Wireless Networking Through ZigBee Technology

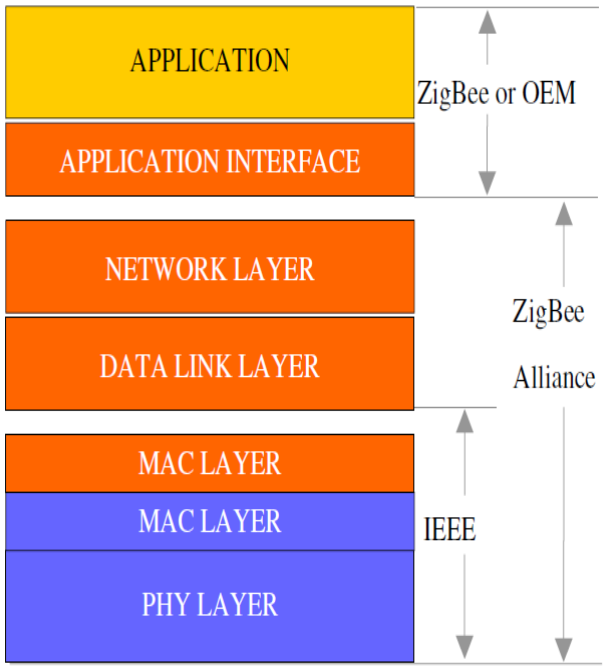
Chhavi Mittal[1]
[1]Department of Electronics & Communication Engineering,
Ganga Institute Of Technology & Management,
Kablana, Jhajjar, Haryana, India

***Abstract*- ZigBee is an IEEE 802.15.4 standard for data communications dealing business and consumer devices. It is designed for low-power consumption enabling batteries to last forever. The ZigBee standard provides network, security, and application support services operating on top of the IEEE 802.15.4 Medium Access Control (MAC) and Physical Layer wireless standard. It employs a group of technologies to enable scalable, self-organizing, self-healing networks that can manage various data traffic patterns. ZigBee is a low-cost, low-power, wireless mesh networking standard. The low cost allows the technologyto be widely deployed in wireless control and monitoring applications, the low power-usage allows longerlife with smaller batteries, and the mesh networking which promises high reliability and larger range. ZigBee has-been developed to meet the growing demand for capable wireless networking between numerous low power devices. In industry ZigBee is being used for next generation automated manufacturing, with small transmitters in every device on the floor, allowing for communication between devices to a central computer. This new level of communication permits finely-tuned remote monitoring and manipulation. This paper focuses on ZigBee as a technology innovation which would bring about low cost connectivity, its architecture and applications.**

Keywords*— *Network Key, protocols, meshes, suite, bandwidth.

I. INTRODUCTION

ZigBee is a specification for a suite of high level communication protocols using tiny, low-power digital radios based on an IEEE 802 standard for personal area networks. 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. ZigBee based traffic management system have also been implemented[1] . The name refers to the waggle dance of honey bees after their return to the beehive. ZigBee is a low-cost, low-power, wireless mesh network standard. The low cost allows the technology to be widely deployed in wireless control and monitoring applications. Low power-usage allows longer life with smaller batteries. Mesh networking provides high reliability and more extensive range. ZigBee chip vendors typically sell integrated radios and microcontrollers with between 60 KB and 256 KB flash memory. The ZigBee network layer natively supports both star and tree typical networks, and generic mesh networks. As shown in figure 1. Every network must have one coordinator device, tasked with its creation, the control of its parameters and basic maintenance. In star networks, the coordinator must be the central node. Both trees and meshes allow the use of ZigBee routers to extend communication at the network level.



A. *Need for ZIGBEE :* 1) There are a multitude of standards that address mid to high data rates for voice, PC LANs, video, etc. However, up till now there hasn't been a wireless network standard that meets the unique needs of sensors and control devices. Sensors and controls don't need high bandwidth but they do need low latency and very low energy consumption for long battery lives and for large device arrays [2].

