A Survey of Congestion Avoidance in Vanet and Vanet Security Algorithm

[1]Nisha.R, [2]Kiruthika.M, [3]Vijaysankar.U, [4]Velayudham.A

[1]PG Scholar, [2]Assistant Professor, [3]Associate Professor, [4]Department Head
Computer Science and Engineering,
Jansons Institute of Technology, Coimbatore, India

***Abstract*: A Vehicular Ad-Hoc Network or VANET is a sub form of Mobile Ad-Hoc Network or MANET that provides communication between vehicles and between vehicles and road-side base stations with an aim of providing efficient and safe transportation. A vehicle in VANET is considered to be an intelligent mobile node capable of communicating with its neighbors and other vehicles in the network. VANET introduces more challenges aspects as compare to MANET because of high mobility of nodes and fast topology changes in VANET. Various routing protocols have been designed and presented by researchers after considering the major challenges involved in VANETs. Information shared in this system is time sensitive and requires robust and quick forming network connections. VANET, being a wireless ad hoc network, serves this purpose completely but is prone to security attacks. Highly dynamic connections, sensitive information sharing and time sensitivity of this network, make it an eye-catching field for attackers. This paper represents a literature survey on VANET with primary concern of the security issues and challenges with it. Features of VANET, architecture, communication, routing protocols, security requisites, attacker type and possible attacks in VANET are considered in this survey paper.**

Index Terms: VANET, Characteristics, Component, Protocols, security, Challenges. (Key words)

I.INTRODUCTION

Vehicular Ad hoc network consist of mobile nodes (vehicles embedded with sensors), fixed infrastructure (Road Side Access Point) and wireless interconnection to allow them to talk with each other. The most important service provided by these networks is driving safety. Almost 1.3 million people die in road accidents and additional 20-50 millions are injured worldwide. Road Traffic crashes ranked as 9th leading cause of death [1]. Some survey shows that 60% of accidents can be avoided if the driver gets the warning even before half a second of the accident [2]. VANET are subset of ad-hoc network working over vehicular domain. VANET has emerged as a solution and become a key component of Intelligent Transportation System (ITS). Main objective of ITS is improving traffic efficiency and providing better road safety. VANET serves the purpose by sharing road safety information, information related to traffic analysis, normal data (files, audio, video etc) using uninterrupted internet connectivity.

VANET differs from other ad-hoc wireless networks of the same class in these terms:

• High processing power

• Large storage capacity

• Energy sufficiency (as work over battery of vehicle).

• Predictable movement of nodes (as vehicles are bound to follow a certain path along the road).

VANET is mainly aimed at providing safety related information and traffic management. Safety and traffic management entails real time information and directly affect lives of people travelling on the road. Simplicity and security of VANET mechanism ensures greater efficiency. Safety is realized as prime attribute of Vehicular Ad Hoc Network (VANET) system. The majority of all nodes in VANET are vehicles that are able to form self organizing networks without prior knowledge of each other. VANET with low security level are more vulnerable to frequent attacks. There are wide range of applications like commercial establishments, consumers, entertainment where VANE Tare deployed and it is very necessary to add security to these networks so that damage to life and property could not occur [3].

Architecture Of VANET

Ad hoc environment: It consists of intelligent vehicles (nodes) that have basically two components:

On Board Unit: It has communicational capabilities.

Application Unit: work behind OBU and executes program that enable OBU to communicate. Infrastructure environment: It consists of Road Side Units and Access network.

Two type of communication occur in VANET:

V2V: Pure wireless communication between vehicles.

V2I: Communication between mobile nodes and infrastructure unit RSU.

Main concern in VANET is spontaneous networking, use of infrastructures like RSU or cellular network is less concerned.

