A SURVEY OF THE STATE OF THE ART IN ZIGBEE

Jobina Mary Varghese[1],Nibi K V[2],Vijo T Varghese[3] and Sethuraman Rao

Amrita Center for Wireless Networks and Applications, Amrita Vishwa Vidyapeetham
Kollam, India

ABSTRACT

ZigBee is one of the most widely used wireless communication technologies. ZigBee is being widely used for sensor communications and many other research fields. Why consider ZigBee? Because it is cheap and has better compatibility when compared to other communication technologies. We have given a detailed description on comparison between all the available technologies. In this paper, we have discussed some basic concepts about ZigBee and its security aspects in networking. We have also listed out the major manufacturers who are into the production of the transceivers for ZigBee.

KEYWORDS

ZigBee, ZigBeePRO, Protocol stack, Security, Physical layer, Application and network layer

1. INTRODUCTION

There has always been a need for transmission of data wirelessly. There are many technologies which are presently being used to transmit data using the unlicensed spectrum in the ISM band. Some of them are Bluetooth, NFC, Wi-Fi, and ZigBee.

In this paper we will be discussing about ZigBee and its protocol standards. ZigBee is used to create small personal area networks using low power digital radios. Because of its low power consumption ZigBee devices can transmit within a transmitting range of 10meters to 100 meters in line of sight. The topologies used are mesh and star network to interface between each other. Most of the ZigBee transceivers are designed to fragment the data if the data size it larger than 128 bytes. The data rate observed in ideal ZigBee transmissions is 250kbps, which is operated in the 2.4 GHz band [1]. ZigBee transceivers are mostly used in sensors boards to send the sensed data, for remotely controlling some devices like quad copter, etc. ZigBee technology is cheaper when compared to Wi-Fi and Bluetooth technology.

Apart from ZigBee there are other wireless transceivers that are used for data transfer or some kind of communication. In this section we will be discussing briefly about some of the most commonly used wireless transfer technology.

Bluetooth is one of the most widely used wireless technologies for short range communication, commonly used in Mobiles and other data sharing devices. It works in the 2.4 to 2.485 GHz band. It uses frequency hop spread spectrum (radio technology). Bluetooth 4.0 has a data rate of 24Mbits/s approximately and it uses the principle of Piconet to establish the connection between the fixed nodes.

MiWi is a wireless protocol designed by Microchip Technology for wireless personal area network. This protocol is only supported on some of the Microchip PIC and dsPIC microcontrollers. And it is to note that it has a simpler protocol than ZigBee, which is more complex.

Some of the other specifications are ISA100.11a and Wireless HART which also uses 802.15.4 as its base but there are some changes on the top layers which are not recognized by the IEEE 802.15.4. All of these mentioned above are used for short range and low data rate communications.

2. NODE TYPES IN ZIGBEE

There are mainly two types of nodes in ZigBee network – FFD (Full function device) and RFD (Reduced function device). Communication of different types of devices is possible through FFD. An FFD has three modes in which it can operate. The first mode is the PAN coordinator mode – In this mode the node sends beacon frames, provides routing information and manages short network specific address. The second mode is the coordinator mode – the node acts as a router. In the third mode, the node acts as a normal device [2].

In a star topology the PAN coordinator selects a unique PAN id (Personal area network), which is used in the communication of all nodes with the PAN coordinator.

An FFD can communicate between every other device in a peer to peer topology, which is in range but a RFD will only communicate with one FFD at a given time. A cluster network can be created with a single cluster head communicating with other clusters.

3. LAYER DESCRIPTION

In this section we will be discussing the different stack layers. The layers are Physical layer, MAC layer, Network layer, Application layer. As in Figure 1.

3.1. The physical layer (PHY)

Physical layer is the first layer in the OSI model. It provides data transmission service. The PHY is responsible for the RF transceiver, channel's selection and signal management.

