Adaptive On-Demand Multicast Routing Protocol for Mobile Ad Hoc Networks

R. Rajeshkanna[1] Dr. A. Saradha[2]
[1]Research Scholar [2]Head of Dept.
[1]Department of Computer Applications [2]Department of Computer Science and Engineering
[1]Bharathiar University, Coimbatore [2]Institute of Road and Transport Technology, Erode, Tamilnadu, India

Abstract— Mobile ad hoc network (MANET) is a collection of autonomous mobile nodes forming an ad hoc network without fixed infrastructure. Dynamic topology property of MANET may degrade the performance of the network. However, multipath selection is a great challenging task to improve the network lifetime. However, E-ODMRP implements an adaptive control mechanism with a cross-layer algorithm for the physical layer. When a node transmits multicast data, E-ODMRP can adjust the transmission rate and power level of the physical layer to minimize packet drop or retransmission due to interference between nodes belonging to the forwarding group. The proposed algorithm performs cluster formation for the base station using the range of direction and threshold of velocity. We calculate the exchange of the cluster head node probability using the direction and velocity for maintaining cluster formation. Simulation results confirmed that E-ODMRP provides an improved throughput of up to 46% compared to ODMRP.

Key words: ODMRP, Routing, Multicasting, Delivery Ratio, MANET

I. Introduction

Mobile ad hoc network (MANET) consists of nodes that have mobility. The nodes both send and receive messages and can communicate with each other. Thus, the network builds its own network structure that is not dependent on infrastructure. Due to the characteristics of mobile ad hoc networks, MANET has been used in the environments of poor communication, such as those where infrastructure cannot be built, as in disaster areas or war zones [4, 5]. Cluster networks using properties of the node have been studied particularly extensively. A cluster network is divided into mobile groups by setting the rules of communication protocols. The mobile groups elect the cluster head node for managing groups. The cluster head node aggregates sensing data sent by a cluster member node and then sends the aggregated data to the base station [6]. However, if the cluster head node is discharged or does not move due to poor environmental conditions, the routing path is disconnected from the cluster head node. Therefore, the network cannot communicate in a stable fashion. In that case, the cluster network reelects the cluster head node to recover the routing path. However, dynamic properties of a node cause frequent disconnections and routing recovery. In addition, the nodes have constraints, such as limited transmission bandwidth and energy, as well as topology changes. To reduce the number of disconnections and in order to set the routing path, the network sends a control packet. Eventually, the load is increased.

Multipath routing in a MANET [8] is established in order to increase the reliability of data transmission that provides load balancing among the nodes. The use of multiple disjoint paths transferred the data in parallel that significantly increases the packet delivery ratio. Multipath routing schemes [9] deal with the problem of scalability, confidentiality, integrity, and network lifetime. Multiple-path routing [10] between source and destination ensures reliability of the data transmission in a MANET. Existing multipath routing schemes in a MANET lead to problems such as flooding, empty set of neighbors, flat addressing, widely distributed information, large energy consumption, interference, and load balancing issues. Therefore, the efficient multipath routing scheme is proposed to solve one or more of these issues. And also the existing multipath routing schemes do not perform well in dynamic environment change and frequent path failure. They also generate a routing overhead in the network. The routing overhead occupies a considerable portion of network bandwidth and the energy of the mobile node exhausts rapidly. Hence, with minimum overhead, the reliable multipath routing protocol is essential for designing to restrict the participation of mobile nodes in a route discovery phase that ensure reliability of data transmission. Evolutionary mechanism paradigm [11, 12] is most suitable to resolve multi object problems because they are based on population. It generates a set of solutions in one run.

II. MANET Multicasting Challenges and Issues

Issues and challenges presented by MANET multicasting include the following [2–10].

A. *Resource Management*

Mobile nodes in MANETs are limited in resources such as power and memory, so a multicast protocol minimizes the consumption of these resources and utilizes them in such a manner as to ensure competent handling of information with efficient resource consumption, such as by minimizing the use of state information packets.

B. *Link Failure*

Because of the random mobility of the nodes and the wireless nature of links, link stability is hard to preserve in mobile ad hoc networks.

