

Internet Engineering Task Force (IETF)
Request for Comments: 8218
Category: Experimental
ISSN: 2070-1721

J. Yi
Ecole Polytechnique
B. Parrein
University of Nantes
August 2017

Multipath Extension for the Optimized Link State Routing Protocol Version 2 (OLSRv2)

Abstract

This document specifies a multipath extension for the Optimized Link State Routing Protocol version 2 (OLSRv2) to discover multiple disjoint paths for Mobile Ad Hoc Networks (MANETs). Considering the characteristics of MANETs, especially the dynamic network topology, using multiple paths can increase aggregated throughput and improve the reliability by avoiding single route failures. The interoperability with OLSRv2 is retained.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for examination, experimental implementation, and evaluation.

This document defines an Experimental Protocol for the Internet community. This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at <http://www.rfc-editor.org/info/rfc8218>.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	4
1.1. Motivation and Experiments to Be Conducted	4
2. Terminology	7
3. Applicability Statement	7
4. Protocol Overview and Functioning	8
5. Parameters and Constants	9
5.1. Router Parameters	9
6. Packets and Messages	10
6.1. HELLO and TC messages	10
6.1.1. SOURCE_ROUTE TLV	10
6.2. Datagram	11
6.2.1. Source Routing Header in IPv4	11
6.2.2. Source Routing Header in IPv6	11
7. Information Bases	11
7.1. SR-OLSRv2 Router Set	11
7.2. Multipath Routing Set	12
8. Protocol Details	12
8.1. HELLO and TC Message Generation	12
8.2. HELLO and TC Message Processing	13
8.3. MPR Selection	13
8.4. Datagram Processing at the MP-OLSRv2 Originator	14
8.5. Multipath Calculation	15
8.5.1. Requirements of Multipath Calculation	15
8.5.2. Multipath Dijkstra Algorithm	16
8.6. Multipath Routing Set Updates	18
8.7. Datagram Forwarding	18
9. Configuration Parameters	18
10. Security Considerations	19
11. IANA Considerations	20
11.1. Message TLV Types	20
12. References	21
12.1. Normative References	21
12.2. Informative References	22
Appendix A. Examples of Multipath Dijkstra Algorithm	24
Acknowledgments	25
Authors' Addresses	26

1. Introduction

The Optimized Link State Routing Protocol version 2 (OLSRv2) [RFC7181] is a proactive link state protocol designed for use in Mobile Ad Hoc Networks (MANETs). It generates routing messages periodically to create and maintain a Routing Set, which contains routing information to all the possible destinations in the routing domain. For each destination, there exists a unique Routing Tuple, which indicates the next hop to reach the destination.

This document specifies an extension of the OLSRv2 protocol [RFC7181] to provide multiple disjoint paths when appropriate for a source-destination pair. Because of the characteristics of MANETs [RFC2501], especially the dynamic topology, having multiple paths is helpful for increasing network throughput, improving forwarding reliability, and load-balancing.

Multipath OLSRv2 (MP-OLSRv2), specified in this document, uses the Multipath Dijkstra Algorithm by default to explore multiple disjoint paths from a source router to a destination router based on the topology information obtained through OLSRv2 and to forward the datagrams in a load-balancing manner using source routing. MP-OLSRv2 is designed to be interoperable with OLSRv2.

1.1. Motivation and Experiments to Be Conducted

This document is an experimental extension of OLSRv2 that can increase the data forwarding reliability in dynamic and high-load MANET scenarios by transmitting datagrams over multiple disjoint paths using source routing. This mechanism is used because:

- o Disjoint paths can avoid single route failures.
- o Transmitting datagrams through parallel paths can increase aggregated throughput.
- o Some scenarios may require that some routers must (or must not) be used.
- o Having control of the paths at the source benefits the load-balancing and traffic engineering.
- o An application of this extension is in combination with Forward Error Correction (FEC) coding applied across packets (erasure coding) [WPMC11]. Because the packet drops are normally bursty in a path (for example, due to route failure), erasure coding is less

effective in single path routing protocols. By providing multiple disjoint paths, the application of erasure coding with multipath protocol is more resilient to routing failures.

In existing deployments, while running code and simulations have proven the interest of multipath extension for OLSRv2 in certain networks [GIIS14][WCNC08][ADHOC11], more experiments and experiences are still needed to understand the effects of the protocol specified in this Experimental RFC. The multipath extension for OLSRv2 is expected to be revised and documented as a Standards Track RFC once sufficient operational experience is obtained. Other than general experiences, including the protocol specification and interoperability with base OLSRv2 implementations, experiences in the following aspects are highly appreciated:

- o Optimal values for the number of multiple paths (NUMBER_OF_PATHS, see Section 5) to be used. This depends on the network topology and router density.
- o Optimal values used in the metric functions. Metric functions are applied to increase the metric of used links and nodes so as to obtain disjoint paths. What kind of disjointness is desired (node disjoint or link disjoint) may depend on the Layer 2 protocol used and can be achieved by applying different sets of metric functions.
- o Use of different metric types. This multipath extension can be used with metric types that meet the requirement of OLSRv2, such as [RFC7779]. The metric type used also has an impact on the choice of metric functions as indicated in the previous bullet point.
- o The impact of partial topology information to multipath calculation. OLSRv2 maintains a partial topology information base to reduce protocol overhead. Experience has shown that multiple paths can be obtained even with such partial information; however, depending on the Multipoint Relay (MPR) selection algorithm used, the disjointness of the multiple paths might be impacted depending on the Multipoint Relay (MPR) selection algorithm used.
- o Use of IPv6 loose source routing. In the current specification, only strict source routing is used for IPv6 based on [RFC6554]. In [IPv6-SRH], the use of the loose source routing is also proposed in IPv6. In scenarios where the length of the source routing header is critical, the loose source routing can be considered.

