A REVIEW ANALYSIS ON VEHICULAR AD-HOC NETWORKS: SECURITY ISSUES AND CHALLENGES

[1]D.Sivabalaselvamani, [2]Dr.A.Tamilarasi, [3]L.Rahunathan, [4]A.S.Harishankher
[1,3,4]Assistant Professors, [2]Professor and Head
Department of Computer Applications,
Kongu Engineering College, Perundurai, Erode-638052, Tamilnadu, India.

***ABSTRACT*: Vehicular Ad Hoc Networks (VANET) is a unique platform to improve road safety and increase passenger convenience in vehicles. In the existing system, they use the air as a medium for communication; they are out in the open to several suspicions in the network that influences there liability of these features. The need for a robust VANET networks is strongly dependent on their security and time alone features through routing, which will be conferred in this paper. In this paper a various types of routing and security problems of VANET been analyzed and discussed; we also discuss a set of way out presentation to solve these challenges and problems.**

Keywords: VANET, MANET, DoS (Denial of Service), SEAD, SMT and NDM

I. INTRODUCTION

Vehicular improvised framework is an exceptional sort of MANET which is a vehicle to vehicle and vehicle roadside remote correspondence framework. It is self-representing and self-sorting out remote correspondence framework, where centers in VANET incorporate themselves as servers and/or clients for exchanging and sharing information [3]. With a sharp augmentation of vehicles out on the town, new development is envisioned to offer workplaces to the voyagers including security application; help to the drivers, emergency alerted et cetera. Vehicular Ad-Hoc Networks (VANETs) is a utilization of MANETs that contemplates correspondence between road transports vehicles and advances security on lanes. There is however circumstances that could make hurt the vehicle and/or its tenants; vehicles could be taken after, taken after or have their messages checked. Vehicular off the cuff framework (VANET) is a sub class of MANET with some exceptional properties. VANETs have creating out these days in view of the necessity for supporting the extended number of remote sorts of rigging that can be used as a piece of vehicles [1]. Some of these things are overall arranging structure, cell phones and convenient workstations. VANETs have some diverse properties then MANETs like road illustration controls, no impediment on framework size, dynamic topology, convenience models, and unending essentialness supply, confinement value and so forth. Each one of these properties made VANET environment a striving for making powerful directing traditions. The principle thought in it is the rapidly moving flexible center points.

The growing immovability of people has achieved a high cost for social requests as aftereffect of the extending number of action stop up, fatalities and wounds. Vehicular Ad-Hoc Networks (VANETs) consider supporting organizations on Intelligent Transportation Systems (ITSs), as total seeing of development, accident avoidance, vehicle course, control of action lights, and development obstruct organization by motioning to drivers. VANETs incorporate vehicles and roadside supplies owning remote interfaces prepared to give among them by remote and multi-ricochet correspondence. VANET security should satisfy four targets [5], it should ensure that the information got right (information believability), the source is who he claims to be (message genuineness and source approval), the center point sending the message can't be perceived and took after (insurance) and the structure is vivacious.

In the year 1998, the gathering of experts from Delphi Delco Electronics System and IBM Corporation proposed a framework vehicle thought went for giving a broad assortment of employments [1]. With the movements in remote exchanges advancement, the possibility of framework auto has pulled in the thought all around all through the world. Starting late, various new assignments have been impelled, concentrating on comprehension the dream of frameworks organization auto and productive use of vehicular frameworks. The endeavor Network on Wheels (NOW) [1] is a German examination wander built up by DaimlerChrysler AG, BMW AG, Volkswagen AG, Fraunhofer Institute for Open Communication Systems, NEC Deutschland GmbH and Siemens AG in 2004, the endeavor grasps an IEEE 802.11 standard for remote access. The standard destinations of this suspect are to comprehend specific issues related to correspondence traditions and data security for auto - to-auto exchanges. The Car2Car Communication Consortium [16] is begun by six European vehicle creators. It will presumably make an European mechanical standard for auto to-auto correspondences stretch out over all brands. FleetNet [1] was another European undertaking which continued running from 2000 to 2003 this exceptionally delegated investigation was ruled by attempts to regulate MANET traditions, and this MANET research focused on the framework layer[1], an authoritative test was to handle the issue of how to accomplish center points not particularly inside radio degree by using neighbors as forwarders, while the European Commission is pushing for another examination effort here with a particular finished objective to accomplish the goal of diminishing the car collisions of half by 2010, hoping to accomplish an alluring level of secure VANET. CarTALK 2000 is a European Project focusing on new driver help structures which are based upon covers - vehicle correspondence. The essential objectives are the change of accommodating driver help structures from one perspective and the progression of a self-orchestrating unrehearsed radio

