Journal of Computer Science 10 (9): 1819-1826, 2014
ISSN: 1549-3636

doi:10.3844/jcssp.2014.1819.1826 Published Online 10 (9) 2014 (http://www.thescipub.com/jcs.toc)

SELF POWERED ENERGY AWARE INTERNET OF THINGS

[1]Vimala, T. and [2]Uma Rajaram

[1]Deptartment of ECE, Dr.M.G.R. Educational and Research Institute University, Chennai, India
[2]Dr.M.G.R. Educational and Research Institute University, Chennai, India

Received 2014-02-12; Revised 2014-02-15; Accepted 2014-04-26

ABSTRACT

Recently embedded things with IP address and giving the ability to communicate self using mailbox/message concepts is gaining importance. In this study, energy conservation by forming a network of smart objects, communicating through central unit via IP address is focused. IoT comprise of smart modules communicating and interacting with each other and the environments. The IoT enabled devices can command and control their operation within themselves without human intervention and save more energy and time.

Keywords: Internet of Things, Energy Conservation, IP Address, Wi-Fi

1. INTRODUCTION

We're entering a new era of computing technology that many are calling the Internet of Things (IoT). Hence, from a technology perspective, the IoT is being defined as smart machines interacting and communicating with other machines, objects, environments and infrastructures, resulting in volumes of data generated and processing of that data into useful actions that can "command and control" things and make life much easier for human beings (Kaivan and Atkinson, 2013).

The aim of this study is to conserve power through internet of things, in which each object is connected to one another and to a central control unit. The objects communicate with each other and to the central unit through IP address and their ports. The Internet of Things (IoT) is a scenario in which objects, animals or people are provided with unique identifiers and the ability to automatically transfer data over a network without requiring human-to-human or human-to-computer interaction. Noelia *et al*. (2013) in the Internet of Things (IoT) paradigm, any of the objects that surround us can be placed on the network in one form or another.

2. MATERIALS AND METHODS

2.1. Wi-Fi

In most countries depending on the regulatory regimes, Wi-Fi operates in three non-interfering, non-overlapping frequency channels in the 2.4 GHz band and up to 24 channels in the 5 GHz band. Wi-Fi networks use multiple non-overlapping channels to avoid co-channel interference and hence optimize performance. However, in dense, high-capacity deployments, co-channel interference may occur and cause degradation in performance is discussed in (Wi-Fi Alliance, 2013).

Wi-Fi networks provide convenient Internet access. Today Wi-Fi networks provide network connectivity for a variety of computing devices.

Wi-Fi network coverage is adequate when signal strength, Received Signal Strength Indicator (RSSI) and/or Signal to Noise Ratio (SNR), everywhere in the coverage area (Vanhatupa, 2013).

2.2. Internet of Things

Imagine a world where billions of objects can sense, communicate and share information, all interconnected over public or private Internet Protocol (IP) networks. These interconnected objects have data regularly collected, analyzed and used to initiate action, providing a wealth of intelligence for planning, management and decision making. This is the world of the Internet of Things (IoT).

The IoT is comprised of smart machines interacting and communicating with other machines, objects, environments and infrastructures. As a result, huge volumes of data are being generated and that data is being processed into useful actions that can "command and control" things to make our lives much easier and

Corresponding Author: Vimala, T., ECE Deptartment Dr.M.G.R. Educational and Research Institute University, Chennai, India

safer-and to reduce our impact on the environment. The creativity of this new era is boundless, with amazing potential. IPv6's huge increase in address space is an important factor in the development of the Internet of Things. The Internet of Things is currently being applied in a wide variety of uses throughout the home, businesses, hospitals, cars and entire cities. This is clearly discussed in the work (Internet of things.pdf).

2.3. IPv4 and IPv6 Structure

Internet Protocol is a set of technical rules that defines how computers communicate over a network. There are currently two versions: IP version 4 (IPv4) and IP version 6 (IPv6). IPv4 was the first version of Internet Protocol to be widely used and accounts for most of today's Internet traffic. There are just over 4 billion IPv4 addresses. While that is a lot of IP addresses, it is not enough to last forever. IPv6 is a newer numbering system that provides a much larger address pool than IPv4 (APNIC eLearning, 2013).

