

Open Shortest Path (OSPF)
Internet-Draft
Expires: April 14, 2008

E. Baccelli
P. Jacquet
D. Nguyen
INRIA
T. Clausen
LIX, Ecole Polytechnique, France
October 12, 2007

OSPF MPR Extension for Ad Hoc Networks
draft-baccelli-ospf-mpr-ext-04

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 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>.

This Internet-Draft will expire on April 14, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

This document specifies an OSPFv3 interface type tailored for mobile ad hoc networks. This interface type is derived from the broadcast interface type, enhanced with MANET techniques based on multi-point relaying (MPR).

Table of Contents

1.	Introduction	3
2.	Terminology	4
3.	Applicability Statement	6
4.	Protocol Overview and Functioning	7
4.1.	Efficient Flooding with MPR	7
4.2.	MPR Topology Reduction	7
4.3.	Multicast Transmissions of Protocol Packets	7
4.4.	MPR Adjacency Reduction	8
5.	Protocol Details	9
5.1.	Data Structures	9
5.2.	Hello Protocol	11
5.2.1.	Flooding MPR Selection	11
5.2.2.	Flooding MPR Selection Signalling in HELLO Packets	11
5.2.3.	Neighbor Ordering in HELLO Packets	11
5.2.4.	Metric Signalling in HELLO Packets	12
5.2.5.	Path MPR Selection	12
5.2.6.	Path MPR Selection Signalling in HELLO Packets	12
5.2.7.	Hello Packet Processing	12
5.3.	Adjacencies	13
5.3.1.	Protocol Packets over 2-WAY Links	13
5.3.2.	Adjacency Conservation	13
5.4.	Link State Advertisements	14
5.4.1.	LSA Flooding	14
5.4.2.	Link State Acknowledgments	15
6.	Security Considerations	17
7.	IANA Considerations	18
8.	References	21
8.1.	Normative References	21
8.2.	Informative References	21
Appendix A.	Flooding MPR Selection Heuristic	22
Appendix B.	Path MPR Selection Heuristic	24
	Contributors	26
	Authors' Addresses	27
	Intellectual Property and Copyright Statements	28

1. Introduction

This document specifies an extension of OSPFv3 [2] adapted to MANETs [6], based on mechanisms providing:

- Flooding reduction: a mechanism reducing the number of (re)transmissions during floods.
- Topology reduction: a mechanism reducing the number and the size of LSAs, by advertizing only a subset of the existing links.
- Adjacency reduction: a mechanism reducing the database synchronization overhead by bringing up only selected adjacencies.

These mechanisms are based on multipoint relaying (MPR), a technique developed in OLSR, the proactive routing solution standardized in MANET [5] [7].

The extension specified in this document integrates the OSPF framework by defining an OSPF interface type: the MANET interface. While this extension enables OSPF to function efficiently on mobile ad hoc networks, operation of OSPF on other types of interfaces or networks remains unaltered, whether there are MANET interfaces in the area or not.

2. Terminology

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 [RFC2119](#) [3].

Additionally, this document uses traditional OSPF terminology as defined in [1] [2], LLS terminology as defined in [4], as well as the following terms:

MANET interface - the OSPF interface type for MANETs, specified in this document.

MANET router - a router which has only MANET interface(s).

Wired router - a router which only has OSPF interface(s) of types other than MANET.

Hybrid router - a router which has OSPF interfaces of several types, including the MANET type.

Neighbor - a router, reachable through an OSPF interface (of any type).

MANET neighbor - a neighbor, reachable through an OSPF interface of type MANET.

Symmetric neighbor - a neighbor, in a state greater than or equal to 2-Way (through an interface of any type).

Symmetric 2-hop neighbor - a symmetric neighbor of a symmetric neighbor, which is not a neighbor of the considered router.

Neighborhood - the set formed by the symmetric neighbors of the considered router.

2-hop neighborhood - the set formed by all the symmetric 2-hop neighbors of the considered router.

Synch router - a router which brings up adjacencies with all its MANET neighbors.

Flooding MPR set - the subset of symmetric neighbors selected as flooding MPR by this router.

