Journal Of Harmonized Research (JOHR)

Journal Of Harmonized Research in Engineering
8(3), 2020, 64-76

ISSN 2347 – 7393

Survey Article

VSCPA: A SURVEY ON VANET SECURITY, CHALLENGES, PROTOCOLS AND ITS APPLICATIONS

Harsh Lohiya

Research Scholar, Sri SatyaSai University of Technology and Medical Sciences, Sehore (M.P.)

Abstract: For the Intelligent Transport System, vehicular ad hoc network is one of the prominent network technologies which is a sub class of mobile ad hoc network. VANET provides the safety information to the driver and passenger. It also provides the communication among the vehicle and vehicle to road side equipment. It is used in enormous number of applications but it is quite different from the mobile ad hoc network (MANET) in terms of characteristics, architecture, challenges and application. This technology proves the various services such as traffic management, safety, and dynamic route planning, cost effective and scalable network but some nodes of the network may compromise from different security attack because of dynamic or scalable nature so it becomes more essential to overcome these threats using security technique first. In this paper, we address the security issues and challenges in vehicular ad hoc network. We also address the architecture, protocols, applications and security attacks in it.

Keywords- VANET, Intelligent Transport System, Road Side Equipment, Security attack, MANET, Dynamic Route Planning.

Introduction: A vehicular ad-hoc network is an extraordinary type of MANET that is a V2V (vehicle and vehicle) side of the road wireless transmission network. This is an autonomous and self – arranging transmission network system. The node in VANET includes themselves as server and terminal for trading and imparting data to one another. Vehicles out and about, new innovation are imagined to give offices to the travellers including safety applications, help to the drivers, emergency admonitions, and so on. Vehicular Ad-Hoc Networks (VANETs) is a use of MANETs that takes into account transmission between street transports vehicles and advances security on streets. There are anyway circumstances that could make harm the vehicle as well as its tenants; vehicles could be followed, followed, or have their messages checked. Vehicular

For Correspondence:
lohiya27harsh@gmail.com.
Received on: March 2020
Accepted after revision: July 2020
DOI: 10.30876/JOHR.8.3.2020.64-76

specially appointed system (VANET) is a subclass of MANET with some interesting properties. VANETs have developed nowadays because of the requirement for supporting the expanded number of wireless hardware that can be utilized in vehicles [1]. A portion of these items are worldwide situating systems, cell phones, and PCs. VANETs have some divergent properties then MANETs like street design limitations, no limitation on network size, unique geography, versatility models, and boundless vitality flexibly, confinement usefulness, etc. Every one of these attributes made the VANET condition trying for creating proficient directing conventions. The central point in it is the quickly moving versatile nodes. The expanding versatility of individuals has caused a significant expense for social orders as a result of the expanding number of traffic clog, fatalities, and wounds. In VANETs, there are two sorts of transmissions: (1) vehicle to vehicle (V2V) and (2) vehicle to foundation (V2I). Vehicles have On-Board Units (OBUs), which comprise of Omnidirectional radio wires, processors, GPS units, and sensors for V2V interchanges. Vehicles additionally perform V2I interchanges with side of the road foundations, which are set inside a fixed separation of one another relying on the transmission scope of the side of the road gadgets, otherwise called Road Side Units (RSUs). RSUs speak with one another through a wireless medium or wired associations. They can likewise be portable. The V2I transmissions can be additionally reached out to give applications, for example, the Internet since RSUs can be associated with a system. The V2V transmissions can be utilized to send crisis and continuous data, for example, an accident or street traffic data so different vehicles can take elective courses to forestall traffic congestions.[4] Vehicular Ad-Hoc Networks (VANETs) conceive supporting administrations on Intelligent Transportation Systems (ITSs), as aggregate checking of traffic, impact shirking, vehicle route, control of traffic lights, and traffic blockage the executives by motioning to drivers. VANETs contain vehicles and side of the road gear possessing wireless interfaces ready to impart among them by wireless and multi-jump transmission. VANET security ought to fulfill four objectives [2, 3], it ought to guarantee that the data got is right (data validness), the source is who he professes to be (message uprightness and source confirmation), the node sending the message can't be distinguished and followed (protection) and the system is robust.

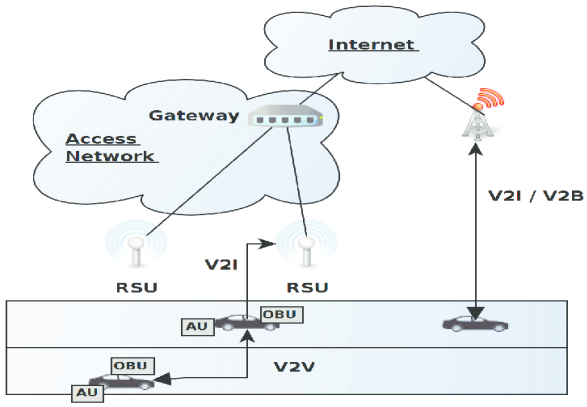

Fig. 1 VANETs Architecture [5]

Since VANETs support emergency continuous applications and furthermore manage life-basic information they ought to follow the security prerequisites, for example, protection, secrecy, respectability, and non-disavowal to give made sure about interchanges against assailants, and malevolent hubs. The principle motivation behind giving the security and protection in VANETs depends on the way that at no time during the communication in VANETs the genuine character of the drivers ought to be uncovered since enemies may utilize this data for propelling assaults with bogus personalities and never get captured. Nonetheless, vehicles and drivers need to reveal their personalities to RSUs to speak with them. Thus, the security and protection issues must be taken care of cautiously with the goal that the enemies can't abuse them. In this paper, we address the security issues and challenges of vehicular ad hoc network. We also address the routing protocols, application and security attack in vehicular ad hoc network with their countermeasures.

