Review of Security in VANET

Poornima Byahatti
PG Student, Computer Science and Engineering
Basaveshwar Engineering College
Bagalkot, India

Dr. S. V.Saboji
Professor, Computer Science and Engineering
Basaveshwar Engineering College
Bagalkot, India

Abstract: **Now a day, Vehicular Ad-hoc Networks (VANET) are becoming more widespread as the accident statistics increase. VANET simply provides numerous safety applications to save folks lives while driving on road, it also eliminates accidents and damage to the vehicles and people. VANET is regarded as MANET which is a subgroup of Mobile Ad-hoc Networks. Vehicles moving at different speeds are treated as the nodes. The main intension of VANET is to enable communication between vehicle to vehicle and in between vehicle to infrastructure. Transportation system's security, safety and efficiency are improved by using Intelligent Transportation Systems (ITS).**

As VANET is becoming more popular, a severe issue in this situation is security. Security of VANET is of great significance reason for this is disastrous accidents are caused by any vulnerability in VANET where accidents result in the loss of live and also loss of integrity of people. There is assurance about the protection of personal data moved through VANET but not to location, identity, and destination, among others due to security schemes and mechanisms.

The challenges of security must be included during the design of VANET architecture, cryptographic algorithm, security protocols etc. security issues such as real time constraint Data Consistency Liability, High Mobility, Low tolerance for error, Key Distribution, Incentives. To successfully deploy VANET, security is one of the major issues such as protection from self-centered vehicles that may block or jumble traffic, false notifications etc. That may harm and losses lives, which must be addressed. There are various types of attacks like DOS, sybli attack, reply, man in middle attack etc. Various solutions for these attacks are available such as SRAN (secure routing for ad-hoc network) routing protocol based on AODV (ad-hoc on demand distance vector) protocol, General Active Position Detectors, Digital Certificate, etc Providing security in VANET is a challenging issue.

Keywords: VANET Security, ITSs, SRAN, DSRC, BS, Sybli attack, DOS attack, User Privacy, Authentication, RSU, OBU, TA, ECC, X.509, TPM, MANET.

I. INTRODUCTION

The capable advanced approach to present safety applications to the passengers as well as drivers is the Vehicular Adhoc Network. Now days, VANET becomes more popular in various nations. It is an important aspect of the Intelligent Transportation Systems (ITSs). In a VANET, an On-Board Unit (OBU) is assumed to be fitted on each vehicle and Road-Side Units (RSUs) are installed along the roads. Some application servers and Trusted Authority (TA) are installed in the back end. The Dedicated Short Range Communications (DSRC) protocol over the wireless channel is used for the communication between OBUs and RSUs. The communication between RSUs, TA and application servers are by using a safe fixed network (e.g., the Internet).

VANET permit arbitrary vehicles to broadcast safety messages such as turning direction, vehicle speed, traffic accident information etc to other close vehicles on usual basis so that traveling routes may be regulated by the other vehicles. The traffic control center may be informed to regulate traffic lights for avoiding traffic congestion by the RSUs. A vehicular ad hoc network uses cars as mobile nodes in a MANET to build a mobile network.

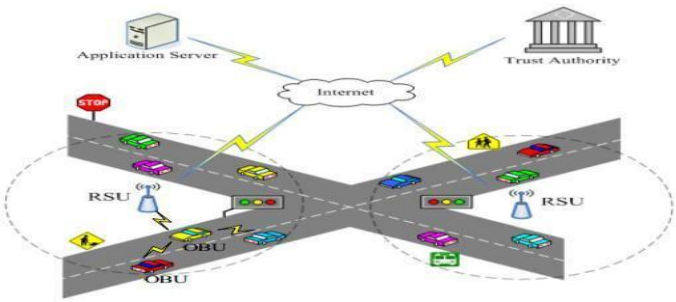

Fig : Architecture of VANET

By means of these units VANET communicates with one another but, VANET adapts different types of communication patterns. By using those patterns VANET decides how VANET packets flow from one unit to another. Types of communication patterns are of the following.