- o Optimal choice of "key" routers for loose source routing. In some cases, loose source routing is used to reduce overhead or for interoperability with OLSRv2 routers. Other than the basic rules defined in the following parts of this document, optimal choices of routers to put in the loose source routing header can be further studied.
- o Different path-selection schedulers. Depending on the application type and transport layer type, either a per-flow scheduler or per-datagram scheduler is applied. By default, the traffic load should be equally distributed in multiple paths. In some scenarios, weighted scheduling can be considered: for example, the paths with lower metrics (i.e., higher quality) can transfer more datagrams or flows compared to paths with higher metrics.
- o The impacts of the delay variation due to multipath routing. [RFC2991] brings out some concerns of multipath routing, especially variable latencies when per-datagram scheduling is applied. Although current experiment results show that multipath routing can reduce the jitter in dynamic scenarios, some transport protocols or applications may be sensitive to the datagram reordering.
- o The disjoint multipath protocol has an interesting application with erasure coding, especially for services like video/audio streaming [WPMC11]. The combination of erasure coding mechanisms and this extension is thus encouraged.
- o Different algorithms to obtain multiple paths, other than the default Multipath Dijkstra Algorithm introduced in Section 8.5.2 of this specification.
- o The use of multitopology information. By using [RFC7722], multiple topologies using different metric types can be obtained. Although there is no work defining how this extension can make use of the multitopology information base yet, experimentation with the use of multiple metrics for building multiple paths is encouraged.

Comments are solicited and should be addressed to the MANET working group's mailing list at manet@ietf.org and/or the authors.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

This document uses the terminology and notation defined in [RFC5444], [RFC6130], and [RFC7181]. Additionally, it defines the following terminology:

OLSRv2 Routing Process: A routing process based on [RFC7181], without multipath extension specified in this document.

MP-OLSRv2 Routing Process: A Multipath Routing Process based on this specification as an extension to [RFC7181].

SR-OLSRv2 Routing Process: An OLSRv2 Routing Process that supports Source Routing (SR) or an MP-OLSRv2 Routing Process.

3. Applicability Statement

As an extension of OLSRv2, this specification is applicable to MANETs for which OLSRv2 is applicable (see [RFC7181]). It can operate on single or multiple interfaces to discover multiple disjoint paths from a source router to a destination router. MP-OLSRv2 is designed for networks with dynamic topology to avoid single route failure. It can also provide higher aggregated throughput and load-balancing.

In a router supporting MP-OLSRv2, MP-OLSRv2 does not necessarily replace OLSRv2 completely. The extension can be applied for certain applications that are suitable for multipath routing (mainly video or audio streams) based on information such as a Diffserv codepoint [RFC2474].

Compared to OLSRv2, this extension does not introduce any new message type. A new Message TLV Type is introduced to identify the routers that support forwarding based on the source routing header. It is interoperable with OLSRv2 implementations that do not have this extension: as the MP-OLSRv2 uses source routing, in IPv4 networks the interoperability is achieved using loose source routing headers; in IPv6 networks, it is achieved by eliminating routers that do not support IPv6 strict source routing.

MP-OLSRv2 supports two different but interoperable multipath calculation approaches: proactive and reactive. In the proactive calculation, the paths to all the destinations are calculated before

they are needed. In the reactive calculation, only the paths to desired destination(s) are calculated on demand. The proactive approach requires more computational resources than the reactive one. The reactive approach requires the IP forwarding plane to trigger the multipath calculation.

MP-OLSRv2 forwards datagrams using the source routing header. As there are multiple paths to each destination, MP-OLSRv2 requires the IP forwarding plane to be able to choose which source route to be put in the source routing header based on the path scheduler defined by MP-OLSRv2. For IPv4 networks, implementation of loose source routing is required following [RFC791]. For IPv6 networks, implementation of strict source routing is required following the source routing header generation and processing defined in [RFC6554].

4. Protocol Overview and Functioning

This specification uses OLSRv2 [RFC7181] to:

- o Identify all the reachable routers in the network.
- o Identify a sufficient subset of links in the networks so that routes can be calculated to all reachable destinations.
- o Provide a Routing Set containing the shortest routes from this router to all destinations.

In addition, the MP-OLSRv2 Routing Process identifies the routers that support source routing by adding a new Message TLV in HELLO and Topology Control (TC) messages. Based on the above information acquired, every MP-OLSRv2 Routing Process is aware of a reduced topology map of the network and the routers supporting source routing.

