Performance Analysis of SNMP in OLSRv2-routed MANETs

Ulrich Herberg

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Performance Analysis of SNMP in OLSRv2-routed MANETs

Ulrich Herberg

N° 7407

October 2010

ISSN 0249-6399 ISRN INRIA/RR--7407--FR+ENG

INSTITUT NATIONAL
DE RECHERCHE
EN INFORMATIQUE
ET EN AUTOMATIQUE

INRIA

centre de recherche
SACLAY - ÎLE-DE-FRANCE

Performance Analysis of SNMP in OLSRv2-routed MANETs

Ulrich Herberg*

Thème : COM – Systèmes communicants
Équipe-Projet Hipercom

Rapport de recherche n° 7407 — October 2010 — 18 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. While SNMP is sometimes considered too "heavy" for MANETs, it remains the predominant management and monitoring protocol in the Internet, with many implementations existing. This memorandum analyzes SNMP in OLSRv2-routed MANETs, with the purpose of investigating performance metrics, such as delivery ratio, delay, overhead and collisions in the network simulator NS2.

Key-words: OLSRv2, MANET, management, control, SNMP, performance study, simulation, NS2

* LIX - Ecole Polytechnique, Ulrich@Herberg.name

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

Analyse de Performance de SNMP dans des réseaux MANETs basés sur 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. Alors que SNMP est parfois considéré trop "lourd" pour des MANETs, il demeure le protocole prédominant de management et monitorage d'Internet, et beaucoup d'implémenations du protocole existent. Ce rapport analyse SNMP dans des MANETs basés sur OLSRv2, avec l'intention de déterminer des métriques de performance, comme le taux de remise, délai, overhead et collisions dans le simulateur de réseaux NS2.

Mots-clés : OLSRv2, MANET, management, contrôle, SNMP, étude de performance, simulation, NS2

1 Introduction

Mobile Ad hoc Network (MANET) routing protocols are commonly assumed to be entirely self-managing: routers 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 operator intervention 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 in order 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 analyzes the performance of SNMP, the prevailing management and monitoring protocol in the Internet, in the context of an OLSRv2 routed MANET in which routers run the Optimized Link State Routing Protocol version 2 (OLSRv2), currently in the process of being standardized by the MANET working group of the IETF[1].

Surveys of performance aspects of SNMP exist [1]), yet – to the best of the author's knowledge – none which consider performance in MANETs. [2] proposes an extension to SNMP that allows aggregation, and presents a study of that extension to SNMP in airborne tactical networks, with a static network with nodes arranged in a grid. However, no general performance analysis is presented in [2].

The reasons for the lack of research in this area may be twofold: (i) SNMP may be considered too "heavy-weight" for MANETs, and (ii) implementing a fully compliant SNMP for network simulators may take a lot of time. Concerning (i), it has to be noted that as no "light-weight" management protocol has been standardized by the IETF yet, SNMP remains the prevailing management protocol[2]. As to (ii), despite the 'S' in SNMP standing for "simple", it is composed by a many RFCs, and therefore it is a time-consuming task to reimplement SNMP for network simulators.

[4] presents a tool called AgentJ, which allows NS2 simulations using unmodified Java routing protocols. This tool is applied in this memorandum in order to study the performance of SNMP in OLSRv2 routed MANETs, using the free SNMP implementation "SNMP4J" [5] and JOLSRv2 [6], a Java implementation of OLSRv2.

1.1 Memorandum Outline

The remainder of this memorandum is organized as follows: Section 2 provides a brief overview of both OLSRv2 and SNMP. Section 3 describes the motivation for monitoring and controlling OLSRv2 routed MANETs. Section 4 presents a management architecture for OLSRv2. Section 5 describes the simulation

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

[2]The IETF has standardized NETCONF [3] in 2006, but not with the focus on constrained devices such as MANET routers

settings for the performance analysis of SNMP in OLSRv2-based MANETs, and details the results. This memorandum is concluded in section 6.

2 Overview of OLSRv2 and SNMP

This section outlines the principal protocol behavior of both OLSRv2 and SNMP. Readers familiar with both protocols may skip this section.