VANET Overview: Since 1980, VANETs which are ad hoc network frameworks develop

suddenly, in which vehicles are associated through wireless communication [6-41]. As of late, VANETs are utilized in upgrading traffic security, improving traffic stream, and lessening traffic congestion and driver direction [7]. The essential model graph of VANETs which shows the vehicles' communication can be recognized into V2V and V2I communication, side of the road units (RSUs), and locally available units (OBUs). The OBU is prepared in every vehicle, which can send the traffic data to the neighboring vehicles and RSU by utilizing committed short-go communication (DSRC) [8].

Initially, we will talk about these boundaries and afterward clarify the one of a kind qualities and focal points of utilizing VANETs over MANETs as far as system geography, transfer speed, dependability, and so on. As we examined over, the VANETs comprise three segments, for example, OBUs, RSUs, and confided in power (TA); these boundaries are talked about beneath.

1) Trusted Authority: TA represents enlistments of RSUs, vehicular OBUs, and vehicle clients. Moreover, it additionally serves to check approvals of real vehicular OBU or client IDs, in order to forestall antagonistic vehicles [9] from getting to VANET frameworks. The TA is set up with a ground-breaking computational foundation and enough stockpiling limit. A TA can uncover the genuine ID of OBUs in case of pernicious informing communicates or different practices.

2) Roadside unit: RSUs are regularly fixed units that are introduced nearby boulevards or in fixed destinations to incorporate stopping or road crossing point areas. RSUs look like OBUs in that they contain handsets, receiving wires, processors, and sensor groups. Each RSU is expected to offer remote types of assistance to vehicle clients. For example, an RSU might be situated almost a road crossing point so as to control the traffic just as to decrease mishap occurrence. Each RSU uses DSRC radios as per IEEE 802.11p radiofrequency innovation to recover radio channels using omnidirectional or directional reception apparatuses. For RSU to send messages to a specific area, directional receiving wires may be introduced. Moreover, it might be further outfitted with different systems administration gear to speak with TAs and farther RSUs. Each RSU has the capacity ability to store the information from vehicular OBUs just as the TA.

3) Onboard unit: OBUs are handsets introduced in vehicles for trading information with RSUs just as the other vehicular OBUs as a team with processing gadgets. The parts of an OBU involve an asset telling processor for computational limit, read/compose limit with regards to information stockpiling and recovery, a UI, and a DSRC radio that works as per IEEE 802.11p radio innovation so as to recover remote channels [10]. OBUs draw power from the vehicular batteries. Every such vehicle moreover highlights sensors, for example, worldwide situating frameworks (GPS) collectors, sealed gadgets (TPD), occasion information recorders (EDR), and speed just as forward-and back confronting sensors that give contributions to OBUs. The sensors assemble information about encompassing conditions. Of this hardware, the GPS recipient is used to gracefully geographic information as far as the area of vehicles. The TPD is used to record delicate data, for example, the private and gathering keys and IDs of vehicles. EDRs are used to record information related to mishaps or vehicular accidents. Speed sensors are used to accumulate chronicles, for example, speed and trading of information. Forward-and back confronting sensors are used to screen occasions happening to the front and back of vehicles. These checked and gathered chronicles are transmitted as messages to neighboring vehicles through remote media.

Features of VANET:

The qualities/characteristic of a vehicular ad hoc network are one of a kind contrasted with another mobile ad-hoc network. The distinctive properties of a VANET offer chances to increase network execution, and simultaneously it presents extensive difficulties. A VANET is in a general sense distinctive [11] from different MANETs.

- High Mobility: The nodes in VANETs as a rule are moving at fast. This makes harder to foresee a node's position and making assurance of node security.
- Rapidly changing network topology: Due to high node versatility and irregular speed of vehicles, the situation of node changes every now and again. Accordingly, network topology in VANETs will in general change as often as possible.
- Unbounded network size: VANET can be actualized for one city, a few urban areas or for nations. This implies network size in VANET is geologically unbounded.
- Frequent change of data: The ad hoc nature of VANET spurs the nodes to accumulate data from different vehicles and street side units. Thus the data trade among node gets visit.
- Wireless Communication: VANET is intended for the remote condition. Nodes are associated and trade their data through remote. In this manner some safety effort must be considered in transmission.
- Time Critical: The data in VANET must be conveyed to the nodes with in time limit so a choice can be made by the node and perform activity in like manner.
- Sufficient Energy: The VANET nodes have no issue of vitality and calculation assets. This permits VANET use of requesting procedures, for example, RSA, ECDSA execution and furthermore gives boundless transmission power.

VANET Applications

Vehicular ad hoc network used in various purposes in different sectors which is discussed below:

- **Safety Applications**

Safety applications are mainly focused on to minimize the possibilities of road accidents and the loss of lifetime of the occupants of vehicles. A vast amount of accidents that occur in all sections of the world are related to vehicle collisions. This category of applications primarily provides active road safety to avoid collisions by helping the drivers with timely data. Data is distributed among vehicles and road side units that are additionally employed to predict vehicle collisions [11].

