ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

An Empirical Study of Vehicles Communication in Vehicular Ad-Hoc Network

Prachi Chauhan[1], Hardwari Lal Mandoria[2]

PG Student, Department of Information Technology, G.B Pant University of Agriculture and Technology Pantnagar, Uttrakhand, India[1]

Professor, Department of Information Technology, G.B Pant University of Agriculture and Technology Pantnagar, Uttrakhand, India[2]

ABSTRACT: Vehicular ad-hoc network (VANET) have been impartially a hot research area over the recent years. Due to increase in vehicle crashes and fatalities, Vanet fascinate so much attention of both academia and industry. Vehicular ad-hoc networks (VANETs) are the dynamic subcategory of mobile ad-hoc network (MANET) in which mobile node presents set of smart vehicles on road. This paper basically described a survey of all aspects of recent review of Vanet, communication amongst vehicles, outlet characteristics, issues, activities of attacks, Sybil attack and also introduced security prevailing in Vanet for both safety and navigational purposes of vehicles on the road.

KEYWORDS: VANET, Vehicle fatalities, MANET, Routing protocols, Security.

I. INTRODUCTION

The wireless network is an Ad-Hoc Network without any static routers and nodes can dynamically connect to the network anywhere. Decentralized ad-hoc wireless network does not rely on a preexisting infrastructure and this network is suitable for emergency situation like natural or human induced disasters due to their minimal configuration and quick deployment. In static ad-hoc network nodes are fixed in the network. Self-configuring and dynamic nature of mobile ad-hoc network (MANET) allows free movement of nodes.In consequence, nodes mobility frequently change the geographic region covered by a MANET. Vehicular ad-hoc network (VANET) is improved application of MANET used to make vehicles intellectual and subsequently help in Traffic Management and it is a wireless network where every one of the vehicles are nodes of the network. It is for the driver security and road safety, the inter-vehicle communication give them.Vehicular specially appointed network is subclass of mobile impromptu networks which gives a renowned approach to canny transport system.It is self-governing and self-organizing wireless communication network, where all of the nodes in VANET includes themselves as servers or client for switching and distributing information. The primary benefits of VANETs are the potential in giving explorers comfort and enhance road safety and vehicle security while protecting drivers' privacy from attacks perpetrated by foes.

Vehicular Ad Hoc Networks (VANETs) is a technology that incorporates the capabilities of new cohort wireless networks to vehicles. A robust Ad-Hoc network between vehicles and roadside units (RSUs) constructs by it. Vehicular ad-hoc network (VANET) can accomplish an effective communication between moving node by using different ad-hoc networking tools such as Wife IEEE 802.11 b/g, Bluetooth, IRA.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

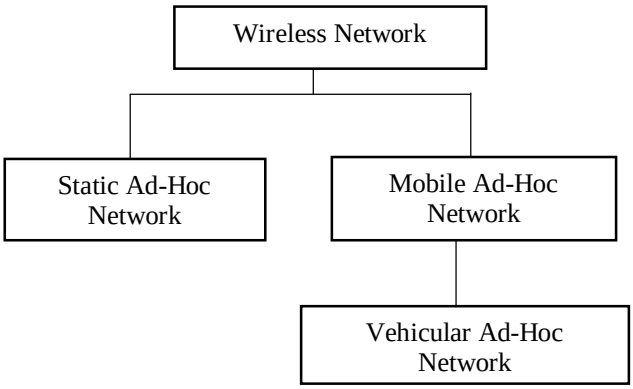

Fig. 1 Wireless Network Type

A) COMMUNICATION IN VEHICULAR AD-HOC NETWORK (VANET)

Vehicular communication is an emergent area of communication amongst vehicles and roadside communication infrastructure. The goal of a VANET architecture is to permit the communication among neighboring vehicles and between vehicles and fixed roadside equipment. Possible Disposition regarding the C2C-CC reference architecture organized with the progresses in heterogeneous communication technologies. Vehicular networks potentially have two main types of communication scenarios: car-to-car (C2C) communication scenario and car-to-infrastructure (C2I) communication scenario. These types of communication circumstances allow a number of deployment possibilities for vehicular networks. Vehicles can even communicate with other vehicles unswervingly without a communication infrastructure, where vehicles can collaborate and forward information on behalf of each other.

