OPEN ACCESS

1st International Electronic Conference on Remote Sensing
22 June - 5 July 2015

Conference Proceedings Paper – Remote Sensing

SNMP Management of Urban Areas Remote Monitoring via Open Platform Proxy-IP

Leandro Machado [1,†], Alexandre Mota [2,*], Lia Mota [3,†]

[1] Pontifical Catholic University of Campinas, Rodovia D. Pedro I, km 136, Campinas (SP), Brazil; E-Mail: leandro@digitallweb.net

[2] Pontifical Catholic University of Campinas, Rodovia D. Pedro I, km 136, Campinas (SP), Brazil; E-Mails: amota@puc-campinas.edu.br;

[3] Pontifical Catholic University of Campinas, Rodovia D. Pedro I, km 136, Campinas (SP), Brazil; E-Mails: lia.mota@puc-campinas.edu.br.

† These authors contributed equally to this work.

* Author to whom correspondence should be addressed; E-Mail: amota@puc-campinas.edu.br; Tel.: +55 19 3343-7348.

Published: 22 June 2015

Abstract: With the advances of Urban Intelligence and Smart Cities, the importance of remote monitoring and data collection increased. Concerning monitoring, a IP-Proxy is an important equipment to perform the interconnection between the sensors and the Internet. In the recent literature, several gateway architectures for network sensors have been proposed to integrate Wireless Sensor Networks (WSN) and Internet. Most implementations of WSN gateways retrieve sensors data on the WSN and display the results to customers through the web. The disadvantage of these solutions is that they use specific protocols to connect the sensors, thereby prohibiting the direct interaction between customers and sensor nodes. As an option, the adoption of the SNMP protocol for sensor management has the potential to reduce the gateway complexity of most gateway. For this reason, this article presents the design and implementation of a low-cost open platform IP-Proxy with the usage and modification of a commercial out-of-the-shelf wireless router, with serial connection to communicate with the sensors, that are connected to an expanded microcontroller Arduino Nano board. The results of the experiments showed that the IP-Proxy can successfully interconnect sensor networks and the Internet, where data can be worldwide broadcasted via Ethernet or WLAN.

Keywords: SNMP; Urban Areas; Remote Monitoring; Open Platform; Proxy-IP; Smart Cities

1. Introduction

One effect of rapid technological change is the change in the urban environment. The so-called urban intelligence is the result of this change, with the use of sensors interconnected to communication networks providing various information on urban environment and enabling the design of Smart Cities.

This concept, also known as Internet of Things (IoT), is presented in [1] as the new evolution of the Internet. Still according to [1], the Internet of Things had an important milestone between 2008 and 2009, when for the first time the number of Internet-connected devices surpassed the number of people worldwide. In 2020 the estimate is that there will be 50 billion connected devices and about 7,6 billion people worldwide.

Following this concept, this work aims at monitoring one or more aspects of the urban environment remotely, using sensors installed in a Proxy-IP platform. The monitoring of these sensors is done via Internet and the protocol used for this management is SNMP (Simple Network Management Protocol). The choice of this protocol is due to the fact that it is being widely used for data management via IP (Internet Protocol).

This article describes in detail the implementation of the Proxy-IP and is structured as follows: Section 2 addresses the SNMP protocol. Section 3 presents the functioning of the Proxy-IP and the components (hardware and software) used for its implementation. Section 4 describes the development of this work and Section 5 presents the experiments that were carried out. Finally, Section 6 presents the main conclusions of this work.

2. The SNMP protocol

Created in the late 1980s [2], the SNMP (version 1) protocol was considered not suitable for critical tasks, and so two more variations of this protocol were created. The second version, known as SNMPv2, provides more efficiency and features than the previous version. The third version, known as SNMPv3, provides more security than the previous versions by adding password and data encryption [3] [4].

