ISSN:2320-0790

An International Journal of Advanced Computer Technology

# Selective Forwarding Scheme for V2V Communications

**S.Mohana Krishnan**[1], **A.Anandhi** [2]

[1,2]Deparment of Computer Science and Engineering

[1] M.Tech Student, Pondicherry Engineering College

[2]Assistant Professor, Christ College of Engineering and Technology

Pondicherry, India.

**Abstract**-Wireless communication between vehicles, known as Vehicular Ad hoc NETworking (VANET), will allow providing drivers with information to increase safety, efficiency and comfort in road travel. A number of safety applications require communications to a group of vehicles and not just pair-wise communications as supported by unicast protocols. Thus for V2V communications, multicast or broadcast schemes may be more applicable than unicast protocols. In safety-oriented applications, providing a driver with advance warning for an accident occurring at some distant ahead has been an ongoing major research goal. InVANETs, broadcast-basedpacket forwarding is usually preferred in order to propagateurgent traffic related information to all reachable nodes within acertain dangerous region. In multicasting technologies, in this paper we discuss with the Location dependent multicast membership. In a multicast group is specified by a particular area of region called a multicast region, and vehicles within the multicast region automatically become members of the multicast group. LBM uses information about a multicast region as destination information for multicast packets instead of information about positions of all individual destinations as used in PBM. Thus, in LBM, forwarding nodes are selected based on the position of a source and the coordinates of the multicast region. This type of networks will allow the reduction of the number of deaths due to car accidents, and the provision of real-time information on traffic and on roads.

**Keywords**: Location dependent, Multicasting, VANET, Vehicular safety – oriented applications, V2V communications.

## I. INTRODUCTION

### A. Networking

A computer network, often simply referred to as a network, is a collection of computers and devices connected by communications channels that facilitates communications among users and allows users to share resources with other users.

In the world of computers, networking is the practice of linking two or more computing devices together for the purpose of sharing data. Networks are built with a mix of computer hardware and computer software. The advantages of the networks are as follows.

- Facilitating communications. Using a network, people can communicate efficiently and easily via e-mail, instant messaging, chat rooms, telephone, video telephone calls, and video conferencing.
- Sharing hardware. In a networked environment, each computer on a network can access and use hardware on the network.
- Sharing files, data, and information. In a network environment, any authorized user can access data and information stored on other computers on the network.
- Sharing software. Users connected to a network can access application programs on the network.

### B. Vehicular Ad-Hoc Networks

The word ad-hoc is highlighted from Latin which means “for this purpose only”. A Vehicular ad-hoc network is an autonomous network system of routers and hosts connected by wireless links. They can be setup anywhere without any need for external infrastructure like wires or base stations. The routers are free to move randomly and organize themselves arbitrarily. Acronym is VANET. Each device in the network is called an NODE.

A Vehicular Ad-hoc Network (VANET) is a type of Mobile Ad-hoc Network (MANET) that is used to provide communications between nearby vehicles, and between vehicles and fixed infrastructure on the roadside. Vehicular Ad hoc Network (VANET) compromises of a set of Vehicles devices that can move around freely and cooperate with each other in relaying packets without the support of any fixed infrastructure or centralized administration. Hence they are known as infrastructure less networks. A mobile node can be laptop computer, personal digital Assistant or a cellular phone. The mobile nodes operate with the help if battery power and they communicate each other through antennas (transceiver – a transmitter and receiver) and the radio waves acts as the medium of communication. There are two types of antennas commonly used by the mobile nodes: 1. Directional antennas 2. Omni - directional antennas. In Omni-directional the data packets are broadcasted in all directions whereas in directional antennas the packets are flooded in a fixed direction.

## II. EXISTING WORK

For Topology-based approaches select forwarding nodes based on the network topology information. A multicast tree or mesh is formed through a query-reply type of sequenced operations: a join-query is flooded and then join-replies are responded toward the source for the join-query. A group of members can be denoted by unique and logical group identifications such as a class-D IP address, usually a multicast group is not constrained by a particular location. ODMRP generates a source-based multicast mesh, but multicast packets are forwarded based on the group address (e.g., destination IP address) rather than the sources of the packets. It is on-demand, A multicast mesh is created only when a multicast source has multicast packets to send. Also, it does not require any underlying unicast routing protocol. The difference is that MOLSR uses the underlying unicast routing protocol to set up source-based multicast trees and forwards multicast packets based on both the source and group addresses of a multicast session. Because of the reactive nature of these protocols, less control overhead is generated for maintaining multicast trees, which are disseminated during the phase of forming a multicast tree, experience some delay and packet applications which require fast and reliable dissemination of information.