2.4. IPv4 Structure

IPv4 employs a 32-bit address, it limits the number of possible addresses to 4, 294, 967, 296. A core function of IP is to provide logical addressing for hosts (Balchunas, 2013). **Figure 1** shows the IPv4 header structure and it indicates 32 bits.

2.5. IPv6 Structure

The total number of IPv6 addresses available actually would be enough to provide an IPv6 address to every single object that exists today; not just computers, kitchen appliances, cars and any other electronic devices but also non-electronic devices such as pens, books, cups, dentures and so on (A10 Networks, 2013).

IPv6 provides a large number of advantages that will benefit all end-users and organizations. Many vendors of enterprise and consumer electronics are offering support for IPv6 network connectivity, for both IPv6 management and IPv6 traffic handling that is on par with IPv4 functionality. However, the transition from IPv4 to IPv6 cannot be achieved instantly. **Figure 2** shows the IPv6 header structure and indicates 128 bits. Companies realize that even with IPv6 implementation in their networks, there still will be a need to communicate with legacy IPv4 servers and applications. On the other side of the equation, companies also realize their IPv4 customers will need to use services developed with IPv6, such as Microsoft Direct Access. This problem is discussed in (Balchunas, 2013).

2.6. Tunneling Concepts

Tunneling techniques are used on top of an existing IPv4infrastructure and uses IPv4 to route the IPv6 packets between IPv6 networks by transporting these encapsulated in IPv4. Tunnelling is used by networks not yet capable of offering native IPv6 functionality. It is the main mechanism currently being deployed to create global IPv6 connectivity. **Figure 3** clearly indicates the tunneling concept. Tunneling is a technique by which one transport protocol is encapsulated as the payload of another (APNIC eLearning, 2013).

2.7. Related Work

Wi-Fi has become such an amazingly successful technology because it has advanced while remaining backwards compatible (ANI, 2013). This study (APNIC eLearning, 2013) explains the latest advance in Wi-Fi, 802.11ac, which provides the next step forward in performance (Kaivan and Atkinson, 2013). The pervasiveness of embedded processing is already happening everywhere around us. At home, appliances as mundane as your basic toaster now come with an embedded MCU that not only sets the darkness of the piece of toast to your preference, but also adds functional safety to the device. This study (Salih *et al*., 2012) discusses about the development of an intelligent omni-directional mobile robot. There are energy-aware systems that can now generate a report on the activity in your house and recommend ways to reduce your energy consumption.

In this article (Serbulent *et al*., 2012) the feasibility of low-power Wi-Fi to enable IP connectivity of battery-powered devices is studied with three key practical areas of concern: Power consumption, impact of interference and communication range. At high data rates, transmitting/receiving data and packet size have small impact on power consumption. In this study (Noelia *et al*., 2013), different representations of Wi-Fi access point signal information are tested on a hierarchical indoors localization sys-tem to identify the one that yields the least amount of localization error.

2.8. Implementation

2.8.1. Example

We assign Node 1 (pyro sensor) to sense the environment and it sends the output to the processor via I2C or SPI communication. Then the processor sends action required signal to the Driver circuit and Driver circuit gives the command to the Device. All the devices including the control unit is connected to one another through Wi-Fi and communicates on the Internet Protocol version 6 (IPv6). The following block diagram explains the communication among two nodes.