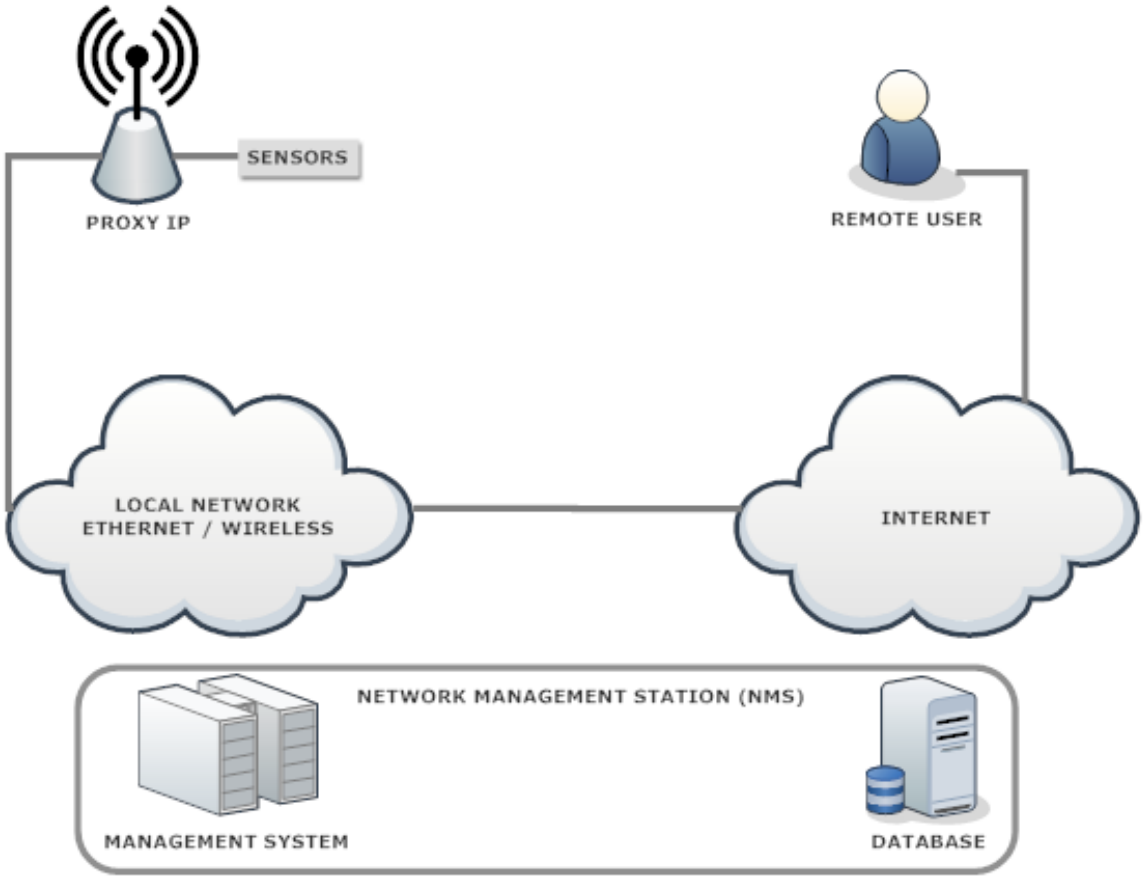
In this work, the protocol adopted version was SNMPv1 because the transmitted data was considered not highly critical, and does not require the implementation of security aspects. This protocol is implemented on the IP network stack in order to manage large computer networks in which the IP stack is a constant presence [3].

A feature of network management based on SNMP protocol is the definition of objects manages, or Object Identification (OID), which is a symbolic representation for a particular information present on the network. The agents, which can be parts of the software of the managed element or equipment separately (probes), interact with the management server, answering requests of “GET” or “SET” type.

3. Implemented Proxy-IP

The main function of the proposed Proxy-IP is to do the "translation" between the sensors and the IP network. The user interacts directly with the sensors, that is, the user receives sensor information or send questions or actions to sensors. The Proxy-IP software and hardware set is addressed in detail in the following. In this work, the Proxy-IP prototype was developed based on a low-cost hardware platform. Figure 1 illustrates the architecture of the monitoring system.

Figure 1. - Architecture of the monitoring system.