A Multipath Routing Set containing the multipath information is maintained. It may be either proactively calculated or reactively calculated:

- o In the proactive approach, multiple paths to all possible destinations are calculated and updated based on control message exchange. The routes are thus available before they are actually needed.
- o In the reactive approach, a multipath algorithm is invoked on demand, i.e., only when there is a datagram to be sent from the source to the destination and there is no available Routing Tuple in the Multipath Routing Set. This requires the IP forwarding information base to trigger the multipath calculation specified in

Section 8.5 when no Multipath Routing Tuple is available. The reactive operation is local to the router and no additional exchange of routing control messages is required. When the paths are being calculated, the datagrams SHOULD be buffered unless the router does not have enough memory.

Routers in the same network may choose either proactive or reactive multipath calculation independently according to their computation resources. The Multipath Dijkstra Algorithm (defined in Section 8.5) is introduced as the default algorithm to generate multiple disjoint paths from a source to a destination, and such information is kept in the Multipath Routing Set.

The datagram is forwarded based on source routing. When there is a datagram to be sent to a destination, the source router acquires a path from the Multipath Routing Set. The path information is stored in the datagram header using the source routing header.

5. Parameters and Constants

In addition to the parameters and constants defined in [RFC7181], this specification uses the parameters and constants described in this section.

5.1. Router Parameters

NUMBER_OF_PATHS: The number of paths desired by the router.

MAX_SRC_HOPS: The maximum number of hops allowed to be put in the source routing header. A value set to 0 means there is no limitation on the maximum number of hops. In an IPv6 network, it MUST be set to 0 because [RFC6554] supports only strict source routing. All the intermediate routers MUST be included in the source routing header, which is a various number of hops. In an IPv4 network, it MUST be strictly less than 11 and greater than 0 due to the length limit of the IPv4 header.

CUTOFF_RATIO: The ratio that defines the maximum metric of a path compared to the shortest path kept in the OLSRv2 Routing Set. For example, the metric to a destination is R_metric based on the Routing Set. Then, the maximum metric allowed for a path is $CUTOFF_RATIO * R_metric$. **CUTOFF_RATIO** MUST be greater than or equal to 1. Setting the number low makes it less likely that additional paths will be found -- for example, setting it to 1 will mean only equal length paths are considered.

SR_TC_INTERVAL: The maximum time between the transmission of two successive TC messages by an MP-OLSRv2 Routing Process.

SR_HOLD_TIME: The minimum value in the TLV with Type = VALIDITY_TIME included in TC messages generated based on SR_TC_INTERVAL.

6. Packets and Messages

This extension employs the routing control messages HELLO and TC as defined in OLSRv2 [RFC7181] to obtain network topology information. For the datagram to support source routing, a source routing header is added to each datagram routed by this extension. Depending on the IP version used, the source routing header is defined in this section.

6.1. HELLO and TC messages

HELLO and TC messages used by the MP-OLSRv2 Routing Process use the same format as defined in [RFC7181]. In addition, a new Message TLV Type is defined to identify the originator of the HELLO or TC message that supports source-route forwarding. The new Message TLV Type is introduced for enabling MP-OLSRv2 as an extension of OLSRv2: only the routers supporting source-route forwarding can be used in the source routing header of a datagram because adding a router that does not understand the source routing header will cause routing failure.

6.1.1. SOURCE_ROUTE TLV

The SOURCE_ROUTE TLV is a Message TLV signaling that the message is generated by a router that supports source-route forwarding. It can be an MP-OLSRv2 Routing Process or an OLSRv2 Routing Process that supports source-route forwarding.

Every HELLO or TC message generated by a MP-OLSRv2 Routing Process MUST have exactly one SOURCE_ROUTE TLV without value.

Every HELLO or TC message generated by an OLSRv2 Routing Process MUST have exactly one SOURCE_ROUTE TLV, if the OLSRv2 Routing Process supports source-route forwarding, and be willing to join the source route generated by other MP-OLSRv2 Routing Processes. The existence of SOURCE_ROUTE TLV MUST be consistent for a specific OLSRv2 Routing Process, i.e., either it adds SOURCE_ROUTE TLV to all its HELLO/TC messages or it does not add SOURCE_ROUTE TLV to any HELLO/TC messages.

6.2. Datagram

6.2.1. Source Routing Header in IPv4

In IPv4 [RFC791] networks, the MP-OLSRv2 Routing Process employs the loose source routing header, as defined in [RFC791]. It exists as an option header with option class 0 and option number 3.

The source route information is kept in the "route data" field of the loose source routing header.

6.2.2. Source Routing Header in IPv6

In IPv6 [RFC8200] networks, the MP-OLSRv2 Routing Process employs the source routing header, as defined in Section 3 of [RFC6554], with IPv6 Routing Type 3.

The source route information is kept in the "Addresses" field of the routing header.

7. Information Bases

Each MP-OLSRv2 Routing Process maintains the information bases as defined in [RFC7181]. Additionally, a Multipath Information Base is used for this specification. It includes the protocol sets as defined below.

