International Journal of Innovative Research in Science and Engineering
Vol. No.2, Issue 08, August 2016
www.ijirse.com
ISSN: 2454-9665

Overview of Challenges in VANET

Er.Gurpreet Singh

Department of Computer Science, Baba Farid College, Bathinda(Punjab), India

ABSTRACT

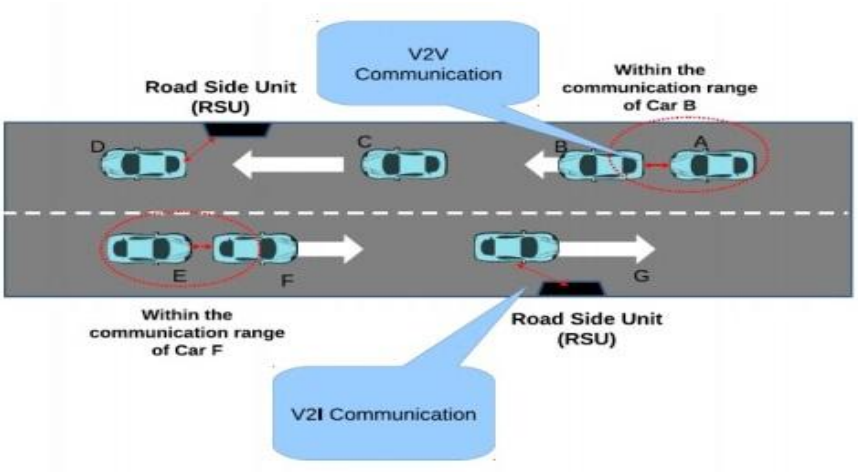
VANET are becoming active area of research and development because it has potential to increase road safety, convenience and comfort to drivers & passengers. A Lot of research work on VANET have done in area of Quality of Service (QoS), routing and security. These concepts relate the facing challenges for technology in VANET. We present a overview of challenges in VANET. Firstly ,we have discussed about VANET technology and routing methods. The aspects related to security have explored with challenges related to threats. Further there is discussion about Quality of Service, routing and technical issues as well as social and economic challenges.

Keywords: VANET, Security, QoS, Routing, Mobility

I. INTRODUCTION

The main objective of VANET is to help a group of vehicles to setup and maintain a communication network among them without using any central base station or any controller.

Vehicular ad-hoc networks are responsible for the communication between moving vehicles in a certain environment. A vehicle can communicate with another vehicle directly which is called Vehicle to Vehicle (V2V) communication, or a vehicle can communicate to an infrastructure such as a Road Side Unit(RSU), known as Vehicle-to-Infrastructure(Fig.1).



ISSN: 2454-9665

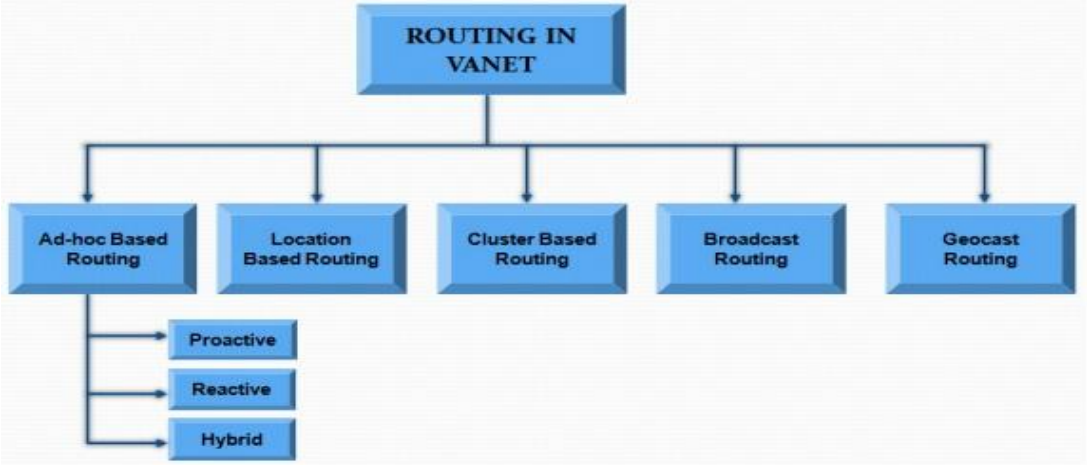
Figure 1.VANET communication and infrastructure

In principal, there is no fixed architecture or topology that a VANET must follow. However, a general VANET consists of moving vehicles communicating with each other as well as with some nearby RSU. A VANET is different than a MANET in the sense that vehicles do not move randomly as nodes do in MANETs, rather moving vehicles follow some fixed paths such as urban roads and highways. While it is easy to consider VANETs as a part of MANETs, it is also important to think of VANETs as an individual research field, especially when it comes to designing of network architecture. In VANET architecture, an on board unit (OBU) in a vehicle consists of wireless transmitter and receiver. In a broad sense, we can loosely define three possible communication scenarios for vehicles. One possibility is that all vehicles communicate with each other through some RSU. This architecture may resemble wireless local area networks (WLAN). Second possibility is where vehicles directly communicate with each other and there is no need of any RSU. This can be classified as Ad-hoc architecture. In third possibility, some of the vehicles can communicate with each other directly while others may need some RSU to communicate [1].