Flooding MPR selector set - the subset of symmetric neighbors that have selected this router as flooding MPR.

Path MPR set - the subset of symmetric neighbors selected as path MPR by this router.

Path MPR selector set - the subset of symmetric neighbors that have selected this router as path MPR.

MPR (selector) set - the union of the flooding MPR (selector) set and the path (selector) MPR set of this router.

3. Applicability Statement

Characteristics of MANETs include mobility and "half-broadcast" capabilities [9], i.e., a router that makes a transmission on a MANET can only assume that a subset of the routers attached to the MANET will hear this transmission. In particular, these characteristics are not compatible with several traditional OSPF mechanisms, including some reducing the amount of control traffic, such as flooding reduction, topology reduction and adjacency reduction (e.g. Designated Router). However, OSPF's efficient operation over MANETs relies on drastic control traffic reduction, as wireless links generally feature bandwidth scarcity and interference issues.

The MANET interface type enables OSPF operation on mobile ad hoc networks, by providing specific flooding reduction, topology reduction and adjacency reduction mechanisms adapted to MANET characteristics. These mechanisms are derived from solutions standardized by the MANET working group. However, while MANET standards address optimized ad hoc routing solutions for truly mobile environments, OSPF's extension for ad hoc networks addresses less mobile scenarios, that possibly include parts of the network that are fixed, using solely the traditional OSPF framework.

4. Protocol Overview and Functioning

This document specifies an OSPFv3 interface type tailored for mobile ad hoc networks: the MANET interface.

The MANET interface makes use of flooding reduction, topology reduction and adjacency reduction mechanisms based on multipoint relaying (MPR), a technique derived from OLSR [5] [7], the proactive routing solution standardized in MANET.

4.1. Efficient Flooding with MPR

MANET interfaces use a flooding reduction mechanism called MPR flooding, whereby only some MANET neighbors (those selected as flooding-MPR) are responsible for retransmitting a routing packet flooded over a MANET interface. This mechanism drastically reduces the number of (re)transmissions during flooding procedures, while still providing a natural high resilience to transmission errors (inherent to the use of wireless links), and obsolete two-hop neighbor information (frequently caused by the mobility of the routers).

4.2. MPR Topology Reduction

MANET interfaces use a topology reduction mechanisms called MPR topology reduction, whereby only necessary wireless links to MANET neighbors (those concerned by path-MPR selection, as belonging to shortest paths) are listed in LSAs. MANET routers periodically generate and flood Router-LSAs describing their selection of wireless links to (current) MANET neighbors as point-to-point links. This mechanism greatly reduces the size of LSAs originated by MANET routers, while still keeping OSPF's traditional properties: optimal paths using synchronized adjacencies.

4.3. Multicast Transmissions of Protocol Packets

In order to reduce the overhead, multicast is used as much as possible for protocol packet transmissions over MANET interfaces, taking advantage of broadcast capabilities of the wireless medium [9]. In particular, LSA acknowledgements are sent via multicast over these interfaces, and retransmissions over the same interfaces are considered as implicit acknowledgements. Intelligent jitter management delaying packets' (re)transmissions may also be used to increase the chance to bundle several packets in a single transmission, or to avoid superfluous retransmissions due to packet collisions (see [10]).

4.4. MPR Adjacency Reduction

Furthermore, MANET routers may form adjacencies with a subset of their MANET neighbors (instead of all of them). However, no Designated Router or Backup Designated Router is elected on an OSPF MANET. Instead, most MANET routers bring up adjacencies only with their MPR and MPR selectors, while some select MANET routers (called Synch routers) must bring up adjacencies with all their MANET neighbors. This reduces the amount of control traffic needed for database synchronization, while ensuring that LSAs still describe synchronized adjacencies only.

5. Protocol Details

This section specifies the information that must be maintained, processed and transmitted by MANET and hybrid routers, and complements [RFC 2740](#) [2].

5.1. Data Structures

In addition to the values used in [RFC 2740](#) [2], the type field in the interface data structure can take a new value, "MANET". Furthermore, in addition to the protocol structures defined by [RFC 2740](#) [2], MANET and hybrid routers make use of the data structures described below.

