ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 2, February 2013

LOW POWER ZIGBEE TECHNOLOGY IN WIRELESS MESH NETWORKS

P.Susmitha[1], V.Bhavya Reddy[2], Maninder Kaur[3]

[1]B.Tech III rd year Student, Dept. of E.C.E, Keshav Memorial Institute of Technology, Hyderabad, India.

[2]B.Tech III rd year Student, Dept. of E.C.E, Keshav Memorial Institute of Technology, Hyderabad, India.

[3]Asst.Professor, Dept. of ECE, Keshav Memorial Institute of Technology, Hyderabad, India

Abstract: Zigbee Technology specification for a suite of high level communication protocols using small, low-power digital radios. The technology is intended to be simpler and cheaper than Blue tooth. ZigBee is the newest specifications which have low data rates, consume very and low power. With ZigBee technology, interoperability will be enabled in multi-purpose, self-organizing mesh networks. ZigBee is standard for embedded application software. The bandwidth of Blue tooth is 1 Mbps and ZigBee has one-fourth of this value. ZigBee has low costs and long battery life. ZigBee is meant to cater to the sensors and remote controls market and other battery operated products.

I. INTRODUCTION

The past several years have witnessed a rapid growth of wireless networking. However, up to now wireless networking has been mainly focused on high-speed communications, and relatively long range applications such as the IEEE 802.11 Wireless Local Area Network (WLAN) standards. The _rst well known standard focusing on Low-Rate Wireless Personal Area Networks (LR-WPAN) was Bluetooth. However it has limited capacity for networking of many nodes. There are many wireless monitoring and control applications in industrial and home environments which require longer battery life, lower data rates and less complexity than those from existing standards. For such wireless applications, a new standard called IEEE 802.15.4 has been developed by IEEE. The new standard is also called ZigBee, The name ZigBee is said to come from the domestic honeybee which uses a zig-zag type of dance to communicate important information to other hive members.

ZigBee has a defined rate of 250 Kbit/s best suited for periodic or irregular data or a single signal transmission from a sensor or input device .Due to its low cost they are used wireless control and monitoring applications. Due to its low power output, ZigBee devices can sustain themselves on a small battery for many months, or even years, making them ideal for install-and-forget purposes, such as most small household systems.

1.Till now,there hasn't been a wireless network standard that meets the unique needs of sensors and control devices sensors do not need high bandwidth but they do need low energy consumption for long battery life

2. There are also many wireless systems that do not require high data rates but do require low cost and very low current drain.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 2, February 2013

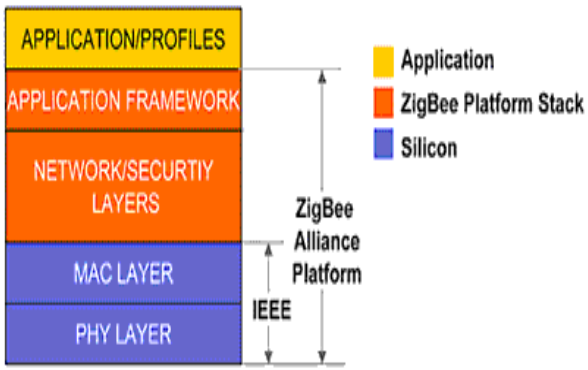

Figure 1. ZigBee protocol stack

3.These systems are creating significant interoperability problems with each other and with newer technologies

II. ZIGBEE DIVICE TYEPS

A) Zigbee devices are of three types:

1) ZigBee coordinator (ZC): The most capable device, the coordinator forms the root of the network tree and might bridge to other networks. There is exactly one ZigBee coordinator in each network since it is the device that started the network originally. It stores information about the network, including acting as the Trust Center & repository for security keys.

2) *ZigBee Router (ZR)*: used to route the messages between the co-ordinator and the end device.It also boots the signal cuming from the end device.