MAODV generates a group-based multicast tree. It requires AODV, the underlying unicast routing protocol, during the formation of multicasting trees. Even though AODV is an on-demand unicast routing protocol, MAODV is proactive instead of on-demand although there is no multicast source, a multicast tree is formed as long as there is any multicast receiver. But in Location-based approaches select forwarding nodes based on location information such as the position of a packet sender, the position of a receiving node, the positions of neighborhood nodes, and/or the coordinates of a multicast region. Since forwarding nodes are selected during dissemination of each multicast packet, location-based approaches are reactive and do not need to maintain multicast trees - no control overhead is generated. They can be further divided into two schemes: approaches with location-independent and location-dependent multicast membership based on location informationloss. Such delay and packet loss may not be acceptable. Especially for V2V safety and emergency.

Stephan Eichler [2], analyzed the capabilities of the standard, to give an overview on the capabilities and primarily thelimitations of the technology. The defined parameter set for the EDCA used in WAVE is capable of prioritizing messages, however, with increasing number of nodes sending AC3 especially, the collision probability increases significantly. Since collisions are detected *after* a transmission if at all, a high collision probability results in many dead times; times where the channel is blocked but no useful data is exchanged. Due to the continuous switching between CCH and SCH, which also use different packet queues, the collisions have an even worse impact. Messages for the CCH queue up further during the SCH intervals, resulting in longer queues and a higher end-to-end delay.

Especially in dense scenarios or in case of filled MAC queues the technology cannot ensure time critical messagedissemination (e.g. collision warnings).We suggest to integrate a re-evaluation mechanism for messages, similar to the concept presented in [10], to continuously reduce the number of high priority messages and prevent long message queues. In addition, the use of different EDCA parameters could mitigate the high collision probability. Yao-Tsung Yang andLi-Der Chou [3], Position-based Adaptive Broadcast algorithm is proposed for traffic safety in highway by exploiting the position and velocity information of the current vehicle, and computing with the same information from the previous sender and the original sender. The protocol adopts event-driven driving direction. The simulation results show that the proposed algorithm can save more time for drivers to react and keep the retransmission more steadily even though headway is changing very much. Furthermore, the protocol not only has the lower latency when disseminating the emergency message, but also retransmits efficiently by fewer intermediates. In addition, Position-based Adaptive Broadcast algorithm can be extended easily for several applications with the dedicated message format, for example, interchange scenario, tollbooth scenario and active emergency warning scenario.

These applications have the different approaches while applied the proposed algorithm. Moreover, simultaneous flooding always occurs when pile-up or bumping, a sophisticated merging methodology is also going to be considerate in the near future.

Yunyue Lin et. al.,[4], we investigated the problems of deploying multiple BSs in WSNs to maximize the network lifetime under one-hop and multi-hop communication models. We formulated the multiple BSs deployment problems as optimization problems and proposed various optimal or heuristic solutions based on geometric optimization techniques and rigorous mathematical derivations. The extensive simulation results illustrated the efficacy of these proposed algorithms. In our future work, we plan to investigate the BS deployment problems in heterogeneous sensor networks where sensor nodes have different initial energy levels. Besides lifetime maximization, we will also consider multifarious performance requirements including network connectivity and data routing quality.

