INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

MANET Network Management and Performance Monitoring for NHDP and OLSRv2

Ulrich Herberg Thomas Clausen, Robert Cole.

N° 7311

June 2010

Rapport de recherche

ISSN 0249-6399 ISRN INRIA/RR--7311--FR+ENG

INSTITUT NATIONAL
DE RECHERCHE
EN INFORMATIQUE
ET EN AUTOMATIQUE

INRIA

centre de recherche
SACLAY – ÎLE-DE-FRANCE

MANET Network Management and Performance Monitoring for NHDP and OLSRv2

Ulrich Herberg[*] Thomas Clausen[†], Robert Cole[‡].

Thème : COM – Systèmes communicants
Équipe-Projet Hipercom

Rapport de recherche n° 7311 — June 2010 — 19 pages

Abstract: Mobile Ad Hoc NETworks (MANETs) are generally thought of as infrastructureless and largely "un-managed" network deployments, capable of accommodating highly dynamic network topologies. Yet, while the network infrastructure may be "un-managed", monitoring the network performance and setting configuration parameters once deployed, remains important in order to ensure proper "tuning" and maintenance of a MANET. This memorandum describes a management framework for the MANET routing protocol OLSRv2, and its constituent protocol NHDP. It does so by presenting considerations for "what to monitor and manage" in an OLSRv2 network, and how. The approach developed is based on the Simple Network Management Protocol (SNMP), and thus this paper details the various Management Information Bases (MIBs) for router status monitoring and control – as well as a novel approach to history-based performance monitoring. While SNMP may not be optimally designed for MANETs, it is chosen due to it being the predominant protocol for IP network management – and thus, efforts are made in this paper to "adapt" the management tools within the SNMP framework for reasonable behavior also in a MANET environment.

Key-words: OLSRv2, MANET, management, control, MIB, SNMP

[*] LIX - Ecole Polytechnique, Ulrich@Herberg.name
[†] LIX - Ecole Polytechnique, Thomas@ThomasClausen.org
[‡] Space and Terrestrial Communications - US Army CERDEC - Aberdeen Proving Ground, MD, USA 21005 - robert.g.cole@us.army.mil

Centre de recherche INRIA Saclay – Île-de-France
Parc Orsay Université
4, rue Jacques Monod, 91893 ORSAY Cedex
Téléphone : +33 1 72 92 59 00

MANET Network Management and Performance Monitoring for NHDP and OLSRv2

Résumé : Lorsquon parle de réseaux mobiles ad-hoc (MANETs), on pense généralement à des réseaux sans infrastructure et à des déploiements en réseaux largement non-gérés, pouvant sadapter à des topologies de réseau très changeantes. Néanmoins, bien que linfrastructure du réseau est de nature non-gérée, la surveillance des performances du réseau et le choix des paramètres de configuration une fois le réseau déployé demeurent primordiaux pour la maintenance et le réglage fin dun réseau MANET. Ce mémorandum décrit une plateforme de gestion pour le protocole de routage OLSRv2 des réseaux MANETs, ainsi que le protocole NHDP constitutif des réseaux MANETs. Il présente les considérations à tenir compte dans le choix de ce quil faut surveiller et gérer dans un réseau OLSRv2 et comment le faire. Lapproche développée est basée sur SNMP (Simple Network Management Protocol). Ainsi cet article dresse une liste détaillée de MIBs (Management Information Bases) pour la surveillance et le contrle des routeurs, mais présente aussi une nouvelle approche tournée vers la surveillance des performances basées sur lhistorique des données. Bien que SNMP ne soit pas idéal pour les réseaux MANETs de par sa conception, son choix repose sur sa prédominance dans le domaine de la surveillance réseau. Ainsi, les efforts sont effectués dans cet article pour adapter les outils de gestion présents dans SNMP à lenvironnement MANET tout en gardant un fonctionnement correct.

Mots-clés : OLSRv2, MANET, management, control, MIB, SNMP

1 Introduction

Mobile Ad hoc Network (MANET) routing protocols are commonly assumed to be entirely self-managing: routers, running such a distributed protocol, perceive the topology of the MANET by means of control message exchange. Any change to the topology is reflected in the local routing tables of each router after a bounded convergence time, which allows forwarding of data traffic towards its intended destination. Usually, no human interaction is required, as all variable parameters required by the routing protocol are either negotiated in the control traffic exchange, or are only of local importance to each router (*i.e.* do not influence interoperability). However, external management and monitoring of a MANET routing protocol may be desirable to optimize parameters of the routing protocol. Such an optimization may lead to a more stable perceived topology and to a lower control traffic overhead, and therefore to a higher delivery success ratio of data packets, a lower end-to-end delay, and less unnecessary bandwidth and energy usage. This memorandum proposes a management framework to manage and control performance related objects on MANET routers running the Optimized Link State Routing Protocol version 2 (OLSRv2), which is currently in the process of being standardized by the MANET working group of the IETF[1].

1.1 OLSRv2 Overview

The Optimized Link State Routing Protocol version 2 (OLSRv2) [2, 3, 4, 5, 6] is a successor to the widely deployed OLSR [1] routing protocol for MANETs. OLSRv2 retains the same basic algorithms as its predecessor, however offers various improvements, *e.g.* a modular and flexible architecture allowing extensions, such as for security, to be developed as add-ons to the basic protocol. OLSRv2 contains three basic processes: Neighborhood Discovery, MPR Flooding and Link State Advertisements. The basic operation of OLSRv2 is illustrated in figure 1 and is detailed in section 1.1.1-1.1.3 below, followed by a description of the flexible message format used by OLSRv2, in section 1.1.4, and a discussion of the configuration and operation of OLSRv2 routers in section 1.1.5.

