

A Review on Security Challenges in Vehicular Internet

A.V Ramana¹, K.N.E. Sai lalith²

Information Technology¹
GMR Institute of technology, Rajam

Computer Science and Engineering²
GMR Institute of technology, Rajam

Abstract— Vehicular Ad-Hoc Network (VANET) is recent technology with propitious future as well as enormous challenges mainly in security. VANETs not simply offers security enhancement but also provides several opportunities in commercial sectors. Many companies suggested driver-less vehicles are more reliable than humans in terms of safety. This has emerged as a technology driven approach, which drives future vehicular technologies and intelligent transportation systems (ITS). Presently, it provides a foundation for the future vehicular Transportation. In this paper, we study on VANET security & privacy challenges and its principles. Besides, we focus on VANET security characteristics to classify its existence and opportunities over existing approaches. User necessities should be taken in to concern to permit the implementation of security in VANETs with systematic communication between clients. The security will be essential to the client however most likely not for each situation and for everybody. An extensive overview of VANETs security characteristics and challenges and we proposed a lightweight mechanism for revoking security certificates. We present a prescribed evidence of the protection of our system by dropping the size of Certificates Revocation Lists (CRLs).

Keywords: Vehicular Ad-Hoc Network (VANET), Security, revocation

1. INTRODUCTION

An ad-hoc network could be a local area network (LAN) that's designed spontaneously as devices connect. Instead of reckoning on a base station to facilitate the flow of messages to every node within the network, the individual network nodes forward packets to and from one another. Mobile ad hoc networks (MANETs) and vehicular ad hoc networks (VANETs) are the two varieties of ad hoc networks. A mobile ad hoc network (MANET) is usually outlined as a network that has several free or autonomous nodes, usually composed of mobile devices or different mobile items which will organize themselves in varied ways in which and operate while not strict top-down network administration. A VANET could be a variety of MANETs that permits vehicles to speak with roadside equipment. The vehicle information is also accustomed live traffic conditions or keeps track of trucking fleets. Modern vehicles are furnished with infotainment frameworks that enable utilization of non-vehicular information, providing drivers helpful installed capacities when driving, for example, without hands calling, content informing and Internet ability. The main distinction between VANETs and MANETs is that the nodes move with higher average speed and also the range of nodes is assumed to be terribly massive. Therefore, an approach to privacy in such networks must not rely on central services or mandatory connections to some fixed infrastructure. In the past decades, automotive industries have emerged several technological advancements for the development of unmanned automotive vehicles. However, this rapid development could not provide any proviso mechanism in terms of road safety. Due to smog Ice, and other natural hazards on the road, vehicles can easily be

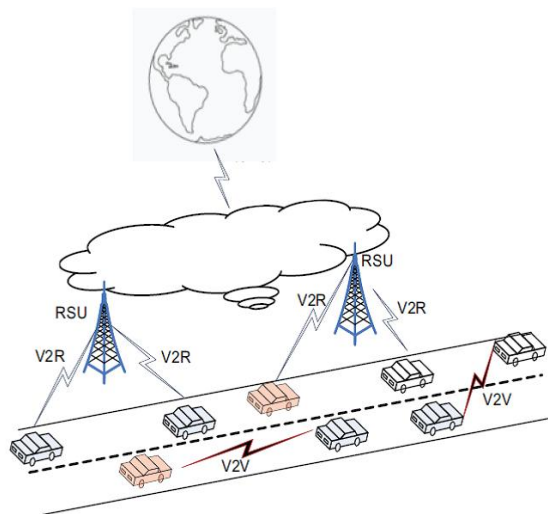
prone to accidents that cause human loss. As a result, several automobile industries have been working continuously for the innovative design of smart sensing car. With the rapid evolution in telecommunication fields, the smart sensing card can connect the vehicles with each other over wireless technologies. It allows the communication and collaboration between the on-board sensing devices. The innovative mechanisms of Industries are promoted mutually for the promotion of governments also.

