Volume 5, Issue 1
February 2016

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Providing Safe, Secure and Trusted Communication among Vehicular Ad-hoc Networks' Users: A Vision Paper

Amit Kumar Tyagi[1], Dr.N.Sreenath[2]
Department of Computer Science and Engineering
Pondicherry Engineering College, Pondicherry -605014, India.
Email: amitkrtyagi025@gmail.com, nsreenath@pec.edu

ABSTRACT- Information which used to be privileged only for the rich and powerful few has become crucial part of our life. In Last few years, vehicular networks (or moving objects for e.g. mobile user, vehicles etc.) are gaining more and more attraction from the researchers and the automobile industries. It emerged as a promising approach to increasing road safety and efficiency, as well as improving the driving experience. This can be accomplished in a variety of applications that involve communication between vehicles, such as warning other vehicles about emergency braking, jamming problem in next lane/road etc. In result, Security and Privacy are two integrated issues in the deployment of vehicular networks. However, if we do not take security and privacy issues into consideration, the attractive features of VANETs are broken, i.e. malicious activities will be on its peak. In particular, security requirements to provide trusted VANETs communication include authentication, data consistency and integrity, availability, non-repudiation and privacy. Among these various requirements, privacy is also one of the essential key to the VANET's users, because a lack of privacy could raise concern about the adoption of this new technology, delaying its widespread diffusion. So this paper defines a vision/answer to these question "How to maintain safe and secure privacy of a VANET users "and "How to find a trusted user for communication" nearby? This paper discusses about various attacks, attacker models, privacy and security issues etc. to provide secure and trusted communication to VANET users.

Index Terms- *Vehicular Ad-hoc Network, Security, Privacy, Trust, Attack.*

1. INTRODUCTION

With the development of micro-electronic technologies and wireless communications, we envision that in the foreseeable future vehicles will be able to communicate with each other (V-to-V) or with roadside units (RSU) which serve as the gateway to the Internet (V-to-I). Today's vehicle plays an important part of everyday life for billions of people around the world. A Vehicular Ad-hoc Network (VANET) is a technology that employs moving vehicles as nodes in a network to create a mobile network to provide communication among nearby vehicles (using on board unit), as well as between vehicles and nearby fixed Road Side Units (RSUs). VANETs have received a great deal of attention for their promises in revolutionizing the Intelligent Transportation Systems (ITS) and Telematics Services (TS) [1]. Besides that, VANET provides a ubiquitous computing environment to drivers and passengers and enables numerous services through a variety of vehicle applications [2]. Vehicles used in on-road delivery, carpooling or notify about jamming problems etc. to other vehicle users. Applications, such as emergency-braking warning, are made possible by communication between vehicles. Also VANET users used services offered by location based services [27]. A location-based service (LBSs) in Vehicular Ad-hoc Networks is to provide services that distribute on demand information for a certain geographic area of interest by taking advantage of vehicular communications [3]. Location-based services that allow vehicle users to release their location to third parties can be implemented in a similar way.

Moreover this, the characteristic of VANETs is high-speed mobility, no power issues, accurate positioning access, large scale connection range; large number of nodes, time sensitive data transfer, and leading to limited communication time among RSUs and vehicles. After then as we know, Human errors are the major source of traffic accidents, therefore building in-car technologies for checking the parking lot, avoiding accidents and guidance to the parking facility or providing secured and trusted information among VANETs users is turning out to be an integral area for research [4]. In general, a VANET used following components to exchange information between their neighbors i.e. On Board Units (OBUs) equipped in mobile vehicles, fixed Road Side Units (RSUs), and a central Trust Authority (TA). Each definition can discuss as in brief [5, 6]:

- *TA (Trusted Authority):* TA is in charge of the registration of immobile RSUs at the road side and mobile on board units (OBUs) equipped on the vehicles, and can reveal the real OBU identity of a safety message by incorporating with its subordinate RSUs. The TA is assumed powered with sufficient computation and storage capability.
- *RSU (Road Side Unit):* The RSUs are subordinated by the TA, which hold storage units for storing

Volume 5, Issue 1
February 2016

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

information coming from the TA and the OBUs. The main tasks of RSUs are (1) issuing a short-time anonymous public key certificate to each OBU when the OBU requests, and (2) assisting the TA to efficiently track the real OBU identity of any safety message [5].

- *OBU (On Board Unit):* The OBUs are installed on the running vehicles, which mainly communicate with each other for sharing local traffic information to improve the whole safety driving conditions, and with RSUs for requesting the short-time anonymous public key certificate.

The fast advances of mobile devices and positioning technologies has led to the flourish of Location-Based Services (LBSs) i.e. people want to enjoy wireless services everywhere like in hotels, colleges, etc. Vehicle users are making communication during using services (offered by LBSs) with other mobile users or others one. Now here, safety and privacy are two issue arises in deployment of using these services in a secured manner [6]. Privacy categorize in various situation like identity privacy or location privacy or personal privacy or data privacy [10, 27].