2.1 OLSRv2 Overview

The Optimized Link State Routing Protocol version 2 (OLSRv2) [8, 9, 10, 11] is a successor to the widely deployed OLSR [12] 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 detailed in section 2.1.1 to 2.1.3 below, followed by a description of the flexible message format used by OLSRv2, in section 2.1.4, and a discussion of the configuration and operation of OLSRv2 routers in section 2.1.5.

2.1.1 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.

2.1.2 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. MPR selection is encoded in outgoing HELLOs.

2.1.3 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.

2.1.4 Flexible Message Format

OLSRv2 employs the format specified in [8], 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.

2.1.5 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. 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 can process correctly these regardless of its own configuration.

2.2 SNMP Overview

SNMP specifies 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 [13] specified a set of basic network management

capabilities, including a relatively simple security model. SNMPv2 [14] was developed to extend SNMP capabilities and to improve the basic security model. However, it was not until the development of SNMPv3 [15] that an acceptable security model was developed. The Structure of Management Information version 2 (SMIv2) [16] 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.

3 Problem Statement

As indicated in section 2.1.5, 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. [9] proposes a value for this constant. 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".

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 for improved responsiveness.

This example requires a more "global view" of the network, than that of a single OLSRv2 router – *i.e.* entails 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 MIBs for managing OLSRv2 networks and monitoring performance of these networks are overviewed.

4 OLSRv2 Management Architecture

The proposed architecture of the OLSRv2 management system consists of three MIBs: the NDHP-MIB [17], the OLSRv2-MIB [18], and the REPORT-MIB [19]. Both the NHDP-MIB and the OLSRv2-MIB consist of different groups, allowing to (i) change control settings, such as message intervals (*e.g.* for HELLOs) and information validity times (*e.g.* hold times), as well as (ii) to monitor the state of the router (*e.g.* the neighbor set).

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 [19]. 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.

For a more detailed description of the MIBs and how they allow monitor the performance of NHDP and OLSRv2 using the REPORT-MIB, refer to [20].

5 Performance Study of SNMP in OLSRv2 MANETs

In the previous sections, the motivation for managing OLSRv2 routed networks has been described. In order to understand the implications when running SNMP in an OLSRv2 routed MANET, this section presents a performance study of SNMP in the NS2 simulator. Typical performance metrics – such as delivery ratio, delay, overhead and collision ratio – are evaluated.

5.1 Simulation Settings

Simulations have been conducted with JOLSRv2 [6] as routing protocol, which is a fully-compliant Java implementation of OLSRv2. SNMP4J [5], a Java implementation of SNMP, has been hooked into NS2 using AgentJ [4], as explained in section 1. According to [5],

> "*SNMP4J is an enterprise class free open source and state-of-the-art SNMP implementation for Java 2 SE 1.4 or later. SNMP4J supports command generation (managers) as well as command responding (agents). Its clean object oriented design is inspired by SNMP++, which is a well-known SNMPv1/v2c/v3 API for C++ [...].*"

Simulations have been performed using relatively standard scenario parameters, as in table 1. Each measured value has been averaged over 10 simulation runs.

In all scenarios, one router (with ID of 0) is positioned at exactly the center of the simulated area (*i.e.* at coordinates (500, 500)) and does not move. It runs an SNMP manager, whereas all other routers run an SNMP agent, providing the NHDP-MIB [17]. During the simulated time of 270 seconds, the SNMP manager sends requests ("get-next-request") for the NHDP parameter `N_HOLD_TIME` to all other routers, one after the other, starting after 10 seconds (in order to allow OLSRv2 to converge before). UDP is used as transport protocol, and a 500ms timeout is set (*i.e.* the manager aborts the request if no response has been

Table 1: NS2 parameters

Parameter	Value
NS2 version	2.34
Mobility scenario	Random walk
Grid size	1000m x 1000m
Number of routers	10 - 50
Communication range	250m
Radio propagation model	Two-ray ground
Simulation time	270 secs
Interface type	802.11b
Radio frequency	2.4 GHz
OLSRv2 parameters	Proposed default values of [11]

received within 500ms, and it proceeds sending a request to the next router). 25 seconds after the first request is sent, the manager restarts sending requests to all other routers, which allows to send requests to all routers (500 ms times 50 routers in the worst case of a 50 router network and all requests failed). The process is repeated every 25 seconds until the end of the simulation.

