American Journal of Networks and Communications
2016; 5(4): 73-81
http://www.sciencepublishinggroup.com/j/ajnc
doi: 10.11648/j.ajnc.20160504.12
ISSN: 2326-893X (Print); ISSN: 2326-8964 (Online)

SciencePG
Science Publishing Group

LabVIEW Based SNMP Proxy Agent for Smart Home Design

Mohammed Basheer Al-Somaidai[1], Omar Mowaffak Ahmad Alsaydia[2]

[1]Electrical Engineering Dept., College of Eng., University of Mosul, Mosul, Iraq

[2]Computer and Information Department, Ninevah University, Mosul, Iraq

Email address:

MohammedBasheerAbdullah@gmail.com (M. B. Al-Somaidai), Alsaydia1@gmail.com (O. M. A. Alsaydia)

To cite this article:

Mohammed Basheer Al-Somaidai, Omar Mowaffak Ahmad Alsaydia. LabVIEW Based SNMP Proxy Agent for Smart Home Design. *American Journal of Networks and Communications.* Vol. 5, No. 4, 2016, pp. 73-81. doi: 10.11648/j.ajnc.20160504.12

Received: August 5, 2016; **Accepted**: August 16, 2016; **Published**: September 8, 2016

Abstract: Simple Network Management Protocol (SNMP) is a well established protocol in network management. In order to apply this protocol in smart home environment, a proxy agent should be used. This proxy agent converts sensor readings to an SNMP compatible form. In this work LabVIEW toolkits are used to play this role. First by acquiring the sensors' readings via multiple sub agents then sending them wirelessly to a single master agent through various approaches. The master agent completes the role of the proxy agent by storing these readings in a database file using LabVIEW database toolkits. This paper demonstrates a test bed representing this system is carried out and an SNMP software is used to monitor and control the sensors remotely. The results show that the proposed smart sending approach greatly reduced the amount of traffic needed.

Keywords: SNMP, Smart Home, LabVIEW

1. Introduction

Smart is ~~a~~ word that is gaining rapid association with many usually dummy objects. These objects are very diverse in their sizes and applications ranging from small sized sensors and phones; towards cars and appliances; ending with buildings and cities. It seems that everything is getting smarter except humans.

A smart device is a device that is capable of adapting to a variable environment in order to function in a predefined or adjustable manner. This requires first, that these devices should sense the variations in the environment, then sharing collected data with other devices or central coordinator to update a database that store history readings of such devices, finally take actions according to some sort of policy. In this sense, smart home or smart building is a term used to define the living space that has automated appliances, lighting, TV, air conditioning, security and camera systems that has the ability to communicate between each other and can be monitored and controlled from any room in the home, as well as remotely from any location in the world using smart phone or Internet [1].

In order to enhance the monitoring and controlling of home devices, Wireless Sensor Network (WSN) are used. WSNs are networks of distributed wireless sensors with low energy. Their use is perceived to be limited to low data intensive applications [2]. WSN consists of a number of sensor nodes which can work together to monitor and manage the smart home to collect data about the environment in real-time [3].

2. Related Works

Al-Kuwari et al. [4] presented a user friendly smart home infrastructure that offers the base platform for modular wireless nodes (utilizing Zig Bee technology integrated with the Arduino microcontroller board) which can collect data, send information and control almost any aspect of the building, as well as the ability to access those wireless nodes and their information through a cross-platform graphical user interface, composing a non-standard system which they called "Bee House".

Zhou et. al. [5] introduced a design of smart home system based on Wireless Sensor Network (WSN). Their work employed different networks (Internet and UMTS) to achieve remote control and monitoring of the house's electric equipment. As the most important part of smart home system, the gateway is not only the bridge between two heterogeneous networks but also the controller, so they introduced two gateway structures: The WSN Integrate

Internet (WII) gateway, which is used to connect the smart home system to the Internet, and a WSN Integrate UMTS (WIU) gateway, which is used to connect the smart home system to the mobile terminal.

In order to keep smart home always operational, robust and efficient; network management architecture is needed. Simple Network Management Protocol (SNMP) [6] had been usually used to diagnose, control and manage IP-based networks.

M. Doudi et al. [7] study the performance of using Zig Bee sensor networks in smart home. The study of performance is depends on the measurements of the Received Signal Strength Indicator (RSSI) in different parts of the Home. After that, discuss the effect of electromagnetic noise on the communication performance of a Zig Bee Sensor Network in the presence of a motor with variable speed drive.

T. Adiono et al. [8] Proposed a smart home platform based on optimized (WSN) protocol and scalable architecture. In this platform, the system is divided into two environments, outdoor and indoor. Outdoor environment uses internet-cloud system, while indoor environment uses WSN system. Those two environments are connected to each other using bridge. Each component of WSN is designed to use an optimized protocol. Mesh topology is used to connect WSN components in order to provide scalable architecture for further changes and extension. In outdoor environment, the proposed platform used existing internet-cloud system as infrastructure. Thus, this smart home platform can be controlled and monitored from smart phone, at any time and form anywhere.

3. Simple Network Management Protocol (SNMP)

SNMP [4] allows for management data to be collected from remote devices, for devices to be configured remotely, and it supports the dissemination of event notifications. Since its first publication (SNMPv1) in August 1988, it has been widely used to manage and monitor networks [9]. This version was susceptible to many attacks because it lacked a security essential cryptography. Many efforts to enhance the security in version 2 failed as they were too complex to apply. Thus; the security mechanisms were removed and the remaining protocol improvements were published as (SNMP ver2c) [10]. It was until the late 1990's when the third version (SNMP v3) was published adding strong cryptographic security to the previous versions of the protocol [11].