framework as a correspondence premise with the purpose of setting up a future standard. Concerning the help system, the essential issues are: an) assessment of today's and future applications for co-specialist driver help systems, b) change of programming structures and computations, i.e. New blend techniques, c) testing and indicating help limits in test vehicles in real or replicated action circumstances. To fulfill a sensible correspondence structure, computations for radio exceptionally designated frameworks with significantly high component framework topologies are created and models attempted in the vehicles. Beside imaginative goals, CarTALK 2000 viably addresses market presentation methods including cost/advantage examinations and legal points of view, and goes for the systematization to pass on these structures to the European business segment. CarTALK 2000 started in August 2001 as a three-year wander which is financed inside the IST Cluster of the fifth Framework Program of the European Commission.

A. VANET Structure

A VANET transforms each partaking auto into a remote switch or hub, permitting autos around 100 to 300 meters of each other to interface and, thus, make a system with a wide range. As autos drop out of the sign range and drop out of the system, different autos can participate, associating vehicles to each other so that a portable Internet is made. Vehicular correspondence frameworks are a kind of system in which vehicles and roadside units are the conveying hubs, furnishing each other with data, for example, security notices and movement data. As a helpful methodology, vehicular correspondence frameworks can be more viable in evading mishaps and movement blockages than if every vehicle tries to take care of these issues exclusively. For the most part, vehicular systems are considered to contain two sorts of hubs: vehicles and roadside stations as appeared in figure 1. The system ought to bolster both private information interchanges and open (for the most part security) correspondences however higher need is given to open correspondences. There are three essential parts of the VANET [4]: Onboard unit (OBU), Roadside unit (RSU) and the backhaul system.

b. VANET Working

Vehicular Networks System comprises of extensive number of hubs, around number of vehicles surpassing 750 million on the planet today [4], these vehicles will require a power to oversee it, every vehicle can speak with different vehicles utilizing short radio signs DSRC (5.9 GHz), for extent can achieve 1 KM, this correspondence is an Ad Hoc correspondence that implies each associated hub can move unreservedly, no wires required, the switches utilized called Road Side Unit (RSU), the RSU functions as a switch between the vehicles out and about and associated with other system gadgets.

Figure 1. VANET Structure

Every vehicle has OBU (on board unit), this unit associates the vehicle with RSU by means of DSRC radios, and another gadget is TPD (Tamper Proof Device), this gadget holding the vehicle insider facts, all the data about the vehicle like keys, drivers character, trip points of interest, velocity, defeat … and so on., see figure 2.

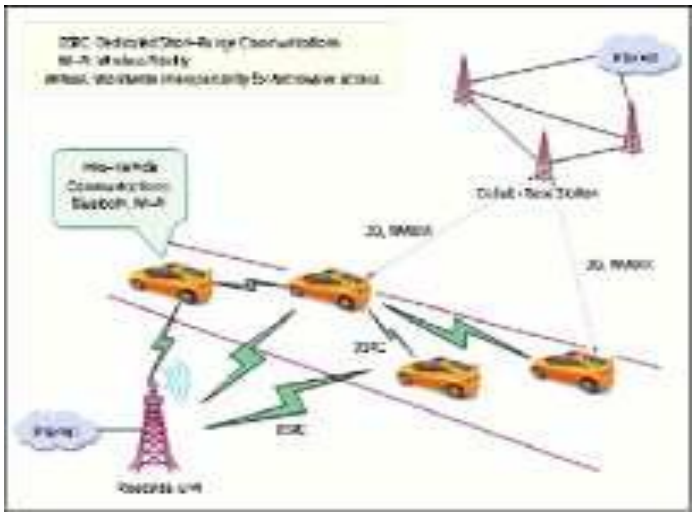

Figure 2. VANET Communication

II. VANET CHARACTERISTICS

The qualities of a vehicular impromptu system are one of a kind contrasted with other portable specially appointed systems. The recognizing properties of a VANET offer chances to expand system execution, and in the meantime it presents significant difficulties. A VANET is on a very basic level distinctive [5] from different MANETs.