In 2015, UK government announced that 100 Million pounds for the researches to design the driver less cars collaborated with Information Technology (IT), Telecommunications and Infrastructure [15]. In US, automobile manufactures like General Motors (GM) offer 4G Long Term Evolution (LTE) that are completely associated as autonomous car and it is expected to be unveiled by the end of 2020. IEEE believes that self-government automotive would be prevalent by 2040 [11]. The manufactures such as GM plus Portage have opened the application advancement for the design of Application Program Interface (API) that is accessible to application designers [9-13]. Vehicular internet includes that vehicle creating cautioning messages that alert drivers he is moving towards to another vehicle. They use a traditional approach to design an application that is available for download after the successful test cases. LTE networks is used as a serving tool to enhance the in-vehicle communication providing rapid web, spilling films, route, music, and live TV, etc. It is also used to offer area based administrations and advancements especially for vehicle travelers. LTE makes the vehicles as a part of Internet hub to facilitate the route of Vehicular Ad Hoc Networks (VANETs). However, Security and safety of clients in VANETs are dynamic be that as it may, in the meantime, a target and practical meaning of

security and protection is additionally required. This indicates the level of safety and protection guaranteed within VANET can be close to it being in this present reality. Securing the motor vehicle from outside attacks so vehicle is not held slightly is danger and it will be the largely critical test to address.

This force is particularly testing in independent or driver-less motor vehicles, as by summary the motor vehicles is necessary to explore without anyone else by controlling the monitoring and manage arrangement of the vehicle. Therefore, securing the control circumstances of the motor vehicle will be the primary thing to must be completed and just conceivable through exceptionally solid security circumstances set up to protect the vehicles from some cyber-attacks. A social network provides a variety of mechanisms for users to share data with other users. Also, it has the ability to search for users with similar interests and to establish and maintain communication between them. These social networks are classified into Mobile Social Networks (MSNs) and Vehicular Social Networks (VSNs). The coordination of these networks gives some novel applications, for the most part dedicated to security and entertainment. These assets went with developing concerns for the privacy of the information. The information could be sensitive, delicate, for example, intimate conversation, credit and money related. As the traditional social networks are incorporated into ad hoc networks, MSNs and VSNs have turned out to be touchy to security and protection issues contrasted with customary MANETs and VANETs. Secure communications for VANETs and MANETs have become an important issue these years. Many protocols for secured communications have been proposed, yet fewer protocols are concerned with secured group communications for both MANETs and VANETs.

1.1 COMMUNICATION IN VANETs:

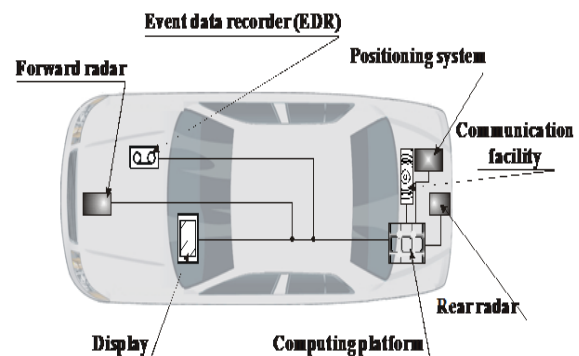


(a). Communication in VANETs

Basically, communication between vehicles improves the protection of vehicle. And it supports intelligent transportation system (ITS). On Board Unit (OBU) is one amongst the fundamental element in VANETs. OBU could be a device that is within the vehicle that processes the information assortment from the varied sensors fitted within the automotive. Communication devices mounted on vehicles. Road side Unit (RSU) is additionally element in VANET's; it's AN infrastructure for contact between the cars for sharing and data from several vehicles. RSUs connect with application servers.

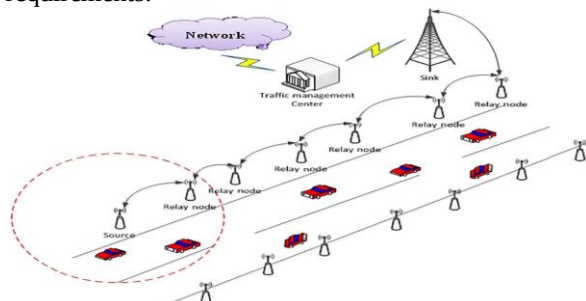
There are mainly two types of communications scenarios in vehicular networks: They are

- Vehicle-to-Vehicle (V2V): V2V is a technology which allows communication between vehicles. It is worked on base of Dedicated Short-Range Communication (DSRC). It is used to reduce accidents. Share key information like traffic, accidents etc.
- Vehicle-to-RSU (V2R): It provides communication between vehicles and RSU. This V2R are facilitating that solution to longer-range vehicular networks. diagram describes about V2V and V2R Communication



The main requirements for a vehicle to be in VANETs are: Vehicles should have an On-Board Unit, which holds a processor, a memory, GPS unit, transceiver, antenna, communication modules like some other components as mentioned in above diagram. Maximum recent vehicles are manufactured with all these to prop up VANET. Still the approval of VANET is not at all easy. Since it is manufactured for safety and security purposes we should take necessary precautions to adopt VANETs. For providing security to VANETs we have some methodologies.

