# Source-destination Routing for Optimised Link State Routing Protocol

Jiazi Yi, Thomas Clausen
Laboratoire d'Informatique (LIX) – Ecole Polytechnique
Route de Saclay, Palaiseau, 91128, France
jiazi@jiaziyi.com, Thomas@ThomasClausen.org

***Abstract*—Typical routing protocols maintain entries in their RIB (Routing Information Base) permitting destination-based forwarding: for a given data packet, the choice of next hop is a function of the destination address only. However, in deployments where a given network is multi-homed, and where ingress filtering is commonly applied, a routing protocol is required to be able to provide routes so as to forward a data packet (i) to the destination address of the data packet, while (ii) routing through the gateway for which the source address of the data packet is topologically correct. This is called *source-destination routing***

**This paper presents an extension to the Optimized Link State Routing Protocol version 2 (OLSRv2), providing support for such source-destination routing. In a multi-homed network, this OLSRv2 extension provides routes for data packets based also on the source prefix announced by the gateways. The extension is interoperable with unextended OLSRv2. The performance of this extension is quantified by way of simulation studies.**

## I. Introduction

Mobile Ad hoc NETworks (MANETs) are leaving the confines of research laboratories, to find place in real-world deployments. Outside specialised domains (military, vehicular, etc.), city-wide community-networks are emerging, connecting regular Internet users with each other, and with the Internet, by way of MANETs. MANET protocols are thus facing more realistic application scenarios and restrictions, such as existence of gateways to communicate with other networks, security requirements, and interoperability with other protocols.

When a MANET is connected to external networks through multiple gateways which applies ingress filtering (*i.e.,*a gateway only accepts forwards data packets, originating from certain source addresses), data packets must be forwarded within the MANET so that they reach the right gateway – *i.e.,*a gateway which accepts and forwards data packets with the given source address, and which provides connectivity to the destination address. Consequently, routing protocols must provide topologies, and topological information, allowing such routing.

### A. Background and History

Since the late 90s, the Internet Engineering Task Force (IETF)[1] has embarked upon a path of developing routing protocols for networks with increasingly more fragile and low-capacity links, with less pre-determined connectivity properties, and with increasingly constrained router resources. The work related to ad hoc networks is performed in Mobile Ad hoc NETwork working group.

*1) Routing Protocol for Mobile ad hoc Networks:* The MANET working group converged on the development of two protocol families: reactive protocols, including AODV (Ad hoc On-demand Distance Vector routing [1]), and proactive protocols, including Optimized Link State Routing (OLSR) [2]. A distance vector protocol, AODV operates in an on-demand fashion, acquiring and maintaining paths only while needed for carrying data, by way of a Route Request and Route Reply message exchange. A link state protocol, OLSR is based on periodic control messages exchanges, with each router proactively maintaining a routing table with entries for all destinations in the network – which provides low delays but constant control overhead. A sizeable body of work exists, including [3], studying the performance of these protocols in different scenarios, and justifying their complementarity.

After acquiring operational experiences with AODV and OLSR, the MANET working group commenced developing successors to these protocols, denoted OLSRv2 and DYMO. Whereas the momentum behind DYMO withered in the MANET working group[2], a relatively large and active community around OLSR thus standardised OLSRv2 [4], [5], [6], [7], [8], [9], [10], [11], as well as numerous extensions [12], [13], [14], [15], [16] and optimisations [12], [14].

*2) Source-destination Routing:* Typical routing protocols maintain, in their RIB (Routing Information Base) entries permitting destination-based forwarding: for a given data packet, the choice of next hop is a function of the destination address only, based on "longest prefix matching" of data packet destination addresses to RIB entry prefixes.

Also, at the periphery of the Internet, network providers are applying *ingress traffic filtering* in order to reduce the effectiveness of source address spoofing denial of service attacks. This, essentially, consists of restricting transit traffic which originates from a downstream network to known, and intentionally advertised, prefix(es). The IETF recommends that all service providers implement this type of filtering on pheriphy routers, by dropping traffic entering their networks that is coming from a source address not legitimately in use by the customer network [17].