C. *Control Overhead*

In multicast transmission, we need to keep track of the members involved in the multicast transmission; thus, we need control packets to be exchanged between them. Since only limited bandwidth is provided in MANETs, this may result in significant overhead requirements, so the design of MANET should take into consideration the need to keep the control packet size to a minimum.

D. Efficiency

In MANETs, errors and failure are more likely to happen than in ordinary networks due to their mobility and limited bandwidth. Therefore, in the multicast protocol design, efficiency is very important. Efficiency as used here is the ratio of received data to the total number of transmitted packets in the network.

E. Reliability

Reliability is the key issue in multicast transmissions in MANETs, and this can be difficult to deliver due to the differentiation in the members involved and the fact that any member can disconnect from the network at any time, in consideration of its environmental conditions.

F. Wireless Nature

The wireless nature of a MANET makes it vulnerable to the numerous types of attacks that are common to wireless links such as snooping, interference, and eavesdropping, which may also affect the network resources. Attackers can use these methods to prevent the normal communication scenario among nodes or to capture valuable information.

G. No Defined Physical Boundary

Due to mobility, we cannot define exactly the boundaries of our network, and the nodes can join or leave the network because of radio coverage. The scalability of MANETs is changing, so the security mechanism must be able to handle large networks as well as smaller networks, which makes for a difficult task.

H. Absence of Centralized Management

Detection of possible attacks is difficult due to the absence of centralized management such as an access point or base station that can monitor the traffic in a MANET, especially if the network is deployed over a large scale, which may delay the trust between involved nodes.

I. Infrastructure

Mobile ad hoc networks are infrastructure less, and there is no central administration that can regulate the communication between involved nodes. This means that every node can communicate with other nodes, which makes it difficult to detect faults happening in the network, and because of the highly dynamic topology of MANET, frequent network separation and route changing can result in the loss of packets.

J. Limitation in Power

The nodes in mobile ad hoc networks are battery powered; this restriction may cause problems such as the loss of packets, or the nodes may work in a selfish manner, meaning that they do not forward messages received.

K. Trust

The lack of central administration and the highly dynamic topology of MANETs may result in a lack of trust between involved nodes due to the absence of verification and the fact that some nodes may participate in a transmission even if they are not part of the network, which may result in security breaches in the network or leaks of valued information.

L. Security

Attacks may happen in MANETs due to their wireless nature and the lack of centralized admission of mobile ad hoc networks, which make these networks vulnerable to attacks such as eavesdropping and wormhole or black hole attacks. As such, it is essential for the multicast protocol to ensure security.

M. Quality of Service

The applications that currently rely on MANETs vary greatly, and these include military applications. Quality of service is an important issue in such applications, but ensuring quality of service by multicast can be difficult for reasons including throughput, delay, and reliability. The design of a multicast protocol should take into consideration the need to provide these parameters.

III. RELATED WORKS

Several multicast routing protocols for ad hoc networks have been proposed in the literature [4].

The Ad Hoc Multicast Routing Protocol (AMRoute) [5] is a tree-based multicast routing protocol for mobile ad hoc networks [6]. Using AMRoute, bidirectional unicast tunnels are continuously created between pairs of group members located nearby. Unlike multicast group members, some nodes constituting the unicast tunnel do not support AMRoute. When a packet is directed to a logically adjacent member, it will be sent through a unicast tunnel, and may pass through many routers. The group members forward and replicate multicast traffic along the branches of a virtual tree. Each group has at least one logical core responsible for member management and tree maintenance. The robustness derives from the virtual mesh links used to establish the multicast tree in AMRoute. A core failure does not prevent data flow. AMRoute is efficient because it constructs a shared tree for each group. However, AMRoute relies on the existence of an underlying unicast routing protocol. This protocol can only be used in networks where the set of nodes supports the AMRoute routing function. The major disadvantage of the protocol is that it suffers from temporary loops and creates suboptimal trees in the presence of mobility.