Different variations of SNMP are tested in the simulations, notably SNMPv2c, SNMPv3 without authentication or privacy (simply denoted "SNMPv3"), SNMPv3 with SHA authentication only (denoted "SNMPv3 (SHA)"), and SNMPv3 with authentication and privacy (denoted "SNMPv3 (SHADES)" and "SNMPv3 (SHAAES128)"). SHADES is specified in [21], and SHAAES128 in [22]. Note that some implementations, such as SNMP4J and Cisco SNMP implementations, provide other cipher algorithms like SHAAES192, SHAAES256 and SHA3DES. However, these have only been proposed as individual drafts (expired) in the IETF, and have never been standardized. For that reason, these mechanisms have not been considered in the simulation.

5.2 Simulation Results

This section presents the results of the simulation study. Figure 1 depicts the accumulated transmitted control traffic of OLSRv2 during the simulation, counting each retransmission of forwarded messages. The control traffic overhead increases with the number of routers in the network.

Figure 2 shows the control traffic in a 50 router network with increasing constant speed of all routers (besides router 0, which does not move). The control traffic overhead increases from a static scenario to a mobile scenario, but then does not change significantly. The reason are triggered HELLO and TC messages, which occur when links break or new links between routers are detected.

Figure 3 presents the accumulated traffic of SNMP messages with different SNMP versions and security mechanisms. The traffic grows linearly with the number of routers in the network, *i.e.* with the number of SNMP agents to which the manager sends SNMP requests. Not surprisingly, SNMPv2 has a far lower overhead than SNMPv3. SNMPv3 with authentication only (SHA) has a higher overhead than SNMPv3 without authentication, but less than both tested encrypted SNMPv3 variants (which have an almost equal overhead).

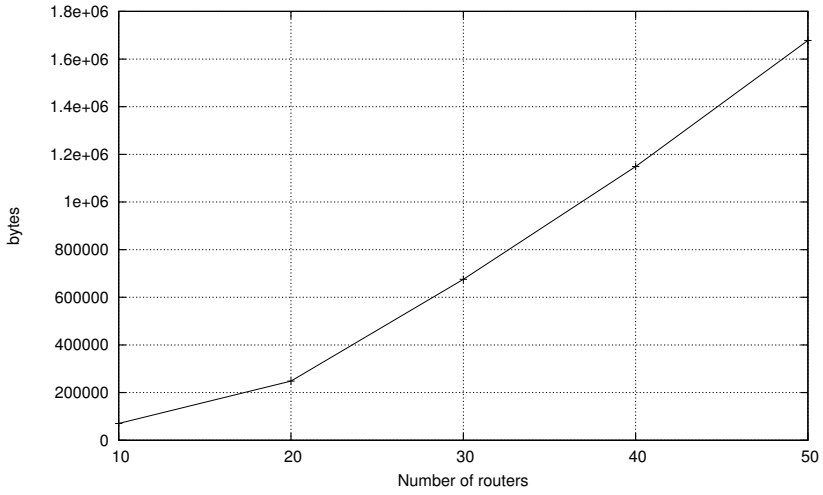

Figure 1: OLSRv2 accumulated control traffic throughout the simulation

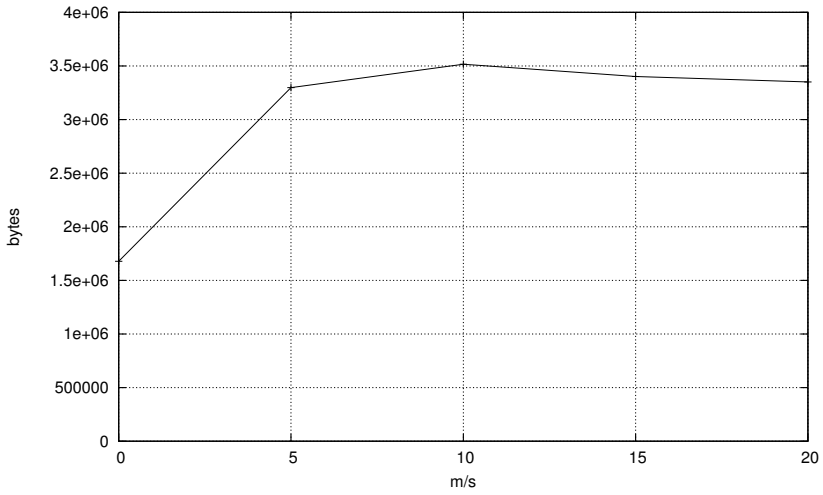

Figure 2: OLSRv2 accumulated control traffic throughout the simulation, with 50 routers