However as networks become multi-homed, *i.e.,*that con-

[1] http://www.ietf.org

[2] http://tools.ietf.org/wg/manet/minutes?item=minutes81.html

nectivity for a given network is provided by multiple distinct providers, ingress-filtering can cause problems: data packets for a given destination must be forwarded first to the proper gateway, *i.e.,*to the gateway for which the source address is topologically correct – least, the data packet will be dropped blocked [18]. Figure 1(a) depicts an example of ingress filtering. Both *Router 2* and *Router 3* advertise a default route (:: /0) to the client's network. An ingress filter is applied to *Router 2* by Provider A, which only accepts source address with prefix A::. The same for *Router 3*, which only accept address with prefix B::. If the a packet originated by host with address $A$ :: 1 is routed to *Router 3*, the packet will be dropped.

One solution to this problem is source-destination routing: a data packet can get to the correct gateway following the default route, by considering not only the destination address of the packet, but also the source address. For example, in Figure 1(a), *Router 1* should be able to forward the packet originated from hosts with address $A$ :: prefix to *Router 2*.

### B. Statement of Purpose

As a routing protocol for mobile and self-organized networks, OLSRv2 aims not only for enabling networking inside an OLSRv2 routing domain, but also having an OLSRv2 network connect to the Internet. Indeed, OLSRv2 as specified [6] provides for network gateway support, and supports multiple gateways – but does not offer provisions for source-destination routing. This paper rectifies this, by proposing a source-destination extension to OLSRv2. The proposed extension is interoperable with non-extended OLSRv2.

Given the potentially dynamic nature of an ad hoc network, support for source-destination routing has the potential to be more important than in many other networks. This, because the gateways through which the ad hic network is connected can be dynamically changing over time: both in terms of internal topology (*i.e.,*distance from a router to each gateway) but also in terms of how many, and which, gateways are present in the network

The desired source-destination extension for OLSRv2 should be able to:

- Distribute destination prefixes and source prefixes, announced by any number of gateways present in the network;
- Unambiguously forward data packets to the correct gateway, based on both the destination and source address of the data packet,
- Be interoperable with unextended OLSRv2.

### C. Paper Outline

The remainder of this paper is organized as follows: section II briefly introduces OLSRv2. A detailed specification of source-destination routing is introduced in section III. Section IV presents a performance analysis by way of a simulation study. Finally, section V concludes this paper.

## II. Optimised Link State Routing version 2: Overview

OLSRv2 is a successor to the widely deployed OLSR [2] routing protocol for MANETs, standardized by the IETF. OLSRv2 retains the same basic algorithms as its predecessor, however offers various improvements, *e.g.* a modular and flexible architecture allowing extensions to be developed, as add-ons to the basic protocol.

### A. The General Message Format

OLSRv2 control signals are encoded as messages within the "Generalized Mobile Ad Hoc Network (MANET) Packet/Message Format" specified in [4]. This format is TLV-based (Type-Length-Value), essential offering a set of fixed header fields (type, address length, originator address, hop-limit, hop-count and sequence number) followed by a block of "message TLVs". After the block of "message TLVs" follows a block of addresses, with associated "address block TLVs" assigning semantics to each address.

This use of the packet/message format in [4] enables unmodified use of protocol parsers, even when designing an extensible and flexible protocol.

### B. Modular Architecture

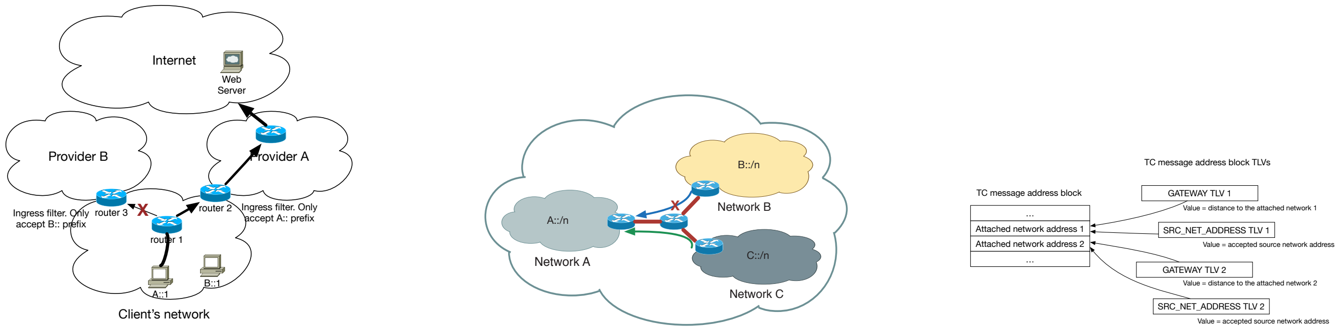
OLSRv2 contains three basic processes: Neighbourhood Discovery, MPR Flooding and Link State Advertisements. The packets are forwarded based on the topology information acquired from the periodic routing message exchange.

