Vehicular Ad-hoc Network, its Security and Issues: A Review

Prof. Vishal Shrivatava[1]
1M.Tech. Coordinator.,
Department of CSE,
Arya College of Engineering & IT

Ajay Samota
2 M.Tech. Scholar,
Department of CSE,
Arya College of Engineering & IT

Abstract:- Vehicular ad hoc network (VANET) is a vehicle to vehicle (VVC) and roadside to vehicle (RVC) communication system. The technology in VANET incorporates WLAN and Ad Hoc networks to achieve the regular connectivity. The ad hoc network is brought forth with the objectives of providing safety and comfort related services to vehicle owners. Collision warning, traffic congestion warning, lane-change warning, road blockade alarm (due to construction works etc.) are among the major safety related services addressed by VANET. In the other category of comfort related services, vehicle users are equipped with Internet and Multimedia connectivity. The major research challenges in the area lies in design of routing protocol, data sharing, security and privacy, network formation etc. We aim here to study the overview of VANET and its security issues.

Keywords*— Vehicular Ad hoc networks, VVC, routing protocols, security and privacy.*

*****

I. INTRODUCTION

Vehicular Ad-Hoc network is a type of MANET, to give correspondence among near to vehicles and amongst vehicles and nearby fixed equipment i.e. roadside equipment. VANET or Intelligent Vehicular Ad-Hoc Networking gives a clever method for utilizing vehicular Networking. Every vehicle outfitted with VANET device will be a node in the Ad-hoc network and can get and transfer different messages through the wireless network [1].

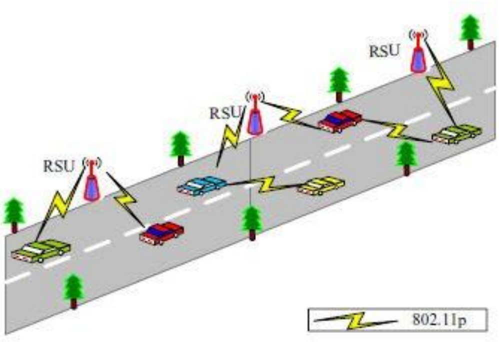

Figure 1.1 VANET

II. EVOLUTION OF VANET

In Vehicular ad-hoc networks, the term “Ad-hoc” is a Latin word with the meaning “for this purpose” [2]. Here, the network comprises of various nodes that are associated through wireless links [2]. For this, the network should send the information through other nodes of the system to perform the communication among any pair of nodes. The primary components of a Wireless Ad-hoc Network (WANET) are nonappearance of previous foundation and settled base stations; transmission inside connection scope and mobile nodes with dynamic associations.

A. CLASSIFICATION OF WIRELESS AD-HOC NETWORKS

Wireless ad-hoc networks [2] being tenacious and temperate can be generally utilized as a part of crisis circumstances like military clashes or natural disasters because of their minimal configuration requirement and quick deployment. Wireless ad-hoc networks are further evolved into three subcategories, according to their use in various applications as shown in Figure 1.9 the three classes of Wireless ad-hoc networks (WANETs) are:

- WSNs
- WMNs
- MANETs

III. COMPONENTS OF VANET

VANET is a self-governing self-sorting out wireless network. VANETs contains taking after elements:

a) **Vehicles**: Vehicles are the nodes of vehicular network.
VANET handle the wireless discussion between vehicles (V2V) and amongst vehicles and base access point (V2I).

b) **Infrastructure:** Infrastructure identified with outside condition incorporate road side base station. Base stations are the roadside unit and they're placed at dedicated place like junctions or near parking areas. Their foremost features are to broaden the communication field of the ad hoc network with the aid of re-allocating the understanding to others and to run security utility like low extension cautioning, mishap cautioning and numerous others.

c) **Communication channels***:* Radio waves are a kind of electromagnetic radiation with wavelengths in the electromagnetic range longer than infrared delicate Radio waves have frequencies from 190 GHz to 3Khz. Radio proliferation demonstrate assumes a solid part in the execution of a protocol to decide the quantity of nodes inside one collision space [2].