N :

the router IDs of the set of symmetric neighbors of the router. More precisely, N lists tuples of the form (1_HOP_SYM_id, 1_HOP_SYM_time). 1_HOP_SYM_id is the router ID of the symmetric neighbor. 1_HOP_SYM_time specifies the time, at which the tuple expires and MUST be removed from the set.

N2 :

the router IDs of the set of symmetric neighbors of routers that are in N, excluding:

- (i) the router performing the computation
- (ii) all routers in N.

More precisely, N2 lists tuples of the form (2_HOP_SYM_id, 1_HOP_SYM_id, 2_HOP_SYM_time). 2_HOP_SYM_id is the router ID of a symmetric 2-hops neighbor. 1_HOP_SYM_id is the router ID of the symmetric neighbor through which the 2-hop neighbor can be reached. 2_HOP_SYM_time specifies the time, at which the tuple expires and MUST be removed from the set.

Flooding-MPR set:

the router IDs of a subset of the routers listed in N, selected such that through this subset, each router listed in N2 is reachable. These neighbors are said to have been "selected as

flooding MPR" by the router. More precisely, the Flooding-MPR set lists tuples of the form (Flooding_MPR_id, Flooding_MPR_time). Flooding_MPR_id is the router ID of the symmetric neighbor selected as flooding MPR. Flooding_MPR_time specifies the time, at which the tuple expires and MUST be removed from the set. For details about MPR selection, see [Section 5.2](#).

Flooding-MPR-selector set:

the router IDs of the set of neighbors that have selected the router as flooding MPR. More precisely, the Flooding-MPR-selector set lists tuples of the form (Flooding_MPR_SELECTOR_id, Flooding_MPR_SELECTOR_time). Flooding_MPR_SELECTOR_id is the router ID of the symmetric neighbor that has selected the router as flooding MPR. Flooding_MPR_SELECTOR_time specifies the time at which the tuple expires and MUST be removed from the set. For details about Flooding MPR selection, see [Section 5.2](#).

Path-MPR set:

the router IDs of a subset of the routers listed in N that provide shortest paths from the members of N2 to the router. These neighbors are said to have been "selected as path MPR" by the router. More precisely, the Path-MPR set lists tuples of the form (Path_MPR_id, Path_MPR_time). Path_MPR_id is the router ID of the symmetric neighbor selected as path MPR. Path_MPR_time specifies the time at which the tuple expires and MUST be removed from the set. For details about path MPR selection, see [Section 5.2](#).

Path-MPR-selector set :

the router IDs of the set of neighbors that have selected the router as path MPR. More precisely, the Path-MPR-selector set lists tuples of the form (Path_MPR_SELECTOR_id, Path_MPR_SELECTOR_time). Path_MPR_SELECTOR_id is the router ID of the symmetric neighbor that has selected the router as path MPR. Path_MPR_SELECTOR_time specifies the time at which the tuple expires and MUST be removed from the set. For details about path MPR selection, see [Section 5.2](#).

5.2. Hello Protocol

On MANET interfaces, packets are sent, received and processed as defined by [RFC 2740](#) [2] and [RFC 2328](#) [1], with the following additions for MPR selection as described in this section.

5.2.1. Flooding MPR Selection

The objective of flooding MPR selection is for a router to select a subset of its neighbors such that a packet, retransmitted by these selected neighbors, will be received by all routers 2 hops away. This property is called the flooding MPR "coverage criterion". The flooding MPR set of a router is computed such that, for each interface, it satisfies this criterion. The information required to perform this calculation (i.e. link sensing and neighborhood information) is acquired through periodic exchange of OSPF HELLO packets.

Flooding MPRs are computed by each MANET or hybrid router. The smaller the flooding MPR set is, the lower the overhead will be. However, while it is not essential that the flooding MPR set is minimal, it is essential that all 2-hop neighbors can be reached through the selected flooding MPR routers. A router **MUST** select a flooding MPR set such that any 2-hop neighbor is covered by at least one flooding MPR router.