It operates in 2.4 GHz frequency band throughout the world with up to sixteen channels. There are two other frequency bands where the 802.15.4 can be used. They are the 868 to 868.6 MHz band (used in Europe) and the 902 to 928 MHz frequency band (used in North America). These bands have one and 30 channels respectively, which can be used by the RF transceiver. The physical layer is based on DSSS (direct sequence spread spectrum). IEEE 802.15.4A was released in the year 2007, expanding the four PHY to six. This also included PHY using UWB and CSS.

The physical layer has the following functions assigned to it.

- Transceiver activation and deactivation.
- Selection of a suitable channel and assessment of the channel.
- To receive and transmit packets

3.2 MAC Layer

The MAC (Medium Access Control) layer enables the transmission of the MAC frames through the physical channel. The services MAC layer provides are:

- Beacon Management
- Channel access
- GTS (Guaranteed Time slot) management
- Frame validation
- Acknowledgment
- Association and Disassociation

3.3 Network Layer

This layer is built on the MAC layer of IEEE 802.15.4. The network layer is responsible for routing which must be specific to the topology being used. It's also responsible for the security. Some other functions dealt by the layer are new device configuration, Network start-up, Joining or leaving of network, addressing, neighbour discovery and reception control.

3.4 Application Layer

- Keeping tables to perform binding.
- Fragmentation and reassembly
- Provide communication endpoints for application
- Determining devices and services available for the layer.
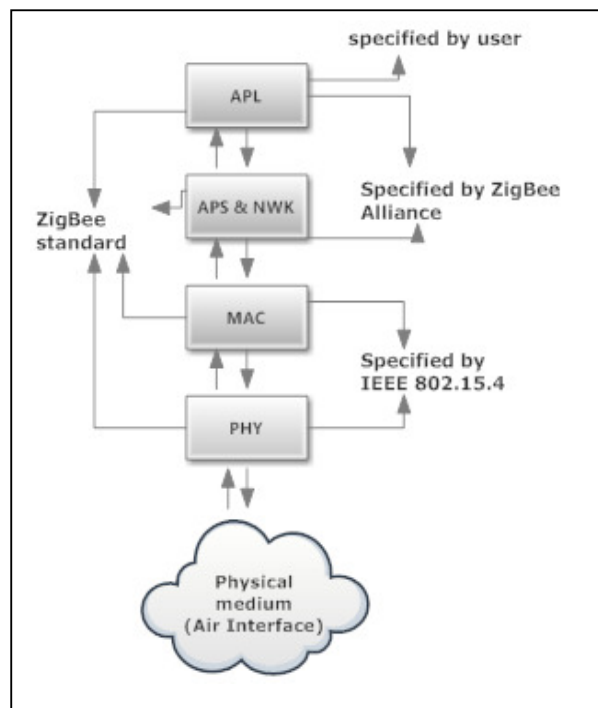- Initiating or responding to binding requests between endpoints.

Figure1. Structure of IEEE802.15.4 protocols stack

4. SECURITY STANDARDS

There always exists the need for encryption of the data. In this section we will be discussing about the security standards used in the ZigBee transceivers while communicating to other nodes. The algorithm used for encryption is advanced encryption standard. The key length is 128 bits. A unique encryption method is necessary due to the fact that most of the ZigBee transceivers have a specific hardware design. The AES algorithm is used for Data Integrity also. This is done by appending a Message Authentication Code (MAC) to the message. The MAC size may vary from 32 to 128 bits, however it is mostly created using 128b AES algorithm [3]. Data security is performed by encrypting the data payload field with 128 bit key.

4.1 ZigBee Security

ZigBee implements two extra security layers on top of the 802.15.4. –First one is the network layer and second one is the application security layer. All the security policies are dependent on the encryption followed.

