Simplified Multicast Forwarding for MANET
draft-ietf-manet-smf-05

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are draft 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.

This Internet-Draft will expire on December 28, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2007).
Abstract

This document describes the Simplified Multicast Forwarding (SMF) protocol. SMF provides a basic IP multicast forwarding capability suitable for mobile ad-hoc networks (MANET). SMF applicability is limited to providing multicast forwarding within MANET routing regions. SMF specifies mechanisms to provide temporally unique multicast packet identification for the purpose of enabling MANET-specific duplicate packet detection (DPD). SMF also specifies the operation of DPD maintenance and checking for both sequence-based and hash-based methods. For IPv6, a hop-by-hop option header is specified that assists in the overall DPD process. The optional operation of intermediate devices, called taggers, is also specified and relates to potential use with multiple border routers. SMF is designed to take advantage of reduced relay sets for efficient MANET multicast forwarding and the document describes use and interaction with a number of approaches. Pseudocode and additional educed relay set discussion is provided in the Appendices. Basic issues relating to the operation of multicast MANET border routers are discussed but ongoing work in this area remains and is beyond the scope of this document.
1. Requirements Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].
2. Introduction and Scope

Past MANET unicast routing protocol designs have demonstrated effective and efficient mechanisms to flood routing control packets throughout a wireless routing region. For example, algorithms specified within MANET RFC 3626 [RFC3626] and RFC 3684 [RFC3684] provide distributed methods of dynamically electing reduced relay sets that attempt to optimize control packet flooding of routing control packets amongst MANET routing peers. The Simplified Multicast Forwarding (SMF) extends this concept to the forwarding of data plane IP multicast packets. The main goals of the SMF specification are to define IPv4 and IPv6 duplicate multicast packet detection (DPD) mechanisms and to adapt efficient reduced relay set designs in MANET environments. The intent is to apply these mechanisms to IP multicast packet forwarding within a MANET routing region. SMF is intended for use when localized efficient flooding is deemed an effective technique for multicast forwarding in dynamic wireless networks. The SMF baseline design limits the scope to best effort multicast forwarding and its applicability is also intended to be constrained within a MANET routing region. Figure 1 provides an overview of the logical SMF node architecture, consisting of optional "Neighborhood Discovery", "Relay Set Selection" and "Forwarding Process" components. Typically, relay set selection (or even self-election) will occur based on input from a neighborhood discovery process, and the forwarding process will be controlled by status based upon relay set selection. This relay set information may be obtained from a coexistent process (e.g., MANET unicast routing protocol using relay sets). In some cases, the forwarding decision for a packet may also depend on previous hop or incoming interface information. The asterisks (*) in Figure 1 mark the primitives and relationships needed by relay set algorithms requiring previous-hop packet forwarding knowledge.
SMF is a network layer multicast forwarding process compatible with different neighborhood discovery protocols and relay set selection algorithms. Different discovery mechanisms or relay set algorithms may be applicable for different MANET routing protocols and deployments and it is not the intent that SMF dictate a single approach. However, interoperable SMF implementations must conform to the specified DPD approach and the related header options. In the simplest case of multicast forwarding, Classical Flooding (CF) with DPD is supported. This mode eliminates the need for any relay set algorithm or neighborhood topology information. However, a reduced relay set mechanism will typically be preferred in a deployment. A reduced relay set is realized by selecting a subset of all possible nodes in a MANET routing region as the forwarding relay set. Known relay set selection algorithms can be used to provide and maintain a dynamic distribution mesh for forwarding user multicast data[MDC04]. A few such relay set selection algorithms are described in Appendices of this document. Additional relay set algorithms or extensions may be specified in the future for use with SMF.

Dynamic neighborhood topology information is often needed to determine and maintain an optimized set of forwarding nodes. It is expected that neighborhood topology discovery functions will be provided by a MANET unicast routing protocol or a MANET NeighborHood Discovery Protocol (NHDP) implementation running in concurrence with SMF. This specification does not preclude a lower link layer from providing necessary neighborhood information through an enhanced interface if available. An SMF implementation SHOULD provide the ability for relay state to be dynamically managed per operating
interface. Some of the relay state maintenance options and interactions are outlined later in Section 6. This document states specific requirements for neighborhood discovery with respect to the forwarding process and relay set selection algorithms described herein. SMF relies on the MANET NHDP specification to assist in relay set maintenance in the absence of any MANET unicast protocol or lower layer information interface.

2.1. Abbreviations

MANET : Mobile Ad hoc Network
SMF : Simplified Multicast Forwarding
CF : Classical Flooding
CDS : Connected Dominating Set
MCDS : Minimum Connected Domination Set
MPR : Multi-point Relay
S-MPR: Source-based MPR
CDS-MPR: CDS-based MPR
E-CDS: Essential Connected Dominating Set
DPD: Duplicate Packet Detection
NHDP: Neighborhood Discovery Protocol
S-DPD: Sequence-based Duplicate Packet Detection
H-DPD: Hash-based Duplicate Packet Detection
HAV: Hash Assist Value
3. Applicability

In highly dynamic mobile topologies, a more traditional tree-based multicast routing protocol may not always be sensible or needed. A basic packet forwarding service that reaches all MANET SMF routers participating within a localized MANET routing region can provide a useful group communication mechanism for various classes of applications. Applications that MAY take advantage of a simple multicast forwarding service within a MANET routing region include multimedia streaming, interactive group application, peer-to-peer middleware multicasting, and multi-hop discovery services.

Note again that Figure 1 provides a notional architecture for _typical_ MANET SMF-capable nodes. However, a goal is that simple end-system (non-forwarding) wireless nodes may also participate in multicast traffic transmission and reception with standard network layer semantics. Also, a multicast border router or proxying mechanism MUST be used when interoperating with other IP multicast routing such as that for fixed-infrastructure networks (e.g., Protocol Independent Multicast (PIM)). In present experiments, proxying methods have demonstrated gateway functionality at MANET border routers operating with external IP multicast routing protocols. Although SMF may be extended or combined with other protocols to provide increased reliability and group specific forwarding state, the details of such enhanced methods will be discussed in future documents.
4. SMF Packet Processing and Forwarding

The SMF Packet Processing and Forwarding actions are conducted with the following packet handling activities:

1. Processing of outbound, locally-generated multicast packets.

2. Reception and processing of inbound packets on a specific network interface(s).

In the case that sequence-based DPD as described in Section 5 is used, the purpose of intercepting outbound, locally-generated multicast packets is to apply resequencing of the IPv4 ID header field or add options headers as needed (e.g. IPv6). In the case that resequencing is deemed necessary, it is RECOMMENDED that sequence numbering be applied such that a different sequence number space per <sourceAddress::destinationAddress> tuple be used. For initial SMF purposes where no distinct routing path decisions for different IP Multicast address destinations occur, it might appear to be sufficient to use sequence number spaces aggregated across all IP Multicast destinations (or across all IP destinations for a source as is the default implementation of the IPv4 ID field in many operating systems). However, future SMF extensions, beyond the present discussion, may contain dynamic forwarding state dependent on the multicast destination address. The future possibility that different multicast address destinations may be routed differently suggests that "per source/destination" identification be used. The default global IPv4 ID sequence space may be sufficient for some SMF deployments and interception of outbound packets may not be required if end systems have numbered the IPv4 ID field in an acceptable manner. In other cases, such as when IPSec headers have been applied to packets, other sequence information may be available for the SMF process to make use of in its duplicate table management.