Mancia anguitaet. Al., [5], shows that it is possible to implement opticalflow in a standard processor with the required performance specifications (real-time with high-resolution image) without needing to design specific purpose hardware or using expensive computers (such as CC-NUMAs, NUMAs or clusters) or FPGAs or GPUs. A standard processor has at least a factor 5 cost reduction compared to equivalent FPGA devices. We found that GPUs (with cards) and modern processors (with motherboard) are similarly priced for normal user products. Nevertheless, if we use the high-performance GPU series, the commodity-processor approach is about 50% cheaper than the high-performance GPU approach. Moreover, note that GPUs need yet a host motherboard, or include a host processor chip or core; this can increase size, power consumption, processing time (due to the communication time between GPU and host) and the price of a GPU-based solution. Our approach also represents a very significant reduction in power consumption compared to implementations based on CC-NUMAs, NUMAs, clusters or GPU. Table I shows the maximum amount of power the cooling system is required to dissipate (TDP) for the processors used in the test. Nowadaysthere are also Core 2 processors with a TDP of 17W (L7500, with two 1.6 GHz cores, 4MB L2, and 800 FSB) and 10W (U7600, two 1.2 GHz cores, 2MB L2, and 533 FSB) more suitable for embedded systems (chipsets for these processors can have TDPs of 20–30 W). These values are lower than the TDP of GPUs in Table VII. The typical power consumption of medium FPGA chips is in the order of 10, 12W. Moreover, the last code version presented outperforms all the previous L&K implementations. Furthermore, the vector functions implemented and optimized can also be used for other applications. The low cost of the implementation on a standard processor allows optical-flow to be more accessible to a wide range of applications, even embedded systems based on these processors. In addition, since the performance satisfiesby far the most demanding applications we can even moveto smaller devices to take advantage of lower cost or power without degrading the quality of the application. We would also like to remark that our approach implies a significant reduction in development time compared to those involved in customizing hardware, such as those based on FPGAs commented upon in the previous section. Compared toGPU approaches, both techniques require knowledge of the underlying architecture to achieve a significant performance; development time will depend upon the problem to be solved and programmer expertise. Within the framework of optical flow computation, we believe that, for experts in the respective fields (commodity processors and GPUs), the development times should be quite similar.

Finally, the implementation and methodology described here is quite general and may be viable for other modern processors and also suitable for use with embedded processors are shown clearly. V2 can be used with any processor and V3 can be used with any ×86 processor since Intel Pentium 4 (released in 2000) or, if the Speed stage version of V2 is used, since Intel Pentium III. V3 could be ported to other processors with multimedia extension. This opens the field to a larger number of applications requiring a wide range of performances, prices and power consumption solely for the use of standard processor and code optimization. GPUs have less flexibility and functionality compared to a general-purpose processor because their streaming processing architecture only allows them to speedup applications that work with large data structures. Wenjing wang et.al, [6], Research on VANETs needs integrated study of vehicular mobility models and network protocols. Physical-world traffic rules, such as road layouts and traffic regulations, have a significant impact on the networking performance and, hence, deserve careful investigation. In this paper, we have proposed a vehicular mobility model based on real-life scenarios. We have simulated vehicle movement traces using real-world maps. Based on the traces, we have designed new routing protocols for VANETs. Considering the routing issues of VANETs, we have first proposed two small-scale VANET routing schemes and carefully studied their performance. We have shown how the packet delivery ratio and delay are affected by different schemes, vehicle densities, and road layouts. However, when applying the existing protocols to large-scale VANETs, the performance degrades. We have argued that it is possible to exploit the road diversity that could potentially provide insights into designing better VANET routing schemes. To this end, we have distinguished the *overlay* roads from the *access* roads, based on the vehicle density and speed limit, and suggested that routing can independently be done on both types of roads. We have presented a TOPO and addressed the packet-routing issue similar to a vehicle moving on a map. The proposed TOPO can also be regarded as a framework in large-scale VANET routing that is compatible with various single-stage routing protocols. We have conducted simulations to verify our ideas, and results have shown much better performance, compared with those of existing methods. Furthermore, results have also shown how the performance of the TOPO is affected by the packet size, packet rate, vehicle density, and packet-caching schemes. As an added benefit, the TOPO has also achieved ITS friendliness with packet prioritization.

Bing Hanet.al., [7], introduced the query range problem which deals with the cooperation of users and sensors when setting their query ranges in order to optimize certain global objective and to avoid congesting the sensors. This problem reveals, in its theoretical aspect, that heuristic algorithms exploiting special underlying network structure would be of interest due to the NP-completeness of the problem; while in its practical aspect, that optimization in favor of users in WSN has great importance when multiple users present in the network as in the fireman scenario that has motivated this study.