7.1. SR-OLSRv2 Router Set

The SR-OLSRv2 Router Set records the routers that support source-route forwarding. This includes routers that run the MP-OLSRv2 Routing Process or the OLSRv2 Routing Process with source-route forwarding support. The set consists of SR-OLSRv2 Routing Tuple:

(SR_addr, SR_time)

where:

SR_addr is the originator address of the router that supports source-route forwarding.

SR_time is the time until which the SR-OLSRv2 Routing Tuple is considered valid.

7.2. Multipath Routing Set

The Multipath Routing Set records the full path information of different paths to the destination. It consists of Multipath Routing Tuple:

(MR_dest_addr, MR_path_set)

where:

MR_dest_addr is the network address of the destination; it is either the network address of an interface of a destination router or the network address of an attached network.

MP_path_set contains the multiple paths to the destination and it consists of a set of Path Tuples.

Each Path Tuple is defined as:

(PT_metric, PT_address[1], PT_address[2], ..., PT_address[n])

where:

PT_metric is the metric of the path to the destination, measured in LINK_METRIC_TYPE defined in [RFC7181].

PT_address[1, ..., n-1] are the addresses of intermediate routers to be visited, numbered from 1 to n-1, where n is the number of routers in the path, i.e., the hop count.

8. Protocol Details

This protocol is based on OLSRv2 and is extended to discover multiple disjoint paths from a source router to a destination router. It retains the formats of the basic routing control packets and the processing of OLSRv2 to obtain the topology information of the network. The main differences from the OLSRv2 Routing Process are the datagram processing at the source router and datagram forwarding.

8.1. HELLO and TC Message Generation

HELLO messages are generated according to Section 15.1 of [RFC7181], plus a single message TLV with Type := SOURCE_ROUTE included.

TC messages are generated according to Section 16.1 of [RFC7181], plus a single message TLV with Type := SOURCE_ROUTE included.

For the routers that do not generate TC messages according to [RFC7181], at least one TC message **MUST** be generated by an MP-OLSRv2 Routing Process during the `SR_TC_INTERVAL` (Section 5), which **MUST** be greater than or equal to `TC_INTERVAL`. Those TC messages **MUST NOT** carry any advertised neighbor addresses. This serves for those routers to advertise the `SOURCE_ROUTE` TLV so that the other routers can be aware of the routers that are source-route enabled so as to be used as destinations of multipath routing. The validity time associated with the `VALIDITY_TIME` TLV in such TC messages equals `SR_HOLD_TIME`, which **MUST** be greater than the `SR_TC_INTERVAL`. If the TC message carries an optional `INTERVAL_TIME` TLV, it **MUST** have a value encoding the `SR_TC_INTERVAL`.

8.2. HELLO and TC Message Processing

HELLO and TC messages are processed according to Sections 15.3 and 16.3 of [RFC7181].

In addition to the reasons specified in [RFC7181] for discarding a HELLO message or a TC message on reception, a HELLO or TC message received **MUST** be discarded if it has more than one Message TLV with `Type = SOURCE_ROUTE`.

For every HELLO or TC message received, if there is a Message TLV with `Type := SOURCE_ROUTE`, create or update (if the Tuple exists already) the SR-OLSR Routing Tuple with:

- o `SR_addr` := originator address of the HELLO or TC message
- o `SR_time` := `current_time` + validity time of the TC or HELLO message defined in [RFC7181].

8.3. MPR Selection

Each MP-OLSRv2 Routing Process selects routing MPRs and flooding MPRs following Section 18 of [RFC7181]. In a mixed network with OLSRv2-only routers, the following considerations apply when calculating MPRs:

- o MP-OLSRv2 routers **SHOULD** be preferred as routing MPRs to increase the possibility of finding disjoint paths using MP-OLSRv2 routers.
- o The number of routing MPRs that run the MP-OLSRv2 Routing Process **MUST** be equal to or greater than `NUMBER_OF_PATHS` if there are enough MP-OLSRv2 symmetric neighbors. Otherwise, all the MP-OLSRv2 routers are selected as routing MPRs, except the routers with willingness `WILL_NEVER`.

8.4. Datagram Processing at the MP-OLSRv2 Originator

If datagrams without a source routing header need to be forwarded using multiple paths (for example, based on the information of a Diffserv codepoint [RFC2474]), the MP-OLSRv2 Routing Process will try to find the Multipath Routing Tuple where:

- o MR_dest_addr = destination of the datagram

If no matching Multipath Routing Tuple is found and the Multipath Routing Set is maintained proactively, it indicates that there is no multipath route available to the desired destination. The datagram is forwarded following the OLSRv2 Routing Process.

If no matching Multipath Routing Tuple is found and the Multipath Routing Set is maintained reactively, the multipath algorithm defined in Section 8.5 is invoked to calculate the Multipath Routing Tuple to the destination. If the calculation does not return any Multipath Routing Tuple, the following steps are aborted and the datagram is forwarded following the OLSRv2 Routing Process.

