CHAPTER 4

IMPLEMENTATION OF MSRDMP FOR GROUP MANAGEMENT AND ROBUSTNESS IN MSRDMP

4.1 INTRODUCTION

Multicast communication takes important role in group communication. The process of achieving reliable packet delivery between a sender to multiple receivers faces a great challenge. Generally multicast routing protocol designed for MANET has to face a lot of problems as the MANET do not support centralized control and no fixed infrastructure. Due to the mobility of nodes, link stability between group leader and members of the group often get terminated in multicast routing. This chapter focuses on implementation of the proposed multicast routing protocol MSRDMP. Robustness refers to the ability to withstand a failure. Attention has to be made in multicast routing when the packet delivered is not received by the members of the multicast group. It is important to know that how the transmitting packet is affected by signal propagation, hidden and exposed terminal problems. The group leader in multicast group has the specific role which should be managed in an effective way so that the performance of multicast routing is highly acceptable. The way group leader is selected and managed help the routing protocol to improve the performance. The recovery of lost packet can improve the throughput. The following section describes about the hurdles to transmitting packet in wireless communication and the hurdles faced by the group leader of multicast routing, leadership selection algorithm, group management through alert message and achievement of robustness in MSRDMP.

4.2 HURDLES TO TRANSMITTING THE DATA PACKET

Wireless communication is quite different from wired communication. The probability of transmitted packet loss is slightly higher than wired communication. The data packet is transmitted in the form of electromagnetic waves. In chapter one, section 1.4 describes the disturbances to signal propagation in wireless communication. In addition to those problems like blocking, reflection, refraction, scattering and diffraction, the hidden and exposed terminal problem is very prevalent and can’t be exempted. These problems cause a greater impact to the loss of data packet in wireless communication.

In the wireless communication the radio spectrum is very limited, so the bandwidth available for multiplex communication is limited. Design of MAC protocol must involve efficient utilization of bandwidth and control overhead associated with this must be kept as minimal as possible. Offering quality of service is very difficult due to the inherent mobility nature of ad hoc wireless networks. The MAC protocols used in real-time application designed for ad hoc wireless should have a resource reservation mechanism. Gupta et al (2003), Chun et al (2004), Wi & Chang (2005) suggested that some MAC protocols for reliable multicast and broadcast use busy tones and control packet exchange to recover hidden terminal problems . Tang & Gerla (2000) stated that the Broadcast Support Medium Access Protocol (BSMA) is one of the first tasks that involve exchange of control packets to provide reliable MAC layer protocol .As stated earlier that MANET does not have centralized control. Coordination and access to the channel should be scheduled in a distributed manner. Besides these problems, hidden and exposed problem is the major issues to be confronted by MAC protocols.

4.2.1 Hidden and Exposed Terminal Problem

The hidden terminal problem leads to collisions of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver. The Figure 4.1 depicts how the hidden terminal problem arises in the wireless network system. The nodes S1 and S2 are interested to send packet simultaneously to the receiver node R1 that causes the packet loss due to collisions of the packet.

The exposed terminal problem refers to the inability of a node, which is prevented to send packet to the indented destination as nearby node is already engaged in sending packet to its destination. In this Figure 4.1, if a transmission from node S1 to another node R1 is already in progress, node S3 cannot transmit to node R2. The hidden and exposed terminal problems significantly affect the throughput of a network. When the traffic load is high, it is therefore desirable that the MAC protocol be free from hidden and exposed terminal problems.

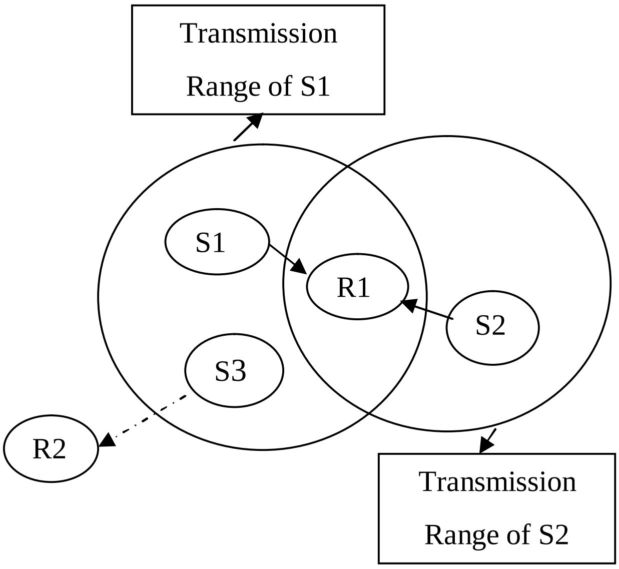

Figure 4.1 Hidden and exposed problems

These problems can be solved with the help of Request To Send (RTS) and Clear To Send (CTS) mechanism but the lost packet due to factors like reflection, diffraction, scattering, fading and interference cannot be recovered. The following section describes how the proposed protocol is designed and address the packet loss and how much helpful to increase the performance of multicast routing protocol.

4.3 HURDLES TO THE GROUP LEADER OF MULTICAST ROUTING

In multicast communication the packet gets transferred from a head of the group to members. This head is normally said to be leader head or group leader. The freedom of moment of nodes is a nature of MANET. Following is the difficulties or additional work has to be faced by the group leader of the multicast group. If nodes are deployed in a larger area then number of groups in that area will also become more. When the group leader moves away from the group it can’t further communicate with members of the group. If a number of group members of group leader are reduced to less than an expected number, then the group leader communicates to only a few group members. Due to bandwidth and hidden and exposed terminal problem the packet loss in the middle of network path is high. If loss of packet occurs, then group leader has to send it back to concerned group member alone.

This packet retransmission would defer the next packet to its entire member. In quite larger area when there are a number of groups, handing over the packets from one group leader to another group leader involves multiple hops between transmissions. This leads to failure packet delivery and it is very high. If there are a number of control messages, handling of control messages by group leader would cause inflexible control overhead. Group maintenance and initialization would make the group leader perform additional task of membership coordination. If it is sender initialization, the source has to look after the joining request made by a node likely to join and has to maintain the state information of the receiver.

4.4 PROPOSED MULTICASTING PROTOCOL MSRDMP

The above mentioned problems associated with group leader described in section 4.3 can be solved by the way group construction is carried out and the way group leader is selected and managed from available nodes in a group. In the previous chapter establishment of group construction in the newly proposed protocol MSRDMP is dealt. The following section of this chapter explains the model assumption, the way how group leader is selected and how robustness is achieved in the group communication established using MSRDMP.

4.4.1 Model Assumption

With the help of following assumptions, MSRDMP protocol has been implemented for effective performance improvement in multicast routing. Most of the mobile nodes available in the market are equipped with global positioning system, but the transmission range of the nodes depends on the IEEE 802.11 standard. This proposed protocol MSRDMP opted for IEEE 802.11b, which is capable of offering 500 meter range of transmission in outdoor. A node must be equipped with global positioning system. Transmission range limit considered based on IEEE 802.11b standard. The virtual reference point is assumed to position the node in the group. The leadership track node is not limited to roaming around virtual reference point. A group is formed within the radius of R/2 if the range is R.

4.4.2 Selection of Group leader in MSRDMP

In a multicast communication, any one of the nodes acts as a group leader. Group leader is selected in a manner that it is capable of transmitting data packets to a maximum number of group members. In this proposed MSRDMP protocol, the group leader is selected in an efficient manner after groups have been constructed with respect to virtual reference point; Leader for each group is selected using hello packets and proper updating of tables maintained by each node. In a group, a node which is closer to VRP floods ‘n’ number of hello packets where ‘n is equal to number of group member expected to join that particular group. Nodes that are in direct transmission range would definitely receive the hello packet. The nodes which are capable of receiving the hello packets would reply by sending Acknowledgment (ACK) messages. The node which sent the hello packet first would update its Number of Nodes in the Range (NNR) value in the table maintained by it, upon receiving ACK messages from nodes in direct transmission range.

Similarly the node which is next closer to VRP performs the same operation to update NNR value in its table. If NNR value of a node is greater than or equal to the half of the total number of nodes in the particular group then the node is eligible to take part in the leadership selection process. All eligible nodes inform about its NNR value to the rest of nodes within that group. On receiving NNR value all nodes compare it with their own value, if it is greater than the received NNR value, then the node with greatest NNR value assumes that it is the group leader of that group. It will send the Request to Join (RTJ) messages to the rest of the nodes in that group.