2) There are a multitude of proprietary wireless systems manufactured today to solve a multitude of problems that also don't require high data rates but do require low cost and very low current drain.

Figure 1. ZigBee protocol stack

3) These proprietary systems were designed because there were no standards that met their requirements. These legacy 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)*: As well as running an application function, a router can act as an intermediate router, passing on data from other devices.

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.

B) Protocols : The protocols build on recent algorithm (Ad-hoc On-demand and Distance vector, nueRFon) to automatically construct a low-speed ad-hoc network of nodes[3]. In most large network instances, the network will be a cluster of clusters. It can also form a mesh or a single cluster. The current ZigBee protocols support beacon and non-beacon enabled networks.In non-beacon-enabled networks, an unslotted CSMA/CA channel access mechanism is used. In this type of network, ZigBee Routers typically have their receivers continuously active, requiring a more robust power supply. However, this allows for heterogeneous networks in which some devices receive continuously, while others only transmit when an external stimulus is detected. The typical example of a heterogeneous network is a WIRELESS SWITCH: The ZigBee node at the lamp may receive constantly, since it is connected to the mains supply, while a battery-powered light switch would remain asleep until the switch is thrown. The switch then wakes up, sends a command to the lamp, receives an acknowledgment, and returns to sleep. In such a network the lamp node will be at least a ZigBee Router, if not the ZigBee Coordinator; the switch node is typically a ZigBee End Device. In beacon-enabled networks, the special network nodes called ZigBee Routers transmit periodic beacons to confirm their presence to other network nodes. Nodes may sleep between beacons, thus lowering their duty cycle and extending their battery life. Beacon intervals depend on data rate; they may range from 15.36 milliseconds to 251.65824 seconds at 250 Kbit/s, from 24 milliseconds to 393.216 seconds at 40 Kbit/s and from 48 milliseconds to 786.432 seconds at 20 Kbit/s[5].

However, low duty cycle operation with long beacon intervals requires precise timing, which can conflict with the need for low product cost. In general, the ZigBee protocols minimize the time the radio is on, so as to reduce power use. In beaconing networks, nodes only need to be active while a beacon is being transmitted. In non-beacon-enabled networks, power consumption is decidedly asymmetrical: some devices are always active, while others spend most of their time sleeping. Except for the Smart Energy Profile 2.0, ZigBee devices are required to conform to the IEEE 802.15.4-2003 Low-Rate Wireless Personal Area Network (LR-WPAN) standard. The standard specifies the lower protocol layers—the (physical layer) (PHY), and the (media access control) portion of the (data link later (DLL)). The basic channel access mode is "carrier sense, multiple access/collision avoidance" (CSMA/CA). That is, the nodes talk in the same way that people converse; they briefly check to see that no one is talking before they start, with three notable exceptions. Beacons are sent on a fixed timing schedule, and do not use CSMA. Message acknowledgments also do not use CSMA. Finally, devices in Beacon Oriented networks that have low latency real-time requirements may also use Guaranteed Time Slots (GTS), which by definition do not use CSMA.

B) ZigBee/IEEE 802.15.4 - General Characteristics

1) Dual PHY (2.4GHz and 868/915 MHz) , Data rates of 250 kbps (@2.4 GHz), 40 kbps (@ 915 MHz), and 20 kbps (@868 MHz) , Optimized for low duty-cycle applications (<0.1%) ,CSMA-CA channel access.

2) Yields high throughput and low latency for low duty cycle devices like sensors and controls

3) Low power (battery life multi-month to years)

4) Multiple topologies: star, peer-to-peer, mesh

5)Addressing space of up to:18,450,000,000,000,000,000 devices (64 bit IEEE address) and 65,535 networks

6)Optional guaranteed time slot for applications requiring low latency

7)Fully hand-shaked protocol for transfer reliability

8) Range: 50m typical (5-500m based on environment)

C) Advantages of ZigBee

is poised to become the global control/sensor network standard. It has been designed to provide the following features:

1) Low power consumption, simply implemented.