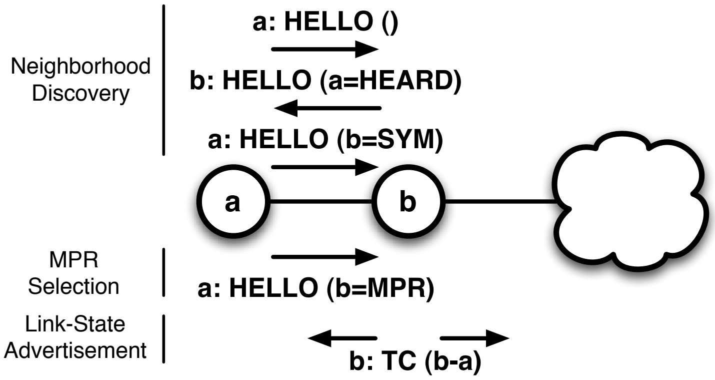

Figure 1: Basic OLSRv2 Operation

---

[1] The Internet Engineering Taskforce: http://www.ietf.org

1.1.1 Neighborhood Discovery (NHDP)

The process, whereby each router discovers the routers which are in direct communication range of itself (1-hop neighbors), and detects with which of these it can establish bi-directional communication. Each router sends HELLOs, listing the identifiers of all the routers from which it has recently received a HELLO, as well as the "status" of the link (HEARD, verified bi-directional – called SYM). A router a receiving a HELLO from a neighbor b in which b indicates to have recently received a HELLO from a considers the link a-b to be bi-directional. As b lists identifiers of all its neighbors in its HELLO, a learns the "neighbors of its neighbors" (2-hop neighbors) through this process. HELLOs are sent periodically, however certain events may trigger non-periodic HELLOs. NHDP enables each router interface to apply a *hysteresis function* which, in addition to the message exchange, may constrain when a link is considered as "usable" or not: for example, a router may elect to not consider, and thus not advertise, a link as SYM or HEARD unless a certain ratio of HELLOs are received, unless the SNR reaches a given threshold etc. Symmetrically, a router may decide to stop advertising a link as SYM or HEARD, subject to similar such constraints. [5] specifies a general framework for a router to implement such a strategy, by way of two thresholds (HYST_ACCEPT and HYST_REJECT) and a link quality value (L_quality). These are used, but not set, by the process in NHDP determining the "link status".

1.1.2 MPR Flooding

The process whereby each router is able to, efficiently, conduct network-wide broadcasts. Each router designates, from among its bi-directional neighbors, 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 neighbors (*i.e.*, the MPR set *"covers"* all 2-hop neighbors). MPR selection is encoded in outgoing HELLOs. The set of routers having selected a given router as MPR is the MPR-selector-set of that router. A study of the MPR flooding algorithm can be found in [7].

1.1.3 Link State Advertisement

The process whereby routers are determining which link state information to advertise through the network. Each router must advertise links between itself and its MPR-selector-set, in order to allow all routers to calculate shortest paths. Such link state advertisements, carried in TC messages, are broadcast through the network using the MPR Flooding process. As a router selects MPRs only from among bi-directional neighbors, links advertised in TCs are also bi-directional. TC messages are sent periodically, however certain events may trigger non-periodic TCs. In order to be able to discriminate between fresh and stale information, Link State Advertisements, emitted by a given router, include a sequence number incremented each time that router changes the set of links advertised.

1.1.4 Flexible Message Format

OLSRv2 employs the format specified in [3], for all protocol messages, thereby enabling scope-limited message flooding, compact (aggregated) address representation, also of non-contiguous network addresses, and the ability to associate any number of arbitrary attributes to either of control messages or addresses, by way of inclusion of Type-Length-Value objects (TLVs). The TLV structure permits any given message to be parsed correctly by allowing an implementation to "skip over" TLVs not recognized, thus enabling extensions to be developed that embed information into existing OLSRv2 control messages. The TLV structure is used by OLSRv2, *e.g.* for indicating MPR selection in HELLO messages, or for indicating message emission intervals and the duration for which the content of a message is valid, by way of including TimeTLVs [4].

1.1.5 OLSRv2 Router Configuration

The configuration of an OLSRv2 router consists of the set of prefixes "owned", and thus advertised, by the router, as well as interfaces of that router, participating in the OLSRv2 routing protocol. For each such interface, a set of parameters apply; other than the IP address(es) of each interface, these parameters consist of control message emission intervals, as well as the hysteresis values and link quality estimation, for setting the link status as described in section 1.1.1. It is important to note that agreement between OLSRv2 routers on the values for any of these is not required for interoperability. Link quality and hysteresis affect only which links a given router permits to become SYM or HEARD. Control message emission intervals and message content validity are encoded in outgoing control messages, by way of TLVs, such that a recipient router correctly can process these regardless of its own configuration.

As it would be, the only value upon which agreement is required between OLSRv2 routers in the same network is C – the "time granularity" parameter, specified in [4].

