# Analysis of Security Attack on VANET

Priti R. Londhe
Student
S.E.C. Washim

## ABSTRACT
Vehicular Ad Hoc Networks(VANET) has basically picked up the consideration of today's examination endeavors ,while ebb and flow answers for accomplish secure VANET, to shield the system from foe assaults still insufficient ,attempting to achieve an acceptable level, for the driver and maker to accomplish wellbeing of life and infotainment. The requirement for a vigorous VANET systems is unequivocally reliant on their security and protection highlight s, which will be circle utilized as a part of this paper .In this paper a different kind of security issues and difficulties of VANET been examined and talked about; more additionally talk about an arrangement of arrangements present to explain these.

## Keywords
Vanet,IVC,RVC,FCC

## 1. INTRODUCTION
Later year's quick advancement in remote correspondence systems has made Inter-Vehicular Communications (IVC)and Road-Vehicle Communications(RVC) conceivable in Mobile Ad Hoc Networks (MANETs),this has brought forth another kind of MANET known as he Vehicular Ad Hoc Network (VANET), pointing o empower street security, productive driving, and infotainment. The world today is carrying on a battle, and the front line lies on the streets, the evaluated number of passing speaks the truth 1.2million people yearly overall [15], and harms around forty times of this number, without overlooking that movement blockage that makes an immense exercise in futility and fuel [1].Vehicular Ad hoc Networks (VANET) is a piece of Mobile Ad Hoc Networks (MANET), this implies that each hub can move openly inside of the system scope and stay associated, every hub can speak with different hubs in single bounce or multi jump, and any hub could be Vehicle, Road Side Unit (RSU).

In the year 1998, the group of architects from Delphi Delco Electronics System and IBM Corporation proposed a system vehicle idea went for giving an extensive variety of utilizations [14]. With the progressions in remote correspondences innovation, the idea of system auto has pulled in the consideration everywhere throughout the world.As of late, numerous new activities have been propelled, focusing on understanding the fantasy of systems administration auto and effective execution of vehicular systems. The undertaking Network On Wheels (NOW) [3] is a German examination task established by DaimlerChrysler AG, BMW AG, Volkswagen AG, Fraunhofer Institute for Open Communication Systems,

NEC Deutschland GmbH and Siemens AG in 2004, The venture receives an IEEE 802.11 standard for remote get to, The primary destinations of this task are to illuminate specialized issues identified with correspondence conventions and information security for auto to-auto interchanges. The Car2Car Communication Consortium [16] is started by six European auto makers. Its will likely make an European mechanical standard for auto to-auto interchanges reach out over all brands. FleetNet [16] was another European program which kept running from 2000 to 2003 this specially appointed exploration was commanded by endeavors to institutionalize MANET conventions, and this MANET examination concentrated on the system layer[2], a definitive test was to tackle the issue of how to achieve hubs not specifically inside of radio extent by utilizing neighbors as forwarders, while the European Commission is pushing for another exploration exertion here keeping in mind the end goal to achieve the objective of decreasing the auto crashes of half by 2010, meaning to achieve a tasteful level of secure VANET.

The radio utilized for the correspondence is Dedicated Short mmunications (DSRC), which been assigned as new band in 1999 by the Federal Communications Commission (FCC)[3], the band dispensed was 75 MHz at 5.9 GHz recurrence for Intelligent Transport System (ITS) applications in north America.VANET security ought to fulfill four objectives, it ought to guarantee that the data got is right (data legitimacy), the source is who he claims to be (message trustworthiness and source confirmation), the hub sending the message can't be distinguished and followed (protection) and the framework is powerful.