High Mobility:

The hubs in VANETs for the most part are moving at rapid. This makes harder to foresee a hub's position and making security of hub protection [2].

Quickly changing system topology:

Because of high hub portability and arbitrary pace of vehicles, the position of hub changes habitually. As an aftereffect of this, system topology in VANETs tends to change much of the time [3].

Unbounded system size:

VANET can be actualized for one city, a few urban areas or for nations. This implies system size in VANET is geologically unbounded [3].

Incessant trade of data:

The impromptu way of VANET rouses the hubs to accumulate data from alternate vehicles and street side units. Subsequently the data trade among hub gets to be incessant.

Remote Communication:

VANET is intended for the remote environment. Hubs are associated and trade their data by means of remote. Along these lines some security measure must be considered in correspondence [2].

Time Critical:

The data in VANET must be conveyed to the hubs with in time confine so that a choice can be made by the hub and perform activity as needs be.

Adequate Energy:

The VANET hubs have no issue of vitality and calculation assets. This permits VANET utilization of requesting strategies, for example, RSA, ECDSA execution furthermore gives boundless transmission power [2].

III. APPLICATIONS

Real utilizations of VANET encapsulate giving security information, activity administration, toll administrations, area principally based administrations and narrative. One among the chief utilizations of VANET typify giving security associated information to maintain a strategic distance from crashes, diminishing aggregate of vehicles when partner mischance and furnishing notices connected with condition of streets and convergences. Mounted with the security associated information are the obligation associated messages, which may affirm that vehicles are available at the area of the mischance and later encourage in settling obligation regarding the mishap.

a. Intelligent Transportation Applications

Intelligent Transport system(ITS) that epitomize a scope of utilizations like on worldwide situating framework, activity perception, investigation of car influx, administration of movement framework, and redirection of courses which bolster the activity situation. As an illustration, existing roadside unit watching movement on the streets and send all the data to a focal power that break down them to control activity stream so that the best movement signal calendars will be planned.

b. Solace applications

Those applications which allow the customers to having anyplace on the web to enhance solace of customers impart data either to option customers in vehicles or with others are known as solace applications. For example, VANETs permits vehicular hubs to associate with web to so that the rearward sitting arrangement travelers will play amusements or exchange music. Generally, some dynamic or attached dispensed systems to web portals are summed up with the systems, so it will send the

information bundles to the VANETs and in this manner the web [1].

c. Crash Avoidance

Vehicles to vehicles and vehicles to roadside unit correspondences will spare a few lives and prevent wounds. As indicated by this application, if a vehicle diminishes its pace significantly once recognizing a mishap then vehicle telecast its area to its neighbor vehicles [1]. Also, distinctive collectors can attempt to exchange the message to the vehicles further behind them and accordingly the vehicle being referred to can radiate some alert to its vehicles and diverse vehicles behind. Amid this procedure, a great deal of vehicles path behind can get a caution signal before they see the mischance and may take any better choice.

d. Helpful Driving

The drivers assume a noteworthy part amid this application. Like turn struggle cautioning, infringement cautioning, bend cautioning, path blending cautioning and so on. These administrations may respectably bring down the life-jeopardizing mischance. Actually, a few of the mishaps return from the lack of collaboration between drivers. Given a great deal of data concerning the possible clashes, we will stop a few mischances [1].

e. Installment Services

This application is extraordinarily fitting for toll variety while not notwithstanding decelerating the vehicle or holding up in line.

f. Area based Services

Finding the closest fuel station, motels, bistros and so forth is done viably by abuse of area based administration. GPS framework is utilized to expand these sorts of administrations in VANET. The different utilizations of VANETs are [5] to help the driver, information scattering, stopping issues, crisis vehicle cautioning, upkeep of least security separation, web network, shared application, clog out and about, data about crossing points, and some more.

IV. CHALLENGES IN VANET

The security of VANET has for the most part coordinated the consideration of today research endeavors, while complete answers for shield the system from foe assaults still should be enhanced, attempting to achieve an attractive level, for the driver and producer to accomplish wellbeing of life and infotainment.