- **Traffic Monitoring and Management Applications**

This kind of applications mainly concentrated on enhancing the vehicular traffic flow, traffic coordination and traffic cooperation. It's liable for providing updated local info, maps and suitable messages finite in space and/or time [11].

- **Driver assist applications**

The objective is to enhance driving and help drivers in particular situations, i.e. in the overtaking of cars, avoidance of channel outputs, discovery and alerts of congestions, alerts of potential traffic queues, etc. Among this class are congested road notifications, parking availability notifications, and toll booth collection information.[12]

- **Passenger comfort applications**

These types are meant to comfort drivers and riders, as they basically provision services including mobile Internet messaging, discussion, and access among vehicles, collaborative networked gaming, and so on. In the remaining part of this section, we shall limit discussion to the explanation of certain services, with implementation examples of vehicle-to-vehicle communication systems.[12]

- **Infotainment Applications**

Infotainment applications offer ease and luxury to drivers and travellers. The objective of infotainment applications intend to supply all type of messages that provide entertainment and helpful messages to the driver and traveller. Finding the closest coffeehouse, movie theater, shopping mall, fuel station that offers the perfect cost in that region, or obtainable parking space are some examples of infotainment or documentary applications [11].

Secuirty Attributes and Challenges: In the following subsections, we present securityattributes in Vehicular Ad hoc Networks (VANETs) andtypes of malicious vehicles.

Security Attributes:

There are a few significant necessities to accomplish security in VANETs, which are examined as follows. [13].

• Availability

The system ought to be accessible regardless of whether it is under an attack utilizing elective mechanism without influencing its exhibition.

• Data Integrity

It guarantees that information or messages are not altered by attackers. Something else, clients are straightforwardly influenced by the changed critical information. For instance, if a vehicle B sends a " street clear" message to a noxious vehicle C and C adjust the message as "automobile overload ahead" this message to a genuine vehicle D, it (D) will be influenced by this message since D will change the street and be in a difficult situation later on. Figure 2 shows such a situation of information trustworthiness.

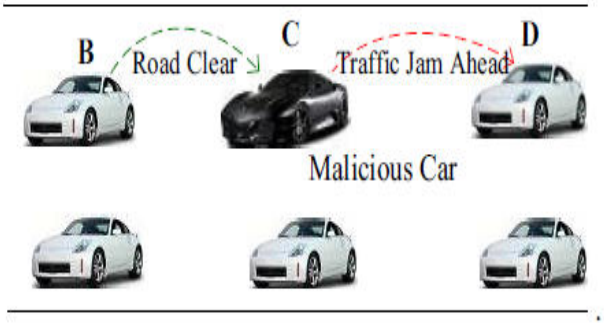

Fig.2 Data Integrity

• Authentication

Vehicles ought to react just to the messages transmitted by authentic individuals from the system. In this way, it is imperative to verify the sender of a message.

• Data Verification

When the sender vehicle is validated the accepting vehicle performs information confirmations to check whether the message contains the right or adulterated information.

• Non-repudiation

A sender must not deny a message transmission at whatever point an examination or personality of a vehicle is required.

• Privacy

The profile or a driver's very own data must be kept up against unapproved get to.

• Real-time constraints

Since vehicles are associated with VANETs for a brief term, ongoing requirements ought to be kept up.

VANETs challenges: The attributes and features of VANETs make a few difficulties which can influence applying security ways to deal with set up secure communications in V2V and V2R. In this we will specify a few difficulties of VANETs [13-18]:

(1) Wireless Link use: VANETs rely upon wireless channel in communication whether in V2V or in V2R as specially appointed systems, and this requires solid security components to get classified channels and have organized honesty.

(2) Multi-jump association: VANETs now and again rely upon communications upon multi-vehicles to send data that every vehicle needs to pass the got messages to potential neighbors in its range. Practices of vehicles must be seen that any misbehaved or got out of hand vehicle ought to be confined and rebuffed.

(3) Delay-Sensitive Applications: some VANETs applications, which are identified with security and travelers' solace, are time-safety that they ought to have estimations of delays with a specific resilience. Along these lines, there ought to defeat strategies that play out their capacities with the message of little overhead and low handling delays. Besides, secure capacities can be built up to make a reconnaissance of got out of hand activities which can diminish the Quality of Service (QoS) for VANETs; and put into thought limitations held for these systems.

(4) Network Scale: VANETs may contain countless vehicles; and this may influence their capacities if there is no powerful classified framework that can circulate cryptographic keys for that huge number. As an outcome of that, a considered framework ought to be done before sending VANETs to make certain of its versatility for any adjustments in the quantity of imparting vehicles.

(5) Network Volatility: the communications between vehicles are transient that the association might be set up for a while, and afterward it is finished because of the speeding

up between them. Along these lines, the chance of having a seemingly perpetual setting in VANETs is little; applying making sure about methodologies relying upon confirming characters is hard.

(6) Liability versus Protection: getting to the vehicle's data, which can be utilized in examinations, ought to be accessible for vehicles that are inside an occasion or can help in removing any data. Additionally, protection must be found for being certain about holding that particular data by approved elements..