## 2. RELATED WORK
The radio utilized for the correspondence is Dedicated Shortmmunications (DSRC), which been assigned as new band in 1999 by the Federal Communications Commission (FCC)[3], the band dispensed was 75 MHz at 5.9 GHz recurrence for Intelligent Transport System (ITS) applications in north America.VANET security ought to fulfill four objectives, it ought to guarantee that the data got is right (data legitimacy), the source is who he claims to be (message trustworthiness and source confirmation), the hub sending the message can't be distinguished and followed (protection) and the framework is powerful.The main security areas that they focused on include anonymity, key management, privacy, reputation, and location. Anonymityis a critical issue in VANETs concerning the physical identity of mobile nodes (i.e., vehicles) that should be kept secret in unauthorized components' point of view. Key managementdeals with problems on generating, distributing, and storing keys. For ad hoc networks, there are three main approaches for key management reported by literature, namely key exchange, key agreement, and key management infrastructure. Privacyrefers to the about them against unauthorized observers. Reputationof a member is usually evaluated by a particular one in answering the question "How much is this member trustable?" in a specific setting or domain of interest. Certainly, trustworthy behavior will be trusted and encouraged by reputation systems. In VANETs, the defense against compromised nodes, and malicious ones can be assured by applying such kinds of systems. Locationrefers to vehicle position in VANETs that can be considered as one of the most valuable pieces of information in geographic routing. It is often readily available through positioning services such as global positioning system (GPS).

In 2012, in the paper "Survey on Security Attacks in Vehicular Ad hoc Networks (VANETs)" [3], Mohammed Saeed Al-kahtani identified different security attacks, classified them, compared their defending mechanism in VANETs and suggested some future possibilities in this area. The author categorized three types of attacker as follow

**Insider vs. Outsider**

In 2010, J.T. Isaac, S. Zeadally, and J.S. Camara distributed a paper on "Security assaults and answers for vehicular specially appointed systems" [6]. They talked about a noteworthy's percentage security assaults that have been accounted for on VANETs before and in 2010. They displayed additionally the relating security arrangements that have been proposed to keep those security assaults and vulnerabilities.

**Malicious vs. Rational**

A maliciousattacker uses various methods to damage the membernodes and the network without looking for its personal benefit. On the contrary, a rationalattacker expects its own benefit from the attacks. Thus, these attacks are more predictable and follow some patterns.

**Active vs. Passive**

An activeattacker can create new parcels to harm the system while a passiveattacker just spy the remote channel however can't produce new bundles (i.e., less destructive). Indeed, there is another ascribe to characterizean assailant, which is displayed in [8]:

**Local vs. Extended**

An attacker is considered as local if it is limitedin scope, even if it possesses several entities (e.g., vehicles or base stations). Otherwise, an extended attacker broadens its scope by controlling several entities that are scattered across the network. This distinction is especially important in wormhole attacks that will be describe later. In 2013, Irshad Ahmed Sumra proposed five different classes of attacks [2] and every class is expected to provide better perspectives for the VANETs security (Table 1). This paper attempted to propose a classification and an identification of different attacks in VANETs.

Table 1: Proposed classification of attacks in [2]

- Monitoring Attacks
- Social Attacks
- Timing Attacks
- Application Attacks
- Network Attacks

In five star Network Attacks, aggressors can specifically influence different vehicles and base. These assaults are on the abnormal state of threat in light of the fact that these influence the entire system. Whilst, in Application Attacks class, the goals of assailants are applications that give included administration in VANETs. The assailant is basically inspired by changing substance utilized as a part of utilizations and mishandling it for their own advantages. The second rate class-Timing Attacks-is a kind of assaults in which assailants' fundamental goal is to include some time opening in unique message, for instance, to make delays with a specific end goal to square this message go to the beneficiary before the lapse of its lifetime. All unmoral messages, which trigger terrible feelings of different drivers, are ordered into the class Social Attacks. At last, assaults in which observing and following exercises are performed are laying in the class Monitoring Attacks. The related works above caution a disturbing situationof VANETs security. In the following segments,here expect to underline security prerequisites in VANETs, then present all the more compactly the conceivable assaults, their relating countermeasures and propose another order of thse class.

# 3. VANET SECURITY CONCERNS

VANET suffer from various attacks; these attacks are discussed in the following subsections:

## A. ATTACKS

In this paper concentrating on attacks perpetrated against the message itself rather than the vehicle, as physical security is not in the scope of this paper.

### 1) Denial of Service attack

This assault happens when the aggressor takes control of a vehicle's assets or jams the correspondence channel utilized by the Vehicular Network so it keeps discriminating data from arriving. It additionally builds the peril to the driver, on the off chance that it needs to rely on upon the application's data. Case in point, if a vindictive needs to make an enormous heap up on the interstate, it can make a mischance and utilize the DoS assault to keep the notice from coming to the drawing closer vehicles [1], [5], [6], and [7]. See figure 2. Creators in [1] examined an answer for DoS issue and saying that the current arrangements, for example, jumping don't totally take care of the issue, the utilization of numerous radio handsets, working in disjoint recurrence groups, can be a plausible approach yet even this arrangement will require adding new and more types of gear to the vehicles, and this will require more supports and more space in the vehicle. The creators in [12], proposed an answer by exchanging between diverse channels or even correspondence innovations (e.g., DSRC, UTRA-TDD, or even Bluetooth for short ranges), in the event that they are accessible, when one of them (commonly DSRC) is cut down.