*1) Neighbourhood Discovery:* the process, whereby each router discovers the routers which are in direct communication range of itself (1-hop neighbours), and detects with which of these it can establish bi-directional communication. Each router sends HELLO messages, listing the identifiers of all the routers from which it has recently received a HELLO message, as well as the "status" of the link (heard, verified bi-directional).

*2) MPR (Multi-Point Relay) Flooding:* the process whereby each router is able to, efficiently, conduct network-wide broadcasts. Each router designates, from among its bi-directional neighbours, a subset (MPR set) such that a message transmitted by the router and relayed by the MPR set is received by all its 2-hop neighbours. MPR selection is encoded in outgoing HELLOs.

*3) Link State Advertisement:* the process whereby routers are determining which link state information to advertise through the network. Each router must advertise, at least, all links between itself and its MPR-selector-set, in order to allow all routers to calculate shortest paths. Such link state advertisements are carried in TCs (Topology Control message), broadcast periodically through the network using the MPR flooding process described above.

To announce the existence of gateways in the network, the gateway must also include the gateway information in the *Local Attached Network Set*, which records the gateway's local non-OLSRv2 interfaces via which it can act as a gateway to other networks.


Internet
Web Server
Provider B
Provider A
router 3
router 2
router 1
Ingress filter. Only accept B:: prefix
Ingress filter. Only accept A:: prefix
A::1
B::1
Client's network
B::/n
Network B
A::/n
Network A
C::/n
Network C
TC message address block TLVs
TC message address block
...
Attached network address 1
Attached network address 2
...
GATEWAY TLV 1
Value = distance to the attached network 1
SRC_NET_ADDRESS TLV 1
Value = accepted source network address
GATEWAY TLV 2
Value = distance to the attached network 2
SRC_NET_ADDRESS TLV 2
Value = accepted source network address

(a) Ingress filtering and source-destination routing

(b) An example of access control in different internal networks.

(c) An example of TLVs for source-destination routing

Figure 1.

*4) Routing and Forwarding:* OLSRv2 is a routing protocol, which implies that it acquires a topology database describing the network, and then produces a routing table – typically, handed off the the underlying operating system for use when forwarding data.

OLSRv2 [6] supports destination routing: the next hop of the data packet is determined exclusively by the destination address of the data packet. If a packet is to be forwarded to another network, it is sent to a gateway of based on the information of the *Attached Network Set*, which records information about networks (which maybe outside the ad hoc network) attached to other routers and their routable addresses.

## III. Source-destination Routing for OLSRv2

This section introduces the source-destination routing extension for OLSRv2, motivating the extension by presenting typical application scenarios in section III-A, followed by a specification of the proposed extension in section III-B.

### A. Application Scenarios

*1) Multihoming:* used as the motivating example in section I, this is when a device, or a network (i) is connected to the larger Internet by way of more than one gateway, and (ii) where the gateways provide connectivity for disjoint address prefixes within the network, and (iii) where the gateways act as default routers, *i.e.,*advertise default routes towards the network, and (iv) where the gateways apply ingress filtering so as to avoid address spoofing denial of service attacks. Under those conditions, data packets generated within the multihomed network must be routed to the gateway corresponding to the source address of the data packet – and, a routing protocol must be able to provide such routing paths. Figure 1(a) illustrates an example.

*2) Access control:* For a network, comprising several internal networks, different access permissions may apply to these – a classical example being the network in a ”private home”, which might have a ”members of the household network” with full access to private file servers, utility, and domotics systems, whereas a guest network in the same ”private home” might provide access to entertainment services only.

The routing protocol of that networks should be able to advertise the gateways through which the different can be reached, plus the list of acceptable prefixes, and maintain the information base for forwarding the packets.

Figure 1(b) shows a simple example. The border router of Network A advertise the gateway information of network $A :: /n$. However, it applies an ingress filter that only accepts source address with $C :: /n$. The packet from Network B to Network A will thus be filtered.

### B. Source-Destination Routing Extension Specification

The extension is specified by way of three independent components: the message format, the necessary information bases, and the associated processing – detailed in the below.