S. Biswaset. al [8], describes that Vehicle-to-Vehicle Wireless Communication Protocols for Enhancing Highway Traffic Safety. Cooperative collision avoidance (CCA) application using the emerging Dedicated Short-Range Communication (DSRC) infrastructure for inter vehicle wireless networking has been presented. The concept of CCA has been introduced with an overview, and its implementation issues have been analyzed in light of specific requirements from the MAC and routing-layer protocols of the underlying wireless networks. Specific constraints and future research directions have then been identified for packet-routing protocols to support an effective CCA system within the DSRC environment.

**Drawbacks**

The literature survey thus provides the clear picture lacking in the following issues.This may not be suitable for highly mobile and dense V2V networks in which positions of vehicles rapidly keep changing and many vehicles happen to be multicast recipients information about the positions of vehicles becomes invalid time to time due to mobility of vehicles, and the size of a packet header would be significantly increased for carrying the position information of many recipients, which results in lower packet utilization and more packet processing as well. Accordingly, delay for packet dissemination would increase.

## III. PROPOSED WORK

We now discuss the approach with Location dependent multicast membership.In a multicast group is specified by a particular area of region called a multicast region, and vehicles within the multicast region automatically become members of the multicast group. LBM uses information about a multicast region as destination information for multicast packets instead of information about positions of all individual destinations as used in PBM. Thus, in LBM, forwarding nodes are selected based on the position of a source and the coordinates of the multicast region. It employs a direct flooding method which limits the forwarding space for multicast packets. That is, all nodes within a forwarding zone between the source and the multicast region are responsible for forwarding multicast packets.

Securing forwarding and dissemination is a critical issue in VANETs. Although various encryption techniques can protect the dissemination message itself,the message may not be forwarded correctly due to the multi-hop nature of VANETs. According to attackers could be insider or outsider, malicious or rational, and active or passive. In VANETs, routing and dissemination security issues could be divided into twoCategories: general attacks and position-related attacks. General attacks, which happen to both topologies based and position-based forwarding solutions, include denial of service attacks, black hole attacks, and bogus information attack, etc. DoS attack aims to bring down the VANET through methods such as channel jamming and aggressive injection of dummy messages. Here we target on the Black hole attack or selective forwarding is carried through a node that has the ability to lure all data around an area through itself, and then simply discards all data or only forwards portion of received data. In bogus information attack, attackers diffuse false information to misguide other vehicles. General attacks except DoS attack could usually be prevented or detected by authentication.

**MADOV in VANET**

Multicasting Ad Hoc On-Demand Distance Vector (MAODV) Routing Protocol is a reactive protocol. There are two phases for the protocol: Route Discovery and Route Maintenance. The MAODV is able to maintain both unicast and multicast routes even for nodes in constant movement. MAODV responds to topological changes that affect active routes of overhead in a quick and timely manner. It builds routes with only a small amount of overhead from routing control messages and no additional network overhead.

If the receiving node is the destination or has a current route to the destination, it generates a Route Reply (RREP). The RREP is unicast in a hop-by-hop fashion to the source. As the RREP propagates, each intermediate node creates a route to the destination. When the source receives the RREP, it records the route to the destination and can begin sending data. If multiple RREPs are received by the source, the route with the shortest hop count is chosen. As data flows from the source to the destination, each node along the route updates the timers associated with the routes to the source and destination, maintaining the routes in the routing table. If a route is not used for some period of time, a node cannot be sure whether the route is still valid; consequently, the node removes the route from its routing table.

### 3.3.2. MAODV Protocol Activities

MAODV requires nodes to maintain only next-hop routing information, thereby decreasing the storage at each of the mobile nodes. Finally, MAODV does not place any additional overhead on data packets because it does not utilize source routing.

- ➢ Reactive Protocol: discovers a route on demand
- ➢ Nodes do not have to maintain routing information.
- ➢ Route Discovery
- ➢ Route Maintenance

### 3.3.2.1. Route Discovery

➢

**Route Request**

Source broadcasts Route Request (RREQ) message for specified destination

- ➢ Intermediate node:
  - Forwards (broadcasts) message toward destination
  - Creates next-hop entry for reverse path to source, to use when sending reply.