3) *ZigBee End Device (ZED)*: Contains just enough functionality to talk to the parent node (either the coordinator or a router); it cannot relay data from other devices. This relationship allows the node to be asleep a significant amount of the time thereby giving long battery life. A ZED requires the least amount of memory, and therefore can be less expensive to manufacture than ZR or ZC.

Protocol Description
The ZigBee Alliance has developed a very low-cost, very low-power consumption, two-way, wireless communications standard. Solutions adopting the ZigBee standard will be embedded in consumer electronics, home and building automation, industrial controls, PC peripherals, medical sensor applications, toys, and games.
Scope
This document contains specifications, interface descriptions, object descriptions, protocols and algorithms pertaining to the ZigBee protocol standard, including the application support sub-layer (APS), the ZigBee device objects (ZDO), ZigBee device profile (ZDP), the application framework, the network layer (NWK), and ZigBee security services.
Purpose
The purpose of this document is to provide a definitive description of the ZigBee
protocol standard as a basis for future implementations, such that any number of companies incorporating the ZigBee standard into platforms and devices on the basis of this document will produce interoperable, low-cost, and highly usable products for the burgeoning wireless marketplace.
Stack Architecture

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 2, February 2013

The ZigBee stack architecture is made up of a set of blocks called layers. Each layer performs a specific set of services for the layer above. A data entity provides a data transmission service and a management entity provides all other services Each service entity exposes an interface to the upper layer through a service access point (SAP), and each SAP supports a number of service primitives to achieve the required functionality. The IEEE 802.15.4-2003 standard defines the two lower layers: the physical (PHY) layer and the medium access control (MAC) sub-layer. The ZigBee Alliance builds on this foundation by providing the network (NWK) layer and the framework for the application layer. The application layer framework consists of the application support sub-layer (APS) and the ZigBee device objects (ZDO). Manufacturer-defined application objects use the framework and share APS and security services with the ZDO. IEEE 802.15.4-2003 has two PHY layers that operate in two separate frequency ranges: 868/915 MHz and 2.4 GHz. The lower frequency PHY layer covers both the 868 MHz European band and the 915 MHz band, used in countries such as the United States and Australia. The higher frequency PHY layer is used virtually worldwide. A complete description of the IEEE 802.15.4-2003 PHY layers can be found in [B1]. The IEEE 802.15.4-2003 MAC sub-layer controls access to the radio channel using a CSMA-CA mechanism. Its responsibilities may also include transmitting beacon frames, synchronization, and providing a reliable transmission mechanism. A complete description

ZIGBEE general characteristics:

1. Yields high throughput and low latency for low duty cycle devices like sensors and controls.
2 .Low power (battery life multi month to years)
3 .Multiple topologies: star, peer to peer, mesh
4. Addressing space of up to: 18,450,000,000,000,000,000 devices (64 bit IEEE address) and 65,535 networks.
5. Optional guaranteed time slot for applications requiring low latency
6. Fully hand-shake protocol for transfer reliability
7. Range:50m typical(5-500m based on environment)

Advantages of Zigbee:

1. Low power consumption
2. Low cost
3. High density of nodes per network
4.Simple protocol, global implementation
5. Ease of installation
6. Reliable data transfer
7. Short range operation

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 2, February 2013

Table1. Comparative analysis of different technologies providing similar services and their trade offs

Category	ZigBee	Bluetooth	Wi-Fi
Distance	50-1600m	10m	50m
Extension	Automatic	None	Depend on the existing network
Power supply	Years	Days	Hours
Complicity	Simple	Complicated	Very complicated
Transmission speed	250Kbps	1Mbps	1-54Mbps
Frequency range	868MHz, 916Mhz, 2.4GHz	2.4GHz	2.4GHz
Network nodes	65535	8	50
Linking time	30ms	Up to 10s	Up to 3s
Cost of terminal unit	Low	Low	High
Cost of use	None	None	None
Security	128bit AES	64bit, 128bit	SSID
Integration level& reliability	High	High	Normal
Prime cost	Low	Low	Normal
Ease of use	Easy	Normal	Hard