4.1 Vehicular Security Challenges

VANET face numerous security assaults and these assaults and risk can be sorted in few classes. The five sorts of attacks for the assaults is a simple distinguishing proof. Each of the classes will speak to various sorts of assault level and need. The following are the proposed classes of assault:

a. System Attack:

System attacks are dependably on the highest priority on the rundown and are named a top need since it can be perilous to the whole system. A solitary fruitful system assault may effectively influence the entire system. Few case of system assault is, for example, Denial of Services (DOS) Attack and Sybil Attack.

b. Denial of Service Attack:

As appeared in figure 3 this assault happens when the assailant takes control of a vehicle's assets or jams the correspondence channel utilized by the Vehicular Network, so it keeps basic data from arriving. It likewise builds the risk to the driver, on the off chance that it needs to rely on upon the application's data.

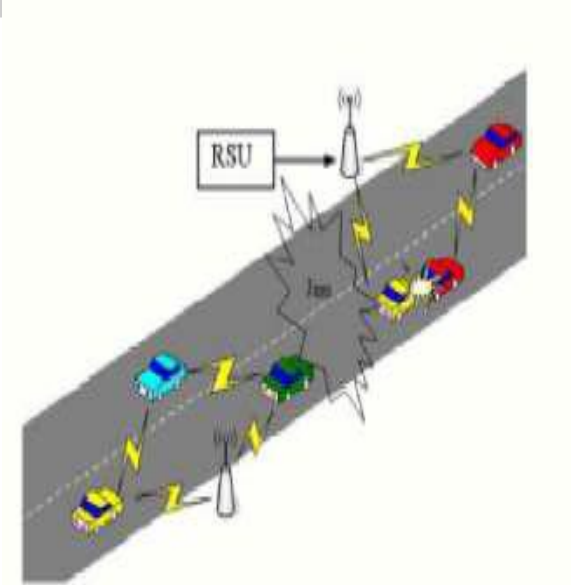

Figure.3 DoS Attack

c. 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 exchange route[3][4]. Sybil assault relies on upon how inexpensively personalities can be created as appeared in figure 4. For example an aggressor can imagine and

act like a hundred vehicle to persuade alternate vehicles in the street that there is clog, go to another defeat, so the street will be clear.

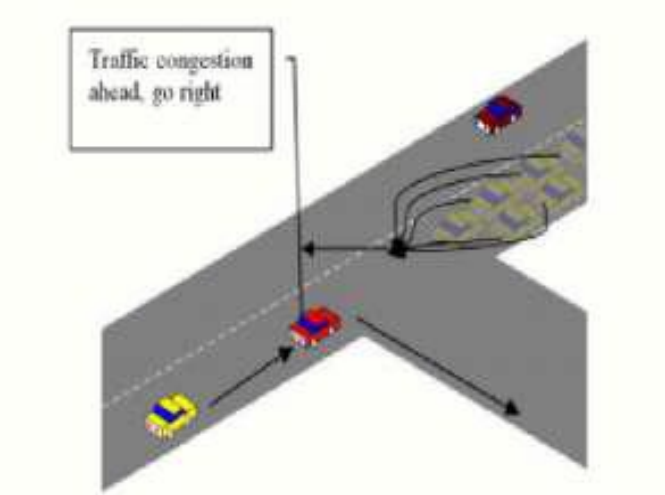

Figure. 4 Sybil Attack

d. Application Attack:

In application assault class, the assailant consideration is no other than to control application content for its own particular advantage. These aggressors will have a tendency to stifle or modify the real message and change it with a false substance which may make hurt other vehicle. This sort of assault may be finished by either pernicious or levelheaded aggressor for no particular reason or to serve their own particular advantages. Couple of case of use assault is, for example, message concealment assault, creation assault, change assault [1].

e. Fabrication Attack:

An aggressor can make this assault by transmitting false data into the system, the data could be false or the transmitter could guarantee that it is another person as appeared in figure 5. This assault incorporates manufacture messages, notices, declarations, personalities [4].