1.2 Memorandum Outline

The remainder of this memorandum is organized as follows: Section 2 outlines related efforts on management of MANETs as well as wireless sensor networks. Section 3 gives a brief overview of SNMP. Section 4 describes the motivation for the proposed SNMP-based management framework for OLSRv2-routed MANETs. The architecture of this framework is presented in section 5. Section 6 describes the construction and functioning of NHDP and OLSRv2 MIBs, while section 7 proposes the related REPORT-MIB – a convenient tool for performance management. This memorandum is concluded in section 8.

2 Related Work

A number of papers analyze different approaches to monitor and to control MANETs as well as wireless sensor networks (WSN). Since the Simple Network Management Protocol (SNMP) [8] is the prevailing management system for networks, many solutions propose SNMP-derived protocols or SNMP extensions for MANETs and WSNs.

[9] proposes a distributed policy-based network management system for MANETs called DRAMA. Based on different policy levels, a hierarchy of management agents is established. In order to facilitate the hierarchy to systematically and autonomously self-form in MANETs, DRAMA enables routers to

form "clusters" and then to link clusters into a tree-like hierarchy, with one cluster-head per cluster. The framework specifies a cluster maintenance system to assure keep-alives from routers within the cluster and to limit the size of the cluster within reasonable boundaries. DRAMA is compared to SNMP in a simulations study, which shows that DRAMA scales better than SNMP in MANETs (in terms of message overhead, timeliness of message delivery and message delivery ratio).

The authors of [10] claim that using proxy-SNMP has several limitations, and that therefore native SNMP should be supported. The paper describes an extended modification of the SNMP protocol for enabling 802.15.4 based networks (denoted 6LoWPAN) to provide efficient management capabilities, based on header and payload compression, as well as multicast SNMP messages and periodic message dissemination. Results have shown that using this extension, the overhead can be reduced by about 50% and that 6LoWPAN-SNMP can be successfully deployed in small sensor networks.

Another approach to allow management of constrained, mobile wireless routers, is [11]. The paper proposes a management tool for WSN based on SNMP: LiveNCM. LiveNCM introduces the concept of non-invasive context-awareness to diagnose the wireless sensor node state in order to reduce the network traffic and the local state on a router. Similar to [10], LiveNCM suggests compression of messages.

While SNMP typically allows to control and to manage a single router, some solutions propose to aggregate SNMP messages using multicast to several routers, such as [12]. This allows to control simple parameters of several routers with a single SNMP message, and also to monitor the state of the routers using aggregated messages. Similarly, [13] suggests a probabilistic scheme for managing only a subset of routers in the MANET, "such that we capture the most *interesting* nodes into the management", where *interesting* is defined with respect to relative good network presence and topology relationship.

Finally, several papers focus on managing MANETs based on particular routing protocols. [14] and [15] specify a MIB for the OLSR [1] routing protocol, allowing to set the protocol parameters and to monitor the state of the router (such as the neighbor and routing set tables).

3 A Brief SNMP Primer

Although it is recognized that the Simple Network Management Protocol (SNMP) [16] is not optimally designed for operation over MANETs, it is the preeminent management protocol for managing IP networks. As such, the management architecture for OLSRv2 routed MANETs is based hereupon.

SNMP consists of a standardized way of exposing management data (system configuration, performance measurements, etc.) by way of defining a set of *objects* on the *managed devices*. These objects may then be read and, if appropriate, set in a standardized manner. This, by way of a *Network Management System* communicating with an *agent* on the managed device – in this case, an OLSRv2 router. SNMP does not mandate that a device must present a specific set of objects to read or set, but rather defines a standardized way in which a device may present such objects – a Management Information Base (MIB). A

Structure of Management Information (SMI) defines modules of related management objects within such a Management Information Base.

Three versions of SNMP have been specified, developed and extensively deployed. Initially, SNMPv1 [16] specified a set of basic network management capabilities, including a relatively simple security model. SNMPv2 [17] was developed to extend SNMP capabilities and to improve the basic security model. However, it was not until the development of SNMPv3 [18] that an acceptable security model was developed [19, 20]. The Structure of Management Information version 2 (SMIv2) [21] is the current version of SMI. Using SMI, developers design and describe the management model for the system, protocol or device being managed. SMIv2 allows for the definition of fairly complex management models, yet allows for simplicity of chosen implementations through the definition of *Compliance statements* within the MIB.

It is useful to structure the MIBs according to a set of associated management functions. Further, it is useful to define the management objects, comprising the set of management functions, into basic management objects and more complex management objects. By doing so, the designer can specify through the Compliance statements a relatively simple version of the MIB for base management functions and a more complex and complete MIB for complete management of the managed device. An example where this structure may be useful is in the area of configuration management. It is common amongst most public IP carriers to perform configuration management through methods other than SNMP, *e.g.*, direct command line interfaces to remote devices. Therefore, following the outlined approach for structuring MIBs, one could define a compliant MIB which provided State, Performance and Fault Management functions while deferring Configuration Management to other methods. At the time of this writing, the IETF is in the process of specifying a new management protocol, *i.e.*, NETCONF [22], and a new information modeling language, *i.e.*, YANG [23], specifically for configuration management[2].

4 Problem Statement: Managing OLSRv2 Networks

As indicated in section 1.1.5, OLSRv2 imposes very minimal constraints on valid router configuration parameters, in order for OLSRv2 routers to interoperate.

Fundamentally, the only parameter upon which agreement is required is C – a constant, used to fix the scale and granularity of validity and interval time values, as included in protocol control messages. [4] proposes a value for this constant; the symbol C is chosen to indicate it to be a "constant of nature" inside an OLSRv2 network, to which all routers must adhere. As control messages carry validity time and interval time values, a recipient OLSRv2 router can behave appropriately, even if it uses vastly different values itself, as long as the recipient and sender use the same value for C.