IV. Characteristics Of VANET

Vehicular network have some unique sort of conduct and characteristics, which distinguishing them from other types of network. As contrast with different networks vehicular network have remarkable and interesting features as follow:

a) Unlimited Transmission Power
b) Computational capacity very high.
c) Predictable mobility
d) High mobility
e) Partitioned network
f) Network topology and connectivity

V. Security In VANET

Security in VANET ought to be considered as vital as securing different networks in registering. Because of the profoundly delicate nature of data being communicated through VANET, all applications intended for vehicular network should be shielded from malicious manipulation. Imagine the likelihood of a basic message been manipulated and the harm it will cause if not detected. Notwithstanding that, comfort and quality applications in VANET need to be protected to prevent loss of revenue. [3] In the event that one applies this model of security at vehicular network, the one risk that truly emerges is the *confidentiality* of the source. For instance, an attacker who is occupied in breaking down, which authentications are appended to every message disseminated in the framework, may likewise have the capacity to track the precise area of the vehicle (trade off of protection). An inside attacker can make bogus safety messages to be distributed in the entire network. This can cause disastrous situations (a threat to Authenticity).ID Disclosure Location information in relation to vehicle exact position (privacy) needs to be protected (a threat to Confidentiality).

Denial of Service Attackers can potentially flood the entire network so that no one will have the capacity to utilize the applications/services. Such conditions can make terrible situations if activated immediately (a risk to Availability). The two key challenges in connection to giving a protected correspondence in VANET can be briefly classified as establishing a robust system of sender authentication and providing a mechanism to keep the user location undisclosed.

VI. Applications Of VANET

Classification of uses is completed by as Car to Car Traffic applications, Car to Home applications, Car to Infrastructure applications and Routing based applications. Authors in [8] discusses about the various attacks depending on the classification. Depend on type of communiqué either V2V or V2I; we are arranging application of VANET into following classes:

A. SAFETY APPLICATION

Safety applications consist of monitoring of approaching vehicles, surrounding road, road curves, surface of road etc. The Road security applications may be categorized as:
a) Real-time traffic monitoring
b) Co-operative Message Transfe*r*
c) Post-Crash Notification.
d) Road Hazard Control Notification
e) Cooperative Collision Warnin*g*
f) Traffic Vigilance [4].

B.COMMERCIAL APPLICATIONS

Commercial applications will give driver using entertainment and services as web access, streaming audio and video. The Commercial applications may be categorized as:

a) Remote Vehicle Personalization/Diagnostics
b) Internet Access
c) Digital map downloading
d) Real Time Video Relay
e) Value-added advertisement

C. CONVENIENCE APPLICATIONS

Convenience application generally bargains in traffic management with mean to upgrade activity effectiveness through boosting level of comfort for drivers. Comfort applications might be ordered as:
a) Route Diversions
b) Electronic Toll Collection.
c) Parking Availability
d) Active Prediction

D. PRODUCTIVE APPLICATIONS

We are purposely calling productive as application is additional using above mentioned applications. Applications of Productive may be categorized as:
a) Environmental Benefits
b) Time Utilization
c) Fuelsaving

VII. Issues In VANETs

Based on our survey on routing protocols of VANET, we found that few challenges and open research issues exist in routing of VANETs which is the most vital range for research today. These open issues and challenges in

VANET routing such as driver’s behavior, loss of signal, interferences caused by tunnels and high buildings [2] have been discussed in this section.

i. Dynamic Topology and High Mobility: Vehicles are the mobile nodes in VANETs and move as indicated by the street pathways which confines the mobility of the nodes. This causes the disturbances in interchanges and evolving topology. For routing protocol advancement, we ought to damage dynamic topology. A solution to give effective information dissemination not withstanding fast changing topology may be broadcast based communication.

ii. Fault Tolerance: Since a VANET has quick evolving topology; a few vehicles could enter or leave the network occasionally. If during the communication, a node leaves the network, a new route should be created by the routing protocols to manage the network. This problem can be solved if the route failure is known in advance, this requires lot of updated information exchange leading to un-scalable communication.

iii. Flexibility and Scalability: Area chooses the quantity of vehicles, for e.g. number of vehicles in country territory is low without road side units; it ends up noticeably hard to keep up the network availability. For development of the road side units, large investments are required, therefore less power constraints can be used by increasing communication ranges with higher transmission power to form every node reach its destination without support of the roadside units. On the contrary, urban area is very large and crowded having a huge range of vehicles running. The routing protocols need to decrease the overhead and control of data packets as a bigger number of vehicles need to convey. It should provide safety communication rather than control overhead.