Here this paper consider only about location privacy, because location privacy is mainly concern using services over road networks. To define location privacy for vehicle users in LBSs, this paper defines three elements i.e. first element is the assumption regarding the existence of an adversary. Studies on location privacy always assume the existence of an adversary (refer figure 1). Moreover this, ultimately privacy is about feeling, and it is awkward for one to scale her feeling using a number. Generally, an adversary is assumed to access and obtain a user's location information without the user's consent. Without the existence of an adversary, talking about location privacy will be meaningless [10]. The second element is the individual, i.e., a natural person. Privacy focuses on the control over information about individuals. The last element of location privacy is location information. As explicitly stated in our definition, location information consists of the information on single locations and multiple locations that reveal an individual's movement in space and time, as well as an individual's identity information. Identity information is an individual's abstract representation in the location information. Nowadays people are more concerned about their privacy [8, 9], and for the successful deployment and public acceptance of VANET technology it is a significant factor: once privacy is lost, it is very difficult to re-establish that state of personal rights [7, 10] and the trust that people delivered into this technology.

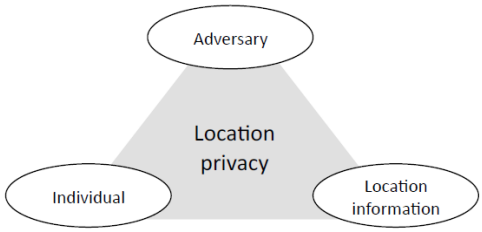

Fig. 1 Three inseparable elements of location privacy

Even though from the vehicle users' point of view to achieve a perfect privacy is preferable. Trust is a vitally important part of human existence. Trust describes the level to which an entity accepts the dependence on another one.

Further, when vehicles communicate with each other, as well as with RSUs, through an open wireless channel, in which attackers can easily get users' private information, such as identity, tracing, preference, etc., if they are not properly protected [6, 10]. After all, we need to design an efficient authentication scheme with certain level of privacy preservation for VANETs users [5]. For that, we counted several challenges; addressed in this work for e.g. a VANET entity is required to transmit periodic safety messages containing its current coordinates, speed, and acceleration to neighboring devices. A vehicle user always needs a trusted user to communicate/ to make further communications. Privacy and security are two integrated issues in the deployment of vehicular networks [10]. And Privacy-preserving authentication is a key technique in addressing these two issues. Now looking about privacy and security, to provide privacy, security is must but not vice versa [14]. Security is a condition, privacy is the prognosis. For security, authentication is a crucial security service for both inter-vehicle and vehicle roadside communications. Between privacy and security, trust is also an important issue [6, 14]. Trust is a vitally important part of human existence. It develops as early as the first year of life and continues to shape our interactions with others until the day we die. Users wish to maintain the vehicle‘s information is known only to those legally authorized to have access to them (e.g. law enforcement authorities) and remain unknown to unauthorized users. On the other hand, vehicles have to be protected from the misuse of their private data and the attacks on their privacy, as well as to be capable of being investigated for accidents or liabilities from non-repudiation [11]. Without the security and privacy guarantee, serious attacks like botnet [28] may jeopardize the benefits by the improved driving safety since an attacker could track the locations of the interested OBUs and obtain their moving patterns.

To subtly capture the safety message authentication with conditional privacy preservation, we essentially define three

Volume 5, Issue 1
February 2016

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

levels [12] of user privacy like: *Level 1:* This privacy level is anticipated by the TA, and is most likely required by the TA which can track the real OBU identity from an authenticated safety message. From the perspective of users, no privacy has been defined in this level. *Level 2:* This privacy level indicates that although each safety message is anonymously authenticated, an adversary can track an individual OBU by collecting a number of safety messages launched by the OBU. This level of privacy is not sufficient to resist a movement tracking attack. *Level 3:* This privacy level is the most desirable for OBUs, since the safety messages are anonymously authenticated, and even though an adversary has collected several safety messages from an OBU, the OBU is still not traceable. Hence the main goal is to develop a frame work that models the trustworthiness of the agents of other vehicles, preserved the privacy of vehicle users/agents including secure communications in order to receive the most effective information.

Finally this paper is organized as: Section 2 introduces the attack models and vulnerabilities. Section 3 gives the information about attacks on Authentication, Privacy and Non-repudiation. VANETs security concerns are introduced in Section 4. Security objectives or goals are provided in Sections 5. Finally this paper is concluded in Section 6. From this section onwards, this work uses terms "vehicle," and "vehicle user" or "mobile user", or "moving object" and "driver," and "user" interchangeably.