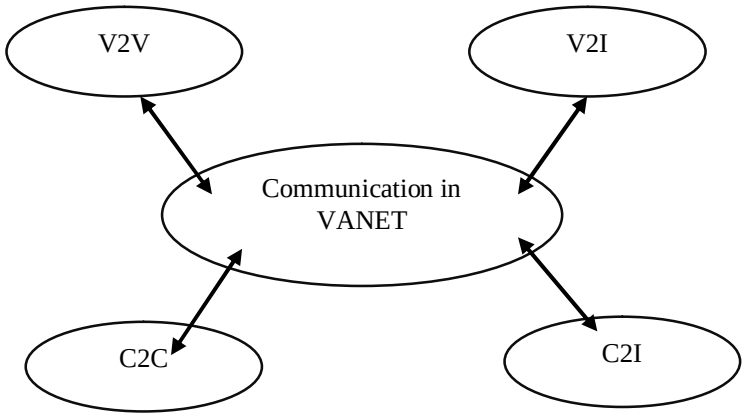

Fig. 2 Communication in VANET

High mobility of vehicles and the environment in which they operate makes vehicular communications differ from other types of wireless communications. Based on their specific characteristics, technologies' the communication among vehicles and the RSU and the infrastructure are classified into three types of domains:

a) Inter-vehicle communication,
b) vehicle-to-roadside communication and
c) Inter-roadside communication.

In **Inter vehicle communication** configurationvehicles or a cluster of vehicles connect with one another and communicate, it uses multi-hop, multicast or broadcast to transmit information related with traffic over multiple hops to a muster of receivers. In intelligent transportation traffic management, vehicles must be concerned with activity on the road onward and not behind. It proves to be very supportive for cooperative driving.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

Vehicular towards road side communication is important part of communication in vehicular ad-hoc networks (VANETs). This communication contain particular hop broadcast system, RSU (roadside unit) sends broadcast message to all supplementary participated vehicles in the neighboring area. In this communication high bandwidth is used for communication between RSUs and vehicles.

In **Inter-roadside communication** message broadcasted in a multi-hop manner until the vehicles carrying the preferred data is accomplish. It means it is a multi-hop unicast. The query is received throughout a vehicle holding the desired piece of information, the application at that vehicle instantly sends a unicast message holding the information to the vehicle, it acknowledged the request from, and forward it to the query source.

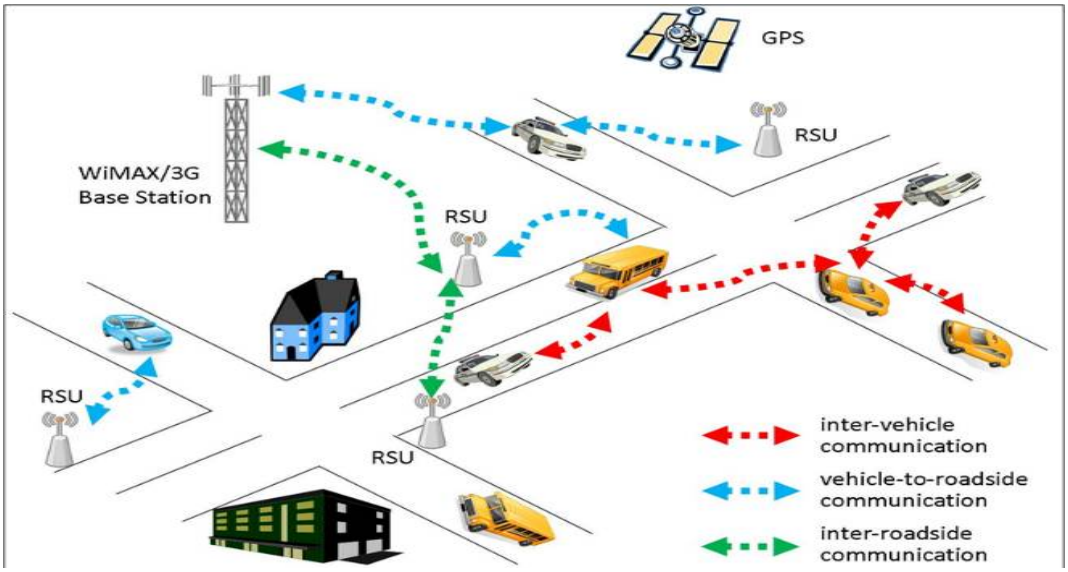

Fig 3. Types of Vehicle Communication

II. CHALLENGING ISSUES OF VANET

Even though the features of VANET discriminates it a divergent network but some characteristics enforces some challenges to deploy the VANET.