SNMP is an application protocol that uses the User Datagram Protocol (UDP) as a transport layer protocol. It enables administrators to monitor network performance and diagnose problems along with setting plans for future network scalability [12].

In general an SNMP-managed network consists of three different components: managed devices (network elements), agents and network-management systems (NMSs). A managed device is a network node that contains an SNMP agent and that resides on a managed network. The main purpose of the managed devices is to collect and store management information and make this information available to the NMSs using SNMP commands. Managed devices can be routers switches, hubs, computer hosts, printers or any other devices.

The SNMP agents store management data as variables in management information base (MIB). These variables are remotely accessed in order to modify or apply new configuration The MIB is organized as hierarchy of management devices. One of the important fields of the MIB is the object identifier (OID) which uniquely identifies a management object in the MIB. The MIB is arranged as tree with nameless root and a hierarchy of branches that are assigned for organizations [13].

The management device has software modules for network management called agent, which has a local knowledge of management information and can translate this information into an SNMP compatible form. The network management system (NMS) monitors and controls these managed devices by providing the processing and memory resources required for network management [14].

The traditional IP networks could be managed through the SNMP protocol, however this protocol cannot directly deployed on the sensor network, because of various WSN characteristics such as [7]:-

a Limited WSN bandwidth.

b The node failure problem which is common in WSNs is not directly addressed by SNMP protocol.

c The limited memory and processing resources of WSN node is not sufficient for storing huge management information base (MIB).

4. LabVIEW Proxy Agent

As it is obvious in Figure 1; SNMP aware devices could directly linked to an SNMP manger; while SNMP proxy agent should be used to link non SNMP devices. The proxy converts management information into a set that is compatible with SNMP and communicates with SNMP manager, thus allowing us to use SNMP with any device [15].

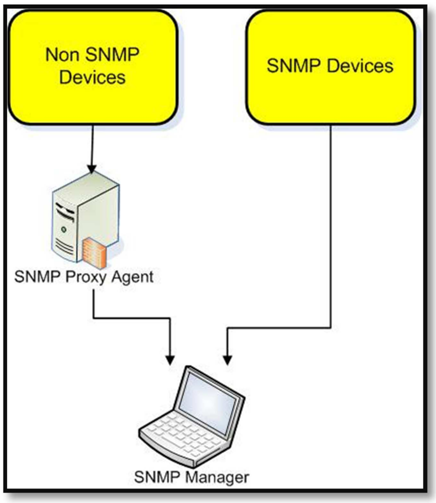


Figure 1. *The role of SNMP proxy agent.*

In this work we have used Laboratory Virtual Instrumentation Engineer's Work bench LabVIEW software as a proxy agent along with WebNMS toolkit as SNMP manager. LabVIEW is a graphical programming environment that is used to develop complex measurement, test, and control systems using specific blocks [16]. LabVIEW is extensively used in this work as it provides very good graphical interface with many toolkits that simplifies practical implementation and interfacing with home sensors.

The proxy agent consists from many subagents and a master agent, the sub agents collect sensors readings and send these readings wirelessly to the master agent whose responsibility to save the received data into Microsoft Access database using LabVIEW database toolkit. The master agent has the ability of communication with many subagents while; each subagent is configured to communicate with the master agent only. Then the master agent uses WebNMS toolkit to make the sensors data available to the manager through a Microsoft Access database that is connected to the MIB via ODBC connection.

5. Practical Implementation

Figure 2 shows a representation of the practical implementation of a test bed consisting of a gas sensor, an ethanol sensor, and a temperature sensor connected to a WLAN host via a data acquisition board NI Elvis II. This WLAN host (called sub agent) is used to send the sensors' readings to another WLAN host called master agent using LabVIEW over TCP connection.

The toolkits of the system are:

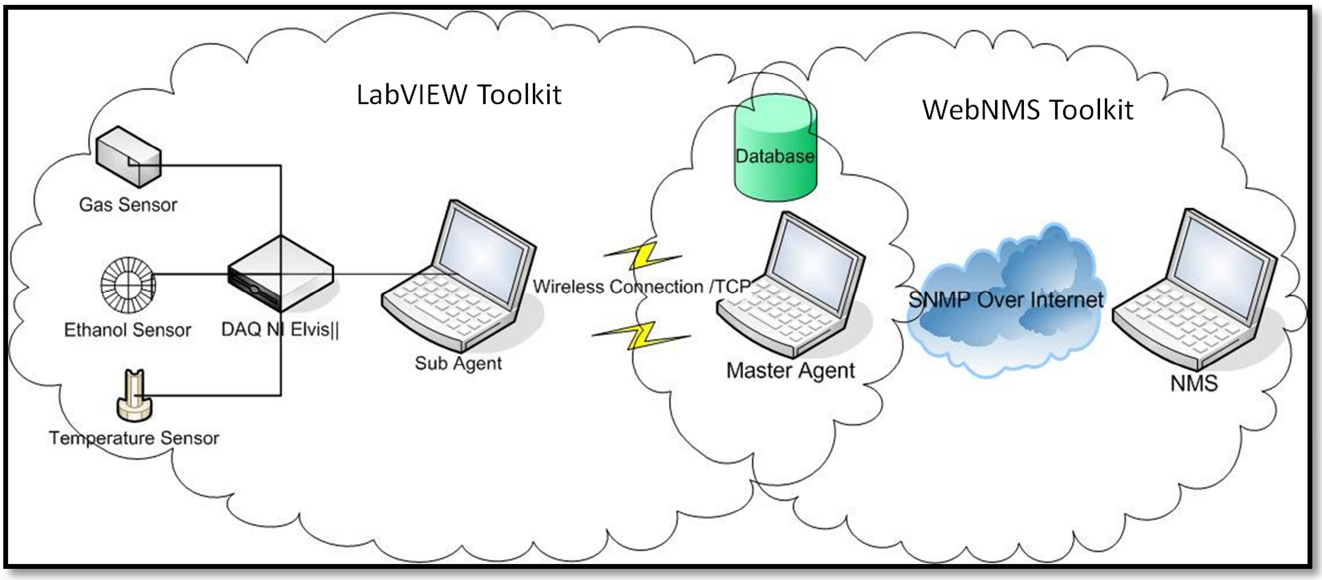


***Figure 2.** Representation of the Practical System.*

5.1. LabVIEW Toolkits

Three approaches to the sub agent sending mechanism had been tested; the first is real time sending of the sensors' readings; the second is sending the sensors' reading at a predefined intervals, these intervals are chosen according to each sensor; the final approach is to send each sensor reading when the change in the reading is more than a specific tolerance value. The last approach has been called smart sending. Then the last two approaches were combined to form smart-timed approach to send the sensor reading, furthermore a user capability to get the sensor reading as soon as he wants is added to this approach.

Figure 3 shows a flow chart of this approach. It starts initializing the system by assigning IP address and port number, and then it opens a TCP connection between the sub agent and the master agent. The first sensor reading is stored as $SR_{(n)}$, then the sensor timer is started, during this interval the sensor reading is updated in real time through data acquisition board $SR_{(n+1)}$ and it is send to the master agent, if a manual get order from the master agent is pressed or there is a difference between the last two successive readings that is more than a specific sensor tolerance, otherwise it waits until the timer is finished and sends the sensor reading.

Figure 4 shows the LabVIEW implementation of the smart timed approach.

On the other hand, the master agent LabVIEW receiver model is shown in Figure 5, it consists of a TCP listen block that waits until a connection on a specific port is opened, then a TCP read block reads the sub agent data, which is demonstrated using a waveform chart block on the front panel.

In order to use the SNMP protocol, the sensors reading should be stored in an MIB database. We chosed Microsoft Access database to store these reading using LabVIEW database toolkits. Figure 6 shows the LabVIEW model for saving the sensor data to Microsoft Access file. The path to the Access database file should be specified in the Universal Data Link (.udl) file which contains also the name of the ODBC connection that is created using ODBC applet of the Windows control panel. The path of this udl file should be specified in the LabVIEW database toolkit along with database table name that stores the sensor reading.