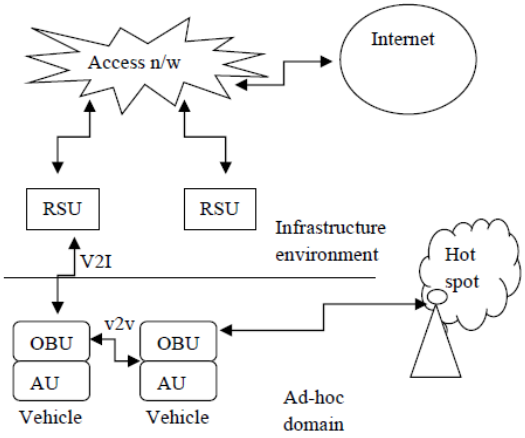

Figure1: Architecture of VANET

II. CHARACTERISTICS OF VANET

There are various appealing and attractive features that make a difference from other types of networks.

1) High Mobility:

The nodes present in VANETs move at a very high speed. These moving nodes can be protected saved from attacks and other security threats only if their location is predicable. High mobility leads to various other issues in VANET [4,[5].

2) Rapidly Changing Network Topology:

Vehicles moving at high speed in VANET lead to quick changes in network topology[5],[7].

3) No Power constraints:

Power constraint always exists in various networks but in VANETs vehicles are able to provide power to on board unit(OBU) via the long life battery so energy constraint is not always an essential challenge as in MANETs.[5]

4) Unbounded Network Size:

The network size in VANET is geographically unbounded because it can be generated for one city or one country [6

5) Time Critical:

Timely delivery of information is very essential. Actions can be performed accordingly only when information is available when it is required.[5,[7].

6) Frequent changing information:

Ad-Hoc nature of VANET motivates the nodes to gather information from other vehicles and roadside units. As vehicles move and change their path, information related to traffic and environment also changes very rapidly.

7) Wireless Communication:

Nodes are connected and exchange their information through wireless.

8) Variable network density:

The network density is changed according to traffic density; it is very high in traffic jam and low in suburban traffic.[7],[8]

9) High computability ability:

Due to computational resources and sensors, the computational capacity of the node is increased.

Routing protocols of VANET:

Protocols	Definition	Example	Pros	Cons
Ad-hoc routing[3]	Used for frequent link breaking as expected	AODV, ,DSR	Improve packet driving ratio communication	Time consuming
DTN	Uses carry & forward strategy to overcome frequent is connection	VADD,GeOpps	Overcome frequent disconnection	Frequent updating by intermediate nodes are not performed with mobility of destination nodes
BEACON	Transmit short hello messages periodically	PBRDV, GRANT, GPSR	Predicting presence & position of nodes	Deletion of entry after every traffic failure
OVERLAY[2]	Connects network by virtual or logical links	GPCR,GSR ,CAR	Good Performance for multi hop data delivery	Due to change of topology & traffic density it causes large delay
Reactive protocol[2]	Also called demand routing because nforces route discovery when needs to communicate with other node	DSR,TORA	Saves bandwidth	High Latency
Proactive	Based on shortest path algorithms and forms tabular structure	FSR, OLSR	No route discovery overhead	Unused paths occupy a significant part of the available bandwidth[
Geocast based	Location based multicast routing protocol where each node deliver message to other node that is isolated in a specific geographic region	TIGER,DRG	Scalability	Requires position determining services
Cluster based	Many groups of nodes are made, every cluster is represented by a clusterhead	COIN,LORACBF	Increase tolerance limit, & dynamic movement schemes	Doesn't consider velocity and direction metrics
Broadcast based	Specially used to communicate safety related message	UMB,HVTRADE	Overcome simple flooding problem	Higher collision overhead

III. COMMUNICATION IN VANET

Various types of communication technique are used in VANET. Some of them are given below:

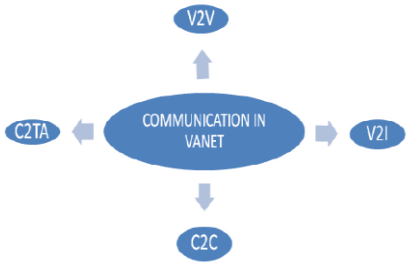

FIGURE:2 Communication in VANET

1. VEHICLE TO VEHICLE COMMUNICATION:
It refers to inter vehicle communication. Vehicles or a group of vehicles connect with one another and communicate like point to point architecture. It proves to be very helpful for cooperative driving.
2. VEHICLE TO INFRASTRUCTURE COMMUNICATION:
Number of base stations positioned in close proximity with a fixed infrastructure to the highways is necessary to provide the facility of uploading/downloading of data from/to the vehicles. Each infrastructure access point covers a cluster.
3. CLUSTER TO CLUSTER COMMUNICATION:
In VANETs network is split into clusters that are self managed group of vehicles. Base Station Manager Agent[10],[11].(BSMA) enables communications between the clusters. BSMA of one cluster communicates with that of other cluster.

Security in VANET

Insecure transmission of information through VANET communication may result into catastrophe. So these information need to be accurate, efficient and reliable. Every single work in domain of VANET has an objective to provide road safety efficiently through frequent sharing of information among nodes of the network. Any successful attack can lead to serious accidents, loss of life or economical loss.
Security is needed in Vehicular Ad-hoc network for following reasons[9]:
• Sensitive information is being broadcasted in VANET which in turn attract various attackers.
• No authentication and association measures are provided in WAVE standard due to fast network establishment need.
• Easy to attack due to infrastructure less model.
• Very high chances of threat to privacy.
• Connections intrusion is very easy due to frequently changing topology.
VANET focuses on improving transportation safety, collision avoidance, traffic efficiency and providing entertainment. Some prerequisites must be ensured by the deployed security system.
• **Authentication:** Authentication gives us an assurance that the information/message is generated by a genuine user. In VANET nodes respond according to the information received from the other end, so it is very necessary that the information propagating in the system is true and generated by a legitimate user.
• **Reliability:** Data receive in communication should be correct and factual. Periodic verification of the system is done to eliminate the factually incorrect information.
• **Integrity:** The information received should not be altered by any unauthorized user. Such alteration can harm the system and can cause serious catastrophic casualties.
• **Anonymity:** Most of the time owners are driving vehicles in such environment. So security measure must ensure privacy of all genuine nodes.
• **Availability:** These system handle urgent data, so data should be available to all authorized user easily and efficiently.
• **Delay handling:** Safety information is time sensitive, so latency should be avoid and handled.
• **Confidentiality:** Sensitive data should not be accessed by unauthorized user.
VANET has a set of various features that provides the base to stand alone in the field of its class. But sometimes these features create obstacle in deployment of VANET. Such challenges are categorized as Technical challenges (covering management of dynamicity of network, latency management, congestion and collision analysis, atmospheric impact and
Security challenges) and Social and Economical Challenges (covering cost impact and social acceptance of VANET) VANET provides safety and traffic analysis measures, so the information communicated must stay secure and the network needs to be robust .We have considered the security challenges to attain an efficient and secure VANET system.
Major securities challenges need to be conquered by security system of VANET are :
• **Consistency of data:** Any malicious alteration in life critical information can lead to accidents, to avoid malicious activity from authenticated and no authenticated nodes that cause inconsistency in data, some mechanism need to be designed. Cross checking of received information from various nodes is done to avoid such activities.
• **High Mobility:** VANET are highly mobile network so they need less complex algorithm for security in spite of being capable of high processing and storing power.
• **Error Tolerance:** Receive and response action in VANET is very quick, so any mistake in protocols or algorithm can harm the system harshly. So protocols need to be designed taking this issue in consideration.

• **Latency Control:** Information shared in this network is time sensitive. To achieve real time restraint, cryptographic and other algorithm used in security must be fast and efficient.
• **Key Management:** All algorithms used in VANET security are key dependent. So creation, maintenance and distribution of keys need to be handled specially.

