Abstract -- Since the last few years VANET have received increased attention as the potential technology to enhance active and preventive safety on the road, as well as travel comfort. Security and privacy are indispensable in vehicular communications for successful acceptance and deployment of such a technology. Generally, attacks cause difference to the network functionality [14]. A safe VANET system, while exchanging information should protect the system against illicit message injection, message modification, eavesdropping. This paper is an attempt to highlights the problems occurred in Vehicle Ad hoc Networks and security issues. The security of VANETs is one of the most critical issues because transmission of information is propagated in open access (wireless) environments.[13] It is necessary that all transmitted data should not be injected or changed by unauthorized users who have malicious goals. So the aim of the paper is to highlight the problems occurred in Vehicle Ad hoc Networks and different security issues.

Keywords: Vanet, security, false message, Dual signature, location tracing, Identity Hazard.

I. INTRODUCTION

A Vehicular Ad-Hoc Networks or VANET is a technology that uses particular nature of wireless ad-hoc networks, formed with short range of wireless communication network, each one to express a vehicle on the road or a static appliance. Vehicular Ad-Hoc Networks (VANETs) provide rapidly deployable, self-configurable network connectivity. The network is made of vehicles interconnected by wireless links and willing to store and forward data for their peers. As vehicles move freely and organize themselves arbitrarily, message routing is done dynamically based on network connectivity.[11] Compared with other ad-hoc networks, VANETs are particularly challenging due in part to the vehicles’ high rate of mobility and the numerous signal-

II. SECURITY ASPECTS RELATED TO VANET:

A. ATTACKS ON PRIVACY:
Attacks on privacy over Vanet are mainly related to illegitimately getting the confidential information about vehicle. Since vehicle is directly related to its driver so any threat [10] in the confidential information of a vehicle may result threat in the privacy of driver.

B. IDENTITY HEZARD:
Getting the drivers identity of a given vehicle could put its privacy at risk. The intruder uses this sensitive information.

C. LOCATION TRACING:
The position of the vehicle in a given instant or the way followed by that vehicle are considered as personal data of the vehicle. The intruder can use this sensitive information in tracing the position of the vehicle and route. So it can perform any illegal action.
D. MESSAGE AUTHENTICATION:

In Vanet the messages are frequently exchanged in between V2V, V2I & I2I. There is a situation when there is no trust in between them. Vehicle, infrastructure etc. means one can deny that he/she is a sender of a given message.[3] In Vanet basically there are three types of possible communication. Vehicle to Vehicle, Vehicle to infra and infra to infra. In a life critical situation like an accident a particular vehicle can communicate with other vehicle and infra to inform them that there is an accident occurred in a particular way or path. The problems with this type (V2V) communication are following:

- There may be an attacker who can send false alert messages to other car or Infra.
- Integrity of the message
- Latency of message (large amount of time taken in a message communication)
- There may be a condition of privacy attack (driver’s path, confidential information etc.)

III. SOLUTION:

Let there is a car A which wants to send a message in an accidental condition [8]. The steps are:

A. It will create the dual signature by using SHA-1 [2] (for hashing). Since SHA-1 is irreversible so no one can retrieve the messages in reverse processing and then encrypt the message with private key of A.

B. After creation of dual signature the four “Accidental message + Message digest of Driver’s privacy (DPMD) + Dual Signature + Pub key certificate of A” is again encrypted with AES-128 bit keys. Result is an encrypted message.

C. AES-128 keys are encrypted with Public key of B [7] (Receiver’s Car). The result is key envelop.

D. At B’s side B got the [9] AES-128 bit keys by decrypting the key envelop with the help of its private key. Then again decrypt the encrypted message with AES-128 bit keys and got the four “Accidental message + Message digest of Driver’s privacy (DPMD) + Dual Signature + Pub key certificate of A”. Then it will again hash the
accidental message and perform a combined hash with DPMD the result is DPAMD.
E. Dual signature is decrypted with Public key certificate of A and the result is DPAMD.
F. Compare both DPAMD.

- If they match means there is no alteration of message. Integrity of message is achieved.[1]
- There is no leakage of driver’s private information because we are using [5] [6] SHA-1 which is irreversible.
- Since the messages are using public key and private key [4] for sign so there is no such fake attack because these keys are assigned by a trusted certification authority.
- All operations are performed on “On Board Units” (OBU). So there is no latency.

IV. CONCLUSION:
The security of VANETs is one of the most critical issues. This approach will be safe and time efficient. We can achieve unaltered messages means integrity of the message is achieved. The privacy of the driver is achieved by using SHA-1. So there is no privacy risk. Since the messages are using public key and private key for sign so there is no such fake attack because these keys are assigned by a trusted certification authority. All operations are performed on “On Board Units” (OBU). So there is no latency.

REFERENCE:
[6] RFC 3174 Secure Hash Algorithm-1
[8] Lawrence C. Paulson Computer Laboratory, University of Cambridge
“Verifying the SET Protocol: Overview”