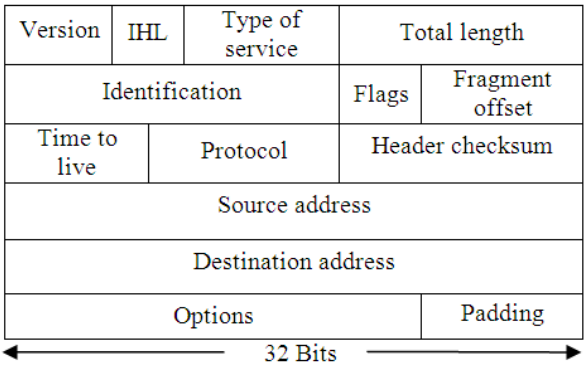

Fig. 1. IPv4 header structure

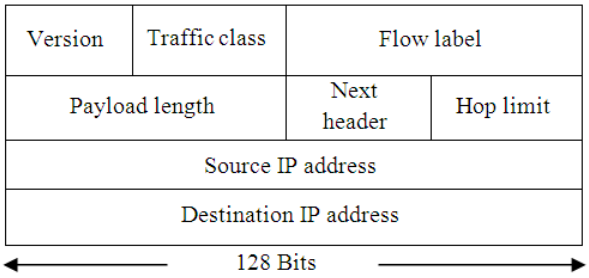

Fig. 2. IPv6 header structure

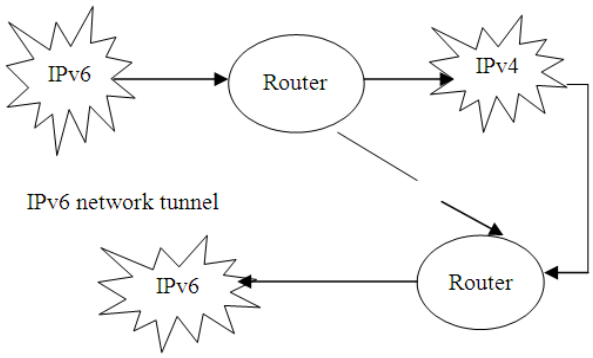

Fig. 3. Tunneling concept

Two nodes 1 and 2 are used with the features shown in the following **Table 1**. The Raspberry Pi has a Broadcam BCM2835 System on Chip (SoC) which includes an ARM1176JZF-S 700 MHz processor, VideoCore IV GPU and was originally shipped with 256 megabytes of RAM, later upgraded to 512 MB. It does not include a built-in hard disk or solid-state drive, but uses an SD card for booting and persistent storage.

Table 1. Features of nodes (Raspberry Pi)

Nodes (Raspberry Pi)	Features
Node 1 and Node 2	IP address Battery powered LAN enabled Wi-Fi enabled ARM II processor HDMI interface USB ports

2.9. Communication Among Nodes

Here Node 1 has a mail id (domain) node1@ gmail.com and Node 2 has a mail id node2@ yahoo. in. Both the nodes are connected with the internet via one switch as shown in **Fig. 5.** Node 1 writes the control action (to be performed at Node 2) to the mail. After receiving the mail, Node 2 reads the mail and the required action is performed. The above operation is explained in **Fig. 5.**

Here the switch is ON and OFF based on the requirements of the environment. When the switch is ON Node 1 writes in the mail as Device needs to be ON. After receiving the mail, Node 2 reads the mail and the device is switched ON. Here SNMP Protocol is used to send the information for node 1 and POP 3 Protocol is used to receive the information for node 2 from node 1 as explained in the following **Table 2**.

Similarly when the switch is OFF, Node2 writes in the mail as devise needs to be OFF. After reading this mail from the mail box the Device is switched OFF. This is explained in the above tabular column.

2.10. Connectivity

Communication between node and device is carried out by processor and Driver circuit is shown in **Fig. 4.** Initially we should check the connectivity of the network whether it is to be LAN or Wi-Fi enabled. After finding the type of network we should assign the network protocol for Node 1 and Node 2 as clearly indicated in **Fig. 6**. SNMP protocol is for Node 1 for writing mail and POP 3 protocol for Node 2 for reading mail. We will discuss these two protocols in short manner.

2.11. Simple Network Management Protocol (SNMP)

SNMP is the most popular protocol used to manage networked devices. One of the most common uses of SNMP is for remote management of network devices. SNMP is popular because it is flexible. Vendors can easily add network-management functions to their existing products. The SNMP protocol enables network and system administrators to remotely monitor and configure devices on their network, such as routers, switches, hubs and servers.

Table 2. Switching process of node 1 and node 2

Node 1(SNMP) Mail id of node 1		Node 2(POP 3) Mail id of node 2	
Switch	node1@gmail.com	node2@yahoo.in	Device
ON	Device needs to be ON	Device is switched ON	ON
OFF	Device needs to be OFF	Device is switched OFF	OFF