Each environment has its own specific challenges to overcome. For example, in a sparse network like highways, the low density of vehicles remains the prime issue. Even in some urban environments, low penetration ratio and low traffic at night times can cause long network delays. One of the most important attributes of mobile ad-hoc wireless network is the mobility associated with the nodes. The highly mobile nature of vehicles makes it very complicated to model the communication scenario. In VANET paradigm, the mobility model must include the behaviour of moving vehicles individually and in a group for an error free efficient packet transmission.

One of the major challenges in the design of vehicular ad-hoc network is the development of a dynamic routing protocol that can help disseminate the information from one node (vehicle) to another. Routing in VANET is different to the traditional MANET routing because of highly dynamic and ever changing topologies in the former. Few protocols that were earlier designed for MANET environment have been tested on VANET. The challenge however remains as how to reduce delay associated with passing the information from one node to another. Overcoming these hurdles in MANET protocols, can help implement real time applications for VANET environment. Other implications such as reducing control overheads also need to be looked into carefully. Keeping an eye on the dynamic characteristics of VANET (as highlighted previously), the routing protocol should be able to withstand the unpredicted and dynamic nature of vehicular network topology. Perhaps the most difficult task in VANET routing is finding and maintaining the optimal paths of communication in desired environments. Most of the routing protocols in VANET are closely linked with the topology being used in the network architecture and the performance deviates whenever there is a change in network topology. As highlighted in Fig. 2, routing in VANET can be classified into five major categories.

ISSN: 2454-9665



SFigure 2.VANET Routing

II. SECURITY CHALLENGES IN VANET

Security in VANET should be considered as important as securing other networks in computing. There are a numbers of possible attacks in VANETs. The purpose of these attacks is to create problem for users to access the system or phishing some information [2].Due to the highly sensitive nature of information being broadcasted via VANET, all applications designed for vehicular network need to be protected from malicious manipulation. Imagine the possibility of a critical message been manipulated and the harm it will cause if not detected. In addition to that, comfort and quality applications in VANET need to be protected to prevent loss of revenue. As per basic computer and network security definitions, attacks on a computer network can be classified in three main groups of threats; threats associated with Authenticity, Confidentiality and Availability of the resource. If one applies this model of security on vehicular network, the one threat that really stands out is the Confidentiality of the source. For example, an attacker who is busy in analysing which certificates are attached to each message distributed in the system might also be able to track the exact location of the vehicle (compromise of privacy). Currently a broadcast authentication scheme is utilised in current standards of security for VANET such as IEEE 1609.2. This scheme is based on the use of a public key signature. Broadcast authentication enables the receivers to verify that received information was really sent by the claimed sender. A better approach in VANET security could be to provide an authentication mechanism to each node. In [3], authors have presented such a security method which encourages the nodes to provide a secure sender authentication. Due to the large number of independent network members (vehicles) and the existence of human factor, misbehaviour can take place. So an authentication trust needs to be established. In VANET security, the attack threats can be classified into different categories. In [4], authors have described three key types of attacks:

Bogus Information

An inside attacker can make bogus information. This can cause disastrous situations (a threat to Authenticity).

ISSN: 2454-9665

ID Disclosure

Location information in relation to vehicle's 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 be able to use the applications/services. Such circumstances can create catastrophic situations if triggered instantaneously (a threat to Availability). The two key challenges in relation to providing a secure communication in VANET can be briefly classified as establishing a robust system of sender authentication and providing a mechanism to keep the user location undisclosed. Since vehicles are boosted with sufficient processing power, the computational resources needed for applying cryptographic techniques in real-test bed should not be a concern. On the other hand, if needed to be implemented in virtual (simulated) environment, computational resources required such as speed of processor and desired memory will need to be looked into.