The node which is interested to elect that node as a group leader would reply by sending the Request to Join Acknowledgement (RTJACK). On receiving RTJACK messages, the node will update its Number of Group Member (NGM) value in its table. After this process is over, a node which has a maximum value of NGM is elected and announced as group leader by leadership track node. Leadership track node updates its own table and announces the address of the group leader to all other nodes within that group. If any of the non participant nodes wants to join the group later may send a Join Request (JR) message and can be the member of that group on receiving Acceptance Reply (ARY) messages from the group leader of that group.

4.4.3 Group Management - Creation of Alert Message

In order to make aware of the movement of the group leader and leadership track node, MSRDMP creates an alert message which is exchanged between group leader and leadership track node. Node stability is identified with the help of location updating approach, the table which provides this information is called as a neighbor table as explained by Misra et al (2008). In this work MSRDMP protocol uses two parameters. One is Received Signal Strength (RSS) which is used to calculate Signal to Noise Ratio (SNR) and the other is location information obtained from global positioning system. Using these two parameters MSRDMP can construct stable group construction.

In this MSRDMP protocol group leader’s distance from virtual reference point is identified with the help of GPS mechanism. This proposed MSRDMP uses both GPS value and RSS value to make a decision that determines leadership track node movement and create alert messages to guide group leader. Lifetimes of route depend on the distance between the nodes, which can be calculated approximately using received signal strength. In noisy environments RSS is used to calculate the signal to noise ratio and thereby link quality can be predicted. Even though a poor SNR value can lead to a broken link, the SNR offers more relevant information because it is related to the node’s movements. More dramatically, SNR greater than zero, assumes that nodes are getting closer or nodes are moving towards a location with less interference. In contrast SNR less than zero, assumes that nodes are moving away or nodes are getting into noisier locations. Signal-to noise ratio is defined as the power ratio between a signal and background noise. Poor bandwidth is also considered as noise

$$\mathrm{SNR} = \frac{P_{Signal}}{P_{Noise}} \tag{4.1}$$

In the formula expressed in (4.1) P is average power. Both signal and noise power are measured at the same points in a system, and within the same system bandwidth. SNR are often expressed using the logarithmic decibel. In decibels, the SNR is defined as expressed in the formula (4.2).

$$\left.\begin{aligned} \mathrm{SNR}_{\mathrm{db}} &= 10\log_{10}\frac{P_{Signal}}{P_{Noise}} \\ \mathrm{SNR}_{\mathrm{db}} &= P_{signal}db - P_{noise}db \end{aligned}\right\} \tag{4.2}$$

As stated earlier MSRDMP uses IPV4 format to multicast the datagram. The option field in the IPV4 is used for updating the information about how far group leader is away from the virtual reference point. Each time a data packet is multicast, this distance about group leader is also padded with datagram packet. The leadership track node is also one of the members of the multicast group. It makes use of this information to create alert message. By default leadership track nodes stores the value of D_O, this D_O is initially is equal to R/2 where R is the transmission range of mobile nodes. D_C is the current location of the group leader and it is padded with packets each time group leader multicast those packets to its group members. The leadership track node calculates the cutoff range Cr using the expression (4.3)

$$\mathrm{C_r = D_o - D_c} \tag{4.3}$$

Using these two values Cr and SNR decibel, LTN creates the alert message. If Cr falls negative, LTN informs the GL that it moves away from the virtual reference point. The Table 4.1 denotes the alert message. This alert message helps the LTN make its move as well as alerts GL. The MSRDMP provides the features that LTN need not be confined to certain radius, it can move either forward or backward depending on the SNR_{db} value and GPS value.

Table 4.1 Mutual Alert Message

SNR_{db}	C_r	Alert Messages
>0	+	LTN moves either forward or backward
<0	+	LTN moves backward
>0	-	LTN holds on
<0	-	LTN moves backward

4.4.4 Persistence Leader Selection Algorithm

The following algorithm explains how leadership selection process is carried out in MSRDMP .The notation used in algorithm is written first before starting of the algorithm. Let

H-pkt represents Hello Packet

n- represents Number of Packet

N- represents Number of nodes in the Group

R_{L-} represents Range Limit

i-refers to indicate each node

BEGIN

```
Flood ((H-pkt), n) to all nodes (N)
$NNR_i$= 0
If $N_i$ within $R_L$ then
          Forward (ACK) by $N_i$ to all $N_{i-1}$to $N_{i-n}$
          Upon receiving an ACK, For all $N_{i-1}$to $N_{i-n,}$ Each node updates
          $NNR_i$=NNR++
Else remains $NNR_i$= 0
For all $N_{i-1}$to $N_{i-n}$
 If ($NNR_i$>=N/2)
Flood ($NNR_i$ Value) by $N_i$ to all nodes $N_{i-1}$to $N_{i-n}$
$NGM_i$= 0
Upon receiving NNR value, If ($NNR_i$ of $N_i$ >$NNR_{i+1}$ of $N_{i+1}$ (other nodes
within range) then Flood (RTJ) by $N_i$ to all $N_{i-1}$to $N_{i-n}$
Upon receiving positive acknowledgement, i.e. If (RTJACK= =1) then
$NGM_i$=NGM++
Else
All other node with its NNR value is the minimum wait for LTN
For all $N_i$ to $N_{i-n}$
For all $N_j$ to $N_{j-n}$
     If ($NGM_i$ >$NGM_j$)
          NGM $_i$= GL (A node which has highest NGM value declared as
          Group Leader)
After selection of GL, LTN updates address of GL as its AGL value
Forward (DP–pkt) by GL to all $N_{i-1}$ to $N_{i-n}$
```

```
If ($SNR_{dp}$>0&& $C_r$= = Positive value) then LTN moves either direction
Elseif ($SNR_{dp}$<0&& $C_r$= = Positive value) then LTN moves backward
Elseif ($SNR_{dp}$>0&& $C_r$= = Negative value) then LTN holds on and Send (Alert- pkt) by LTN to GL
Elseif ($SNR_{dp}$<0&& $C_r$= = Negative value) then LTN moves backward Send (Alert- pkt) by LTN to GL
Else
    Forward (DP–pkt) by GL to all $N_{i-1}$to$N_{i-n}$
  END
```

4.5 ROBUSTNESS IN MSRDMP

It is a well known fact that the number of collisions increases with respect to the number of nodes in a group and transmission range of the node. The primary objective of this protocol MSRDMP is, group leader has to transmit the packet to its member without failure. If any mishap occurs during the transmission, how a failed transmission to a particular group member can get a lost packet is a greater challenge in multicast group communication. To overcome the hidden and exposed problem CTS and RTS mechanism is introduced in many protocols, but they have not considered the packet loss after transmission is over.

4.5.1 Primary Collision Avoidance CSMA/CA Mechanism

The medium access mechanism of IEEE 802.11 uses CSMA/CA for unicast packet transmission. Carrier sensing is performed by physical and virtual mechanism. The virtual mechanism uses some control frames that are transmitted to reserve the medium prior to transmission of unicast data packets. Figure 4.2 describes working of CSMA/CA mechanism. A node which acts as a transmitter, keeps sensing the medium, if it finds the medium to be idle for some period of time, it sends a RTS control frame with source and destination address and the duration for which the medium is to be reserved. All nodes other than the receiver, which hear the RTS, set their Network Allocation Vector (NAV) as mentioned in the RTS control frame. NAV is a time period, which is equal to the time to be elapsed for transmitting a CTS control frame, a DATA packet and acknowledgment (ACK) and the summation of three Short Interframe Space (SIFS) time. After a SIFS time period receiver replies with CTS control frame when it senses the medium to be free .At this time all nodes other than the transmitter, which hear the CTS and had not heard the RTS before, would set their NAV to the time period stated in the CTS.