   There are three keys that need to be considered:
- Master key- They are preinstalled in the device/ node. Their function is to keep the link keys exchange confidential in the Key Establishment procedure.
- Link keys- These are unique in each node and are managed by the application layer. More memory resources are required because there is a need for encrypting the information shared between two devices.
- Network Key- It's a key that is shared among all the nodes in the network. It is generated at different intervals. Only if the node has the network key they can join the network. The new network key is shared using the old network key.

There are two policies that the trust centre (the one which generates the network key) follows:

- Commercial mode: Shares the master and link keys with any devices in the network.
- Residential mode: Share only the Network key (this is done in order to cope with low memory resources).

5. ZIGBEE ALLIANCE

The ZigBee Alliance is an association of a group of companies which are working together to achieve the vision to [4] enable low power, reliable, low-cost, wirelessly networked, monitoring and control products based on an open global standard. The revolution in wireless technology has caused emergence of many standards in ISM radio band. There have been multiple types of proprietary protocols for control applications, which need interfacing. For a globally accepted communication standards between sensors in low data rate wireless networks many companies have forged an alliance. Thus this ZigBee Alliance that created ZigBee came into being. ZigBee has been developed for communication with sensors which deal with simple data structures. For high data rate operations like multimedia files and software etc. we normally use Wi-Fi and Bluetooth.

ZigBee alliance improved the specification and published it for the first time in 2005. In 2007 they updated old versions of the existing ZigBee and introduced two feature sets ZigBee and ZigBee Pro. ZigBee Alliance provides the hardware, software and reference designs to the members to build ZigBee applications. ZigBee is a low power by-product of Wi-Fi. Low size low power radios on IEEE 802.11.15.4 Wireless Personal Area Networks standard was accepted by

the ZigBee alliance in December 2004. ZigBee PRO Feature Set is most popular among developers. It increases the capabilities of the ZigBee Feature Set, and supports creation of wider networks. It is also compatible with ZigBee Feature Set networks.

6. ZIGBEE STANDARDS

Industry experts design innovative standards for specific market needs of consumers. ZigBee standards help product manufacturers to improve their product capability to meet customer needs. They take advantage of the strengths of ZigBee low-power wireless standards so that products can run on batteries for years. This feature makes them easy to use for greener homes and offices.

- ➢ ZigBee Building Automation [5] (Efficient commercial spaces)
  - • Interoperable products enabling the secure and reliable monitoring and control of commercial building systems.
  - • Appliances, Thermostats, Door locks, Lights ,Security, sensors, Closures
  - • BACnet® approved wireless mesh network standard
  - • Networking with ZigBee PRO
- ➢ ZigBee Remote Control [6] (Advanced remote controls)
  - • ZigBee Remote Control 2.0
  - • Backward compatible with 1.0 and 1.1versions
- ➢ ZigBee Smart Energy [7] (Home energy savings)
  - • ZigBee Smart Energy version 1.1
- ➢ Smart Energy Profile 2 [8]
  - • IP-based home energy management for both wired and wireless product standard
  - • SEP 2 is an evolution of ZigBee Smart Energy 1.x
  - • Designed for the ZigBee RF4CE specification.
- ➢ ZigBee Light Link (LED lighting control)
  - • Global standard for interoperable and easy-to-use consumer lighting and control products.
- ➢ ZigBee Telecom Services [9] (Value-added services)
  - • Global standard for interoperable products enabling value-added services, such as information delivery, mobile gaming, location-based services, advertising, billing, payments, and peer-to-peer data-sharing.
- ➢ ZigBee Network Devices [10]
  Device specific standards designed to assist and expand ZigBee PRO-based networks.

7. SPECIFICATIONS

ZigBee Alliance provides three specifications, namely ZigBee IP, ZigBee RF4CE, and ZigBee PRO with Green power specifications. It enables the creation of interoperable market standards for base networking system. Specifications support robust and competitive supply chain. This will help the consumer to add ZigBee to the product appropriately.