Link admittance, by way of the hysteresis values and link quality estimation, require no agreement; these are used for an individual router to determine a suitable threshold for "considering that a link *could* be a candidate for being advertised as usable".

---

[2] The IETF has approved YANG [23] for publication as Proposed Standard on June 9, 2010

Still, external monitoring and management may be desirable in an OLSRv2 network. A network may benefit from having its control message emission tuned according to the network dynamics: in a mostly static network, *i.e.* a network in which the topology remains stable over long durations, the control message emission frequency could be decreased in order to consume less bandwidth or less energy. Conversely, of course, in a highly dynamic network, the emission frequency could be increased from improved responsiveness. Concerning the hysteresis and link quality estimation, a management application might detect a region of an OLSRv2 network with a high link density – but also a high degree of "flapping": links coming "up" (SYM) only to disappear as LOST shortly thereafter. Detecting such behavior, on a global level and for multiple routers in the same region, could enable appropriately "tuning" the thresholds towards more stable links and, thus, a more stable routing structure in the network.

These are but two examples, and have as common that a more "global view" of the network, than that of a single OLSRv2 router, is required – *i.e.* entail that a *Network Management System* is able to inquire as to various performance values of the network, and to set various router parameters.

Thus, a first-order task is to identify suitable management data for an OLSRv2 routed MANET, and to describe these by way of MIBs for use by an SNMP Network Management System.

In the following sections, the proposed MIBs for managing OLSRv2 networks and monitoring performance of these networks are described in detail.

5 OLSRv2 Management Architecture

The proposed architecture of the OLSRv2 management system is depicted in figure 2. As is standard for SNMP management architectures, a Network Management System interacts with the various components of the device models directly over the network. However, frequent polling for object values in such a system involves a frequent and bandwidth-consuming message exchange. Further, due to highly variable network delays, it is not possible for a management application to determine the time associated with object values obtained via polling. In order to specifically address the issues associated with running SNMP for Performance Management over low bandwidth and high latency networks, typical of MANETs, the proposed Performance Management architecture is based upon a proxy capability, denoted REPORT-MIB [24]. This proxy is located in close proximity to the managed devices and offers remote generation of performance reports established via the management application using Remote Monitoring (RMON) style control and reporting. The proxy then polls (locally) for the current values of the relevant objects necessary for the generation of the performance reporting.

6 NHDP and OLSRv2 MIBs

This section describes the design of the NHDP-MIB [25] and the OLSRv2-MIB [26]. As the protocols themselves are designed in a similar fashion, so are their associated MIBs. At the highest level, both the NHDP-MIB and the OLSRv2-MIB are organized into the following groups:

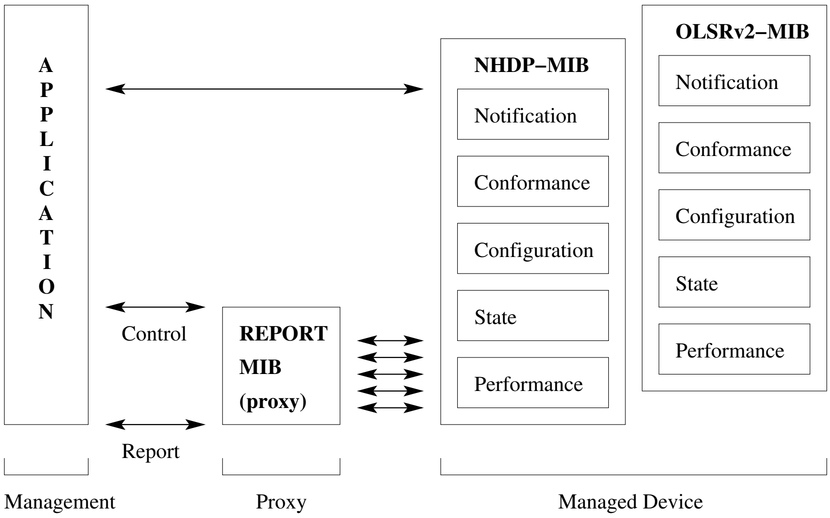

Figure 2: The OLSRv2 management model

- Configuration Group – switches, tables, objects which are initialized to default settings or set through the management interface defined by this MIB.
- State Group – automatically generated object values which define the current operating state of the NHDP or OLSRv2 protocol process in the router.
- Performance Group – automatically generated object values which help an administrator or automated tool to assess the performance of the protocol process on the router and the overall performance within the routing domain.
- Notification Group – objects defining triggers and associated notification messages allowing for asynchronous tracking of pre-defined events on the managed device.
- Conformance Group – groupings of the above objects defining various levels compliance to the MIBs.

The Configuration Group for the NHDP-MIB and OLSRv2-MIB includes objects which control message intervals (*e.g.* for HELLOs), information validity times (*e.g.* hold times), link quality (*e.g.* thresholds to determine usefulness of the links), and message jitter. For the OLSRv2-MIB, additional configuration information include objects related to hop limits and routers' willingness measures to act as Multi-Point Relays (MPRs). Details on the actions these objects have on the respective protocols are found in [5] and [6].