*1) Message Format:* OLSRv2 defines a *GATEWAY* TLV, included in TC messages generated by a gateway. All networks addresses of attached networks must be associated with *GATEWAY* TLV(s), with the value equal to the number of hops from the gateway router to the attached network.

To enable source-destination routing, the source prefix that can be accepted by the gateway must also be advertised to the whole OLSRv2 network. This can be achieved by way of extending TC messages so as to include a new TLV *SRC_NET_ADDRESS*, to be associated with the attached network address(s). The value of this TLV equals the network address or prefix of the source addresses that can be accepted by the gateway(s). This is illustrated in figure 1(c). Due to the extensibility of the general message format [4], such extended TC message can still be correctly parsed (although not interpreted) by the routers without source-destination extension.

*2) Information Base:* To support source-destination routing, two information sets from OLSRv2 are extended.

*a) Local Attached Network Set:* The Local Attached Network Set records its local non-OLSRv2 interfaces via which it can act as a gateway to other networks. It consists of Local Attached Network Tuples defined as:

`(AL_net_addr, AL_dist, AL_metric,`
**`AL_src_net_addr`**`)`

In addition to these fields, as defined in [6], this tuple is extended by:

`AL_src_net_addr` – the source network address can be accepted by the current gateway.

*b) Attached Network Set:* The Attached Network Set records information about networks (which may be outside the MANET) attached to other routers and their routable addresses. It consists of Attached Network Tuples:

```
(AN_orig_addr, AN_net_addr,
AN_seq_number, AN_dist, AN_metric,
AN_time, AN_src_net_addr)
```

In addition to the fields defined in [6], this tuple is extended by:

`AN_src_net_addr` – the source network address can be accepted by the gateway with address AN_orig_addr.

*3) Processing:* In addition to the TC and HELLO message processing specified in [6], the processing of TC messages and the forwarding of data packets have to be extended according to this section.

*a) TC Message Processing:* On receiving a TC message carrying valid source-destination gateway information, as defined in section III-B1, the Attached Network Set must be updated. An Attached Network Tuple is created, or updated with:

- AN_src_net_addr equals network address carried in SRC_NET_ADDRESS TLV of the TC message.
- AN_net_addr equals the attached network address that are associated with the GATEWAY TLV of the TC message.
- AN_orig_addr equals the address of the TC message originator.

By doing so, the OLSRv2 router receiving the TC message can learn the gateway address and the source address that the gateway accepts.

*b) Data Packet Forwarding:* For source-destination routing, the next hop for a data packet must be chosen by considering the source prefix.

For convenience, two network addresses $A :: /n_1$ and $B :: /n_2$ are denoted $A :: /n_1 \subseteq B :: /n_2$ if and only if:

- $n_1 \geq n_2$, and
- The first $n_2$ bits of $A$ and $B$ are identical.

where $n_1$ and $n_2$ are the prefix length of IPv6 address (the same applies for IPv4 address). This is also called $A :: /n_1$ matches $B :: /n_2$.

Due to the hierarchical nature of the IP addresses, there is possible ambiguity in address matching. A common example is the default gateway: a gateway might advertise an address $(:: /0)$, which makes

$$\forall addressA \in IPaddress : addressA \subseteq (:: /0)$$

To avoid ambiguity, when a router receives a packet to another network with destination address $A :: B$ (which is not in the local routing table) and source address $C :: D$, the following procedure must be followed:

1) Find the Attached Network Tuple that
$$A :: B \subseteq AN\_net\_addr$$
with the longest match prefix length $n$;
2) Verify the tuple found in Step 1) has
$$C :: D \subseteq AN\_src\_net\_addr$$
3) If yes, then $AN\_orig\_addr$ is the valid gateway. If no, repeat Step 1) without considering the tuple just found.
4) If a valid gateway with address $AN\_orig\_addr$ is found, the next hop is found by consulting the *Routing Set* with destination address equals $AN\_orig\_addr$.
5) If all the Attached Network Tuples have been visited and no valid gateway is found, the data packet is discarded.

## IV. Performance Evaluation

This section presents a simulation study of the proposed OLSRv2 extension.