Geographic multicast protocols [7, 8] support a two-tier membership management and forwarding structure. The first tier is based on position information, where a zone structure is built. When a zone has members, a leader is elected on-demand. The leader manages group membership and collects the positions of the members in its zone. In the second tier, the leader has a direct relationship with the source. If the source wishes to send a message, it sends it to the leader. It is then the responsibility of the leader to transfer the message to its members in the group. In this two-tier approach, because message transmission is executed in two phases, there exists the possibility of additional transmissions. Electing a leader on-demand, zone management, and managing empty zones are issues afflicting this approach. Nodes must inform the zone leader of the multicast sessions in which they are involved, resulting in further overhead.

A cluster-based quality of service (QoS) multicast routing protocol has been proposed in [9]. This protocol partitions the network into square clusters, and the node nearest to the center of the cluster is elected the cluster head. A gateway node is selected between adjacent clusters to relay packets when adjacent clusters are beyond the effective transmission range. The gateway forwards a probe packet to the appropriate neighbor cluster until the destination, or an intermediate node with a valid route to the destination, is reached. The destination or the intermediate node selects the optimal route using the best predecessor replacement strategy [10], where the node chooses the next-best predecessor satisfying QoS constraints (delay, cost). In this protocol, only the gateway is responsible for packet forwarding. Thus, the selection of the gateway becomes the key point of this protocol. A drawback of this protocol appears when the network is sparse. In this case, gateway nodes may fail to reach a neighbor cluster head, and the route may not be established.

The core-assisted mesh protocol (CAMP) [11] is a mesh-based multicast routing protocol for mobile ad hoc networks [12]. CAMP is a proactive multicast routing protocol based on shared meshes. The mesh structure provides at least one path from each source to each receiver in the multicast group. CAMP relies on an underlying unicast protocol. Every node maintains a routing table (RT) created by the underlying unicast routing protocol. A multicast routing table (MRT) is based on the RT that contains a set of known groups. CAMP modifies this table when a multicast group joins or leaves the network. Unlike Core-Based Tree (CBT) [13], where all traffic flows through core nodes, the core nodes in CAMP are used to limit the control traffic when receivers are joining multicast groups.

ODMRP is a representative mesh-based multicast protocol that provides richer connectivity among multicast members. By building a mesh and supplying multiple routes, multicast packets can be delivered to destinations in the presence of node movements and topology changes. Moreover, the drawbacks of multicast trees in mobile wireless networks, such as intermittent connectivity, traffic concentration, frequent tree reconfiguration, and nonshortest path in a shared tree, are avoided. To establish a mesh for each multicast group, ODMRP uses the concept of the forwarding group [14]. ODMRP also applies on-demand [15, 16] routing techniques to avoid channel overhead and improve scalability. ODMRP uses a soft-state approach to maintain multicast group members, can reduce overhead due to group maintenance, channel, and storage, and has superior connectivity in mobile wireless networks. Two other proposals related to ODMRP. These are R-ODMRP [2] and MR2-ODMRP [3]. R-ODMRP was proposed to quickly recover a disconnected path, whereas MR2-ODMRP was proposed to improve performance using multiple wireless interfaces.

Excluding ODMRP, these options require an underlying unicast routing scheme. They incur heavy protocol overhead and must be aware of their own position information. They do provide effective performance in static environments, however. Conversely, ODMRP has a simple design and can reduce maintenance overhead as it does not require an underlying unicast routing scheme. It appears to be well-suited to dynamic situations. However, ODMRP does not have a control mechanism for the physical layer. The nodes within ODMRP transmit multicast data at a fixed transmission rate and power level for the physical layer. As the number of nodes belonging to the forwarding group increases, there is significant packet drop or retransmission due to interference between the nodes that send the multicast data. Therefore, in this paper, we propose an improved version of ODMRP.

IV. E-ODMRP

In this paper, we propose E-ODMRP, which resolves the problems in ODMRP described in the previous subsection. E-ODMRP improves both data transfer and path forming processes of ODMRP.