III. FORMING A ZIGBEE NETWORK & ARCHITECTURE

The Co-coordinator is responsible for starting a ZigBee network. Network initialization involves the following steps:

1. Search for a Radio Channel. The Co-coordinator first searches for a suitable radio channel (usually the one which has least activity). This search can be limited to those channels that are known to be usable - for example, by avoiding frequencies in which it is known that a wireless LAN is operating.
2. Assign PAN ID the Co-coordinator starts the network, assigning a PAN ID (Personal Area Network identifier) to the network. The PAN ID can be pre-determined, or can be obtained dynamically by detecting other networks operating in the same frequency channel and choosing a PAN ID that does not conflict with theirs. At this stage, the Co-coordinator also assigns a network (short) address to itself. Usually, this is the address 0x0000.
3. Start the Network - The coordinator then finishes configuring itself and starts itself in Co-ordinator mode. It is then ready to respond to queries from other devices that wish to join the network.

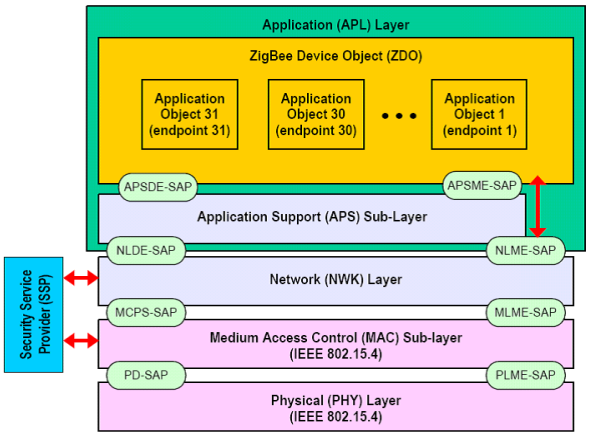

Figure2.Layered Architecture of Zigbee

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 2, February 2013

Joining a ZigBee Network: Once the network has been created by the coordinator, other devices (Routers and End Devices) can join the network. Both Routers and the coordinator have the capability to allow other nodes to join the network. The join process is as follows:

1. Search for Network - The new node first scans the available channels to find operating networks and identifies which one it should join. Multiple networks may operate in the same channel and are differentiated by their PAN IDs.
2. Select Parent- The node may be able to 'see' multiple Routers and a Coordinator from the same network, in which case it selects which one it should connect to. Usually, this is the one with the best signal.
3. Send Join Request- The node then sends a message to the relevant Router or coordinator asking to join the network.
4. Accept or Reject Join Request- The Router or coordinator decides whether the node is a permitted device, whether the Router/coordinator is currently allowing devices to join and whether it has address space available. If all these criteria are satisfied, the Router/coordinator will then allow the device to join and allocate it an address. Typically, a Router or coordinator can be configured to have a time-period during which joins are allowed. The join period may be initiated by a user action, such as pressing a button. An infinite join period can be set, so that child nodes can join the parent node at any time.

Network Topology

The ZigBee network layer (NWK) supports star, tree, and mesh topologies. In a star topology, the network is controlled by one single device called the ZigBee coordinator. The ZigBee coordinator is responsible for initiating and maintaining the devices on the network. All other devices, known as end devices, directly communicate with the ZigBee coordinator. In mesh and tree topologies, the ZigBee coordinator is responsible for starting the network and for choosing certain key network parameters, but the network may be extended through the use of ZigBee routers. In tree networks, routers move data and control messages through the network using a hierarchical routing strategy. Tree networks may employ beacon-oriented communication as described in the IEEE 802.15.4-2003 specification. Mesh networks allow full peer-to-peer communication. ZigBee routers in mesh networks do not currently emit regular IEEE 802.15.4-2003 beacons. This specification describes only intra-PAN networks, that is, networks in which communications begin and terminate within the same network.

