

IMPLEMENTATION OF SNMP(SIMPLE NETWORK MANAGEMENT PROTOCOL) ON SENSOR NETWORK: A REVIEW

Neha, Mahendra Singh Meena, Rajbir

Abstract—A WSN (Wireless sensor network) interconnected with IP networks could help bridging physical world and also helps in external monitoring and controls Wireless Sensor Network. In this paper implementation of SNMP (Simple Network Management Protocol) on Sensor network in IPv6 based on TCP/IP such as GPRS is shown. By showing packet transmission between the nodes considering them as server and client nodes by using location based IP addressing protocol.

Keywords: Server and Client nodes, IPv6, WSN, Contiki Software and SNMP.

I. INTRODUCTION

Wireless sensor networks need to be dynamic in nature to provide systematic and, we monitor the smart sensor networks with elements of network management[1].

Security, configuration and performance are to be monitored. Smart sensor nodes are used at different levels which provide network and sensor management dynamically using a Simple network management protocol. This Network is implemented in traffic control (signal lights) in metropolitan area, Monitor automobile control roadways, civil structures and Monitor the environment.

SNMP is used to manage the network for longer duration is a network management protocol. In this system computers are called managers and these managers perform a task of managing a group of nodes. They even execute software components called agents and inform manager via SNMP. These managed nodes in network are founded by ping operation and the information is extracted using SNMP protocol by manager from the nodes. Agent reports the manager when he requests the information and even maintains it. It has capability of reporting manager system about these asynchronous messages[5].

Manuscript received May,2016.

Neha, ECE, Amity University Haryana, Bahadurgrah, India, 9599236623.

Mahendra Singh Meena, ECE, Amity University Haryana, Gurgoan, India,9650175116.

Rajbir, ECE, Amity University Haryana, Gurgoan India,9650549774.

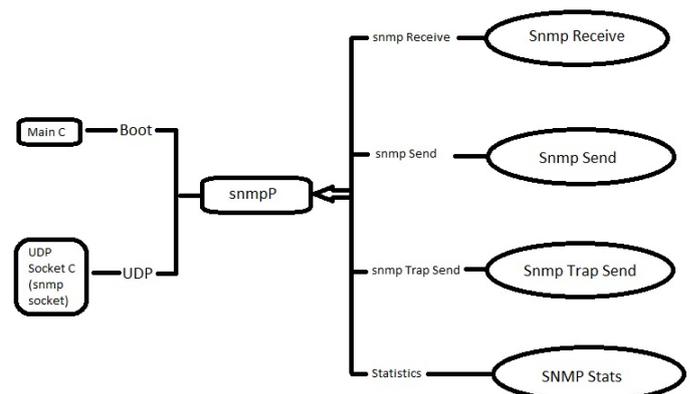


Figure 1: Wiring diagram of SNMP component.[11]

The solutions proposed for WSN monitoring and management are ground on the SNMP (Simple network management protocol) or you can say that implement some concepts found in the SNMP. Most of these works based on the SNMP also do not make use of 6LoWPAN. Mostly SNMP based solutions take advantage of the proxy based deployment model, or some form of sub agent. This deployment model sees a proxy type device deployed between the management station and SNMP agent (managed device). A few SNMP based implementations use this proxy based deployment model to facilitate protocol translation which makes it possible to perform compression of messages[10].

IPv6 arrival over 6LoWPAN(low power wireless personal area network) has changed the tag of WSN as separate network which uses custom, non-standard and application specific protocols. This IP (Internet protocol) is common protocol between conventional IP Network's and WSN. WSN uses tiny OS as operating system and make use of advantages that the common IP layer brings. The reuse of technique, protocols and software that are already developed are included in it.

Standard SNMP software can be used to communicate with the implementation of SNMP software agent. Therefore network monitoring packages like Cacti and Nagios are used monitor WSN. The implementation, SNMP on sensor network software agent is examined, along with then study of an SNMP "GetRequest" message in assistance of understanding the structure of SNMP message.

II. SENSOR NETWORK

A. Working

Sensor network has authorized us to use personal aid devices to be used anywhere. The user can monitor the components of network which shows the dynamic nature of a network. It plugs the sensor into signal conditioning which is automatically configured and is ready to take the measurements.

It announces its presence to other node. The configuration of default setting is done during setup and an acknowledgement is sent to the client or server in the network.