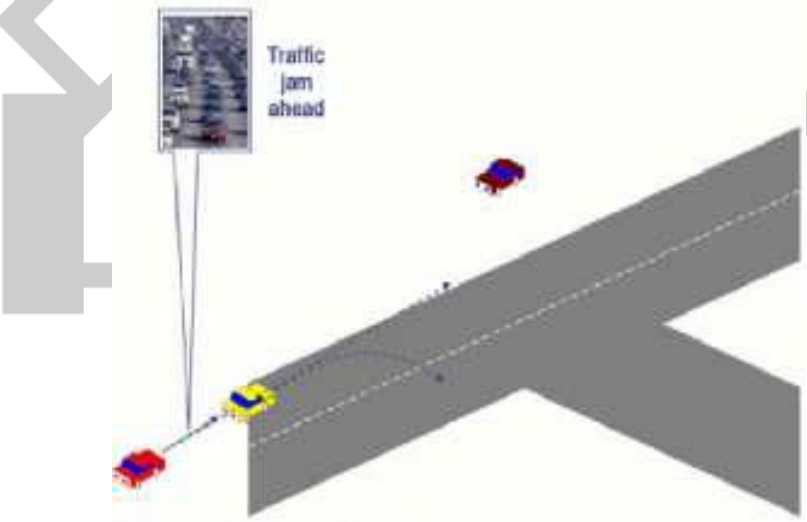

Figure. 5 Fabrication Attack

f. Transformation Attack:

This assault happens when aggressor adjusts current information, it incorporates postponing the transmission of the data, replaying prior transmission, or modifying the real section of the information transmitted [3]. For example, as appeared in figure 6 boycott assailants can adjust a message telling different vehicles that the present street is clear while the street is congested [5].

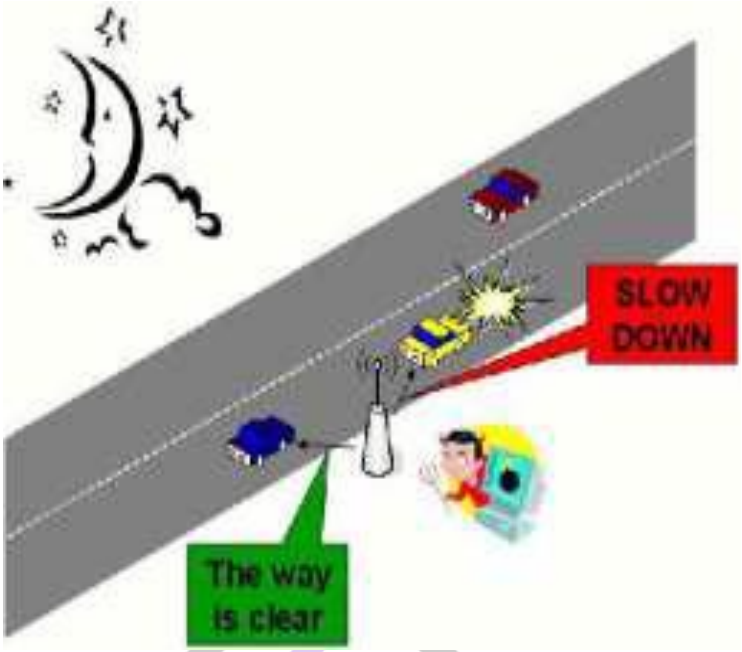

Figure. 6 Alteration Attack

g. Social Attack:

Social assault contains all unmoral and passionate messages [4]. The fundamental target in a large portion of social assault is to in a roundabout way make issue in the system by awful and undesirable messages which can influence the conduct of others street clients.

h. Burrow Attack:

Since GPS signals vanish in passages, an aggressor may abuse this provisional loss of situating data to infuse false information once the vehicle leaves the passage and before it gets a credible position overhaul as appeared in figure 7. The physical passage in this illustration can likewise be supplanted by a range stuck by the aggressor, which results in the same impacts.