A two-layer vehicular network was tended to in recent explores. The top layer comprises of TA (Trust Authority) and application servers (Traffic Control Center). The communication in the middle of them depends on the Dedicated Short Range Communication (DSRC) protocol. Every vehicle has its own particular open/private key sets issued by TA as indicated by the security standard of VANET. Before messages are sent, vehicles need to sign the messages with their private keys to ensure the



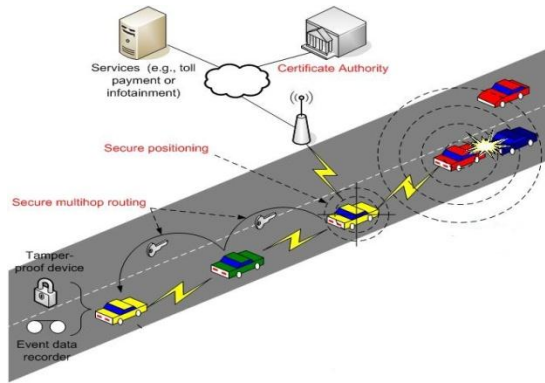
4) Non-repudiation: A pernicious vehicle can't communicate wrong messages to mislead an RSU and deny the practices when TA follows it by its message signature

- Hartenstein et al [2], in 2008 projected about. A sermon review on Vehicular Ad hoc Networks. In this VANETs involve vehicle-to-vehicle plus vehicle-to-framework connections based on wireless technologies and LAN advancements. Vehicular communication systems can be more useful to keep away from accidents and traffic jams.
- Haas, J.J., Yih-ChunHu et al [3], in 2009 proposed about Design and scrutiny of a lightweight license revocation mechanism for VANET. They projected a certificate organization technique where certificates meant for a single vehicle are related by a single, secret revocation key. They had studied and improved the feasibility of distribute Certificate Revocation Lists (CRLs).
- Benin et al [4], in 2010 suggested Unified pseudonym circulation in VANETs. The associated vehicle is inevitable and it is essential that means

- P. B. et al., [1] in 2003 December projected about “The Arbitron national in-car study”, In a recent study bring into being that American spent 15 hours/week in a car. Each certificate is used for ten-minute period and not at all reused. Then 4660 certificates are consumed each year. so, a vehicle will require around 5K certificates per year. And for every five years we need to store 25k certificates tech. rep., December 2003.

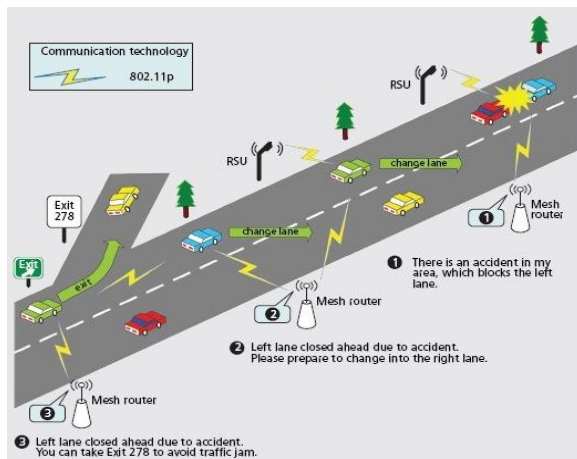
Vehicles could contribute the role of an agreeing structure for several massively used apps for example, disaster cautioning system, traffic information etc. There are countless factors to consider when designing a VANET. VANET contact is noticed in self-motivated security systems, which aspire is to boost security of travelers by interchanging some caution messages among vehicles.