Message Propagation: The way that a message propagates through a ZigBee network depends on the network topology. However, in all topologies, the message usually needs to pass through one or more intermediate nodes before reaching its final destination. The message therefore contains two destination addresses:

1. Address of the final destination
2. Address of the node which is the next "hop"

The way these addresses are used in message propagation depends on the network topology, as follows:

- **Star Topology**: All messages are routed via the coordinator. Both addresses are needed and the "next hop" address is that of the coordinator.
- **Tree Topology**: A message is routed up the tree until it reaches a node that can route it back down the tree to the destination node. Both addresses are needed and the initial "next hop" address is that of the parent of the sending node. The parent node then resends the message to the next relevant node - if this is the target node itself, the "final destination" address is used. The last step is then repeated and message propagation continues in this way until the target node is reached.

- **Mesh Topology**: In this case, the propagation path depends on whether the target node is in range:
  - If the target node is in range, only the "final destination" address is used.
  - If the target node is not in range, the initial "next hop" address is that of the first node in the route to the final destination. The message propagation continues in this way until the target node is reached.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 2, February 2013

IV. ZIGBEE SECURITY SERVICES

As one of its defining features, ZigBee provides facilities for carrying out secure communications, protecting establishment and transport of cryptographic keys, cyphering frames and controlling devices. It builds on the basic security framework defined in IEEE 802.15.4. This part of the architecture relies on the correct management of symmetric keys and the correct implementation of methods and security policies.

Basic Security Model

The basic mechanism to ensure confidentiality is the adequate protection of all keying material. Trust must be assumed in the initial installation of the keys, as well as in the processing of security information. In order for an implementation to globally work, its general conformance to specified behaviors is assumed.

Keys are the cornerstone of the security architecture; as such their protection is of paramount importance, and keys are never supposed to be transported through an insecure channel. A momentary exception to this rule occurs during the initial phase of the addition to the network of a previously unconfigured device. The ZigBee network model must take particular care of security considerations, as ad hoc networks may be physically accessible to external devices and the particular working environment cannot be foretold; likewise, different applications running concurrently and using the same transceiver to communicate are supposed to be mutually trustworthy: for cost reasons the model does not assume a firewall exists between application-level entities.

Within the protocol stack, different network layers are not cryptographically separated, so access policies are needed and correct design assumed. The open trust model within a device allows for key sharing, which notably decreases potential cost. Nevertheless, the layer which creates a frame is responsible for its security. If malicious devices may exist, every network layer payload must be ciphered, so unauthorized traffic can be immediately cut off. The exception, again, is the transmission of the network key, which confers a unified security layer to the network, to a new connecting device.

Security architecture

ZigBee uses 128-bit keys to implement its security mechanisms. A key can be associated either to a network, being usable by both ZigBee layers and the MAC sub layer, or to a link, acquired through pre-installation, agreement or transport. Establishment of link keys is based on a master key which controls link key correspondence. Ultimately, at least the initial master key must be obtained through a secure medium (transport or pre-installation), as the security of the whole network depends on it. Link and master keys are only visible to the application layer. Different services use different one-way variations of the link key in order to avoid leaks and security risks.

Key distribution is one of the most important security functions of the network. A secure network will designate one special device which other devices trust for the distribution of security keys: the trust center. Ideally, devices will have the trust center address and initial master key preloaded; if a momentary vulnerability is allowed, it will be sent as described above. Typical applications without special security needs will use a network key provided by the trust center (through the initially insecure channel) to communicate.

Thus, the trust center maintains both the network key and provides point-to-point security. Devices will only accept communications originating from a key provided by the trust center, except for the initial master key. The security architecture is distributed among the network layers as follows:

- The MAC sub layer is capable of single-hop reliable communications. As a rule, the security level it is to use is specified by the upper layers.
- The network layer manages routing, processing received messages and being capable of broadcasting requests. Outgoing frames will use the adequate link key according to the routing, if it is available; otherwise, the network key will be used to protect the payload from external devices.
- The application layer offers key establishment and transport services to both ZDO and applications. It is also responsible for the propagation across the network of changes in devices within it, which may originate in the devices themselves (for instance, a simple status change) or in the trust manager (which may inform the network that a certain device is to be eliminated from it). It also routes requests

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 2, February 2013

from devices to the trust center and network key renewals from the trust center to all devices. Besides this, the ZDO maintains the security policies of the device.