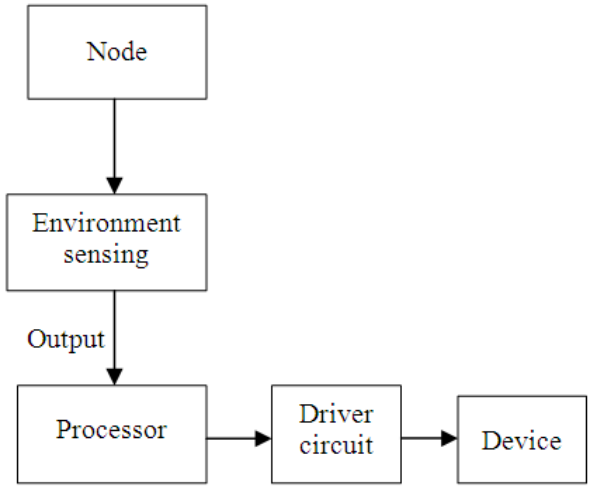

Fig. 4. Block diagram of communication between two nodes

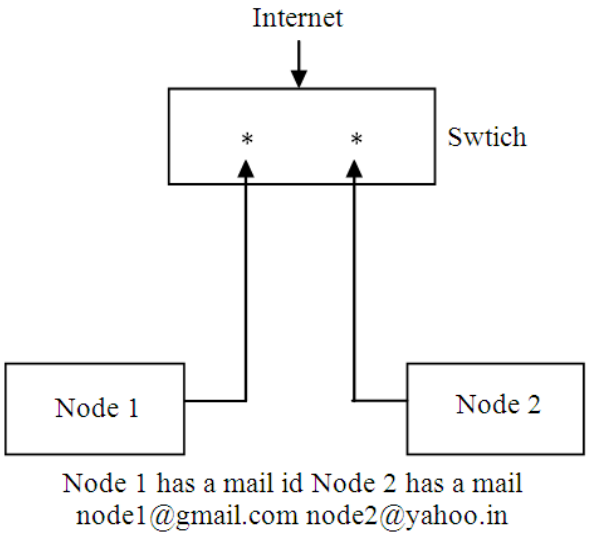

Fig. 5. Communication among two nodes

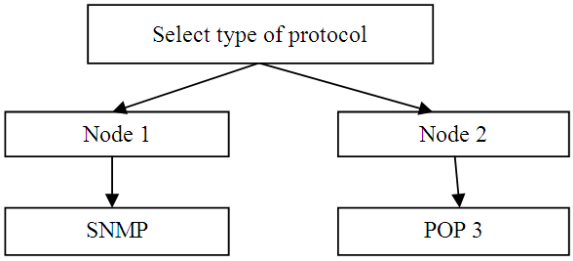

Fig. 6. Protocol selection

For example, if a system administrator wants to know how much traffic is flowing through network device, she might poll the device using SNMP. Once the data is pulled from the router or switch, it can be interpreted in a number of different ways. Network traffic throughput is not the only thing you can monitor using SNMP. It is also used to monitor CPU usage, device voltage and attributes and environmental conditions. For example, a system administrator could monitor the temperature of a router chassis based on information obtained through use of SNMP. These information is discussed in detail in this work (CERT®CC, 2002).

2.12. Post Office Protocol 3 (POP 3)

This protocol is the most often used protocol for receiving email over the Internet. A connection to a POP3 server must be made in order to read email. However, POP3 is by far the most common protocol for reading email from an email account. Once connected, the email messages in an account are numbered (starting with 1) and the account is locked. This number identifies email in the account. The account is not renumbered when email is deleted, but it is renumbered after the connection is closed. Only one connection to your POP3/IMAP account is allowed at any one time. Once connected, any new arriving email is not posted until you have closed the connection (UsersManual, 2013).

2.13. Experimental Setup

The Procedure for network initialization of Wi-Fi and LAN in Raspberry Pi are tabulated in **Table 3** and **Table 4**. The Raspberry Pi is a credit-card-sized single board computer developed in the UK by the Raspberry Pi Foundation. The hardware implementation of sensor side interface in IOT and device side interfaced in IOT as shown in the **Fig. 7 and 8.**