Regarding the State Group, both protocols are defined in terms of the various databases developed by the protocols in order for their proper function. These (state) databases include the following set for the NHDP protocol:

- The Local Information Base (LIB), contains the network addresses of the interfaces (MANET and non-MANET) of the local router.
- The Interface Information Based (IIB), records information regarding links to a local MANET interface and symmetric 2-hop neighbors which can be reached through such links.
- The Neighbor Information Base (NIB), records information regarding current and recently lost 1-hop neighbors of the local router.

The OLSRv2 protocol extends the above databases, as well as defines the following additional databases:

- The Topology Information Base (TIB), records information used for the calculation of the Routing Set.
- The Received Message Information Base (RMIB), records information regarding messages, that have been previously received, processed, or forwarded by the local router.

The state tables in the OLSRv2 and NHDP MIBs are linked through two constructs (or TEXTUAL CONVENTIONS) developed within the MIBs as illustrated in figure 3. Within the NHDP and OLSRv2 protocol definitions, the various Information Bases provide information on discovered address sets, which are associated with discovered interfaces, which belong to discovered (or local) routers. These are used as indexes into the various State Tables; specifically as *IpAddr*, *DiscNeighborIfIndex* and *DiscNeighborRouterId*. And these objects are correlated through the *nhdpDiscIfSetTable* in the NHDP-MIB. Further, as the related State Tables rely on the same indexing, it is relatively straightforward for a network management application to cross-reference data from the two MIBs.

Finally, the MIBs define two levels of Conformance; a Basic Compliance which includes only Configuration Group objects and a Full Compliance which includes Configuration, State, Performance and Notification Group objects.

7 Performance Management

Apart from objects for monitoring and controlling parameters and data sets in NHDP and OLSRv2 (specified in section 6), we propose a number of objects which permit to analyze the performance of NHDP and OLSRv2. This section describes the different types of objects and their intent for NHDP and OLSRv2.

7.1 Object Types

Some of the objects (denoted “base objects”) explicitly appear in the NHDP-MIB and OLSRv2-MIB while others are obtainable through a combination of base objects from the MIB and reports available through the REPORT-MIB.

The full list of base objects in the NHDP-MIB and the OLSRv2-MIB is comprised of different counters (*e.g.* for counting the total number of transmitted HELLO messages, number of changes to the neighbor set and to the 2-hop set, up-times of neighbor routers, etc.).

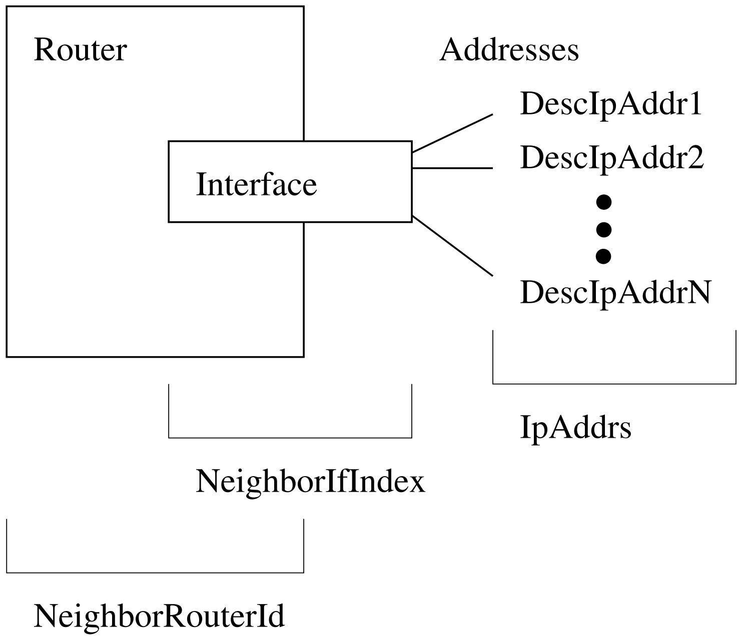

Figure 3: The linkage between the OLSRv2 and the NHDP MIBs

In order to infer performance problems in an OLSRv2 network, it may not be sufficient to access objects describing the total number of events, but objects describing the development of events over time. These objects, denoted "derived objects", are not specified in the NHDP-MIB and OLSRv2-MIB, but can be acquired using the REPORT- MIB. The REPORT-MIB allows to create reports "offline", possibly on another, more powerful device than the router running NHDP and OLSRv2. Notably, histories (based on timestamps) can be created over all of the performance related base objects.

For example, it is possible to create a histogram of intervals between transmitted HELLO messages, separated by periodic and triggered HELLOs. The histogram would display the distribution of intervals between two consecutive HELLOs of the same type (triggered or periodical) using a given bin size. Figure 4 depicts such a histogram.

Moreover, the NHDP- and OLSRv2 MIBs in combination with the REPORT-MIB allow to display the changes of the frequency by displaying the changes of histograms over time. The total duration of recorded events is split into a given number of equal bins. Then, a histogram is created for each bin and the "distances" are calculated between each two adjacent histograms in time (using the Bhattacharyya distance [27]). Note that while visualizing a change in the frequency of events may help the network administrator to understand changing properties of the network, it is out of scope of the MIB, and of this memorandum , to automatically determine whether such a change indicates a performance problem or is part of the natural change of topology of the network.