The security levels infrastructure is based on CCM*, which adds encryption- and integrity-only features to CCM.

There are three types of security modes : unsecured mode, access control list and secured mode.

1 Unsecured mode- No security used.

2 Access control list- No encryption used, but the network rejects frames from unknown devices.

3 Secured mode- In the secured mode the devices can use the following security services.

- Access control list.
- Data encryption using the Advanced Encryption Standard (AES) 128 bit encryption algorithm.
- Frame integrity is a security service that uses a Message Integrity Code (MIC) to protect data from being modified by parties without the cryptographic key. It further provides assurance that data come from a party with the cryptographic key.

V. ZIGBEE APPLICATIONS

Since it is cost effective ,has got long battery life and wireless connectivity, the zigbee technology is programmed in a chip and is used in many devices to function automatically. Some of the applications are:

1. It can be used in the health care system to monitor the status of the patients.
2. It can be used in automotive applications
3. It can be used to increase the security of the homes using zigbee technology.
4. It can be used for controlling and monitoring a whole factory unit by just sitting at one place.

VI. FUTURE SCOPE OF ZIGBEE

The near future of Zigbee technology will prevail in almost every walk of life. Zigbee would provide revolutionizing statistics in the upcoming years which would entirely change the wireless world.

A. Revenue: Zigbee revenues would increase by astonishing 3400% in next four years.

B. Sales: It sales would touch a remarkable figure of 700m$ in 2008.

C. Zigbee in every home: Within next two to three years, a minimum of 100-150 Zigbee chips would be present in every home.

D. Cost: It would cost only $5 for a single chip .But the smaller memory size of protocol stack will further lower the prize of Zigbee to around $2 per chip.

VII. CONCLUSIONS

Zigbee is playing a vital role in the future of computer and communication technology.In terms of protocol stack size ,zigbee's stack size is about one fourth of the stack size of Bluetooth. The Zigbee Alliance targets applications across consumer, commercial, industrial and government markets worldwide. Zigbee technology is designed to best suite the applications that require long battery-life, low power consumption, short distance propagation. Its most important advantage of being available at a very less cost enables it to be deployed in wireless control and monitoring applications

REFERENCES

[1] Reinhold Ludvig and Pavel Bretchko, RF Circuit Design - Theory and Applications, Prenctice Hall 2000.

[2] IEEE Standards 802.15.4, IEEE 2003

[3] Chipcon AS, Chipcon AS SmartRF CC2420 Preliminary Data sheet (rev 1.2)

[4] Atmel Corporation, ATmega128L Data sheet Rev. 2467M-AVR-11/04

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 2, February 2013

[5] Freescale Semiconductor, http://www.freescale.com, 2005-03

[6] Maxim-Ic, http://www.maxim-ic.com, 2005-03

[7] Atmel Corporation, http://www.atmel.com, 2005-03

[8] Chipcon, http://www.chipcon.com, 2005-03

[9] GigaAnt, http://www.gigaant.com, 2005-03

[10] Figure 8 Wireless, http://www._gure8wireless.com, 2005-03

[11] AVR Freaks, http://www.avrfreaks.com, 2005-03

[12] Texas Instruments, http://www.ti.com, 2005-03

BIOGRAPHY

Sushmita and Bhavya Reddy are under graduate students of ECE and their aggregate is 80% .There research area is Wireless Sensor Networks , Artificial Intelligence, Mobile Communications

Maninder Kaur is working in ECE Department from the past 6 years. My research area is Wireless Communication and Networks, Artificial Intelligence