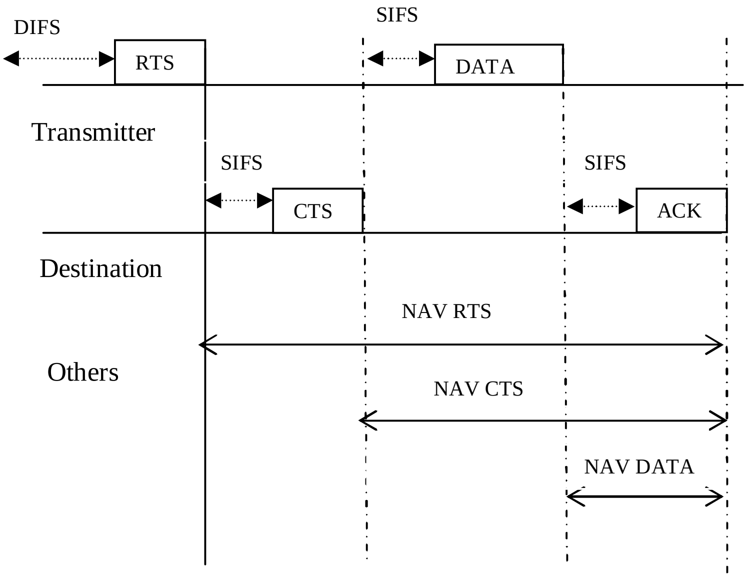

Figure 4.2 Basic CSMA/CA mechanism

Here NAV set by these nodes is equal to the time period to be elapsed for transmitting a DATA packet, an ACK and summation of 2 SIFS time. After the successful reception of the CTS frame by the transmitter, it is confirmed that the medium has been reserved for some period of time. On knowing this confirmation the transmitter waits for a SIFS time and sends the data packet to the intended receiver. The receiver waits for a SIFS time and replies an ACK to transmitter confirms that DATA have been delivered successfully. When a transmitter senses that the medium is not idle, it waits for a Distributed Interframe Space (DIFS) time period. It means that the transmitter defers the transmission deliberately until end of DIFS time interval that is calculated from back-off counter. The value of this back-off counter changes from 0 to Contention Window size (CW).

The back off counter time is chosen between contention window size minimum (CW_{min}) and contention window size maximum (CW_{max}). The value of CW varies from 32 to 1024 based on the recent history of transmissions made by the transmitter. If the transmitter is not successful in transmitting a packet, it implies that it has suffered collisions, and then its CW becomes larger. The CW value is doubled with every unsuccessful transmission of a packet and is reset to 32 on a single success. The back-off counter value is a random number between 0 and CW. During back-off interval the transmitter keeps on sensing the medium, if the medium is found busy, the transmitter freezes its back-off counter until the medium becomes free again, then the medium becomes idle, the back-off counter is resumed from where it was frozen. If the medium remains free and back-off counter becomes 0 after that the transmitter sends the DATA packet. All receivers detect the transmitted packet, and receive the same and send it up to routing layer. The routing layer decides that the packet is required to be forwarded if the node is in the multicast tree.

The above mechanism does not ensure protection from hidden terminals nor guarantee the DATA was received correctly. If any of the group members does not receive the packet, what does it do? It is a question to be addressed seriously. This report explains a new data recovery mechanism to recover the lost data packet if the data is not received correctly by any of the group members in the multicast group

4.5.2 Interim CTS request- Recovery mechanism

The robustness and reliability can be achieved while performing effective collision avoidance and recovery mechanism. The proposed MSRDMP protocol introduces a new CTS request called interim CTS used by the group member which has not received the packet within the threshold time set in every transmission. It is presumed that at most three possible collisions may occur in this MSRDMP multicast protocol. The one is, the time leadership track node floods the address of group leader. The second is, the collision may occur when new member sends join request to group leader and third one is, when the interim CTS request sent by the victim group member. The group member is said to be the victim group member if it has not received the packet sent by the group leader.. If a collision occurs, it is necessary to defer the transmission for a quiet period of time using optimum contention window.

4.5.2.1 Contention widow deferred transmission time

The MSRDMP calculates the contention window time. It is used to determine that how long a data packet is to be deferred before multicasting the packet. Only if the medium is sensed idle for the full duration of DIFS, the node can access the medium for transmission. If not, sending station has to wait a random amount of time chosen within a contention window. Chhaya & Gupta (1997), Ho & Chen (1996) have explored that constant or geometrically distributed back off window has been employed in many medium access protocol design while Ho & Chen(1996) stated that an exponential back off time is limited to two phase method employing Markov Chain analysis.

The value of CW differs between CW_{min} and CW_{max}. The time duration is all integral multiples of slot times. To construct optimum contention window, SIFS short interframe space time of 10µs is set for the MAC 803.11 DCF distributed coordination function and consequently DIFS is also set. SIFS is the minimum time period between the data frame and its acknowledgement and DIFS refers to the minimum time period; the medium has to be idle for transmission. If the channel is identified busy during the DIFS interval the station must have to defer its transmission. DIFS duration is calculated as follows DIFS= SIFS+2*Slot time. In IEEE 802.11b standard slot time is 20µs, therefore DIFS measured as 50µs.

In MSRDMP protocol, the group is constructed in such a way that all group members are wandering within its transmission range. A single hop transmission is carried out within a group. Hence number of intermediate nodes at most is only one. This intermediate is also called leadership track node. It takes responsibility to send the packet to group leader that belongs to adjacent group and to the victim group member which has not received the packet within the group to which LTN belongs.

Once a collision is happening, it is essential to defer the transmission to achieve the reliability. Here MSRDMP employed the truncated binary exponential back off time calculation to create contention window, which represents a random number of slot time between 0 and 2^d-1, chosen after d collusions. It is denoted by CWmax and calculated using the formula expressed in Equation (4.4). Here d denotes the number of RTS request sent by the group leader on every SIFS time period. If CTS are not received after SIFS of time, then d value is one, again the group leader sends RTS request, if it is not received with CTS request, then d value is two, the same way d is calculated on every attempt of RTS request failure.

$$CW_{max} = 2^d - 1 \qquad (4.4)$$

$$CW_{max} = N \qquad (4.5)$$

In the formula (4.4) d is used to denote the number of collision likely to be occurring. In the formula (4.5) N represents a maximum contention value which is also called the expected back off time equal to CW_{max}. If a collision occurs, the number of collisions have to be identified and CW_{max} found out, which in turn gives N value. Using this N value, truncated mean slot time is calculated using the formula expressed in (4.6). $M_{d.}$is referred to denote truncated mean slot time.

$$M_d = \frac{1}{N+1} \sum_{i=0}^{N} i \qquad (4.6)$$

For Example, if the collision occurs three times, then the expected back off time is calculated applying the equations (4.4) (and 4.5) as follows

$CW_{max}=2^3-1=8-1$

$CW_{max}=7$ N=7

To calculate the Truncated mean slot time, apply the formula expressed in (4.6) as given below

$$M_3 = \frac{1}{7+1} \sum_{i=0}^{7} i$$

$$= \frac{1}{8}(0+1+2+3+4+5+6+7)$$

$$= \frac{28}{8}$$

$$M_3 = 3.5$$

The truncated mean slot time is 3.This truncated mean slot time is used to determine Contention Waiting Time (CWT) expressed in the formula (4.7).

$$\text{CWT} = M_d \times \text{DIFS} \qquad (4.7)$$

Normally DIFS refers to distributed interframe space, which specifies how much delay is to be made before performing sending operation. DIFS is taken as 50µs for simulation. If d is 3 then M_d is 3.5 after being truncated, then the value becomes 3 so CWT is 150µs by applying the Equation (4.7). If collision occurs three times, packet delivery is deferred for 150µs.