Challenges in VANET:

There are many issues in VANET. Some of them are given below:
1) Technical Issue: Due to high portability, the network topology and channel condition changes rapidly. It is difficult to manage network and control congestion collision in network. In VANET the electromagnetic waves of communication are used and these are affected by environment. Environmental impact need to be considered in VANET. Other technical issues are related to design and architecture of Mac layer[10].
2) Security Issue: VANET is time critical where safety related message should be delivered with 100ms transmission delay. Even authenticate node can perform malicious activities than can disturb the network. The major challenge is to distribute privacy keys among vehicles
3) Security Requirement issue: Authentication ensures that the message is created by the authorized user. Do attacks can bring down the network. Non repudiation means a node can't deny that she/he doesn't transmit message. It may be crucial to determine correct sequence. A regular verification of data is required to eliminate the false messaging
4) Attackers on VANET:
Insider and outsider: Insiders are the authenticated members of network whereas Outsiders are the intruders and hence limited capacity to attack. Malicious and Rational: Malicious attackers have not any personal benefit after attack; they just harm the functionality of the network. Rational attacks can be predicable as they have the personal profit .Active and Passive: Active attackers generate signals or packet whereas passive attackers only sense the network.
5) Attacks in VANET: Hijackers hijacks the session easily after connection establishment. Generally, a drivers itself owner of the vehicles so getting owner's identity can put the privacy at risk. Eavesdropping is a most common attack on confidentiality. Routing attacks are the attacks which destroy the vulnerability of network layer routing protocols.

IV. ATTACKS IN VANET

Different types of attacks are possible in ad-hoc environment, especially in vehicular domain. Impact of these attacks over the system primarily depends over the intensions of the attackers behind the Attackers composes' malicious behavior for several reasons such that to get benefit of the system facilities for which he is not a legitimate user, to get confidential data of the system or just to disturb the efficient functionality of the network.
These attackers can be classified:
On the basis of Membership: Any authorized or unauthorized node can perform malicious activity in the network. Membership function highly affects the impact of the attack and its prevention. There are two types of attackers on this basis;
Internal Attackers (Im): These are the authorized member nodes that perform malicious activity to gain personal benefit or just to disturb the network. These attackers put stronger impact than the external one.
External Attackers (Em): They are the intruders who try to enter in network either by impersonation or other attacks.
On the basis of Activity: Whether an attacker is active and makes frequent changes to network or not, the attackers are classified as:
Active Attacker (Aa): These types of attackers try to alter the network information and generate malicious packets and signals. Attacks made by them are more effective than that made by passive attackers.
Passive Attackers (Pa): These types of attackers do not alter the network information. They silently sense the network
On the basis of Intensions: Any attack is associated with the intension of the attacker, i.e. main objective of the attacker behind that attack. Following type of attackers are identified on this basis:
Rational Attackers (Ri): These attackers seek personal benefit from the attacks and hence are more predictable.
Malicious Attackers (Mi): These attackers not gain personal benefit from attacks. Their main motive is to create obstacle in proper network functionality.

V. VANET SECURITY SOLUTION

As discussed above, VANET are susceptible to various kinds of attacks. Since research in this field has new and interesting scope, various effective works has been done to provide security solution in VANET. In this section some solution are being discussed for VANET security.
ARAN: This routing protocol, named as Authenticated Routing for Ad-hoc Network (ARAN), is an AODV based protocol [16]. In this approach, a third party CA is present that provide signed certificate to nodes. Each node coming into the network need to sent request certificate to CA. Public key of CA is known to all authorized nodes. Asymmetric cryptographic technique is used for authenticated secure route discovery and timestamps are used for freshness of route.
ARAN basically has 5 steps;

- Certification
- Authenticated Route Discovery
- Authenticated Route Setup
- Route Maintenance

- Key Revocation

Route authentication process is done at each step, through addition of sign and certificate of each intermediate node, so Impersonation problems are solved by this protocol.