2. ATTACK MODEL AND VULNERABILITIES

A vehicle user always needs a trusted user to make further communications among neighbour vehicles in LBSs. We assume here, our communication channel is not secure, and participating OBUs (on board units) and RSUs are also not trustworthy. So major attacks and malicious behavior (refer figure 2) of an adversary anticipated on an anonymous authentication scheme (in VANETs environment) which are following as:

a) *Message Forging:* An adversary may attempt to forge a message by altering the original contents of a valid message from a legitimate OBU. It may also try to produce a valid signature on the altered message payload. Required secret credentials of the target node are either derived by guessing or stolen from a legitimate OBU as OBUs are not equipped with tamper-resistant hardware [5, 17].

b) *OBU/RSU Compromise and Repudiation:* An adversary may compromise an OBU to obtain its secret credentials, which are used for generating valid signatures. In addition, a compromised node may deliberately send false and harmful messages and later deny its involvement in signing any such messages [17]. Denial of responsibility of such kind from an adversary is called a repudiation attack.

c) *Message Replaying and Tunnelling:* An attacker may collect and store a signed emergency message from a particular traffic area and attempt to deliver it at a later time when the original message is invalid. Similarly, an attacker may collude with another attacker from a different area. A colluding attacker may tunnel the legitimate emergency messages from a specific traffic area to a different area where the message content is irrelevant for the given traffic. This unnecessary replaying of legitimate emergency or safety messages would create confusion among the VANET users in the new area. In replay attack, here an attacker replays the transmission of earlier information to take advantage of the situation of the message at time of sending. The adversary replays the valid messages sent some time before in order to disturb the traffic [5, 17].

d) *Linking of Signatures:* Signature linking refers to a situation when an attacker or an eavesdropper successfully distinguishes an anonymous entity within a group by linking some of its signatures. Back-to-back periodic messages might contain similar information in the message payload from a particular OBU. An adversary may attempt to use two or more consecutive signed messages from a node to identify the signer based on the received contents. In a group-signature-based approach, each vehicle belongs to a group that allows "group anonymous" message signature for vehicular authentications. However, if the ratio of the number of OBUs and the number of groups in a specific scenario is not high enough, user anonymity of the VANET is compromised. It is a type of linkability attack in which authentication linkability is necessary for the TA (trusted authority) [5, 30] to identify misbehaving users. In the linkability attack, a malicious user falsely claims that it has verified multiple message–signature pairs, and it also disables the TA to trace its unique identifier to avoid being punished.

e) *Random Verification Attack:* This attack is a consequence of the vulnerability induced by a random verification policy. Success of a random verification approach is highly reliant on traffic density or the number of participants in the VANET and, therefore, unsustaining [17, 29]. A harmful message may get through the authentication process without verification to jeopardize the safety of the

traffic system. In a dense traffic condition, it is quite unlikely that all received messages would be authenticated. Knowing that a verifier would randomly verify received messages, an adversary may take advantage of this situation by injecting a large number of harmful messages in each authentication cycle. This attack may bring fatal traffic consequences for a VANET-based traffic system. We define this attack as a *random verification attack* in VANETs. Hence, a real-time system such as a VANET must not risk an abuse by deploying the ordinary random verification approach, which might allow a harmful message from a malicious VANET entity.

f) *False-Signature Attack on Batch Verifications:* Signatures can be aggregated in batches for batch verifications. However, the whole batch would be dropped or rejected, even if there is just one false signature in the batch. An improved mechanism of batch verification can isolate all false signatures in a batch. Upon detection of a false signature in a batch, the verification algorithm divides the batch recursively and follows a binary authentication tree down to its leaves where individual signatures are associated. Nonetheless, this approach is effective only under normal situations when there are few false signatures in a batch. A collusion of multiple attackers could make this approach un-scalable in a high-density traffic scenario, since a verifier would require longer time to isolate individual malicious messages [17] than the message inter arrival time. This may eventually turn up as a denial-of-service (DoS) attack if all receivers in a VANET fail to process subsequent batches of signatures due to resource unavailability. It is a type of bogus information attack in which adversary may send fake messages to meet a specific purpose for example; one may send a fake traffic jam message to the others such that it can manipulate to get a better traffic condition [18].

g) *Free-riding attack without authentication efforts (or passive free-riding attack):* Such an attack is launched by a malicious user who aims to enjoy the authentication efforts of other users at no cost [19], e.g., by passively listening to the information sent from nearby users. It reduces the attacker's authentication overhead and breaks the fairness among users [8-11].

h) *Free-riding attack with fake authentication efforts (or active free-riding attack):* Such an attack is launched by an active malicious user who participates in the cooperative authentication protocol by generating fake authentication efforts [19]. Considering the asynchronism in a cooperative authentication process, the attacker checks the authentication efforts of other users and combines them to forge an authentication effort for itself. By doing so, it does not actually authenticate any original message but provide valid verification efforts because these signatures have been checked by others. This attack is more intelligent than the second one. It can be hardly detected by nearby users or the TA.

i) *Unauthorized preemption attack:* In many places, an RSU, particularly a traffic light, can be controlled to provide special traffic priority for emergency vehicles, such as ambulance, police, and fire vehicles. Similar to a bogus information attack, the adversary may illegally interrupt traffic lights by manipulating the traffic light preemptive system in order to get a better traffic condition [18, 19].