Vanet Routing Protocols: VANET applications' fitness and accomplishment rely basically upon the manner by which messages are passed on between the vehicles. A few steering conventions have been built for correspondence between the vehicles in an impromptu situation. In VANET, steering is a troublesome errand to do due to the high portability of hubs, which causes fast changes of geography, so finding and keeping up courses is a difficult assignment and to convey a bundle inside a base timeframe. Different issues are fluctuating thickness and speed of the vehicles out and about and meager dispersion of vehicles in some geological locales which prompts the helpless availability and execution debasement of the system. VANET directing conventions are widely ordered into Topology based, Position-based, Cluster-based, Broadcast, and Geocast based conventions [19]. Figure 2 shows the grouping of routing protocols in VANET.

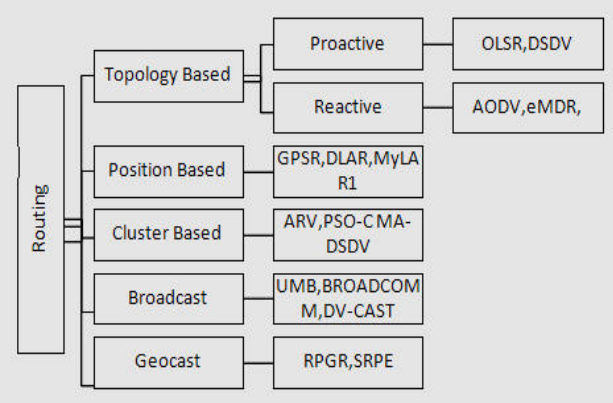

Fig. 2 Classification of Routing Protocols [4]

Topology based routing: Topology based routing is castoff to accumulate source to destination information in the routing table. It can be classified into Proactive and Reactive routing protocols[19].

- Proactive routing protocol

This is used to store entirely the network nodes routing information in the routing table. All the entries in a routing table comprehends next hop node information and make availablea path to the destination. Everynode sustains the absolute image of a network until it accepts the new one.

Advantages [21]

1. It entails less routing overhead
2. It devour less resources because of the absence of large routing tables

Disadvantages [21]

1. More latency time in path finding.
2. Extreme flooding can lead to network congestion

Fisheye State Routing

FSR [24] is a proactive or table-driven routing protocol where the info of every node accumulates from the neighboring nodes. Formerly calculate the routing table. It is based on the link state routing & an enhancement of Global State Routing.

Advantages

1. FSR decreasesexpressively the expended bandwidth as it exchanges incomplete routing update information with neighbors solitary.
2. Diminish routing overhead.
3. Altering in the routing table will not transpire even if there is any connection failure because it doesn’t trigger somewhat control message for link disruption.

Disadvantages

1. Extremely poor performance in trivial ad hoc networks.
2. Fewer knowledge about detached nodes.
3. The growth in network size the storing complexity and the giving out overhead of routing table also improve.
4. Inadequateevidence for route establishing.

- Reactive routing protocol

This protocol is also called the on-request routing protocol. This protocol doesn't think about the geography of the whole system. It begins the route disclosure process when it needs. At the point when the source node needs

to speak with the destination node at that point source node send a solicitation message. Any node that presents on this route towards the destination, in the wake of accepting this solicitation message sends back a route affirmation message to the source node utilizing unicast correspondence. These sorts of routing protocols are helpful for huge measured ad hoc network which have progressively evolving geography.

Advantages

1. To refresh routing table not require occasional flooding the system. Flooding requires when it is requested.
2. Beaconless so it spares the transfer speed. [22]

Disadvantages

1. For route discovering idleness is high.
2. Exorbitant flooding of the system causes interruption of nodes communication.[22]

Ad-hoc on- Demand Distance Vector routing protocol (AODV)

AODV [23] is receptive routing protocols which set up a route when a node requires sending information packets. It has the capacity of unicast and multicast routing. It utilizes a destination sequence number (DestSeqNum) which makes it not quite the same as other on request routing protocols.

Advantages

1. A up to date path to the destination in light of utilizing destination sequence number.
2. It diminishes over the excessive memory prerequisites and the route excess.
3. AODV reactions to the connection failure in the system.
4. It very well may be applied to huge scope ad-hoc network.

Disadvantages

1. Additional time is required for connection setup and initial communication to build up a route contrasted with different methodologies.
2. If intermediate nodes contain old passages it can lead irregularity in the route.
3. For a solitary route answer bundle if there has numerous route answer parcels this will prompt overwhelming control overhead.
4. In view of intermittent beaconing it expend additional transfer speed.

Position Based Routing Protocol: Position Based Routing Protocols Position based routing comprises of class of routing algorithm. They share the property of utilizing geographic situating data so as to choose the following sending hops. The packet is sent with no guide information to the one hop neighbor, which is nearest to destination. Position based routing is valuable since no worldwide course from source node to destination node should be made and kept up. Position based routing is comprehensively separated in two sorts: Position based avaricious V2V protocols, Delay Tolerant Protocols. [25]

Position Based Greedy V2V Protocols

In covetous methodology and middle of the road node in the course forward message to the farthest neighbor toward the following destination. Avaricious methodology necessitates that middle of the road node should had position of itself, position of its neighbor and destination position. The objective of these protocols is to transmit information packets to destination as quickly as time permits that is the reason these are otherwise called min delay routing protocols. Different kinds of position based ravenous V2V protocols are GPCR, CAR and DIR.

