# TECHNICAL RESEARCH REPORT

## Multicast Routing in Mobile Ad Hoc Networks Using Source Grouped Flooding

*by Karthikeyan Chandrashekar, John S. Baras*

**CSHCN TR 2003-6**
**(ISR TR 2003-12)**

# Multicast Routing in Mobile Ad hoc Networks Using Source Grouped Flooding

Karthikeyan Chandrashekar and John S. Baras
Institute for Systems Research
University of Maryland
College Park, Maryland 20742
Email: karthikc@isr.umd.edu , baras@isr.umd.edu

*Abstract: In this paper, we address the multicast routing problem for mobile ad hoc networks (MANETs). We present the Source Grouped Flooding approach to achieve multicast in MANETs. The protocol creates multiple multicast routes between the source and group members based on hop count distance constraints. We also propose a probabilistic data forwarding mechanism to achieve efficient data dissemination. The protocol aims to achieve the robustness of flooding and data distribution efficiency of tree based protocols. Simulation results verify performance.*

## I. INTRODUCTION

Mobile ad hoc networks are flat networks comprised of mobile wireless devices. The ease and speed of deployment of these networks makes them ideal for situations where fixed infrastructure is not readily available (e.g. battlefield communications, disaster recovery). Limited bandwidth, energy constraints and unpredictable dynamic topologies pose difficult problems for the design of applications for these networks. Multicast applications like video conferencing and subscription services have become very popular with the advancements in current technology. Multicast is an important communication paradigm in ad hoc networks due to the inherent broadcast nature of the medium. Multicast routing protocols for ad hoc networks are either tree based or mesh based. Tree based protocols like [1], [2], [3] achieve efficient data distribution, however suffer when the network is highly dynamic. Mesh protocols like [4], [5], [6] are robust against network dynamics due to redundant transmission of data, however at the cost of increased overhead. Flooding achieves network wide broadcast and hence it can be considered as a multicast routing protocol that is highly robust against topology changes.

The Source Grouped Flooding protocol is designed to provide robustness similar to that of flooding i.e. to create a stable multicast structure at high node speeds. At the same time the protocol improves the efficiency of data delivery. For further details of the protocol and its performance we refer to [7].

## II. RELATED WORK

Adhoc Multicast Routing using Increased Sequence ids (AMRIS) [3] creates a shared multicast tree structure rooted at a special node (Sid). Nodes adapt to connectivity changes based on id numbers obtained from the Sid. A multicast extension to Adhoc On-demand Distance Vector (AODV) [1] creates a shared multicast tree rooted at the group leader which periodically updates routes through destination sequence numbers. The Adhoc Multicast Routing Protocol (AMRoute)[2] creates a user level shared multicast tree consisting of unicast tunnels between the group members. The On-demand Multicast Routing Protocol (ODMRP)[4] creates a mesh of nodes connecting the sources and the group members. Multiple paths provides stability against topology changes. The Core Assisted Mesh Protocol (CAMP) [5] relies on affiliations to core nodes to create multicast structure. The core nodes forward the data. Flooding as a multicast protocol is discussed in [8]. The broadcast storm problem and methods to reduce the overhead of flooding are discussed in [9].

## III. SOURCE GROUPED FLOODING PROTOCOL

This is an on-demand protocol that creates and maintains a mesh of nodes called the *flooding group* based on hop count distance metrics. Nodes in the network learn these metrics during a request-reply phase.

### A. Creation of the flooding group

*1) Request Phase:* When a source has packets to send to a multicast group it initiates the request phase by broadcasting a JOIN REQUEST message. The request message contains the *multicast group address* and a *hop count* field. When a node in the network receives a non-duplicate request packet, it stores the *hop count* for that source (D$_{sn}$) i.e., the hop count of the node from the source. The node then increments the hop count and re-broadcasts the packet. This is illustrated in Figure 1(a). ‘S’ is the source and ’M1’ and ’M2’ are the multicast members. The number in each node indicates hop count to the source ’S’. A combination of the source address and a counter is used as a unique packet identifier to identify duplicate packets. An active source will periodically update the flooding group every *refresh_interval* seconds.

