

# Communication and Implementation of Plug and Play Enabled Devices in Sensor Network

Mr. Mahesh Kumar M.R <sup>#1</sup>, Mr. Sreenatha M <sup>#2</sup>

Assistant Professor <sup>#1, #2</sup>

Department of CS & E,

J.S.S Academy of Technical Education,

Affiliated to Visvesvaraya Technological University,  
Bangalore, India.

**Abstract** - Most of sensor networks are static in nature and do not provide standardized and systematic network management capabilities. Intelligence is not associated with the sensors. In order to make a sensor network more dynamic in nature, there is need to monitor the sensor network with the elements of the network management like Fault, Configuration, Security and Performance. This project is on the demonstration of Plug and Play (PnP) enabled devices (smart sensor node) in different levels to provide network and sensor management in dynamic fashion using Simple Network Management Protocol (SNMP) and Hyper Text Transfer Protocol (HTTP).

**Keywords** – SNMP, HTTP, smart sensor, Plug and Play.

## I. INTRODUCTION

Sensing technology is a cornerstone for many industrial applications. The ease and flexibility of sensor network has enabled us to use personal assistance devices to be used anywhere but at the same time it has many anomalies as well. Sensor network should be well monitored in order to detect anomalies in the network.

### A. Plug and Play

A network becomes dynamic when each of the components in the network must have Plug and Play (PnP) capability. Plug and Play suggest that a user can plug the sensor into the signal conditioning everything is automatically configured and is ready to take the measurements. Thus Plug and Play plays a very important role in managing a dynamic network. A Plug and Play enabled node in the network has to perform the following features:

- Announce its presence to other nodes in the network.

- Configure itself to the default setting during the startup.
- Acknowledge to client/servers in the network.

### B. Smart Sensor Node

A node becomes intelligent or smart sensor node:

- If it can communicate the data in the network and measure of the health of the node in the network (battery life).
- Smart sensor node should communicate through a network using common internet protocols such as TCP/IP [2].

There are many examples of implementation of smart sensor networks. Applications include using smart sensors to control traffic signal lights in metropolitan area, [1]. Another application has smart sensors used to monitor automobile controls, [5]. Other applications include large scale urban monitoring where wireless sensor nodes are used to monitor the environment, roadways, civil structures, [4].

### C. Problem Statement

Unlike the traditional network are more static in nature, sensor networks are dynamic and need strict monitoring in order to detect any anomalies in the sensor. Maintaining a good health of a sensor network is important in order to get reliable sensor data. There can be multiple levels of Plug and Play (PnP) in a system. While managing a sensor network involves detecting and anomalies in the sensors, detecting different events and alerts. Thus a node has to be intelligent in order to provide a good management support. It would not be possible for nodes on the network to communicate with each other if they are not interoperable. To be interoperable, the application layer protocol should be standardized.

#### D. Expected Outcome

SNMP and HTTP protocol has been proposed in order to achieve greater standardization base that includes widely accepted internet technologies and to make use of the tools that enable better visualization of network.

#### II. SENSOR NETWORK MANAGEMENT

A network management system consists of one or more management stations and several managed nodes in the network. The manager should be able to:

- Discover the network topology using the discovery messages obtained from all the managed nodes.
- Requests and reply information from managed nodes.
- Track various asynchronous events and alerts are also possible.

Since the nodes we want to keep track of are distributed, our only option is to use the network to manage the network. This means we need a protocol that allows us to read and write various pieces of state information on different network nodes. This project presents network management approach using two protocols: SNMP and HTTP.

#### A. Simple Network Management Protocol (SNMP)

SNMP is a specialized request/reply protocol that is used to manage the network for a long time. In an SNMP system one or more computer are called managers with a task of managing a group of nodes, where each managed nodes executes a software component called agent and reports information via SNMP to the manager.

Features of SNMP are:

##### 1) SNMP network topology discovery

This provides a way to discover the various SNMP managed nodes in the network using SNMP ping. The manager can request information using SNMP protocol from any of the discovered nodes.

##### 2) SNMP information exchange

An agent maintains information about the management variables and reports to the manager when requested.

##### 3) SNMP alert/event monitoring

Agent also has the capability of reporting asynchronous messages to manager systems.

#### B. Management Information Base (MIB) or Log file

Exactly how does the client indicate which piece of information it wants to retrieve and how does the server know which variable in memory to read to satisfy the request. SNMP uses an extensible design where the available information is defined by MIB. In this project MIB is replaced by a Log file which supports the features of MIB. The Log file is automatically created when system is started and it show which device is initially sensing with IP address, at what time systems received messages with date and if security provided, it shows an encrypted key generated for that session.