### A. Simulation Settings

In order to evaluate the performance of the source-destination extension, and compare its performance to that of unextended OLSRv2, network simulations by way of NS2 are employed. While network simulations are, at best, an approximation of real-world performance (particularly due to the fidelity of their lower layers to reality), they do provide a baseline for comparison and, generally, best-case results, *i.e.,*real-world performance is expected to be no better than that which is obtained through simulations. The reason for using network simulations is that it allows running experiments with different protocols under identical conditions and parameters (MAC layer, distribution, number of nodes, etc.).

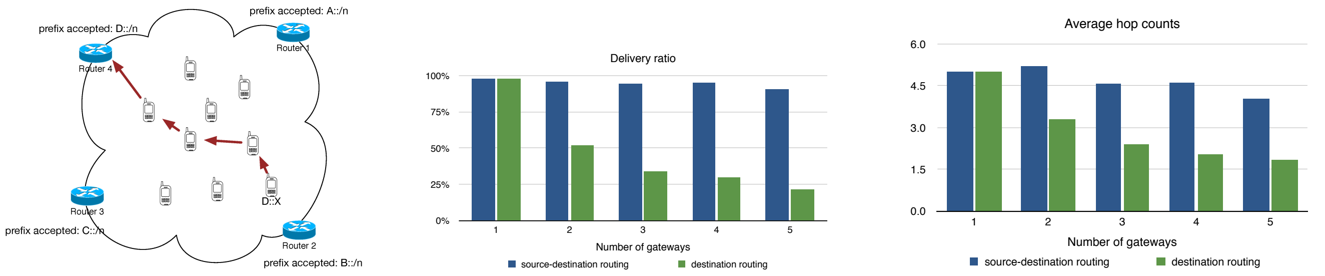
Simulations were conducted using the TwoRayGround propagation model and the IEEE 802.11 MAC. The transmission range of the radio is 250 meters. There are 50 OLSRv2 routers distributed randomly in a 1000m × 1000m square. For the purpose of this study, no mobility is considered for the OLSRv2 routers.

Depending on the scenario settings, there are $n$ gateways $(1 \leq n \leq 5)$ located on the edge of the network, exemplified in figure 2(a). All the gateways advertise a default gateway $:: /0$ to the OLSRv2 network. Each gateway only accept $50/n$ source addresses of OLSRv2 routers, with data packets with other source addresses being dropped. All the OLSRv2 routers generates a data packet to an external network every 5 seconds.

A full implementation of OLSRv2 [6] is developed, and compared with a version of [6] extended with this source-destination routing extension.

### B. Results and Analyses

Figure 2(b) depicts the data delivery ratio of data packets. Unextended OLSRv2 causes routers to forward data packets to the topologically nearest gateway – which may or may not be the source-address-wise correct gateway. More gateways in the network causes a greater possibility that the topologically nearest gateway is not the correct gateway – causing increasing packet drops as the number of gateways increases. The source-destination extension, as shown in figure 2(b) effectivelya avouds this. Consequently, as can be seen in figure 2(c), the



(a) Network topology of simulation with 4 gateways

(b) Average delivery ratio with multiple gateways

(c) Average hop count with multiple gateways

Figure 2. Simulation Topology and Results

extension also causes an increased average path length for successfully delivered data packets: data packets no longer reach simply the nearest gateway, but the correct gateway.

## V. Conclusion

OLSRv2 supports multiple gateways to external networks to be present in a network – however the operating hypothesis for this mechanism, as specified in [6] is, that all gateways will accept all traffic for al destinations that they advertise. In some deployments, for example where gateways apply source-address ingress filters to reduce the effectiveness of source address spoofing denial of service attacks, this mechanism is insufficient: data traffic must be routed both towards the destination, and via the source-address appropriate gateway.

This paper has proposed a source-destination routing extension for OLSRv2: source-prefix information for gateways is disseminated with link advertisements by way of adding a TLV to TC messages. Based on the gateway information so disseminated, the RIB can be constructed for correct packet forwarding, accounting for gateway selection by way of source address matching, and path destination by way of the destination addresses.

## Acknowledgement

This work was, in part, supported by the Cisco-Polytechnique Chaire "Internet of Everything" (http://www.internet-of-everything.fr/).

## References

[1] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," Experimental RFC 3561, July 2003.

[2] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)," RFC 3626, IETF, October 2003.

[3] T. Clausen, P. Jacquet, and L. Viennot, "Comparative study of routing protocols for mobile ad-hoc networks." Proceedings of the IFIP MedHocNet, September, Sardinia, Italy, 2002.