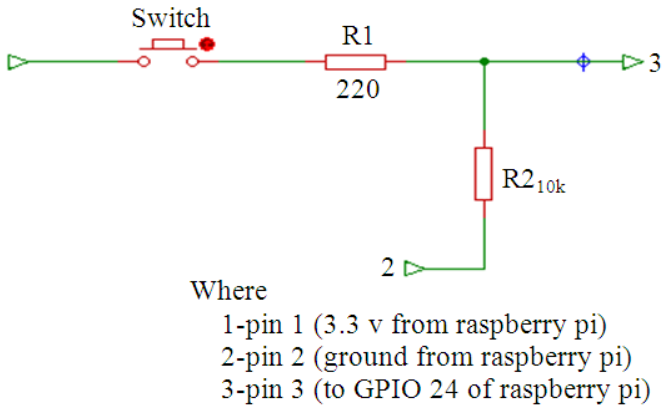

Fig. 7. Sensor side interface in IoT

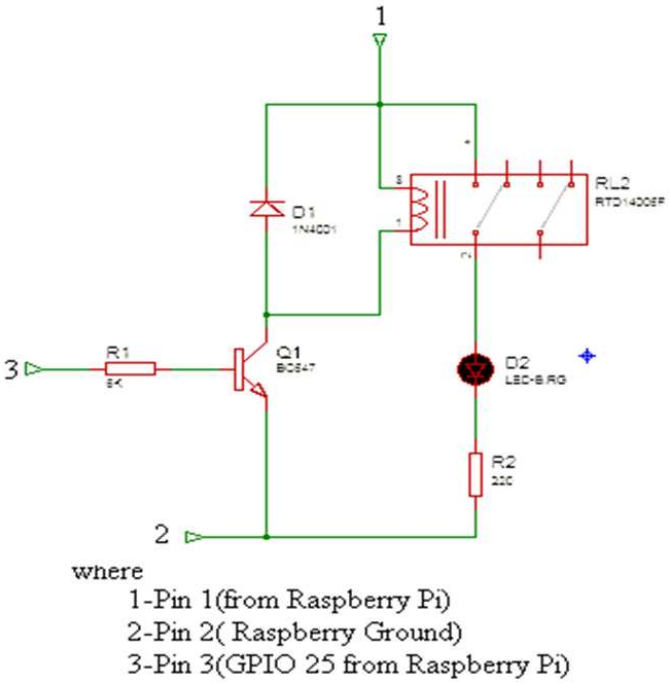

Fig. 8. Device side interfaced in IOT

Table 3. Wi-Fi initialization of raspberry Pi

Wi-Fi network initialization in raspberry Pi
Auto lo
iface lo inet loopback
auto wlan0
allow-hotplugh wlan0
iface wlan0 inetdhcp
wpa-ssid “mgruniv” #wifinetwort name
wpa-ssid “samurai123” #wifi password

Table 4. LAN initialization of raspberry Pi

LAN Network initialization in raspberry Pi
Iface lo inet loopback
Iface eth0 inetdhcp
allow-hotplug wlan0
iface wlan0 inet manual
wpa-roam /etc/wpa_suppplicant/wpa_supplicant.conf
iface default inetdhcp

3. RESULTS

The following two snap shots (**Fig. 8 and 9**) of mail boxes indicates that node 1 sent the mail to node 2 using their specified mail ids. Selected option, mail id and sensor IoT sent mailbox are shown as 1, 2 and 3 in the snapshots. The **Fig. 10** shows the mail box of Device IoT. It indicates that node 2 receive the mail from node 1 using their specified mail ids. Device IoT mail, inbox of Device IoT received mail from node 1 as shown as 1 and 2 in snap shot. The **Fig. 11** shows the Device IoT mailbox which clearly indicates the mail received from Sensor IoT.

4. DISCUSSION

Previously Many IoT related research work has been conducted under different names such as pervasive and ubiquitous computing, wireless sensor networks and so forth. In the research work of (Erin *et al*., 2013), they discussed about data from the sensors could be read or accessed through mobile RFID readers or smart phones. They discussed IoT Architecture is an integration of heterogeneous Wireless Sensor and Actuator Networks (WS and AN) into a common framework of global scale and made available to services and applications via universal service interfaces.

