Network Working Group T. Clausen
Internet-Draft LIX, Ecole Polytechnique
Intended status: Informational U. Herberg
Expires: October 16, 2014 Fujitsu Laboratories of America
April 14, 2014

Snapshot of OLSRv2-Routed MANET Management
draft-ietf-manet-olsrv2-management-snapshot-00

Abstract

This document describes how Mobile Ad Hoc Networks (MANETs) are typically managed, in terms of pre-deployment management, as well as rationale and means of monitoring and management of MANET routers running the routing protocol OLSRv2 and its constituent protocol NHDP. Apart from pre-deployment management for setting up IP addresses and security related credentials, OLSRv2 only needs routers to agree one single parameter (called "C"). Other parameters for tweaking network performance may be determined during operation of the network, and need not be the same in all routers. This, using MIB modules and related management protocols such as SNMP (or possibly other, less "chatty", protocols). In addition, for debugging purposes, monitoring data and performance related counters can be sent to the Network Management System (NMS) via standardized management protocols.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

The MANET routing protocol OLSRv2 [RFC7181], as well as its constituent parts NHDP [RFC6130], [RFC5497], [RFC5148], [RFC5444], [RFC7182], [RFC7183], is designed to autonomously maintain routes across a dynamic network topology. OLSRv2 is designed so as to minimize operator intervention throughout the duration of a network deployment, and to allow for heterogeneous configuration of routers within the same network deployment: most configuration values are either of local significance only (e.g., message jitter parameters) or, when they are not, are carried in control signals exchanged between routers (e.g., information validity time).

All the same, a small set of configuration options must be established in each router prior to deployment, with some requiring agreement among all the routers within the same deployment. Furthermore, throughout the duration of a network deployment, external management and monitoring of a network may be desirable, e.g., for performance optimization or debugging purposes.

1.1. Statement of Purpose

Deployments of OLSRv2 are diverse, and may include community networks, constrained environments, tactical networks, etc. Each such environment may present distinctly different requirements as to management and monitoring.

This document does therefore explicitly not pretend to provide an exhaustive description of how all OLSRv2 network deployments should be managed and monitored - and does, specifically, not prescribe any management model.

What this document does, however, is to present how some OLSRv2 network deployments are managed and monitored, using well-established management patterns and well-known protocols.

2. Terminology

This document uses terminology from [RFC7181], [RFC6130], and [RFC5497].

3. Pre-Deployment Management

Prior to operation of an OLSRv2 network, or more precisely, prior to proper operation of OLSRv2 and its constituent parts, certain parameters need to be configured on each router. The following

sections describe the required pre-deployment management.

3.1. Lower Layer Alignment

Interoperability between routers requires alignment of lower protocol layers below OLSRv2. In particular, all routers in the same MANET topology must be pre-configured to use the same IP address family (IPv4 or IPv6). In a single OLSRv2 topology, it is not possible to mix IPv4 and IPv6 addresses, notably because [RFC5444] messages can contain either IPv4 *or* IPv6 addresses, but not both at the same time. It is, however, possible to run two instances of OLSRv2, one instance for IPv4 and another one for IPv6, within the same network.

In addition to the IP address family, other lower layer parameters may also need to be aligned, e.g., radio channel selections. A single OLSRv2 topology may, of course, span different link layers (or the same link layer with different configuration settings such as cryptographic keys) when routers in the topology have OLSRv2 interfaces towards these different link layers.

3.2. Interface Addresses

According to [RFC6130], and as used by [RFC7181], each interface of a router must be configured with at least one IP address. [RFC6130] provides guidance as to the characteristics of such IP addresses, including the (limited) conditions under which an IP address may be configured on multiple interfaces.

While automatic configuration of IP addresses on router interfaces is

not excluded, currently no address autoconfiguration protocols have been standardized (in the IETF) to accomplish this. As a consequence, static configuration, or proprietary (as in: non-standardized) protocols ensure this.

Note that this required pre-deployment of interface addresses does not include "external" IP addresses, i.e., IP addresses that are configured on local non-MANET interfaces or IP addresses from remote destinations reachable through this router (i.e., addresses for which this router serves as gateway). These can be added or removed dynamically during runtime of OLSRv2. Such local non-MANET interface addresses are managed by way of the Local Interface Set (as defined in [RFC6130]) and remote addresses by way of the Attached Network Set (as defined in [RFC7181]).

3.3. Security Material

Security material (keys, algorithms, etc.) must be available for generating Integrity Check Values (ICVs) for outgoing control

messages, and to allow validating ICVs in incoming control messages [RFC7182] [RFC7183].