[4] T. Clausen, C. Dearlove, J. Dean, and C. Adjih, "Generalized manet packet/message format," Std. Track RFC 5444 (Proposed Standard), The Internet Engineering Task Force (IETF), February 2009. [Online]. Available: http://www.ietf.org/rfc/rfc5444.txt

[5] T. Clausen, C. Dearlove, and J. Dean, "Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)," Std. Track RFC 6130 (Proposed Standard), The Internet Engineering Task Force (IETF), April 2010. [Online]. Available: http://www.ietf.org/rfc/rfc6130.txt

[6] T. Clausen, C. Dearlove, P. Jacquet, and U. Herberg, "Optimized Link State Routing Protocol Version 2 (OLSRv2)," RFC 7181 (Proposed Standard), The Internet Engineering Task Force (IETF), April 2014. [Online]. Available: http://www.ietf.org/rfc/rfc7181.txt

[7] U. Herberg, T. Clausen, and C. Dearlove, "Integrity Check Value and Timestamp TLV Definitions for Mobile Ad Hoc Networks (MANETs)," RFC 7182 (Proposed Standard), The Internet Engineering Task Force (IETF), April 2014. [Online]. Available: http://www.ietf.org/rfc/rfc7182.txt

[8] U. Herberg, C. Dearlove, and T. Clausen, "Integrity Protection for the Neighborhood Discovery Protocol (NHDP) and Optimized Link State Routing Protocol Version 2 (OLSRv2)," RFC 7183 (Proposed Standard), The Internet Engineering Task Force (IETF), April 2014. [Online]. Available: http://www.ietf.org/rfc/rfc7183.txt

[9] U. Herberg, R. Cole, and T. Clausen, "Definition of Managed Objects for the Optimized Link State Routing Protocol Version 2," RFC 7184 (Proposed Standard), The Internet Engineering Task Force (IETF), April 2014. [Online]. Available: http://www.ietf.org/rfc/rfc7184.txt

[10] C. Dearlove, T. Clausen, and P. Jacquet, "Link Metrics for the Mobile Ad Hoc Network (MANET) Routing Protocol OLSRv2 - Rationale," RFC 7185 (Proposed Standard), The Internet Engineering Task Force (IETF), April 2014. [Online]. Available: http://www.ietf.org/rfc/rfc7185.txt

[11] J. Yi, U. Herberg, and T. Clausen, "Security Threats for the Neighborhood Discovery Protocol (NHDP)," RFC 7186 (Proposed Standard), The Internet Engineering Task Force (IETF), April 2014. [Online]. Available: http://www.ietf.org/rfc/rfc7186.txt

[12] C. Dearlove and T. Clausen, "Routing Multipoint Relay Optimization for the Optimized Link State Routing Protocol Version 2 (OLSRv2)," RFC 7187 (Proposed Standard), The Internet Engineering Task Force (IETF), April 2014. [Online]. Available: http://www.ietf.org/rfc/rfc7187.txt

[13] C. Dearlove and T. Clausen, "Optimized Link State Routing Protocol Version 2 (OLSRv2) and MANET Neighborhood Discovery Protocol (NHDP) Extension TLVs," RFC 7188 (Proposed Standard), The Internet Engineering Task Force (IETF), April 2014. [Online]. Available: http://www.ietf.org/rfc/rfc7188.txt

[14] C. Dearlove and T. Clausen, "An Optimization for the Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)," RFC 7466 (Proposed Standard), The Internet Engineering Task Force (IETF), March 2015. [Online]. Available: http://www.ietf.org/rfc/rfc7466.txt

[15] ——, "Multi-Topology Extension for the Optimized Link State Routing Protocol version 2 (OLSRv2)," Internet Draft, The Internet Engineering Task Force (IETF), Februray 2015. [Online]. Available: https://tools.ietf.org/html/draft-ietf-manet-olsrv2-multitopology

[16] J. Yi and B. Parrein, "Multi-path Extension for the Optimized Link State Routing Protocol version 2 (OLSRv2)," Internet Draft, The Internet Engineering Task Force (IETF), May 2015. [Online]. Available: https://tools.ietf.org/html/draft-ietf-manet-olsrv2-multipath

[17] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," RFC 2827, IETF, May 2000.

[18] F. Baker and P. Savola, "Ingress Filtering for Multihomed Networks," RFC 3704, IETF, March 2004.