*2) Reply Phase:* A multicast group member upon receiving the JOIN REQUEST, stores the hop count distance to the source $D_{sm}$, waits for a short fixed interval and then broadcasts a JOIN REPLY message. The delay prevents collision of the request and the reply messages in the region of the group member. The JOIN REPLY contains the multicast group information and the hop count distance from the group member to the source. The TTL (Time To Live field in the IP header) for this message is set to the hop count from the source ($D_{sm}$). This ensures that the reply message does not propagate beyond the source. When a node receives a JOIN REPLY the node will compare its stored hop count to the source (stored during the request phase $D_{sn}$), and the value in the *hop count* field of the reply message ($D_{sm}$). If the hop count distance constraint (1) is satisfied the node becomes a flooding node else the packet is dropped. The nodes marked ’FN’ in Figure 1(b) are the flooding nodes for the source ’S’. The propagation of the reply message is limited by the distance constraint (2). Only nodes that are activated as flooding nodes, propagate the reply message. Moreover, the node re-broadcasts the reply message only if it is not activated as a flooding node during the current route refresh sequence. Therefore a node will re-broadcast only the first reply message for each source during a particular refresh sequence. The protocol thus creates the flooding group for each source consisting of nodes that satisfy hop count distance constraint (1); the set of nodes being determined by constraint (2). Constraint (2) directly follows from the fact that the group member sets the TTL in the reply message to $D_{sm}$, which was obtained during the request phase. Each source thus creates its own *flooding group*, connecting the source to all the group members. The source maintains a different *flooding group* for each multicast group, as the group membership is different for different groups.

$$D_{sn} \le D_{sm} \tag{1}$$

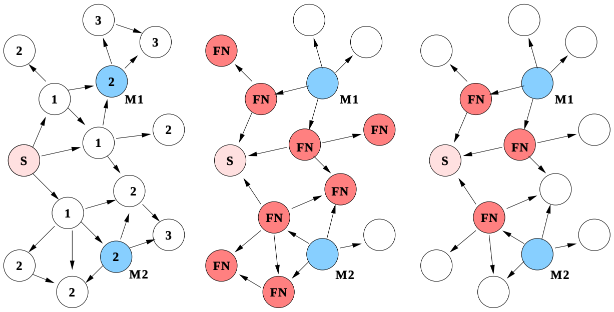
$$D_{mn} \le D_{sm} \tag{2}$$

where $D_{sm}$, $D_{sn}$, $D_{mn}$ are as described above.

Controlling group membership with the above relaxed distance constraint could lead to large flooding groups per source, as can be seen in Figure 1(b). An ideal flooding group would be one that consists of nodes that form the shortest paths between the source and the group members. We derive the following distance constraints recognizing that a node lies in the shortest path between a source and a member if the sum of the node’s distance to the source and the node’s distance to the member is less than or equal to the distance between the source and the member.

$$D_{sn} + (D_{sm} - TTL_{rep}) \le D_{sm} \longleftrightarrow D_{sn} \le TTL_{rep} \tag{3}$$

$D_{sm}$ is the initial value of the TTL in the reply message sent by the member, and $TTL_{rep}$ is the decremented value of TTL in the reply message that the node receives. Thus ($D_{sm}$ - $TTL_{rep}$) is the hop count distance between the node and the group member. The nodes use the reduced form of this constraint to decide to join the flooding group and thus only the nodes that form the shortest path can become members of the flooding group. This is illustrated in Figure 1(c); clearly only the nodes in the shortest path between the source and the members become flooding nodes. As before the propagation of the reply messages is controlled by the distance constraint (2). If multiple shortest paths exist then all nodes in these paths are included in the flooding group. Thus, the reduced constraint limits the size of the flooding group while ensuring that the shortest path(s) between the source and the members are always included.



Request phase (a)

Response phase (b)

Response phase (c)

Fig. 1. Flooding Group Formation

## B. Data Forwarding

*1) Hop Count Data Forwarding:* Only members of the flooding group forward data packets for that source. All duplicate packets are dropped. To reduce MAC layer contention and collision due to redundant transmission of data, a *hop count* field is included in the data packet, which is initialized to zero by the source. When an active flooding node receives a data packet, it compares its latest hop count value for this source ($D_{sn}$) with the hop count field in the data packet. The node re-broadcasts the packet only if the stored hop count is greater than the hop count value in the packet. The node stores its hop count distance to the source in the data packet before retransmitting it. This mechanism ensures that data packets are not repeatedly transmitted in the same region of the network and allows the flooding wave to progress towards the group members.