Figure 3 shows the difference in the Join Query process between E-ODMRP and ODMRP. As indicated in Figure 3, when the node in ODMRP receives a Join Query, the node verifies that the packet has been duplicated, updates the routing metric (hop-count), verifies whether to update its routing table or stay, calculates the routing metric of the packet, and rebroadcasts the packet.

E-ODMRP uses the new routing metric proposed in this paper, which includes a new feature to address a duplicated Join Query. When a node with E-ODMRP receives a duplicated Join Query, the node compares the old metrics with the new metrics. If the metric of the new Join Query is less than the old metric, the node can rebroadcast it even though it is a duplicate Join Query. Unlike ODMRP, which cannot rebroadcast a duplicated Join Query, E-ODMRP can establish the path that has the best metric and prevent overhead due to Join Query flooding. Additional information regarding the new routing metric proposed in this paper is provided at the end of this section.

Algorithm 1 allows a node to process a received Join Query. The node using E-ODMRP compares old Join Queries with the new metrics, calculates a new metric, updates Up_Node_ID_Table as well as the metric field of the Join Query, and rebroadcasts the Join Query. The sum of the transmission power level (*P*) and the minimum transmission rate (*R*) of the physical layer of the path are stored in a metric field of the Join Query.

A. *Algorithm 1*

if duplication(Join Query) then
    R_{old} , P_{old} from Message Cache
    R_{new} , P_{new} from Join Query
    M_{old} = cal_metric(R_{old} , P_{old})
    M_{new} = cal_metric(R_{new} , P_{new})
    if $M_{old} \le M_{new}$ then
    drop Join Query
    end if
end if
R_{this} = get_tx_rate(Neighbor_Table, SenderID)
P_{this} = get_tx_power(Neighbor_Table, SenderID)
$P_{new} = P_{new} + P_{this}$
$R_{new} = \min(R_{new}, R_{this})$
if empty(Up_Node_ID_Table) then
    update(Up_Node_ID_Table)
else
    R_{old} , P_{old} from Up_Node_ID_Table
    M_{old} = cal_metric(R_{old} , P_{old})
    M_{new} = cal_metric(R_{new} , P_{new})
    if $M_{old} > M_{new}$ then

21) update(Up_Node_ID_Table)
22) end if
23) end if
24) update_Join_Query(R_{new} , P_{new})

To calculate a suitable transmission power level and transmission rate for the physical layer, E-ODMRP uses a measurement of the signal-to-noise ratio (SNR) between nodes. When a node receives a beacon from a neighboring node, each node measures the SNR between a neighboring node and the sender of the beacon and stores the SNR and the sender ID of the beacon in Neighbor_Table. E-ODMRP uses the information of the Neighbor_Table to form the metric of path. The detailed explanation is at the end of this section.

Figure 4 shows the differences in the Join Table handling process between E-ODMRP and ODMRP. As shown in Figure 4, when a node using ODMRP receives a Join Table, it determines whether it is the destination node of the packet. If it is, it sets FG_Flag and broadcasts its own Join Table.

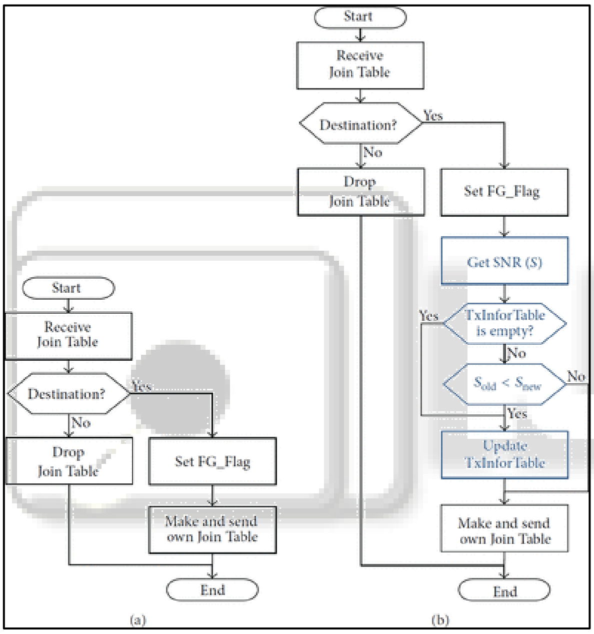

Fig. 1: Flowchart for handling Join Table (a) of ODMRP and (b) of E-ODMRP.