**Route Reply**

- ➢ Destination unicasts Route Reply (RREP) message to source
  - RREP contains sequence number, hop-count field (initialized to 0)
  - Will be sent along "reverse" path hops created by intermediate nodes which forwarded RREQ
- ➢ Intermediate node:
  - Create next-hop entry for destination as RREP is received, forward along "reverse path" hop
  - Increment hop-count field in RREP and forward
- ➢ Source:
  - If multiple replies, uses one with lowest hop count

### 3.3.2.2. Route Maintenance

Used when link breakage occurs:

- ➢ Link breakage is detected by link-layer ACK, "passive ACK", AODV "Hello" messages.

Detecting node may attempt "local repair":

- ➢ Send RREQ for destination from intermediate node.

Route Error (RERR) message generated

- ➢ Contains list of unreachable destinations
- ➢ Sent to neighbors who recently sent packet which was forwarded over broken link and propagated recursively

### 3.3.3. MAODV message Format

| 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Type | | | | | | | | Data | | | | | | | | | | | | | | | | | | | | | | | |

**Figure.1.MAODV message Format**

MAODV message format is of 32-bit length. The first 8-bits are used to display the type of MAODV message and the remaining 24-bits are allotted for data.

**Type:** Specifies the format of the message.

**Table -1 Message Types**

| Type | Description |
|---|---|
| 1 | RREQ, Route Request. |
| 2 | RREP, Route Reply. |
| 3 | RERR, Route Error. |
| 4 | RREP-ACK, Route Reply Acknowledgment. |

**Data:** Variable length.

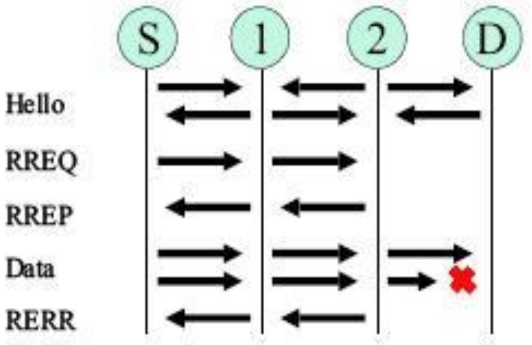
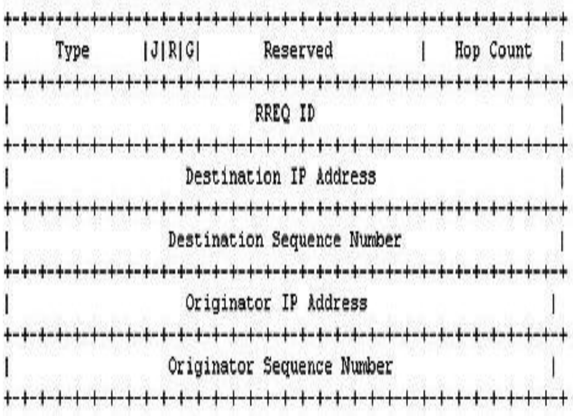


Figure .2MAODV- RREQ and RREP sequence

S-Source D-Destination 1, 2-Intermediate nodes

#### 3.3.3.1. RREQ message format



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |J|R|G|      Reserved         |   Hop Count   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            RREQ ID                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination IP Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Destination Sequence Number                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Originator IP Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Originator Sequence Number                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

**Figure.3 RREQ message format**

While communication routes between nodes are valid, MAODV does not play any role.

- A RREQ message is broadcasted when a node needs to discover a route to a destination.
- As a RREQ propagates through the network, intermediate nodes use it to update their routing tables (in the direction of the source node).
- The RREQ also contains the most recent sequence number for the destination.
- A valid destination route must have a sequence number at least as great as that contained in the RREQ.