2)Users expect batteries to last many months to years! Consider that a typical single family house has about 6 smoke/CO detectors. If the batteries for each one only lasted six months, the home owner would be replacing batteries every month.

3)Bluetooth has many different modes and states depending upon your latency and power requirements such as sniff, park, hold, active, etc.; ZigBee/IEEE 802.15.4 has active (transmit/receive) or sleep. Application software needs to focus on the application, not on which power mode is optimum for each aspect of operation. 4)Even mains powered equipment needs to be conscious of energy. Consider a future home with 100 wireless control/sensor devices, *Case 1:* 802.11 Rx power is 667 mW (always on)@ 100 devices/home & 50,000 homes/city = 3.33

megawatts *Case 2:* 802.15.4 Rx power is 30 mW (always on)@ 100 devices/home & 50,000 homes/city = 150 kilowatts *Case 3:* 802.15.4 power cycled at .1% (typical duty cycle) = 150 watts.

ZigBee devices will be more ecological than its predecessors saving megawatts at it full deployment.

5)Low cost (device, installation, maintenance)

Low cost to the users means low device cost, low installation cost and low maintenance. ZigBee devices allow batteries to last up to years using primary cells (low cost) without any chargers (low cost and easy installation). ZigBee's simplicity allows for inherent configuration and redundancy of network devices provides low maintenance [4].

6) High density of nodes per network

ZigBee's use of the IEEE 802.15.4 PHY and MAC allows networks to handle any number of devices. This attribute is critical for massive sensor arrays and control networks.

7)Simple protocol, global implementation

ZigBee's protocol code stack is estimated to be about 1/4th of Bluetooth's or 802.11's as shown in figure 1 and table 1. Simplicity is essential to cost, interoperability, and maintenance. The IEEE 802.15.4 PHY adopted by ZigBee has been designed for the 868 MHz band in Europe, the 915 MHz band in N America, Australia, etc; and the 2.4 GHz band is now recognized to be a global band accepted in almost all countries. Table 1. Comparative analysis of differnet technologies providing similar services and their tarde 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

Fig 2

III. FORMING A ZIGBEE NETWORK AND ARCHITECTURE

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

1. Search for a Radio Channel-The Co-ordinator 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[6], [7].

2. Assign PAN ID- The Co-ordinator 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-ordinator also assigns a network (short) address to itself. Usually, this is the address 0x0000.

3. Start the Network- The Co-ordinator 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.

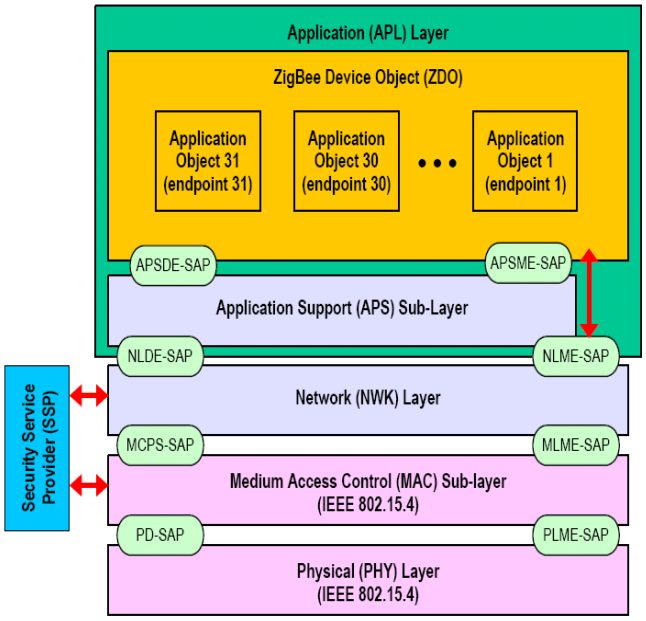


Figure 3. Layered Architecture of ZigBee

IV. FORMING A ZIGBEE 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[8]. 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: 1) 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.