4.5.2.2 Invocation of interim CTS request for robustness

Once medium is idle for sending the packet, group leader send the RTS request to group members. This RTS request contains Packet Delivery Time (PDT) value which represents how much time a transmitting packet takes to arrive at destination nodes. The PDT value depends on packet size, transmission time and propagation time. Transmission time is defined as the amount of time taken by the packet from the first bit to the last bit, leaving the transmitting node, the following formula (4.8) expresses, the transmission time.

$$\text{Transmission Time} = \text{Packetsize/Bitrate} \tag{4.8}$$

On the other hand, propagation time is defined as the amount of time taken by the packet to reach its destination. The propagation speed depends on communication medium of the link. For wireless communication propagation speed is equal to the speed of the light. The propagation time of the physical link is calculated by dividing distance in meter by its propagation speed in m/s

$$\text{Propagation Time} = \text{Distance in meter/Propagation speed} \tag{4.9}$$

Here transmission range of the node is 250m. The packet delivery time is calculated as the sum of both transmission time and propagation time, which is expressed in the following formula (4.10)

$$\text{Packet Delivery Time} = \text{Transmission Time} + \text{Propagation Time} \tag{4.10}$$

Among the multicast routing protocol having been introduced in the market, no protocols provide recovery of the packet lost by a particular multicast group member. The packet propagated in wireless medium has to suffer a lot of electromagnetic interference problem, Problems like diffraction, reflection, signal fading cause a packet to lose. In MSRDMP protocol offers both collision avoidance and recovery mechanism. The RTS / CTS mechanism is used to avoid the collision among the participating nodes. The MSRDMP protocol uses the Interim CTS (ICTS) request to recover the lost packet from leadership track node of the multicast group. The ICTS is the extension of the RTS / CTS mechanism.

The decision to invoke the Interim CTS is carried out by the Group member that has not received the multicast packet yet within PDT .When group leader sends the RTS request to its indented destination, it also mentions the packet delivery time with RTS request. All the nodes within the group know about packet delivery time. The multicast group makes use of threshold packet delivery time to determine whether it loses a packet or not. The following diagram shown in the Figure 4.3 narrates how Interim CTS request works on recovery of lost packet. In fact ICTS request is invoked whenever the group member has not received the packet.

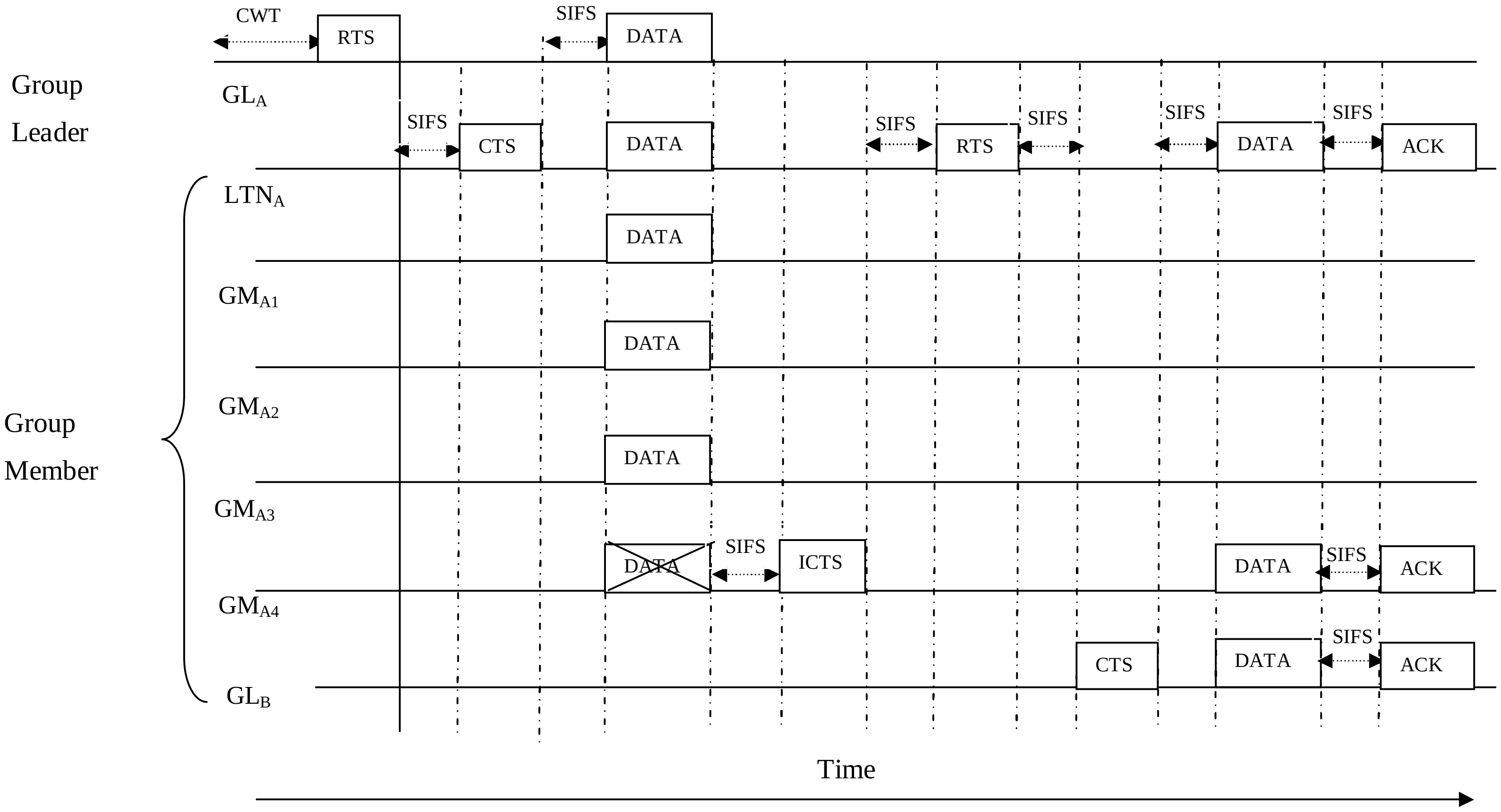

Figure 4.3 Reliable recovery ICTS mechanism

After a definite time of CWT the Group Leader (GL_A) of Group A sends an RTS request to Leadership Track Node (LTN_A) of Group A. On receiving the RTS signal, LTN_A sends back the CTS signal to GL_A after a definite time of SIFS. GL_A assumes that it is free to send data packet to its entire group member (GM_{Ai-n}). GL_A sends multicast packet to all group members. In case if any of the group members has not received the packet within the threshold packet delivery time then it has to invoke the ICTS request to LTN_A.

For instance in the Figure 4.3 the Group Member (GM_{A4}) has not received the packet, and henceforth called as a victim group member then it sends the ICTS request to LTN_A. Meantime LTN_A has the responsibility to send the received data packet to its adjacent Group Leader B (GL_B). Upon receiving the ICTS request from GM_{A4}, LTN_A gets an additional responsibility to send the lost data packet to GM_{A4}.

Once LTN_A finishes RTS/CTS request cycle between LTN_A and Group Leader (GL_B) of Group B, then it is ready to send data packet to Group Leader (GL_B) of Group B and the victim group member (GM_{A4}) of Group A. After SIFS of time, Group Leader (GL_B) of Group B and the victim group member (GM_{A4}) of Group A send acknowledgment to LTN_A. As soon as LTN_A receives the acknowledgement, it also sends the acknowledgement to Group Leader (GL_A) of Group A. The reliable packet transmission flow diagram is shown in the Figure 4.4. This is how MSRDMP protocol provides a recovery mechanism to a lost data packet.