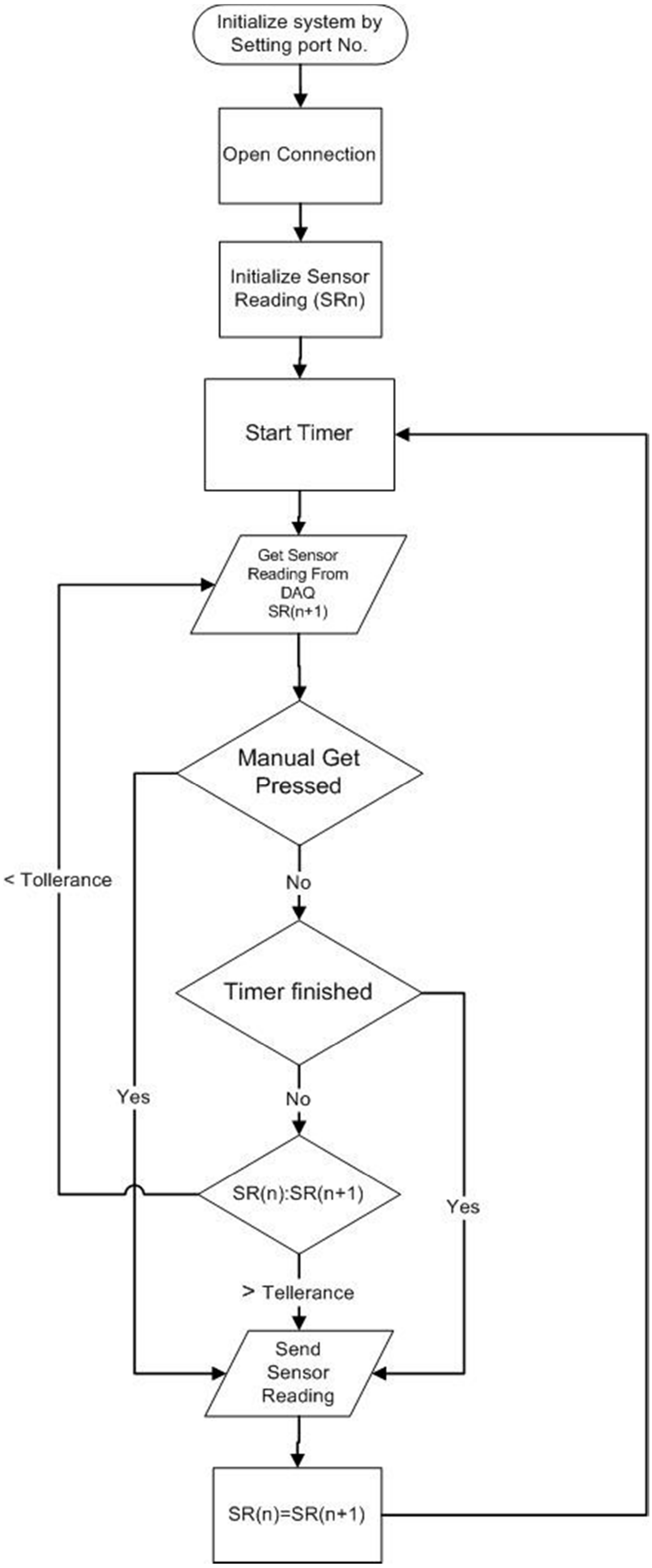


Figure 3. *Flow chart for Smart-Timed approach to send sensor reading.*

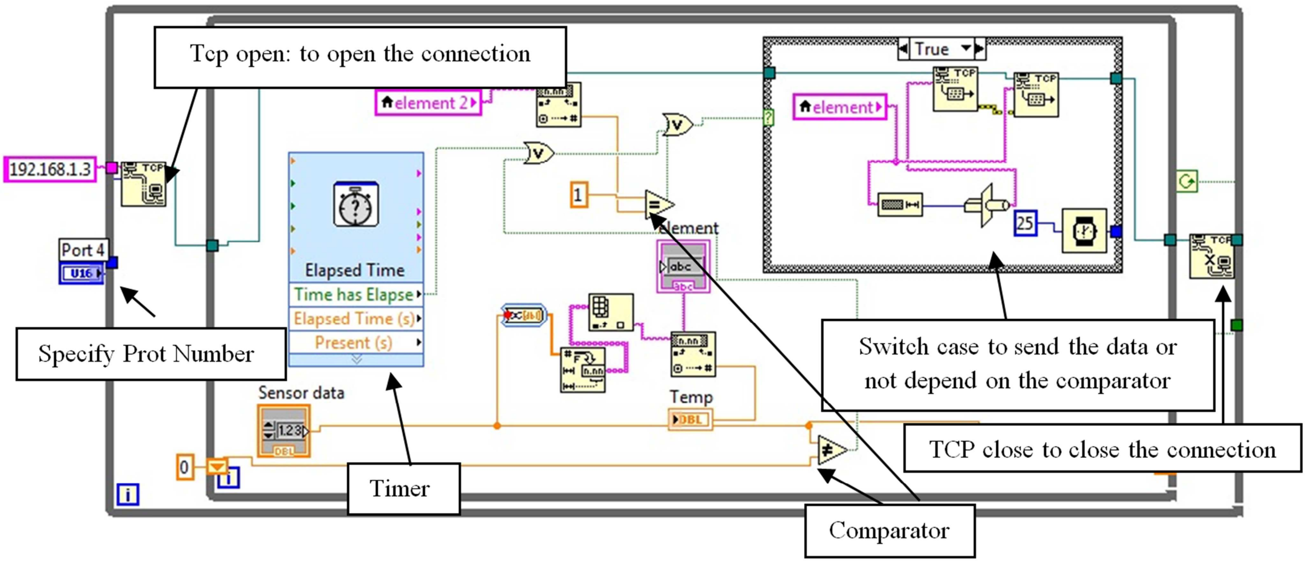


Figure 4. LabVIEW Model for Smart-Timed Approach.

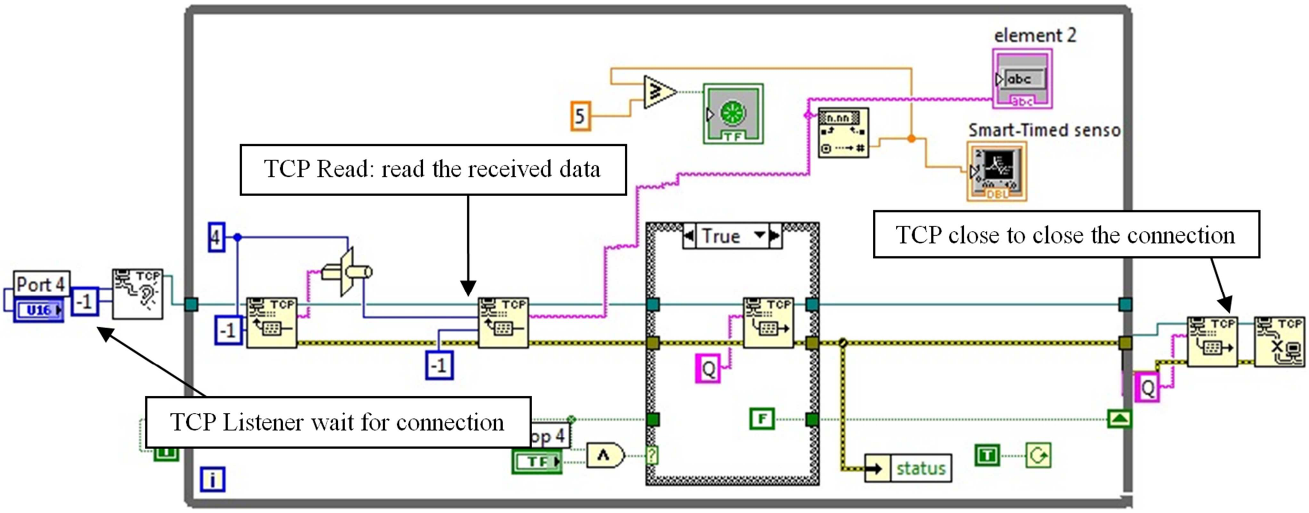

element 2
5
Smart-Timed senso
TCP Read: read the received data
TCP close to close the connection
4
True
Port 4
U16
-1
TCP Listener wait for connection
Q
F
status

Figure 5. LabVIEW Model of the receiver for sensor reading in the master agent side.