2)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. 3)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 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 [9],[12] . The security levels infrastructure is based on CCM*, which adds encryption- and integrity-only features to CCM.

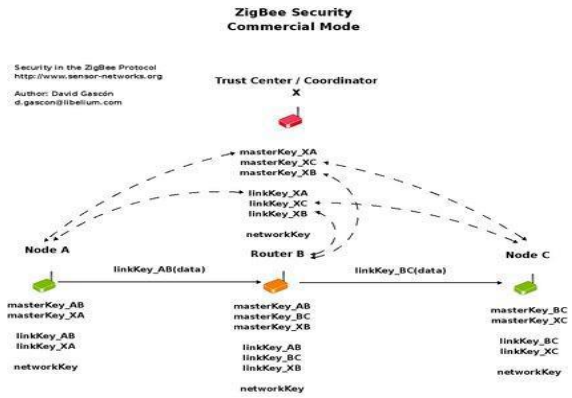


Figure 4. Security Scenario in ZigBee

ZigBee implements two extra security layers on top of the 802.15.4 one: the Network and Application security layers. All the security policies rely on the AES 128b encryption algorithm so the hardware architecture previously deployed for the link level (MAC layer) is still valid. There are three kinds of Keys: master, link and network keys. 1) Master Keys: They are pre-installed in each node. Their function is to keep confidential the Link Keys exchange between two nodes in the Key Establishment Procedure (SKKE). 2) Link Keys: They are unique between each pair of nodes. These keys are managed by the Application level. They are used to encrypt all the information between each two devices, for this reason more memory resources are needed in each device.

3) Network key: It is a unique 128b key shared among all the devices in the network. It is generated by the Trust Center and regenerated at different intervals. Each node has to get the Network Key in order to join the network. Once the trust center decides to change the Network Key, the new one is spread through the network using the old Network Key[11]. Once this new key is updated in a device, its Frame Counter (see in the previous sections) is initialized to zero. This Trust Center is normally the Coordinador, however, it can be a dedicated device. It has to authenticate and validate each device which attempts to join the network. We have been able to analyze both IEEE 802.15.4 and ZigBee security protocol stacks on the sensor platform Waspmote due to the fact they support two different "pin to pin" compatible transceivers as shown in figure 2. The XBee OEM 802.15.4 implements the IEEE protocol over the Free scale chipset platform. On the other hand the ZigBee stack has been studied using the XBee ZB transceiver which uses de Ember chipset solution. When security of MAC layer frames is desired, ZigBee uses MAC layer security to secure MAC command, beacon, and acknowledgement frames. ZigBee may secure messages transmitted over a single hop using secured MAC data frames, but for multi-hop messaging ZigBee relies upon upper layers (such as the NWK layer) for security. The MAC layer uses the Advanced Encryption Standard (AES) [10] as its core cryptographic algorithm and describes a variety of security suites that use the AES algorithm. These suites can protect the confidentiality, integrity, and authenticity of MAC frames. The MAC layer does the security processing, but the upper layers, which set up the keys and determine the security levels to use, control this processing. When the MAC layer transmits (receives) a frame with security enabled, it looks at the destination (source) of the frame, retrieves the key associated with that destination (source), and then uses this key to process the frame according to the security suite designated for the key being used. Each key is associated with a single security suite and the MAC frame header has a bit that specifies whether security for a frame is enabled or disabled. Each pair of devices can have set both Network and Link Keys. In this case the Link key is always used (more security although more memory is needed). There are two kinds of security policies which the Trust Center can follow: -

Commercial mode: the Trust Center share Master and Link Keys with any of the devices in the network . This mode requires high memory resources. This mode offers a complete centralized model for the Key Security control. –

Residential mode: the Trust Center shares just the Network Key (it is the ideal mode when embedded devices have to cope with this task due to the low resources they have). This is the mode normally chosen for the Wireless Sensor Network model[13].