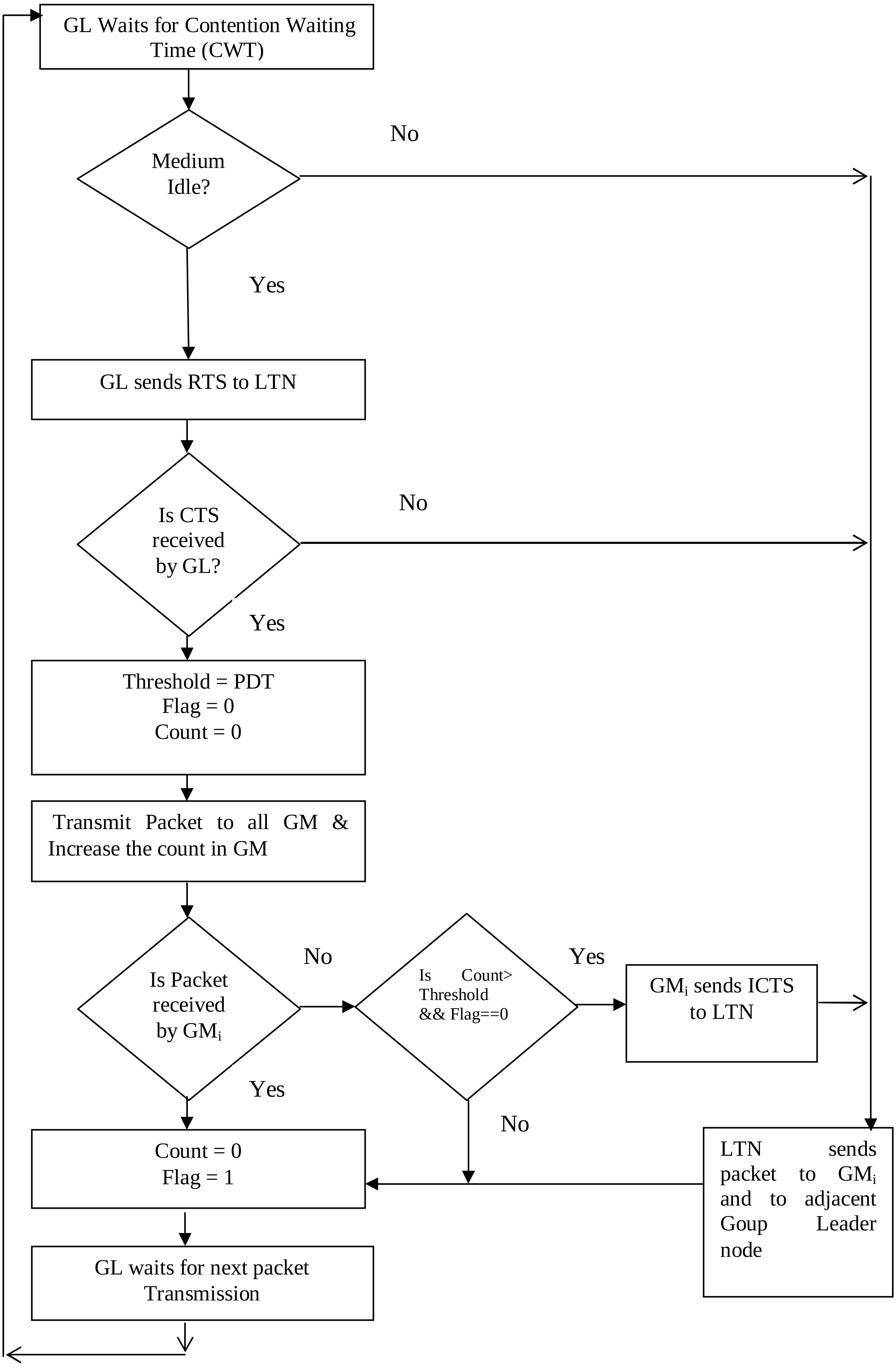
GL Waits for Contention Waiting Time (CWT)
Medium Idle?
No
Yes
GL sends RTS to LTN
Is CTS received by GL?
No
Yes
Threshold = PDT
Flag = 0
Count = 0
Transmit Packet to all GM & Increase the count in GM
Is Packet received by GM$_i$
No
Yes
Is Count> Threshold && Flag==0
Yes
No
GM$_i$ sends ICTS to LTN
Count = 0
Flag = 1
LTN sends packet to GM$_i$ and to adjacent Goup Leader node
GL waits for next packet Transmission

Figure 4.4 The reliable packet transmission flow diagram

4.5.2.3 Reliable transmission algorithm

The algorithm given below describes how reliable transmission takes place in MSRDMP. The notation used in the algorithm is written before starting of the algorithm.

n	-	(Number of Packet)
N	-	Number of nodes in the Group
DP-pkt		-Data Packet
GL_A	-	Group Leader for Group A
LTN_A	-	Leadership Track Node for Group A
GL_B	-	Group Leader for Group B

Step1: GL_A waits up to CWT

Step2: GL_A sends an RTS signal

Step3: If LTN_A is free from transmission, sends CTS to GL_A

Step4: Set Threshold equal to PDT

Step5: Forward (DP–pkt) by GL_A to all N_{i-1}toN_{i-n}

Step6: If Count of GM_i is greater than Threshold then GM_i sends ICTS to LTN_A

Step7: LTN_A sends RTS to GL_B

Step8: GL_B sends CTS to LTN_A

Step9: Forward (DP–pkt) by LTN_A to GMi and GL_B

Step10: GM_i sends ACK to LTN_A

Step11: GL_B sends ACK to LTN_A

Step12: GL_B waits for CWT for its group

Step13: LTN_A sends ACK to GL_A

Step14: GL_A waits for CWT for the next cycle of transmission for its group

4.6 RESULT AND DISCUSSION

The protocol MSRDMP designed for multicast routing ensures the robustness in a dynamic environment. In performance evaluation, the proposed MSRDMP is compared with RSGM and ODMRP. RSGM is geographical aided multicast routing protocol, whereas ODMRP is mess structured multicast routing protocol for MANET. In order to compare and analyze the performance of proposed multicast routing protocol MSRDMP, the result data set for RSGM and ODMRP are extracted from a manuscript titled stateless multicasting in mobile ad hoc networks written by Xiaojing et al (2010)

4.6.1 Comparative scenario

The ODMRP is the fundamental multicast routing protocol and most of the protocols are derived based on it. The RSGM is the location aware scalable multicast routing protocol based on zone based group partition. The proposed MSRDMP is the location aware, scalable and robustness. So comparison is done with these two protocols. The MSRDMP is implemented with the help of the Global mobile simulation library.

In MSRDMP, the group is formed based on the transmission range. It is very much suited to be competent with hardware configuration and protocol evolution changes in present day scenario. In the military application robustness is very much needed to survive in the battle field. The following metrics were studied considering the impact of mobility, impact of node density for MSRDMP protocol: Packet delivery ratio is the ratio between the number of packets received and the total number of packets sent, Normalized control overhead is the total number of control messages transmitted divided by the total number of received data packets, Average Path length is the average number of hops traversed by each delivered data packet and Joining delay is the average time interval between a member joining a group and its first receiving of the data packet from that group

4.6.2 Impact of Mobility

The moving speed of a node makes a great impact on the performance of any protocol designed for MANETs. The link connectivity between any two nodes become too low as much speed as the two nodes travel a long distance per second. If moving speed is higher then connectivity would become lesser as a result of that a number of packets delivered per unit time will also decrease.

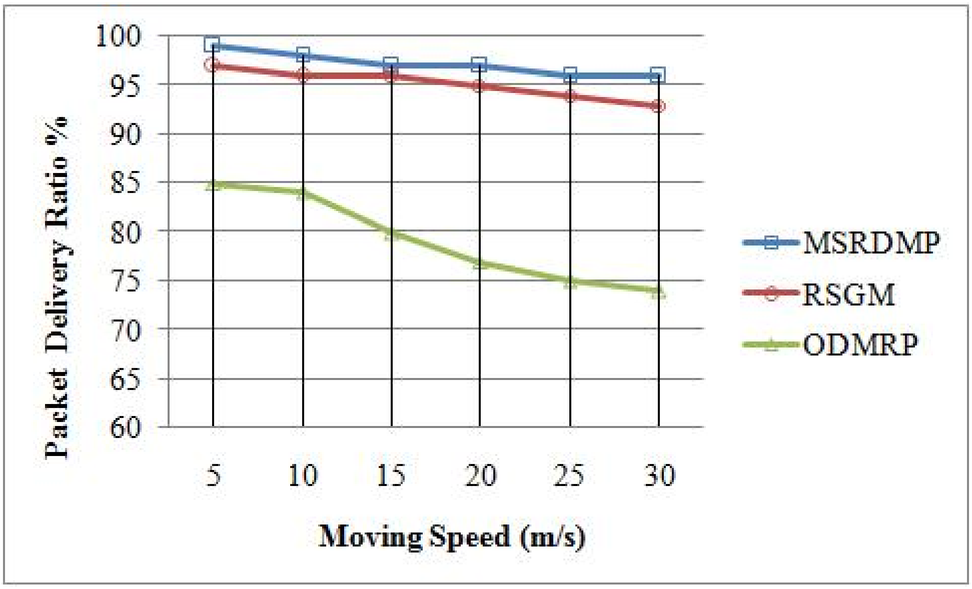

Figure 4.5 Packet delivery ratio versus moving speed

The Figure 4.5 shows the graph for packet delivery ratio versus moving speed. It clearly shows that the value for the packet delivery ratio for MSRDMP falls between 99% and 96% though the moving speed increasing gradually. The blue line goes in the graph shown in the Figure 4.5 is almost straight for MSRDMP. The RSGM is slightly inferior to MSRDMP. The green line for ODMRP moves downwards as the moving speed of node increases.