*2) Probabilistic Data Forwarding:* The *flooding group* provides multiple paths from the source to the group members. Redundant transmission of data along these paths will improve data delivery, however it will result in excessive overhead. We propose a probabilistic data forwarding mechanism to reduce data overhead and describe a method to determine a meaningful value for the retransmission probability ($P_{send}$) of a packet. In this scheme, when a node receives a non-duplicate data packet, it stores the packet and waits for a short random interval of time for arrival of duplicate packets. The node increments a counter for every data packet received from a node in its peer distance level from the source, i.e., data packets having hop count value same as this node's stored hop count value. All other duplicate data packets are dropped. When the wait interval is over, the node calculates the retransmission probability of the packet using (4). The node decides to retransmit the packet with probability $P_{send}$ and drop the packet with probability $(1-P_{send})$. Once the wait interval is over, all duplicates irrespective of hop count value will be dropped.

$$P_{send} = \frac{1}{1+n} \tag{4}$$

where, *n* is the number of duplicate packets received from the same hop count peer level. Figure 2 demonstrates the benefit of the probabilistic forwarding scheme. Source S is connected to member M through flooding nodes F1, F2 and F3 that form the shortest paths between S and M. When the source S transmits a packet, F1, F2, and F3 receive the packet. Let us assume, node F2 times out first and transmits with probability 1. Nodes F1 and F3 which are in the same peer hop count level will increment their duplicate counters upon receiving the packet from F2. Thus F3 and F1 will retransmit the packet with probability 0.5. Thus the number of retransmissions is potentially reduced and at the same time, at least one packet is forwarded in each peer hop count level ensuring that the member receives the packet.

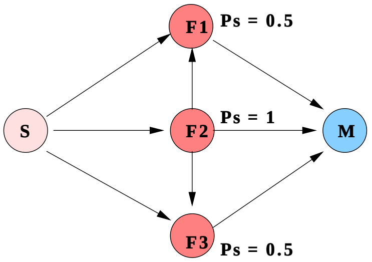


Fig. 2. Probabilistic Forwarding of data

## IV. SIMULATION SETUP AND RESULTS

### A. Simulation setup

OPNET 7.0 [10] discrete event engine was used to simulate our algorithms. The simulation modeled a network of 50 nodes randomly placed within a $1000m$ x $1000m$ area. Nodes in the network move according to the "Billiard Mobility" model [11]. This model is similar to the random way point model with the wait period set to $0$. At the physical layer, radio propagation distance for each node was set to $250m$ and the shared channel capacity was $1Mbps$. Our model does not support radio capture [12] so, in the case of packet collisions all packets are dropped. The IEEE 802.11 (DCF) was used as the Medium Access Control (MAC) protocol. The communication medium is broadcast and nodes have bi-directional connectivity. Group members and sources are randomly chosen from the nodes in the network. A source generates CBR traffic at $2packets/secs$ with each packet having a payload of 128 bytes. Each simulation was run for 100 seconds. Multiple runs were conducted with different seed values for each scenario and the collected data were averaged over these runs. The multicast algorithms were developed as separate OPNET routing layer protocols.

The performance of the following schemes are evaluated:

- flooding: flooding as a multicast routing protocol is used as a baseline.
- basic-sgfp: this scheme uses the relaxed or basic distance constraints (1) and (2) to create the group and hop count data forwarding.
- sp-sgfp: this scheme uses the shortest path distance constraints (3) and hop count data forwarding.
- p-sgfp: this scheme uses relaxed distance constraints and probabilistic data forwarding.
- psp-sgfp: this scheme uses shortest path distance constraints and probabilistic data forwarding.

The following simulation metrics are considered for comparing the schemes:

- Packet Delivery Ratio: the ratio of the number of data packets received by the group members to the number of data packets expected to be received by the group members (number of packets sent by the source times the number of members).
- Total Overhead: is defined as the ratio of the total packets transmitted in the network (control + data) to the number of data packets received by the group members.

### B. *Simulation Results*

Figures 3 and 4 show the Packet Delivery Ratio (PDR) and the Total Overhead as a function of node speed $(0 - 30m/s)$. The network has $5$ sources and $20$ group members.The refresh interval is $4$ seconds. The *flooding* scheme has the best PDR performance (around $95\%$) for all mobilty speeds as every node rebroadcasts every packet. Redundant data transmission contributes to total overhead and this remains constant against mobility as every node retransmits the packet. All the source initiated schemes show a linear decrease in packet delivery with increased mobility speed; this is to be expected as the movement of the nodes will disrupt the flooding group resulting in loss of packets. However, it should be noted that even at node speeds of $30m/s$ the PDR is around $84\%$ indicacating that the flooding group is a very robust multicast structure. The total overhead of the probabilistic schemes is less than that of flooding. Particularly, the total overhead of psp-sgpf is $20\%$ less than that of flooding. Thus the source initiated multicast protocol using shortest path flooding groups and probabilistic data forwarding achieves comparable robustness to flooding while significantly reducing the total overhead.