Following diagram describes about the basic architecture of a VANET:



(b) Architecture of VANET

The major areas of these events are to increase road safety and transportation efficiency as well as to reduce the impact of transportation on the environment. It uses GPS and DGPS equipped devices. In above diagram we can clearly understand that communication in VANETs. In that diagram there is situation, a vehicle meet with an accident then that area got blocked by traffic and may chance for traffic jam, during that situation that vehicle sends information to another vehicle through V2V or V2R. Then another vehicle receives the information that in his way there is traffic jam due to an accident. So, it suggests another path to travel. Like below diagram



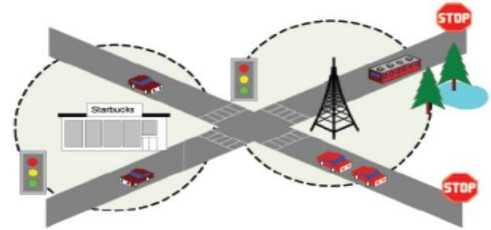
If any accident may happen in an area: it transmits message to nearby RSU or Vehicle like

1. There is an accident in my area which blocks the area with traffic by vehicle near to incident. Sends information to another vehicle.
2. Like this information communicates from vehicle to vehicle.
3. Finally, who have chance to slide to another for those it will transmits message like "This way was blocked due to accident you can take another way which was located on your left to avoid traffic jam".

VANETs are mainly falls within three categories: pure cellular/WLAN, pure ad hoc, and hybrid. They are discussed as follows:

3.1 Cellular/WLAN:

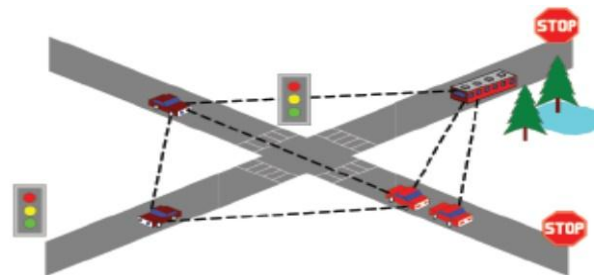
In this type of network architecture, a static cellular entrances and WLAN/WiMAX access points at traffic relations are used to append in to the Internet, for to collect traffic records, or for routing purpose. The system architecture in this scenario is a pure cellular.



Cellular/WLAN net architecture

3.2 Ad Hoc:

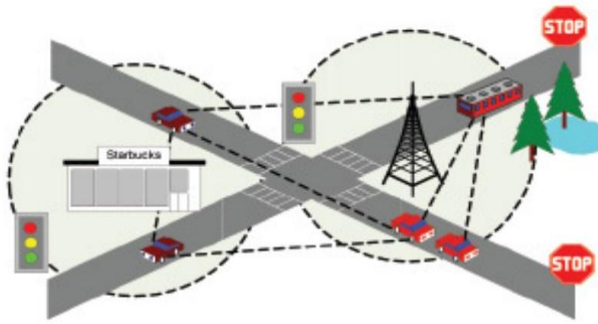
The cellular/WLAN net architecture is costlier since it incorporates permanent gateways and other hardware contraption consequently to overcome these crisis vehicles and roadside wireless contraption can exterior a clean ad hoc network.



Ad hoc Network architecture

3.3 Hybrid:

Hybrid architecture in below is a combination of infrastructure network and ad hoc network. This is too a feasible solution for VANET. The hybrid style can afford better coverage.



Hybrid Network architecture

4. Existing Methodology

The existing scheme deals with preserving user privacy for V2I and V2V communications in VANET. There are three algorithms in the scheme:

1. Energy Saving via Opportunistic Routing (ENS_OR) Algorithm
 2. Fast Randomized Algorithm (FRA)
 3. Chord Algorithm
- ❖ Based on checking relay node energy, ENSOR is used to find the best and shortest path for query travelling to sink
 - ❖ FRA is used to give a key for individual vehicles and it is used for sink to assign a primary key for each registered vehicle
 - ❖ Chord algorithm is used control the speed of the vehicle to avoid accidents

ENS_OR Algorithm:

- This algorithm provides explanation on how to choose and prioritize position by using some optimal energy approach on each one node and how to pick the optimal relay node.
- As well, the dispatch data can be classified into two categories:
 - 1) It collected information and records of its own
 - 2) It relay information and records from other nodes

5. ETHODOLOGY

Many security threats in VANETs. Security of users in VANETs are very important but, at the same time, an objective and realistic definition of security also needed. In the actual world, a vehicle can be identified by its registration plate, for fear that of accidents, which implicit trackable. The existing techniques have the following contributions:

- Certificate Organization Method
- Privacy Preserving Certificate Groups
- Revocation Method
- OCSP (Online Certificate Status Protocol)
- Efficiently Disseminating Certificate Revocation Lists

5.1 Certificate Organization Method:

Certificate Organization Method is where the certificates for an single vehicle are identified by a single key. Nodes can exchange certificates upon first encounter. An example is shown in Table 1. In a VANET, there is a pressure between privacy and authentication. traditional safety acknowledgement obligation be trusted, and this requires trusting the dispatcher.