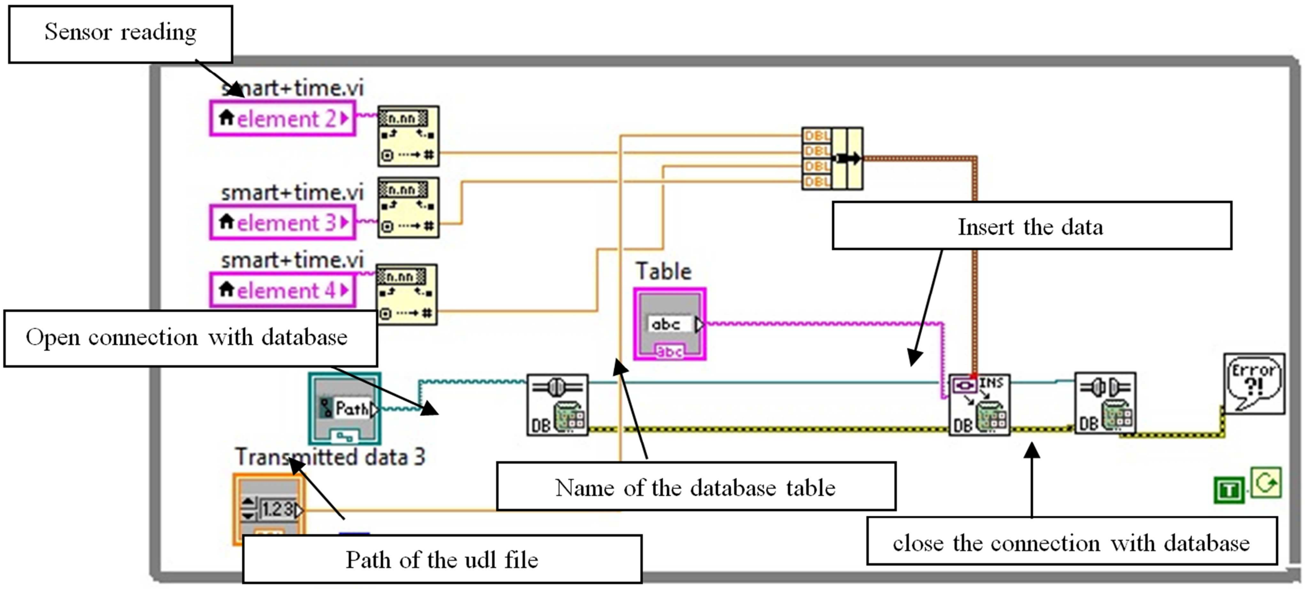


Figure 6. LabVIEW Model for saving the sensor data to the Microsoft Access file.

5.2. WebNMS Toolkits

The first step in using WebNMS for SNMP protocol is to design the MIB using MIB editor tool, the MIB file must be shared between the master agent and the manager (NMS). In this paper the MIB file is divided into two parts, the first is called sensor properties and contain all sensors information such as sensor ID, sensor name, threshold value and time interval for updating sensor value. The second part of the MIB is called sensor reading which contains the current value of each sensor. Figure 7 shows the desired MIB tree.