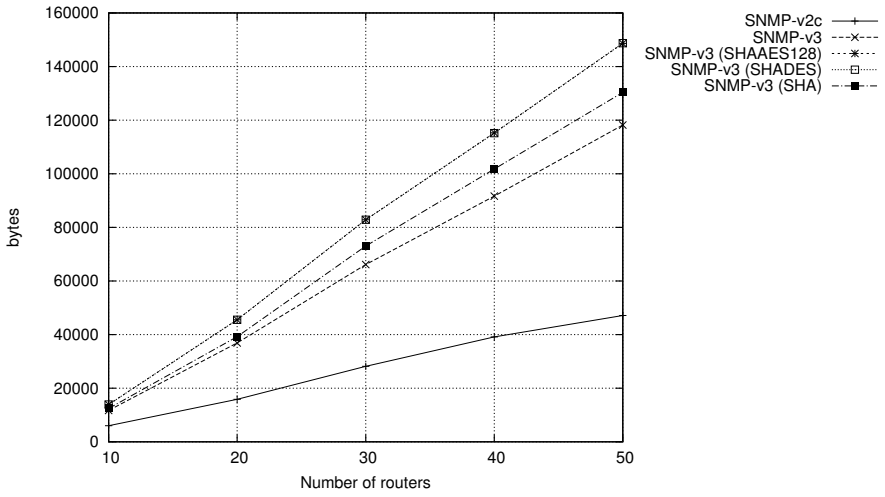

Figure 3: Accumulated SNMP traffic overhead

The difference in the cumulated message overhead has several reasons: First, the SNMP messages contain different amount of security related parameters. Table 2 shows the message sizes of the get-next-request message that is sent from the manager to the agents (as measured with Wireshark between two real machines, but the same SNMP implementation, SNMP4J).

Table 2: SNMP message sizes

Variant	Frame size	SNMP message size	PDU size
SNMPv3	140	103	48
SNMPv3-SHA	146	109	48
SNMPv3-SHADES	159	122	48
SNMPv3-SHAAES128	163	125	48

It can be observed that SHADES and SHAAES128 have very similar SNMP message sizes, which confirms the almost equal plots in figure 3. Another observation is that the payload (the PDU) is of equal size. This is due to the used mode of operation of the block cipher (fore more details refer to [23]). SHADES applies a CBC (Cipher-block Chaining) operation mode, which splits the plaintext in multiples of 8 bytes with possible padding. Since the payload happens to be a multiple of 8 bytes, the cypher text has the same length as the plaintext. SHAAES128 uses a CFB (Cipher Feedback) operation mode, which always outputs the same length as the input plaintext.

Another reason for the different total SNMP traffic is the number of transmitted messages, which is depicted in figure 4. The figure compares SNMPv2c with the SHAAES128 variant of SNMPv3 (for the other encrypted variants, the output is similar). The reason for the higher number of messages is that between each pair of routers exchanging SNMP messages, an additional initial message exchange has to be performed, in order to provide a replay mechanism. Figure 5 shows an initial message exchange in SNMPv2 and SNMPv3 with privacy.