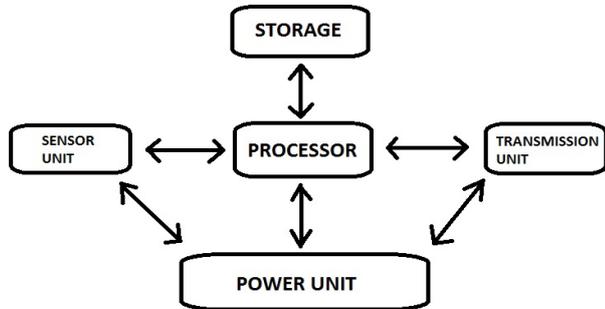


Figure 2: Wireless sensor node.[26]

A smart sensor node is basically used to check the battery life. It can communicate the data in the network and can even measure the health of the node. These nodes always communicate along the network by using internet protocol (TCP/IP)[2].

Examples where Smart Sensor Network is implemented:

- Traffic control (signal lights) in metropolitan areas.
- Monitors- Roadway, Civil structure and environment.
- Monitor automobile control.

Traditional network were more static in nature in comparison to sensor network which are dynamic by nature. In these cases they need strict monitoring for detecting any kind of abnormality in the sensor. Nodes need to act smart in order to provide good management and TCP/IP application layer is to be standardized for being interoperable.

In starting the sensor network management protocols were developed for traditional network, but now a day these networks are used for advanced technologies and for cryptography and other uses.

B. IMPLEMENTATION OF SNMP ON WSN IN DIFFERENT FIELDS

1. SNMP Proxy for WSN

Implementation of SNMP on WSN using MicaZ notes is effective and feasible solution for monitoring health applications. For global and remote monitoring it is connected to internet. Firstly the network of WSN gathers the medical and environment data by using graphical user interface(GUI) which is based on the software known as code blue, after this the data is displayed and stored on the personal computer and this data which is stored in personal computer is able to use for remote access by using SNMP as a proxy connections[13].

A series of experiments were established earlier and the systems were tested to govern all the parameters used for future extension of the health monitoring networks by instigating new sensors, alarms active algorithms are

introduced in the security technique and for location tracking and also for determining the reliability of scenarios that have been established.

2. COST EFFECTIVE WSN USING SNMP

SNMP is used for the examination all the management and control of low cost WSN. It is one of the most accepted protocol, and is used for network management in an network based on IP(Internet Protocol). Since the packet fields in SNMP are very much changeable so Type Length Value (TLV) is required for encoding before transmission of packet takes place. Its size also increases considerably and makes it quite impossible to use in a WSN network. SNMP is basically used for recovering information of management from the network but not for starting actions on the network nodes[19]. In WSN which is cost effective, a light weight SNMP protocol is presented which do not need TLV encoding. This is used for not only controlling the network and their nodes but also for managing the WSN. SNMP protocol has been tested successfully under configurations such as star configuration which is based on WSN network. These nodes comprises on cost effectiveness of a 8 bit microcontrollers and HC-05 Bluetooth modules[23].

• Advantages

If we will create a proxy server for the connection of non TCP/IP networks with a TCP/IP authorized network using SNMP as a protocol, Wireless sensor network(WSN) will collect the data and monitor it till it become an supplement to the existing network management.

It has now become as a supplement to the existing network management infrastructure. SNMP give permission to devices (multiple agents) to connect multiple managers. It has multiple managers for survey which the gateway node or personal computer have without even increasing the data loads on the notes for given information. SNMPv3 even provides end to end point security and supports encryption of data.

• Disadvantage

SNMP a network management protocol, tool was not designed to deal with medical system applications[13].

III. IMPLEMENTATION METHODOLOGY

Space limitation was one of the biggest concern in IPv4 addressing, so we use one IP address to uniquely link a WSN. IP network is connected to WSN through one or more gateway and this IP address is used to route packets from IP network to the WSN. In WSN each destination could be uniquely addressed by a UDP port number with its location mentioned. We recommend using private port numbers, which are in the range of 49,151 to 65,536 for this purpose which allows for more than 16,000 nodes in a WSN and assuming each node to support one addressable destination. If more destinations are needed in a WSN for this purpose then one could use unused port numbers from the UDP registered port number range. This approach will resolves addressing issue from an IP network perspective. By using this addressing scheme, an IP network could route a message to the gateway for a WSN and with the implementation of a mapping scheme between port numbers and WSN

destinations, a gateway could then forward the message to the correct destination i.e. to server.