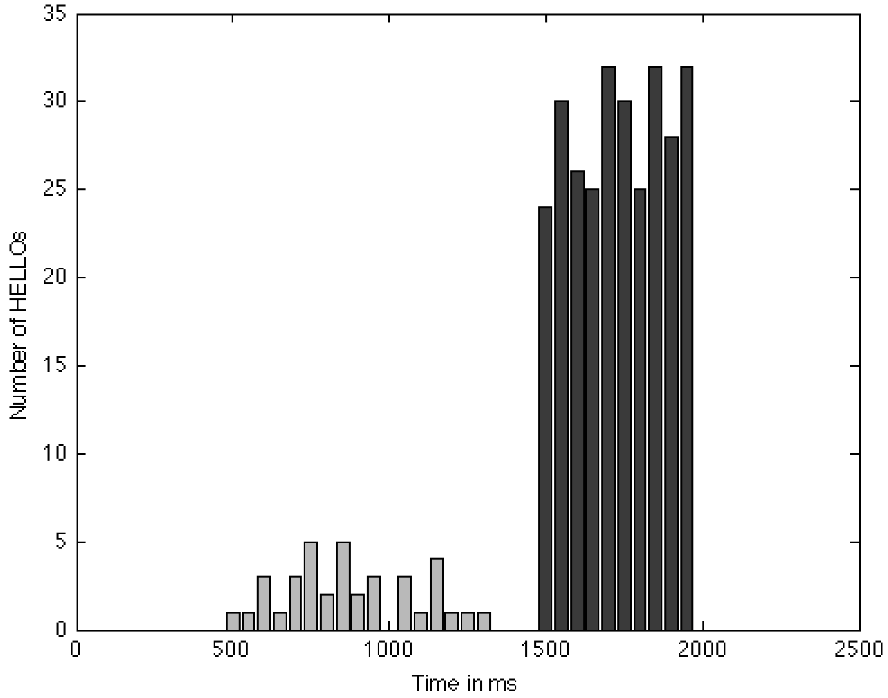

Figure 4: Example histogram: number of periodic (dark gray, between 1500ms and 2000ms) and triggered (light gray, between 500ms and 1500ms) HELLOs in 500s time, with a HELLO interval of 2000ms and a maximum jitter value of 500ms

7.2 Derived Objects in NHDP and OLSRv2

As described in section 7.1, changes of the frequency of certain events may indicate performance issues in the MANET. Notably unstable neighbors or 2-hop neighbors and frequent changes of sets may have a negative influence on the performance of NHDP and OLSRv2, wherefore a number of derived objects have been specified in the MIBs that allow management applications to acquire information related to the stability of NHDP and OLSRv2. The following list describes several derived objects from the MIBs that are relevant for NHDP and OLSRv2 networks:

7.2.1 Frequency changes of message scheduling

A change in the message scheduling frequency can appear if, for example, suddenly many triggered HELLO or TC messages are sent, whereas only very few such triggered messages were sent in the past. This can indicate a sudden change in the topology experienced by a router.

7.2.2 Frequency changes of Neighbor Set modifications

This derived object allows to visualize the changes of frequency of neighbor set modifications. A neighbor set modification is defined as a new neighbor that is added, a neighbor that is removed, or a neighbor that changes its symmetry status. If, for example, there are five changes of the neighbor set per minute in average, and then this frequency is increased to 100 changes per minute, this can indicate a performance problem.

7.2.3 Frequency of changes of the online status of a given neighbor

If a neighbor (identified by its IP address) changes its "online" status very frequently (*i.e.* a neighbor tuple for that neighbor is alternatively added and removed again in a very short time), this may indicate a performance problem.

7.2.4 Frequency of changes of the online status of a given 2-hop neighbor

Similar to the frequency of changes of the online status of a neighbor, a derived object in the MIB allows to track the frequency of change of the online status of 2-hop neighbors.

7.2.5 Frequency of changes of the link over which a neighbor is reachable

If a neighbor changes the interface over which it is reachable very frequently, that can cause performance issues: (i) more in-router resources for updating the internal data structures, and (ii) additional control traffic messaging may be required (*e.g.* when sending triggered HELLO messages).

The example in figure 5 depicts such a "flapping" of a neighbor between several links. Router A has two interfaces over which it can communicate with router B. If the corresponding link tuple for the neighbor frequently switches between interface 1 and 2, the above-mentioned performance issues may arise.

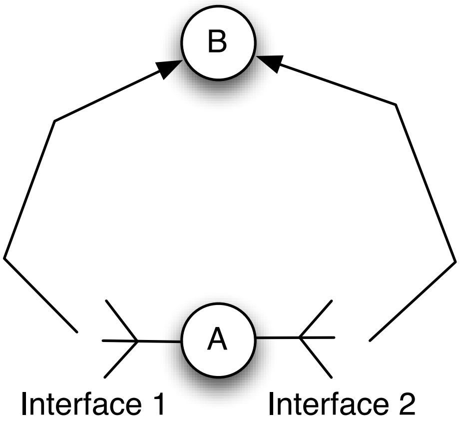

Figure 5: Router flapping between several interfaces

Such flapping of a neighbor may, for example, stem from inappropriate hysteresis values of the link quality selection of NHDP. Analyzing the frequency of neighbor flaps facilitates to modify the values to stabilize the link formation and removal on the OLSRv2 interfaces.

7.2.6 Frequency of changes of the neighbor over which a 2-hop neighbor is reachable

Similar to the link-flapping of a neighbor as described above, a two-hop neighbor can flap between several one-hop neighbors, as depicted in the example in figure 6.

