

IETF MANET Working Group
INTERNET-DRAFT

Jorjeta G. Jetcheva
Yih-Chun Hu
Carnegie Mellon University
David A. Maltz
AON Networks
David B. Johnson
Rice University
17 November 2000

**A Simple Protocol for
Multicast and Broadcast in Mobile Ad Hoc Networks**

<[draft-ietf-manet-simple-mbcast-00.txt](#)>

Status of This Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC 2026](#) except that the right to produce derivative works is not granted.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>.

Abstract

The protocol specified in this document is designed to provide multicast and broadcast functionality in mobile ad hoc networks. It utilizes the Route Discovery mechanism defined by the Dynamic Source Routing protocol (DSR) [[4](#), [5](#), [7](#)] to flood the data packets through the network. Although this protocol is derived from DSR, it can be implemented as a stand-alone protocol. In fact, it does not rely on unicast routing to operate. If DSR is already implemented on the network, very minor modifications are required to enable this protocol.

This multicast and broadcast protocol utilizes controlled flooding to distribute data in the network and does not require the establishment of state in the network for data delivery. It is not intended as a general purpose multicast protocol. Its applicability is mainly in environments characterized by very high mobility or by a relatively small number of nodes. In the former case, protocols relying on the establishment of multicast state perform inadequately because they are unable to track the rapid changes in topology. In the latter case, the overhead of keeping multicast state exceeds the overhead of flooding.

Contents

Status of This Memo	i
Abstract	ii
1. Introduction	1
2. Assumptions	2
3. Protocol Overview	3
3.1. Overview of DSR	3
3.2. Overview of the Multicast and Broadcast Protocol	4
4. Detailed Operation	5
4.1. Originating a Packet	5
4.2. Originating a Route Request	5
4.3. Processing a Received Route Request Option	5
5. IANA Considerations	6
6. Security Considerations	7
Acknowledgments	8
References	9
Chair's Address	10
Authors' Addresses	11

1. Introduction

This document describes a protocol for multicast and broadcast in wireless ad hoc networks. This protocol was developed by the Monarch Project [6, 3] at Rice University and Carnegie Mellon University. This protocol is not meant to be a general purpose multicast protocol. It is applicable to small networks, or networks characterized by very high mobility.

The definition of this protocol is derived from the Dynamic Source Routing protocol (DSR) for unicast routing in wireless ad hoc networks described in [4, 5, 7]. Even though this protocol uses some mechanisms that are defined as part of DSR, it can be implemented and used independently. In fact, this protocol does not require any unicast functionality to operate. If DSR is employed as the unicast routing protocol in an ad hoc network, adding this protocol to it requires trivial modifications.

DSR is an on-demand routing protocol which allows nodes to dynamically discover a source route across multiple network hops to any destination in the ad hoc network. DSR employs two mechanisms to enable unicast routing -- Route Discovery and Route Maintenance. When a node wishes to communicate with another node, it employs Route Discovery to flood a control packet, called a Route Request, through the network, in search of a route to the destination of the communication. The Route Maintenance mechanism monitors the status of source routes in use, detects link-failures and repairs routes with broken links.

Multicast and broadcast forwarding in this protocol is based on the Route Discovery mechanism of DSR. Data packets are included in Route Requests and are thereby flooded through the network. No multicast state is setup in the network for data delivery.

This protocol is superior to protocols which require explicit establishment of multicast state for data distribution in certain types of networks. In small networks, this protocol requires less overhead and provides the same level of functionality. In networks with a very high degree of mobility, a stateful protocol may not be able to track the rapidly changing topology and will only contribute overhead.

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [2].

2. Assumptions

We assume that all nodes wishing to communicate with other nodes within the ad hoc network are willing to participate fully in the protocols of the network. In particular, each node participating in the network should also be willing to forward packets for other nodes in the network.

Packets may be lost or corrupted in transmission on the wireless network. A node receiving a corrupted packet can detect the error and discard the packet.

3. Protocol Overview

3.1. Overview of DSR

DSR employs two mechanisms termed Route Discovery and Route Maintenance. Route Discovery is the mechanism whereby a node S wishing to send a packet to a destination D obtains a source route to D.

Route Maintenance is the mechanism whereby S is able to detect, while using a source route to D, if the network topology has changed such that it can no longer use its route to D because a link along the route no longer works. When Route Maintenance indicates a source route is broken, S can attempt to use any other route it happens to know to D, or can invoke Route Discovery again to find a new route.

When the application layer on S first starts sending data to a destination D, the DSR layer buffers the data and initiates a Route Discovery. A Route Request packet with a target of D is broadcast in the network. It is forwarded hop-by-hop outward from the node initiating the Route Discovery. When the Route Request reaches D or a node N that has a route to D, it is not forwarded on. Instead, a Route Reply packet is sent back to S. The Route Reply packet includes a full source route to the destination D. This source route is included in the source header of each data packet sent to D and enables stateless forwarding by nodes in the network who can determine whether they need to forward the packet by checking whether they are listed on the source route in the data packet's header. Data sent to D by the application layer, is buffered by DSR, until a Route Reply with a route to D is received, at which point, these packets are forwarded to D along the acquired route.

A Route Request is forwarded by a node if the node (1) is not already listed in the recorded source route in this copy of the Request, and (2) has not recently seen another Route Request packet belonging to this same Route Discovery. A node can determine if it has recently seen such a Route Request, since each Route Request packet contains a unique identifier for this Route Discovery, generated by the initiator of the Discovery. Each node maintains an LRU cache, called a Route Request Table, of the unique identifier from each recently received Route Request. By not propagating any copies of a Request after the first, the overhead of forwarding additional copies that reach this node along different paths is avoided.