7.1 ZigBee and ZigBee PRO

ZigBee is robust mesh network defined by the core ZigBee specification. It is an innovative, self-healing, self-configuring system, with battery-free nodes that provide ease of use, flexibility and mobility. ZigBee PRO and ZigBee are two available feature sets for ZigBee. As seen in Table 1 we can compare ZigBee and ZigBee Pro. ZigBee PRO supports larger networks with more than thousand devices with low power consumption and is a widely accepted specification. The new

innovative feature of ZigBee PRO is the Green Power which supports energy harvesting devices without external power supplies.

Table 1.Comparison of ZigBee and ZigBee pro

Features	ZIGBEE	ZIGBEE PRO
Addressing	Tree addressing	Tree addressing with stochastic addressing.
Mesh data management	AODV mesh routing.	AODV routing with many-to-one source routing.
Fragmentation	Enable	Enable
Dynamic best channel choice		Enable
Node to node connections	Not asymmetric	Asymmetric
Security	AES 128bit and a global network key to create secure communications.	P2p encryption for couple of nodes with their own key.
Communication	Unicast, broadcast and group communication.	Limited broadcast addressing hence "high" level security.

7.2 ZigBee IP Specification

The first open standard for the full wireless IPV6 mesh network is ZigBee IP. ZigBee IP provides Internet connections to have less power and low cost devices. It has the capacity to connect various devices into a single central control network. Its design purpose is to support the upcoming ZigBee Smart Energy version 2[11]. The most promising ZigBee Internet Protocol specification was released in March 2013. In a wireless mesh network, it has the properties of auto-configuring and self-healing. So it will help to achieve high robustness and reliability. It has no-touch deployment with automatic channel selection and route establishment etc. Node addressing of IPv6 protocol supports individual addressing on each node. This specification support radio frequencies for global operation in 2.4 GHz, frequency of 915MHz in America , 868 MHz frequency in Europe and 920 MHz frequency in Japan. TLS v1.2 protocols with a range of cryptographic algorithms are used for end-to-end security [15].

7.3 ZigBee RF4CE Specification

The ZigBee RF4CE was designed for a simple, two-way device-to-device control application. In spite of the ZigBee specification, it does not require the full-featured mesh networking ability, enabling low cost implementation of ZigBee RF4CE designed with lower memory size requirements. Other advantages are simple device-to-device topology, easy development and testing, and faster time to market. For duplex communication, the ZigBee RF4CE provides simple, robust and low-cost communication. It is the best interoperable consumer electronics featuring solution [12].

It standardizes multi-vendor control for consumer electronics and home entertainment equipment. Originally it was defined for four CE companies, Panasonic, Philips, Samsung and Sony, in 2009. The main design criteria for the ZigBee RF4CE is for connecting the consumer electronic devices such as remote controls, keyboards, mice, pointers, etc. It has the ability for multivendor interoperability between end-devices and host devices (targets) like HD-TV, DVR, Set-top box, Blue-ray player, computers, etc. It works based on 2.4 GHz MAC/PHY IEEE 802.15.4 Standard. It has a thin, flexible and future proof networking layer. This will easily coexist with various 2.4GHz technologies. ZigBee RF4CE Network (NWK) layer is a thin layer enabling a star

topology network. This layer is also responsible for channel management, device discovery and pairing mechanism, secure communication link establishment, power saving mechanisms, and multiple packet data transmission option [16].

7.4 ZigBee PRO with Green power Specification

ZigBee has been modifying its specifications since 2004. In 2012 ZigBee Alliance introduced ZigBee PRO with Green power. The low power networking ability in IoT applications of ZigBee PRO with Green power helps large networks with numerous devices to be handled easily. It is compatible with ZigBee PRO networks. ZigBee router can create proxies of ZigBee PRO Green Power devices so that it will create an illusion that the device is always present in the network whether it is powered ON or OFF. The packet forwarding and resend of the proxies communicate to the sink devices which are not in direct range of the ZigBee Green power devices. It is battery less and uses 100-500 AμJ of energy, energy gained by flipping a switch via common energy harvesting techniques. Lighting, HVAC, Closure (ending the process of power consumption) and Energy management devices are ideal for Green Power Feature [17].