Inbound multicast packets will be received by the SMF implementation and processed for possible forwarding. There will be some well-known multicast groups for flooding to all routers of an ad hoc network specified for use with the network-layer flooding provided by SMF. These multicast groups are specified to contain all MANET routers of a contiguous MANET routing region, so that packets transmitted to the multicast address associated with the group will be delivered to all nodes as desired. For IPv6, the multicast address is specified to be "site-local". The names of the multicast groups are given as "SL_MANET_ROUTERS". This document does not support transmissions to any directed broadcast address ranges. Minimally SMF SHALL forward, as instructed by the relay set selection algorithm, unique (non-duplicate) packets received for these well-known group addresses when the TTL or hop count value in the IP header is greater than 1.
Optionally, SMF deployments SHOULD forward packets for additional "global scope" multicast groups to support application needs or to distribute multicast packets that ingress the MANET routing region via border routers. These additional addresses will be specified by an _a priori_ list or possibly through a implementation of a dynamic address management interface that may interact with a yet to be defined MANET dynamic group membership extension. In all cases, the following rules SHALL be observed for SMF multicast forwarding:

1. Multicast packets with TTL <= 1 MUST NOT be forwarded*.

2. Link Local multicast packets MUST NOT be forwarded.

3. Incoming multicast packets with an IP source address matching one of those of the local host interface(s) MUST NOT be forwarded.

4. Received packet frames with the MAC source address matching the local host interface(s) MUST NOT be forwarded.

5. Received packets for which SMF cannot ensure DPD uniqueness MUST NOT be forwarded.

Note that rule #3 is important because in wireless networks, the local host may receive re-transmissions of its own packets when they are forwarded by neighboring nodes. This rule avoids unnecessary retransmission of locally-generated packets even when other forwarding decision rules would apply.

Once these criteria have been met, the implementation should reference a forwarding decision algorithm, possibly in concert with duplicate packet detection, to determine the next step in packet processing. The forwarding decision may be implicit, dependent upon DPD results, only if the SMF implementation is configured to perform classical flooding (CF) of IP multicast packets. Otherwise, a forwarding decision is controlled using additional information including relay set state. Neighborhood discovery protocols coupled with the Source-based Multi-Point Relay (S-MPR) or other CDS selection algorithms described later MAY be used to determine the local host’s status with respect to forwarding. For example, algorithms may control forwarding based on a relay set election and previous hop identifier (e.g. S-MPR forwarding), while others may designate the local host as a forwarder of all neighbor packets based on the neighborhood broadcast topology (e.g. Essential CDS (E-CDS)).

DPD is a fundamental and critical portion of the SMF forwarding process. In general, detection of received duplicate packets is required to avoid forwarding the same packet multiple times. However, in some cases (e.g., S-MPR), duplicate detection of some
non-forwarded packets is also needed to maintain efficient forwarding. Details on different duplicate packet detection and forwarding rules for the S-MPR, and E-CDS algorithms are given in Appendices of his document.
5. SMF Duplicate Packet Detection

MANET topologies are often mesh-based and the maintenance of any tree structure can be complex under mobile and dynamic conditions. These MANET characteristics lead to DPD being a common requirement in MANET packet flooding. While this requires increased per-packet processing, it is often necessary in MANET-specific multicasting because packets may be forwarded out the same physical interface upon which they arrived and nodes can receive copies of previously-transmitted packets from other forwarding neighbors. This section describes a basic SMF DPD mechanism and some alternative operational options as considerations.

SMF MUST implement detection of duplicate multicast packets by a temporal packet identification scheme. It is RECOMMENDED this be implemented by keeping a history of previous received and forwarded packet identifiers for comparison against recently forwarded multicast packets. In the IPv6 case, SMF specifies two approaches to multicast duplicate packet identification: a sequence numbering mechanism and a hash-based ID mechanism. In the IPv4 case, SMF specifies a sequence-based approach but does not necessarily preclude hashing. To enforce proper avoidance of duplicate forwarding, SMF implementations MUST manage DPD packet state for received and forwarded packets. In the case that sequence-based packet identification is used, implementations SHOULD timeout stale histories for <sourceAddress::destinationAddress> entries where new, non-duplicate packets have not been recently received. The proper minimum duration of any timeout delay SHOULD cover the expected maximum network traversal time, MAX_PACKET_LIFETIME. We define MAX_PACKET_LIFETIME as a system dependent estimate of the maximum lifetime of a multicast packet being forwarded between any source and destination nodes in the SMF network region. If the timeout is reset only upon reception of non-duplicate packets, it also limits the time that packets might be incorrectly dropped if a source node is stopped and restarted in the case of sequence-based packet identification. The required size of the DPD cache is similarly governed and is also a function of the maximum expected packet rate. It should be noted that less stateful bitmask approaches to marking packet status can be used if there is a contiguous space of tuple-based sequence numbers rather than explicit lists of arbitrary packet identifiers.

The DPD mechanism SHOULD avoid keeping unnecessary state for packet flows such as those that are locally generated or link local destinations that would not be considered for forwarding.
5.1. SMF IPv4 Packet Identification

For SMF purposes, IPv4 multicast packets from a particular source are assumed to be marked with a temporally unique identification number in the ID field of the IPv4 packet header that can serve as a "packetIdentifier" for SMF purposes. Unfortunately, in present operating system networking kernels, the IP ID header field value is not always generated or applied in a consistent manner with respect to SMF needs. In order to build a working implementation without encapsulating packets, an SMF implementation SHOULD provide a sequence generation and marking module that can maintain and set a monotonically increasing IP ID field for locally-generated multicast packets with independent sequence number spaces applied on a <sourceAddress::destinationAddress> tuple basis. This process will also need to recalculate and replace a proper IP header checksum for the modified header. For border routers ingressing external IPv4 traffic into an SMF MANET routing region, the border routers SHOULD perform this same IP ID field re-sequencing. Note the presence of IPSec may prevent such resequencing, but fortunately, IPSec does provide its own organic means for duplicate packet detection that is defined for use by SMF.