1) Roadside-to-Vehicle Communications (RVC or V2I) 2) Inter-Vehicle Communications (IVC or V2V) 3) Inter road side communication

A. VANET's security

As VANET is becoming more well-liked, a major challenge in this situation is security. VANET is sub branch of MANET. Therefore, VANET takes over all the security challenges associated with MANET. The malevolent actions of users, like alteration of the messages, could be critical to the

other vehicular users, etc. Security and privacy in VANETs are vital for their authorization. Developers are provided an atmosphere for the use of a wide variety of applications by VANET's architectures and communication schemes. Though, chief concerns of such environments are privacy and security. In order to protect both applications and users from feasible attacks, strong security mechanisms are essential. Therefore, powerful schemes are required to protect user's confidential information.

Any susceptibility could lead to disastrous accidents so VANET's security is of great importance. Assurance about the protection of personal data transmitted through VANET is provided by security mechanisms and schemes. In VANET, multiple threats or attacks are possible.

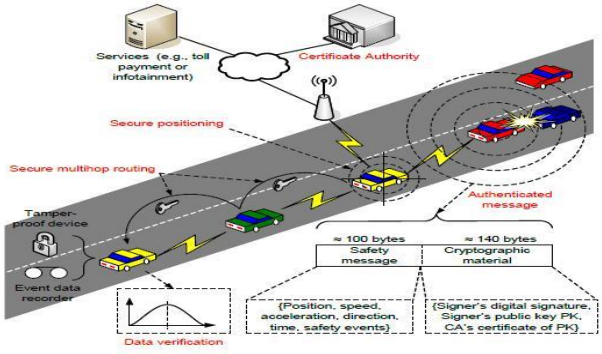

Fig 2: General security architecture [10]

II. VANET SECURITY ISSUES

Along with all the issues of the VANET, security got a lesser amount of consideration so far. Life critical information is contained by VANET packets, as a result it is fundamental to make certain that these packets are not changed by the attacker, likewise the legal responsibility of drivers should also be established that they report to the traffic environment properly within time. These security problems do not analogous to general communication network. The range of network, mobility, geographic relevancy etc could lead to difficulty of the implementation and it is different from other network safety.

The issues of security must be considered during the design of architecture, security protocols, cryptographic algorithm etc. some challenges of security are listed below:

- *Real time Constraint:* VANET is time significant where security associated message should be delivered with 100ms transmission delay. So to achieve actual time constraint, fast cryptographic algorithm should be used. Message and entity authentication must be completed in time.
- *Data Consistency Liability:* In VANET, malicious actions can be performed by authenticated node. Accidents or disturbance of the network can be caused by these malevolent activities. Hence, in order to avoid this inconsistency a technique should be designed. Association with the received data from different node on specific information may avoid this type of deviation.
- *Low tolerance for error:* On the basis of possibility some protocols are considered. Life critical information is used by VANET, on the basis of which action is performed in very short time. Damage to VANET may be caused by a small fault in probabilistic algorithm.
- *Distribution of key:* All the security methods implemented in VANET reliant on keys. Encryption of message is done at sender using key and there is need to decrypt at receiver end either with similar key or different key. Keys can be installed in different ways and in public key infrastructure trust on Certificate Authority (CA) by different manufacturers, this become severe challenge. Therefore key distribution among vehicles is a main issue during the security protocol's designing.
- *Incentives*: Manufactures are interested to construct applications that consumer likes the most. Any traffic rule violation is automatically reported by vehicle and this will be agreed by few consumers. Hence successful use of VANET will need incentives for vehicle consumers, manufacturers and the government and this is a challenging issue to implement security in VANET.
- *High Mobility*: The supply of energy and computational capacity in VANET is similar as that of wired network node but the high mobility of VANET nodes needs the less execution time of security protocols for similar throughput than that of wired network. Hence the some approaches are used to reduce the execution time by design of security protocol.

A. Security requirements

VANET must satisfy a number of security requirements before they are used. Requirements of a VANET security system are of the following [9]:

- *Authentication:* Legitimate user generates message that is ensured by Authentication. In VANET a vehicle reacts upon the data received from the other vehicle hence authentication must be satisfied.
- *Availability:* Availability requires that the data must be obtainable to the legitimate users. Denial of Service Attacks can bring down the network and hence information cannot be shared.
- *Non-Repudiation:* Non-repudiation means a node cannot deny that he/she does not broadcast the message. It may be crucial to decide the right sequence in crash renovation.
- *Privacy:* The privacy of a node in opposition to the unauthorized node should be guaranteed. This is necessary to remove the message delay attacks.
- *Data Verification:* In order to remove the false messaging, the regular verification of data is required.