Flooding MPR selection priority may be given to neighbor routers in descending order of their willingness to flood traffic on behalf of other routers. [Appendix A](#) gives a heuristic for flooding MPR selection.

5.2.2. Flooding MPR Selection Signalling in HELLO Packets

A router that has selected flooding MPRs among its neighbors **MUST** signal this selection through appending LLS information (TLV type 3) at the end of its HELLO packets as described in [Section 7](#). This information signals the list of neighbors the router has selected as flooding MPR, and the willingness of the router to be flooding traffic on behalf of other routers.

5.2.3. Neighbor Ordering in HELLO Packets

Neighbors listed in the HELLO packets sent over MANET interfaces **MUST** be listed such that symmetric neighbors are listed before other neighbors. Moreover, neighbors selected as flooding MPR **MUST** be listed before other symmetric neighbors. This specific ordering corresponds with LLS information (TLV type 3) appended to the HELLO packet, as described in [Section 7](#).

5.2.4. Metric Signalling in HELLO Packets

HELLO packets sent over MANET interfaces MUST advertize the costs of links towards ALL its symmetric MANET neighbors. If the router has several MANET interfaces, links to ALL the symmetric MANET neighbors over ALL the MANET interfaces of the router MUST have their costs listed. The costs of the links from the router to its neighbors as well as from the neighbors to the router (the reverse costs) are specified using the LLS format (TLV type 4) described in [Section 7](#), appended at the end of Hello packets.

5.2.5. Path MPR Selection

Using the LLS metric information included in HELLO packets, a MANET router MUST identify a subset of its links to neighbors that are on shortest paths with respect to the metric in use. This mechanism is called Path MPR selection. [Appendix B](#) gives a heuristic for path MPR selection.

Hybrid routers MUST select ALL their MANET and hybrid neighbors as path MPRs. MANET routers MAY select a subset of MANET neighbors as path MPR. However a MANET router MUST ensure that for each element of N or N2 that is not in the path MPR set, there exists a shortest path that goes from this element to the router through a neighbor selected as path MPR (unless the shortest path is only one hop, of course).

5.2.6. Path MPR Selection Signalling in HELLO Packets

A router that has selected path MPRs among its neighbors MUST signal this selection through appended LLS information (TLV type 4) at the end of its HELLO packets as described in [Section 7](#). This information signals the list of neighbors the router has selected as path MPR. Neighbors listed in the TLV type 4 MUST be listed such that adjacent neighbors are listed before other neighbors. Moreover, neighbors selected as path MPR MUST be listed before other adjacent neighbors.

5.2.7. Hello Packet Processing

In addition to the processing specified by [RFC 2740](#) [2], N and N2 MUST be updated when received HELLO packets signal changes in the neighborhood of a MANET interface. The flooding MPR set and the path MPR set MUST then be recomputed if N or N2 have changed.

Moreover, the flooding MPR selector set and the path MPR selector set MUST be updated upon receipt of a HELLO packet containing LLS information signalling change in the list of neighbors that has selected the router as MPR.

5.3. Adjacencies

When adjacencies are brought up between MANET and hybrid neighbors, procedure goes on as defined in [RFC 2740](#) [2] and [RFC 2328](#) [1].

However, in order to further reduce the control traffic overhead on the wireless medium, MANET routers MAY bring up adjacencies with a subset of their MANET or hybrid neighbors.

Over a MANET interface, a router MUST bring up adjacencies with the neighbors it has included in its MPR set and its MPR Selector set.

Some routers (called synch routers) MUST bring up adjacencies with other MANET neighbors as well. Other routers MAY bring up adjacencies with MANET neighbors other than MPRs and MPR selectors, at the expense of more synchronisation overhead. The proposed heuristic for routers to decide whether they are a synch router is as follows:

- o a MANET router decides it is a synch router if and only if the router has a higher ID than any other ID present in Hello packets or Router-LSAs it has received from other reachable routers in the area.

Other algorithms are possible. However, algorithms MUST ensure that if there are no hybrid routers in the MANET, at least one router in the MANET selects itself as synch router. Moreover, a MANET router that selects itself as synch router MUST signal this by setting the S bit in the TLV type 4 appended to the Hello packets it generates, as described in [Section 7](#).