The use of IPSec for candidate packet flows presents the opportunity to make use of the additional, perhaps more reliable, sequencing information of the IPSec header for unique packet identification. The IPSec header provides a packet identifier field that can be used on a "per-security association" basis. The IP addressing and IPSec Security Parameters Index (SPI) fields are used to identify security associations and, hence, packet flows. So, if the packet is IPSec encapsulated, SMF will check the <sourceAddress::destinationAddress::SPI::packetIdentifier> where the <ESP_seq_number> or <AH_seq_number> from the IPSec header serves as the "packetIdentifier" value.

Although it would be possible to support IPv4 network layer multicast packet fragmentation, we presently do not specify the details of managing such a DPD approach and we recommend having SMF intended sources set the don’t fragment bit and have detected IPv4 fragments dropped SMF. This recommendation avoids the complexity and inefficiencies arising from an implementation supporting IP layer fragmentation of multicast packets and is often recommended best practice in general for multicast.

To perform IPv4 duplicate detection for multicast packets, SMF will check the <sourceAddress::destinationAddress::SPI::packetIdentifier> combination against a history of received packet identifiers. SMF use of the IPv4 ID field has been demonstrated in running prototype code. The adoption of the IPv4 ID field for widespread packet duplication detection has some
disadvantages that need discussion. A main disadvantage is the use
and interpretation of the field is known to be inconsistent across
operating systems. The IPv4 ID field is also limited and may provide
less robust detection for high bandwidth applications since sequence
wrap-around may occur relatively frequently if it is not possible to
achieve "per source/destination" sequencing. As an alternative, the
use of a header option or encapsulation header in future
implementations may provide more flexibility and consistency (see
IPv6 DPD). Another advantage of using a header option (or other
encapsulation, if determined absolutely necessary) is that it would
be possible for MANET SMF border router to assess whether packets
ingressing a MANET routing region have already been properly
sequenced to avoid unnecessary re-injection of packets. We leave
these design alternatives to be further defined and discussed in
future work. A basic sequencing and marking design similar to the
one we formulate here can be easily adapted to work with future
approaches or can be bypassed when not needed.

5.2. SMF IPv6 Packet Identification

The following section describes the mechanism and options for SMF
IPv6 DPD. The core IPv6 header does not provide an explicit
identification header field that can be exploited for DPD. SMF
defines the following two areas to aid in DPD identification:

1. a hop-by-hop DPD options header (supporting sequencing and hash
   assistance), and

2. the use of IPSec sequencing (in sequencing DPD mode) when an
   IPSec header is detected.

SMF MUST provide a DPD marking module that can insert the hop-by-hop
IPv6 header option defined for locally generated multicast packets.
If the packet is _not_ IPSec encapsulated, SMF may use the IPv6
packet header and IPv6 DPD option to form the <sourceAddress::
destinationAddress::packetIdentifier> tuple that is checked against a
cache history of received IPv6 packet identifiers. Alternatively,
SMF may perform general DPD functionality by generating packet
hashing identifiers at the initial ingress and forwarders and
comparing these against a hash history cache. In this case, the IPv6
DPD header option can add a short hash assist value (HAV) when the
source detects a duplicate hash value has been generated. In this
case, implementations SHOULD use a common hash identifier calculation
to ensure the false positive detection method is robust at all nodes.
A header option is defined in Section 5.2.3 to help with the case of
false positives and to ensure a more robust approach in the case of a
weaker hashing algorithm or in the case of temporal packet content
similarities (e.g., multimedia streams, keep alives). It is also
RECOMMENDED that any cache history be managed on a tuple <sourceAddress::hash value> basis.

In sequence-based DPD deployments, it MAY be necessary for an MANET multicast border router to apply the DPD marking on ingressing packets. In this document, such an intermediate system is referred to as a "tagger" (i.e., "tagging" the packet with DPD information) and a "Tagger ID" field is provided in the IPv6 DPD marking mechanism described below. In the case that a packet is tagged, SMF SHOULD perform DPD processing on a <taggerID:destinationAddress> or <taggerID::sourceAddress::destinationAddress::packetIdentifier> depending upon the policy handling the case of multiple border routers ingressing and tagging multiple copies of the same packet flow. The usage of the "Tagger ID" is described in further detail in Section 8. Similarly to the case for IPv4, the presence of IPSec may prevent the intermediate addition of a hop-by-hop options header. Again, the IPSec header provides a packet identifier field that can be used on a "per-security association" basis. The IP addressing fields and IPSec Security Parameters Index (SPI) fields are used to identify security associations and, hence, packet flows. So, if the packet is IPSec encapsulated, SMF will check the <sourceAddress::destinationAddress::SPI::packetIdentifier> where the <ESP_seq_number> or <AH_seq_number> from the IPv6 IPSec header serves as a "packetIdentifier" value.

5.2.1 IPv6 SMF-DPD Header Option Format

Figure 2 illustrates the format of the IPv6 SMF Duplication Packet Detection (SMF-DPD) hop-by-hop header option. If this is the only hop-by-hop option present, the optional "Tagger ID" field is not included, and the size of the DPD packet identifier (sequence number) or hash token is 24 bits or less, this will result in the addition of 8 bytes to the IPv6 packet header including the "Next Header", "Header Extension Length", SMF-DPD option fields, and padding.
"Option Type" = (TBD pending IANA assignment)

"Opt. Data Len" = Length of option content (I.e., 1 + (<IDType> ? (<IDLen> + 1): 0) + Length(DPD ID)).

"H-bit" = a hash indicator bit value identifying DPD marking type. 0 == sequence-based approach w/ optional taggerID and a tuple-based sequence number. 1 == indicates a hash assist value (HAV) field follows to aid in avoiding hash-based DPD collisions.

The following sections will provide specification for both sequence-based DPD (S-DPD) and hash-based DPD (H-DPD) header option implementations.

5.2.2. IPv6 Sequence Based DPD (S-DPD) Header Mode

Figure 3 illustrates the format of the IPv6 SMF-DPD hop-by-hop header option for supporting S-DPD. For S-DPD mode header options the H-bit must be set to zero as shown in Figure 3.

"IDType" = 3-bit type indicating either optional "Tagger ID" field or basic sequencing. An enumeration of initial type values is given below.

"ID Len" = 4-bit length of optional "Tagger ID" field in bytes minus one iff non-zero IdType (I.e., if IdType is non-zero and IdLen==0,
then the length of the "Tagger ID" field is one byte). The "IDLen" field MUST be set to ZERO if "IDType" is ZERO.