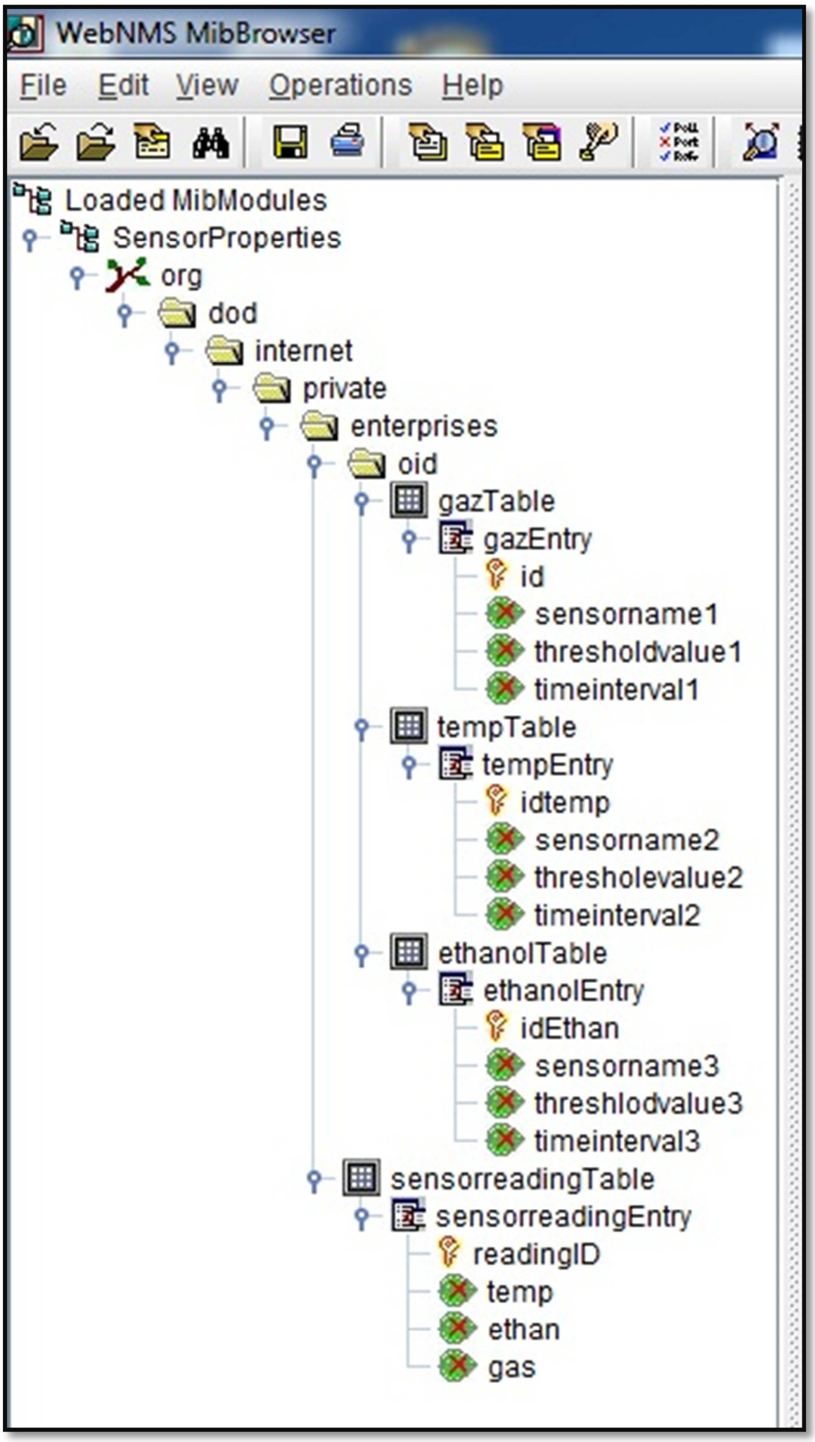


Figure 7. *MIB tree.*

The second step of applying WebNMS toolkit is using MIB compiler tool to associate the MIB file with the previously designed Microsoft Access file and setting some configuration properties such as SNMP version and port number.

Once the MIB is designed and compiled, the NMS can browse each sensor reading via the MIB browser tool of the WebNMS using the SNMP commands such as (Get, GetBulk, GetNetxt and Set), the master agent will respond to the SNMP command.

6. Results

The front panel shown in Figure 8 contains three wave form charts to demonstrate the three sensors' reading; while Figure 9 shows a zoomed in image of one of these sensors' front panel graphs. Each sensor front panel contains an alarm lamp to indicate that the sensor reading is above a threshold value specific to each sensor; also, it contains a push button to get the data instantly as the user wants.

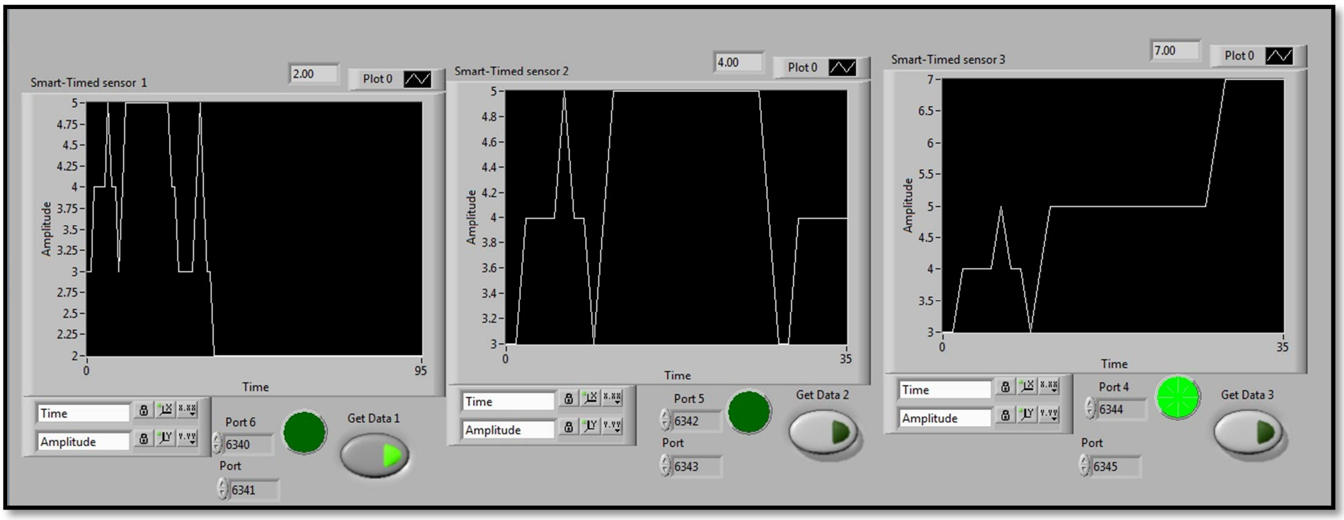


Figure 8. Front Panel of the Master Agent.