Table 1: An instance of a public key certificate substitute. At what time vehicle A hears a message from a earlier unknown vehicle X.

$X \rightarrow *: \langle \text{Message}_i \rangle$	A receives a broadcast from X but does not have X's short-term key.
$A \rightarrow *: \langle \text{cert}_A, \text{pub}_A, X \rangle$	A broadcasts its certificate, its signed short-term public key, and a request for X's certificate
$X \rightarrow *: (\text{cert}_X, \text{pub}_X)$	X broadcasts its certificate and its signed short-term public key.

An attacker A, who attacks privacy needs only to link P to V one time (e.g. by listening to messages sent by V near V's home location). Then, by employing listening stations near a location of interest, A can determine if and when V visits that location.

5.2 Confidentiality Preserving Certificate Groups:

A CRL is a file of cancel certificates that include distributed canceled by a given Certification Authority(CA). Certificates may be canceled for a number of reasons with of a gadget that is using a given certificate. For creating a group of certificate id's for a vehicle v1. Even the vehicle have more number of certificate we have a single secret key. That key is unique value to every vehicle. The mechanism used for certificate revocation depends on the Certification Authority. Most Certification Authorities support cert revocation from the management interface.

5.3 Revocation Method:

When CA wishes to revoke vehicle 'V'. It simply add the value of (RK)s to CRL. When a vehicle receives a new CRL

that includes a new secret key S , it encrypts each r , which are known to every vehicle. If the results matches the certificate ID, then certificate is revoked. To do this, a vehicle generates all possible revoked $Es(r)$ given a key s . The consequential certificate identifiers can then be integrated in a Bloom filter[3]. Revoked certificate storage for the vehicles use Bloom filters to store all revoked certificates.

❑ Deterministic vs. Probabilistic:

To evaluate the concert of deterministic versus probabilistic, AVL trees and red-black trees can be expand to include and search the certificates

❑ False Positive Rate:

A certificate from a non-revoked vehicle could trigger a false positive when using a Bloom filter, that is, the certificate could appear to be revoked. False positive rate can be chosen by setting 3 parameters: the number of elements to be inserted (n), the size of the data structure (m , here species in bits), and the number of hash or index functions used for insertions and searches (k).

$$P(\text{false positive}) = 1 - \left(1 - \left(1 - \frac{1}{m}\right)kn\right)^k$$

5.4 OCSP (Online Certificate Status Protocol):

It allows you to removes many of the drawbacks of CRL by allowing the user to make sure that the certificate status for a single certificate. The OCSP process in shown below,

- Client receives certificate.
- Client sends OCSP appeal to OCSP Responder with the certificates index number.
- Then it responds with a certificate grade of good, anonymous. The central **benefit** to OCSP is that because the user cans inquiry the status of mono certificate, before having to download and also analyze total file there is much less overhead on the client and network.

Now, following algorithm describes Certificates generation:
Certificates generation algorithm

1. Require: M =number of Certificate for this vehicle
2. Begin: certificate loading for vehicle V
3. $s \leftarrow \text{generate_revocation_key}()$
4. for $r=1$ to M do
5. $(K^+, K^-) \leftarrow \text{generate_public_private_key}()$
6. $\text{sigCA}, r \leftarrow \text{sign}(H(\{Es(r), K^+\}), KCA^-)$
7. $\text{Cetr} \leftarrow \{Es(r), K^+, \text{sigCA}, r\}$
8. END for
9. send($V, \{\text{Cert1}, \dots, \text{CertM}\}$)
10. END

Certificates must incorporate another field containing a single integer.

Initially, the CA picks a secret Revocation key (Rk) ' s ' for each and every vehicle.

That Revocation key s is the key to block cipher, which takes selected length inputs and permutes them into yields of

a similar length, where the specific stage picked depends on the key.

On the other hand, s can be the seed for a $PRNG$ rather than the key to a block cipher.