A destination within a WSN is uniquely identified by a node ID (Identifier) and an endpoint ID logically. An endpoint ID is used to uniquely identify an endpoint within a node in sensor network. An endpoint could be an application, or physical or a logical entity within a node. This concept of endpoint is supported in both TinyOS [2] and ZigBee [9]. For example, ZigBee uses 8 bits to identify an end point within a node and in TinyOS, one could use AM (Active Message) and an 8-bit value [8] is used to designate an entity or end point within a node. There are two approaches to how a WSN could logically view a destination in an external IP network. It could be viewed as an endpoint at the gateway node or an end-point at a separate node that could be reached through the gateway node. As the endpoint identifier is typically 8 bits, only 256 or less IP destinations could be supported if a WSN has only one gateway. On the other hand, if we view an IP network destination as a WSN endpoint at a separate node, we have more flexibility in terms of the number of IP endpoints that could be supported in WSN. Therefore, we suggest assigning a WSN node ID and endpoint ID to each IP destination[9].

IV. SOFTWARE USED

CONTIKI is the networking software which is used for the implementation of SNMP on sensor network in this paper. In this software standard C language is used for writing the programs.

Development is easy and fast with Contiki. Contiki applications are written in NesC, with the Cooja simulator Contiki networks can be emulated before burned in an hardware and this software Contiki provides an entire development environment in a single download. It is basically open source software and can be freely used both in commercial and non-commercial systems and the full source code is available.

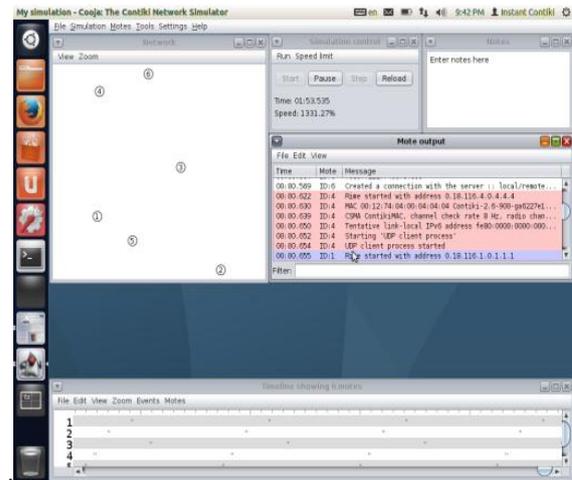


Figure 4: Example showing Simulation



Figure 5: Mote output

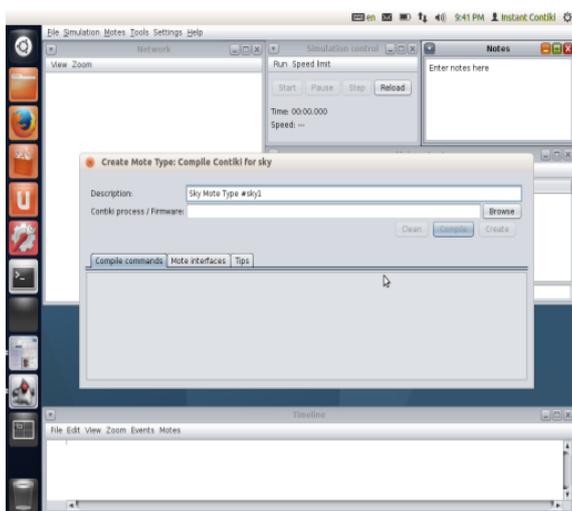


Figure 3: Creation of new simulation

V. CURRENT AND FUTURE USES

Current Uses

SNMP monitors all the internet network management tasks on sensor network these days. SNMP is useful for your home or office network monitoring and management needs. It is performing network monitoring application to watch, collect and graph bandwidth utilization at your wifi router for your home or office network.

Future Uses

Internet of things might be coming in the following years which will be significant innovation in field of wireless technology. SNMP technology will get a new life as all small and low power gadgets which need to be monitored and managed using wireless sensor network.

VI. FURTHER ADVANCEMENT

- Implementation of Interconnection of wireless sensor and IP network (IPv6) using SNMP.

- Location based IP Addressing in IP enable Wireless Sensor using SNMP in IPv6 in TCP/IP.