III. SOLUTIONS TO VANET SECURITY

In [1], author proposed security and authentication process using ECC (Elliptic Curve Cryptography) in VANET, real time road information from VANET is collected by a system, this leads the drivers to reach at desired destinations in a real-time and distributed manner. The system has the benefit of using real-time road situation which is used to compute a better route at the same time. The information source can be properly authenticated**.** In this system the use of Elliptic Curve algorithm is to authenticate source and also decreases the network overhead and delay. It takes use of the online road information collected by a VANET to direct the drivers to desired destinations in a real-time and distributed manner with Privacy-Preserving Navigation. Hence a system is proposed to solve single server problem by introducing replica server. Whenever primary server stops working:

- Every vehicle's and RSU's information is stored in backup/replica server.
- Whenever main server is not able to function then, every vehicle starts to communicate with Secondary server. All the process starts with step 1 by secondary server.
- All the newly generated certificates are stored in secondary server.
- All authentication and key sharing is done only by secondary server.

ECC was invented in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington) as different mechanism for implementing public-key cryptography. This model also uses ECC algorithm.

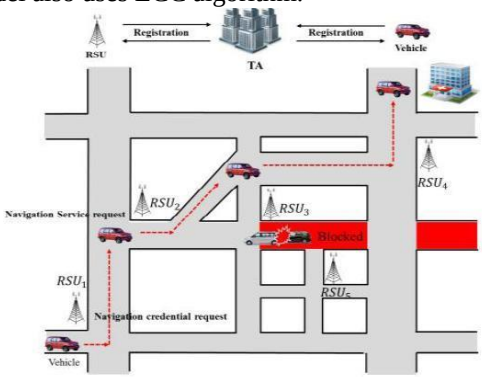

Fig 4: Security System architecture

It consists of a Trusted Authority (TA), RSUs, a Tracing Manager (TM), and vehicles.

- TA- Issuing of digital certificates for RSUs and vehicles is the liability of the TA. Also it holds a Certificate Revocation List (CRL) containing the certificates of revoked vehicles. The TA is assumed to be completely powerful, rigid to cooperate, and trustable, i.e. with sufficient calculation and storage capability.
- TM- When the content of a safety message broadcast by a vehicle is found to be fake, real identity of the vehicle should be determined by the ability of it.
- RSU- In this protocol road side must have an environment in which RSUs are densely distributed, RSUs are utilized to issue secret member keys to vehicles and aid the TM to proficiently track the real identity of a vehicle from any safety message. OBUs are assumed to be fitted in each vehicle. By using OBUs, vehicles can interact with each other as well as with the RSUs. The interaction among them is depending on the DSRC protocol.

In [2], authors achieved Security and Data Privacy for VANET using X.509 Certificates, public key certificate or public key cryptography is regarding a set of techniques that combine together in a particular system to allow secure interaction. This work aims to promote the use of x.509 certificate due to its capability to reduce security risks. Public Key Infrastructure (PKI) is an infrastructure that can be used to support digital signing and encryption for electronic transaction. The aim of PKI is to support security using X.509 certificate. In this paper X.509 v3 certificate is evaluated. X.509v3 added certificate extensions to augment X.509v1/v2 Certificates.