j) *Message modification attack:* The message is altered during or after transmission. The adversary may wish to change the source or content of the message in terms of the position or time information that had been sent and saved in its device to escape from the consequence of a criminal/car accident event [5, 19].

k) *RSU replication attack:* Due to the fact that there exist a large number of RSUs, cost considerations prevent the RSUs from having sufficient protection from malicious attacks, which results in an RSU compromise [5, 18]. Afterward, an adversary can relocate the captured RSU to launch any malicious attack, such as broadcasting fake traffic information.

l) *Denial-of-service (DoS) attack:* The adversary sends irrelevant bulk messages to take up the channel and consume the computational resources of the other nodes, such as RF interference or jamming or layer-two-packet flooding.

m) *Movement tracking:* Since wireless communication is on an openly shared medium, an adversary can easily eavesdrop on any traffic. After the adversary intercepts a significant amount of messages in a certain region, the adversary may trace a vehicle in terms of its physical position and moving patterns simply through information analysis [18, 19].

n) *Sybil attack*: The attacker uses different identities at the same time. In this way, e.g., a single attacker could pretend vehicles to report the existence of a false bottleneck in traffic. This attack happens when an attacker creates large number of pseudonymous, e.g.: jam ahead and force them to take alternate route [5, 15].

Volume 5, Issue 1
February 2016

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Hence to resist the aforementioned attacks and stimulate cooperation among autonomous vehicles, it is important to ensure fairness during cooperation, i.e., the greater efforts that a vehicle make, the more advantages the vehicle can obtain. In other words, selfish users cannot take advantage of the others without contributing anything themselves. This section discusses about various malicious activities countermeasure over road networks. Now next section dealt with various attacks on authentication, privacy and non-repudiation.

3. ATTACKS ON AUTHENTICATION, PRIVACY AND NON-REPUDIATION

Concerning security in VANETs, there are many attacks which threaten the V2R (Vehicle to RSU), R2V (RSU to Vehicle) and V2V (Vehicle to Vehicle) communications over the road. Here, we investigate these attacks specifically on authentication, privacy preservation and non-repudiation, and explain How they are triggered and the potential consequences. Various attacks are presented on authentication, privacy and non-repudiation, trust etc. (refer figure 2) summarized in brief as:

3.1 Attacks on the authentication: There are two kinds of attacks related to authentication in VANETs and are given as follows [24].

a) *Impersonation attack*: The attacker pretends to be another entity. The impersonation attack can be per formed by stealing other vehicular entities' credentials for authentication [5]. As a consequence, some warnings sent to a specific entity would be sent to an undesired one i.e. the adversary may pretend to be another vehicle or even an RSU to fool the others.

b) *Sybil attack*: as discussed in section 2.

3.2 Attacks on the privacy: Attacks on privacy over VANETs are related to illegally gathering sensitive information about vehicles (e.g., eavesdropping). As there is a relation between a vehicle and its driver, the exposure of a vehicle's secret/sensitive information could affect its driver privacy.

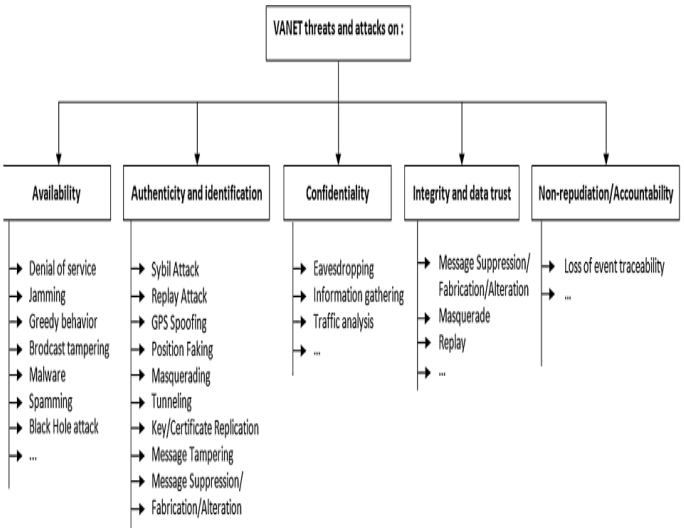

Fig. 2 Summarization of VANET threats and attacks

a) *Identity revealing attack*: Getting the owner's identity of a given vehicle 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 [6, 14].

b) *Location tracking attack*: The location of a vehicle in a given moment, or the path followed during a period of time is considered as personal data. It allows the attacker to build the vehicle's profile and, therefore, tracking its driver [10, 14].

3.3 Attacks on the non-repudiation: In VANETs, the non-repudiation is related to a fact that a vehicle cannot deny a specific message if it has sent that message. Conventionally, by producing a signature for the message in VANETs, the vehicle cannot later deny the sent messages. The attack on the message non- repudiation is explained as follows [25]:

a) *Repudiation attack*: Repudiation refers to a denial of participation in all or part of communications in VANETs [20, 29] for example, a selfish driver could deny conducting an operation on a credit card purchase, or malicious vehicles could abuse anonymous authentication techniques to achieve malicious goals or escape from their liabilities.