Tagger ID = identifies an intermediate node that has applied the SMF-DPD option to the packet (instead of the source).

DPD packet identifier = monotonically increasing n-bit sequence number assigned on a tuple basis as per <sourceAddress::destinationAddress> or <taggerID::sourceAddress::destinationAddress> basis. If "IdType" is non-zero, the length of this field is (<Opt. Data Len> - <IdLen> - 2). Otherwise, the length of this field is (<Opt. Data Len> - 1).

The following list of Tagger ID type values are defined below. Additional Tagger "IDType" values may be assigned in subsequent specifications. Tagger IDTypes only valid when H bit is set to 0.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>NULL</td>
<td>0</td>
<td>Indicates no &quot;Tagger ID&quot; field is present. IdLen MUST be also set to ZERO.</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>1</td>
<td>The &quot;Tagger ID&quot; field of unknown context is present. &quot;ID Len + 1&quot; defines field length in bytes.</td>
</tr>
<tr>
<td>IPv4</td>
<td>2</td>
<td>The &quot;Tagger ID&quot; represents an IPv4 address. The &quot;ID Len&quot; MUST be set to 3.</td>
</tr>
<tr>
<td>IPv6</td>
<td>3</td>
<td>The &quot;Tagger ID&quot; represents an IPv4 address. The &quot;ID Len&quot; MUST be set to 15</td>
</tr>
</tbody>
</table>

This specified format allows a quick check of the "IdType" field to detect whether a "Tagger ID" is present. If "IdType" is NULL, then the length of the "DPD packet identifier" (sequence number) corresponds to (<Opt. Data Len> - 1). If the "IdType" is not NULL, then the length of the "Tagger ID" field is equal to (<IdLen> + 1) and the remainder of the option content comprises the "DPD packet identifier" field. When the "Tagger ID" field is present, duplicate packet detection SHALL be conducted using the <taggerID::sourceAddress::destinationAddress> tuple from the packet to identify the applicable sequence space. When the "Tagger ID" field is not present, then it is assumed that the source host applied the DPD option and the packet’s <sourceAddress::destinationAddress> SHALL be used to identify the sequence space for duplicate packet detection. Thus "Tagger ID" fields sized up to 16 bytes may be applied and the
size of the DPD packet identifier is configurable to meet the needs of different network environments. In fact, if an 8-bit "Tagger ID" and a 16-bit "DPD packet identifier" are used, the size of the SMF-DPD hop-by-hop header extension would still be the minimum possible IPv6 size if no other options are present.

The rationale for providing "Tagger ID" context (i.e., the "IdType" field) is that the tagger identifier may correspond to some commonly-available identifier such as an IP address so that management of a specific identifier space for border routers possibly applying the SMF-DPD may not be necessary. While the context of the "Tagger ID" (what the "Tagger ID" actually represents) is not necessary for SMF DPD processing, it is possible that this context may be useful as part of additional network management or policies that might be operate in concert with SMF.

Figure 4 illustrates a specific example of the SMF-DPD option format when the "Tagger ID" is _not_ applied and a 16-bit "DPD packet identifier" is used. It is RECOMMENDED that a 16-bit "DPD packet identifier" be used for most purposes.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     | Option Type   |OptDataLen = 3 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
          |IdType&IdLen=0 |   DPD packet identifier       |     ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Fig. 4 - Example SMF-DPD Option w/ no "Tagger ID" and 16-bit DPD ID

### 5.2.3. IPv6 Hash Based DPD (H-DPD) Header Mode

Figure 5 illustrates the format of the IPv6 SMF-DPD hop-by-hop header option for supporting hash-based DPD (H-DPD) approaches. Within a H-DPD mode header, the H-bit must be set to 1 as shown in Figure 5. The length of the H-bit + Hash Assist Value (HAV) is equal to (<Opt.Data Len> -1) bytes.
The H-DPD mode header option SHOULD be applied when SMF is operating in a hash-based DPD mode and the source calculates a duplicate hash value within the tuple-based <sourceAddress:: hash value> cache history. The hash marking default approach is RECOMMENDED to be a non-zero monotonically increasing value of 31 bits maintained within the tuple history. This should provide enough variability to resolve envisioned ambiguities given a reasonable strong hash index approach.

5.2.4.  H-DPD Mode Operation

To ensure the robustness of the H-DPD method and the consistent use of the H-DPD option header we specify a default hashing approach for use by H-DPD SMF nodes.

The default mode of SMF H-DPD is as follows. SMF SHOULD perform an MD5 [RFC1321] hash of the immutable fields and header options of the IPv6 multicast header and data contents resulting in a 128 bit digest result. The parsing exception is that SMF should include any detected H-DPD HAV option header in its hash calculation. Other mutable header options should be skipped. SMF H-DPD mode SHOULD maintain a cache history of lower 64 bits of the digest (MD5_64) based upon the tuple <sourceAddress::MD5_64). This approach is likely to have a reasonably low probability of digest collision when packet headers and content are varying. In the SMF case, MD5 is only be applied to provide a reasonable low probability of collision and is not being used for cryptographic or authentication purposes.

If a collision is detected, an H-DPD option header is generated and retested for collision. If rehashing with the generated options header provides a non-collision event after testing the cache history, then the multicast packet is forwarded with the addition of an the IPv6 H-DPD header option. If a collision is detected with the option header in place, the header option should generate a new HAV and retest for collision until a non-colliding digest entry results.

The MD5, indexing, and HAV approach are specified at present for consistency and robustness. Future approaches and experimentation may discover designs tradeoffs in hash robustness and efficiency.
worth considering for future versions of SMF. This MAY include reducing the maximum payload length that is processed, determining shorter indexes, or applying more efficient hashing algorithms.
6. Reduced Relay Set Forwarding and Relay Selection Capability

SMF MUST support CF-based forwarding as a basic forwarding mechanism when reduced relay set information is not available or not selected for operation. In CF mode, each node transmits a locally generated or newly received packet exactly once. The DPD techniques mentioned in the previous section are critical to proper operation and prevent duplicate packet retransmissions by the same forwarding node.

In addition to DPD specification, an additional goal of SMF is to support reduced relay sets as a forwarding mechanisms within dynamic topologies. To accomplish this SMF MUST support the ability to modify local multicast packet forwarding rules based upon relay set state received dynamically during operation. In this way, SMF forwarding can continue to operate effectively as adjacencies within the topology mesh change.

In early SMF implementations, the relay set information has been derived from a coexistent unicast MANET protocol (e.g., OLSR and MANET-OSPFv3) calculation of a reduced relay set for control plane traffic. From current experience, extra pruning considerations are sometimes required when utilizing a relay set from an independent routing protocol process, since a relay set formed for the unicast control plane flooding MAY include a more redundant set of nodes than desired for multicast forwarding use.

