Evaluation of the Resource Requirements of SNMP Agents on Constrained Devices

Siarhei Kuryla and Jürgen Schönwälder

Computer Science, Jacobs University Bremen, Germany
{s.kuryla,j.schoenwaelder}@jacobs-university.de

Abstract. Constrained devices equipped with a microcontroller and a low-power low-bitrate wireless interface are becoming part of the Internet. We investigate whether the monitoring and configuration of such constrained devices can be performed by adapting the Simple Network Management Protocol (SNMP) to the capabilities of these devices. To this end, we have implemented an SNMP agent under the Contiki operating system. We provide an analysis of its resource requirements and its runtime behaviour on an 8-bit AVR Raven platform.

Keywords: SNMP, 6LoWPAN, Contiki, Internet of Things.

1 Introduction

The Simple Network Management Protocol (SNMP) [1] is widely deployed to monitor, control, and sometimes also configure network elements. Even though the SNMP technology is well documented and well understood, it remains unclear what the exact resource requirements are of running SNMP on constrained devices, such as an 8-bit microcontroller with 16 kB of RAM connected to the Internet via an IEEE 802.15.4 transceiver. The origins of SNMP date back to the late 1980s when computers had much less resources compared to what we are used to today. In fact, one of the stated goals was that "the impact of adding network management to managed nodes must be minimal, reflecting a lowest common denominator" [2]. From this historic perspective, SNMP seems to be a reasonable fit for managing today's constrained devices. However, it must be noted that SNMP did evolve during the 1990s and in particular security mechanisms present in SNMP version 3 (SNMPv3) add significant complexity, increasing the code size and impacting runtime performance. Hence, we were approached with question such as the following:

- What are the resource requirements of a minimal SNMPv3 implementation running on constrained devices?
- Which parts of an SNMP protocol engine are most expensive?
- What is the cost of adding instrumentation (additional MIB objects)?
- What is the runtime behaviour of SNMP over an IPv6 link using an IEEE 802.15.4 radio and the 6LoWPAN adaptation layer?

I. Chrisment et al. (Eds.): AIMS 2011, LNCS 6734, pp. 100–111, 2011.

The answers to these questions are crucial in order to understand whether it is feasible to run multiple protocols concurrently on constrained devices providing end-to-end interoperability with deployed systems or whether it is necessary to adopt architectures, where interoperability with deployed systems is achieved via gateways translating between standard Internet protocols and a single protocol (e.g., CoAP [3]) interfacing constrained devices.

The rest of the paper is structured as follows. We first discuss some architectural options for using SNMP in constrained networks in Section 2 before we review related work in Section 3. The design choices behind our SNMP implementation running on the Contiki [4] operating system are summarized in Section 4. In Section 5, we describe our experimental setup in. We present an analysis of the memory requirements in Section 6, which is followed by a discussion of the observed latency in Section 7. We conclude the paper in Section 8.

2 Architectural Considerations

Low-Power Wireless Personal Area Networks (LoWPANs) typically consist of a (potentially large) number of constrained devices embedded into everyday objects. Unlike conventional networks, nodes in such networks should need minimal configuration, they should preferably work "out of the box", they should be easy to bootstrap, and they should be largely self-healing [5]. However, even the best automated mechanisms may fail and require explicit management once in a while. As such, a certain amount of explicit management can never be completely removed. Since the goal of IPv6 over LoWPANs (6LoWPAN) is to reuse existing protocols as much as possible, it makes sense to look at the question how SNMP can be used to manage 6LoWPAN networks consisting of constrained devices. Figure 1 outlines four architectural options for the common scenario where a network management system residing in the normal Internet manages constrained devices connected via a 6LoWPAN network.

Figure 1(a) assumes direct end-to-end SNMP communication. This option provides straight forward access to individual 6LoWPAN nodes. Reuse of existing deployed SNMP-based tools is easy and end-to-end security can be provided. The downsides of this option are related to message sizes and fragmentation issues, the requirement to embed a full SNMP engine into constrained devices, and the trap-directed polling nature of SNMP if energy consumption is a concern.

By utilizing an SNMP proxy (see Figure 1(b)), it is possible to optimize the transport of SNMP messages on the 6LoWPAN network, e.g., by using an alternate encoding or by using different security mechanisms. Since SNMP proxies are well defined in the SNMP specifications, management applications supporting SNMP proxies should need no modifications. Note that this approach still requires an SNMP agent on the constrained devices and that it does not overcome the trap-directed polling nature of SNMP.

Figure 1(c) outlines the usage of SNMP subagent technology where a single SNMP agent, typically running on an edge router, provides access to management information, utilizing a special purpose subagent protocol to interact with