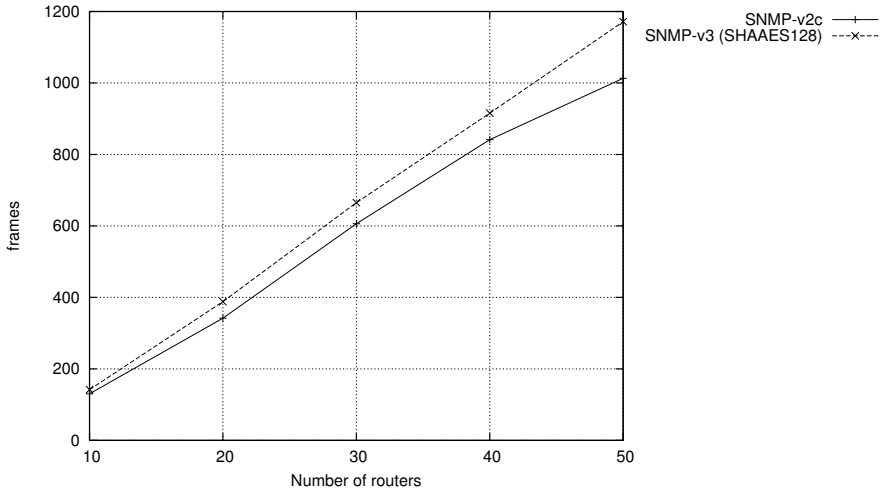

Figure 4: Number of transmitted SNMP messages

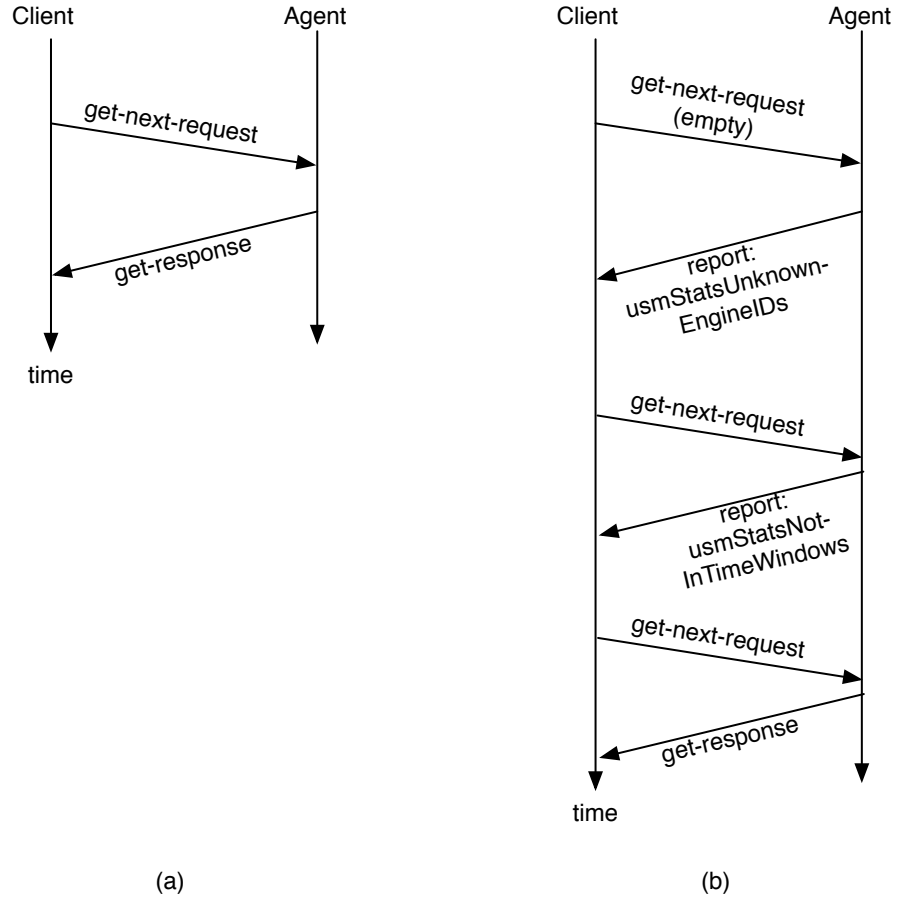

Figure 5: SNMP message exchange: (a) in SNMPv2 (b) in SNMPv3 with privacy

While in SNMPv2, the get-next-request is directly sent and answered, SNMPv3 exchanges the Authorative EngineID and a counter how often the agent has been rebooted, in order to provide replay protection. In our simulations, this initial exchange of parameters is only performed at the first request from the manager to an agent, not in any subsequent one, which explains why the plot in figure 4 for SNMPv3 is only slightly higher.

Figure 6 depicts the MAC frame collision rate. Due to the increased number of control traffic exchange and unicast traffic, the collision rate increases with the number of routers in the network. There is no significant difference between the different SNMP variants, since the main traffic in the scenario comes from the control traffic exchange of OLSRv2. It has to be noted that this is no general observation: in the simulated scenarios, only a single SNMP message exchange is performed at a time, and no other unicast traffic is added, which leads to a very low bandwidth consumption of the unicast traffic.