Here is a recommended criteria list for relay set selection algorithm candidates:

1. Robustness to topological dynamics and mobility
2. Localized election or coordination of any relay sets
3. Heuristic support for preference or election metrics (Better enables management of relay set)

Some relay set algorithms meeting these criteria are described in the Appendices of this document. Different algorithms may be more suitable for different MANET routing types or deployments. Additional relay set selection algorithms may be specified in separate documents in the future. The Appendices in this document can serve as a template for the content of such potential future specifications.

Figure 6 depicts a state information diagram of possible relay set control options. There are basically three style of SMF operation with reduced relay sets as follows.
1. Unicast dependent operation with a coexisting MANET unicast routing protocol (e.g., MANET-OSPF, OLSR) in which the relay set state is derived from the unicast CDS information.

2. Unicast independent operation in which SMF performs its own Relay Set Selection and derives dynamic neighborhood information from a MANET NHDP process. Additional TLV definitions for related CDS collection may be required as specified in the Appendices.

3. Possible crosslayer implementation that uses L2 neighborhood information and possible triggers to assist the dynamic relay set selection and maintenance process.

Fig. 6 - SMF Relay Set Control Options
7. SMF Neighborhood Discovery Requirements

In absence of a compatible, coexisting unicast routing protocol or lower layer protocol providing neighborhood topology information sufficient for relay set selection, this section defines the issues and additional requirements for a MANET Neighborhood Discovery Protocol (NHDP) that MAY be operational between SMF nodes.

With respect to neighborhood topology knowledge and/or discovery, there are three basic modes of SMF operation:

1. Classical Flooding (CF) mode: with no requirements for discovery or knowledge of neighborhood topology,

2. External CDS control mode: an external process dynamically determines the local SMF relay status (e.g., SMF prototypes have leveraged neighborhood topology information collected by MANET unicast routing protocols such as OLSRv2 or Manet-OSPF ), and

3. Independent CDS control mode: SMF uses the MANET Neighborhood Discovery Protocol (NHDP) [NHDP] to collect localized link information required for the various CDS algorithm modes discussed in the Appendices.

We have previously discussed modes 1 and 2. This section will describe mode 3, using NHDP to support CDS relay set capability independent of any MANET unicast routing protocol process. This design uses and is consistent with the Generalized MANET Packet/Message Format [PacketBB] and NHDP protocol work in progress within the MANET WG.

Core NHDP messages and the neighborhood information base are described separately within the NHDP specification (IETF work in progress). In this mode, SMF uses and relies upon an implementation of NHDP. The NHDP protocol provides the following basic functions:

1. 1-hop neighbor link sensing: maintaining neighbor lists and performing a basic bidirectionality check of neighbor links

2. 2-hop Neighborhood Discovery: collecting 2-hop bidirectional neighborhood information and any information relevant to relay set election

3. The collection and maintenance of the above information across multiple interfaces.

4. Relay Set Signaling: signal relay set selection to neighbor nodes if the relay set algorithm requires such information
The Appendices discuss a set of implemented SMF CDS approaches and the related TLV requirements that may be needed by an NHDP implementation to support each approach.
8. SMF Multicast Border Gateway Considerations

Typically, it is expected that SMF will be used to provide a more simplified forwarding of multicast traffic within a MANET mesh routing topology. However, a border router method should be used to allow interconnection of SMF operation with networks using other multicast routing protocols (e.g., PIM). It is important to note that there are many scenario specific issues that should be addressed when discussing border routers. At the present time, working deployments of SMF and PIM border router approaches are being experimented with.

In general, some of the functionality border routers may need to address include the following.

1. Determining which multicast groups should transit the border router whether entering or exiting the attached MANET routing region(s).

2. Enforcement of TTL threshold or other scoping policies.

3. Any marking or labeling to enable DPD on ingressing packets.

4. Interface with exterior multicast routing protocols.

5. Possible operation with multiple border routers (presently beyond scope of this document).


Note the behavior of border router nodes is the same as that of non-border routers when forwarding packets on interfaces within the MANET routing region. And packets that are passed outbound to interfaces operating more fixed Internet multicast routing protocols SHOULD be evaluated for duplicate packet status since present standard multicast forwarding mechanisms do not usually perform this function.

8.1. Forwarded Multicast Groups

Determining which groups should be forwarded into a MANET SMF routing region is an evolving technology area. Ideally, only groups for which there is active group membership should be injected into the SMF domain. This might be accomplished by providing an IPv4 Internet Group Membership Protocol (IGMP) or IPv6 Multicast Listener Discovery (MLD) proxy protocol so that MANET SMF nodes can inform attached border routers (and hence multicast networks) of their current group membership status. For specific systems and services it may be possible to statically configure group membership joins in border
border routers, but it is RECOMMENDED that some form of IGMP/MLD proxy or other explicit, dynamic control of membership be provided. Specification of such an IGMP/MLD proxy protocol is beyond the scope of this document.

Outbound traffic is less problematic. SMF border routers can perform duplicate packet detection and forward non-duplicate traffic that meets TTL/hop limit and scoping criteria to other interfaces. Appropriate IP multicast routing (PIM, etc) on those interfaces can then make further forwarding decisions with respect to the given traffic and its MANET source address. Note that the presence of multiple border routers associated with a MANET routing region may create some additional issues. This is further discussed in Section 8.5.

8.2. Multicast Group Scoping

Multicast scoping is used by network administrators to control the network routing regions which are reached by multicast packets. This is usually done by configuring external interfaces of border routers in the border of an routing region to not forward multicast packets which must be kept within the routing region. This is commonly done based on TTL of messages or the basis of group addresses. These schemes are known respectively as:

1. TTL scoping.
2. Administrative scoping.

For IPv4, network administrators can configure border routers with the appropriate TTL thresholds or administratively scoped multicast groups in the router’s interfaces as with any traditional multicast router. However, for the case of TTL scoping it must be taken into account that the packet could traverse multiple hops within the MANET SMF routing region before reaching the border router. Thus, TTL thresholds must be selected carefully.

For IPv6, multicast addresses themselves include information about the scope of the group. Thus, border routers of an SMF routing region know if they must forward a packet based on the IPv6 multicast group address. For the case of IPv6, we recommend a MANET SMF routing region be designated a site. Thus, all multicast packets in the range FF05::/16 will be kept within the MANET SMF routing region by border routers. Packets in any other wider range (i.e., FF08::/16, FF0B::/16 and FF0E::16) MAY traverse border routers unless other restrictions different from the scope applies.