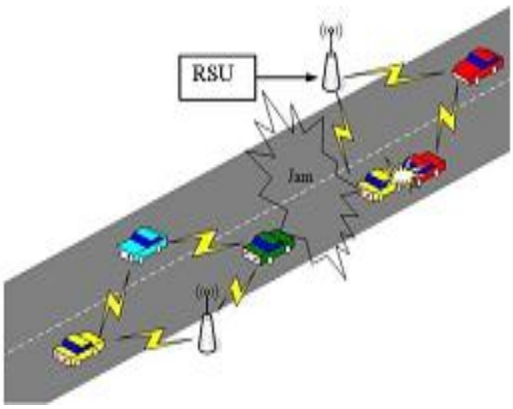


**Fig.1 Dos attack**

### 2) Message Suppression Attack

An aggressor specifically dropping parcels from the system, these bundles may hold basic data for the recipient, the assailant smother these bundles and can utilize them again in other time[5]. The objective of such an assailant would be to keep enlistment and protection powers from finding out about crashes including his vehicle and/or to abstain from conveying impact reports to roadside access focuses [17]. For example, an assailant may stifle a blockage cautioning, and utilize it in

some other time so vehicles won't get the notice and compelled to hold up in the activity.

**3) Fabrication Attack**

An attacker can make this attack by transmitting false information into the network, the information could be alse or the transmitter could claim that it is somebody else. This attack includes fabricate messages, warnings, certificates, identities [5], [7] [17].

**4) Alteration Attack**

This attack happens when attacker alters an existing data, it includes delaying the transmission of the information, replaying earlier transmission, or altering the actual entry of the data transmitted [5]. For instance, an attacker can alter a message telling other vehicles that the current road is clear while the road is congested [17].

**5) Replay Attack,**

This attack happens when an attacker replay the transmission of an earlier information to take advantage of the situation of the message at time of sending [5]

Basic 802.11 security has no protection against replay. It does not contain sequence numbers or timestamps. Because of keys can be reused, it is possible to replay stored messages with the same key without detection to insert bogus messages into the system. Individual packets must be authenticated, not just encrypted. Packets must have timestamps. The goal of such an attack would be to confuse the authorities and possibly prevent identification of vehicles in hit-and-run incidents [17].

**6) Sybil Attack**

This assault happens when an assailant makes substantial number of pseudonymous, and claims or acts like it is more than a hundred vehicles, to tell different vehicles that there is jam ahead, and constrain them to take substitute route[5],[8]. See Figure 3. Sybil attackdepends on how inexpensively characters can be created, the extent to which the framework acknowledges inputs from substances that don't have a chain of trust connecting them to a trusted element, and whether the framework treats all elements indistinguishably. For example an assailant can imagine and act like a hundred vehicle to persuade alternate vehicles in the street that there is congestion,go to another defeat so the street will be clear

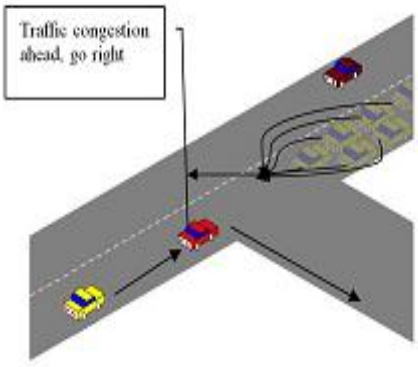


**Fig.2 Sybil attack**

**B. ATTACKERS**

**1) Selfish Driver**

The general idea for trust in Vehicular Network is that all vehicles must be trusted initially, these vehicles are trusted to follow the protocols specified by the application, some drivers try to maximize their profit from the network, regardless the cost for the system by taking advantage of the network resources illegally [5]. 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 for it. See figure 4.