When a node using A-ODMRP creates its own Join Table, information regarding the Up_Node received from Neighbor_Table is included in the Join Table. Without the transmission of additional packets, a node can acquire information regarding itself. Its neighbor node uses beacons sent by the node itself to estimate this information. Moreover, unlike ODMRP, a node with A-ODMRP can adjust the transmission rate and power level of the physical layer depending on the SNR between itself and the sender. It updates its Tx_Infor_Table. A node with A-ODMRP has an information table that includes the suitable transmission power level and rate of the physical layer based on the SNR between the nodes. We use a heuristic to create this information table. Additional information regarding this information table is provided at the end of this section.

Algorithm 2 allows a node to process a received Join Table. The node using A-ODMRP checks the destination of the Join Table, sets the FG_Flag of the node, and updates Tx_Infor_Table. It then creates and broadcasts its own Join Table.

B. *Algorithm 2*

1) if dest_is_me(Join Table) then
2) set(FG_Flag)
3) D_{new}= get_SNR(Neighbor_Table, SenderID)
4) R_{new}= get_tx_rate(Neighbor_Table, SenderID)
5) P_{new}= get_tx_power(Neighbor_Table, SenderID)
6) if empty(Tx_Infor_Table) then update_Tx_Infor_Table
7) D_{new} , R_{new} , P_{new})
8) Else
9) D_{old}= get_SNR(Tx_Infor_Table)
10) if $D_{old} < D_{new}$ then update_Tx_Infor_Table
11) D_{new} , R_{new} , P_{new})
12) end if
13) end if

E-ODMRP improves the data transfer process of ODMRP. When a node with E-ODMRP transmits multicast data, each node uses the transmission rate and power level of the physical layer stored in Tx_Infor_Table. The main features of the E-ODMRP are as follows:

– When a node transmits multicast data, the node using E-ODMRP uses a suitable transmission power level and rate for the physical layer based on the SNR between the nodes.
– It reduces energy consumption during transmission.
– It minimizes interference between nodes belonging to the forwarding group.
– A node with E-ODMRP efficiently uses valuable resources, such as channel bandwidth, and improves performance through multicast data transfer.

In this paper, we use a heuristic procedure to calculate a suitable transmission power level and rate for the physical layer based on the SNR of the nodes. In our simulation, we used sender and receiver nodes that communicated with each other using multicast. The sender transmitted the beacon periodically and the receiver estimated the SNR of the beacon. In this situation, we changed the distance between sender and receiver and recorded the SNR of the beacon for the different distances. Based on this recorded data, we obtained a suitable transmission power level and rate for the sender for each SNR value to communicate with the receiver at the maximum bandwidth. The details are as follows.

The sender sets the transmission power level for its physical layer to maximum. In this situation, we can obtain the maximum transmission rate of the physical layer of the sender for each distance. For each distance, we set the transmission rate to appropriate for each SNR. Following this, while reducing the transmission power level, we estimate the transmission power level for the sender to successfully communicate with the receiver at the maximum transmission rate for each SNR.

V. SIMULATION

In this section, we study the performance of E-ODMRP and compare it to ODMRP. We implemented the details of E-ODMRP and conducted a set of simulations.

A. *Performance Metrics*

– The proposed scheme uses five performance metrics to evaluate the proposed scheme and related schemes.

– Packet Delivery Ratio. It is the ratio of the number of data packets received successfully by the destination node.
– Routing Overhead. The number of control packets was generated during data transmission in routing.
– Energy Consumption. It is the average energy consumed for the data transmission in routing.
– Multicast Efficiency: Defined as the number of data packets delivered to multicast receivers over the number of total data packets forwarded. Higher value implies better performance.