In addition, the Time-to-Live field in the IP header of the packet carrying the Route Request MAY be used to limit the scope over which the Request will propagate, using the normal behavior of Time-to-Live

defined by IP [[8](#), [1](#)].

3.2. Overview of the Multicast and Broadcast Protocol

When a node wants to send a broadcast packet, it uses the DSR Route Discovery mechanism to propagate the packet in the network. This is accomplished by including the data packet in a Route Request packet. The Route Request is flooded through the ad hoc network using the normal Route Discovery procedure described in [Section 3.1](#), within the specified TTL of the originator.

Multicast data packets are flooded through the network in the same fashion. The target of the Route Request is the multicast group address. Multicast group receivers make a copy of the data packet included in the Route Request and pass it up the protocol stack, before forwarding the Route Request onward.

4. Detailed Operation

4.1. Originating a Packet

When node A originates a packet, the following steps **MUST** be taken before transmitting the packet:

If the destination address is a multicast or broadcast address, piggyback the data packet on a Route Request packet targeting that address. Route Request origination is described in [Section 4.2](#).

4.2. Originating a Route Request

Route Discovery is the on-demand process by which nodes actively obtain source routes to destinations to which they are actively attempting to send packets. Route Discovery is initiated for each multicast or broadcast packet by the originator of this packet as described in [Section 4.1](#). A Route Request is transmitted with the multicast group or broadcast address as the "target" of the Route Discovery. The Route Request initialization proceeds as described in [7], except for the following condition:

Route Discoveries for a multicast or broadcast address **SHOULD** always be permitted and **SHOULD** not be rate limited.

4.3. Processing a Received Route Request Option

Processing of a received Route Request option, proceeds as described in [7], except for the following:

If node A is a member of the multicast group indicated by Request.Target_Address, then create copy of the data packet piggybacked in the Route Request and pass it up the protocol stack before re-propagating the Route Request.

Non-duplicate Route Request packets with multicast or broadcast target addresses **MUST** always be re-propagated.

The Route Cache **SHOULD NOT** be consulted on behalf of Route Requests with multicast and broadcast targets.

5. IANA Considerations

This protocol does not define any new constants or packet types. It does use, however, packet types and constants defined by [\[7\]](#) which must be assigned by IANA.

6. Security Considerations

Security issues relevant to DSR [\[7\]](#) apply also to the protocol described here. This protocol does not introduce any new security considerations.

Acknowledgments

The protocol described in this draft has been designed within the Monarch Project, a research project at Rice University and Carnegie Mellon University which is developing adaptive networking protocols and protocol interfaces to allow truly seamless wireless and mobile node networking [[6](#), [3](#)].

References

- [1] Robert T. Braden, editor. Requirements for Internet hosts---communication layers. [RFC 1122](#), October 1989.
- [2] Scott Bradner. Key words for use in RFCs to indicate requirement levels. [RFC 2119](#), March 1997.
- [3] Carnegie Mellon University Monarch Project. CMU Monarch Project Home Page. Available at <http://www.monarch.cs.cmu.edu/>.
- [4] David B. Johnson. Routing in ad hoc networks of mobile hosts. In Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications, pages 158--163, December 1994.
- [5] David B. Johnson and David A. Maltz. Dynamic Source Routing in ad hoc wireless networks. In Mobile Computing, edited by Tomasz Imielinski and Hank Korth, chapter 5, pages 153--181. Kluwer Academic Publishers, 1996.
- [6] David B. Johnson and David A. Maltz. Protocols for adaptive wireless and mobile networking. IEEE Personal Communications, 3(1):34--42, February 1996.
- [7] David B. Johnson, David A. Maltz, Yih-Chun Hu, and Jorjeta Jetcheva. The Dynamic Source Routing protocol for mobile ad hoc networks. Internet-Draft, [draft-ietf-manet-dsr-04.txt](#), November 2000. Work in progress.
- [8] J. B. Postel, editor. Internet Protocol. [RFC 791](#), September 1981.

Chair's Address

The Working Group can be contacted via its current chairs:

M. Scott Corson

Institute for Systems Research

University of Maryland

College Park, MD 20742

USA

Phone: +1 301 405-6630

Email: corson@isr.umd.edu

Joseph Macker

Information Technology Division

Naval Research Laboratory

Washington, DC 20375

USA

Phone: +1 202 767-2001

Email: macker@itd.nrl.navy.mil

Authors' Addresses

Questions about this document can also be directed to the authors:

Jorjeta Jetcheva
Carnegie Mellon University
Computer Science Department
5000 Forbes Avenue
Pittsburgh, PA 15213-3891
USA

Phone: +1 412 268-3053
Fax: +1 412 268-5576
Email: jorjeta@cs.cmu.edu

Yih-Chun Hu
Carnegie Mellon University
Computer Science Department
5000 Forbes Avenue
Pittsburgh, PA 15213-3891
USA

Phone: +1 412 268-3075
Fax: +1 412 268-5576
Email: yihchun@cs.cmu.edu

David A. Maltz
AON Networks
3045 Park Blvd.
Palo Alto, CA 94306
USA

Phone: +1 650 688-3128
Fax: +1 650 688-3119
Email: dmaltz@cs.cmu.com

David B. Johnson
Rice University
Computer Science Department, MS 132
6100 Main Street
Houston, TX 77005-1892
USA

Phone: +1 713 348-3063
Fax: +1 713 348-5930
Email: dbj@cs.rice.edu