#### C. Optimized Link State Routing Protocol (OLSR)

OLSR is an IP routing protocol for wireless networks. OLSR is a proactive links state routing protocol, which uses Hello and topology control messages to discover and then disseminate link state information throughout the network [3]. Individual nodes use this topology information to compute next hop destination for all nodes in the network using shortest hop forwarding paths.

#### D. RC4 Algorithm

RC4 is a stream cipher, symmetric key algorithm. This algorithm is used for both encryption and decryption as the data stream is XORed with the generated key sequence. The steps for RC4 encryption algorithm is as follows:

- Collect the data to be encrypted with the selected key.
- Create two arrays of string type
- Initialize one of the arrays with numbers from 0 to 255.
- Assign the left out array using selected key.
- Depending on the array of the key, randomize the first array.
- The final key stream is to be generated by randomizing the first array within itself.
- To obtain the cipher text, XOR the data to be encrypted with the final key stream.

This project will display only an encrypted key in the respective application for each session. The same encrypted key can also be used for decryption (called symmetric key).

#### III. DEMONSTRATION OF THREE LEVEL OF PLUG AND PLAY USING SNMP

In order to make a network more dynamic in nature, intelligent nodes should be used means each

such node should provide data processing and networking capability. Intelligent nodes are called MobeeNet and Mobee. Both of these devices are manufactured by Mobitrum Corporation. In this project, MobeeNet and Mobee are replaced by laptops which support the features of intelligent nodes. MobeeNet (laptop) communicates with Mobee (laptop) using IEEE 802.11g/b wireless router as the data link layer protocol.

Figure 1 shows three level of PnP possible using SNMP protocol. Initially manager (laptop 1) try to connect with number of systems in the network by making a ping operation or selecting the IP address of system which is displayed on the application then manager will know the systems in the network. This discovery is done periodically and thus manager detects new MobeeNet and Mobees in the network. Manager should check the battery status of system before going to start a application so that possible runtime failures can be avoided or whether the system are suitable for long time operation or not.

At the second level each MobeeNet (laptop 2) has SNMP agent and Log file. Mobees do not provide SNMP agent capabilities and make use of MobeeNet's Log file to store all its management information. Log file provides a table for indicating the Mobees connected to MobeeNet and which information the system has been received with date and time. First level of PnP can be achieved between manager and MobeeNet.

At the third level each Mobee (laptop 3) should have two options: on and off. Whenever a Mobee is turned on, it should broadcast messages to MobeeNet and MobeeNet store this information in Log file. Whenever a Mobee is in turned off, it fails to broadcast message to MobeeNet and its entry in the Log file is not stored. Thus second and third level of PnP is also possible between MobeeNet and Mobee and Mobee with built in sensor.

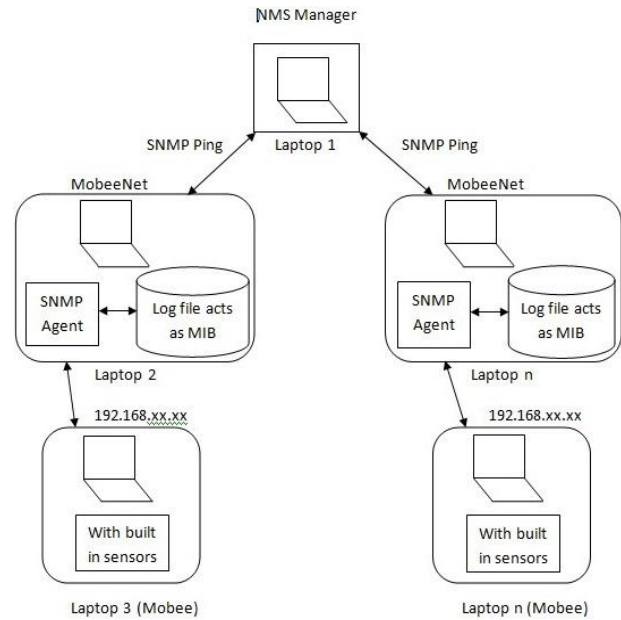


Fig. 1: Three level of Plug and Play using SNMP.