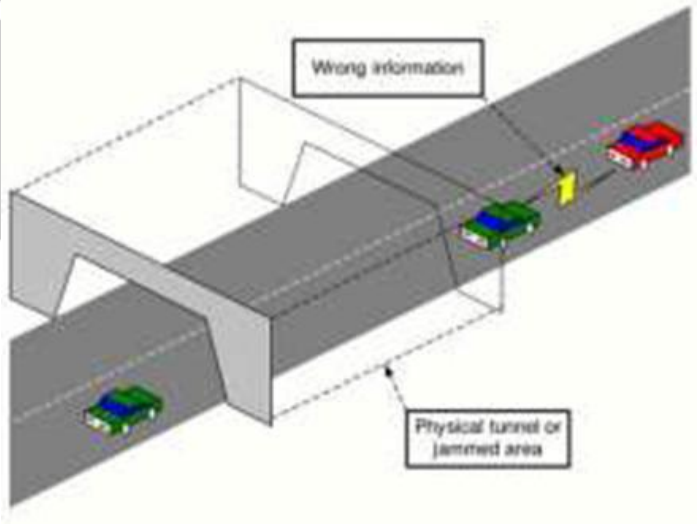

Figure. 7 Burrow Attack

I. Checking Attack:

Checking Attack is a genuine danger for the street wellbeing authorities. In this sort of assault, the aggressors which can be viewed as both neighborhood and pariah would noiselessly screen and track essential messages which shouldn't be discharge openly arrange. Assailants would utilize the significant data assembled from listening stealthily to serve their own particular advantage. In observing assault, the assailant simply screen the entire system, listen the correspondence amongst V2V and V2I. On the off chance that they locate any related data then pass this data to concern individual.

j. Eavesdropping Attack:

Eavesdropping Attack is a system layer assault comprising of catching bundles from the system transmitted by others' PCs and perusing the information content looking for delicate data like passwords, session tokens, or any sort of classified data. Spying is subtly listening to the private discussion of others without their assent as appeared in figure 8. Listening stealthily is the

unapproved constant block attempt of a private correspondence, for example, a telephone call, text, video meeting or fax transmission. The term spy gets from the act of really remaining under the roof of a house, listening to discussions inside Eavesdropping should likewise be possible over phone lines (wiretapping), email, texting, and different strategies for correspondence considered private.

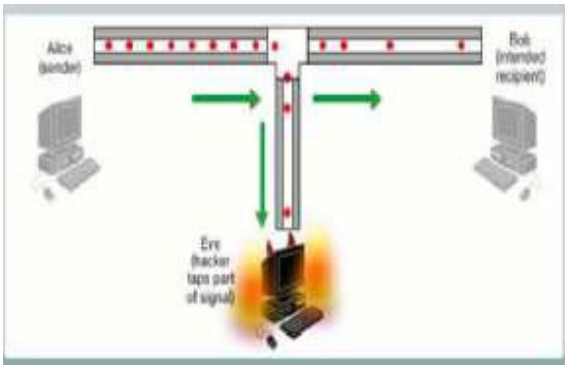

Figure. 8 Eavesdropping Attack

4.2 Vehicular Networks Challenges

Portability

The essential thought from Ad Hoc Networks is that every hub in the system is versatile, and can move starting with one place then onto the next inside the scope territory, yet at the same time the portability is constrained, in Vehicular Ad Hoc Networks hubs moving in high portability, vehicles make association toss their way with another vehicles that perhaps never confronted, and this association goes on for just few moments as every vehicle goes toward its, and these two vehicles may never meet again. So securing versatility test is difficult issue [3].

Unpredictability

The network among hubs can be profoundly fleeting, and possibly won't happen once more, vehicles voyaging toss scope region and making association with different vehicles, these associations will be lost as every auto has a high versatility, and perhaps will go in inverse direction[1][3]. Vehicular systems does not have the generally long life setting, so individual contact of client's gadget to a problem area will require long life watchword and this will be unreasonable for securing VC [5].

Protection VS Authentication

The significance of confirmation in Vehicular Ad Hoc Networks is to avert Sybil Attack that been talked about before [3]. To evade this issue we can give a particular character for each vehicle, yet this arrangement won't be proper for the vast majority of the drivers who wish to keep their data secured and private[1][3].

Security VS Liability

Obligation will give a decent open door for lawful examination and this information can't be denied (if there should be an occurrence of accidents)[1], in other hand the protection mustn't be damaged and every driver must be able to keep his own data from others (Identity, Driving Path, Account Number f or toll Collector and so on.) [5].

System Scalability

The size of this system on the planet around surpassing the 750 million hubs [5], and this number is developing, another issue emerge when we should realize that there is no a worldwide power administer the measures for this system [5], for instance: the benchmarks for DSRC in North America is deferent from the DSRC norms in Europe, the guidelines for the GM Vehicles is deferent from the BMW one.

Bootstrap

As of now just few number of autos will be have the hardware required for the DSRC radios, so on the off chance that we make a correspondence we need to accept that there is a predetermined number of autos that will get the correspondence, later on we should focus on getting the number higher, to get a money related advantage that will bravery the business firms to put resources into this innovation [5].