8. PROGRAMMABILITY OF ZIGBEE

Cost effective wireless connectivity to devices in ZigBee mesh network can be established by means of XBee and XBee-PRO (an XBee module that uses ZigBee Pro mesh networking protocol) ZigBee modules. The important features of these modules are they are interoperable with other ZigBee devices; they require only minimal power and provide reliable delivery of data between remote devices, as seen in Table 2. The module can operate within the ISM 2.4Ghz frequency band and it is compatible with XBee RS-232 Adapter, X Bee RS-485 Adapter, XBee Analog [13] I/O Adapter, XBee Digital I/O Adapter, XBee Sensor, XBee USB Adapter, XStick, Connect Port X Gateways, and XBee Wall Router.

9. CHIPSET VENDORS

In this section we will be discussing the chipset vendors for the ZigBee transceiver. It is to note that even though there are radio modules which are 802.15.4 enabled they will not support ZigBee stack because of not enough flash memory. Some of the vendors who create only the RF transceiver are (does not include microprocessor) given in Table 3. Table 4 consists of the Manufacturers list that makes Integrated MCU and transceiver modules.

Table 2.Features of each module

XBee	XBee-PRO (S2)
Indoor/Urban: up to 40 m	Indoor/Urban: up to 90m and 60 m
Outdoor line-of-sight: up to 120 m	Outdoor line-of-sight: up to 2 miles
Transmit Power: 2 mW (3 dBm)	Transmit Power: 50mW (17dBm), 10mW (10dBm)
Receiver Sensitivity: -96 dBm	Receiver Sensitivity: -102 dBm
TX Peak Current: 40 mA (@3.3V)	TX Peak Current: 295mA

Table 3. List of RF transceiver manufacturers

Manufacturer	Module name
Flexi Panel Ltd	EasyBee
Embit	EMB-TRX169PA, 169 MHz
Microchip Technology	MRF24J40MA

Table 4. List of manufacturers who are making ZigBee transceivers.

Manufacturer	Module Name
Atmel	ZigBit 2.4 GHz (ATZB-24-B0)
	ZigBit 2.4 GHz (ATZB-24-A2)
	ZigBit 2.4 GHz Amplified (ATZB-A24-U0)
California Eastern Laboratories	ZICM357SP2
	ZICM357SP0
	ZICM3588SP0
Digi International	Series 1 XBee
	Series 1 XBee-PRO
Embit	EMB-Z2530PA, 2.4 GHz
	EMB-ZRF212B, 868 MHz, 915 MHz
	EMB-ZRF231PA, 2.4 GHz
NXP	JN5168-001-M00
	JN5168-001-M05
	JN5168-001-M06
FlexiPanel Ltd	Pixie
	Pixie Lite
Radiocrafts	RC2200
	RC2304
	RC2302
Radios, Inc.	MXR-EM20
Telegesis Ltd	ETRX2
	ETRX2-PA
	ETRX351
	ETRX357
Sena Technologies	ProBee-ZE20S DIP/SMD

10. EQUIPMENT VENDORS

There are a lot of ZigBee equipment vendors. Here the equipment vendors are the organizations that would provide support and assistance for the ZigBee equipment's in the market. Most of them are working in the 2.4 GHz band. Lists of the equipment vendors and some of the features are given Table 5.

11. APPLICATION OF ZIGBEE

11.1 Health, Wellness and Fitness applications using ZigBee Wireless Sensor.

The ZigBee technology can be used in the field of healthcare monitoring such as chronic, personal wellness and personal fitness monitoring. Episodic and continuous patient monitoring (e.g.: measuring the blood glucose level and measuring the heart beat), patient alarm monitoring (e.g. the abrupt decrease or increase in heart rate, temperature etc. will be indicated as an alarm and responses/actions could be triggered automatically) are the major things carried out in chronic disease monitoring. In each scenario, the system will try to send commands, requested data as well as collected data .The processing of the commands and requests is done over the ZigBee network.