The Figure 4.6 shows graph for control overhead versus moving speed. The control overhead increases for all protocols when moving speed increases. The ODMRP incurs more control over head than the rest of two protocols MSRDMP and RSGM. For moving speed 30 m/s, the control overhead for RSGM and ODMRP is almost twice that of MSRDMP. The control overhead is 1.7 for RSGM and 2.1 for ODMRP .The graph depicted in Figure 4.6 shows that the blue line for MSRDMP falls below the ODMRP and RSGM.

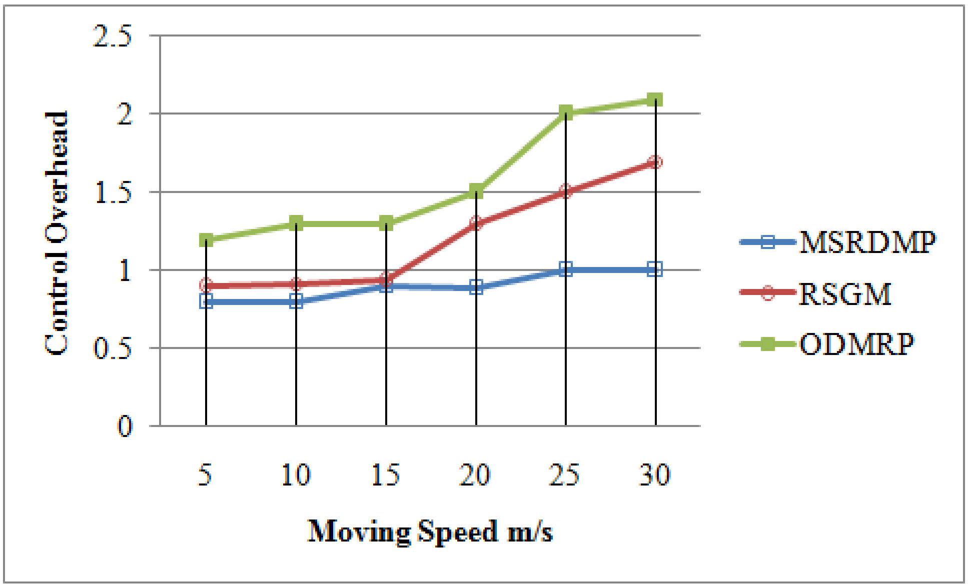

Figure 4.6 Control overhead versus moving speed

The Figure 4.7 shows the graph for average path length versus moving speed. A number of hops taken by the multicast packet is higher when the moving speed of node increases. In MSRDMP average path length increases due to the leadership track node moving away from the virtual reference point. The speed of the moving node does not affect the average path length of packets. In case of RSGM and ODMRP the packets take the number of hops when the speed of node increases.

The Figure 4.7 clearly depicts that the packets in MSRDMP take a moderate average path length because the packets take less than 5 hops. The blue color for MSRDMP goes far below the RSGM and ODMRP. Though adjacent group leader is far away from leadership track, the leadership track node delivers the packet to its next neighbor. The neighbors forwards the packets to its group leader later group leader would multicast the packet to all group members, therefore the average hops travelled by a packet is minimized in MSRDMP.

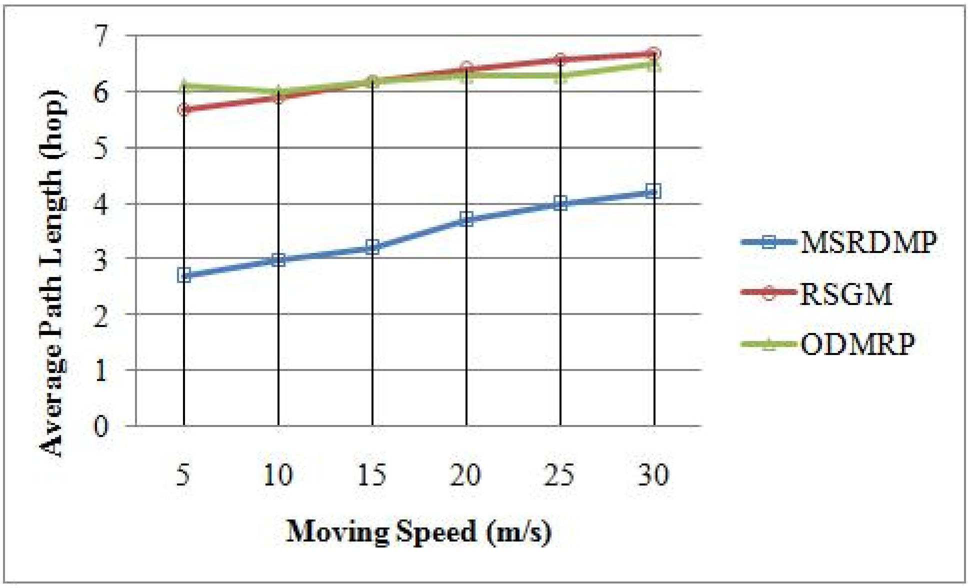

Figure 4.7 Average path length versus moving speed

The Figure 4.8 clearly indicates the graph for average joining delay versus moving speed for three protocols. As the mutual sharing alert message is exchanged between group leader and the leadership track node in MSRDMP, the group leader is mostly available within transmission range, the new node wants to join the group is easy and quickly responded by the group leader of that group. Even though the moving speed of the node increases gradually, the MSRDMP incurs a minimum joining delay.

For the moving speed 30 m/s, the joining delay for RSGM is almost as twice as the joining delay for MSRDMP. The joining delay for ODMRP is three times more than MSRDMP. The Figure 4.8 shows the graph in which blue line for MSRDMP passes along the x axis .Though joining delay is reduced to some extent for ODMRP when the speed of node increases, the green line is still high from MSRDMP.

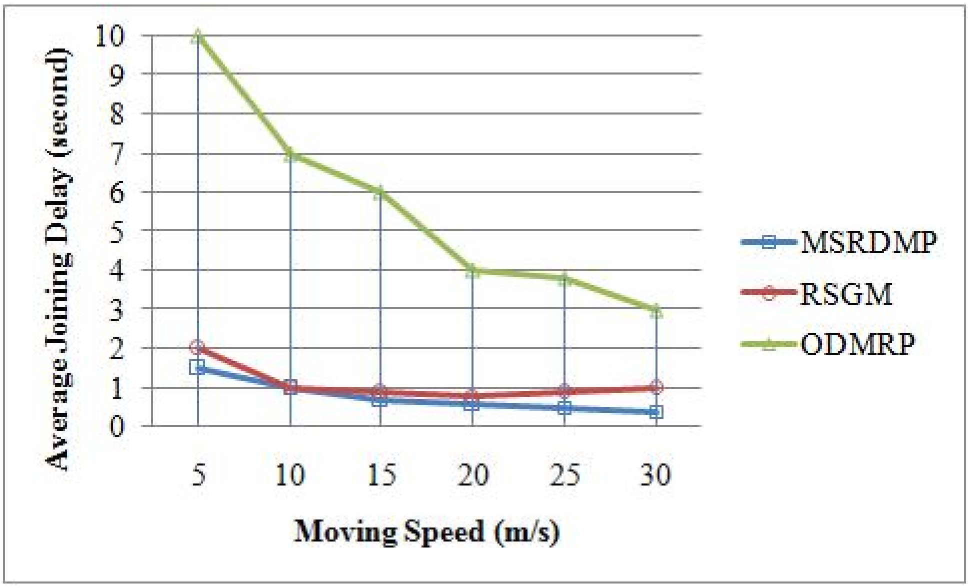

Figure 4.8 Average joining delay versus moving speed

4.6.3 Impact of Node Density

The total number of nodes deployed in the area greatly creates a great impact on the performance of the any protocols for MANET. The node density refers to a number of nodes per unit area. Here the unit area is square kilometer. As the air medium is shared by all the mobile nodes deployed in it the collisions among the nodes are prevalent. In multicast communication a group leader has to manage all the nodes in its group. The delivery of packets leads to more failure, if the group members are sparsely scattered. If the destination node is far away, average path length will also increase. The Figure 4.9 shows the graph for packet deliver ratio versus node density.