iv. Delay Constraints and Real-time Transmission: To deal with sudden occurring situations, drivers do not have enough time to respond as the information is distributed in the real time. Mishaps can be maintained a strategic distance from. Thus the courses are to be kept up and developed for continuous applications.

v. Security Enhancement: Security [2] stands the most important and challenging issue in safety applications of VANETs. If no security is provided in routing protocols, a malicious node can enter the network and cause damage. This could lead in deceiving of data which can be utilized by fear based oppressors to trap blameless individuals as dead end tunnel. So in turn to protect the information; authentication, integrity and non-repudiation must be achieved such that there is no entry of any unauthorized vehicle into the network and no modification of the data packets is allowed during the communication. Hence, security is an important issue as future research area.

VIII. ATTACKS ON VANET

A Vehicular framework can be traded off by an attacker by controlling either vehicular framework or the security protocols. Thus two kinds of attacks can be imagined against vehicular frameworks: assaults against messages and attacks against vehicles. General diagrams of the attacks are specified beneath Basic Attacks against Messages.

a) Forgery Attacks: In this case, colluding attackers spread false data to influence the choices of different vehicles and accordingly make room of attacker .

b) Cheating with sensor information: Attackers in this utilization this attack to change their apparent position, speed, heading, and so forth so as to escape risk, quite on account of a mishap. In the most pessimistic scenario, colluding attackers can clone each between the attackers [5].

c) In-transit traffic tampering: Any node going about as a transfer can upset interchanges of different nodes: it can drop or degenerate messages, or genuinely alter messages. Thusly, the gathering of profitable or even basic traffic notices or safety messages can be controlled.

d) Masquerading: The attacker actively pretends (imitates) to be another vehicle by utilizing false personalities and can be roused by malicious or rational objectives. Message creation, adjustment, and replay can likewise be utilized towards masquerading. An impostor can be a danger: consider, for instance, an attacker masquerading on the appearance of a crisis vehicle to delude different vehicles to slow down and yield. At that point derivations on the drivers' close to personal data could be made, and hence abuse her or his protection.

e) Denial of Service (DoS): The attacker might need to bring down the VANET or even cause a mischance. There are numerous approaches to play out this attack, either by sending messages that would prompt inappropriate results or by sticking the wireless channel (this is known as a DoS attack) so that vehicles cannot exchange safety messages.

f) Sybil attack: However, if a sole defective entity can exist in several individualities, it can handle a solid segment of the system, thereby undermining this redundancy. The Sybil attack particularly goals distributed system atmospheres. The attacker tries to performance like many dissimilar nodes/ identities rather than one.

g) Sinkhole attack: Attract surrounding nodes with unfaithful routing info by an intruder and then execution choosy alters or forwarding the data passing thru it. Node tries to offer a very attractive link by the attacking e.g. to a gateway. Besides essay traffic study other attacks as choosy forwarding or DOS can be joint with the sinkhole attack.

h) Wormhole attack: The attacker joins two afar kinds of the ad hoc network exploiting an extra communication channel like a tunnel.

IX. CONCLUSION

One of the main challenges in Vehicular ad hoc network is of searching and maintaining an effective route for transporting data information. Security and privacy are indispensable in vehicular communications for successful acceptance and deployment of such a technology. To enhance secure and efficient data transmission in VANET we must first detect and eliminate malicious node in the network.

REFERENCES

[1]. Sameena Naaz " Routing in Vehicular Ad Hoc Network (VANET)" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 12, December 2014.

[2].] Divya Chadha, Reena, "Vehicular Ad hoc Network (VANETs): A Review", IJIRCCE, 2015.

[3]. C. Lochert, H. Hartenstein, J. Tian, H. Fussler, D. Hermann, and M. Mauve, "A routing strategy for vehicular ad hoc net-works in city environments," IEEE Symposium Proceedings on Intelligent Vehicles, pp. 156–161,2003.

[4]. Frank Karg, Zhendong Ma, and Elmar Schoch, "Security Engineering for VANETs" In 4th Workshop on Embedded Security in Cars (ESCAR 2006), Berlin, Germany, 11/2006.

[5]. Aijaz, B. Bochow, F. D¨otzer, A. Festag, M. Gerlach, R. Kroh and T. Leinm¨uller, "Attacks on Inter Vehicle Communication Systems – an Analysis," The Network on Wheels Project, Tech. Rep., 2005. Available: http://www.network-on- wheels.de/documents.html.