4.3 Vehicular Technical Challenges

The specialized difficulties manage the specialized deterrents which ought to be determined before the organization of VANET. Some difficulties are given beneath:

System Management:

Because of high portability, the system topology and channel condition change quickly. Because of this, we can't utilize structures like tree in light of the fact that these structures can't be set up and kept up as quickly as the topology changed [2].

Clog and impact Control:

The unbounded system estimate likewise makes a test. The movement burden is low in rustic ranges and night in even

urban zones. Because of this, the system parcels regularly happens while in surge hours the activity burden is high and consequently system is congested and impact happens in the system.

Ecological Impact:

VANETs utilize the electromagnetic waves for correspondence. These waves are influenced by nature. Henceforth to convey the VANET the ecological effect must be considered.

Macintosh Design:

VANET for the most part utilize the mutual medium to impart henceforth the MAC configuration is the key issue. Numerous methodologies have been given like TDMA, SDMA, and CSMA and so on. IEEE 802.11 received the CSMA based Mac for VANET.

Security:

As VANET gives the street wellbeing applications which are lives basic in this way security of these messages must be fulfilled.

V. CURRENT SOLUTIONS

There are numerous arrangements gave to relieve the assaults in VANET. The accompanying are the five best arrangements that are most usually utilized. The framework ought to have the capacity to build up the obligation of drivers; yet in the meantime, it ought to ensure the security of the drivers and travelers [2].

B. Dahilletal proposed a safe directing convention for specially appointed system taking into account verification. This depends on AODV yet it keeps from assaults including satirizing. ARAN utilizes general society key cryptography and requires an endorsement server whose open key is known not hubs. It utilizes timestamp for the freshness of the course. A source hub telecasts the course revelation bundle (RDP) to all its neighbors for course disclosure [2]. Every hub keeps the record of its neighbor from which it gets the message. Subsequent to getting the message all the neighbor again advances this message to their neighbors with their sign and own authentication. At the point when the message got by the destination, it answers to the main hub from which it got the message. No middle of the road hub can answer the RDP other than destination regardless of the possibility that that transitional hub knows the way of destination. The destinations will uncast the answer (REP) in converse from destination to source. All REP is marked by the sender and checked by the following bounce. For the briefest way, the source starts with the scrambled most limited way affirmation (SPC) message and shows it to its neighbor. Destination hub answers with the recorded most brief way (RSP) to the source through its antecedent. Every neighbor signs the encoded part of the message and connects its declaration. ARAN requires that every hub must keep one steering table for every hub in a system. At the point when no activity is found on hub in lifetime it is essentially deactivated from the table. On the off chance that information is gotten on dormant course, the blunder message ERR is created which goes through converse way of the source. In the event that a hub is broken because of the hub development, the ERR message is produced.

5.1. SEAD (Secure and Efficient Ad hoc Distance Vector):

Y. C. Hu, D. B. Johnson and A. Perrig proposed another safe directing convention which secures against numerous clumsy aggressors who makes inaccurate steering in whatever other hub. It depends on the Destination sequenced Distance Vector (DSDV) directing. SEAD bolsters the hub which has constrained CPU preparing ability and shields from the DoS assault in which aggressors' endeavors to expend overabundance system transfer speed. It utilizes the restricted hash work instead of more costly uneven cryptographic operation. ++One way hash capacity is made by picking an arbitrary beginning vale through the hub. After that the rundown of qualities are computed as underneath:

h0, h1, h2… hn

Where h0= x and hi=H (greetings 1)

For 0< I =n.

For the confirmation a hub with the validated worth hello can verify howdy 4 by registering H (H (greetings 4)) [4]. It utilizes destination-succession number to keep away from the seemingly perpetual steering circle furthermore shields from replay assault as the destination-grouping number give the freshness of the parcel.

5.2. SMT (Secure Message Transmission):

P. Papadimitratosetal [2] proposed Secure Message Transmission convention which is light weight and works on end to end way. It requires a security relationship amongst source and destination. It doesn't utilize the cryptographic operation for middle of the road hubs. The source first finds the way through existing course revelation convention and decides the underlying Active Path Sets (APS) for correspondence. After consummation of this a source has an arrangement of APS. The source scatters the each cordial message into various pieces and encodes and transmits crosswise over various courses. Each scattered piece conveys a MAC (Message Authentication Code) which is utilized to check the honesty and verification of its source. Taking into account the parcel got or fizzled on various APS, the source hub rates the APS way. The destination accepts and sends an input affirmation to the source.