Greedy Perimeter Coordinator Routing (GPCR)

GPCR depends on the way that city road structure a characteristic planner diagram. GPCR doesn't require outside static road map for its activity. GPCR comprises of two parts: A Restricted Greedy sending system, a repair methodology for routing algorithm. A GPCR follows a destination based Greedy sending procedure, it courses messages to nodes at convergence. Since GPCR doesn't utilize any outside static road map so nodes at convergence are hard to track down. GPCR utilizes heuristic technique for discovering nodes situated at convergences and assigns those nodes as facilitators. Organizer has the duty of settling on routing choices. There are two methodologies utilized for organizer assurance they are

(a) Neighbor Table Approach: The nodes occasionally transmit guide messages which

contains their position data and last known position data all things considered, by tuning in to reference point messages a n tribute as data about its own position, position of its neighbor and's neighbor. Utilizing this data node X believe itself to be inside the crossing point.

(b) Correlation coefficient approach: For this situation node utilizes its position data and the position data of its prompt neighbor to discover the relationship coefficient, pxy. This methodology performs superior to neighbor table methodology. By utilizing this methodology the algorithm can maintain a strategic distance from conditions on outside road map.

Cluster Based Routing Protocol: This sort of protocol is identified with the clustering approach. The primary thought of this method is to partition the system into clusters called groups, as indicated by a few measurements and standards. For each group, one of the individuals assumes the job of cluster head. It is answerable for correspondence inside the bunch and outside between the various groups. Under a depiction of a lot of steering protocols in VANET dependent on the clustering approach is given.

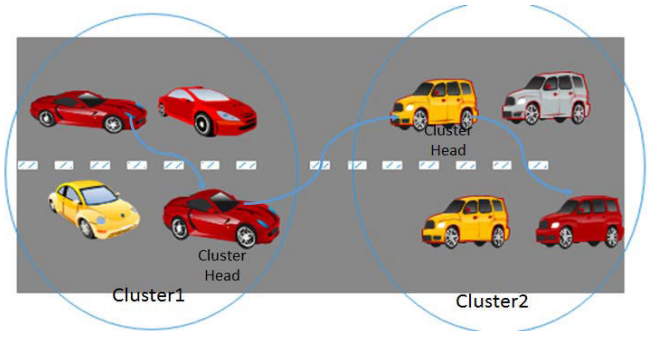

Fig. 3. Cluster-based routing protocol [32]

Cluster-Based Directional Routing Protocol (CBDRP)

In [20], proposed a Cluster-Based Directional Routing Protocol in VANET (CBDRP). It utilizes a straightforward clustering procedure, which separates the system into clusters called groups as indicated by the moving bearing of vehicles and afterward assigns a vehicle among individual from cluster to be a cluster head (CH) in each cluster. This proposed protocol chooses the closest vehicle to the focal point of cluster as CH. Following the instatement stage, the protocol begins the information transmission stage. This last mentioned, is made out of four stages: directing solicitation, steering foundation, steering upkeep and connection detach. During the information transmission stage, the source vehicle sends information packet to its cluster head, which thus forward information to the following group head of transitional cluster. At the point when the packet shows up at the group top of the cluster where the destination node is found, the CH hands information packet to the destination.

Advantages

System overhead is decreased because of the immediate transmission of the packet to cluster head.

Disadvantages

It happens when the vehicle can't arrive at the group head and is obliged to communicate the packet with a great strategy. Also, the group execution is influenced by the dynamic difference in cluster head.

Broadcast based routing protocols: This is the most ordinarily utilized routing protocol in VANETs, especially in security related applications.[26] In broadcast mode, a packet is sent to all (even obscure or unknown) nodes in the system and thusly every node re-broadcasts the message to different nodes in the system. Flooding is an inimitable technique utilized in broadcast routing protocols. [27] However, daze flooding brings about broadcast storm issue. A broadcast tempest can over-burden the restricted channel limit, causing channel clog that lessens correspondence reliability.[28] Broadcast routing is as often as possible utilized in VANET for sharing, traffic, climate and emergency, route conditions among vehicles and conveying commercials and announcements.[29] The different Broadcast routing protocols are BROADCOMM, UMB, VTRADE, and DV-CAST.