- Due to high mobility all nodes are not interacted appropriately with each other on the grounds, that they essential to learn about others conduct first as per learn centered scheme. It moreover decreases proficiency of the system.
- VANET applications are developed for hazard warning, collision avoidance and accident warning information, so applications contain strict deadlines for legitimate message delivery.

- The vehicles for the identification of vehicles from the message they send for authentication of all message transmission, which most consumers won't care for others to think about their personal identification. Hence a system needs to be introduced which enables message to be unknown to the common nodes additionally recognition by central authorities in cases like accidents.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

- For the best possible location awareness GPS system is required to handle the VANET application. On the off chance that there is no Proper system for location identification, hence there is delay automatically.
- In a VANET delay issue ought to be less for the new path identification. In this system vehicle and RSU detect chances of collision between multiple vehicles are not ready to transfer information among themselves. The system will gather information about vehicles that are coming towards the destination. For this, there are numerous safety applications are available in VANET to decrease the road accident and loss of life of the occupants of vehicles. Collision drives the stick problem. To conquer this problem delay ought to be less.

III. SECURITY ISSUES OF VANET

Among all the general communication network VANET security is diverse from wireless and wired networks due to its unique characteristics of VANET packets contains life critical information therefore it is necessary to make sure that these packets are not introduced or modified by the attacker; similarly the liability of drivers should also be conventional that they inform the traffic environment correctly and within time. The size of network, mobility constraints, infrastructure-less framework, and short duration of link between nodes makes the implementation difficult and distinct from other network security.

VANET must satisfy some security requirements for safety messaging before they are deployed and these are follows:

a) **Authentication:** Authenticity is a foremost challenge of VANETs security. It ensures that the message is generated by the legitimate user not by greedy drivers or the other adversaries. All active nodes in the network should authenticate prior to accessing available facilities. Any violation or attack involving the process of identification or authentication exposes the entire network to serious consequences. The main purpose of authenticity in a vehicular network is to protect the authentic nodes from outside or inside attackers infiltrating the network using a forged identity. It, therefore, absolutely essential to validate that a sender which gives certification as per the application. In VANETs, authentication prevents Sybil attacks by transfer a specific identity to each vehicle. For example, in location based services this property could be that a vehicle is in a particular location from where it claims to be.

b) **Availability:** Availability guarantees that the information must be available to the legitimate users. It means network to be available at all times and useful information not shared to selfish nodes present in the network, in order to send and receive messages at any functional time. The main purpose of this security requirement for VANETs is to make sure the users' lives, is a significant target for most of the attackers. The most famous examples are the DoS (Denial-of-Service) and jamming attacks.

c) **Integrity:** Integrity of message ensures that the message is not changes in transit between the moment it was sent and received as the received message must match the message sent. Then the receiver will be able to validate the sender's identity during the transaction. Integrity shields against the unauthorized creation, destruction or alteration of data. If a modified message is accepted, the integrity property is violated and the protocol would be deemed faulty. To attain integrity, the system must prevent attackers from altering messages since the messages must be trusted. Thus, the attacker injects it again in the network packets previously received.

d) **Confidentiality:** Major security requirement challenges for VANETs communications is confidentiality. It ensure data are only read/write and understand by certified users. Confidentiality is required to maintain privacy of entities (vehicle or infrastructure), outsiders are not capable to discriminate confidential information among the vehicles throughout communication. It must be achieved by encryption of message thus; it can keep the confidential information of each and every driver such as custom profiles and users' identity. For instance, sensitive information which is related to safety-related messages. Law administration authority can only enforce this privacy between communicating nodes.

e) **Non-Repudiation:** It is defined as one of the entities that transmit the message in a communication channel deny for participate impracticality in all or part of a communication event. The main objective of nonrepudiation consists of collecting, making available, maintaining, and validating undeniable evidence about a claimed event or an action in order to resolve disputes about the occurrence or non-occurrence of that event or action. Nonrepudiation depends on authentication, but it may be crucial to determine drivers

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

causing accidents should be reliably identified. It means violators or misbehaving users cannot deny their actions (it may be crucial for investigation to determine the correct sequence and content of messages exchanged before the accident).