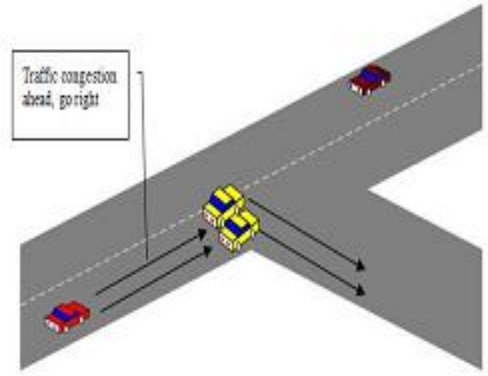


**Fig.3 Selfish driver**

**2) Malicious Attacker,**

This kind of attacker tries to cause damage via the applications available on the vehicular network. In many cases, these attackers will have specific targets, and they will have access to the resources of the network [1], [5].

For instance, a terrorist can issue a deceleration warning, to make the road congested before detonating a bomb.

**3) Pranksters**

Incorporate exhausted individuals examining for vulnerabilities and programmers trying to achieve acclaim by means of their harm [5]. For example, a prankster can persuade one vehicle to back off, and advise the vehicle behind it to expand the rate

## 4. VEHECULAR NETWORKS CHALENGES

**1) Mobility**

The basic idea from Ad Hoc Networks is that each node in the network is mobile, and can move from one place to another within the coverage area, but still the mobility is limited, in Vehicular Ad Hoc Networks nodes moving in high mobility, vehicles make connection throw their way with another vehicles that maybe never faced before, and this connection lasts for only few seconds as each vehicle goes in its direction, and these two vehicles may never meet again. So securing mobility challenge is hard problem.

**2) Volatility**

The availability among hubs can be exceptionally transient, and perhaps won't happen once more, vehicles voyaging toss scope territory and making association with different vehicles, these associations will be lost as every auto has a high portability, and possibly will go in inverse direction[1],[5]. Vehicular systems does not have the moderately long life setting so individual contact of client's gadget to a problem area will require long life secret word and this will be illogical for securing VC.

**3) Privacy VS Authentication**

The importance of authentication in Vehicular Ad Hoc Networks is to prevent Sybil Attack that been discussed earlier [8]. To avoid this problem here can give a specific identity for every vehicle, but this solution will not be

appropriate for the most of the drivers who wish to keep their information protected and private[1],[5].

**4) Privacy VS Liability**
Obligation will give a decent open door for legitimate examination and this information can't be denied (if there should arise an occurrence of accidents)[1], in other hand the security mustn't be damaged and every driver must be able to keep his own data from others (Identity, Driving Path, Account Number for toll Collector and so forth.).

**5) Network Scalability**
The scale of this network in the world approximately exceeding the 750 million nodes [4], and this number is growing, another problem arise when we must know that there is no a global authority govern the standards for this network [1], [5], [7], for example: the standards for DSRC in North America is deferent from the DSRC standards in Europe, the standards for the GM Vehicles is deferent from the BMW one.

**6) Bootstrap**
Right now just few number of autos will be have the gear required for the DSRC radios so if make a correspondence we need to accept that there is a predetermined number of autos that will get the correspondence, later on focus on getting the number higher, to get a budgetary advantage that will strength the business firms to put resources into this innovation [5].

# 5. SECURITY REQUIREMENTS

**1. Authentication**
In Vehicular Communication each message must be validated, to verify for its cause and to control approval level of the vehicles, to do this vehicles will relegate each message with their private key alongside its authentication, at the beneficiary side, the collector will get the message and check for the key and endorsement once this is done, the recipient confirms the message [1], [5]. Marking every message with this, causes an overhead,to lessen this overhead utilize the methodology ECC (Elliptic Curve Cryptography), the proficient open key cryptosystem, or sign the key only for the discriminating messages just.

**2. Availability**
Vehicular system must be accessible constantly, for some applications vehicular systems will require realtime, these applications require quicker reaction from sensor systems or even Ad Hoc Network, a deferral in seconds for a few applications will make the message inane and perhaps the outcome will be devastating[1][5]. Endeavoring to meet ongoing requests makes the framework defenseless against the DoS assault. In a few messages, a postponement in millisecond makes the message pointless; the issue is much greater, where the application layer is inconsistent, since the potential approach to recoup with questionable transmission is to store incomplete messages in wants to be finished in next transmission.