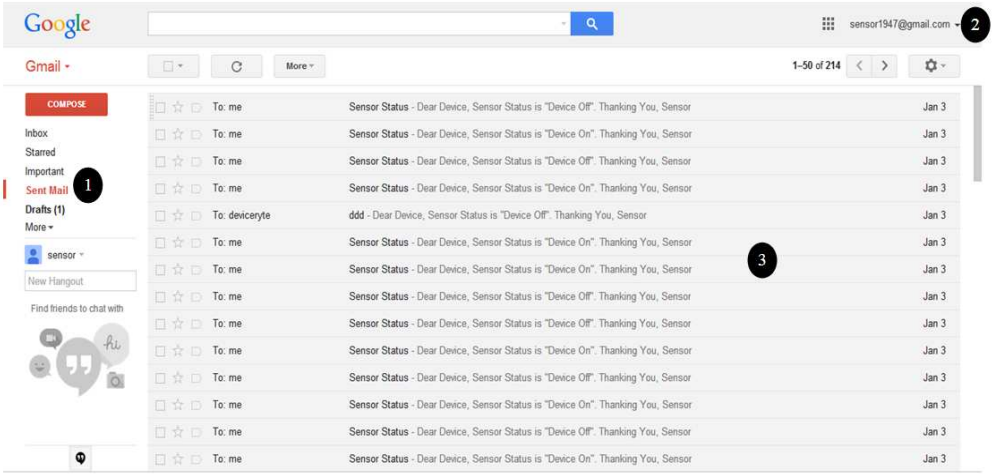

Fig. 8. Selected option (2) Mail ID and sensor IOT (3) sensor IOT sent mailbox

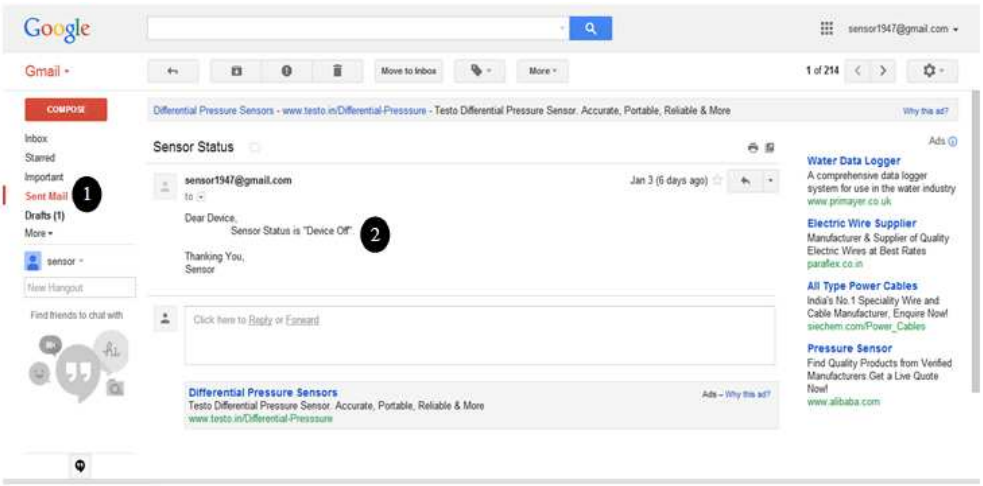

Fig. 9. Selected option (2) sent mail of sensor IOT

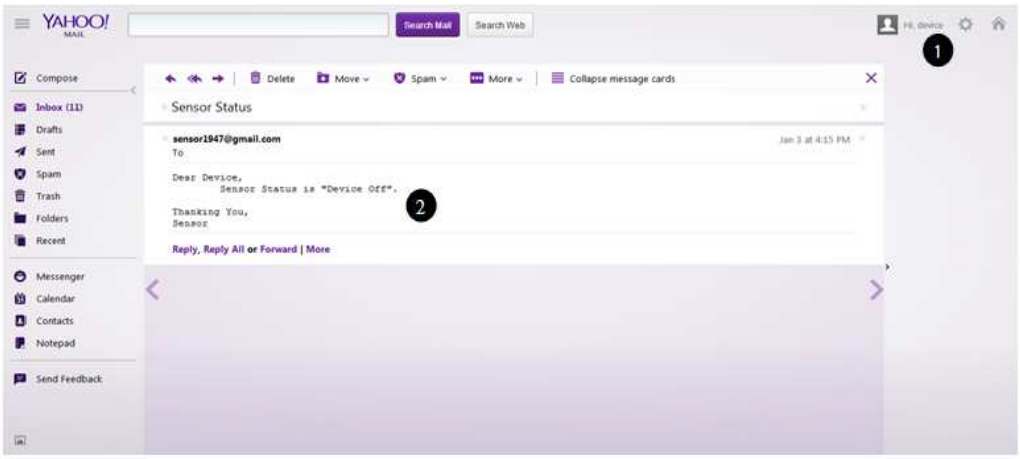

Fig. 10. Device IoT mail (2) inbox of device IOT received mail from sensor1947@gmail.com