11.2 ZigBee for Intelligent Transportation System applications

ZigBee technology can be used for in-vehicle and vehicle to infrastructure communication. For example, using ZigBee radio communication, vehicles can detect, identify, and localize the road sign ahead with sufficient time and even in poor visibility. In the field of intelligent transportation system, the goal is to provide drivers with smart system which would alert the drivers about the oncoming curves and traffic signals ahead. Thus road accidents can be prevented. This system can be introduced with the advantage of low cost.

11.3 ZigBee for Home Area Network (HAN)

ZigBee can be used for Advanced Metering Infrastructure (AMI), commonly known as the smart meter. ZigBee is an ultra-low power wireless networking technology which makes it ideal to be used in a home area network. It is also being used for climate controls to lighting ballasts, smoke and security alarms with low cost. Many homes have issues with fluctuating load. ZigBee can be used to monitor the load. This helps ZigBee to emerge as the preferred standard for HAN.

11.4 ZigBee wireless sensor network for military

The system consists of a large number of sensors, ZigBee node, Host computer and a processor. Sensor will collect the information from the surrounding and it will be given to the ZigBee node [14]. The ZigBee node will send this information to the coordinator. This will be forwarded further to the processor. Processor will take all the necessary action to process the information and that information is provided back whenever the host computer queries the ZigBee wireless network.

11.5 Parameter monitoring and control for DC motors using ZigBee.

Starting and stopping of a DC motor can be performed by means of ZigBee using a computer interface [13]. During the faulty conditions like over current, higher /lower voltage, overheating, overloading, etc., it is possible to protect the motor. Also it is possible to take the online measurements of the motor parameters and store them with the help of a data base. So in this way, it is easy to control, monitor and protect the system.

11.6 ZigBee for landslide monitoring

ZigBee is the main transceiver used to communicate in order to send alerts and data for landslide monitoring. The sensors deployed are connected to these transceivers and the data is sent to a

common cluster head from where the data is sent to the base station or the collection point where all the analysis will be done [18].

Table 5: Equipment vendors and features

Vendor	Part Number	RAM	Processor
Texas Instruments	CC2531	8 kB	8051
Silicon Labs	EM358x	32-64 kB	6/12/24 MHz CM3
Marvell	88MZ100	160 kB	32/64 MHz CM3
Freescale	MC1323x	8 kB	32 MHz HCS08QE
NXP	JN-516x	8-32 kB	32 MHz
Atmel	ATZB-24-B0	8 kB	4 MHz ATmega1281V
Telink	TLSR8636	16 kB	48 MHz 32bit MCU

12. FUTURE WORK

In the near future, ZigBee will play a major role in communication technology. The stack size of ZigBee is as low as 4KB for limited capability end devices. And when considering other wireless technologies, ZigBee's stack size is much less. ZigBee is designed for efficient remote control of sensors which may be many in number but have less data packets to send, thus reducing the power consumption and increasing the lifetime. In the present world unwired applications are more preferred, though it must also meet the minimum power consumption and long battery life requirements. ZigBee has become the preferred technology for consumer, commercial and government markets worldwide.

13. CONCLUSION

In this paper we have discussed the protocol that the ZigBee transceiver uses i.e. 802.15.4. We have also discussed about the network topologies and security protocols being employed in ZigBee. ZigBee is one of the most widely used technologies for various applications in the present world since it's cheap and easy to use. One of the reasons why ZigBee is not used in Mobiles is because of the hardware (since both Bluetooth and ZigBee are designed for very different purposes) and its low data rate capacity. But it is to be noted that ZigBee has a wider range when compared to other technologies such as Bluetooth and NFC (Near Field Communication).