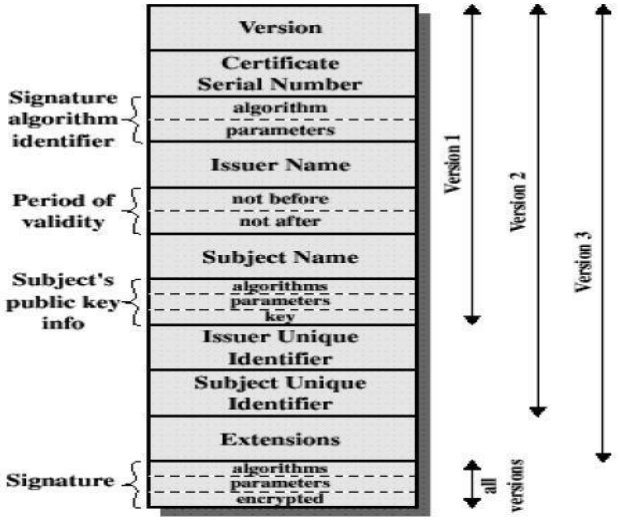

Fig 5: X.509 Certificate

In order to include extra data Version 3 launches a mechanism whereby certificates can be extended, in a standardized and generic style. The term standard extensions refer to the fact that the some broadly-applicable extensions to the version 2 certificate are defined by version 3 X.509 standard. However, certificates are not constrained to only the standard extensions and an extension with the appropriate authorities (e.g., ISO) can be registered by anyone. Each extension consists of three fields: criticality, value and type. The extension criticality field is a single-bit flag. When an extension is flagged as critical, it indicates that the attached extension value contains data of such significance that an application cannot disregard the data. If critical extension cannot be processed by a particular certificate-using application, the application should discard the certificate. The

extension type field defines the type of the data in the extension value field. The type could, for example represent a numerical value, a graphic, a simple text string, a date, or a complex data structure. To promote interoperability, all extension types should be registered with an internationally-recognized standards association.

In [3], authors proposed Security Protocol for VANET by Using Digital Certification to give security with low bandwidth, in this paper an algorithm have been proposed by authors in order to beat network attacks via low message passing and try to decrease the bandwidth at the time of authentication, message passing.

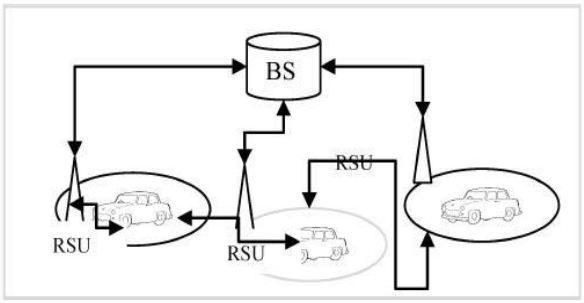

Fig 6: Global scenario of VANET

They basically split their proposed protocol into three phases- first Initial Phase (Base station to Road Side Units), second phase (Road Side Unit to car) and third phase (Car to Car communication). In first phase BS and RSU interact with each other and proof their own identity via group Identification number. In the Second phase the mutual authentication performed in between RSU and the Car where we basically use the concept of certification, public key cryptography concept. Lastly the authentication held at the time of car to car communication.

In [4], authors proposed General Active Position Detectors Protect VANET; there are significant amount of VANET applications that are location based such as navigation and weather forecast. Positions of vehicles in VANET are regarded as sensitive data exposed to attackers for violent actions. Malicious users can also fake their true locations for misbehaving. Typical position based attacks include: dropping packet, replaying packets and inserting bogus packets. A general active detection architecture consisting of two components: ear-devices and eye-devices are proposed by them. Eye devices consist of infrared, radar, camera, etc. Ear-device is the wireless transceiver. A vehicle is identified by infrared detector using its relative near but wide eyesight. A far remote vehicle with a relatively sharp but focus eyesight can be identified by microwave radar. A real image of a vehicle on the fly, and even a live stream of traffic can be identified by a vehicular camera. They attain local security by enlisting the help of several on-board eye devices to notice neighboring vehicles and to confirm their announced position coordinates heard by ear-device. They apply cosine similarity to these data to reach an agreed-location.