The appropriate way of making such security material available is dependent on the deployment type. For example, community networks (such as "Funkfeuer", http://funkfeuer.at), do currently not use any security at all. Other deployment types may use a simple manual shared key distribution mechanism, or may use a proprietary key distribution protocol. Tactical networks have much more stringent requirements for distributing key material, e.g., using manual distribution of the keys on encrypted USB keys, and with defensive mechanisms (up to and including mechanisms involving depleted uranium) if the keys are compromised.

In general, Automatic Key Management (AKM) as well as static/manual or other out-of-band mechanisms, can be viable options for distributing keys. Currently, no standardized AKM mechanism for MANETs exist. If the IETF standardizes such mechanisms in the future, for deployment types where such is appropriate, these can be used for distributing keys. Until such time, manual key distribution as well as proprietary mechanisms, prevail.

The important point to make here, however, is that by whichever method (automatic/manual, dynamic/static, ...) a key and other security material is made available, the security mechanisms of OLSRv2, as defined by [RFC7183], will be able to properly use it for generating and validating ICVs.

3.4. The Value of C

The only pre-deployment configuration parameter that directly impacts protocol operation is the value of C. This value is used by each router for calculating the representation of interval and validity time, as included in control messages. All routers in a deployment must agree on the value of C, as described in [RFC5497].

4. How do we Manage MANETs?

A deployed OLSRv2 network is, as previously discussed, operating autonomously, but occasionally with internal or external management operations being desirable, described in the following two sections.

4.1. Internal Management

Internal management describes a local process running on an router that automatically (i.e., without external messaging or human interaction) modifies the configuration of OLSRv2 based on different

environmental factors. For example, the HELLO interval may be updated according to the rate of topology changes measured (or, inferred: after all, the 'M' in MANET is for "Mobility") locally: if the rate is high, then a more frequent HELLO update assures that routes are more accurate. At a lower rate of topology changes, network capacity and energy capacity of the router may be conserved by increasing the HELLO interval.

Depending on the use case, many different automatic configuration agents can be envisioned. As parameters in NHDP and OLSRv2 are either only used locally or, in the case of HELLO_INTERVAL and REFRESH_INTERVAL, are selected locally and then included in the messages exchanged between adjacent routers in their HELLO messages, none of these automatic local configuration methods needs necessarily to be standardized: different routers doing different things will

interoperate.

4.2. External Management

For the deployments described by this document (but see Section 6), external management operations are undertaken by a central Network Management Station (NMS).

The MIB modules developed for OLSRv2 [RFC7184] and for its constituent protocol NHDP [RFC6779] are verbose, in as much as that they expose for interrogation the complete protocol and router state, as well as enable setting all parameters (timer intervals, time-outs, jitter values etc.). They do explicitly not enable setting the value of C (as that is required to be constant and uniform across the network, see Section 3.4), nor distributing security material (see Section 3.3).

In some deployments, the NMS communicates with individual routers by way of SNMP - and, more commonly, by way of "proprietary" simpler, less verbose and (often) less secure protocols, and over UDP. Note that this does not constitute a recommendation, but rather an observation that (apparently) SNMP has found less application in MANETs.

The predecessor of OLSRv2, OLSR [RFC3626] did not have an associated MIB module. Many deployments of OLSR did not support network management operations per se (i.e., configuration-on-launch was the way in which routers in these deployments were managed). Those implementations and deployments of OLSR that did support network management operations used a similar architecture to the one described in this document, but with "proprietary" protocols and APIs for parameters and router states, "proprietary" data-models, etc. It can be speculated that the "proprietary" protocols used for

communication between the NMS and the MIB modules on each router also for OLSRv2, in part, exist as inherited from the protocols used for OLSR.

Finally, it is uncommon to see an NMS permanently active in a deployed OLSRv2 network; rather, on an "ad hoc" basis an NMS is introduced into the network, parameters configured or state interrogated, following which the NMS disappears.

5. What and Why do we Manage and Monitor?

As indicated earlier, OLSRv2 and its constituent protocol NHDP, are reasonably robust with respect to parameter values: a deployment can operate with different parameters used in different routers in the same network. That being said, adapting these parameters according to circumstances is (often) desired. For example, in a stable network (such as a wired network), TC messages may be sent infrequently and with long validity times, whereas in a highly dynamic network (such as in a vehicular network) TC messages may need to be sent more frequently and HELLO messages for discovering the local topology (almost) continuously. In a similar vein, the message emission intervals and the information validity times should also be commensurate with the available network capacity: millisecond intervals between TC messages, for example, will consume all available network capacity whereas hourly intervals will be inappropriate even for a static and stable, wired, network (by way of simply new routers arriving in the network, which will not "learn" the network topology before undue long delays).

This adaptation may happen autonomously by a central NMS monitoring and adopting the parameters globally, autonomously by an NMS in each router, monitoring its local topology (and its stability) and adapting parameters locally, or by manual operator intervention.