5.3.1. Protocol Packets over 2-WAY Links

When a router does not form a FULL adjacency with a MANET neighbor, the state does not progress beyond 2-WAY (as defined in [RFC 2740](#) [2] and [RFC 2328](#) [1]). A MANET interface MAY send routing protocol packets while in 2-WAY state.

Therefore, any routing protocol packet received from a symmetric MANET neighbor MUST be processed. Similar to the OSPF broadcast interface [1], the next hop in the forwarding table MAY be a neighbor that is not adjacent. However, when a data packet has travelled beyond its first hop, the MPR selection process guarantees that subsequent hops in the SPT will be over adjacencies.

5.3.2. Adjacency Conservation

Adjacencies are torn down as defined in [RFC 2740](#) [2] and [RFC 2328](#) [1]. This means that when the MPR set or MPR selector set is updated

(due to changes in the neighborhood), and when a neighbor was formerly, but is no longer, in the MPR set or the MPR selector set, the adjacency with this neighbor is kept, unless it is no longer a symmetric neighbor.

When a router receives Hello packets from a symmetric neighbor which cease to list the router as being adjacent (see [Section 5.2.3](#)), the state of this neighbor MUST be changed to (i) 2-WAY if the neighbor is not in the MPR set or the MPR selector set, or (ii) ExStart if the neighbor is in the MPR set or the MPR selector set, or if the neighbor or the router itself is a synch router.

5.4. Link State Advertisements

The Router-LSAs originated by a hybrid router list adjacencies over interfaces other than MANET as specified in [RFC 2740](#) [2] and [RFC 2328](#) [1]. Hybrid and MANET routers MUST list in the Router-LSAs they originate the links to the neighbors that are in their Path MPR set and their Path MPR Selector set. MANET routers MAY list other links they have through MANET interfaces, to the expense of more overhead.

Hybrid and MANET routers MUST flood updated Router-LSAs when a new adjacency has been brought up reflecting change in the MPR set (or the MPR Selector set), and when a neighbor formerly listed in originated LSAs is no longer adjacent.

5.4.1. LSA Flooding

LSUpdates received on an interface of a type other than MANET are processed and flooded as specified in [1] and [2], over every interface. If an LSUpdate was received on a MANET interface, it is processed as follows, with regards to flooded LSAs.

1. Consistency checks are made on the received packet, as specified in [1] and [2], before being handed to the procedure described in the following steps, and the Link State Update packet is thus associated with a particular neighbor and a particular area.
2. If the LSU was received from a router other than a symmetric neighbor, the LSUpdate MUST be discarded without further processing. Otherwise, for each LSA contained in LSUpdates received on MANET interfaces, the following steps replace steps 1 to 5 of section 13.3 of [1].
 1. If there exists an LSA in the Link State Database, with the same Link State ID, LS Type and Advertizing Router values as the received LSA, and the received LSA is not newer (see section 13.1 of [1]) then the received LSA MUST not be

processed EXCEPT for acknowledgement as described in [section 5.4](#).

2. Otherwise, the LSA MUST be attributed a scope according to its type, as specified in section 3.5 of [2].
3. If the scope of the LSA is link local or reserved, the LSA MUST not be flooded on any interface.
4. Otherwise:
 - If the scope of the LSA is the area, the LSA MUST be flooded on all the interfaces of the router in that area according to the default flooding algorithm described below.
 - Otherwise, the LSA MUST be flooded on all the interfaces of the router according to the default flooding algorithm described below.

The default flooding algorithm is then the following:

1. The LSA MUST be installed in the Link State Database.
2. The Age of the LSA is increased by InfTransDelay.
3. The LSA is flooded over all interfaces of type other than MANET.
4. If the sender interface address is an interface address of an flooding MPR selector of this router, the LSA MUST also be retransmitted out all MANET interfaces concerned by the scope, with the multicast address all_SPF_Routers.

Note that MinLSArrival SHOULD be set to a value that is appropriate to MANET dynamic topologies: LSA updating may need to be more frequent in MANET parts of the OSPF network than in traditional parts of the OSPF network.