Detecting false position information and decreasing the chances of attacks are the keys to success in securing VANETs. This paper focuses on this prime area. The eye devices act as the virtual “eye” of the system and verify the data heard by the ear-devices within its transmission range. The capacity to verify records is also used for achieving global security. This approach is efficient in determining compromised vehicles and decreases the burden on channel availability. This work concerns much accuracy issues. They decrease the measure errors by enlisting multiple eye-devices and process data to decrease large variance by using similarity model

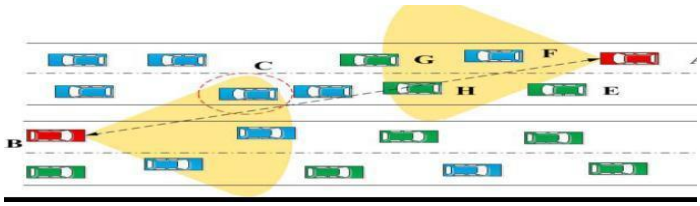

Fig 8: The system scheme. There are three types of position information. The ear devices can obtain position reports from neighboring vehicles. Observer’s eye devices and the eye devices on the oncoming traffic are both used.

In [5], authors proposed VANET Security against Sybil Attack by Using New SRAN Routing Protocol**,** In VANET security is the most important factor for secure interaction. Sybil attack is one of the major threats in the network. Multiple malicious vehicle nodes are injected by sybli attack in the network and that also troubles the networks or causes the loosing of life. Authors proposing new secure routing protocol named as Secure Routing for Ad hoc Network (SRAN) routing protocol. This SRAN protocol detects as well as prevents Sybil attack. SRAN is based on AODV. Sybil node is not allowed into Route discovery by SRAN protocol hence Sybil node is eliminated from the route. This Sybil node from the Network is eliminated by using RSU.

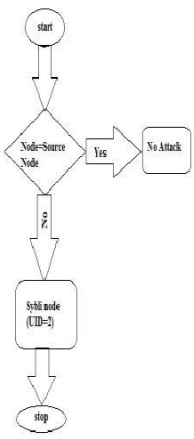

Fig 9: Flow of Sybil attack alg

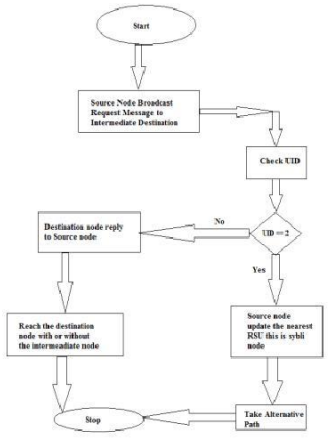

Fig 10: Execution of SRAN Protocol

In [6], author proposed Solution for Denial of Service Attack in VANET, in this attack the attacker attacks the interaction medium to cause the channel jam or to create some troubles for the nodes from accessing the network. The main goal of the attacker is to prevent authentic nodes from using the network services. Either vehicular nodes or network infrastructure may be attacked by attacker. Levels of DOS Attacks are: logic attack, Bandwidth attack and protocol attack.

The proposed model provides solution against DOS attack. The model is lying on the use of On-Board-Unit that is fitted on each vehicle node, to make decision as to prevent a DOS attack. In the case of DOS attack, OBU will be suggested to switch technology, channel or to use frequency hopping technique by the processing unit. To make decision depend on the received attack message four options are available for On-Board-Unit. After necessary opinion and processing, the information is sent to next On-Board-Unit in the network.

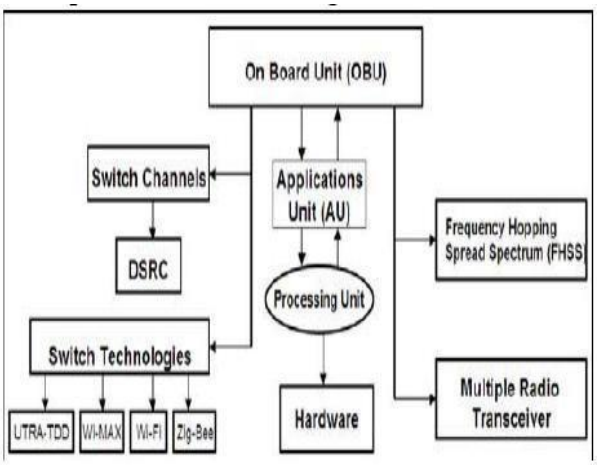

Fig 11: Model of solution to DOS attacks

In [7], author proposed security framework in VANET for trusted grouping utilizing TPM hardware, the default test asymmetric PKI/ECDSA security mechanism is well-known for its high computational cost, thus missing applicability in life-critical safety messaging. Alternative Security schemes, like symmetric methods provide faster interaction at the cost of reduced security. Hence, to ease the issue researchers proposed hybrid and hardware based solutions. However, these solutions either do not support the existing VANET PKI standard or have larger message size. In this paper, hardware based security framework is presented by authors that uses both standard asymmetric PKI and symmetric cryptography for faster and secure safety message swapping. The proposed framework is expected to improve security method in VANET by rising trust relationship among the neighboring nodes, hence forming trusted groups. The trust is established via TPM and group communication.