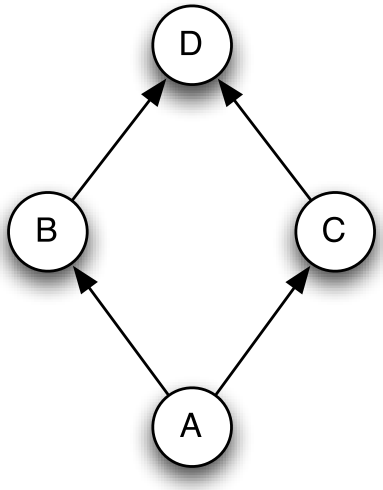

Figure 6: 2-hop router flapping between several neighbors

In addition to the in-router resource requirements for updating the internal data structures, this flapping between neighbors can – in the worst case – induce (i) routing set recalculation on all routers in the MANET, (ii) MPR set recalculations in the 2-hop neighborhood, and (iii) transmission of triggered HELLO and TC messages. The reason is that each time the 2-hop neighbor flaps between neighbors, a new MPR selection may be necessary. In the example, router A might initially have selected B as MPR in order to reach D. If A is forced to switch the MPR to C because B is not available any more, TC messages with the updated topology information will be disseminated throughout the network, forcing every router to recalculate its routing set.

7.2.7 Frequency of routing set recalculations and MPR set recalculations

The MIB provides two derived objects for observing routing-set- and MPR-set recalculations over time. Both operations are costly in terms of in-router resources (such as memory and CPU time), and too frequent recalculations may reduce the life-time of the MANET when using battery-powered routers. The MIB objects allow an administrator to "tune" parameters of OLSRv2 in order to reduce the number of unnecessary recalculations.

8 Conclusion

The MANET routing protocol OLSRv2 does not require any external interaction once deployed, as routers are able to accommodate frequently changing network topologies in a self-organizing manner, as well as to accommodate OLSRv2 routers with heterogenous configuration in the same network. However, it is often desirable to monitor the network performance and to "tweak" parameters for improving the performance of an existing deployment of the routing protocol. This memorandum proposes a management and monitoring architecture for OLSRv2 routers based on SNMP, which allows a Network Management System (possibly used by a human or automated network operator) (i) to acquire the state of the router (*i.e.* all parameters and information bases of the routing protocol), (ii) to modify parameters during runtime, and (iii) to generate offline performance reports. As for (i) and (ii), two Management Information Bases (MIBs) are proposed for OLSRv2 and for the neighborhood discovery part of OLSRv2, called NHDP. (iii) is derived through the creation of an external proxy service, the REPORT-MIB, located in close proximity of the managed devices where it may poll for the current values necessary for generation of the performance reporting. The rationale for this proxy service, which typically runs on the same machine as the agents (exposing the information defined by the OLSRv2-MIB and NHDP-MIB), is to avoid frequent polling over the network, leading to a frequent and bandwidth-consuming message exchange.

The REPORT-MIB does polling of counters from the OLSRv2-MIB and NHDP-MIB, and creates history-based performance reports based on these counters over time – reports which, then, are made available via SNMP. This memorandum specifies a number of such performance reports that concern the stability of the nearby topology of a router. When some of the router parameters in OLSRv2 and NHDP (such as the link quality related parameters) are unwisely set with respect to the characteristics of a given network, the local topology may “flap” between several possible configurations, thus leading to additional control traffic overhead, in-router calculations and deteriorated performance. Detecting such behavior, on a global level and for multiple routers in the same region, could enable appropriately “tuning” the parameters towards a more stable routing structure in the network.

References

[1] T. Clausen, P. Jacquet, “RFC3626: Optimized Link State Routing Protocol (OLSR)”, Experimental, http://www.ietf.org/rfc/rfc3626.txt

[2] T. Clausen, C. Dearlove, B. Adamson, “RFC5148: Jitter Considerations in Mobile Ad Hoc Networks (MANETs)”, Informational, http://www.ietf.org/rfc/rfc5148.txt

[3] T. Clausen, C. Dearlove, J. Dean, C. Adjih, “RFC5444: Generalized Mobile Ad Hoc Network (MANET) Packet/Message Format”, Std. Track, http://www.ietf.org/rfc/rfc5444.txt

[4] T. Clausen, C. Dearlove, “RFC5497: Representing Multi-Value Time in Mobile Ad Hoc Networks (MANETs)”, Std. Track, http://www.ietf.org/rfc/rfc5497.txt

[5] T. Clausen, C. Dearlove, J. Dean, “I-D: MANET Neighborhood Discovery Protocol (NHDP)”, Work In Progress, http://tools.ietf.org/id/draft-ietf-manet-nhdp-12.txt

[6] T. Clausen, C. Dearlove, P. Jaquet, “I-D: The Optimized Link State Routing Protocol version 2 (OLSRv2)”, Work In Progress, http://tools.ietf.org/id/draft-ietf-manet-olsrv2-11.txt

[7] A. Qayyum, L. Viennot, A. Laouiti, “Multipoint relaying: An efficient technique for flooding in mobile wireless networks”, 35th Annual Hawaii International Conference on System Sciences (HICSS), 2001

[8] D. Levi, P. Meyer, B. Stewart, “RFC3413: Simple Network Management Protocol (SNMP) Applications”, Std. Track, http://www.ietf.org/rfc/rfc3413.txt

[9] C. Chiang *et. al.*, “Performance Analysis of DRAMA: A Distributed Policy-Based System for Manet Management”, Military Communications Conference (MILCOM), 2006

[10] H. Choi, N. Kim, H. Cha, “6LoWPAN-SNMP: Simple Network Management Protocol for 6LoWPAN”, 11th IEEE International Conference on High Performance Computing and Communications (HPCC), 2009