**Table -2 RREQ Packet Header**

| FIELD | DESCRIPTION |
|---|---|
| Type | 1 |
| J | Join flag; reserved for multicast |
| R | Repair flag; reserved for multicast |
| G | Gratuitous RREP flag; indicates whether a gratuitous RREP should be uni-cast to the node specified in the Destination IP Address field |
| Reserved | Sent as 0; ignored on reception. |
| Hop Count | The number of hops from the Originator IP Address to the node handling the request. |

| | |
|---|---|
| RREQ ID | A sequence number uniquely identifying the particular RREQ when taken in conjunction with the originating node's IP address |
| Destination IP Address | The IP address of the destination for which a route is desired |
| Destination Sequence Number | The greatest sequence number received in the past by the originator for any route towards the destination. |
| Originator IP Address | The IP address of the node which issued the Route Request |
| Originator Sequence Number | The current sequence number to be used for route entries pointing to (and generated by) the originator of the route request |

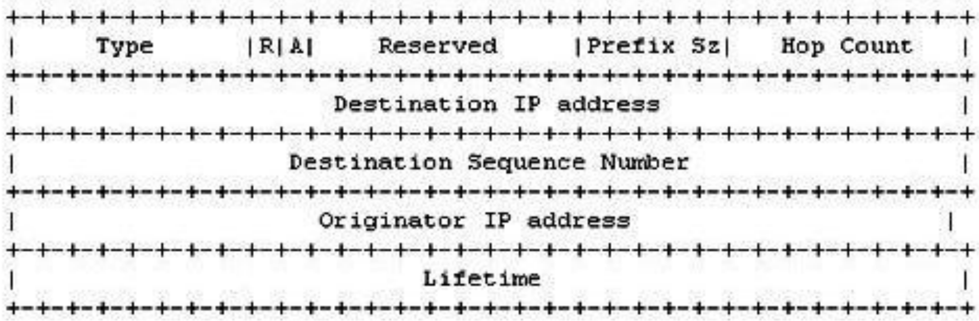
### 3.3.3.2. RREP message format

When a RREQ reaches a destination node, the destination route is made available by unicasting a RREP back to the source route.

A node generates a RREP if:

- It is itself the destination.
- It has an active route to the destination. Ex: an intermediate node may also respond with an RREP if it has a “fresh enough” route to the destination.

As the RREP propagates back to the source node, intermediate nodes update their routing tables (in the direction of the destination node)



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |R|A|    Reserved     |Prefix Sz|   Hop Count   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Destination IP address                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Destination Sequence Number                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Originator IP address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Lifetime                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

**Figure.4. RREP message format**

**Table-3 RREP Packet Header**

| FIELD | DESCRIPTION |
|---|---|
| R | Repair flag; used for multicast. |
| A | Acknowledgment required; |
| Reserved | Sent as 0; ignored on reception |
| Prefix Size | If nonzero, the 5-bit Prefix Size specifies that the indicated next hop may be used for any nodes with the same routing prefix (as defined by the Prefix Size) as the requested destination |
| Hop Count | The number of hops from the Originator IP Address to the Destination IP Address. For multicast route requests this indicates the number of hops to the multicast tree member sending the RREP. |
| Destination IP Address | The IP address of the destination for which a route is supplied |
| Destination Sequence Number | The destination sequence number associated to the route |
| Originator IP Address | The IP address of the node which originated the RREQ for which the route is supplied |
| Lifetime | The time for which nodes receiving the RREP consider the route to be valid. |

#### 3.3.3.3. RERR message

This message is broadcast for broken links.Generated directly by a node or passed on when received from another node.With a type number=3, RERR indicates error messages for broken links, non-transmitted packets.

#### 3.3.3.4. RREP-ACK message

This message is broadcasted for passive acknowledgement from the destination or intermediate node.When a source even after receiving RREP does not send packets to the destination, delivers the above temporary message.It can ask the destination to wait for a while for packet transfer. This message is uni-directional i.e., it is transmitted from sender to receiver with type number=4.It helps in maintaining route information and its status.

### 3.3.4. Security in Vehicular Ad Hoc networks

Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. Unlike the wire line networks, the unique characteristics of mobile ad hoc networks pose a number of nontrivial challenges to security design, such as open peer-to-peer network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. These challenges clearly make a case for building multifence security solutions that achieve both broad protection and desirable network performance. In this article we focus on the fundamental security problem of protecting the multihop network connectivity between mobile nodes in a VANET. We identify the security issues related to this problem, discuss the challenges to security design, and review the state-of-the-art security proposals that protect the VANET link- and network-layer operations of delivering packets over the multihop wireless channel. The complete security solution should span both layers, and encompass all three security components of prevention, detection, and reaction.