REFERENCES

- [1] DSP-OS Company, Inc., Available in <http://www.dspos.com/>, 2005
- [2]. Interniche Technologies Company, Inc., Available in <http://www.iniche.com/index.shtml>, 2005
- [3]. Micro Digital Company, Inc., Available in <http://www.smxinfo.com/>, 2005
- [4]. J.L. Hill and D.E. Culler, Mica: A wireless platform for deeply embedded networks, *IEEE Micro*, 22(6):12–24, 2002. ISSN: 0272-1732.
- [5]. G.J. Holzmann, *Design and Validation of Computer Protocols*, Prentice Hall, 1991.
- [6]. C. Shen, C. Srisathapornphat and C. Jaikaeo, Sensor Information Networking Architecture and Applications, *IEEE Personel Communication Magazine*, 8(4):52–59, August, 2001.
- [7]. A. Pras, T. Drevers, R. Meent, D. Quartel, Comparing the Performance of SNMP and Web Services-Based Management, *IEEE Transactions on Network and Service Management*, 1(2), December, 2004.
- [8] J. Thorn, "Deciphering TinyOS Serial Packet," *Octave Tech Brief #5-01*, 2005. Retrieved February 28, 2005. From: <http://www.octavetech.com/pubs/TB501%20Deciphering%20TinyOS%20Serial%20Packets.pdf>
- [9] ZigBee Alliance, ZigBee Specification (Document 05347r13), December 2006.
- [10] . J. Case, R. Mundy, D. Partain, B. Stewart , "RFC 2570 Introduction to Version 3 of the Internet-standard Network Management Framework " TIS Labs at Network Associates, Inc. (April 1999).
- [11] Richardt H. Wilkinson, Shaun Kaplan "Wireless sensor network monitoring using SNMP" From: [file:///C:/Users/Inspiron/Downloads/wireless%20sensor%20network%20onitoring%20using%20the%20simple%20\(1\).pdf](file:///C:/Users/Inspiron/Downloads/wireless%20sensor%20network%20onitoring%20using%20the%20simple%20(1).pdf)
- [12] D. Culler and W. Hong, "Wireless Sensor Networks " ed. Communications of the ACM, June 2004 From: <http://www.pbol.org/projects/genie/publications/infomanage.pdf>, 47:6 (2004).
- [13] B. Deb et al, "Wireless Sensor Networks Management," From: <http://www.research.rutgers.edu/~bdeb/sensor-networks.html> (2005).
- [14] M. Devoti, "Remote Healthcare Monitoring Not so Distant," *Information Society Technologies*, From: <http://istresults.cordis.lu/index.cfm?section=news&tpl=article&ID=74817> (March. 2005).
- [15] E. L. Lee et al, "Network Management in Wireless Sensor Networks," *Handbook of Mobile A Hoc and Pervasive Communication* (2007).
- [16] L. B. Ruiz, "MANNNA: A Management Architecture for Wireless Sensor networks," *IEEE Communications Magazine* (2003), pp 116-125.
- [17] SNMP4J, "The Object Oriented SNMP API for Java Managers and Agents.," From: <http://www.snmp4j.org/>.
- [18] G. Tolle and D. Culler, "Design of an Application Cooperative Management System, for Wireless Sensor Networks," (February 2005).
- [19] Choi, H., Kim, N. & Cha, H., 2009, 6LoWPAN-SNMP: Simple Network Management Protocol for 6LoWPAN, in *High Performance Computing and Communications*, 10th IEEE International Conference on, 305–313, URL <http://www.computer.org/portal/web/csdl/doi/10.1109/HPCC.2009.49>.
- [20] Jason L. Hill, David E. Culler: Mica: A Wireless Platform for Deeply Embedded Networks. *IEEE Micro* 22(6): 12-24 (2002)
- [21] J. Beutel, O. Kasten, F. Mattern, K. Römer, F. Siegemund and L. Thiele: "Prototyping Wireless Sensor Networks with BTnodes". *Proc. 1st European Workshop on Wireless Sensor Networks (EWSN 2004)*, Springer LNCS, vol. 2920, Berlin, pages 323-338, January 2004.
- [22] J. Beutel, M. Dyer, L. Meier, and L. Thiele, "Scalable topology control for deployment-sensor networks," in *Proc. 4th Intl Conf. Information Processing in Sensor Networks (IPSN 05)*, pp. 359-363, IEEE, Piscataway, NJ, Apr. 2005.
- [23] Ing. Jakub Saliva, "Technologies used in Wireless Sensor Networks", 15th International Conference on Systems, Signals and Image Processing, 25-28 June 2008.
- [24] Yen Yang Lim, Marco Messina, Frank Kargl , Leena Ganguli, Martin Fischer, Tommy Tsang, "SNMP-Proxy For Wireless Sensor Network", *IEEE 5th International Conference on Information Technology*, 7-9 April 2008.
- [25] SOHRABY, Kazem, Daniel, Minoli, Taieb, Znati, "Wireless Sensor Networks: Technology, protocols and Applications ", Wiley, 2006, ISBN 978-0-471-74300-2.
- [26] Pradeep K. Mohanty, "A framework for interconnecting wireless sensor and IP networks", *IEEE international symposium on personal, indoor and mobile radio communications (PIMRC'07)*.