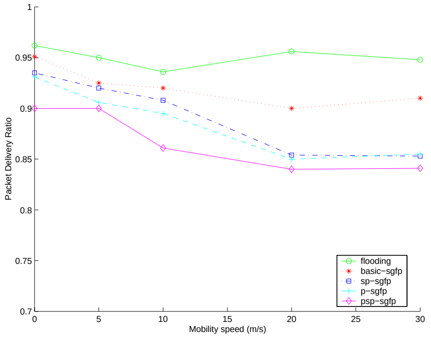


Fig. 3. Packet Delivery Ratio vs Mobilty Speed

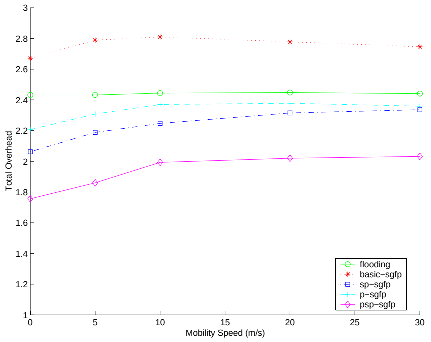


Fig. 4. Total Overhead vs Mobilty Speed

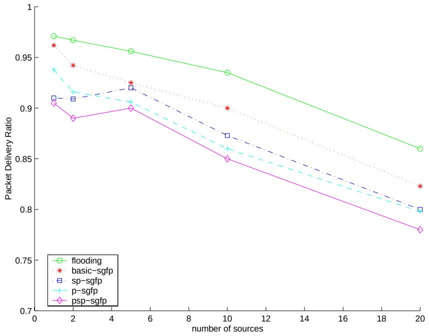


Fig. 5. Packet Delivery Ratio vs Number of Sources

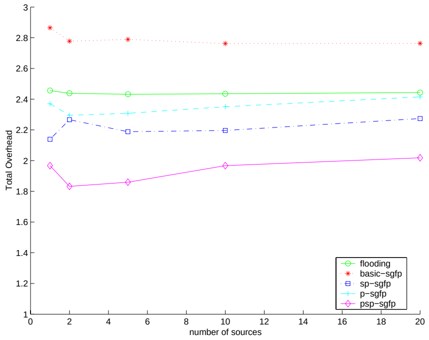


Fig. 6. Total Overhead vs Number of Sources

Figures 5 and 6 show the Packet Delivery Ratio (PDR)and the Total Overhead as a function of the number of sources $(1 - 20)$. Node mobility was set to $5m/s$. The network had $20$ group members.The refresh interval is $4$ seconds. The PDR decreases linearly with increase in the number of sources. This is due to increased MAC layer collisions resulting in loss of data packets and outdated flooding groups. The total overhead for all the schemes remains the same, as even though the control and redundant packets increase the number of data packets delivered also increases. The source initiated schemes imitate the performance of flooding. The psp-sgpf scheme achieves efficient data distribution while maintaining a comparable Packet Delivery Ratio to flooding. Figures 7 and 8 show the Packet Delivery Ratio (PDR) and the Total Overhead as a function of the multicast group size $(10 - 40)$. Node mobility was set to $5m/s$. The network had $5$ sources.The refresh interval is $4$ seconds. PDR for the flooding scheme remains constant as the group size increases. Since every node rebroadcasts the packet, every node receives the packet irrespective of whether it is a group member or not. The source initiated schemes have packet delivery performance within $10\%$ of that of flooding. Particularly, the PDR for *psp-sgfp* is around $90\%$ as the group size increases. This is because of the efficient data distribution achieved due to the shortest path flooding group and probabilistic data forwarding. The total overhead decreases for all the schemes as the group size increases. We see that the overhead for all the schemes converges, this is because as the group size increases multicast resembles broadcast.