Given that scoping of multicast packets is performed at the border
routers, and given that existing scoping mechanisms are not designed to work with mobile routers, we assume that non-border SMF routers, will not stop forwarding multicast data packets because of their scope. That is, we assume that the whole MANET SMF routing region is a non-divisible scoping area except in the case of link-local addresses that are not forwarded by SMF.

8.3. Duplicate Packet Detection Marking

Packets sourced external to an SMF routing region may not have duplicate packet sequencing properly applied, or hash ID collision may not have been previously checked, and the border router may need to provide that sequencing information or hash collision detection upon entry into the MANET routing region. In the case of IPv6, the border router can apply the SMF DPD Hop-by-Hop options header to packets forwarded into the MANET routing region for those packets that do not already have the option applied. If this option has been applied, this indicates the packet has already been marked for potential handling by SMF relays. Similarly, IP packets that have been encapsulated with IPsec may also be treated as appropriately marked for DPD and may be forwarded without modification. Both of these indicators (the IPv6 SMF DPD option and IPsec encapsulation) provide the side benefit for the border router to explicitly determine if the packet has already been marked. In this case, the border router can use the packet identification field to ensure it is not re-injecting a duplicate packet into the MANET routing region. For IPv4 packets that are not IPsec encapsulated, it is RECOMMENDED that border routers re-sequence the ID field of packets injected into the routing region. However, the IPv4 ID field does not provide the border router with explicit information on whether the field has been previously set for SMF purposes. Thus, the potential exists that duplicate IPv4 packets may be re-injected by a border router into an SMF routing region if a multicast routing loop has occurred. If multiple multicast border routers are envisioned, additional future considerations must be taken into account and solutions are considered out of scope for this document. See Section 8.5 for more discussion of related issues.

8.4. Interface with Exterior Multicast Routing Protocols

The traditional operation of multicast routing protocols is tightly integrated with the group membership function. Leaf routers are configured to periodically gather group membership information, while intermediate routers conspire to create multicast trees connecting routers with directly-connected multicast sources and routers with active multicast receivers. In the concrete case of SMF, we can consider border routers as leaf routers. Mechanisms for multicast sources and receivers to interoperate with border routers over the...
multihop MANET SMF routing region as if they were directly connected to the router need to be defined. The following issues need to be addressed:

1. Mechanism by which border routers gather membership information.
2. Mechanism by which multicast sources are known by the border router.
3. Exchange of exterior routing protocol messages across the MANET routing region if the MANET routing region is to provide transit connectivity for multicast traffic.

It is beyond the scope of this document to address implementation solutions to these issues. As described in Section 8.1, IGMP/MLD proxy mechanisms can be deployed to address some of these issues. Similarly, exterior routing protocol messages could be tunneled or conveyed across the MANET routing region. But, because MANET routing regions are multi-hop and potentially unreliable, as opposed to the single-hop LAN interconnection that neighboring IP Multicast routers might typically enjoy, additional provisions may be required to achieve successful operation.

The need for the border router to receive traffic from recognized multicast sources within the MANET SMF routing region is important to achieve a smooth interworking with existing routing protocols. For instance, PIM-S requires routers with locally attached multicast sources to register them to the Rendezvous Point (RP) so that other people can join the multicast tree. In addition, if those sources are not advertised to other autonomous systems (AS) using MSDP, receivers in those external networks are not able to join the multicast tree for that source.

8.5. Multiple Border Routers

A MANET might be deployed with multiple participating nodes having connectivity to external (to the MANET), fixed-infrastructure networks. Allowing multiple nodes to forward multicast traffic to/from the MANET routing region can be beneficial since it can increase reliability, and provide better service. For example, if the MANET routing region were to fragment with different MANET nodes maintaining connectivity to different border routers, multicast service could still continue successfully. But, the case of multiple border routers connecting a MANET routing region to external networks presents several challenges for SMF:
1. Detection/hash collision/sequencing of duplicate unmarked IPv4 or IPv6 (without IPSec encapsulation or DPD option) packets possibly injected by multiple border routers.

2. Source-based relay algorithms handling of duplicate traffic injected by multiple border routers.

3. Determination of which border router(s) will forward outbound multicast traffic.

4. Additional challenges with interfaces to exterior multicast routing protocols.

One of the most obvious issues is when multiple border routers are present and may be alternatively (due to route changes) or simultaneously injecting common traffic into the MANET routing region that has not been previously marked for SMF DPD. Different border routers would not be able to implicitly synchronize sequencing of injected traffic since they may not receive exactly the same messages due to packet losses. For IPv6 operation, the "Tagger ID" optional field described for the SMF-DPD header option can be used to mitigate this issue. When multiple border routers are injecting a flow into a MANET routing region, there are two forwarding policies that SMF DPD-S nodes may implement:

1. Redundantly forward the multicast flows (identified by <sourceAddress:destinationAddress>) from each border router, performing DPD processing on a <taggerID:destinationAddress> or <taggerID:sourceAddress:destinationAddress> basis, or

2. Use some basis to select the flow of one tagger (border router) over the others and forward packets for applicable flows (identified by <sourceAddress:destinationAddress>) only for that "Tagger ID" until timeout or some other criteria to favor another tagger occurs.

It is RECOMMENDED that the first approach be used in the case of DPD-S unless the SMF system is specifically designed to implement the second option. Additional specification may be required to describe an interoperable forwarding policy based on this second option. Note that the implementation of the second option requires that per-flow (i.e., <sourceAddress:destinationAddress>) state be maintained for the selected "Tagger ID".

The use of DPD-H may actually improve the case of duplicate packet detection when ingressing traffic comes from multiple border routers. Non-colliding hash indexes (those not requiring the DPD-H options header should be resolved effectively.
8.6. Non-SMF MANET Nodes

There may be scenarios in which some peer wireless MANET nodes may not wish to run the SMF protocol and/or conduct forwarding, but they are interested in receiving multicast data. For example, a MANET service might be deployed that is accessible to wireless edge devices that do not participate in MANET routing and/or SMF forwarding operation. These devices include:

1. Devices that opportunistically receive multicast traffic due to proximity with SMF relays (possibly with asymmetric IP connectivity e.g., sensor network device).

2. Devices that participate in NHDP (directly or via routing protocol signaling) but do not forward traffic.

Note there is no guarantee of traffic delivery with category 1 above, but the election heuristics shown in Figure 2 may be adjusted via management to better support such devices. It is RECOMMENDED that nodes participate in NHDP when possible. Such devices may also transmit multicast traffic, but it is important to note that SMF routing regions using source-specific relay set algorithms such as (S-MPR) may not forward such traffic. These devices SHOULD also listen for any IGMP/MLD Queries that are provided and transmit IGMP/MLD Reports for groups they have joined per usual IP Multicast operation. While it is not in the scope of this document, IGMP/MLD proxy mechanisms may be in place to convey group membership information to any border routers or intermediate systems providing IP Multicast routing functions.
9. Security Considerations

Gratuitous use of option headers can cause problems in routers. Routers outside of MANET routing regions should ignore SMF specific header options if encountered.