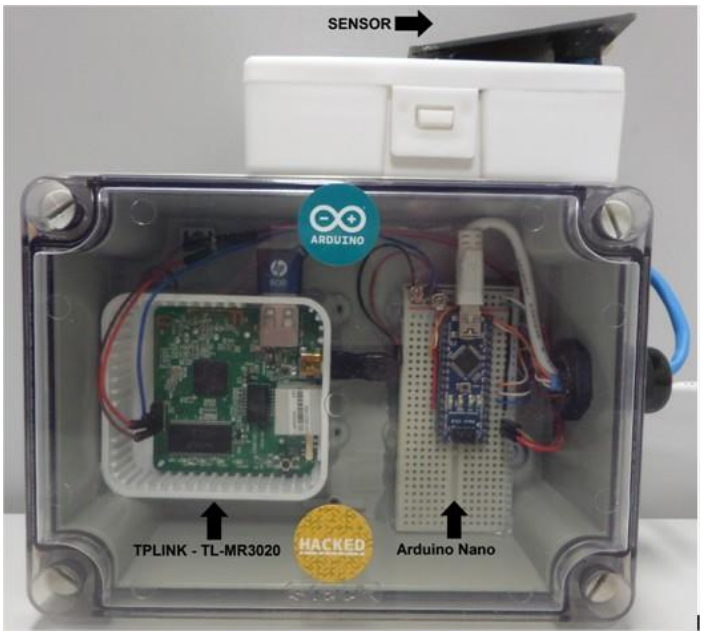
3.1. Components

3.1.1 – Wireless Portable Router 3G/4G - TPLINK TL-MR3020

The TL-MR3020 [5] is a low cost wireless/wired network connection device, integrated with 1 port LAN / WAN 100Mbps and an Internet sharing router. This router is compatible with the IEEE 802.11 b / g / n standards and offers performance up to 150Mbps using the IEEE 802.11n standard.

This router has an Atheros AR7240 processor clocked at 400 MHz, has 32MB of RAM and 4MB of FLASH memory. In addition, it features 1 port LAN / WAN 10 / 100Mbps and 1 serial port. Furthermore, this router is compatible with OpenWrt [6], which is a Linux distribution optimized for home routers. Figure 2 illustrates the hardware used in the Poxy-IP and its main components

Figure2. – Hardware used in the Proxy-IP and its main components.



3.1.2 – Arduino Nano V3.0

The Arduino Nano is an electronic prototyping platform that has a low cost and portable design [7]. It uses the ATmega328 microcontroller of Atmel. The main characteristics of the Arduino used in this work are described as follows:

- Microcontroller Atmel ATmega328.
- I/O: 14 digital pins and 8 analog pins.
- USB 2.0 port.
- 32KB FLASH memory.
- Low cost.
- Portable design.

3.1.3 – OpenWRT Operational System

OpenWrt [8] is a compact and open source Linux which is mainly used in embedded devices for handling with routing problem in a network setting. The kernel and all other components are optimized to be small enough to fit in the generally reduced memory of a common router.

OpenWrt also offers a package manager (as other Linux distributions) that can be used to install packages from a repository or to upload applications.

4. Development

The original firmware of the TPLINK router was substituted by the OpenWRT operational system, allowing the installation of various packages for the Proxy-IP platform development.

One of these packages was SNMPD, which is a SNMP agent. The SNMP waits for requests from the SNMP Manager. When it receives a request, it processes it, collects the information that was requested and returns the information to the requestor.