[5.4.2](#). Link State Acknowledgments

When a router receives an LSA on a MANET interface, the router MUST proceed to acknowledge the LSA as follows

1. If the LSA was not received from an adjacent neighbor, the router MUST NOT acknowledge it.
2. Otherwise, if the LSA was received from an adjacent neighbor if the LSA is already in the database (i.e. the LSA has already been received and processed) the router MUST send an acknowledgement

for this LSA on all MANET interfaces, to the multicast address all_SPF_Routers.

3. Otherwise, if the LSA is not already in the database:
 1. If the router decides to retransmit the LSA (as part of the flooding procedure), the router MUST NOT acknowledge it, as this retransmission will be considered as an implicit acknowledgement.
 2. Otherwise, if the router decides to not retransmit the LSA (as part of the flooding procedure), the router MUST send an acknowledgement for this LSA on all MANET interfaces, to the multicast address all_SPF_Routers.

If a router sends an LSA on a MANET interface, it expects acknowledgements (explicit or implicit) from each adjacent neighbors. In the case where the router did not originate the LSA (i.e. relays the LSA), the router MUST only expect acknowledgements (explicit or implicit) from adjacent neighbors that have not previously acknowledged this LSA. If a router detects that some adjacent neighbor has not acknowledged the LSA, the router retransmits the LSA.

If, due to efficient flooding procedure decision, a router decides to not relay an LSA, the router MUST still expect acknowledgements of that LSA (explicit or implicit) from adjacent neighbors that have not previously acknowledged this LSA. If a router detects that some adjacent neighbor has not acknowledged the LSA, the router retransmits the LSA.

Note that it may be beneficial to aggregate several acknowledgements in the same transmission, taking advantage of multicasting. A timer wait MAY thus be used before any acknowledgement transmission in order to avoid multiple OSPF acknowledgement transmissions.

Additional jitter delay in packet (re)transmission may be used in order to increase the opportunities to bundle several packets together per transmission (which provides a reduction in the number of overall transmissions, and therefore the number of collisions over the wireless media).

6. Security Considerations

This document does currently not specify security considerations.

7. IANA Considerations

This document defines the new TLV types below, to be allocated by IANA.

OSPF packets sent by MANET and hybrid routers are formatted as defined by [RFC2740](#) [2] and [RFC2328](#) [1]. The LLS extension [4] is used in HELLO packets sent over MANET interfaces, as follows.

The Hello packets sent over an OSPF MANET interface have the L bit set. An LLS datablock containing flooding MPR selection information is appended to these Hello messages. The TLV of Type 3 is defined as the flooding MPR selection TLV type shown in Fig. 1.

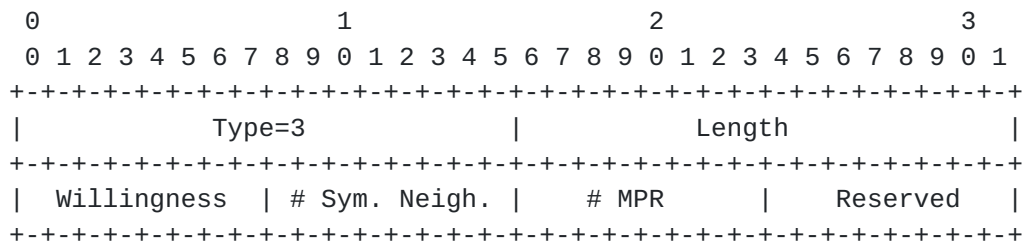


Fig. 1 : Flooding MPR selection (TLV type 0)

Willingness

This field specifies the willingness of the router to flood link state information on behalf of other routers. It can be set to any integer value from 1 to 6. By default, a router SHOULD advertise a willingness of WILL_DEFAULT = 3.

Sym. Neigh.

Number of symmetric neighbors, listed first among the neighbors in a HELLO packet.

MPR

Number of neighbors, listed first among the symmetric neighbors on this interface in a HELLO packet, that are selected by the router as flooding MPR.

Reserved

This field is 16 bits long and must be set to 0 to be in compliance with this specification.