IV. ATTACKS IN VANET

Since mobile ad-hoc network is multi-hop in environment and it strictly depend on the cooperation amongst the nodes. So the guarantee of cooperation of nodes is required. A variety of attacks have been recognized and detected in the network. Keeping in mind the end goal is to make available a secure communication, one needs to confront the security challenges. For instances, eavesdropping attack, dropping attack, modification attack, fabrication attack, black hole, gray hole, worm hole, jellyfish attack, spoofing, Sybil attack, traffic analysis. Fundamentally, there are two types of attacks:-

a) **Passive Attacks**: A passive attack would not interrupt the normal operation of mobile ad --hoc network, while data have been exchanged from the network. The attacker don't damage to the network explicitly. Be that as it may, they can get information for future harmful attacks. The types of passive attacks are eavesdropping and traffic analysis. For instances, eavesdropping attack (technique for collecting information by snooping on transmitted data on legitimate network), traffic analysis (to monitor and analyze which sort of the transmission is going on).

b) **Active Attacks**: In this attack, an attacker consistently tries to change or destroy the data or normal operation on MANET. Active attacks can be either internal or external. In external attack, the attacker concentrates on to cause congestion in the network. For this reason, they proliferates fake information or to disturb the nodes from giving services. In internal attacks, the attacker needs to get the normal access to participate in the network activities. For instances, dropping attack, modification attack, fabrication attack, black hole, gray hole, worm hole, jellyfish attack, spoofing, Sybil attack etc.

Sybil Attack in VANET

Unfortunately, in VANETs, most privacy-preserving schemes are vulnerable to Sybil attacks, where malicious vehicles can communicate with each other in a multi-hop manner.It comprises of sending multiple messages from one hub with multiple identities. Sybil attack is continuously possible aside from the extreme conditions and assumptions of the likelihood of resource parity and coordination among entities.

At the point when any entity makes multiple copies of itself then it makes confusion in the network. Claim all the illegal and fake ID's and Authority. It can make collision in the network. This sort of situation is known as Sybil attack in the network. This system can attack both internally and externally in which external attacks can be restricted by authentication yet not internal attacks.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

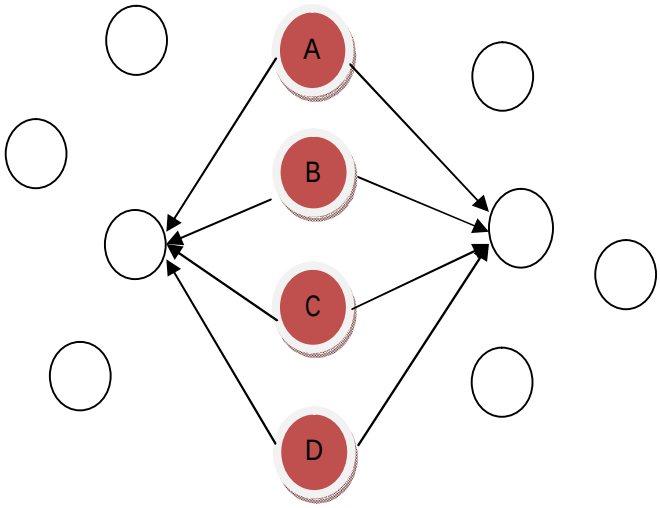

Fig 5: Sybil Attack in Vanet

V. CONCLUSION

Vehicular ad-hoc network is an emerging and attractive technology means of communication between moving vehicles and dedicated to safety and comfort services to the vehicle users. VANET provides information about car speed warning,traffic signal violation warning,collision risk warning and lane change warning for safety purpose. This paper explain all of the characteristics vehicular ad-hoc networks (VANETs),vehicles communication, security requirements and describe Sybil attack in which attacker pretends to have manifold identities or nodes. Through this extensive survey, we concluded that effective and efficient communication between vehicles should be more secure. VANET would provide better platform and communication between vehicles with more advancement and evolution of new approaches.