**3. Non-repudiation**
Non-repudiation will facilitate the ability to identify the attackers even after the attack happens [5], [8]. This prevents cheaters from denying their crimes. Any information related to the car like: the trip rout, speed, time, any violation will be stored in the TPD, any official side holding authorization can retrieve this data.

**4. Privacy**
Keeping the drivers' data far from unapproved onlookers, this data like genuine personality, trip way, speed and so forth… The security could be accomplished by utilizing brief (mysterious) keys, these keys will be changed much of the time as every key could be utilized only for one time and lapses after use [1], every one of the keys will be put away in the TPD, and will be reloaded again in next time that the vehicle makes an official checkup [5]. For saving the genuine character of the driver, an ELP (Electronic License Plate) is utilized, this permit is introduced in the production line for each new vehicle, it will give an ID number to the vehicle, to recognize the vehicle in anyplace, with the RFID innovation to hold the ELP. On the off chance that when the police or any official needs the genuine personality, it can take a request from the judge to recoup the character of particular vehicles EL

**5. Real-time constraints**
Vehicles move in high speed, this will require a realtime response in some situation, or the result will be devastating [5]. Current plans for vehicular networks rely on the emerging standard for dedicated short-range communications (DSRC), based on an extension to the IEEE 802.11 technology.

# 6. CONCLUSIONS AND FUTURE WORK

Vehicular Ad Hoc Networks is promising technology,which gives abundant chances for attackers, who will tryto challenge the network with their malicious attacks.This paper gave a wide analysis for the currentchallenges and solutions, and critics for these solutions, signature is also mentioned in [10][19], as the authors proposed a protocol for guarantee the requirements of the security and privacy, and to provide the desired traceability and liability, but the result of the study was not quit encouraging, After 9 ms for group signature verification delay, the average message loss ratio was 45%, another result was the loss ratio reaches as high as 68% when the traffic load is 150 vehicles. The other solution been suggested is the use of CA and this requires infrastructure for it. VANET requires a large number of CA to govern it. until now we don't have a real authority that govern the world of VANET, the CA been suggested by[4],[7],[10],[11],[12],[13] , all of these researchers mentioned the CA to handle all the operations of certificate generating, renewing and revoking, and CA must be responsible in initiating keys, storing, managing and broadcasting the CRL.

# 7. REFERENCES

[1] M Raya, P Papadimitratos, JP Hubaux, "Securing Vehicular Communications", IEEE Wireless Communications, Vol 13, October 2006 .

[2] H Fussler, S Schnaufer, M Transier , W Effelsberg ,"Vehicular Ad-Hoc Networks: From Vision to Reality and Back", Proc. Of IEEE Wireless on Demand Network Systems and Services, 2007.

[3] GMT Abdalla, SM Senouci "Current Trends in Vehicular Ad Hoc Networks", Proceedings of UBIROADS workshop, 2007.

[4] M Raya, D Jungels, P Papadimitratos, I Aad, JP Hubaux,"Certificate Revocation in Vehicular Networks " , Laboratory for PC Communications and Applications (LCA) School of Computer and Communication Sciences ,EPFL, Switzerland, 2006 .

[5] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks", Proc. of HotNets-IV, 2005.

[6] I Aad, JP Hubaux, EW Knightly, "Effect of Denial of Service Attacks on Ad Hoc Networks", Networking, IEEE/ACM Transactions on Volume 16, August, 2008.

[7] M Raya, J Pierre Hubaux," The security of VANETs", Proceedings of the second ACM universal workshop on Vehicular impromptu systems, 2005.

[8] J. Douceur," the Sybil Attack", First International Workshop on Peer-to-Peer Systems, first ed, USA, Springer, 2003.

[9] F. Karnadi, Z. Mo, "Quick Generation of Realistic Mobility Models for VANET ", proc. IEEE Wireless Communications and Networking Conference, 2007.

[10] X Lin, R Lu, C Zhang, H Zhu, P Ho,and X Shen. "Security in Vehicular Ad Hoc Networks ", IEEE Communications Magazine, vol. 4, April 2008.

[11] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and JP Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks ", IEEE Magazine, vol. 10, October 2007.

[12] R. Lind et al, .The system vehicle.A look into the eventual fate of portable media, IEEE Aerosp. Electron. Syst. Mag., 1999.