REFERENCES

[1] Trodhanl, "Introduction to Zigbee," Atmel Coorporration ,2006.
[2] Aamir Shaikh and Siraj Pathan, "Research on wireless sensor network Technology" , International Journal of Information and Education Technology, Vol. 2, No. 5, October 2012.

[3] Anneleen Van Nieuwenhuyse, Mario Alves and Anis koubaa, "Technical report on the use of the Zigbeeprotocol for wireless sensor networks," Technical Report HURRAY-TR-060601, 2006.

[4] Silabs,wireless ZigBee,http://www.silabs.com/products/wireless/zigbee/Pages/zigbee.aspx

[5] ZigBee Alliance, ZigBee remote control http://zigbee.org/zigbee-for-developers/applicationstandards/zigbeeremotecontrol/

[6] ZigBee Alliance, smart energy http://zigbee.org/zigbee-for-developers/applicationstandards/zigbeesmartenergy/

[7] ZigBee Alliance, smart energy profile 2 http://zigbee.org/zigbee-for-developers/applicationstandards/zigbeesmartenergyprofile2/

[8] ZigBee Alliance, ZigBee Telecom service http://zigbee.org/zigbee-for-developers/applicationstandards/zigbee-telecom-services/

[9] ZigBee Alliance, ZigBee Network devices http://zigbee.org/zigbee-for-developers/applicationstandards/zigbee-telecom-services/

[10] ZigBee Alliance, ZigBee Ip Specification Zigbee.org/specification/ZigBeeIP/overview.as

[11] ZigBee Alliance, ZigBee RF4CE ,Zigbee.org

[12] ZigBee Alliance, Specification http://old.zigbee.org/Specifications.aspx

[13] Mohini Reddy,Vidya sawant, WSN based parameter monitoring and control system for DC motor,international journal of innovative technology and exploring engineering,Feb 2014.

[14] Prof. Pravin R.Lakhe,Wireless sensor network using ZigBee, International Journal of Engineering Research and Applications.

[15] http://www.embedded.com/design/connectivity/4419558/Zigbee-s-new-IP-specification-for-IPv6-6LoPAN-wireless-network-designs.

[16] https://docs.zigbee.org/zigbee-docs/dcn/12/docs-12-0629-01-0mwg-zigbee-rf4ce-a-quiet-revolution-is- underway-webinar-slides.pdf

[17] http://www.embedded.com/design/connectivity/4419558/Zigbee-s-new-IP-specification-for-IPv6-6LoPAN-wireless-network-designs

[18] Y.Srinivas and K.Ragahava Rao , Landslide Warning System Using ZigbeeAnd GPS, IOSR Journal of Engineering (IOSRJEN)

AUTHORS

Jobina Mary Varghese received BTech degree in Electronics and Communication from Marian Engineering College, Kerala, India in July 20 13.She is currently pursuing MTech in Wireless Networks and Applications from Amrita University, Kollam, Kerala

Nibi K V received BTech degree in Electronics and Communication from Matha College of Technology, Kerala, India in July 2012. She is currently pursuing MTech in Wireless Networks and Applications from Amrita University, Kerala, India.

Vijo T Varghese received B.Tech degree in Electronics and Communication from KNS Institute of Technology, Bangalore, India in July 2012. He is currently pursuing his M.Tech in Wireless Networks and Applications from Amrita University, Kerala, India.

Prof. Sethuraman Rao is an associate professor at Amrita Center for Wireless Networks and Applications, Amrita University, Kollam, Kerala, India. He holds a Masters degree in Computer Science and a Bachelor's degree in Mechanical Engineering from IIT Madras, India. He has over 20 years of international experience in the networking industry having held technical and management positions at Juniper Networks, Alcatel-Lucent and a few start-ups. His areas of interest include wired and wireless LANs, wireless security, software engineering and network management.