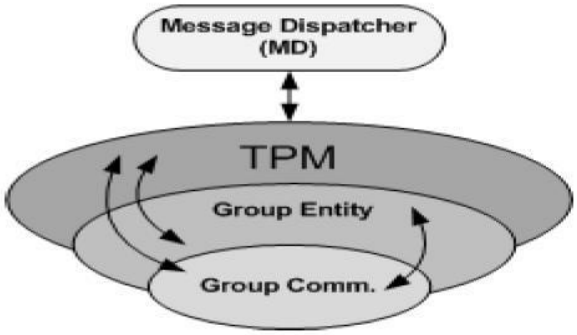

Fig 11: Security framework for VANET

Based on the requirement to provide hybrid cryptography scheme, they proposed a VANET security framework with support of TPM chip. The framework consists of three basic components: hardware entity (TPM chip), Group Communication and Group entity. To achieve trusted safety messaging in VANET, all the components are functioning collectively with each other as illustrated in Fig 11 to create a trusted group. Importantly, the proposed framework is planned to achieve trusted group communication among the vehicle nodes within a group

In [8], author proposed an identity based VANET security system that can efficiently resolve the disputes between privacy and tractability. In order to protect user privacy, pseudonym based scheme is utilized by system. In order to allow tractability for law enforcements a threshold signature based scheme is engaged by it. The essential part of the system is the privacy preserving defense scheme that leverages the authentication threshold. Any additional authentication beyond the threshold will point out misbehavior and result revocation of the user's credentials. A dynamic accumulator for the authentication thresholding is employed by scheme and this result in further restrictions beyond the threshold on other interacting users. This is particularly nice-looking to service providers since they can attain better efficiency of their services. Figure 12 depict interactions in the ID base system.