5.3. NDM (Non-Disclosure Method):

A. Fasbenderetal [12] proposed this technique to ensure area data in portable IP. They determined the issue of activity investigation and area revelation. The NDM approach expects various free Security specialists and every SA utilizes people in

general and private key sets. Henceforth this methodology depends on deviated cryptography. In this approach a sender sends the message to the collector without unveiling any area data. Correspondence amongst sender and collector is performed by means of SAs. Each SAi knows the location of ASi-1and ASI+1. Sender sends the message to SA1, and afterward SA1sends it to SA2and so on. Every SA epitomizes the message with its open key. In any case, assailant can follow the message by their length amid correspondence henceforth a variable cushioning Scheme is likewise presented.

Sr. No	Solution	Attacks Covered	Technology used	Security Requirements
1.	ARAN	1. Replay Attack 2. Impersonation 3. False Warning	1. Cryptographic Certificate	1. Authentication 2. Message integrity 3. Non - Repudiation
2.	SMT	1. Information Disclosure	1. MAC (Message Authentication Code)	1. Authentication
3.	SEAD	1. DoS 2. Routing Attack 3. Resource Consumption	1. One Way Hash Function	1. Authentication 2. Availability
4.	NDM	1. Information Disclosure 2. Location Tracking	1. Asymmetric Cryptography	1. Privacy

Table 1. Comparative study of solutions

6. CONCLUSION

Security is the real zone under exchange to actualize the VANET. The investigation of assaults found that the aggressor goal is to assault the system layer straightforwardly or in a roundabout way, subsequently the directing convention must be ensure enough to keep the most sorts of assaults. Every arrangement must protect the security prerequisites like confirmation, trustworthiness, and security which are more overpowered. Vehicular Ad Hoc Networks is a developing and promising innovation, this innovation is a fruitful district for assailants, who will attempt to go up against the system with their vindictive assaults. This report gives an investigation about the present situation and answers for the improvement. Aside from guaranteeing accessibility of data that offers a protected driving conduct and a superior voyaging background, the system is a financial correspondence, and information administration empowering influence. In any case, despite the fact that advantages, data security dangers and protection issues represent a colossal test to VANET extension and utilization. A standout amongst the most fascinating parts of the system is the capacity of the system to self-sort out in an exceedingly portable system environment. This paper furnished perusers with a concise representation of the system by portraying the system qualities, design, applications, correspondence examples, and security challenges.

REFERENCES

[1] Bijan Paul, Md. Ibrahim, Md. Abu NaserBikas. VANET Routing Protocols: Pros and Cons. International Journal of Computer Applications (0975 – 8887) Volume 20– No.3, April 2011.

[2] D.Sivabalaselvamani, Dr.A.Tamilarasi, L.Rahunathan, "Experimental Evaluation of Safety through Automatic Identification of Drunk Driving (DD) and Road Accidents (RA) as a part of Vehicular Ad Hoc Network (VANET)", June 16 Volume 4 Issue 6 , International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), ISSN: 2321-8169, PP: 127 – 134.

[3] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures. Security Analysis of Vehicular Ad HocNetworks (VANET). 2010 Second International Conference on Network Applications, Protocols and Services.

[4] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures. Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET). National AdvancedIPv6 Center, UniversitiSainsMalaysia Penang, Malaysia. June 28, 2010.

[5] Komal Mehta, Dr. L. G. Malik, Dr. Preeti Bajaj. Security Challenges, Issues and Their Solutions for VANET. International Journal of NetworkSecurity & Its Applications (IJNSA), Vol.5, No.5, September 2013. Ambedkar Institute of Advanced communication Technologies & Research Delhi, India.

[6] Patrick I. Offor. Vehicle Ad Hoc Network (VANET): Safety Benefits and Security Challenges. Nova Southeastern University (po125@nova.edu). December 3, 2012.

[7] Surmukh Singh, Sunil Agrawal VANET Routing Protocols: Issues and Challenges Proceedings of 2014 RAECS UIET Panjab University Chandigarh, 06 – 08 March, 2014.