Next, the CA makes M public/private key-sets ($M=25,000$) (K^+, K^-), $r \in [1, M]$. Then the CA creates a similar group of M certificates.

Then for each r it creates a certificate.

$$\text{Cetr} = \{Es(r), K^+, \text{sigCA}\}$$

Here, $Es(r)$ is certificate ID and the value produced by encrypting the integer r using the block cipher or by $PRNG$.

After that it will sends those certificates to each vehicle. send ($V, \{\text{Cert1}, \dots, \text{CertM}\}$).

Then 4660 certificates are consumed each year. So, a vehicle will require around 5K certificates per year. And for every five years we need to store 25k (M) certificates. In the above algorithm the value of M is 25000.

Finally, we got a certificate like $\text{Cetr} = \{Es(r), K^+, \text{sigCA}\}$. After that it will sends those certificates to each vehicle. Send ($V, \{\text{Cert1}, \dots, \text{CertM}\}$).

We have types of certificates before a CA issuing a certificate to a company the CA performs a level of validation on the authenticity that the company. Here we have 3 levels of confirmation.

Domain Validation (DV): This is the one of the least expensive certificate of the 3. It only requires a crucial form of DV to be performed. Validation is performed by electronic mail.

Organization Validation (OV) - When obtaining an OV certificate the company name is checked against a company register, i.e. Chamber of Commerce.

Extended Validation (EV) - Like OV a company search is performed; however, the physical location is also checked and the contact who requested the certificate is also validated.

6. RESULT

A recent study brings into being that American spent 15 hours/week in a car. Each certificate is used for ten-minute period and not at all reused. CRLs are updated regularly every 5-14 days. The attack unbolt until the subsequently update of CRL, it can create a large amount of users and client must search through the revocation list. Then 4660 certificates are consumed each year. So, a vehicle will require around 5K certificates per year. And for every five years we need to store 25k certificates.

Assuming certificate identifiers are uniformly and independently distributed among vehicles, the expected number of certificates triggering false positives per vehicle is given by:

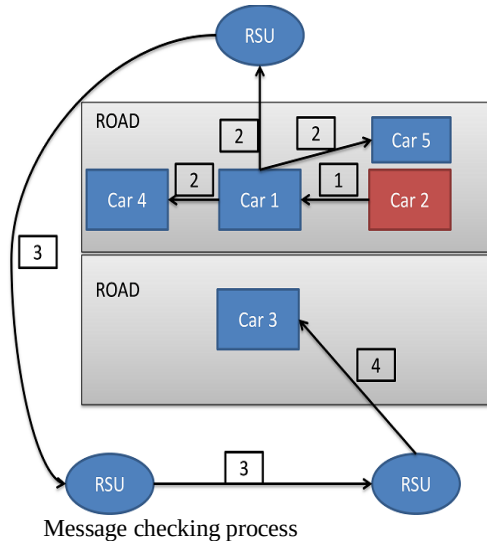
$$E[P_{fp}] = P_{fp}(1 + p)c = pc$$

Where:

p are the Fraction additional certificates to load;

P_{fp} is the Probability of a false positive; and

pc is the number of additional certificates to be loaded on each vehicle;



Certificate revocation occurs when a problematic certificate is developed. It revokes the certificate which avoiding other vehicles getting the message from these problematic certificates. Road Side Unit (RSU) is accountable for track the vehicle and cancelation of the certificates by communications CRL. How to recognize the ordinary certificate and problematic certificate?

In the new revocation method, when any vehicle receives a message from another vehicle, it will ensure that the sender's certificate validity. If the sender doesn't contain a valid certificate (VC), then the message will be mistreated. If the sender doesn't have a certificate, the receivers will testimony the sender to RSU. Then RSU will check the suitability of the message. If that message is correct, RSU will allocate a VC to the sender. Else, they will give an invalid certificate (IC) to the node, and record the vehicle's id to the CRL [15].

In above diagram, 1 shows vehicle-1 notice vehicle-2 has an IC by acceptance a packet from vehicle. 2. Specify that vehicle-1 then transmit a caution to the nearest vehicle as well as the nearby RSU. Procedure 3 shows RSU then educated other RSUs. 4 illustrate the process that other RSUs then transmit the warning to the vehicle that is within its scope. Then the vehicles which containing IC get record the vehicle to CRL. The course of action of revocation is as follows: When a receiver receives a message from an untrusted vehicle, the receiver then sends a message to RSU to obtain Session Key (SK). RSU then replies to the receiver the sender whether has a VC. BMW, Ford, Audi, Nissan like some other companies are playing a major role in VANET research.