#### IV. DEMONSTRATION OF THREE LEVEL OF PLUG AND PLAY USING HTTP

This approach is similar to the SNMP except that there is no requirement of Log file. All the information related to a node can be displayed on the web page (web browser) in the manager station. Hyper Text Transfer Protocol (HTTP) protocol is used to transfer information from a node to manager station. In this approach, each MobeeNet has to run a web server to reply to the requests sent by manager. Web server retrieves all the information and sends this updated information to manager to display it on html page. In figure 2, the architecture of a sensor network management using HTTP protocol is presented.

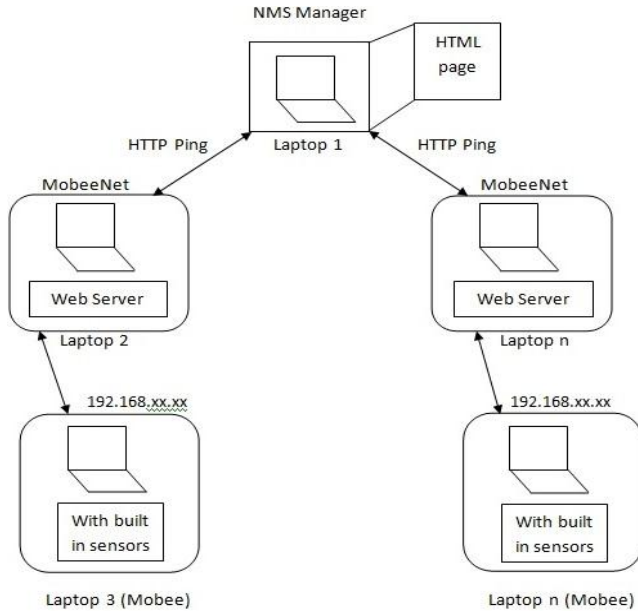


Fig. 2: Three level of Plug and Play using HTTP

V. RESULTS AND DISCUSSIONS

Figure 3 and 4 shows a snapshot for manager or network management system application and MobeeNet application showing battery status and IP address of neighboring systems in the network. Once Manager and MobeeNet application are started, IP address of manager should display in the interface list of MobeeNet application and IP address of MobeeNet should display in the interface list of manager application. Then we select the respective IP address and press start button in both the applications and after some time observe the neighboring IP address should show in neighbor box of both the applications. A Log file is created automatically when we start the application with started date. Communication between the two applications should show in a Log file. Log file acts as a database that can store communicating messages with received date and time, how many possible routes are there for communication, information about sensing system with IP address, encrypted key for each session.

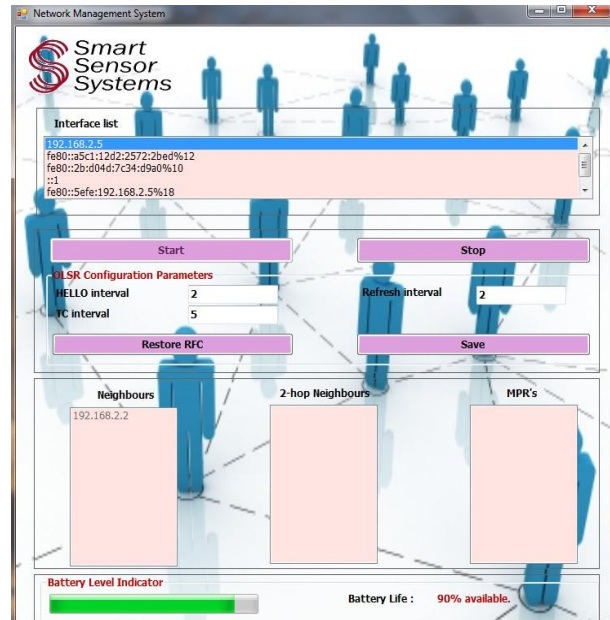


Fig. 3: Manager Start up screen showing battery status at the end and MobeeNet IP address in neighbor box.