This section dealt with various attacks on authentication, privacy and non-repudiation. Next section dealt with security concerns required in VANET to provide a safe and secure communication in location based services.

4. VANET SECURITY CONCERNS

As discussed in section 3, VANET suffers from various types of attacks (i.e. malicious activities). Further this section

Volume 5, Issue 1
February 2016

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

categorise these attacks into a form of attacker's type like; selfish attacker, insider attacker, outsider attacker, active attacker, or passive attacker etc. some of these are discuss in brief in the following subsections with desired security requirements.

4.1 Attacks: There are different types of attacks are discussed as:

i. *Message Suppression Attack*: An attacker selectively dropping packets from the network, these packets may hold critical information for the receiver.
ii. *Fabrication Attack*: An attacker can enforce by transmitting false information into the network.
iii. *Alteration Attack*: The attacker alters an existing data, like delay in the transmission, replaying earlier transmission, or altering the data transmitted.
iv. *Denial of Service attack*: as discussed in section 2.
v. *Replay Attack*: as discussed in section 2.
vi. *Sybil Attack*: as discussed in section 2.

4.2 Attackers: Different types of attackers as follows:

i. *Selfish Driver*: A Selfish Driver can tell other vehicles that there is congestion in the road, so they must choose an alternate route, so the road will be clear.
ii. *Malicious Attacker*: This kind of attacker tries to cause damage via the applications available on the vehicular network.
iii. *Pranksters*: Include bored people probing for vulnerabilities and hackers seeking to reach fame via their damage.
iv. *Insider:* An employee at Transportation Management Center (TMC) with access to floating car data (FCD).
v. *Outsider:* Someone outside the TMC without legitimate access to FCD data.
vi. *Active:* A hacker poses as authority and queries a vehicle about its position
vii. *Passive:* An eavesdropper deploys receivers along the road to collect beacon messages.

4.3 Desired Security Requirements: To countermeasure and mitigate the potential threats in the aforementioned security threats/attack models, a well-developed security protocol should meet the following requirements [18]. There are various security requirements that have to be fulfilled for a secure transmission among VANETs users.

i. *Authentication*: In Vehicular Communication every message must be authenticated, to make sure for its origin and to control authorization level of the vehicles [21]. Two types of authentication discussed here; first is *Data origin authentication:* All the messages should be unaltered in the delivery and can be authenticated by the receiver no matter how the messages are sent by an RSU or an OBU. Secondly, *Anonymous user authentication:* Anonymous user authentication is the process of attempting to verify that a user is authentic and legitimate but does not reveal the real ID of the user.
ii. *Availability*: Vehicular network must be available all the time [21], for many applications vehicular networks will require real-time.
iii. *Non-repudiation*: Non-repudiation will facilitate the ability to identify the attackers even after the attack happens. This prevents cheaters from denying their crimes.
iv. *Privacy*: Keeping the information of the drivers away from unauthorized observers, this information like real identity, trip path, speed etc. [5, 6, 10, and 14].
v. *Real-time constraints*: Vehicles move in high speed, this will require a real-time response in some situation, or the result will be devastating.
vi. *Integrity*: Integrity for all messages should be protected to prevent attackers from altering message contents.
vii. *Confidentiality*: The privacy of each driver must be protected from outsiders from gaining the drivers information [21].
viii. *Correctness:* With the proposed security protocol, a group signature σ generated by a valid group member can surely be identified by the aforementioned verification procedure.
ix. *Unforgeability:* Only a valid group member can sign a message on behalf of the group. A valid group signature cannot be forged; otherwise, the SDH assumption will be in contradiction.
x. *Anonymity:* Given a valid group signature σ of some messages, it is computationally difficult to identify the actual signer by everyone but the group manager [6, 10]. Due to the linear Diffie–Hellman assumption, the interactive protocol underlying the group signature scheme is zero knowledge, such that no information is revealed by σ.
xi. *Unlinkability:* According to the verification procedure, it is computationally hard to decide whether two valid signatures of different groups are computed by the same group member [10].
xii. *Traceability:* The group manager can always create a valid signature and identify the actual signer by the membership recovery procedure [29].
xiii. *Revocation:* Membership revocation can be fulfilled by the aforementioned two revocation schemes.
xiv. *Vehicle anonymity:* The ID of a vehicle should be transparent to any normal message receiver to support the sender anonymity while providing their position information [18, 19].