#### 3.3.4.1. Security Issues

Security for Vehicular ad-hoc networks is becoming an attractive challenge for many researchers today. To secure an ad hoc network, the following attributes may be considered:

- Availability
- Confidentiality
- Integrity
- Authentication
- Non-repudiation

Other factors that serve as challenge for a VANET are lack of centralized node, poor authentication, no packet loss recovery, etc.Without some form of network-level or link-layer security, a VANET routing protocol is vulnerable to many forms of attack. It may be relatively simple to snoop network traffic, replay transmissions, manipulate packet headers, and redirect routing messages, within a wireless network without appropriate security provisions. While these concerns exist within wired infrastructures and routing protocols as well, maintaining the "physical" security of the transmission media is harder in practice with VANETs. Sufficient security protection to prohibitdisruption of modification of protocol operation is desired. This may be somewhat orthogonal to any particular routing protocol approach, e.g. through the application of IP Security techniques.

## IV.CONCLUSION AND FUTURE ENHANCEMENTS

In the Wireless Technology, vehicles are becoming a part of the global network.In VANET packet forwarding is usually preferred in order to propagate urgent traffic related information to all reachable nodes within a certain dangerous region. The selective forwarding based alert message propagation scheme that uses a few predetermined forwarders with the right to re-broadcast the message. Multicasting can efficiently support a wide variety of application that are characterized by a close degree of collaboration typically for VANETs.The performance of a multicast session in a VANET depends on many factors such as the number of multicast senders, the number of multicast receivers, and the positions of vehicles. Secure communication, an important aspect ofany networking environment, is an especially significantchallenge in ad hoc networks. In this thesis we provide a thorough description of the existing of the multicast protocol MAODV and how the protocol can be made more secure by providing end to end data forwarding between the node.The general feeling is that vehicles could benefit from spontaneous wireless communications in a near future, making VANETs a reality. Vehicular networkswill not only provide safety and life saving applications, but they will become a powerful communication tool for theirusers. Thus the MAODV is being simulated and solutions are realized in Ns-2(Network Simulator) to prove assumptions considered in current work. Ns-2 is an object-oriented event-driven simulator with extensive support for simulation of MAODV. An initial study of network simulator has been done.

## V. REFERENCE

[1] V. Naumov and T. R. Gross, "Connectivity-Aware Routing (CAR) in Vehicular Ad Hoc Networks," in *INFOCOM.* IEEE,pp.1919 - 19272007.

[2] Stephan Eichler , "Performance Evaluation of the IEEE 802.11pWAVE Communication Standard", in proceedings of *66th Vehicular Technology Conference,IEEE,* pp. 2199 – 2203, 2007. VTC-2007.

[3] Yao-Tsung Yang, Li-Der Chou, "Position-based Adaptive Broadcast for Inter-Vehicle Communications*", in proceedings of IEEE Communications Society subject matter experts for publication in the ICC 2008 workshop,*pp.410-414,2008.

[4] Yunyue Lin, QishiWu, XiaoshanCai, Nageswara S.V. Rao, "Optimizing Base Station Deployment in Wireless Sensor NetworksUnder One-hop and Multi-hop Communication Models",*15th International Conference on Parallel and Distributed Systems*,pp.96-103,2009.

[5] Mancia anguita, javierd´iaz, eduardoros, and f. Javier fern´andez-baldomero, "optimization strategies for high-performance
Computing of optical-flow in general-purpose processors", *IEEE Transactions On Circuits And Systems For Video Technology*, vol. 19, no. 10, pp .1475-1488,2009.

[6] Wenjingwang, feixie and mainakchatterjee, "Small-Scale And Large-Scale Routing In Vehicular Ad Hoc Networks*", IEEE Transactions on Vehicular Technology*, vol. 58, no. 9, pp.5200-5213, 2009.

[7] Bing Han, Jimmy Leblet, and Gwendal Simon, "Query Range Problem in Wireless Sensor Networks", *IEEE Communications Letters*, vol. 13, no. 1, pp55-57, 2009.

[8] S. Biswas, R. Tatchikou, and F. Dion, "Vehicle-to-Vehicle Wireless Communication Protocols for Enhancing Highway Traffic Safety," *IEEE Communication Magazine,* vol. 44, pp. 74–82, 2006.