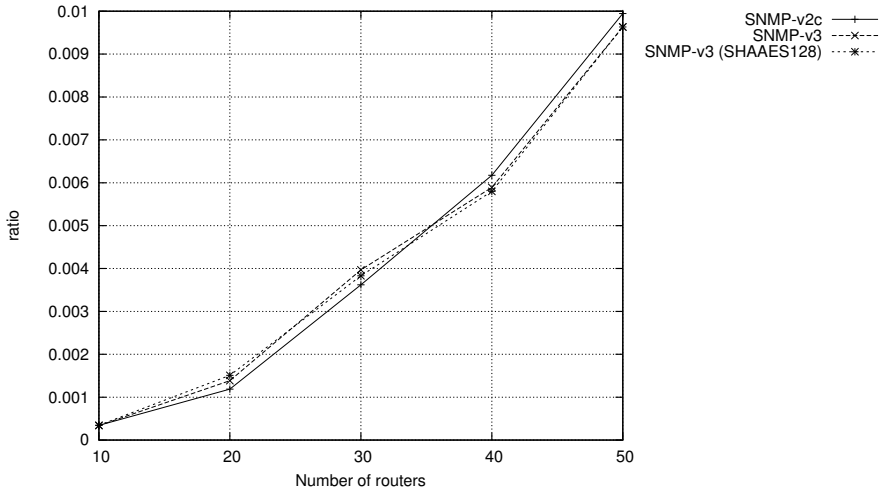

Figure 6: MAC collision ratio

Figure 7 illustrates the collision ratio with increasing speed of the routers. As the control traffic accounts for the majority of the traffic in the simulation, and the control traffic does not considerably increase with higher speed (as shown in figure 2), the collision ratio remains at a stable level of about 12%.

Figure 8 shows the average time duration between a transmission of the get-next-request and the reception of a response. With increasing number of routers in the network, the delay increases in all SNMP variants. SNMPv3 and SNMPv3 with privacy has a higher delay due to the initial message exchange for means of replay protection as depicted in figure 5.

Figure 9 shows the delivery ratio of SNMP messages. Since the collision ratio is only very low (as depicted in figure 6), the delivery ratio is relatively high, increasing with a higher density of the network. There is no significant difference between the different SNMP variants.

Figure 10 depicts the delivery ratio when routers are mobile. The delivery ratio decreases, but remains at a relatively high level, due to the low number