Multicast Efficiency=total received packets / total forwarded packets

B. *Effect of Number of Senders*

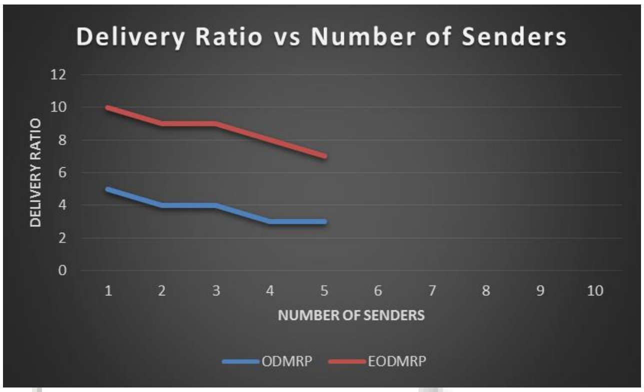

Fig. 2: Delivery Ratio vs Number of Senders

A comparison was made with ODMRP and EODMRP. EODMRP uses a mesh structure to provide an efficient delivery ratio. ODMRP uses the traditional shared-based structure to construct a delivery tree and it needs a rendezvous point. Various performance metrics were considered for 10 to 100 senders among a network of 100 nodes. The number of receivers was set to 10. The simulation results are shown in Figure 2. Because each sender of EODMRP floods control messages into the entire network periodically, the packet collision probability becomes higher when the number of senders increases. The senders in the ODMRP protocol must forward data packets to a rendezvous point; the rendezvous point is very busy when many senders are sending data. This situation may also increase the packet collision probability. As a starting set of simulations we have varied the number of senders to evaluate the protocol scalability based on the number of multicast source nodes and the traffic load. We inferred from the fig-1 that EODMRP is over 27% more effective than ODMRP in data delivery ratio as the number of senders incremented from 1-10.

C. *Effect of Multicast Group Size*

EODMRP performance is not affected to that extent by the increase in the number of multicast members. AMRIS also shows improvement with the member size growth but they are less dramatic because redundant routes are not established in ODMRP. This is shown in fig. 3 where we see the comparison between EODMRP and ODMRP. With respect to the increase in the group member size ODMRP is doing well than EODMRP, which can be attributed because of the collision that occur due to the frequent broadcast through the network.

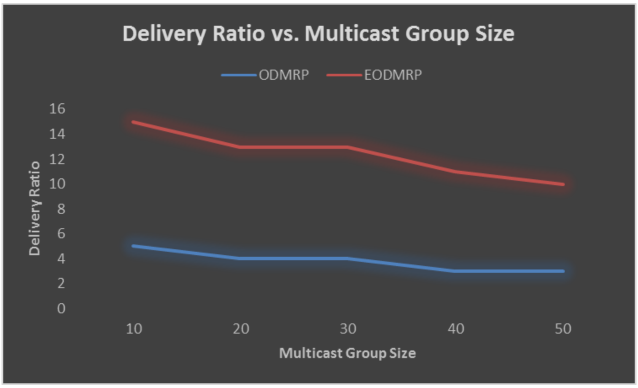

Fig. 3: Multicast Group Size vs Delivery Ratio

VI. Conclusion

We have presented EODMRP for mobile ad-hoc network and shown its features in comparing to ODMRP. EODMRP inherits most key properties of ODMRP, performs better with high scalability and deals well with unidirectional link problem. Simulation results show that EODMRP is effective and efficient in dynamic environments and scales well to a large number of multicast members.