REFERENCES

[1] IEEE P1609.2/D2 – Draft Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages, November 2005.
[2] M. Sivasakthi et al (2013), "Research on vehicular ad hoc networks (VANETs): an overview," Journal of Applied Sciences and Engineering Research, vol.2, no.1, pp.23–27.
[3] X.Su (2013), "A comparative survey of routing protocol for vehicular sensor networks," in Proceedings of the IEEE International Conference on Wireless Communications,Networking and Information Security(WCNIS'10), pp. 311–316.
[4] Raya, M. et al (2007), "Securing vehicular ad hoc networks", Journal of Computer Security, pp.39-68.
[5] Xiao, B. et al (2006), "Detection and localization of Sybil nodes in VANETs", In Proceedings of the workshop on Dependability issues in wireless ad hoc networks and sensor networks pp. 1-8.
[6] Hao, Y. et al (2011), "Cooperative Sybil attack detection for position based applications in privacy preserved VANETs" IEEE In Global Telecommunications Conference (GLOBECOM 2011), IEEE pp. 1-5.
[7] Chang, S. et al (2011), "Footprint: Detecting Sybil attacks in urban vehicular networks", IEEE sponsored Parallel and Distributed Systems, pp.1103-1114.
[8] Lee, B. et al (2013), "A DTSA (Detection Technique against a Sybil Attack) Protocol using SKC (Session Key based Certificate) on VANET", International Journal of Security & Its Applications, pp.1-10.
[9] Li, M., Xiong et al (2013), "A Regional Statistics Detection Scheme against Sybil Attacks in WSNs", IEEE Sponsored In Trust, Security and Privacy in Computing and Communications (TrustCom), 12th IEEE International Conference on pp. 285-291.
[10] Gañán, C. et al (2011), "PPREM: privacy preserving revocation mechanism for vehicular ad hoc networks", Computer Standards & Interfaces, pp-513-523.
[11] S. Husain et al (2010), "A proposed model for Intrusion Detection System for mobile ad-hoc network", IEEE International Conference in Computer and Communication Technology (ICCCT), pp.99-102.
[12] RenuBahuguna et al (2013), "Routing Protocols in Mobile Ad-hoc Network",Springer Lecture Notes of the Institute for Computer Science, vol. 115, pp.52-60.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

[13] PranaviTayal et al (2013), "Simulation in Wireless Sensor Network", Proceedings of National Conference on Trends in Signal Processing & Communication (TSPC'13), vol.12.
[14] MK Joshi et al (2013), "A Review on wireless ad-hoc network security", International Journal of engineering Sciences and Research Technology, pp.1632-1635.
[15] Awantika et al (2014), "Efficiency of Proactive and Reactive Routing Protocols in VANET", i-manager's Journal on Wireless Communication Networks, vol.3, pp.17-21.
[16] HusianShahnawaz et al (2013) "Design of Detection Engine for Wormhole attack in ad-hocnetwork", published in International Journal of Engineering and Technology, pp. 381-395.
[17] JosianeNzouonta et al (2008), "VANET Routing on City Roads using Real-Time Vehicular Traffic Information" IEEE, and Cristian Borcea, Member IEEE, pp. 1-18.
[18] Jason J. Haas et al (2002), "Real-World VANET Security Protocol Performance" University of Illinois at Urbana-Champaign Urbana, Illinois, U.S.A, pp.1-7.
[19] Khaled Mohamed et al (2011), "Combating Sybil Attacks in Vehicular Ad Hoc Networks", CCIS 162, pp. 65–72.
[20] Kung et.al (2002), "A survey of mobility models for ad hoc network research", wireless communication & mobile computing (WCMC): special issue on mobile ad hoc networking: research, trends and applications, vol. 2, no. 5, pp. 483-50.