Advantages

1. Since packet is conveyed through numerous nodes so the parcel transmission is reliable.

2. Limit overhead by event of broadcast storms
Disadvantages
1. Devour the huge measure of network bandwidth.
Distributed Vehicular Broadcast in VANET (DV-CAST)
Another Distributed Vehicular Broadcast protocol known as the DV-CAST appropriate for the roadway condition and health application in VANET.[31] In DVCAST, routing stage utilized availability data's of single bounce neighboring. During the routing technique, DV-CAST presents three new fundamental boundaries: Destination Flag (DF), Message Direction Connectivity (MDC) and Opposite Direction Connectivity (ODC). It utilizes these boundaries to spread the messages in a productive and safe manner. It expect that every vehicle in the system is outfitted with a GPS gadget, so as to gather the essential data about the neighborhood availability during the routing technique.
Advantages
Extremely suitable for thick and meager traffic situations. Also, DV-CAST protocol diminishes the system overhead.
Disadvantages
This protocol is that every vehicle needs a GPS framework, which is extravagant.
Multicast/geocast routing protocols: Multicast routing enables dispersal of messages from single source to a group of beginning stage nodes of interest.[30][26] Geocast routing is essentially an area based multicast routing, which intends to convey data from a source node to every single other node inside a predefined geological locale called a Zone of Relevance (ZOR). A Zone of Forwarding (ZOF) is differentiated, inside which the packets are coordinated rather than essentially flooding the packets wherever in the system. In Geo cast routing vehicles outside the ZOR are not made aware of evade pointless rushed response. [30][29] Geo give is viewed as a role as a multicast administration inside a particular geographic locale. It regularly characterizes a sending zone where it coordinates the flooding of packets so as to lessen message overhead and system blockage brought about by essentially flooding packets wherever [25].
Advantages
1. Diminished system overhead and clog.
2. Dependable packet conveyance in profoundly powerful geography.
Disadvantages
Packet transmission delay because of system disengagement.
Inter-Vehicule Geocast(IVG)
The fundamental objective of IVG routing protocol [32] is to advise all vehicles situated in the hazard territory (Fig. 4) about any perilous circumstance happens, for example, a mishap. This hazard territory alleged multicast bunch is resolved progressively as far as area, speed and driving bearing of vehicles, which can be influenced. Every node gets an alert message ought not to rebroadcast it quickly yet needs to stand by some time which decreases the quantity of unwarranted caution message. The benefit of IVG routing protocol is that it can keep away from activities of the support, for example, routing and neighbor calculation. Be that as it may, these methods are incredibly exorbitant in profoundly unique situations, for example, transportation frameworks.

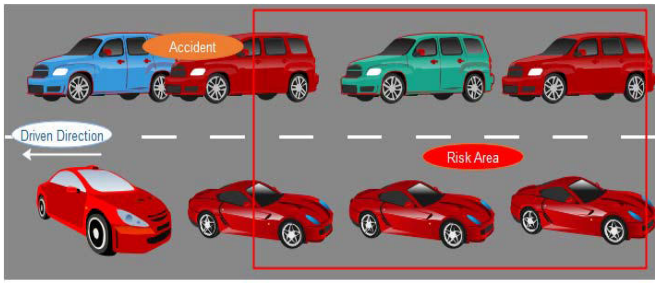

Fig. 4. IVG multicast Protocol [32]

Security Attacks in VANET: Because of open remote nature, there exist number of security threats and attacks which are very non-inconsequential for VANETs. In this segment, we give a review of attacks that may follow in the scene of VANETs. Clearly, all potential attacks can't be canvassed in this paper. Subsequently, we are identifying some nonexclusive and big attacks that are ordinarily accessible in writing. For curtness, we depict the conceivable idea of attacks and their imaginable situations.

Authentication Attacks: Authentication is an obligatory prerequisite to give successful security. In VANETs, security applications particularly require proficient verification instrument in light of the fact that most wellbeing related messages contain life basic data. Without satisfactory authentication instruments, attackers can dispatch various sorts of attacks. Some potential validations attacks are specified here.

1. Impersonation Attack: The attacker claims to be another substance in Impersonation attack. By utilizing MAC and IP parodying, the aggressor conceals his unique identity – utilizes personality of another node – to play out any criminal behavior in the system. In the event that, if validation endorsements are utilized by clients, Impersonation attacks are practically inconceivable on the grounds that authentications can't be fashioned.

2. Masquerading: In this sort of attack, attacker claims to be another vehicle by utilizing false identity. Targets of attacker can be vindictive or objective [34]. By imagining another vehicle, attacker can dispatch various attacks like message creation, modification and replay. For instance, the aggressor professes to be crisis vehicle to delude different vehicles to back off or leave place for it [39].

3. Sybil attack: In such attack, attacker utilizes numerous identities to send various messages; various personalities are utilized simultaneously. Thusly, the aggressor make a deception that messages are being sent from various nodes. The fundamental goal of the attack is to misdirect different vehicles. This attack can disturb routing protocols, may likewise prompt circulated DoS and unreasonable dissemination of assets and so forth [39].

4. GPS Spoofing: Malicious client attempts to delude the real clients – in a manner that – they think they are in an alternate area. This is conceivable by giving false GPS data to clients. This attack can be propelled by utilizing a GPS satellite test system that produces more grounded signal than that of the certified satellite [39].

Attacks on confidentiality: Essentially, the listening stealthily (getting illicit access to client's information) is an attack on client's privacy. The aggressor can records and utilize the data about vehicles without their proprietor's authorization. Later on, this data is utilized by the market merchants and organizations for information mining and example discoveries purposes.

Denial of Service (DoS): In DoS attacks, the principle target of the sly aggressor is to upset the correspondence channel or overpowers the vehicle's accessible administrations from the real clients. The fundamental reason for this attack is to make the framework pointless, yet because of the constant nature VANET administrations, pointlessness of the framework – in any event, for a little moment of time – isn't moderate for clients. A couple of praiseworthy situations of DoS are listed beneath.

1. By truly Jamming the correspondence channel by creating the high recurrence signals in the channel that denies genuine node to get to it.

2.The system can be overwhelmed by communicating message parcels which take up a vehicle's processing assets and over-burdens the correspondence channel. Thusly, the basic data can't be passed on to different vehicles on schedule. Additionally, it can cause or increment threat to the driver on the off chance that she/he is relying upon the application's data for dynamic. For instance, if a malignant foe needs to make a gigantic accident on the thruway he can likewise incite a mishap – by a DoS attack, he just needs to keep the suitable deceleration alerts from arriving at different drivers [36][37][40][35].