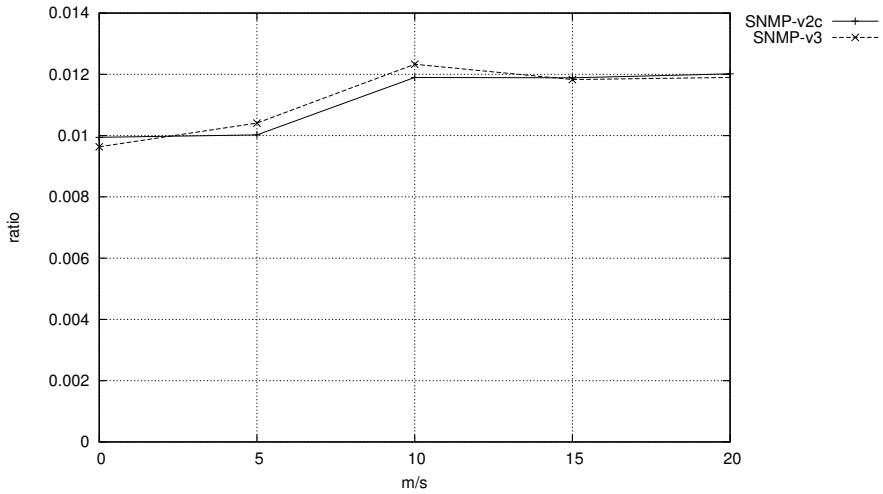

Figure 7: MAC collision ratio with variable router speed with 50 routers

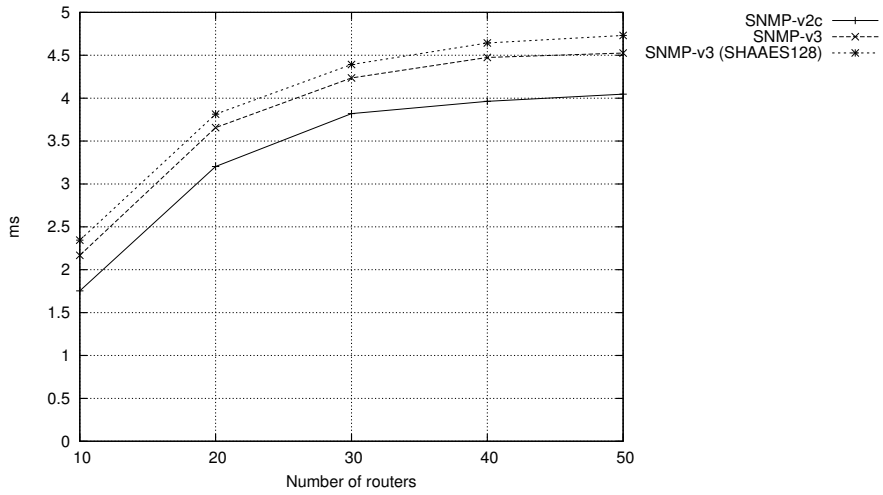

Figure 8: Message exchange delay

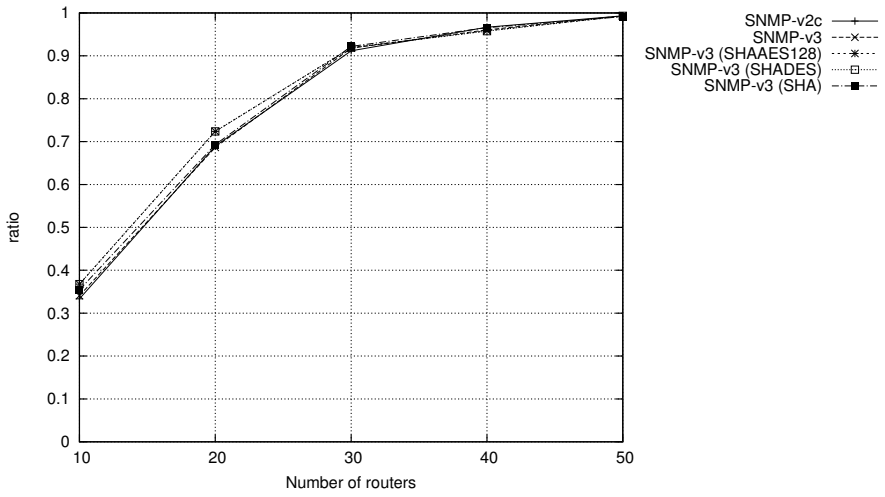

Figure 9: Delivery ratio of SNMP messages

of collisions and the relatively short distance in hops from the manager to all agents.

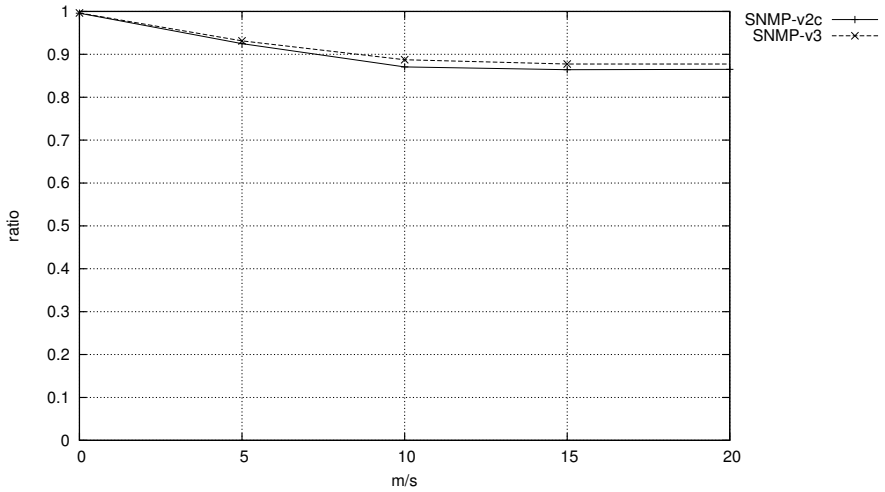

Figure 10: Delivery ratio in a mobile network of 50 routers

Finally, figure 11 illustrates the average path length in hops between the SNMP manager and the agents. There is no significant difference between the different SNMP variants.