Volume 5, Issue 1
February 2016

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

xv. *RSU ID exposure:* The RSUs or any other roadside infrastructure are not subject to any privacy issue; instead, they should evidently present their identities, including the physical locations and the services that can be provided [5, 19].

xvi. *Prevention of RSU replication:* It is very likely to happen that an RSU is compromised and/or relocated to any other place by an adversary, by which the adversary can launch various attacks through the compromised/relocated RSU [18, 19], possibly causing the whole VANET into disruption. Effective countermeasures to the RSU replication attack must be provided to maintain the security of VANETs.

xvii. *Vehicle ID traceability:* The authorities should be able to reveal the real identities of the message senders in order to guard the truth when there is any dispute.

xviii. *Efficiency:* The communication overhead of each packet and processing latency at each vehicle must be as small as possible [22].

4.4 Privacy principles (from privacy laws and regulations): Various privacy principles needed to create a vision for providing secured and trusted communication among vehicle users. Every principle can be categorized as:

1. Notice/Awareness
2. Data minimization
3. Purpose specification
4. Collection limitation
5. Use limitation
6. Onward transfer
7. Choice/Consent
8. Access/Participation
9. Integrity/accuracy
10. Security
11. Enforcement/Redress

Anonymity-related principles

12. Anonymity
13. Pseudonymity
14. Unobservability
15. Unlinkability
16. Deniability

Other desirable principles for privacy enhancement

17. User preference
18. Negotiation
19. Seclusion
20. Ease of adoption
21. Ease of compliance
22. Usability
23. Responsiveness
24. DoS resilience authentication
25. Strong privacy preservation
26. Low certificate management [5]
27. Low bandwidth consumption [5]
28. Low network delay
29. RSU- aided system key updating

4.5 Privacy Requirements: Following privacy elements required to provide a certain level of privacy to moving objects (or mobile user) during using location based services. Each one can be discusses in brief as:

1. *Mitigate the observability threat:* No federation entity shall be able to aggregate data about the usage of multiple services by users (principals), therefore being unable to deduct personal interests or behavior [23]. (Compare to limited observability in the glossary.)
2. *Mitigate the linkability threat:* Aggregation of personally identifiable information (PII) used for different purposes or in different contexts is undesirable [10, 23]. That being so, two service providers processing data of a principal shall not be able to link that data without explicit user consent or the help of a designated opener. If complete pseudonymous authentication is not achievable, then at least those attributes that identify a user uniquely shall be pseudonymized. This applies, e.g., to the ubiquitous e-mail address. (Compare to limited linkability in the glossary.)
3. *Prevent the unauthorized aggregation of attributes:* No federation entity shall be able to collect attributes beyond the specified purpose of a service and deduct personal information and behavior.
4. *Enable authorized aggregation of attributes:* A service provider shall be able to request attributes from different attribute providers within the limits of the purpose of the service [23].
5. *Prevention of unauthorized attribute polling:* A mechanism to prevent unauthorized discovery of attributes shall be provided.
6. *Prevention of replay and reuse attacks:* An identity provider must limit each assertion to used only once at a specific service provider.
7. *Consent handling:* The flow of releasing attributes should regard the processing of user consent, where explicit consent is appropriate.
8. *No supreme deity:* Actors managing trust roots must not have access to either attributes or transaction data.
9. Maximize compatibility with existing single-sign-on profiles to the extent that other requirements are not compromised:
    a. *Feasible implementation effort:* The model shall make use of existing profiles and implementations as far as reasonable.

b. *Feasible deployment effort:* It shall be possible to use existing SAML service provider implementations within current configuration limits. For identity providers, that is desirable as well.

10. *Minimize the release of attributes:* The identity authority, in its role as personal identifying information (PII) controller of a principal's identity information, must be assured that only those attributes deemed necessary for the purpose of the service are released to the relying party because large number of attributes make system complex only.

This section discusses about some of VANET attacks again with types of attackers and requirement needed to provide a secure communication among VANETs users. Now next section dealt with required security goals for VANETs users in detail.

5. SECURITY GOALS

As discussed, VANET is a large-scale wireless network scenario for public service; it faces serious security and privacy challenges. As discussed, authentication, confidentiality and non-repudiation are key properties of security that have a special significance in the domain of privacy. And the important key element in a security system is *trust*. A system should be able to prevent any generic attack on vehicular networks [24]. The system should use a secure and trusted communication infrastructure, able to satisfy a set of security requirements *authentication*, *integrity*, *availability*, *non-repudiation* and *privacy*. In the PASS scheme [16], we aim to achieve the following security and privacy objectives. Further we consider the following objectives to design secure location-aware services in VANETs:

a) *Location Assurance*: A location-aware service should guarantee the semantics that the information about a certain location of interest is related to the claimed target location. That is, it must be possible for a requesting vehicle to verify that a response message was actually originated from a vehicle within the target location area [25].

b) *Location Tracking Avoidance*: The real identity and location privacy of a vehicle should be preserved from illegal tracing through a vehicular communication even though location assurance is supported.

c) *Vehicle Tracing:* The authorities should be able to trace the originator of a message by revealing the real identity in case of any disputed situation such as liability investigation. That is, privacy preservation protocols in a VANET must be conditional by way of precaution against problematic cases.