3. Black hole Attack: Another accessibility issue is Black hole attack in which an aggressor utilizes its own routing protocol, so as to publicize itself or for having most brief way to the goal node. These egotistical nodes don't offer their types of assistance to assist different nodes so as to spare their own assets.

4. Jamming Attack: Jammers purposely create meddling transmissions or signs to forestall correspondence over the system. Since, the

system inclusion regions are all around characterized in VANETs; in this manner, an aggressor can undoubtedly – without trading off cryptographic instruments and with constrained transmission power – parcel the vehicular system. This is on the grounds that Jamming is known as low-exertion misuse.

5. Malware: Different classifications of pernicious programming – (for example infection, worm and trojans and so forth populated in organize) – can cause threats for administration accessibility in VANET. Besides, these malevolent projects can cause traffic related threats extending from blockage to enormous scope mishaps. Inside attacker normally present malware in organize yet some worm-like malware can spread in VANET without human mediation (as a rule infused into the system when vehicles get refreshes) [33].

Attacks on Privacy: The hackersillicitly get the delicate data about vehicle or driver. Some example attacks are recorded here.

1. Location tracking: Attacker can find and track a vehicle through messages – which it transmits during transmission – with some other vehicle or side of the road unit. By tracking a vehicle, it gets conceivable to manufacture vehicles profile; along these lines, the security of the driver of vehicle is penetrated.

2. Identity uncovering: For the situation of identity uncovering attack, the aggressor gets vehicle's personality and put its protection in danger. In a large portion of the cases, driver of the vehicle is its proprietor; so thusly, the assailant is getting individual information of the vehicle's proprietor.

Conclusion: VANET is a data driven intelligent transport system for the users but there is a big challenge for the safety, security and reliability. Because of its scalable in nature most of the security threats may compromise from the networks. So need to develop such framework or protocols which can efficiently and effectively handle such challenges. In this paper, we present the survey on VANET security, challenges, protocols and applications. We have discussed various protocols like topology based; cluster based etc. similarly discusses the various security threats like, denial of service attack, attacks on availability, privacy and confidentiality and also discusses the various applications of VANET in different sectors. After analysis of various protocols and security threats it is found that need to design the hybrid routing protocols which uses the effective features of the any two or more protocols to prevent the network from compromising the networks.

REFERENCES

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

[2] Marshall Riley, Kemal Akkayaand Kenny Fong, "A Survey of Authentication Schemes for Vehicular Ad hoc Networks",Security and Communication Networks Published online 15 July 2010 in Wiley Online Library.

[3] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures "Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)" National Advanced IPv6 Center, University Sains Malaysia Penang, Malaysia. June 28, 2010.

[4] Mohammed Saeed Al-kahtani, "Survey on Security Attacks in Vehicular Ad hoc Networks (VANETs)",In proceeding of IEEE, 2012.

[5] Leiding, B., Memarmoshrefi, P., & Hogrefe, D. "Self-managed and blockchain-based vehicular ad-hoc networks" Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing Adjunct - UbiComp '16. doi:10.1145/2968219.2971409

[6] X. Liang, T. Yan, J. Lee, and G. Wang, "A distributed intersection management protocol for safety, efficiency, and
driver's comfort," IEEE Internet of Eings Journal, vol. 5, no. 3, pp. 1924–1935, 2018.

[7] T. Neudecker, N. An, T. Gaugel, and J. Mittag, "Feasibility of virtual traffic lights in non-line-of-sight environments," in Proceedings of the Ninth ACM International Workshop on Vehicular Inter-Networking, Systems, and Applications—VANET'12, pp. 103–105, Lake District, UK, June 2012.