[11] A. Jacquot *et. al.*, “A new approach for Wireless Sensor Network management: LiveNCM”, New Technologies, Mobility and Security (NTMS), 2008

[12] G. Kuthethoor *et. al.*, “Performance analysis of SNMP in airborne tactical networks”, IEEE Military Communications Conference (MILCOM), 2008

[13] R. Badonnel, R. State, O. Festor, “Probabilistic Management of Ad-Hoc Networks”, Network Operations and Management Symposium (NOMS), 2006

[14] V. Pacheco, R. Puttini, "An administration structure for the OLSR protocol", Computational Science and Its Applications (ICCSA), 2007

[15] R. Badonnel, R. State, O. Festor, "Management of mobile ad hoc networks: information model and probe-based architecture", International Journal of Network Management, Volume 15, Issue 5, Pages: 335 - 347, 2005

[16] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "RFC1175: A Simple Network Management Protocol (SNMP)", http://www.ietf.org/rfc/rfc1175.txt

[17] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "RFC1441: Introduction to version 2 of the Internet-standard Network Management Framework", http://www.ietf.org/rfc/rfc1441.txt

[18] R. Presuhn et. al., "RFC3416: Version 3 of the Protocol Operations for the Simple Network Management Protocol (SNMP)", Std. Track, http://www.ietf.org/rfc/rfc3416.txt

[19] U. Blumenthal, B. Wijnen, "RFC3414: User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", Std. Track, http://www.ietf.org/rfc/rfc3414.txt

[20] B. Wijnen, R. Presuhn, K. McCloghrie, "RFC3415: View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", Std. Track, http://www.ietf.org/rfc/rfc3415.txt

[21] K. McCloghrie *et. al.*, "RFC2578: Structure of Management Information version 2 (SMIv2)", Std. Track, http://www.ietf.org/rfc/rfc2578.txt

[22] R. Enns, "RFC4741: NETCONF Configuration Protocol", Std. Track, http://www.ietf.org/rfc/rfc4741.txt

[23] M. Bjorklund, "I-D: YANG - A data modeling language for NETCONF", Work in Progress, http://tools.ietf.org/id/draft-ietf-netmod-yang-13.txt

[24] R. G. Cole, J. Macker, A. Morton, "I-D: Managed Objects for the Definition of Performance Reports – the REPORT-MIB", Work in Progress, http://tools.ietf.org/id/draft-cole-report-mib-02.txt

[25] U. Herberg, R. Cole, T. Clausen, "I-D: MANET MIB for Neighborhood Discovery Protocol (NHDP)", Work In Progress, http://tools.ietf.org/id/draft-ietf-manet-nhdp-mib-03.txt

[26] U. Herberg, R. Cole, "I-D: MIB for the Optimized Link State Routing Protocol version 2 (OLSRv2)", Work In Progress, http://tools.ietf.org/id/draft-ietf-manet-olsrv2-mib-01.txt

[27] A. Bhattacharyya, "On a measure of divergence between two statistical populations defined by their probability distributions", Bull. Calcutta Math. Soc. 35, 99–109, 1943

Contents

1 Introduction 3
- 1.1 OLSRv2 Overview . . . 3
  - 1.1.1 Neighborhood Discovery (NHDP) . . . 4
  - 1.1.2 MPR Flooding . . . 4
  - 1.1.3 Link State Advertisement . . . 4
  - 1.1.4 Flexible Message Format . . . 4
  - 1.1.5 OLSRv2 Router Configuration . . . 5
- 1.2 Memorandum Outline . . . 5

2 Related Work 5

3 A Brief SNMP Primer 6

4 Problem Statement: Managing OLSRv2 Networks 7

5 OLSRv2 Management Architecture 8

6 NHDP and OLSRv2 MIBs 8

7 Performance Management 10
- 7.1 Object Types . . . 10
- 7.2 Derived Objects in NHDP and OLSRv2 . . . 13
  - 7.2.1 Frequency changes of message scheduling . . . 13
  - 7.2.2 Frequency changes of Neighbor Set modifications . . . 13
  - 7.2.3 Frequency of changes of the online status of a given neighbor 13
  - 7.2.4 Frequency of changes of the online status of a given 2-hop neighbor . . . 13
  - 7.2.5 Frequency of changes of the link over which a neighbor is reachable . . . 13
  - 7.2.6 Frequency of changes of the neighbor over which a 2-hop neighbor is reachable . . . 14
  - 7.2.7 Frequency of routing set recalculations and MPR set recalculations . . . 15

8 Conclusion 15

Centre de recherche INRIA Saclay – Île-de-France
Parc Orsay Université - ZAC des Vignes
4, rue Jacques Monod - 91893 Orsay Cedex (France)

Centre de recherche INRIA Bordeaux – Sud Ouest : Domaine Universitaire - 351, cours de la Libération - 33405 Talence Cedex
Centre de recherche INRIA Grenoble – Rhône-Alpes : 655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier
Centre de recherche INRIA Lille – Nord Europe : Parc Scientifique de la Haute Borne - 40, avenue Halley - 59650 Villeneuve d'Ascq
Centre de recherche INRIA Nancy – Grand Est : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex
Centre de recherche INRIA Paris – Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex
Centre de recherche INRIA Rennes – Bretagne Atlantique : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex
Centre de recherche INRIA Sophia Antipolis – Méditerranée : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399