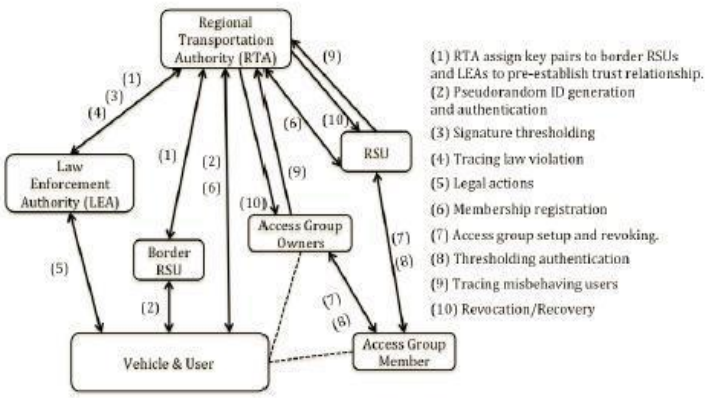

Fig 12: Interactions of the ID based Security System

TABLE I. TABLE OF COMPARISION OF SOLUTIONS

Authors and years	Description of various problems and solution		
	Problem addresses	***Proposed solution mechanism***	***Our Review***
Rukaiya Shaikh, Disha Deotale. [1] (2015)	Security and Authentication process in VANET	Elliptical Curve Cryptographic algorithm(ECC)	Message is generated by legitimate user.
Sowmyashree H, Sharmila K.P. [2] (2015)	Security and Data Privacy for VANET	Public key certificate such as X.509	Ensuring location privacy.
Neeraj Varshney, Tumpa Roy, et al. [3] (2014)	Security Protocol for VANET	Digital Certification to provide Security with Low Bandwidth	It gives secured interaction with better performance. It is cost-effective, consuming sufficient bandwidth.
Gongjun Yan, et al. [4] (2011)	VANET Security	General Active Position Detectors (eye-device and ear-device)	identifying false location data and decreasing the Chances of attacks.
Omkar Shete, et al. [5] (2015)	Security aginst Sybli attack	Secure Routing for Ad Hoc Network protocol(SRAN)	SRAN differentiates between fake node and original node. Sybil attack is identified and prevented by SRAN. So leads to high performance.
Tejaswini Daf and Prof Avinash Jadhao. [6] (2015)	Denial of Service Attack in VANET	Each vehicle node contain on-board-unit, and it depends on on-board-unit to make decision about the detection of a DOS attack.	DOS attacks and network transmissions are effectively handled by it.
Asif Ali Wagan, et al. [7] (2010)	VANET Security Framework for Trusted Grouping	The hybrid method employs Trusted Platform Module (TPM).	Trusted group interaction along with the vehicle nodes within a group.
Jinyuan Sun, et al. [8] (2010)	An identity based security system for VANET	privacy preserving defense scheme	Conflicts between privacy and tractability are efficiently solved by it

CONCLUSION

VANET is emerging technology for vehicle to vehicle communication. VANET efficiency is increased by intelligent transport system (ITS). General Adhoc network security concerns are shared by it. Attacks such as eavesdropping, traffic analysis, Dos, Reply attack, etc are exposed in VANET. New security challenges such as illegal tracking, position detection and jamming are raised by the distinct character of VANET. General cryptographic approaches that relate in VANET specifies the certificate schemes for authentication and randomizing traffic patterns in opposition to traffic analysis, public key schemes to distribute one time symmetric session keys for message encryption. In this paper solutions on specific security issues and solution to various attacks are also addressed. This paper gives a broad analysis for the current challenges and solutions. In our future work we will propose new solutions that will help to manage a securer VANET network, and test it by simulation.

REFERENCES

[1] Rukaiya Shaikh, Disha Deotale, “Security and Authentication Process using ECC in VANET”, Volume 3, Issue 5, May 2015 International Journal of Advance Research in Computer Science and Management Studies Research Article / Survey Paper / Case Study.

[2] Sowmyashree H, Sharmila K.P, “Achieving Security and Data Privacy for VANET Using X.509 Certificates”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 5, May 2015

[3] Neeraj Varshney, Tumpa Roy, Niharika Chaudhary, “Security Protocol for VANET by Using Digital Certification to Provide Security with Low Bandwidth”, International Conference on Communication and Signal Processing, April 3-5, 2014, India.

[4] Gongjun Yan, Bhed Bahadur Bista, Danda B. Rawat, Earl F. Shaner, “General Active Position Detectors Protect VANET Security” 2011 International Conference on Broadband and Wireless Computing, Communication and Applications.

[5] Omkar Shete, Sachin Godse, “VANET Security against Sybil Attack by Using New SRAN Routing Protocol” International Journal of Computer Applications Technology and Research Volume 4– Issue 7, 535 - 539, 2015, ISSN:- 2319–8656

[6] Tejaswini Daf and Prof Avinash Jadhao, “Solution for Denial of Service Attack in VANET”, International journal for research in emerging science and technology.

[7] Asif Ali Wagan, Bilal Munir Mughal & Halabi Hasbullah, “VANET Security Framework for Trusted Grouping using TPM Hardware” 2010 Second International Conference on Communication Software and Networks.

[8] Jinyuan Sun, Chi Zhang, Yanchao Zhang, Yuguang Fang, "An IdentityBased Security System for User Privacy in Vehicular Ad Hoc Networks," Parallel and Distributed Systems, IEEE Transactions on, vol.21, no.9, pp.1227,1239, Sept. 2010. doi: 10.1109/TPDS.2010.14

[9] Maxim Raya e al., “The Security of Vehicular Ad Hoc Networks”, SASN’05, Nov 7 2005, Alexandria, Verginia, USA, pp. 11-21

[10] Kenneth P. Laberteaux, J.J. Haas, and Y.C.Hu, -Security Certificate revocation list distribution for VANET‖. In VANET '08 Proceedings of the fifth ACM international workshop on Vehicular Inter-NETworking