If a matching Multipath Routing Tuple is obtained, the Path Tuples of the Multipath Routing Tuple are applied to the datagrams using either per-flow or per-datagram scheduling, depending on the transport layer protocol and the application used. By default, per-flow scheduling is used, especially for the transport protocols that are sensitive to reordering, such as TCP. The path-selection decision is made on the first datagram and all subsequent datagrams of the same flow use the same path. If the path breaks before the flow is closed, another path with the most similar metric is used. Per-datagram scheduling is recommended if the traffic is insensitive to reordering such as unreliable transmission of media traffic or when erasure coding is applied. In such a case, each datagram selects its paths independently.

By default, the traffic load should be equally distributed in multiple paths. Other path-scheduling mechanisms (e.g., assigning more traffic over better paths) are also possible and will not impact the interoperability of different implementations.

The addresses in PT_address[1, ..., n-1] of the chosen Path Tuple are thus added to the datagram header as the source routing header. For IPv6 networks, strict source routing is used; thus, all the intermediate routers in the path are stored in the source routing header following the format defined in Section 3 of [RFC6554] with the Routing Type set to 3.

For IPv4 networks, loose source routing is used with the following rules:

- o Only the addresses that exist in the SR-OLSR Router Set can be added to the source routing header.
- o If the length of the path (n) is greater than MAX_SRC_HOPS (Section 5) or if adding the whole path information exceeds the MTU, only the "key" routers in the path are kept. By default, the key routers are uniformly chosen in the path. If further information, such as the capacity of the routers (e.g., battery life) or the routers' willingness in forwarding data, is available, the routers with higher capacity and willingness are preferred.
- o The routers that are considered not appropriate for forwarding indicated by external policies should be avoided.

It is not recommended to fragment the IP packet if the packet with the source routing header would exceed the minimum MTU along the path. Depending on the size of the routing domain, the MTU should be at least $1280 + 40$ (for the outer IP header) + $16 * \text{diameter of the network in number of hops}$ (for the source routing header). If the links in the network have different MTU sizes, by using technologies like Path MTU Discovery, the routers are able to be aware of the MTU along the path. The size of the datagram plus the size of IP headers (including the source routing header) should not exceed the minimum MTU along the path; otherwise, the source routing should not be used.

If the destination of the datagrams is out of the MP-OLSRv2 routing domain, the datagram must be source routed to the gateway between the MP-OLSRv2 routing domain and the rest of the Internet. The gateway MUST remove the source routing header before forwarding the datagram to the rest of the Internet.

8.5. Multipath Calculation

8.5.1. Requirements of Multipath Calculation

The Multipath Routing Set maintains the information of multiple paths to the destination. The Path Tuples of the Multipath Routing Set (Section 7.2) are generated based on a multipath algorithm.

For each path to a destination, the algorithm must provide:

- o The metric of the path to the destination,
- o The list of intermediate routers on the path.

For IPv6 networks, as strict source routing is used, only the routers that exist in the SR-OLSRv2 Router Set are considered in the path calculation, i.e., only the source-routing-supported routers can exist in the path.

After the calculation of multiple paths, the metric of paths (denoted c_i for path i) to the destination is compared to the R_metric of the OLSRv2 Routing Tuple ([RFC7181]) to the same destination. If the metric c_i is greater than $R_metric * CUTOFF_RATIO$ (Section 5), the corresponding path i SHOULD NOT be used. If less than two paths are found with metrics less than $R_metric * CUTOFF_RATIO$, the router SHOULD fall back to OLSRv2 Routing Process without using multipath routing. This can happen if there are too many OLSRv2-only routers in the network, and requiring multipath routing may result in inferior paths.

By invoking the multipath algorithm, up to `NUMBER_OF_PATHS` paths are obtained and added to the Multipath Routing Set by creating a Multipath Routing Tuple with:

- o `MR_dest_addr` := destination of the datagram.
- o An `MP_path_set` with calculated Path Tuples. Each Path Tuple corresponds to a path obtained in the Multipath Dijkstra Algorithm, with `PT_metric` := metric of the calculated path and `PT_address[1, ..., n-1]` := list of intermediate routers.

8.5.2. Multipath Dijkstra Algorithm

This section introduces the Multipath Dijkstra Algorithm as a default algorithm. It tries to obtain disjoint paths when appropriate, but it does not guarantee strict disjoint paths. The use of other algorithms is not prohibited, as long as the requirements described in Section 8.5.1 are met. Using different multipath algorithms will not impact the interoperability.

The general principle of the Multipath Dijkstra Algorithm [ADHOC11] is to use the Dijkstra Algorithm for multiple iterations and to look for the shortest path $P[i]$ to the destination d at iteration i . After each iteration, the metric of used links is increased. Compared to the original Dijkstra's algorithm, the main modification consists in adding two incremental functions, named metric functions fp and fe , in order to prevent the next steps resulting in similar paths:

- o $fp(c)$ is used to increase metrics of arcs belonging to the previous path $P[i-1]$ (with $i>1$), where c is the value of the previous metric. This encourages future paths to use different arcs but not different vertices.
- o $fe(c)$ is used to increase metrics of the arcs that lead to intermediate vertices of the previous path $P[i-1]$ (with $i>1$), where c is the value of the previous metric. The "lead to" means that only one vertex of the arc belongs to the previous path $P[i-1]$ while the other vertex does not. The "intermediate" means that the source and destination vertices are not considered.