Neighbor ID

This field specifies the router ID of a MANET neighbor.

Cost

This field specifies the cost of the link going from the router towards the neighbor indicated in the neighbor ID field. If a neighbor is reachable through several interfaces at the same time, the advertized cost is set to the minimum of the costs over these different interfaces.

Reverse Cost

This field specifies the cost of the link going from the neighbor indicated in the neighbor ID field towards the router. By default it is set to 0xFFFF (maximal value, i.e. infinity), unless information received via HELLO packets from the neighbor specifies otherwise. If a neighbor is reachable through several interfaces at the same time, the advertized cost is set to the minimum of the costs over these different interfaces.

8. References

8.1. Normative References

- [1] Moy, J., "OSPF version 2", [RFC 2328](#), 1998.
- [2] Moy, J., Coltun, R., and D. Ferguson, "OSPF for IPv6", [RFC 2740](#), 1999.
- [3] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [RFC 2119](#), 1997.
- [4] Zinin, A., Friedman, B., Roy, A., Nguyen, L., and D. Yeung, "OSPF Link Local Signaling", [draft-nguyen-ospf-lls-04](#) (work in progress), 2004.

8.2. Informative References

- [5] Clausen, T. and P. Jacquet, "The Optimized Link State Routing Protocol", [RFC 3626](#), October 2003.
- [6] Macker, J. and S. Corson, "MANET Routing Protocol Performance Issues and Evaluation Considerations", [RFC 2501](#), January 1999.
- [7] OLSRV2, Design Team., "OLSR version 2", [draft-ietf-manet-olsrv2-02](#) (work in progress), June 2006.
- [8] Ngyuen, D. and P. Minet, "Analysis of MPR Selection in the OLSR Protocol", 2nd Int. Workshop on Performance Analysis and Enhancement of Wireless Networks , 2007.
- [9] Macker, J., Chakeres, I., and T. Clausen, "Mobile Ad hoc Network Architecture", ID [draft-ietf-autoconf-manetarch](#), February 2007.
- [10] Adamson, B., Dearlove, C., and T. Clausen, "Jitter Considerations in MANETs", ID [draft-ietf-manet-jitter](#), June 2007.

[Appendix A.](#) Flooding MPR Selection Heuristic

The following specifies a proposed heuristic for selection of flooding MPRs. It constructs a flooding MPR set that enables a router to reach routers in the 2-hop neighborhood through relaying by one flooding MPR router.

The following terminology will be used in describing the heuristics: $D(y)$ is the degree of a 1-hop neighbor router y (where y is a member of N), defined as the number of neighbors of router y , EXCLUDING all the members of N and EXCLUDING the router performing the computation. The proposed heuristic can then be described as follows. Begin with an empty flooding MPR set. Then:

1. Calculate $D(y)$, where y is a member of N , for all routers in N .
2. Add to the flooding MPR set those routers in N , which are the only routers to provide reachability to a router in N_2 . For example, if router b in N_2 can be reached only through a router a in N , then add router a to the flooding MPR set. Remove the routers from N_2 which are now covered by a router in the flooding MPR set.
3. While there exist routers in N_2 which are not covered by at least one router in the flooding MPR set:
 1. For each router in N , calculate the reachability, i.e. the number of routers in N_2 which are not yet covered by at least one router in the flooding MPR set, and which are through this 1-hop neighbor;
 2. Select as a flooding MPR the neighbor with highest willingness among the routers in N with non-zero reachability. In case of a tie among routers with same willingness the router which provides reachability to the maximum number of routers in N_2 . In case of another tie between routers also providing the same amount of reachability, select as flooding MPR the router whose $D(y)$ is greater. Remove the routers from N_2 which are now covered by a router in the flooding MPR set.
4. As an optimization, process each router, y , in the flooding MPR set in increasing order of willingness. If all routers in N_2 are still covered by at least one router in the flooding MPR set excluding router y , then router y MAY be removed from the flooding MPR set.