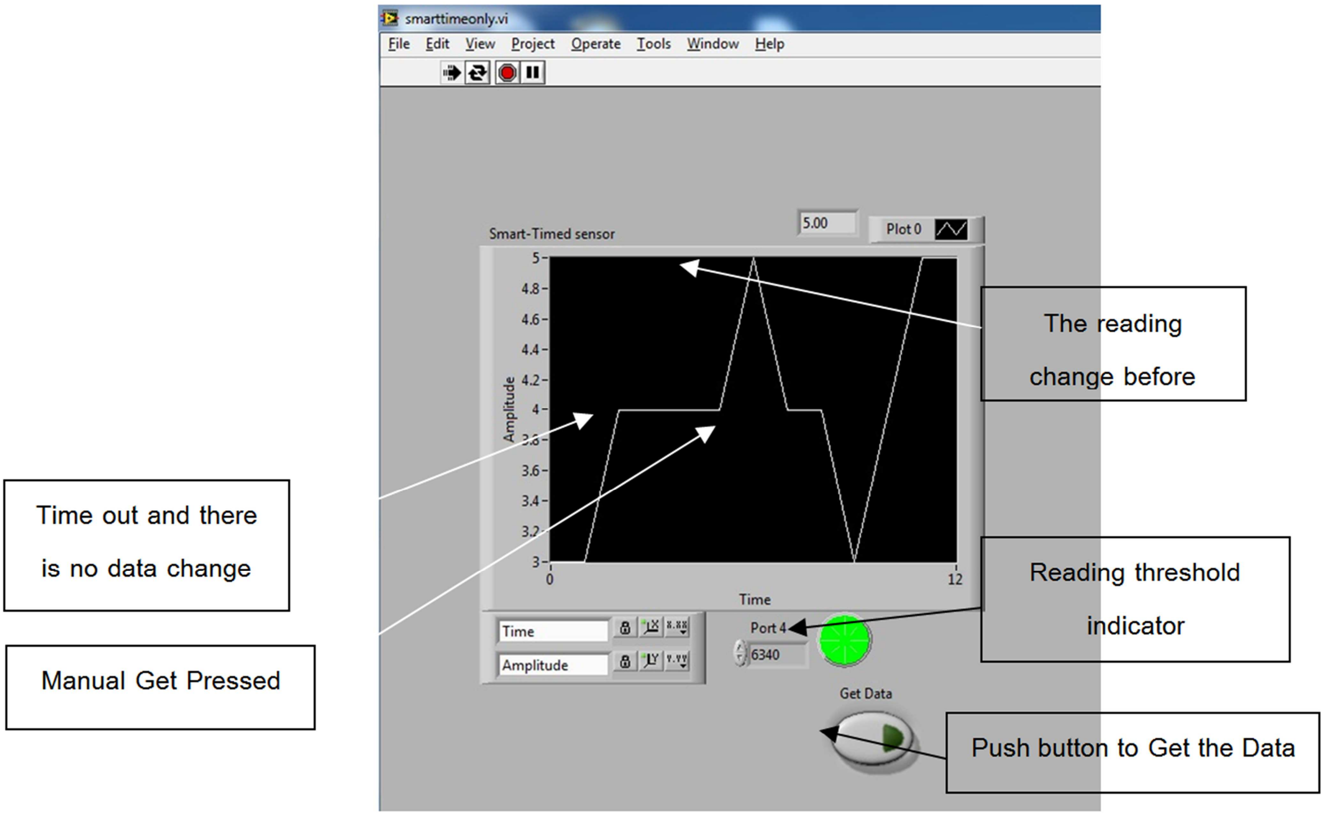
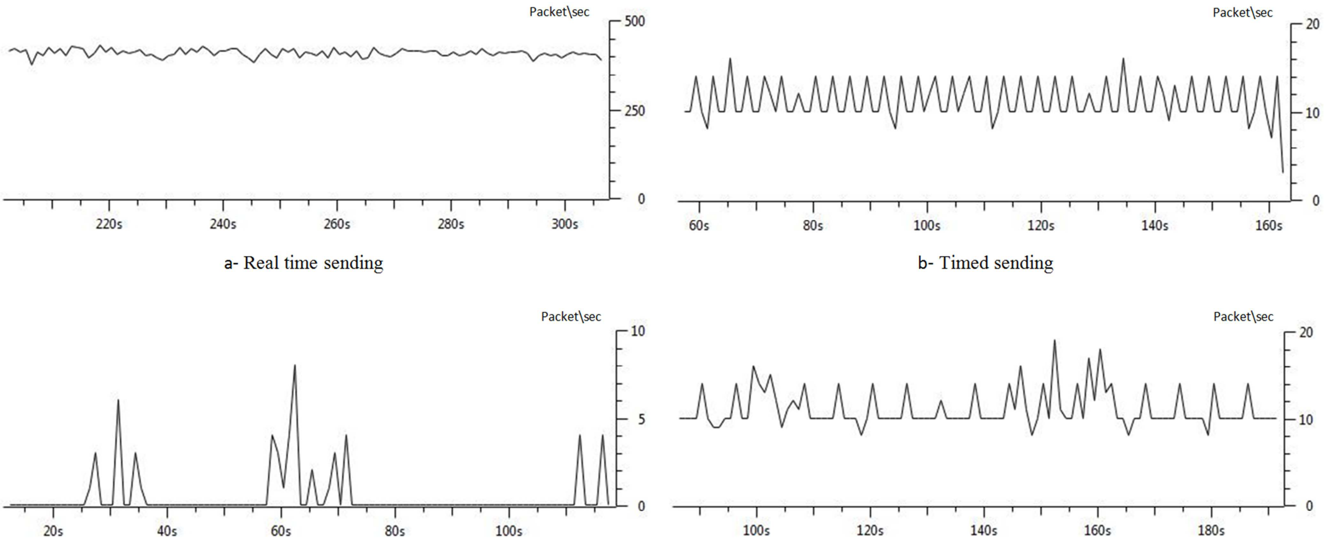

smarttimeonly.vi
File Edit View Project Operate Tools Window Help
Smart-Timed sensor
5.00
Plot 0
Amplitude
Time
0
12
Time
Amplitude
Port 4
6340
Get Data
The reading change before
Time out and there is no data change
Manual Get Pressed
Reading threshold indicator
Push button to Get the Data

Figure 9. Zoomed Front Panel for one.

Wireshark software was use to record the network traffic between the sub agent and the master agent for the three sending approaches, Figure 10 shows this network traffic.



a- Real time sending

b- Timed sending

c- Smart sending

d- Smart-Timed sending

Figure 10. *Traffic between sub agent and master agent for various sending approaches.*

It is obvious from Figure 11, which shows the traffic for real time, and smart-timed approaches the amount of traffic reduction using the later approach.

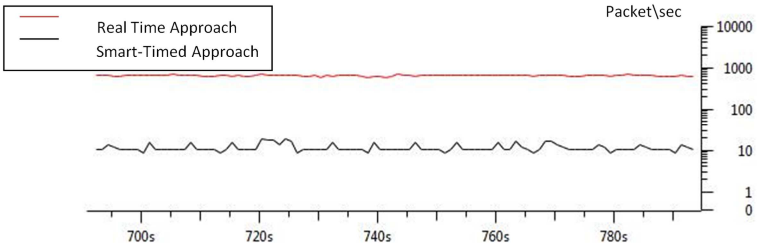


Figure 11. *Traffic for Smart-Timed Sending with Real Time Sending.*

The SNMP traffic between the master agent and the NMS is shown in Figure 12 for two modes: the first mode (Fig. 12a) using regular (every 5 sec) automated Get command and the second (Fig. 12b) using random manual issue of the Get command by the user. Figure 12 clearly shows the benefit of using SNMP protocol in reducing the traffic between the master agent and the NMS.