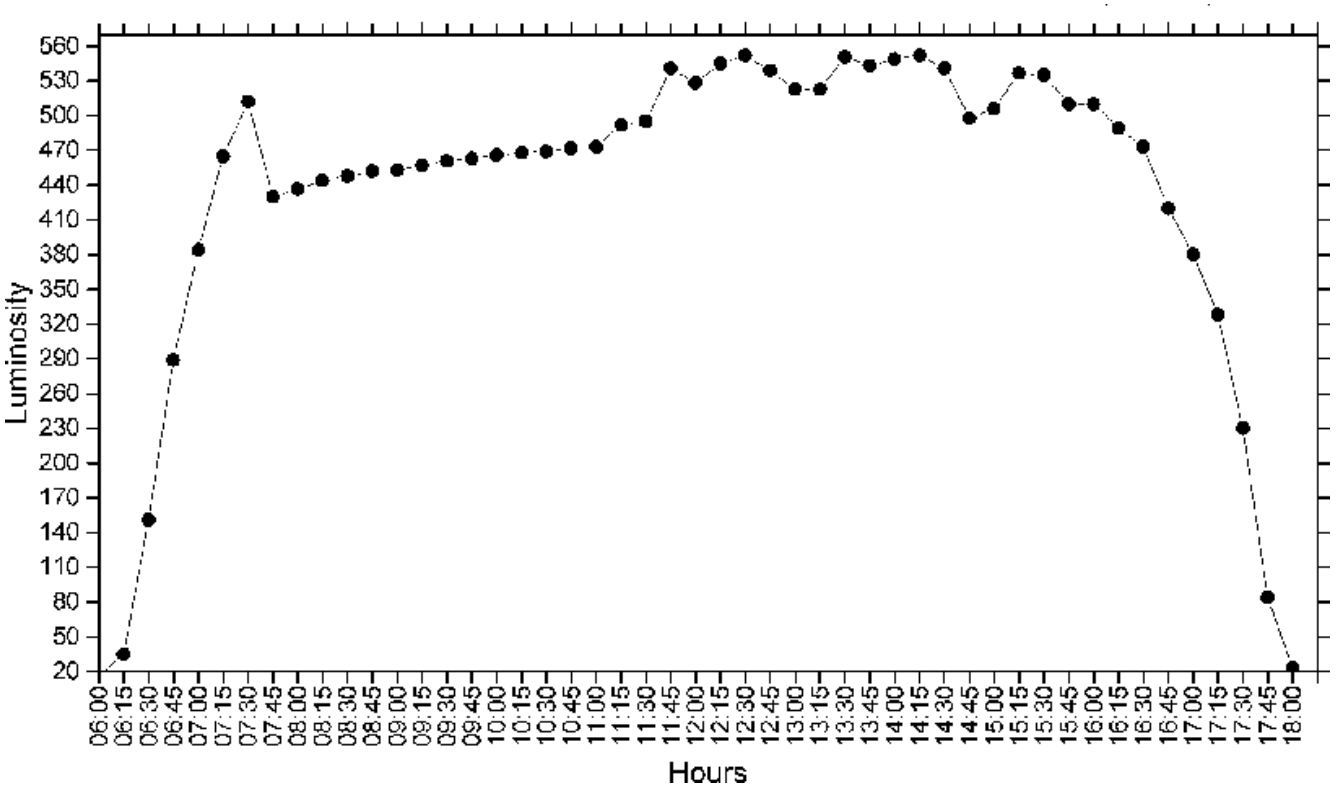
The sensor data collection process begins with the firing of a “GET” request by the manager for the IP of the Proxy-IP, with a single OID addressing, for example “1.3.6.1.2.1.1.21.100.1”. When this “GET” request is received, the SNMPD processes and checks in the “snmpd.conf” configuration file if this OID exists. If so, it checks the command script that will be (“sensores.sh” script). This script was developed in programming language ASH, that is native to OpenWRT. The “sensores.sh” script makes the solicitation via serial port to the Arduino Nano to read the sensor and returns the obtained value. This value is sent via SNMP to the manager.

5. Experimental Section

The goal of the laboratory experiment carried out was to functionally validate the implemented Proxy-IP. The sensor used in this test was a light sensor (LDR – Light Dependent Resistor) on the pin "A0" of Arduino. Consequntly, using the OpenWRT, every time a SNMP “GET” request was address to the OID “ .1.3.6.1.2.1.1.20.101.1”, the answer was the value/data associated to the light sensor.

So, it is possible to monitor this data (light intensity) from anywhere, if the user of the system and the Proxy-IP are connected to the same wireless network and if a MIB-Browser able to generate graphs is used. Figure 3 shows the MIB-Browser monitoring the luminosity of an urban area, for a whole day, with one hour interval.

Figure3. – Remote monitoring of luminosity.



6. Conclusions

This work presented the implementation of a Proxy-IP for the remote monitoring of urban areas, using the SNMP protocol and an open source platform. The laboratory test that was carried out validate the proposed Proxy-IP, since it was able to monitor the light intensity (luminosity) in an urban area, using the SNMP protocol. The proposed system has also important characteristics that make its implementation easy as low cost and flexibility.

References and Notes

1. D, Evans. The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. San Jose, CA. Cisco White paper. Apr. 2011. Available online: http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (accessed on 10/05/2015).

2. RFC 1157 Case, J. D.; Fedor, M. Schofsstall, M. L.; Davin, C. A Simple Network Management Protocol (SNMP).Network Working Group, Maio 1990.

3. R STALLINGS, W., "SNMP, SNMPv2, SNMPv3, and RMON 1 and 2", 3rd edition, Addison-Wesley, 1999.

4. UDUPA, D. K., "TMN – Telecommunications Management Network" , McGraw-Hill Telecommunications, 1999.

5. Roteador Portátil Wireless N 3G/4G TL-MR3020. Available online: http://www.tp-link.com.br/products/details/?model=TL-MR3020. (accessed on 10/05/2015).

6. OpenWrt Table of Hardware – TP-Link TL-MR3020. Available online: http://wiki.openwrt.org/toh/tp-link/tl-mr3020. (accessed on 10/05/2015).

7. Arduino Nano Board. Available online: http://www.arduino.cc/en/Main/ArduinoBoardNano. (accessed on 10/05/2015).

8. OpenWrt Linux Distribution. Available online: https://www.openwrt.org/. (accessed on 10/05/2015).