Other algorithms, as well as improvements over this algorithm, are

possible. Different routers may use different algorithms independently. The only requirement is that the algorithm used by a given router MUST provide the router with an MPR set that fulfills the MPR flooding coverage criterion, i.e. it MUST select a flooding MPR set such that any 2-hop neighbor is covered by at least one flooding MPR router.

[Appendix B](#). Path MPR Selection Heuristic

The following specifies a proposed heuristic for selection of path MPRs. It constructs a path MPR-set that enables a router to reach routers in the 2-hop neighborhood through shortest paths via routers in its path MPR-set. The following terminology will be used:

- The router where the computation is done will be called A.
- For a router B neighbor of A, $\text{cost}(A,B)$ is the cost of the path through the direct link, from A to B, and this is an entry in the router cost matrix defined below.
- For a router C in the neighborhood or 2-hop neighborhood of A, $\text{dist}(C,A)$ is the cost of the shortest path from C to A and this is an entry in the router distance vector defined below.

The cost matrix is populated with the values of the costs of links originating from router A (available locally) and by values listed in Hello packets received from neighbor routers. More precisely, the cost matrix is populated as follows:

1. The coefficients of the cost matrix are set by default to 0xFFFF (maximal value, i.e. infinity).
2. The coefficient $\text{cost}(A,B)$ of the cost matrix for a link from router A to a neighbor B (the direct cost for this link) is set to the minimum cost over all interfaces that feature router B as a symmetric neighbor. The reverse cost for this link, $\text{cost}(B,A)$, is set at the value received in Hello packets from router B. If router B is reachable through several interfaces at the same time, $\text{cost}(B,A)$ is set as the minimum cost advertised by router B for its links towards router A.
3. The coefficients of the cost matrix concerning the link between two neighbors of A, routers C and B, are populated at the reception of their Hello packets. The cost (B,C) is set to the value advertised by the Hello packets from B, and respectively, the cost (C,B) is set to the value advertised in Hello packets from C.
4. The coefficients of the cost matrix, $\text{cost}(B,C)$ for a link that connects a neighbor B to a 2-hop neighbor C is obtained via the Hello packets received from router B. In this case $\text{cost}(B,C)$ and $\text{cost}(C,B)$ are respectively set to the values advertised by router B for the direct cost and reverse cost for node C.

Once the cost matrix is populated, the proposed heuristic can then be

described as follows. Begin with an empty path MPR set. Then:

1. Using the cost matrix and the Dijkstra algorithm, compute the router distance vector, i.e. the shortest distance for each pair (X,A) where X is in N or $N2$ minimizing the sum of the cost of the path between X and A .
2. Compute N' as the subset of N made of the elements X such that $\text{cost}(X,A)=\text{dist}(X,A)$.
3. Compute $N2'$ as the subset of N and $N2$ made of the elements Y that do not belong to N' and such that there exist X in N' such $\text{cost}(Y,X)+\text{cost}(X,A)=\text{dist}(Y,A)$.
4. Compute the MPR selection algorithm presented in [Appendix A](#) with N' instead of N and $N2'$ instead of $N2$. The resulting MPR set is the path MPR set.

Other algorithms, as well as improvements over this algorithm, are possible. Different routers may use different algorithms independently. However, a MANET router MUST ensure that for each element of N or $N2$ that is not in the path MPR set, there exists a shortest path that goes from this element to the router through a neighbor selected as path MPR (unless the shortest path is only one hop).

Contributors

The authors thank Cedric Adjih, Acee Lindem, Padma Pillay-Esnault and Laurent Viennot for their contributions to this document.

Authors' Addresses

Emmanuel Baccelli
INRIA

Phone: +33 1 69 33 55 11
Email: Emmanuel.Baccelli@inria.fr

Philippe Jacquet
INRIA

Phone: +33 1 3963 5263
Email: Philippe.Jacquet@inria.fr

Dang-Quan Nguyen
INRIA

Phone: +33 1 3963 5511
Email: Dang-Quan.Nguyen@inria.fr

Thomas Heide Clausen
LIX, Ecole Polytechnique, France

Phone: +33 6 6058 9349
Email: T.Clausen@computer.org
URI: <http://www.lix.polytechnique.fr/Labo/Thomas.Clausen/>

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).