Authentication mechanisms to identify the source of an option header should be considered to reduce vulnerability to a variety of attacks.

A source may produce large quantities of multicast packets with the same header and content value to force the collision detection for every packet when operating in H-DPD. Well known packet types may be spoofed intentionally a priori to corrupt temporal cache histories and force collisions for key networking packets and in this case the authentication of packet sources should be strongly considered.

Additional security considerations TBD.
10. IANA Considerations

There are number of discussions within this SMF specification that will be subject to IANA registration. The IP Header Extensions being defined within this document MUST have an IANA registry established for them upon publication of the first RFC. Additionally, the well-known multicast addresses intended for default use by the SMF forwarding process should be registered and defined by the first RFC published.
11. Acknowledgments

Many of the concepts and mechanisms used and adopted by SMF resulted from many years of discussion and related work within the MANET WG since the late 1990s. There are obviously many contributors to past discussions and related draft documents within the WG that have influenced the development of SMF concepts that deserve acknowledgment. In particular, the document is largely a direct product of the SMF design team within the IETF MANET WG and borrows text and implementation ideas from the related individuals. Some of the contributors who have been involved in key document content editing, prototype implementation, and core discussions are listed below. We appreciate input from others we may have missed in this list as well.

SMF Core Design Team Contributors:

Brian Adamson
Ian Chakeres
Thomas Clausen
Justin Dean
Brian Haberman
Charles Perkins
Pedro Ruiz
Maoyu Wang

The RFC text was produced using Marshall Rose’s xml2rfc tool.
12. References

12.1. Normative References


12.2. Informative References


Appendix A. Source-based Multipoint Relay (S-MPR)

The source-based multipoint relay (S-MPR) set selection algorithm enables individual nodes, using two-hop topology information to select a minimum set of neighboring nodes that can provide relay to all nodes within a two-hop radius. This distributed technique has been shown to approximate selection of a MCDS in [JLMV02]. Individual nodes must collect two-hop neighborhood information from neighbors, determine an appropriate current relay set, and then inform the resultant selected neighbors of their relay status. The Optimized Link State Routing (OLSR) protocol has used this algorithm and protocol for relay of link state updates and other control information[RFC3626] and has been shown to operate well even in dynamic network environments.

Because a node’s status as a relay is with respect to neighboring nodes who have selected it (i.e., its "selectors"), the relaying node must know the previous-hop transmitter of packets it receives in order to make an appropriate forwarding decision. Additionally, it is important that relay nodes forward packets only for those nodes currently identified as symmetric, one-hop neighbors to maintain correctness. Also, because the selection of relays does not result in a common set among neighboring nodes, relays MUST mark in their duplicate table any transmissions from non-selector, symmetric, one-hop neighbors (for a given interface) and not forward subsequent received copies of that packet even if received from a selector neighbor. Deviation here may result in unnecessary, even excessive, repeat transmission of packets throughout the network. Or incorrect duplicate table recording of packets received from non-symmetric neighbors may result in incomplete flooding. In these respects, flooding based on the S-MPR algorithm is more complex than that based upon some other relay set selection algorithms.

When multiple interfaces are present, the S-MPR SMF forwarded must keep some independent state for each interface with regards to duplicate packets. For example, when a packet is received from a non-selector, one-hop symmetric neighbor, an SMF forwarder using the S-MPR algorithm must update its duplicate packet state with respect to the interface on which the packet was received. If the SMF forwarder receives that same packet from a selector neighbor on a different interface, it MUST still forward that packet on all interfaces it has not received that packet from a one-hop symmetric neighbor. Once a packet has been forwarded in this fashion, subsequent duplicates received on any interface are ignored.
A.1. S-MPR Relay Set Selection

If SMF is operating S-MPR relay set election independent of coexistent OLSR operation, based upon NHDP mechanisms, the election algorithm defined within RFC3626 [RFC3626] should be used.

A.2. Neighborhood Discovery Requirements

S-MPR election operation requires 2-hop neighbor knowledge as provided by the NHDP protocol [NHDP] or as available from external sources. MPRs are dynamically selected by each node and selections MUST be advertised and dynamically updated within the SMF NDP or equivalent protocol. In this mode, the MPR specific TLVs defined in OLSRv2 [OLSRv2] are also required to be implemented by NHDP.
Appendix B. Essential Connecting Dominating Set (E-CDS) Algorithm

The "Essential Connected Dominating Set" (E-CDS) algorithm [E-CDS] allows nodes to use two-hop topology information to appropriately elect themselves as relay nodes to form an efficient (for flooding) CDS. While this algorithm does not tend to produce as small a set of relay nodes (per forwarded packet) as the previously-described S-MPR algorithm, it is not dependent upon previous-hop information to make a forwarding decision; it simply forwards any received non-duplicate packets. This property also allows relay nodes using the E-CDS algorithm to be intermixed with nodes performing only classical flooding. Additionally, the semantics for multiple interface support are simplified as compared to S-MPR and even packets that are received from non-symmetric neighbors may be forwarded without compromising flooding efficiency or correctness.

B.1. E-CDS Relay Set Selection

This section provides a short description of the E-CDS based relay set selection algorithm and is based upon Richard Ogier’s original summary within [E-CDS]. This was originally discussed in the context of forming partial adjacencies and efficient flooding for MANET-OSPF work but its core algorithm is applied here.

E-CDS requires two-hop neighbor information collected through the SMF-NDP or other process. Each router has a Router Identifier (may be represented by an interface address) and Router Priority value. The Router Priority value may be dynamic and represent such metrics as node degree. The fundamental election steps are as follows:

1. If an SMF node has a higher (Router Priority, Router ID) than all of its symmetric neighbors, it elects itself to the relay set.

2. Else, if there does not exist a path from neighbor j with largest (Router Priority, Router ID) to some other neighbor, via neighbors with larger values of (Router Priority, Router ID), then it elects itself to the relay set.

The basic form of E-CDS described and applied within this specification does not at present define redundant relay set election but such capability is supported by the E-CDS design.

B.2. E-CDS Forwarding Rules

E-CDS forwarding is quite simple and straightforward. As mentioned, there is no need to check previous hop information during forwarding. Upon electing itself as an E-CDS relay set forwarder, SMF nodes perform DPD functions and forward all ranges of non-duplicative packets.
multicast traffic allowed by the present forwarding policy.