The reliance authority generates and pre-processes the system parameters for all RSUs and vehicles. RSU or vehicle checks the received messages in the message verification phase to ensure that the corresponding vehicles are not trying to disseminate false messages, RSU or vehicle checks the signatures of messages. On the other hand, a large number of messages may congest in an RSU at the same period in some situations the batch verification has been introduced in order

to lessen the bottle neck trouble. To improve the signature verification speed, many signatures can be verified at the same time and can be used to achieve better scalability

7. CONCLUSION

It is clear from the above discussion that the security and privacy challenges in vehicular web are huge. The vehicular internet will make the upcoming vehicular technology more secure and reliable. We have a contribution in this paper we discussed a certificates organization technique where certificates for a unique vehicle relate to a single, secret revocation key, existing methodologies and network architecture has been discussed. Without this key, certificates are difficult to gathering, along these lines safeguarding the privacy of a vehicle. Security and privacy is the major challenges in development of VANETs. The risks associated with adoption of technologies connected with VANETs will be evaluated against the benefits they provide. In any case, a revoked vehicle's certificates can be effectively identified once the revocation key is appropriated by means of a CRL. The risks associated with adoption of technologies connected with VANETs will be evaluated against the benefits they provide. It improves the safety of vehicles. Supports Intelligent Transportation System and it improve advanced traffic information, crash warning and restricted threat warning. The autonomous car is a reality today and there is no doubt that it will become common place in the years to come.

REFERENCES

1. P. B. et al., "The Arbitron national in-car study," tech. rep., December 2003.
2. Hartenstein, H.; Laberteaux, K.P. A Tutorial Survey on Vehicular Ad hoc Networks. IEEE Commune. Mag. 2008, 46, 164–171.
3. Haas, J.J.; Hu, Y.-C.; Design and analysis of a lightweight certificate revocation mechanism for VANET. In Proceedings of VANET; ACM: New York, NY, USA, 2009.
4. Benin, J.; Owen, H. Unified pseudonym distribution in VANETs. In Proceedings of the 2010 IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications (Wi Mob), Niagara Falls, ON, USA, 11–13 October 2010 529–533.
5. Abumansoor, O.; Towards a Secure Trust Model for Vehicular Ad Hoc Networks Services. In Proceedings of the 2011 IEEE Global Telecommunications Conference (GLOBECOM 2011), Houston, TX, USA, 5–9 December 2011.
6. Zhang, J. A Survey on Trust Management for VANETs. In Proceedings of the 2011 IEEE International Conference on Advanced Information Networking and Applications (AINA), Bio polis, Singapore, 22–25 March 2011.

7. Faezipour, M.; Nourani, M.; Saeed, A.; Addepalli, S. Progress and Challenges in Intelligent Vehicle Area Networks. Commune ACM 2012.
8. Samara12] Ghassan Samara, Wafaa A.H. Ali Alsalihi, "A New Security Mechanism for Vehicular Communication Networks", International Conference on Cyber Security, Cyber Warfare and Digital Forensic, 2012,.
9. General Motors. Available online: <https://developer.gm.com/>(accessed on 10 June 2015).
10. Baguena, M.; Tornell, S.; Torres, A.; Calafate, C.; Cano, J.-C.; Manzoni, P. Vacamobil: Vanet car mobility manager for omnet++. In Proceedings of the 2013 IEEE International Conference on Communications Workshops (ICC), Budapest, Hungary, 9–13 June 2013.
11. General Motors. Available online: http://media.gm.com/media/us/en/gm/news.detail.html/content/Pages/news/us/en/2013/Feb/0225_4g-Ite.html (accessed on 10 June 2015).
12. IEEE Intelligent Transportation System Society. Available online: <http://its.ieee.org/2014/09/15/you-wont-need-a-drivers-license-by-2040/>(accessed on 09 June 2015).
13. Ford. Available online: <http://developer.ford.com/>(accessed on 09 June 2015).
14. The Telegraph Available online: <http://tinyurl.com/telegraph-co-uk-finance-budget> (accessed on 10 June 2015).
15. The Telegraph Available online: <http://tinyurl.com/telegraph-co-uk-finance-budget> (accessed on 10 June 2015)