It is clearly understood that if the node density is sparse, all the protocols yields a poor packet delivery ratio. When 50 percent of the density is increased from initial value the MSRDMP gives much better packet delivery ratio than the other protocol ODMRP. The RSGM gives an equal packet delivery ratio only if the node density is about 70 nodes per square kilometer.

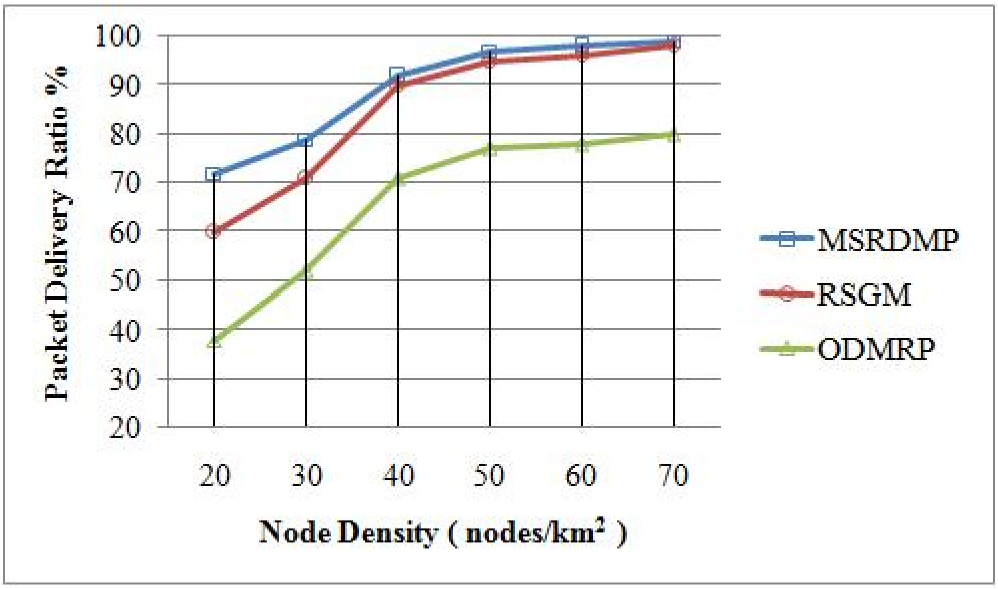

Figure 4.9 Packet delivery ratio versus node density

The graph shown in the Figure 4.9 depicts that the blue line for MSRDP starts going up once the density is 30 nodes per square kilometer and above. The green line for ODMRP goes straight despite of the increase in node density. The RSGM goes almost parallel with MSRDMP after 50 nodes

The Figure 4.10 shows the graph for control overhead versus node density for three multicasting protocols. The control overhead for location aware protocol RSGM incurs a little bit more than MSRDMP and ODMRP. Initially ODMRP claims less control overhead ,but later control overhead increases when node density increases because multiple nodes claims the membership at a time to the group leader. Managing more nodes at a time leads to higher control over head in ODMRP.

Only one group leader exits in RSGM for entire zone. It involves more control overhead when a number of nodes are lesser in the area because the control messages could not be reached on time to intended destination. In transmission range based multicast group there exits one group leader for each group, the membership coordinator between leadership track node and the group leader is quite cooperative so the control overhead is minimized.

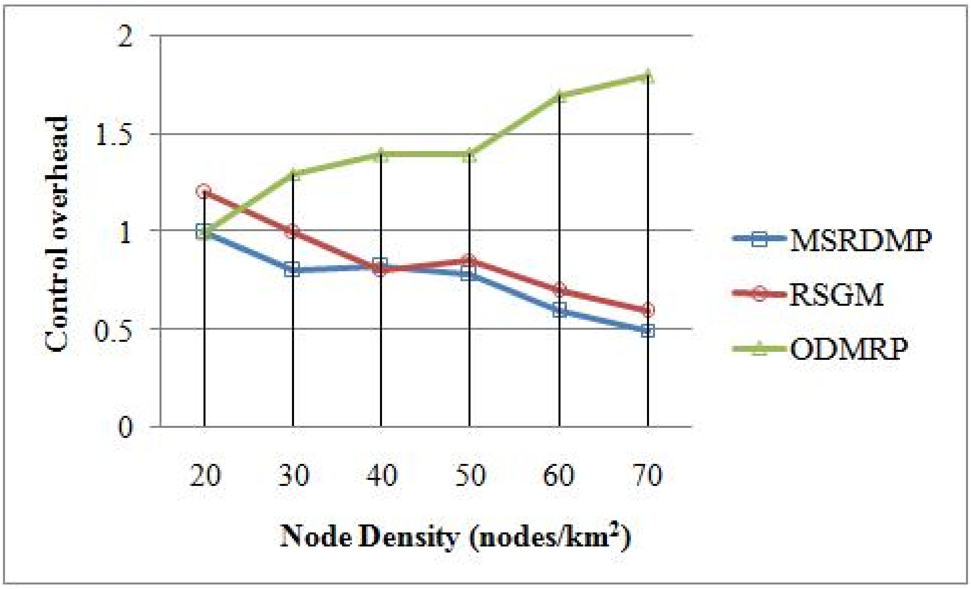

Figure 4.10 Control overhead versus node density

The graph shown in Figure 4.10 clearly portraits that the blue color for MSRDP move towards the horizontal axis, whereas the green color goes upwards along the vertical axis. The red color line for RSGM travels almost parallel with MSRDMP when node density increases.

The Figure 4.11 displays the graph for average path length versus node density. Average path length falls between 6 and 7 for RSGM and ODMRP when node density increases. As far as MSRDMP is concerned the average path length is very less when node density is somewhat high. As node density increases, the average path length falls between 3 and 5. If the group leader is away from its adjacent leadership track node, the packets have to take some more hops to reach its destination otherwise hops always fall within the optimum range. Both RSGM and ODMRP maintains the tree structure, structure often gets changed due to movements of node without a cooperation so packets have to travel some more intermediate nodes.

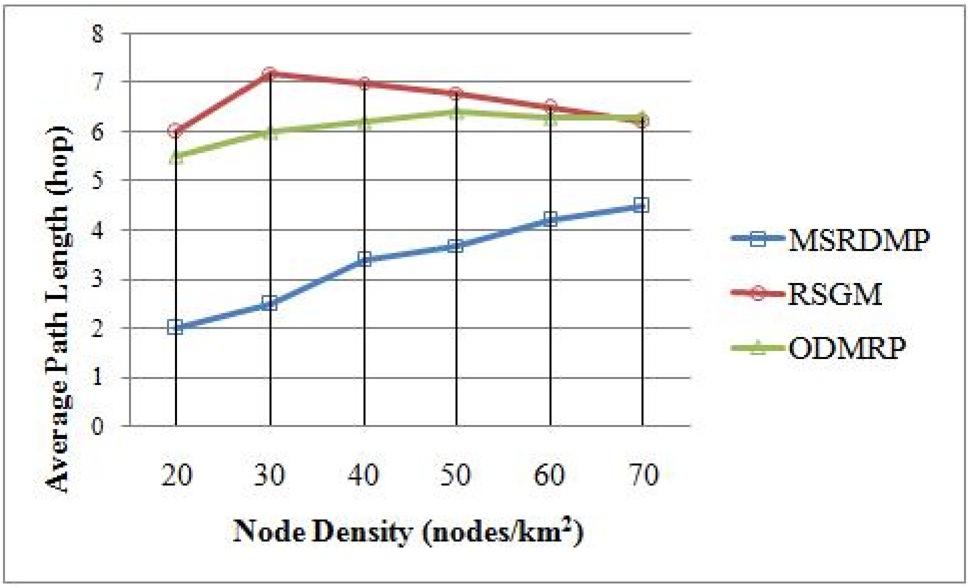

Figure 4.11 Average path length versus node density

The graph shown in the Figure 4.11 shows the flow line for each protocol. Three lines start at almost same point, but the blue color for MSRDMP deviates and path length travels between 3 and 5. The RSGM and ODMRP travels above 6. As long as a number of hops reduces, the performance of the protocol looks brighter.