III. QUALITY OF SERVICE (QOS)

Provision of certain quality of service levels in VANET is an important task. A network with minimum delay for data delivery, less retransmissions, and high connectivity time can provide certain QoS guaranteed to the users. Promising this kind of QoS with different user applications and dynamic network environment is an interesting and challenging task in VANET design. QoS support over VANETs remains a challenge when current routing paths become no longer available as a result of changes in node velocity, node positioning, network topology or distance between vehicular nodes [5]. It may be a challenging issue both for network engineers and researchers to utilize the available bandwidth allocated for VANET to improve delivery of messages as well as to develop adaptive QoS routing protocols that will establish new routes quickly and efficiently.

IV. EFFICIENT ROUTING

In order to timely and properly sending data packets from one node to another node an efficient routing algorithm is required. In VANET, efficient routing algorithm means a routing scheme with minimum delay, maximum system capacity and less computational complexity. Design such an algorithm which can be implemented in multiple topologies of the network and satisfies all of the above mentioned properties is an active area of research in VANET. Generally, sense and uphold the optimal route to send data packets via intermediate nodes is the main motive of a routing algorithm. In VANETs, due to the dynamic nature of mobile nodes, searching and saving routes is a complex task. In view of the fact that VANETs used special routing protocols originally implemented for MANETs. The addresses and topology-based routing protocols require a unique address for each participating node. This means that a mechanism is desired that can be used to assign

ISSN: 2454-9665

unique addresses for vehicles, but these protocols do not guarantee to avoid duplicate allocation addresses in the network [6].

V. TECHNICAL CHALLENGES

The technical challenges deals with the technical obstacles which should be resolved before the deployment of VANET [7]. Some challenges are given below:

• **Network Management:** Due to high mobility, the network topology and channel condition change rapidly. Due to this, we can't use structures like tree because these structures can't be set up and maintained as rapidly as the topology changed.

• **Congestion and collision Control:** The unbounded network size also creates a challenge. The traffic load is low in rural areas and night in even urban areas. Due to this, the network partitions frequently occurs while in rush hours the traffic load is very high and hence network is congested and collision occurs in the network.

• **Environmental Impact**: VANETs use the electromagnetic waves for communication. These waves are affected by the environment. Hence to deploy the VANET the environmental impact must be considered.

• **MAC Design:** VANET generally use the shared medium to communicate hence the MAC design is the key issue. Many approaches have been given like TDMA, SDMA, and CSMA etc. IEEE 802.11 adopted the CSMA based Mac for VANET.

• **Security:** As VANET provides the road safety applications which are life critical. Therefore security of these messages must be satisfied.

VI. SOCIAL AND ECONOMIC CHALLENGES

Apart from the technical challenges to deploy the VANET, social and economical challenges should be considered. It is difficult to convince manufacturers to build a system that conveys the traffic signal violation because a consumer may reject such type of monitoring. Conversely, consumer appreciates the warning message of police trap. So to motivate the manufacturer to deploy VANET will get little incentive. Other factors are scalability, robustness and co-operative communication. The avoidance from malicious data is necessary so it can be more reliable and securable information system. The routing or traffic management is needed to met the smooth communication through network using best design.

VII. CONCLUSION

In this paper, it has been observed that in implementation of VANETs, the designers have to take care of a number challenging issues. In the research area of VANETs, it becomes more conscious matter related to Security and routing choice. Further this study can be extended by exploring new

challenges and their solutions for smooth infrastructure of VANETs. The avoidance from malicious data is necessary so it can be more reliable and securable information system. The routing or traffic management is needed to meet the communication through network using appropriate design.

VIII. REFERENCES

[1]. **S**Sabih, M. Arif, Tanveer, Lihong ,Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges, Journal of Wireless Networking and Communications 2013.

[2]. Ahmad, Saadia, Murizah, A Literature Survey on Security Challenges in VANETs, International Journal of Computer Theory and Engineering, Vol. 4, No. 6, December 2012

[3]. S. Zeadally, R. Hunt, Y. S. Chen, A. Irwin, and A. Hassan ,Vehicular ad hoc networks (VANETS): status, results, and challenges, Telecommunication Systems, Dec. 2010

[4]. M. Raya and J. P. Hubaux, The security of vehicular ad hoc networks, Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks - SASN '05, p. 11, 2005.

[5]. Sherali Zeadally, Ray hunt, Yuh shyan chen, Angela Irwin, aamir Hassan, Vehicular ad hoc networks (VANETS): status, results and challenges, Telecommunication System, 2012, 50:217-241

[6]. Vishal, Harsukhpreet Shashi, Challenging Issues in VANET Network and its Routing Algorithms-An Analysis, Proc. of Int. Conf. on Advances in Communication, Network, and Computing 2013

[7]. Ram, Manish, Nanhay, Security challenges, issues and their solutions for VANET, International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013.