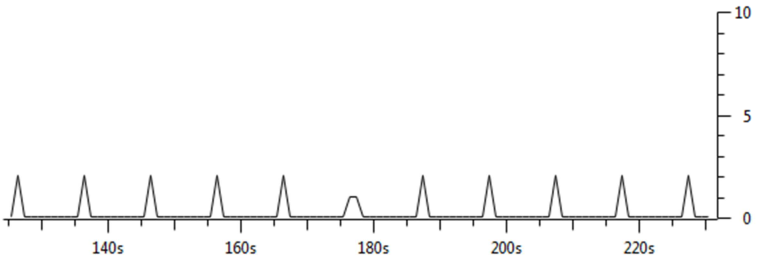


Figure 12a. *Regular automated Get command every 5sec.*

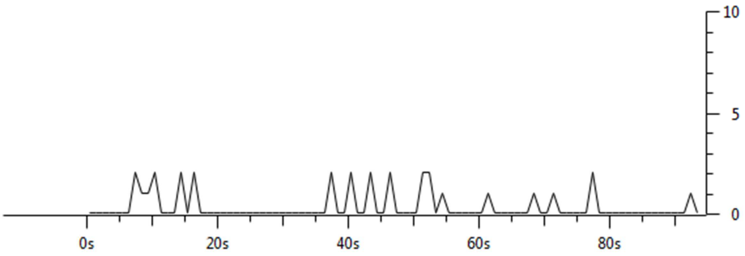


Figure 12b. *Random manual Get command.*

7. Conclusions

This paper demonstrates the application of LabVIEW as an SNMP proxy agent for smart home environment. Various sensors were connected to the system and their readings were observed remotely through the SNMP protocol. Three approaches for sending the sensor readings to the master agent were testes; one of them is a proposed smart sending which results in maximum reduction of traffic between the sub agent and the master agent.

References

[1] R. J. Robles and T Kim, “A Review on Security in Smart Home Development”, International Journal of Advanced Science and Technology, Vol. 15, pp. 13-22, February 2010.

[2] S. Tennina, M. Di Renzo, E. Kartsakli, F. Graziosi, A. S. Lalos, A. Antonopoulos, P. V. Mekikis, and L. Alonso, "WSN4QoL: A WSN-Oriented Healthcare System Architecture", International Journal of Distributed Sensor Networks, 2014.

[3] A. Ghobakhlou, A. Kmoch and P. Sallis, "Integration of Wireless Sensor Network and Web Services", 20th International Congress on Modelling and Simulation, Adelaide, Australia, 1–6 December 2013.

[4] A. M. A. H. Al-Kuwari, Dr. C. O. Sanchez, A. Sharif and V. Potdar “User Friendly Smart Home Infrastructure: BeeHouse”, 5th IEEE International Conference on Digital Ecosystems and Technologies, pp 257-262, 31 May -3 June 2011.

[5] X. Zhou, T. Huang, P. Liu, and Z. Liao, "Research on Smart Living Technology based on WSN", IEEE, pp. 938-941, International Conference, Intelligent Computing and Integrated Systems (ICISS), 2010.

[6] S. A. Chaudhry, G. Boyle, W. Song and C. Sreenan, "EMP: A Network Management Protocol for IP-Based Wireless Sensor Networks", International Conference on Wireless and Ubiquitous Systems, 2010.

[7] MonacmlDOUDI, H. Elkhorchani, K. Grayaa, "Performance Evaluation of Wireless Sensor Networks Based On Zigbee Technology in Smart Home", International Conference on Electrical Engineering and Software Applications (ICEESA), 2013.

[8] T. Adiono, R. V. W. Putra, M. Y. Fathany M. A. Wibisono and W. Adijarto, "Smart Home Platform Based on Optimized Wireless Sensor Network Protocol and Scalable Architecture", 9th International Conference on Telecommunication Systems Services and Applications (TSSA), At Bandung, Indonesia, 2015.

[9] D. Harrington, R. Presuhn and B. Wijnen “An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks” RFC3411, The Internet Society 2002.

[10] J. Schönwälder, and V. Marinov, “On the Impact of Security Protocols on the Performance of SNMP”, IEEE Transactions on Network and Service Management, Vol. 8, No. 1, pp 52-64, March 2011.

[11] D. R. Mauro and K. J. Schmidt, “Essential SNMP” 2nd edition, Published by O’Reilly Media, 2005.

[12] E. Bibbs and B. Matt, "Comparison of SNMP Versions 1, 2 and 3" ICTN 4600-001, 2006.

[13] Z. Yongliang, X. Yong, X. Jun and Z. Jiang, "Design of Remote Monitoring and Controlling System for Unattended Machine Room", IEEE, Fourth International Conference on Intelligent Computing Technology and Automation, pp 646-649, 2011.

[14] Cisco Press, "Internetworking Technologies Hand Book" 4th Edition, 2003.

[15] M. Fischer, “Enhancing the Re Mote Care Prototype by Adding an SNMP Proxy and Video Surveillance” Diploma Thesis in Computer Science, University of Sydney, 2008.

[16] J. Prasad and S. Indumathi, “Energy Conservation in Smart Home using LabVIEW” International Conference on Computing and Control Engineering, April, 2012.