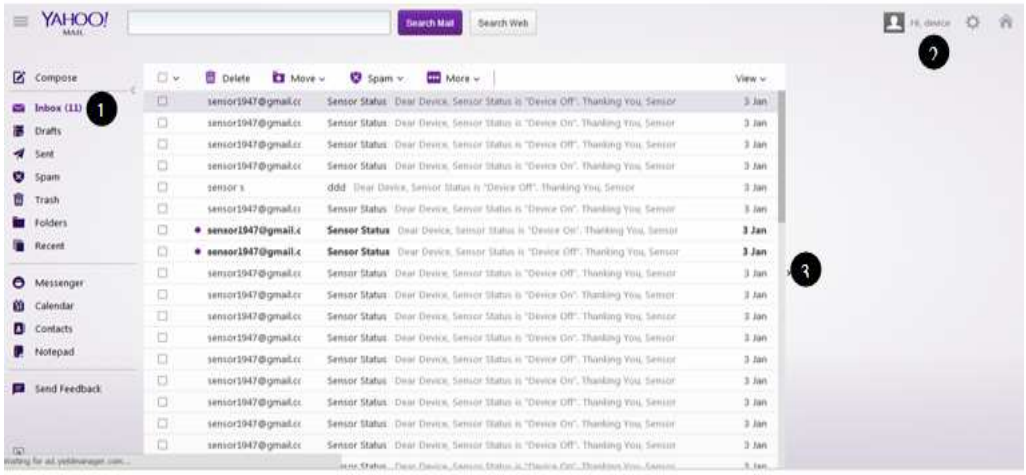

Fig. 11. Selected option (2) device IoT mail (3) Inbox showing mails received from sensor IOT

5. CONCLUSION

We propose Self powered energy aware nodes which are enabled by Wi-Fi network and capable of communicating self using mail box based on Internet of Things. In this setup all the nodes is connected to one another through Wi-Fi and communicates on the Internet Protocol version 6(IPv6). Here two nodes are accessing their own mail box, according to the specified work indicated in the mailbox and the required action is taken. We have implemented sensor side interface IoT and Device side interface IoT to communicate both two nodes self using their mail id. Our experiments demonstrate that node 1 writes the control action to be taken at the mail node1@gmail.com and node 2 opens the mail reads the message content and appropriate action is taken place. Future direction of study shall focus on connecting IoT in a grid with more nodes coordinating (without a domain mode) in the Internet Protocol address space.

5. REFERENCES

A10 Networks, 2013. The End of IPv4? Migration paths to IPv6. ©2013 A10 Networks.

ANI, 2013. 802.11ac In-Depth. Aruba White Paper, Aruba Networks, Inc. 2013.

APNIC eLearning, 2013. IPv4 to IPv6 Transition. APNIC eLearning

Balchunas, A., 2013. IPv4 Addressing and subnetting. IPv4 Addressing and subnettingv1.41.

CERT®CC, 2002. A brief tour of the simple network management protocol. CERT® Coordination Center.

Erin, A., A. Bassi, D. Caprio, S. Dodson and R.V. Kranenburg *et al*., 2013. Discussion paper on the internet of things. Ekahau Wi-Fi Design White Paper Commissioned Institute.

Kaivan, K. and G. Atkinson, 2013. What the Internet of Things (IoT)needsto become a reality. White Paper, Freescale Semiconductor.

Noelia, H., J.M. Alonso, M. Oca˜na and M.K. Marina, 2013. Impact of signal representations on the performance of hierarchical wifi localization systems.

Salih, J.E.M., M. Rizon and S. Yaacob, 2012. Designing omni-directional mobile robot with mecanum wheel. Am. J. Applied Sci., 3: 1831-1835. DOI: 10.3844/ajassp.2006.1831.1835

Serbulent, T., M. Senel, W. Mao and A. Keshavarzian, 2012. Wi-Fi enabled sensors for internet of things: A practical approach. IEEE Commun. Magaz., 50: 134-143. DOI: 10.1109/MCOM.2012.6211498

UsersManual, 2013. (SEE-USR). SMTP/POP3/IMAPemail Engine. Version, 7.2.

Vanhatupa, T., 2013. Wi-Fi capacity analysis for802.11ac and 802.11n: Theory and practice. Ekahau Wi-Fi Design Paper Copyright © 2013 Ekahau, Inc.,

Wi-Fi Alliance, 2013. Wi-Fi in Healthcare: Improving the user experience for connected Hospital applications and devices.