Consider the simple example in Figure 1: a path $P[i]$ $S \rightarrow A \rightarrow D$ is obtained at step i . For the next step, the metric of link $S \rightarrow A$ and $A \rightarrow D$ are to be increased using $fp(c)$ because they belong to the path $P[i]$. $A \rightarrow B$ is to be increased using $fe(c)$ because A is an intermediate vertex of path $P[i]$, and B is not part of $P[i]$. $B \rightarrow D$ is unchanged.

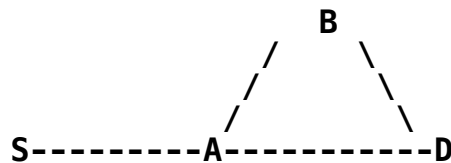


Figure 1

It is possible to choose a different fp and fe to get link-disjoint paths or node-disjoint paths as desired. A recommendation for configuration of fp and fe is given in Section 9.

To get `NUMBER_OF_PATHS` different paths, for each path $P[i]$ ($i = 1, \dots, \text{NUMBER_OF_PATHS}$):

1. Run Dijkstra's algorithm to get the shortest path $P[i]$ for the destination d .
2. Apply metric function fp to the metric of links (in both directions) in $P[i]$.
3. Apply metric function fe to the metric of links (in both directions) that lead to routers used in $P[i]$.

A simple example of the Multipath Dijkstra Algorithm is illustrated in Appendix A.

8.6. Multipath Routing Set Updates

The Multipath Routing Set **MUST** be updated when the Local Information Base, the Neighborhood Information Base, or the Topology Information Base indicate a change (including a change of any potentially used outgoing neighbor metric values) of the known symmetric links and/or attached networks in the MANET, hence, changing the Topology Graph as described in Section 17.7 of [RFC7181]. How the Multipath Routing Set is updated depends on whether the set is maintained reactively or proactively:

- o In reactive mode, all the Tuples in the Multipath Routing Set are removed. The new arriving datagrams will be processed as specified in Section 8.4.
- o In proactive mode, the routes to all the destinations are updated according to Section 8.5.

8.7. Datagram Forwarding

In IPv4 networks, datagrams are forwarded using loose source routing as specified in Section 3.1 of [RFC791].

In IPv6 networks, datagrams are forwarded using strict source routing as specified in Section 4.2 of [RFC6554], except the applied routers are MP-OLSRv2 routers rather than RPL routers. The last hop of the source route **MUST** remove the source routing header.

9. Configuration Parameters

This section gives default values and guidelines for setting parameters defined in Section 5. Network administrators may wish to change certain or all the parameters for different network scenarios. As an experimental protocol, the users of this protocol are also encouraged to explore different parameter settings in various network environments and provide feedback.

- o **NUMBER_OF_PATHS** := 3. This parameter defines the number of parallel paths used in datagram forwarding. Setting it to 1 makes the specification identical to OLSRv2. Setting it to too large of a value may lead to unnecessary computational overhead and inferior paths.
- o **MAX_SRC_HOPS** := 10, for IPv4 networks. For IPv6 networks, it **MUST** be set to 0, i.e., no constraint on the maximum number of hops.
- o **CUTOFF_RATIO** := 1.5. It **MUST** be greater than or equal to 1.

- o `SR_TC_INTERVAL := 10 x TC_INTERVAL`. It MUST be greater than or equal to `TC_INTERVAL`. It SHOULD be significantly greater than `TC_INTERVAL` to reduce unnecessary TC message generations.
- o `SR_HOLD_TIME := 3 x SR_TC_INTERVAL`. It MUST be greater than `SR_TC_INTERVAL` and SHOULD allow for a small number of lost messages.

If the Multipath Dijkstra Algorithm is applied:

- o `fp(c) := 4*c`, where `c` is the original metric of the link.
- o `fe(c) := 2*c`, where `c` is the original metric of the link.

The setting of metric functions `fp` and `fc` defines the preference of obtained multiple disjoint paths. If `id` is the identity function, i.e., `fp(c)=c`, three cases are possible:

- o if `id=fe<fp`, only increase the metric of related links;
- o if `id<fe=fp`, apply equal increase to the metric of related nodes and links;
- o if `id<fe<fp`, apply greater increase to the metric of related links.

Increasing the metric of related links or nodes means avoiding the use of such links or nodes in the next path to be calculated.

10. Security Considerations

As an extension of [RFC7181], the security considerations and security architecture illustrated in [RFC7181] are applicable to this MP-OLSRv2 specification. The implementations without security mechanisms are vulnerable to threats discussed in [RFC8116].

In a mixed network with OLSRv2-only routers, a compromised router can add `SOURCE_ROUTE` TLVs in its TC and HELLO messages, which will make other MP-OLSRv2 Routing Processes believe that it supports source routing. This will increase the possibility of being chosen as MPRs and put into the source routing header. The former will make it possible to manipulate the flooding of TC messages and the latter will make the datagram pass through the compromised router.

As with [RFC7181], a conformant implementation of MP-OLSRv2 MUST, at minimum, implement the security mechanisms specified in [RFC7183] to provide integrity and replay protection of routing control messages.