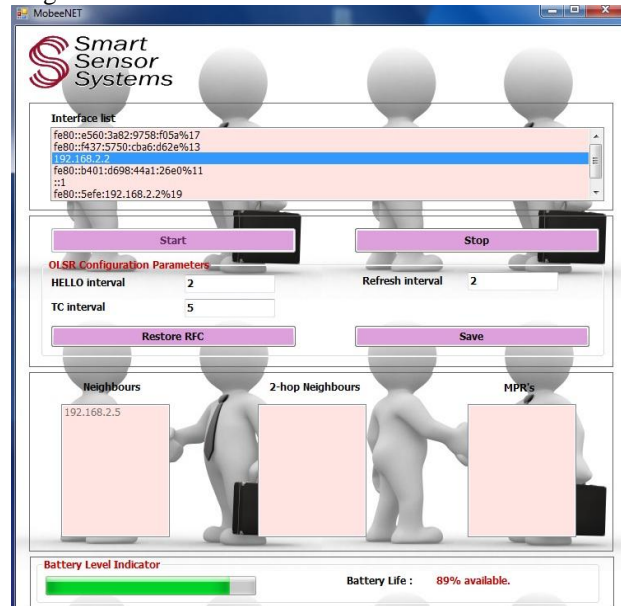
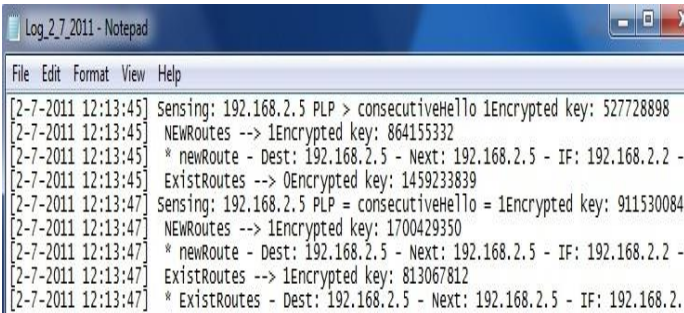


Fig. 4: MobeeNet application showing battery status at the end and manager IP address in neighbor box.



```
Log_2_7_2011 - Notepad
File Edit Format View Help
[2-7-2011 12:13:45] Sensing: 192.168.2.5 PLP > consecutiveHello 1Encrypted key: 527728898
[2-7-2011 12:13:45] NEWRoutes --> 1Encrypted key: 864155332
[2-7-2011 12:13:45] * newRoute - Dest: 192.168.2.5 - Next: 192.168.2.5 - IF: 192.168.2.2 -
[2-7-2011 12:13:45] ExistRoutes --> 0Encrypted key: 1459233839
[2-7-2011 12:13:47] Sensing: 192.168.2.5 PLP = consecutiveHello = 1Encrypted key: 911530084
[2-7-2011 12:13:47] NEWRoutes --> 1Encrypted key: 1700429350
[2-7-2011 12:13:47] * newRoute - Dest: 192.168.2.5 - Next: 192.168.2.5 - IF: 192.168.2.2 -
[2-7-2011 12:13:47] ExistRoutes --> 1Encrypted key: 813067812
[2-7-2011 12:13:47] * ExistRoutes - Dest: 192.168.2.5 - Next: 192.168.2.5 - IF: 192.168.2.
```

Fig. 5: Log file showing communication between Manager and MobeeNet.

## VI. CONCLUSION

This project is on the demonstration of three levels of Plug and Play achieved using intelligent nodes and SNMP. SNMP protocol and Log file defined for all the components that make up a sensor network then it will be simple and easy to identify them and also used to achieve PnP from one access point such as a manager on the network. SNMP and HTTP usage has been proposed in order to achieve greater standardization that includes widely accepted internet technologies and to make use of the tools that enable better visualization of network.

## REFERENCES

- [1] Wall, R.W.; Huska, A., "Design platform for plug-and-play IEEE 1451 traffic signal", Industrial Electronics Society, 2005. IECON 2005. 31<sup>st</sup> Annual Conference of IEEE Volume Issue, 6-10 Nov. 2005.
- [2] suman gumudavelli, Deniz Gurkan, and Syed Alamdar Hussain and Ray Wang., "A Network Management Approach for Implementing the Smart Sensor Plug and Play", IEEE 2009.
- [3] Nesrine Ayed Sahloul, Lamia Ben Azzouz and Farouk Kamoun., "OLSR based Peer to Peer Instant Messaging for Ad-hoc Networks", IEEE 2010.
- [4] C. F. Garcia-Hernandez and P.B. Ibarquengoytia-Gonzalez, J. Garcia- Hernandez, and J. Perez-Diaz, Wireless Sensor Networks and Applications: a Survey, International Journal of Computer Science and Network Security, Vol. 7, No. 3, March 2007.
- [5] Lee, K., Kim, M., Lee S., Lee, H., "IEEE 1451 Based Smart module for In-Vehicle Networking Systems of Intelligent Vehicles", IEEE Transactions on Industrial Electronics, Vol. 51, No. 6, Dec. 2004.