References

[1] Lee S.-J., Su W., Gerla M.On-demand multicast routing protocol in multihop wireless mobile networks Mobile Networks and Applications 200276441453 doi:10.1023/a : 10207566001872- s2.0-0036924499
[2] Kharraz M.-A., Sarbazi-Azad H., Zomaya A. Y.On-demand multicast routing protocol with efficient route discovery Journal of Network and Computer applications 2012353942950doi:10.1016/j.jnca.2011.03.0122-s2.0-84855461958
[3] Oh K. J., Lee C. Y. MR2_ODMRP: improvement of end-to-end transmission delay in wireless multicast routing Wireless Personal Communications 2014742245257 doi:10.1007/s11277-013-1283-92-s2.0-84895071036
[4] Al-Hemyari A., Jumari K., Ismail M., Saeed S.A comparative survey of multicast routing protocol in MANETs Proceedings of the International Conference on Computer & Information Science (ICCIS '12) June 2012 Kuala Lumpur, Malaysia IEEE830835 doi:10.1109/ICCISci.2012.6297141
[5] Xie J., Talpade R. R., McAuley A., Liu M.AMRoute: Ad Hoc multicast routing protocol Mobile Networks and Applications200276429439doi:10.1023/A:10207484311382-s2.0-0036920382
[6] Wu C. W., Tay Y. C.AMRIS: a multicast protocol for ad hoc wireless networks Proceedings of the IEEE Military Communications Conference Proceedings (MILCOM '99)October-November 1999Atlantic City, NJ, USAIEEE2529 doi:10.1109/ MILCOM 1999.822636
[7] Xiang X., Wang X., Yang Y.Stateless multicasting in mobile ad-hoc networks IEEE Transactions on Computers 201059810761090doi:10.1109/TC.2010.102
[8] Xiang X., Zhou Z., Wang X. Robust and scalable geographic multicast protocol for mobile ad hoc networks Proceedings of the 26th IEEE International

Conference on Computer Communications (IEEE INFOCOM '07)May 2007Anchorage, Alaska, USA23012305 doi:10.1109/infcom.2007.2692-s2.0-34548295761
[9] Shih T.-F., Shih C.-C., Chen C.-L.Location-based multicast routing protocol for mobile ad hoc networksWSEAS Transactions on Computers200878127012792-s2.0-59249109490
[10] Shih C.-C., Shih T.-F.Cluster-based multicast routing protocol for MANETWSEAS Transactions on Computers2007635665722-s2.0-33847789718
[11] R.Rajeshkanna and Dr.A.Saradha Adaptive Multicast Multimedia Transmission Routing Protocol System (ACMMR) for Congestion Control and Load Balancing Techniques in Mobile Adhoc Networks , Global Journal of Computer Science and Technology: E Network, Web & Security, Volume 14 Issue 8 Version 1.0 Year 2014
[12] Garcia-Luna-Aceves J. J., Madruga E. L.The core-assisted mesh protocol IEEE Journal on Selected Areas in Communications199917813801394doi:10.1109/49.7799212-
[13] Das S. K., Manoj B. S. B. S., Murthy C. S. R.A dynamic core based multicast routing protocol for ad hoc wireless networks Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc '02)June 2002Lausanne, Switzerland ACM2435 doi:10.1145/513800.513804
[14] Ballardie T., Francis P., Crowcroft J.Core based trees (CBT)Proceedings of the ACM Conference on Communications Architectures, Protocols and Applications (SIGCOMM '93)September 1993San Francisco, Calif, USA
[15] Chiang C.-C., Gerla M., Zhang L.Forwarding Group Multicast Protocol (FGMP) for multihop, mobile wireless networks Cluster Computing 199812187196 doi:10.1023/A:1019037500012
[16] Corson M. S., Ephremides A.A distributed routing algorithm for mobile wire-less networks Wireless Networks1995116181doi:10.1007/bf011962592-s2.0-0002159357
[17] Maltz D. A., Broch J., Jetcheva J., Johnson D. B.The effects of on-demand behavior in routing protocols for multihop wireless ad hoc networks IEEE Journal on Selected Areas in Communications199917814391453doi:10.1109/49.7799252-s2.0-0032667063
[18] R.Rajeshkanna and Dr.A.Saradha Adaptive Multicast Multimedia Transmission Routing Protocol System (ACMMR) For Congestion Control And Load Balancing Techniques In obile Adhoc Networks , pp. 21531-21540,IJAER Volume 9, Number 23 (2014)
[19] R. Rajeshkanna, Dr. A. Saradha, “Energy Efficient Enhanced AODV Routing Protocol for Maximize the Lifetime of Mobile Ad hoc Networks”, ISSN:2229-6093, Int.J.Computer Technology & Applications,Vol 4 (5),856-863, Sept-Oct 2013.