The Figure 4.12 depicts the graph for average joining delay versus node density for three multicasting routing protocols for MANET. Joining delay for MSRDMP and RSGM is very low. When a new node wants to become a member of that group, it passes the joining request. The request is immediately responded. In RSGM, the group leader periodically floods the address of the group leader so that new node directly contacts the group leader. However, joining request passes some intermediate hops in RSGM. In MSRDMP a new node is assisted by the leadership track node as soon as the node comes across the new membership group. Almost RSGM and MSRDMP give the same response time. In case of ODMRP when the node density is low, the joining request packet has to travel long distances through more intermediate packets when group leader is far away. So ODMRP takes more initialization time.

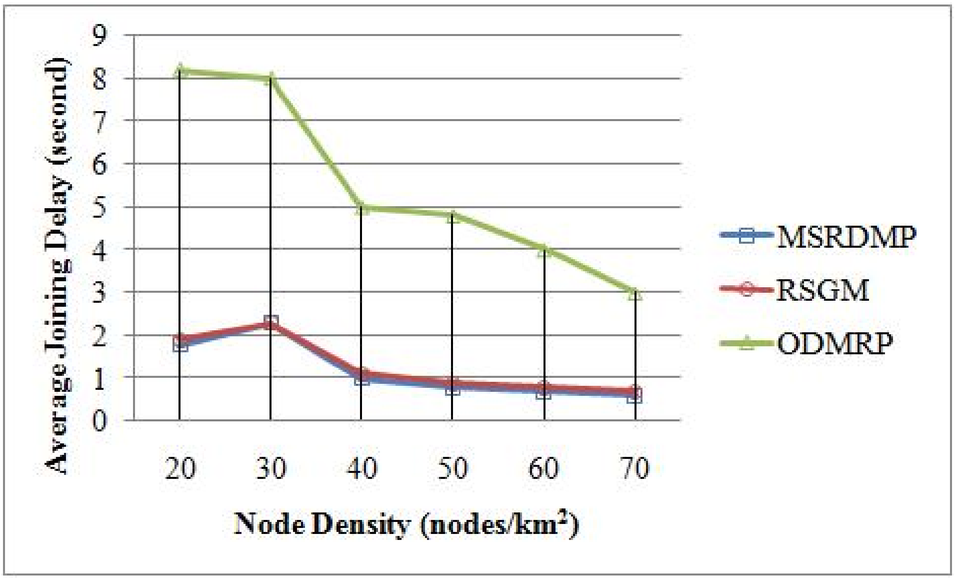

Figure 4.12 Average joining delay versus node density

The graph shown in the Figure 4.12 tells that the green color line for ODMRP initially starts at the peak and gradually goes down when node density increases. For MSRDMP and RSGM the blue and red color line almost overlaps each other when node density increases.

4.7 NUMERICAL INVESTIGATION AND DISCUSSION ON MOBILITY

The proposed multicast routing protocol MSRDMP is compared with the other standard protocols the RSGM and the ODMRP. The performance parameters packet delivery ratio, control overhead, average path length and average joining delay are analyzed under the varying moving speed of the node. The average performance of those protocols is shown in the Table 4.2 for six sets of values. It is observed that the MSRDMP offers better average performance than the other protocols. The average packet delivery ratio is 97.16 % for the MSRDMP. It is 2 % more than the RSGM and 18% more than the ODMRP.

The MSRDMP suffers less control overhead. The average control overhead for the MSRDMP is 0.89. It is 0.32 less than the RSGM and 0.67 less than the ODMRP. The number of hops traversed by a packet in the MSRDMP is optimized. The average performance of path length is 3.46 hops for the MSRDMP, 6.25 hops for the RSGM and 6.23 for the ODMRP. The average performance of joining delay for the MSRDMP is 0.7 second and 1.1 seconds for the RSGM. The ODMRP suffers more joining delay than the rest of two protocols the RSGM and the MSRDMP. The average performance shows that joining delay for the MSRDMP is 0.4 second less than the RSGM and 4.53 seconds less than the ODMRP.

4.8 NUMERICAL INVESTIGATION AND DISCUSSION ON NODE DENSITY

The number of nodes per square area greatly influences the performance of routing protocols. If there are more nodes, the bandwidth is consumed by all of them. Subsequently the packet loss would be more. The proposed multicast routing protocol MSRDMP is compared with the RSGM and the ODMRP. The Table 4.3 shows the result of packet delivery ratio, control overhead, average path length and average joining delay on six sets of node density value. The average performance shows that the packet delivery ratio for the MSRDMP is 89.5 %, which is 4.5% more than the RSGM and 23.5% more than the ODMRP. The control overhead is 0.75 for the MSRDMP, 0.86 for the RSGM and 1.4 for the ODMRP. The average performance of the path length is very low for the MSRDMP. The MSRDMP yields 3.38 hops, which is almost 50% of the RSGM and the ODMRP. The average performance for joining delay shows that the MSRDMP offers better performance than the RSGM and the ODMRP. It is observed that average joining delay 1.2 seconds for the MSRDMP and 1.28 seconds for the RSGM and 5.5 seconds for the ODMRP.

Table 4.2 Numerical investigation and discussion on mobility

Moving speed m/s	Packet delivery ratio %			Control overhead			Average path length (hop)			Average joining delay (second)		
	MSRDMP	RSGM	ODMRP	MSRDMP	RSGM	ODMRP	MSRDMP	RSGM	ODMRP	MSRDMP	RSGM	ODMRP
5	99	97	85	0.8	0.9	1.2	2.7	5.7	6.1	1.5	2	10
10	98	96	84	0.8	0.92	1.3	3	5.9	6	1	1	7
15	97	96	80	0.9	0.94	1.3	3.2	6.2	6.2	0.7	0.9	6
20	97	95	77	0.89	1.3	1.5	3.7	6.4	6.3	0.6	0.8	4
25	96	94	75	1	1.5	2	4	6.6	6.3	0.5	0.9	3.8
30	96	93	74	1	1.7	2.1	4.2	6.7	6.5	0.4	1	3
Average Performance	**97.16**	**95.16**	**79.16**	**0.89**	**1.21**	**1.56**	**3.46**	**6.25**	**6.23**	**0.7**	**1.1**	**5.63**

Table 4.3 Numerical investigation and discussion on node density

Node density nodes/km^2	Packet delivery ratio %			Control overhead			Average path length (hop)			Average joining delay (second)		
	MSRDMP	RSGM	ODMRP	MSRDMP	RSGM	ODMRP	MSRDMP	RSGM	ODMRP	MSRDMP	RSGM	ODMRP
20	72	60	38	1	1.2	1	2	6	5.5	1.8	1.9	8.2
30	79	71	52	0.8	1	1.3	2.5	7.2	6	2.3	2.3	8
40	92	90	71	0.82	0.8	1.4	3.4	7	6.2	1	1.1	5
50	97	95	77	0.78	0.86	1.4	3.7	6.8	6.4	0.8	0.9	4.8
60	98	96	78	0.6	0.7	1.7	4.2	6.5	6.3	0.7	0.8	4
70	99	98	80	0.5	0.6	1.8	4.5	6.2	6.3	0.6	0.7	3
Average Performance	**89.5**	**85**	**66**	**0.75**	**0.86**	**1.4**	**3.38**	**6.61**	**6.11**	**1.2**	**1.28**	**5.5**

4.9 SUMMARY

The beginning of the chapter deals with hurdles to transmitting the packet, and a specific overload occurs to the group leader of the multicast communication. A model assumption for proposed multicast routing protocol is briefed. How the selection of group leader is narrated by the persistence leader selection algorithm. The way alert message is created and how the group leader is assisted by the leadership track node is explained. The primary collision avoidance mechanism is discussed and how the introduction of the interim CTS request is used to recover the lost packet. Finally the performance of proposed multicast routing protocol MSRDMP is compared with existing multicast routing protocol RSGM and ODMRP and also numerical investigation and discussion on mobility and node density is given The result shows that the MSRDMP offers better performance than the other two protocols.