SEAD: Secure and Efficient Ad hoc Distance vector protocol work over DSDV. It uses one way hash function for authentication process. This protocol protects against incorrect routing. It uses estimation-sequence number to ensure freshness of the route and to avoid long lived route. At each intermediate node hashing is applied to ensure the authenticity of routes.

Ariadne: This protocol works over on-demand routing protocol DSR . Symmetric cryptographic operations work very efficiently in this protocol. One way hash function and MAC are used for authentication and are communicated between nodes using shared key[9]. TESLA broadcast authentication technology is basis of this protocol. In route discovery and authentication process TESLA time interval are used.

SAODV: This protocol was proposed to embed security measures in AODV protocol . All routing messages are digitally signed to insure authenticity and to protect hop count hash functions are used. In this approach intermediate node cannot send route reply even if the fresh route is known to them. Through Double Signature this problem can be solved but it increases the complexity of the system.

A-SAODV: This protocol is an extension to SAODV that has an experimental feature of *adaptive reply decision.* Each intermediate node can decide whether to send reply to source node or not, depending on the queue length and threshold conditions.

One Time Cookie: Generally for session management, cookies are assigned per session. But to prevent the system from session hijacking and theft of SID, this protocol gives the concept of OTC (one time cookie) . OTC generate token for each request and these token are tied to request using HMAC to prevent the re-use of the token.

VI. CONCLUSION

VANET are very effective means of communication between moving vehicles. VANET being a safety information sharing medium, needs secure and safe environment. VANET has very wide scope for attacks due to its highly dynamic nature, wireless medium of communication and frequently changing topology .In this paper various protocols have been presented and analyzed. Various research issues and security requirements have been described.. From this survey it has been realized that standard protocols must exist that enables effective communication for various

Applications all together in a multidimensional way and overcome issues related to those applications. VANET would provide better platform and effective communication between vehicles with further advancement and evolution of new approaches.

References:

1. Road Crash Statistics- Association for Safe International Road Travel.Available: http://asirt.org/initiatives/informing-road-users/road-safety-facts/roadcrash- statistics

2. Maxim Raya et al., “The Security of Vehicular Ad Hoc Networks”, SASN’05, Nov 7 2005, Alexandria, Virginia, USA, pp. 11-21

3. Stampoulis, Antonios, and Zheng Chai, ‘A Survey of Security in Vehicular Networks’, *Project CPSC*, 2007.

4.J. Jakubiak and Y. Koucheryavy , ‘ State of the Art And Research Challenges for VANETs’, Consumer Communications and Networking Conference, *Proc. 5th IEEE CCNC*, pp.912 -916, 2008.

5. S. Yousefi , M. S. Mousavi and M. Fathy, ’Vehicular Ad Hoc Networks (VANETs): Challenges and Perspectives’, *Proc. 6th IEEE Int. Conf. ITST*, pp.761 -766, 2006 .

6. Raw, Ram Shringar, Manish Kumar, and Nanhay Singh, ‘Security Issues and Solutions in Vehicular Ad hoc Network: A Review Approach’, *ICCSEA, SPPR, CSIA* , 2013.

7. S. Olariu and M. Weigle , ’ Vehicular Networks: From Theory to Practice’, Chapman & Hall/CRC, 2009

8. Nekovee, Maziar, ’Sensor Networks on the Road: The Promises and Challenges of Vehicular Ad Hoc Networks and Vehicular GridsProceedings of the Workshop on Ubiquitous Computing and e-Research, 2005.

9. M. Feiri, J. Petit, R. K. Schmidt, F. Kargl, “The impact of security on cooperative awareness in VANET”, Vehicular Networking Conference (VNC), 2013 IEEE, pp. 127-134, Dec 2013.

10. H. Moustafa and Y. Zhang, ’Vehicular Networks: Techniques, Standards, and Applications’, 2009 .

11. Raya, Maxim and Jean-Pierre Hubaux, ’Securing vehicular ad hoc networks’, Journal of Computer Security, pp.39-68, 2007.