The MP-OLSRv2 Routing Process **MUST** drop datagrams entering or exiting an OLSRv2/MP-OLSRv2 routing domain that contain a source routing header. Compared to OLSRv2, the use of the source routing header in this specification introduces vulnerabilities related to source routing attacks, which include bypassing filtering devices, bandwidth exhaustion of certain routers, etc. Those attacks are discussed in Section 5 of [RFC6554] and [RFC5095]. The influence is limited to the OLSRv2/MP-OLSRv2 routing domain because the source routing header is used only in the current routing domain.

If the multiple paths are calculated reactively, the datagrams **SHOULD** be buffered while the paths are being calculated. Because the path calculation is local and no control message is exchanged, the buffering time should be trivial. However, depending on the CPU power and memory of the router, a maximum buffer size **SHOULD** be set to avoid occupying too much memory of the router. When the buffer is full, the oldest datagrams are dropped. A possible attack that a malicious application could launch would be one in which it initiates a large amount of datagrams to all the other routers in the network, thus triggering path calculation to all the other routers and during which the datagrams are buffered. This might flush other legitimate datagrams. But the impact of the attack is transient: once the path calculation is finished, the datagrams are forwarded and the buffer goes back to empty.

11. IANA Considerations

This section adds one new Message TLV, allocated as a new Type Extension to an existing Message TLV.

11.1. Message TLV Types

This specification updates the "Type 7 Message TLV Type Extensions" registry [RFC7181] by adding the new Type Extension SOURCE_ROUTE, as illustrated in Table 1.

Type Extension	Name	Description	Reference
2	SOURCE_ROUTE	Indicates that the originator of the message supports source-route forwarding. No value.	This specification

Table 1: SOURCE_ROUTE Type for Type 7 Message TLV Type Extensions

12. References

12.1. Normative References

- [RFC791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <<https://www.rfc-editor.org/info/rfc791>>.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC5444] Clausen, T., Dearlove, C., Dean, J., and C. Adjih, "Generalized Mobile Ad Hoc Network (MANET) Packet/Message Format", RFC 5444, DOI 10.17487/RFC5444, February 2009, <<https://www.rfc-editor.org/info/rfc5444>>.
- [RFC6130] Clausen, T., Dearlove, C., and J. Dean, "Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)", RFC 6130, DOI 10.17487/RFC6130, April 2011, <<https://www.rfc-editor.org/info/rfc6130>>.
- [RFC6554] Hui, J., Vasseur, JP., Culler, D., and V. Manral, "An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL)", RFC 6554, DOI 10.17487/RFC6554, March 2012, <<https://www.rfc-editor.org/info/rfc6554>>.
- [RFC7181] Clausen, T., Dearlove, C., Jacquet, P., and U. Herberg, "The Optimized Link State Routing Protocol Version 2", RFC 7181, DOI 10.17487/RFC7181, April 2014, <<https://www.rfc-editor.org/info/rfc7181>>.
- [RFC7183] Herberg, U., Dearlove, C., and T. Clausen, "Integrity Protection for the Neighborhood Discovery Protocol (NHDP) and Optimized Link State Routing Protocol Version 2 (OLSRv2)", RFC 7183, DOI 10.17487/RFC7183, April 2014, <<https://www.rfc-editor.org/info/rfc7183>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.

12.2. Informative References

- [ADHOC11] Yi, J., Adnane, A., David, S., and B. Parrein, "Multipath optimized link state routing for mobile ad hoc networks", Elsevier Ad Hoc Networks, Volume 9, Number 1, pp 28-47, DOI 10.1016/j.adhoc.2010.04.007, January 2011.
- [GIIS14] Macedo, R., Melo, R., Santos, A., and M. Nogueira, "Experimental performance comparison of single-path and multipath routing in VANETs", In the Global Information Infrastructure and Networking Symposium (GIIS), Volume 1, Number 6, pp 15-19, DOI 10.1109/GIIS.2014.6934283, September 2014.
- [IPv6-SRH] Previdi, S., Ed., Filsfils, C., Raza, K., Leddy, J., Field, B., Voyer, D., Bernier, S., Matsushima, S., Leung, I., Linkova, J., Aries, E., Kosugi, T., Vyncke, E., Lebrun, D., Steinberg, D., and R. Raszuk, "IPv6 Segment Routing Header (SRH)", Work in Progress, draft-ietf-6man-segment-routing-header-07, July 2017.
- [RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, DOI 10.17487/RFC2474, December 1998, <<https://www.rfc-editor.org/info/rfc2474>>.
- [RFC2501] Corson, S. and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", RFC 2501, DOI 10.17487/RFC2501, January 1999, <<https://www.rfc-editor.org/info/rfc2501>>.
- [RFC2991] Thaler, D. and C. Hopps, "Multipath Issues in Unicast and Multicast Next-Hop Selection", RFC 2991, DOI 10.17487/RFC2991, November 2000, <<https://www.rfc-editor.org/info/rfc2991>>.
- [RFC5095] Abley, J., Savola, P., and G. Neville-Neil, "Deprecation of Type 0 Routing Headers in IPv6", RFC 5095, DOI 10.17487/RFC5095, December 2007, <<https://www.rfc-editor.org/info/rfc5095>>.
- [RFC7722] Dearlove, C. and T. Clausen, "Multi-Topology Extension for the Optimized Link State Routing Protocol Version 2 (OLSRv2)", RFC 7722, DOI 10.17487/RFC7722, December 2015, <<https://www.rfc-editor.org/info/rfc7722>>.