[8] Dsrc, http://grouper.ieee.org/groups/scc32/dsrc/.
[9] Ghosh, M., Varghese, A., & Kherani, A. A. "Distributed misbehavior detection in VANETs" IEEE Wireless Communication and Networking Conf., WCNC 2009, Budapest, Hungary.
https://doi.org/10.1109/WCNC.2009.4917675.
[10] Dhamgaye, A., & Chavhan, N. (2013). Survey on security challenges in VANET, Int. J. Comput. Sci. 2,88–96, ISSN 2277-5420.
[11] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures, "Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)", National Advanced IPv6 Center, University Sains Malaysia Penang, Malaysia. June 28, 2010.
[11] Gaganpreet Kaur, Dr. Sandeep Singh Kang, "Study of various Data Dissemination types and its Protocols- A Review" International Journal of Information Management and Technology, ISSN NO. 2356-2600, Volume 1, Issue 1, Aug 2016
[12] Zaid A. Abdulkader, Azizol Abdullah, Mohd Taufik Abdullah & Zuriati Ahmad Zukarnain, "Vehicular Ad Hoc Networks and Security Issues: Survey", Modern Applied Science; Vol. 11, No. 5; 2017 ISSN 1913-1844 E-ISSN 1913-1852.
[13] Maxim Raya et al., "The security of vehicular ad hoc network", Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks (SASN '05), 2005.
[14] M. Raya et al, Securing vehicular communications, IEEE Wireless Commun. Mag., Special Issue Inter-Veh. Commun.
13 (2006) 8–15.
[15] D. Djenouri et al, A survey of security issues in mobile ad hoc networks, IEEE Commun. Surv. 7 (2005) 2–28.
[16] K.C. Lee, et al., Survey of routing protocols in vehicular ad hoc networks, Advances in vehicular ad-hoc networks: developments and challenges, 2010, pp. 149–170.
[17] Y.-W. Lin et al, Routing protocols in Vehicular Ad Hoc Networks: a survey and future perspectives, J. Inf. Sci. Eng. 26 (2010) 913–932.
[18] P. Nithya Darisini, N.S. Kumari, A survey of routing protocols for VANET in urban scenarios, in: Pattern Recognition, Informatics and Mobile Engineering (PRIME), 2013 International Conference on, 2013, pp. 464–467.
[19] Sourav Kumar Bhoi, Pabitra Mohan Khilar, "Vehicular communication: a survey", IET (The Institution of Engineering and Technology), Vol.3, Iss.3, pp. 204–217, 2014.
[20] T. Song, W. Xia, T. Song and T.Shen. "A ClusterBased Directional Routing Protocol in VANET." in IEEE International Conference on Communication Technology (ICCT), 2010; pp. 1172-1175.
[21] Mohammed Aziz Ahmed, Mohammed Sirajuddin, Nazia Kouser, "A Review on Reactive & Proactive Routing Protocols and Security Breaches and Remedies in MANETs", International Journal of Computer Science and Information Technologies, Vol. 7 (4) , 2016, 1962-1965.
[22] Bijan Paul, Md. Ibrahim, Md. Abu Naser Bikas "VANET Routing Protocols: Pros and Cons", International Journal of Computer Applications (0975 – 8887) Volume 20– No.3, April 2011.
[23] Perkins, C.; Belding-Royer, E.; Das, S. (July 2003)"Ad hoc On-Demand Distance Vector (AODV) Routing".
[24] Pei, G., Gerla, M., and Chen, T.-W. (2000), "Fisheye State Routing: A Routing Scheme for Ad Hoc Wireless Networks," Proc. ICC 2000, New Orleans, LA, June 2000.
[25] Rakesh Kumar, Mayank Dave, "A Comparative Study of Various Routing Protocols in VANET", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011 ISSN (Online): 1694-0814.
[26] Venkatesh, Indra. A ,Murali. R, "Vehicular AdHoc Networks (VANETs): Issues andApplications", Journal of Analysis and computation, Vol. 8, No. 1, 2012, pp.31-46.
[27] A. K. Saha and D. B. Johnson, "Modeling mobility for vehicular ad hoc networks," ACM

International Workshop on Vehicular Ad Hoc Networks (VANET), Oct. 2004, pp.91-92.
[28] Venkatesh, AIndra, R Murali, "Routing Protocols for Vehicular Adhoc Networks (VANETs): A Review", Journal of Emerging Trends in Computing and Information Sciences Vol. 5, No. 1 January 2014 ISSN 2079-8407, pp 25-43.
[29] Surmukh Singh, Sunil Agrawal, "VANET Routing Protocols: Issues and Challenges", Proceedings of 2014 RAECS UIET Panjab University Chandigarh, 06 – 08 March, 2014 978-1-4799-2291-8/14/$31.00 ©2014 IEEE, pp 205-210.
[30] Surmukh Singh, Poonam Kumari, Sunil Agrawal, "Comparative Analysis of Various Routing Protocols inVANET", 2015 Fifth International Conference on Advanced Computing & Communication Technologies 2327-0659/15 $31.00 © 2015 IEEEDOI 10.1109/ACCT.2015.113, pp 315-319.
[31] O. Tonguz, N. Wisitpongphan, F. Bai, P. Mudalige and V. Sadekar. "Broadcasting in VANET." in Mobile Networking for Vehicular Environment (MNVE), 2007, pp. 7-12.
[32] A. Bachir and A. Benslimane, "A multicast protocol in ad hoc networks inter-vehicle geocast," IEEE Semiannual Vehicular Technology Conference, vol. 4, pp. 2456–2460, 2003.
[33] S. A. Khayam, H. Radha, Analyzing the Spread of Active Worms over VANET, ACM Mobicom International Workshop on Vehicular Ad Hoc Networks, 2004.
[34] M. Raya, P. Papadimitratos, and J.-P. Hubaux, Securing vehicular communications, IEEE Wireless Communications Magazine, vol. 13, no. 5, pp. 8-15, 2006.
[35] M Raya, J Pierre Hubaux, The security of VANETs, Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks, 2005.
[36] M. Raya, P. Papadimitratos, JP. Hubaux, Securing Vehicular Communications, IEEE Wireless Communications, Vol. 13, 2006.
[37] B. Parno and A. Perrig, Challenges in Securing Vehicular Networks, Proc. Of HotNets-IV, 2005.
[38] Zeadally S., Hunt R., Chen Y., Irwin A., and Hassan A.,Vehicular Ad Hoc Networks: Status, Results, and Challenges, 2010.
[39] D. Gada et al., A Distributed Security Scheme for Ad Hoc Networks, ACM Crossroads, Special Issue on Computer Security. Volume 11, No. 1, pp. 1-10, 2004.
[40] I Aad, JP Hubaux, EW Knightly, Impact of Denial of Service attacks on Ad Hoc Networks, IEEE/ACM Transactions on Networking, Vol. 16, 2008.
[41] Harsh Pratap Singh and Rashmi Singh, "A mechanism for discovery and prevention of coopeartive black hole attack in mobile ad hoc network using AODV protocol",International Conference on Electronics and Communication Systems (ICECS), 2014. Pp. 1-8. In proceeding of IEEExplore.