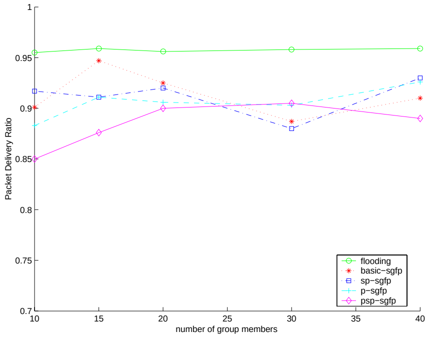


Fig. 7. Packet Delivery Ratio vs Multicast Group Size

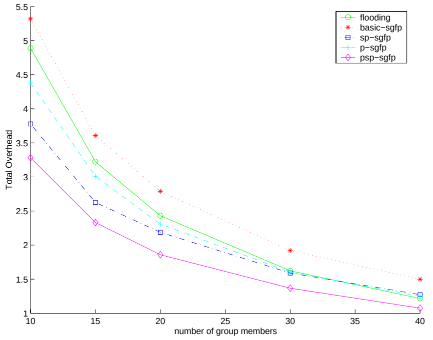


Fig. 8. Total Overhead vs Multicast Group Size

Figure 9 shows the tradeoff between the Packet Delivery Ratio and the total overhead as a function of the refresh interval i.e. the frequency of flooding group update. The network had $5$ sources, $20$ group members and the nodes moved at $5m/s$. This interesting curve shows that the Packet Delivery Ratio remains almost the same as the refresh interval increases. Thus the psp-spfp scheme can achieve comparable packet delivery to that of flooding while having a $40\%$ lesser overhead than that of flooding.

## V. CONCLUSIONS

The inherent constraints of MANETs viz mobility, bandwidth and energy limitations pose difficult challenges in designing multicast routing protocols. Thus, it is necessary for a multicast protocol to not only be efficient but also be robust against mobility and other network dynamics. The Probabilistic Shortest Path Source Grouped protocol (PSP-SGFP) described in this paper achieves robustness similar to that of flooding while at the same time considerably improving the data delivery efficiency. The steady packet delivery performance of the protocol even at high node speeds $(30m/s)$ proves the robustness of the flooding group multicast structure. At the same time the total overhead is $20\%$ less than that of plain flooding. Moreover, the tradeoff curve as a function of the refresh interval indicates that the protocol can be $40\%$ more efficient than plain flooding without compromising robustness. The protocol provides a highly robust multicast structure for a wide range of node speeds while achieving significant reduction in overhead.

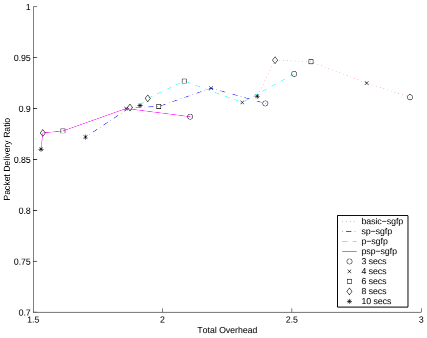


Fig. 9. Trade-off curve for refresh intervals

## REFERENCES

[1] E. Royer and C. E. Perkins. Multicast operation of ad hoc on-demand distance vector routing protocol. In *Proceedings of MobiCom*, Seattle, WA, August 1999.

[2] M. Liu, R. Talpade, A. McAuley, and E. Bommaiah. AMRoute: Ad hoc multicast routing protocol. Technical Report 8, University of Maryland, 1999.

[3] C. W. Wu and Y. C. Tay. AMRIS: A multicast protocol for ad hoc wireless networks. In *Proceedings of IEEE MILCOM*, Atlantic City, NJ, November 1999.

[4] S.-J. Lee, M. Gerla, and C.-C. Chiang. On-demand multicast routing protocol. In *Proceedings of IEEE WCNC*, pages 1298–1304, New Orleans, LA, September 1999.

[5] E. L. Madruga and J. J. Garcia-Luna-Aceves. Scalable multicasting: The core assisted mesh protocol. *ACM/Baltzer Mobile Network and Applications Journal, Special Issue on Management of Mobility*, 1999.

[6] P. Sinha, R. Sivakumar, and V. Bharghavan. MCEDAR: Multicast core extraction distributed ad hoc routing. In *Proceedings of the Wireless Communications and Networking Conference*, 1999.

[7] K. Chandrashekar. Multicast routing in mobile wireless ad hoc networks using source grouped flooding. Master's thesis, University of Maryland, 2002 www.glue.umd.edu/ karthikc.

[8] C.Ho, K.Obraczka, and G.Tsudik K.Vishwanath. Flooding for reliable multicast in multi-hop ad hoc networks. In *MobiCom Workshop on Discrete Algorithms and Methods for Mobility*.

[9] S.Y.Ni, Y.-C.Tseng, Y.-S.Chen, and J.-P. Sheu. The broadcast problem in a mobile ad hoc network. In *Proceedings of MobiCom*, August 1999.

[10] Opnet modeler version 7.0. www.opnet.com.

[11] Billiard mobility
. http://w3.antd.nist.gov/wctg/manet/prd␣aodvfiles.html.

[12] C.Ware, T.Wysocki, and J.F.Chicharo. Simulation of capture behaviour in ieee 802.11 radio modems. *Journal of Telecommunications and Information Theory*, 2001.