveal the identities of the senders when required. The privacy requirement of V2I is not as sensitive as V2V communication. Thus GSIS chooses a signature scheme using ID based cryptography (IBC) to digitally sign each message sent by the RSUs to ensure origin authentication and this greatly minimizes the signature overhead

D.*An Improved privacy-preserving Navigation protocol in VANET*

W. Cho, Y. Park, C. Sur, and K. H. Rhee proposed an improved privacy-preserving navigation protocol. This protocol is based upon the concept of a two person multi signature and identity based cryptographic schemes as a building blocks. In the proposed protocol [11] an attacker cannot obtain vehicle's real identity from eavesdropping on navigation services. Identity related information of a vehicle v is rH1PIDi for key agreement with RSU during the navigation service token request protocol, and PIDij encrypted under identity-based encryption of RSU's ID during the navigation service request. Here, PIDiis vi's pseudonym as the result of EncpkTAk VID for the real identity. Therefore, neither an attacker nor an RSU can reveal the real identity of vii from PIDii

E.*Tracking together efficient authentication, revocation and privacy in VANET (TRACKS)*

Temporary Anonymous Certified Keys (TACKs) [12] is a scheme that offers authentication, privacy, short-term likability, traceability, revocation, and efficiency. TACK mainly employs group signatures to satisfy its security requirements. The design of TACKs groups the roads into geographic regions and assumes that in each geographical region there is Regional Authorities (RA) s which can serve as a certificate authority. TACK employs the group signature scheme the idea is that each member of a group has a group user key, a long-term private key, issued by a trusted group manager, such as the Department of Motor Vehicles (DMV). When a vehicle wants to obtain a certificate for short-lived TACK from its respective RA, it signs the request message with its group user key. The short-lived TACK is used for signing messages. The vehicle periodically broadcasts its certificate, so that others can verify the signed message it sends. The TACK has a very short life time and it has to be updated when the lifetime ends or when the vehicle joins a new geographical region.

VIII. CONCLUSION

In this paper various methodologies proposed for privacy preservation in VANET is discussed. Cryptographic schemes are the basic methods used in any of the security &privacy preserving technique in VANET. Each scheme discussed above has its own merits & demerits and they are suitable for specific conditions like TRACKS is well suited for interoperability environment, whereas SECPP incurs very less computational cost as compared to other privacy schemes. GSIS scheme provides best security solutions for V2V & V2I communication by requiring minimal infrastructure support. Privacy preserving navigation

Table 1: Comparison of Various Privacy Preserving Schemes in VANET

Criteria	**Cryptographic schemes**	**SECPP**	**GSIS**	**Privacy preserving navigation protocol**	**TRACKS**
Provide security to both V2V & V2I communication	Yes	Yes	Yes	Yes	No
Use of Group-based signatures & identity based sig schemes	Yes	No, it is Based on Blind signature based scheme	Yes	No, it is based on two person multi signature scheme	Yes
Revocation mechanism	Strong	Strong	Strong	Strong	Weak
Suitability for Interoperable Vehicular network	Yes	Yes	No	Yes	Yes

Protocol is providing strong authentication by using multiple signature schemes. Although each scheme is well defined & strong enough to provide security, but if we compare the performance of three schemes SECPP, GSIS, and TRACS, GSIS is proved to be better out of three. So combing the performance of Privacy preserving navigation protocol with GSIS can be a future aspect for creating a new Privacy model for securing VANET.

IX. REFRENCES

[1] Saif Al-Sultan,Moath M.Al-Doori,Ali H. Al-Bayatti,Hussien Zeden, “A Comprehensive survey on vehicular ad hoc network”, Journal of Network and Computer Applications at Sciverse ScienceDirect, Febraury 2013

[2] Sagarika Mohanty, Debasish Jena, “Secure Data Aggregation in Vehicular-Adhoc Networks: A survey” in 2nd International Conference on Communication,computing & security [ICCCS-2012] Procedoa Technology 6(2012)922-929, 2012

[3] Irshad Ahmed Sumra,Halabi Bin Hasbullah, Jaamalul-lail Ab Manan, “ Using Grades Mechanism to differentiate users in vehicular ad hoc network (VANET)”, in Ist International conference on future trends in computing and communication technologies,2012

[4] Shidrokh Goudarzi, Abdul Hanan Abdullah, Satria Mandala,Seyed Ahmad Soleymani, Mir Ali Rezazadeh Baee, Mohammad Hossein Anisi, Mirajo Aliyu, “ A system review of security in vehicular ad hoc network “, 2nd symposium on wireless sensors and cellular networks (WSCN’13) in jeddah , Saudi Arabia , paper no 0144261225-13-016 held on December 2013

[5] Mohammed A Moharrum , Ahmad A Al Daraiseh, “Toward Secure vehicular Ad-hoc Networks: A survey”,in IETE Technical Review, Vol 29, issue 1 , page 80-89, 2012

[6] David Antolino Rivas, Jose M. Barcelo-Ordinad, Manel Guerrero Zapata, Julian D. Morillo-Pozo, “Security on Vanets:Privacy,misbehaving nodes,false information and secure data aggregation”, in Journal of Network and Computer applications Elsevier 34(2011)1942-1955

[7] Moahmoud Al-Qutayri,Chan Yeun and Faisal al-Hawi ,” Security and privacy of intelligent VANETs”, in Journal of Computational Intelligence and modern Heuristics page 348, February 2010

[8] Jose Maria De Fuentes, Ana Isabel Gonzalez-Tablas, Arturo Ribagorda,,”Overview of Security issues in Vehicular Ad-hoc networks”, in Handbook of Research on mobility and computing ,2010

[9] Chun-Ta Li, Min-Shiang Hwang and Yen-ping Chu, “ A secure and efficient communication scheme with authenticated key establishment and privacy preserving for Vehicular Ad- hoc networks”, in Journal of computer communications Elsevier, pp 2803-2814, 2008

[10] Xiaodong Lin,Xiaoting Sun,PinHan Ho and Xuemin(Sherman)Shen, “ GSIS: A secure and privacy preserving protocol for Vehicular Communications”, in IEEE transactions on Vehicular technology, vol xx no xx, month 2010

[11] Wonjun Cho,Youngho Park, Chul Sur, and Kyung Hyune Rhee, “ An Improved privacy preserving navigation protocol in VANETs”, in Journal of wireless Mobile Networks,Ubiquitous Computing and Dependable Applications, Vol 4,Number 4,pp. 80-92

[12] Ahren Studer,Elaine Shi Fan Bai Adrian Perrig , “Tracking together efficient authentication,revocation,and privacy in VANETs”, in CMU-CyLab-08-011, March 2008