B.3. Neighborhood Discovery Requirements

To support functions required by the core E_CDS relay set algorithm, the following TLV is required to be transmitted by each node within a NHDP HELLO message:

*Router Priority*: type=SMF_ROUTER_PRIORITY, length=1, value = priority*

For E-CDS operation, some value of SMF_ROUTER_PRIORITY must be given or assumed for each address in the <address-block> portion of the SMF_HELLO message. If a SMF_HELLO message originator does not provide a SMF_ROUTER_PRIORITY value for given address(es), a default value SMF_RPRI_DEFAULT=(TBD) should be assumed. Local determination of a node SMF_ROUTER_PRIORITY value can be done in multiple ways as described in the [E-CDS]. An early implementation of SMF and E-CDS has used node degree computed during neighbor discovery, yet it is still unclear if this is the best method. Unlike the MPR method, the E-CDS is a self-electing algorithm. SMF_ROUTER_PRIORITY needs to be shared with all immediate neighbor nodes and 2-hop neighbor knowledge is needed during the self election process. Further algorithm examples and details are covered in the Appendices.
Appendix C. Multipoint Relay Connected Dominating Set (MPR-CDS) Algorithm

The MPR-CDS algorithm is an extension to the basic MPR election algorithm and results in a shared relay set that forms a CDS. Its forwarding rules within SMF are non-dependent upon previous hop information similar to E-CDS.

C.1. MPR-CDS Relay Set Selection

An overview of the MPR-CDS selection algorithm is provided in [MPR-CDS]. The basic requirements for election are similar to the basic MPR algorithm with the addition that some node ordering knowledge is required. This is similar to the E-CDS requirement and can be based upon node IP address or some other unique router identifier. The rules for election are as follows:

A node decides it is in the relay set if:

1. the node is smaller than all its neighbors (Rule 1)
2. or the node is an MPR of its smallest neighbor (Rule 2)

C.2. MPR-CDS Forwarding Rules

MPR-CDS forwarding are quite simple and straightforward. As with E-CDS, there is no need to check previous hop information during forwarding. Upon electing itself as a MPR-CDS relay set forwarder, SMF nodes perform DPD functions and forward all ranges of multicast traffic allowed.

C.3. Neighborhood Discovery Requirements

No additional discovery requirements are needed beyond the basic MPR-related TLVs already discussed.
Appendix D. Pseudo Code for Relay Set Selection Algorithms

D.1. Definitions

node : A MANET router which is implementing SMF Routing protocol.

\( n_0 \) : The node performing the SMF algorithm computation.

\( N_1 \) : A set of 1-hop neighbors of \( n_0 \). Initially set to all 1-hop neighbors.

\( N_2 \) : A set of 2-hop neighbors reachable by \( n_0 \), excluding \( n_0 \) and all nodes in \( N_1 \). Initially set to all 2-hop neighbors excluding \( n_0 \) and all nodes in \( N_1 \).

\( N_2(y) \) : The subset of \( N_2 \) nodes which are 1-hop neighbors of node \( y \), where node \( y \) is in \( N_1 \).

\( N_1(z) \) : The subset of \( N_1 \) nodes which are 1-hop neighbors of node \( z \), where \( z \) is in \( N_2 \).

RtrPri : an expression of router priority. For example, use \(|N_1|\) as \( n \)’s router’s priority then break ties with \( n_0 \)’s address.

\( rp_{\text{max}_1} \) : The node with the largest RtrPri of \( N_1 \).

MPRs : The subset of \( N_1 \) which have been selected by \( n_0 \) to forward packets from \( n_0 \).

MPR-Selectors : The subset of \( N_1 \) for whom \( n_0 \) has been selected to forward packets.

D.2. S-MPR Selection Algorithm

1. Calculate \( N_1(z) \) for all nodes \( z \) in \( N_2 \).
2. Calculate \( N_2(y) \) for all nodes \( y \) in \( N_1 \).
3. For each \( z \) in \( N_2 \) where \(|N_1(z)|\) is equal to 1, select the node in \( N_1(z) \) as an MPR by using Appendix D.2.1.
4. While \( N_2 \) is not empty select the node \( y \), with the largest \(|N_2(y)|\), as MPR by using Appendix D.2.1.
5. Restore \( N_1 \) and \( N_2 \).
6. Node \( n_0 \) shares its MPRs with \( N_1 \).
7. Each node in $n_0$’s MPRs set add $n_0$ to their MPR-Selectors set.

8. Nodes forward all unique multicast packets which are first received from a node in their MPR-Selectors set.

**D.2.1. Procedure to Select a Node as an MPR**

1. Add $n$ to the MPRs set.
2. Remove node $n$ from $N_1$.
3. For each $y$ in $N_2(n)$, remove $y$ from $N_2$.
4. Calculate $N_1(z)$ for all nodes $z$ in $N_2$.
5. Calculate $N_2(y)$ for all nodes $y$ in $N_1$.

**D.3. NS-MPR Selection Algorithm**

1. Perform steps 1-7 of Appendix D.2.
2. If $|MPR-Selectors| > 0$, then $n_0$ selects itself as a forwarder for all nodes.

**D.4. MPR-CDS Selection Algorithm**

1. Perform steps 1-7 of Appendix D.2.
2. If $n_0$ RtrPri value is greater than $rp_{max}_1$’s RtrPri value, and $|MPR-Selectors| > 0$, then $n_0$ selects itself as a forwarder for all nodes.
3. If $rp_{max}_1$ is in the MPR-Selectors set, then $n_0$ selects itself as a forwarder for all nodes.

**D.5. 1-Hop E-CDS Selection Algorithm**

1. If $n_0$ has a larger value of RtrPri than $pr_{max}_1$, then $n_0$ selects itself as a forwarder for all nodes.
2. If there does not exist a path from $pr_{max}_1$ to every other node in $N_1$ using only $N_1$ nodes that have RtrPri larger than $n_0$’s, then $n_0$ selects itself as a forwarder for all nodes.
D.6.  2-Hop E-CDS Selection Algorithm

1. If \( n_0 \) has a larger value of \( \text{RtrPri} \) than all nodes in \( N_1 \) and \( N_2 \), then \( n_0 \) selects itself as a forwarder for all nodes.

2. If there does not exist a path from \( r_{\text{max}}_1 \) to every other node in \( N_1 \) and \( N_2 \) using only \( N_1 \) and \( N_2 \) nodes that have \( \text{RtrPri} \) larger than \( n_0 \)'s, then \( n_0 \) selects itself as a forwarder for all nodes.
Authors’ Addresses

Joseph Macker
NRL
Washington, DC 20375
USA

Email: macker@itd.nrl.navy.mil

SMF Design Team
IETF MANET WG

Email: manet@ietf.org
Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).