d) *Syntactic privacy*: In brief, all vehicles that use pseudonyms must change those pseudonyms from time to time.

e) *Semantic privacy:* This captures the idea that vehicles must not be traceable by reconstructing the trajectories implied by their heartbeat messages [26].

f) *Identity privacy:* This techniques attempt to forestall the re-identification of users (deprived of their real identity) in LBSs providing anonymous services [6, 7, 10 and 14].

g) *Robust privacy:* This captures how misbehaving entities within the system may affect privacy and security [26].

h) *Authentication*: Only legitimate entities should take part in the VANETs. In addition, the originator of a message must be authenticated to guard against the impersonation and message forgery attacks [5, 13].

i) *Non-repudiation:* Any entity cannot deny the messages generated by itself. It is necessary for accident investigation that the malicious user should pay the fiddler for misleading the victims;

j) *Identity revocation:* It should be possible to exclude an unexpired membership from VANET. It is a fundamental requirement to defend the inside attacks and restore the security of VANET [10].

k) *Availability:* It assures that the system works properly and that service is provided to authorize users as and when required. An adversary may deny services to valid nodes by jamming the channel, by disrupting the routing protocol, by draining the battery power, etc.

l) *Conditional anonymity:* It means the TA can reveal the real identity of the members while other entities could neither identify the real identity nor correlate these messages signed by the same member in a long term [16]. In pseudonymous authentication schemes, conditional anonymity is supposed to be held if the validity period length of a pseudonymous certificate is less than a threshold [24].

m) *Backward privacy:* Once a membership was revoked, it should not reveal any information that decreases the conditional anonymity for the same member in the period before the revocation takes effect.

n) *Integrity:* It is the assurance that the data received are exactly the same sent by the authorized node without any modification, deletion, insertion or replay. To ensure integrity of data unauthorized manipulation must be detected.

Volume 5, Issue 1
February 2016

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

o) *Confidentiality:* It deals with the protection of data from unauthorized disclosure. Disclosure of this data may lead to identification of vital information.

Other features should also maintain in a VANET to provide secure communication like: DoS resilience authentication, Strong privacy preservation, Low certificate management overhead, Low bandwidth consumption, Low network delay, RSU-aided system key updating etc. In last, some of challenges in VANET are summarized as in brief i.e. Network management; Congestion and collision control; Environmental impact; Security; Social and Economic challenges.

Hence this section defines various security goals/objectives required to provide a trusted, secured, and privacy persevered communication among vehicle users over road networks. Finally next section concludes this work with some important future works in brief.

6. CONCLUSION AND FUTURE WORKS

Without the security and privacy guarantee, serious attacks may jeopardize the benefits by the improved driving safety since an attacker could track the locations of the interested OBUs and obtain their moving patterns. Therefore, How to provide anonymous safety message authentication has become a fundamental design requirement in securing vehicular networks. However, anonymous message authentication in vehicular networks is a double-edge sword. Moreover this, This work discusses about various terms like attacks in VANETs, privacy and security issues, required security objectives, and requirements to provide secure communication to VANET users over road networks (in LBSs). As discussed, till now there is no single framework to protect privacy (for e.g. data, location, identity etc.), while various models are there but they are insufficient to preserve privacy against various attacks like continuous query or ranging query attack etc. As conclusion, *this work proposed only a vision i.e. to provide answer of a question "How to maintain safe and secure privacy (i.e. secure communication) in VANETs "*. For future research, there is needed to build a generic architectural framework towards addressing these security and privacy issues/challenges in a holistic manner. Now we are in a new era where provided security and privacy issues will help us to discover new knowledge that no one has discovered before. So everybody is warmly invited to provide a safe, secure and trusted environment to moving objects.

ACKNOWLEDGEMENT

The authors have declared that they have no acknowledgement.

AUTHOR'S PROFILE AND COMPETING INTERESTS

Amit Kumar Tyagi is currently working as Ph.D Research Scholar (Full-Time) in Pondicherry Engineering College, Puducherry. He has completed his M.Tech in Computer Science and Engineering from **Pondicherry Central University, Puducherry**, in 2012. His research interests include Smart and Secure Computing, Network and Information Security, Theoretical Computer Science, Privacy (including Genomic Privacy), Evolvable Hardware, Parallel Algorithms, Cloud Computing.

Dr. N. Sreenath is currently working as Professor in Pondicherry Engineering College, Puducherry. He completed his PhD in Computer Science and Engineering from **Indian Institute of Technology, Madras**, in 2003. His primary research interest lies in WDM Optical Networks. High speed networks.

REFERENCES

[1] Y.hou et al., Simulation Based Testing and Evaluation Tools for Transportation Cyber-Physical Systems, IEEE, 2015, Online available at http://www.cse.buffalo.edu/CTS/papers/TVT Simulation_Survey.pdf

[2] Md. Humayun Kabir, Research Issues on Vehicular Adhoc Network, International Journal of Engineering Trends and Technology (IJETT) – Volume 6, Number 4, Dec 2012.