Given the dynamic and evolutive topology of OLSRv2 networks, a highly desirable property of an NMS is the ability to display and offer visibility of the current network status - for example, to display a graphical map of which routers are currently part of the network. As a proactive protocol, OLSRv2 maintains, in each router, a topology map including all destinations and a subset of the links present in the network (particularly true in a very dense network). A typical feature of an NMS is to inquire as to the topology map of a single router. A slightly less typical feature is to inquire all (or, at least, many) routers in a network, with the purpose of presenting a complete topology map.

In addition to actively monitoring an OLSRv2 network, erroneous or

unusual conditions on an router can be flagged to management, e.g.,

detection of an unusually high number of 1-hop or 2-hop neighborhood changes in a short amount of time, indicating potential problems in that area of the network. [RFC6779] and [RFC7184] facilitate proactively sending "notifications" (also known as traps) from the router towards an NMS. The MIB modules defined in [RFC6779] and [RFC7184] allow for defining both the threshold and the time window of how many times this erroneous condition may occur in the time window before the notification is sent to the NMS. Once the NMS receives a notification, a network operator may investigate if there is a problem that needs to be resolved, e.g., by changing parameters via the above-described external management.

6. This Document does not Constrain how to Manage and Monitor MANETs

As explained in Section 1, this document describes how, what and why some (typical) OLSRv2 networks are managed and monitored as of early 2014. As such, the document is reflexive, not prescriptive: it does not stipulate requirements for how to manage OLSRv2 networks, nor does it claim to be a complete list of all management patterns or protocols. Other ways of managing an OLSRv2 network are very well imaginable - now, or in future deployments of OLSRv2.

As an example of such a "future management scenario", rather than managing and monitoring routers from a central NMS, a distributed, autonomous management system between multiple routers can be envisioned. In particular, monitoring data that is used to debug network problems and to tweak inefficiencies could be distributed amongst a group of routers in the same network. This would both address problems of single point of failure when using only a single NMS, as well provide additional information about groups of multiple routers, rather than a single router. An example use for such a distributed information flow would be to identify areas of a network wherein, e.g., due to different router densities, message sending interval parameters could be exchanged and optimal values negotiated between routers, so as to obtain locally optimized performance.

While such a management model is highly interesting, it is also at present entirely fictional - at least outside the realm of research. It is included to, both, indicate directions being explored (but not exploited), and to insist that the intent of this document is not to prescribe how MANETs are to be managed, in the presence or in the future, but to describe the (known) state of how MANETs are managed, presently.

7. Acknowledgments

The authors would like to gratefully acknowledge the following people for intense technical discussions, early reviews, and comments on the documents: Alan Cullen (BAE Systems), Christopher Dearlove (BAE Systems), and Adrian Farrel (Juniper).

8. Informative References

[RFC3626] Clausen, T. and P. Jacquet, "The Optimized Link State Routing Protocol", RFC 3626, October 2003.

[RFC5148] Clausen, T., Dearlove, C., and B. Adamson, "Jitter Considerations in Mobile Ad Hoc Networks (MANETs)", RFC 5148, February 2008.

[RFC5444] Clausen, T., Dearlove, C., Dean, J., and C. Adjih, "Generalized MANET Packet/Message Format", RFC 5444, February 2009.

[RFC5497] Clausen, T. and C. Dearlove, "Representing Multi-Value Time in Mobile Ad Hoc Networks (MANETs)", RFC 5497, March 2009.

[RFC6130] Clausen, T., Dearlove, C., and J. Dean, "Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)", RFC 6130, April 2011.

[RFC6779] Herberg, U., Cole, R., and I. Chakeres, "Definition of Managed Objects for the Neighborhood Discovery Protocol", RFC 6779, May 2012.

[RFC7181] Clausen, T., Dearlove, C., Jacquet, P., and U. Herberg, "The Optimized Link State Routing Protocol Version 2", RFC 7181, April 2014.

[RFC7182] Herberg, U., Clausen, T., and C. Dearlove, "Integrity Check Value and Timestamp TLV Definitions for Mobile Ad Hoc Networks (MANETs)", RFC 7182, April 2014.

[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, April 2014.

[RFC7184] Herberg, U., Cole, R., and T. Clausen, "Definition of Managed Objects for the Optimized Link State Routing

Protocol Version 2", RFC 7184, April 2014.

Authors' Addresses

Thomas Clausen
LIX, Ecole Polytechnique
91128 Palaiseau Cedex,
France

Phone: +33-6-6058-9349
Email: T.Clausen@computer.org
URI: http://www.thomasclausen.org

Ulrich Herberg
Fujitsu Laboratories of America
1240 E Arques Ave
Sunnyvale CA 94086,
US

Phone:
Email: ulrich@herberg.name
URI: http://www.herberg.name