- [RFC7779] Rogge, H. and E. Baccelli, "Directional Airtime Metric Based on Packet Sequence Numbers for Optimized Link State Routing Version 2 (OLSRv2)", RFC 7779, DOI 10.17487/RFC7779, April 2016, <<https://www.rfc-editor.org/info/rfc7779>>.
- [RFC8116] Clausen, T., Herberg, U., and J. Yi, "Security Threats to the Optimized Link State Routing Protocol Version 2 (OLSRv2)", RFC 8116, DOI 10.17487/RFC8116, May 2017, <<https://www.rfc-editor.org/info/rfc8116>>.
- [RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <<https://www.rfc-editor.org/info/rfc8200>>.
- [WCNC08] Yi, J., Cizeron, E., Hama, S., and B. Parrein, "Simulation and Performance Analysis of MP-OLSR for Mobile Ad hoc Networks", In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), DOI 10.1109/WCNC.2008.395, 2008.
- [WPMC11] Yi, J., Parrein, B., and D. Radu, "Multipath Routing Protocol for MANET: Application to H.264/SVC Video Content Delivery", Proceedings of the 14th International Symposium on Wireless Personal Multimedia Communications, 2011.

Appendix A. Examples of Multipath Dijkstra Algorithm

This appendix gives two examples of the Multipath Dijkstra Algorithm.

A network topology is depicted in Figure 2.

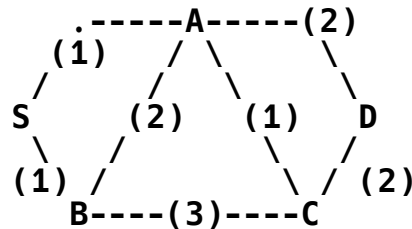


Figure 2

The capital letters are the names of routers. An arbitrary metric with value between 1 and 3 is used. The initial metrics of all the links are indicated in the parentheses. The incremental functions $fp(c)=4c$ and $fe(c)=2c$ are used in this example. Two paths from router S to router D are demanded.

On the first run of the Dijkstra Algorithm, the shortest path S->A->D with metric 3 is obtained.

The incremental function fp is applied to increase the metric of the link S-A and A-D, and fe is applied to increase the metric of the link A-B and A-C. Figure 3 shows the link metrics after the increment.

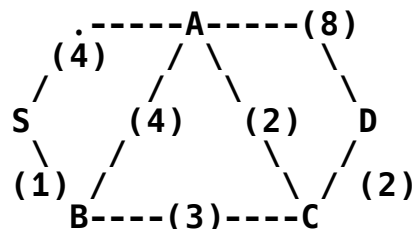


Figure 3

On the second run of the Dijkstra Algorithm, the second path S->B->C->D with metric 6 is obtained.

As mentioned in Section 8.5, the Multipath Dijkstra Algorithm does not guarantee strict disjoint paths in order to avoid choosing inferior paths. For example, given the topology in Figure 4, two paths from node S to D are desired. On the top of the figure, there is a high cost path between S and D.

If an algorithm tries to obtain strict disjoint paths, the two paths obtained will be S--B--D and S--(high cost path)--D, which are extremely unbalanced. It is undesirable because it will cause huge delay variance between the paths. By using the Multipath Dijkstra Algorithm, which is based on the punishing scheme, S--B--D and S--B--C--D will be obtained.

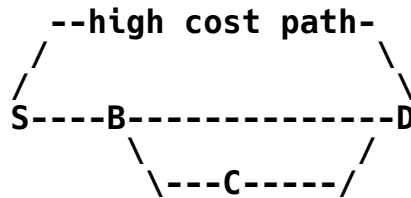


Figure 4

Acknowledgments

The authors would like to thank Sylvain David, Asmaa Adnane, Eddy Cizeron, Salima Hamma, Pascal Lesage, and Xavier Lecourtier for their efforts in developing, implementing, and testing the specification. The authors also appreciate valuable discussions with Thomas Clausen, Ulrich Herberg, Justin Dean, Geoff Ladwig, Henning Rogge, Marcus Barkowsky, and especially Christopher Dearlove for his multiple rounds of reviews during the working group last calls.

Authors' Addresses

Jiazi Yi
Ecole Polytechnique
91128 Palaiseau Cedex
France

Phone: +33 (0) 1 77 57 80 85
Email: jiazi@jiaziyi.com
URI: <http://www.jiaziyi.com/>

Benoit Parrein
University of Nantes
IRCCyN Lab - IVC team
Polytech Nantes, rue Christian Pauc, BP50609
44306 Nantes cedex 3
France

Phone: +33 (0) 2 40 68 30 50
Email: Benoit.Parrein@polytech.univ-nantes.fr
URI: <http://www.irccyn.ec-nantes.fr/~parrein>