[3] Youngho Park, Chul Sur, Kyung-Hyune Rhee, A Privacy-Preserving Location Assurance Protocol for Location-Aware Services in VANETs, Wireless Personal Communications, December 2011, Volume 61, Issue 4, pp 779-791.

[4] Mahmud, S A, Khan, G M, Rahman, M, Zafar, H, A Survey of Intelligent Car Parking System, Journal of Applied Research and Technology, 2013.

[5] Amit Kumar Tyagi, N. Sreenath, Preserving Location Privacy in Location Based Services against Sybil Attacks, IJSIA Vol.9, No.12 (2015), pp.189-210, December, 2015.
[6] Amit Kumar Tyagi, N.Sreenath, "Location Privacy Preserving Techniques for Location Based Services over road networks", ICCSP, 2-4 April, India. 2015.
[7] Maria Luisa Damiani, Location privacy models in mobile applications: conceptual view and research directions, springer, 2014.
[8] Bail hoh et al., Protecting Location Privacy through Path Confusion, IEEE Xplore, 2005.
[9] Serna, Jetzabel, Luna, Jesus, Medina, Manel, Geolocation-based Trust for VANET ' s Privacy, Journal of Information Assurance and Security 4 (2009) 432-439.
[10] Amit Kumar Tyagi, N. Sreenath, A Comparative Study on Privacy Preserving Techniques for Location Based Services, BJMCS, and July, 2015 10(4): 1-25, 2015.
[11] Jie Li, et al., ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs, parrellel and distributed system, Issue No.04 - April (2015 vol.26) pp: 938-948.
[12] Rongxing Lu, Xiaodong Lin, et al., ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications, IEEE INFOCOM 2008 proceedings.
[13] Mingzhong Wang, Dan Liu, et al., LESPP: lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication, Springer-Verlag Wien 2014.
[14] Amit Kumar Tyagi, N. Sreenath, "Future Challenging Issues In Location Based Services", IJCA, volume 114, no. 5, March, 2015.
[15] Thiago M. de SALES et al., A Privacy-Preserving Authentication and Sybil Detection Protocol for Vehicular Ad Hoc Networks, IEEE, 2014.
[16] Yipin Sun, Rongxing Lu,et al., An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications, IEEE Transactions on Vehicular Technology, VOL. X, NO. X, XX 2010.
[17] Subir Biswas et al. "A Cross-Layer Approach to Privacy-Preserving Authentication in WAVE-Enabled VANETs," IEEE Transactions on Vehicular Technology, VOL. 62, NO. 5, JUNE - 2013.
[18] Xiaodong Lin, Xiaoting Sun, et al., "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications," IEEE Transactions on Vehicular Technology, Vol. 56, NO. 6, November, 2007.
[19] Xiaodong Lin, Rongxing Lu, Book: Vehicular Ad Hoc Network Security and Privacy.
[20] Al-Sakib Khan Pathan, Book: Security of Self-Organizing Networks: MANET, WSN, WMN, VANET
[21] Ghassan Samara et. al., Security Analysis of Vehicular Ad Hoc Networks (VANET), 2010 Second International Conference on Network Applications, Protocols and Services.
[22] Ma Hui, Security and Privacy Protocol for Traffic Tracing, International Journal of Advancements in Computing Technology (IJACT) Volume5, Number4, February 2013.
[23] Rainer Hörbe et. al. A Model for Privacy-enhanced Federated Identity Management, 2014. Online available: http://arxiv.org/ftp/arxiv/papers/1401/1401.4726.pdf
[24] JM Serna-Olvera, A Trust-driven Privacy Architecture for Vehicular Ad-Hoc Networks, 2012, Thesis: http://www.tdx.cat/bitstream/handle/10803/116542/TJSO1de1.pdf?sequence=1
[25] Chul Sur, Youngho Park et. al., Securing Location-Aware Services Based on Online/Offline Signatures in VANETs, springer, 2011.
[26] Levente Butty´an Tam´as Holczer, SLOW: A Practical Pseudonym Changing Scheme for Location Privacy in VANETs, IEEE Xplore-2009.
[27] Amit Kumar Tyagi, Dr.N.Sreenath, A Robust and Secure Infrastructure to Preserve Privacy for Location Based Services over Road Networks, ICADET, 2015.
[28] Amit Kumar Tyagi, G.Aghila, A Wide Scale Survey on Botnet, International Journal of Computer Applications, Volume 34– No.9, November-2011.
[29] Amit Kumar Tyagi, Dr.N.Sreenath, Exposing and Classifying attacks in Vehicular Ad-Hoc Network (VANETs), ICADET, 2015.
[30] Amit Kumar Tyagi, N. Sreenath, Providing together Security, Location Privacy and Trust for moving objects, IJHIT Vol.9, No.3 (2016), March, 2016.