V. APPLICATIONS OF ZIGBEE TECHNOLOGY

It is not limited to a certain level but because of being cost-effective, low-power battery and wireless connectivity, this Zigbee technology is used in almost every appliance if not in all. Zigbee technology is programmed in a chip form and is used in many devices to function automatically[12]. For controlling and monitoring a whole factory unit while sitting in one cabin is possible by using Zigbee technology It centralizes all the units in one place and enables the

remote monitoring. In a similar way, a home can be centralized by increasing the security aspect. Many small equipments are coming with embedded Zigbee technology chips and really works like a miracle. Zigbee technology is swiftly prevail the market by introducing devices like smoke and heat sensor, medical and scientific equipments, control units of home and industry and wireless communication devices. The revolutionize turn in the field of technology with the introduction of zigbee technology; the near future of Zigbee technology will prevail in almost every walk of life.

VI. FUTURE SCOPE OF ZIGBEE

Zigbee has a very promising future in front of it. Research claims that fuelled by rapid rise in home networking, 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. CONLUSION

It is likely that ZigBee will increasingly play an vital role in the future of computer and communication technology. In terms of protocol stack size, ZigBee's 32 KB is about one third of the stack size necessary in other wireless technologies. The IEEE 802.15.4–based ZigBee is designed for remote controls and sensors, which are very many in number, but need only small data packets and, extremely low power consumption for longer life. Therefore they are naturally different in their approach to their respective application arenas. The ZigBee Alliance targets applications across consumer, commercial, industrial and government markets worldwide. Unwired applications are extremely sought after in many networks that are characterized by copious nodes consuming minimum power and enjoying long battery lives. ZigBee technology is designed to best suit these applications, for the reason that it enables lesser costs of development and very swift market adoption.

REFERENCES

[1] ZigBee Alliance, ZigBee Specification. Version 1.0 ZigBee Document 053474r06, December 14th, 2004.
[2] William Stalling, ―Wireless Communication and Networks‖, Fourth Edition, Pearson Publication Limited, 2004, Pp 39-118.
[3] 802.15.4, Part 15.4: Wireless Medium *Access* Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LRWPANs).
[4] Sheng-Fu Su, The Design and Implementation of the ZigBee Protocol Driver in Linux, White Paper dated 26 July 2005.
[5] Jacob Munk-Stander,Implementing a ZigBee Protocol Stack and Light Sensor in TinyOS,White Paper dated October 2005.
[6] Freescale Semiconductor, ZigBee Implementer's Guide; Document Number: F8W-2004-0007, May 23, 2005
[7] Weiser, M. (1991). The Computer for the 21st Century. *Scientific America*, September 1991, 94-104. Journal of Theoretical and Applied Information Technology © 2005 - 2009 JATIT.
[8] Pister K. S. J., Kahn J. M., and Boser B. E. (1999). Smart dust: Wireless networks of millimeter-scale sensor nodes. In 1999 UCB Electronics Research Laboratory Research Summary
[9] IEEE 802 Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks, IEEE Computer Society, 2003.
[10] *ZigBee Specification v1.0*, ZigBee Alliance, December 14th, 2004. Tanenbaum, A. S., Gamage, C., & Crispo, B. (2006). Taking sensor networks from the lab to the jungle.Computer, 39(8), 98-100.
[11]Kohvakka, M., Kuorilehto, M., Hännikäinen, M., & Hännikäinen, T. D. (2006). Performance analysis of IEEE 802.15.4 and ZigBee for large-scale wireless sensor network applications.
[12]Gorbis, M., & Pescovitz, D. (2006). IEEE fellow's survey: Bursting tech bubbles before they balloon. *IEEE Spectrum*, 43(9), 50-55.
[13]Ran, P., Sun, M., Zou, Y. (2006). ZigBee routing selection strategy based on data services and energy-balanced ZigBee routing. *APSCC '06*, December 2006, 400