6 Conclusion

The MANET routing protocol OLSRv2 does not require any external interaction once deployed, as routers are able to accommodate frequently changing network

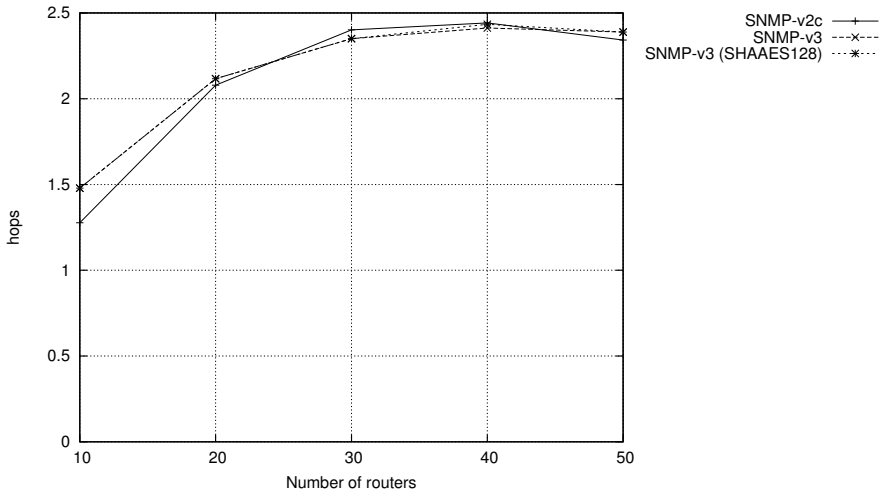

Figure 11: Average path length

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 analyzes the behavior and the performance of SNMP, the predominant management and monitoring tool for routers in the Internet, in MANETs where routers run OLSRv2. Different evaluation metrics are considered, such as delivery ratio, delay, overhead, collisions, both in static and in mobile networks. Different variants of SNMP, notably SNMPv2c, SNMPv3 without authentication or privacy, SNMPv3 with SHA authentication only, and SNMPv3 with authentication and privacy (AES128 and DES) are considered.

References

[1] L. Andrey, O. Festor, A. Lahmadi, A. Pras, J. Schönwälder, "Survey of SNMP performance analysis studies", International Journal of Network Management, 19: 527-548, 2009

[2] G. Kuthethoor *et. al.*, "Performance analysis of SNMP in airborne tactical networks", Proceedings of the IEEE Military Communications Conference (MILCOM), 2008

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

[4] U. Herberg, I. Taylor, "Development Framework for Supporting Java NS2 Routing Protocols", Proceedings of the 2010 International Workshop on Future Engineering, Applications and Services (FEAS), May 2010

[5] SNMP4J Website, http://www.snmp4j.org

[6] U. Herberg, "JOLSRv2 – An OLSRv2 implementation in Java", Proceedings of the 4th OLSR Interop workshop, October 2008

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

[8] 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

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

[10] 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-14.txt

[11] 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

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

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

[14] 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

[15] 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

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

[17] U. Herberg, R. Cole, I. Chakeres, "I-D: Definition of Managed Objects for the Neighborhood Discovery Protocol", Work In Progress, http://tools.ietf.org/id/draft-ietf-manet-nhdp-mib-04.txt

[18] U. Herberg, R. Cole, T. Clausen, "I-D: Definition of Managed Objects for the Optimized Link State Routing Protocol version 2", Work In Progress, http://tools.ietf.org/id/draft-ietf-manet-olsrv2-mib-02.txt

[19] R. G. Cole, J. Macker, A. Morton, "I-D: Definition of Managed Objects for Performance Reporting", Work in Progress, http://tools.ietf.org/id/draft-ietf-manet-report-mib-00.txt

[20] U. Herberg, T. Clausen, R. Cole, "MANET Network Management and Performance Monitoring for NHDP and OLSRv2", accepted for the 6th International Conference on Network and Services Management (CNSM), October 2010

[21] 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

[22] U. Blumenthal, F. Maino, K. McCloghrie, "RFC3826: The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model", Std. Track, http://www.ietf.org/rfc/rfc3826.txt

[23] A. Menezes, P. van Oorschot, S. Vanstone, "Handbook of Applied Cryptography", CRC Press, ISBN 0-8493-8523-7, 1996

Contents

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