THE ROLE OF ZIGBEE TECHNOLOGY IN FUTURE DATA COMMUNICATION SYSTEM

Dr.S.S.Riaz Ahamed.

Professor & Head, Dept of Computer Applications, Mohamed Sathak Engg College,Kilakarai & Principal, Sathak Institute of Technology, Ramanathapuram,TamilNadu, India-623501.

E-mail: ssriaz@ieee.org , sssriaz@gmail.com

ABSTRACT

ZigBee is an IEEE 802.15.4 standard for data communications with business and consumer devices. It is designed around low-power consumption allowing batteries to essentially 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 (PHY) wireless standard. It employs a suite 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 technology to be widely deployed in wireless control and monitoring applications, the low power-usage allows longer life with smaller batteries, and the mesh networking provides 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.

Keywords: *Medium Access Control (MAC), Physical Layer (PHY), Wireless Personal Area Networking (WPAN), Open Systems Interconnection (OSI)*

1. INTRODUCTION

ZigBee is an established set of specifications for wireless personal area networking (WPAN), i.e. digital radio connections between computers and related devices. WPAN Low Rate or ZigBee provides specifications for devices that have low data rates, consume very low power and are thus characterized by long battery life. ZigBee makes possible completely networked homes where all devices are able to communicate and be controlled by a single unit. The ZigBee Alliance, the standards body which defines ZigBee, also publishes application profiles that allow multiple OEM vendors to create interoperable products. The current list of application profiles either published or in the works are:

- Home Automation
- ZigBee Smart Energy
- Telecommunication Applications
- Personal Home

The relationship between IEEE 802.15.4 and ZigBee is similar to that between IEEE 802.11 and the Wi-Fi Alliance. For non-commercial purposes, the ZigBee specification is available free to the general public. An entry level membership in the ZigBee Alliance, called Adopter, costs US$ 3500 annually and provides access to the as-yet unpublished specifications and permission to create products for market using the specifications. ZigBee is one of the global standards of communication protocol formulated by the relevant task force under the IEEE 802.15 working group. The fourth in the series, WPAN Low Rate/ZigBee is the newest and provides specifications for devices that have low data rates, consume very low power and are thus characterized by long battery life. Other standards like Bluetooth and IrDA address high data rate applications such as voice, video and LAN communications.

ZigBee devices are actively limited to a through-rate of 250Kbps, compared to Bluetooth's much larger pipeline of 1Mbps, operating on the 2.4 GHz

ISM band, which is available throughout most of the world.In the consumer market ZigBee is being explored for everything from linking low-power household devices such as smoke alarms to a central housing control unit, to centralized light controls.

The specified maximum range of operation for ZigBee devices is 250 feet (76m), substantially further than that used by Bluetooth capable devices, although security concerns raised over "sniping" Bluetooth devices remotely, may prove to hold true for ZigBee devices as well. 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. Predictions of ZigBee installation for the future, most based on the explosive use of ZigBee in automated household tasks in China, look to a near future when upwards of sixty ZigBee devices may be found in an average American home, all communicating with one another freely and regulating common tasks seamlessly.

The ZigBee Alliance has been set up as “an association of companies working together to enable reliable, cost-effective, low-power, wirelessly networked, monitoring and control products based on an open global standard”. Once a manufacturer enrolls in this Alliance for a fee, he can have access to the standard and implement it in his products in the form of ZigBee chipsets that would be built into the end devices. Philips, Motorola, Intel, HP are all members of the Alliance . The goal is “to provide the consumer with ultimate flexibility, mobility, and ease of use by building wireless intelligence and capabilities into every day devices. ZigBee technology will be embedded in a wide range of products and applications across consumer, commercial, industrial and government markets worldwide. For the first time, companies will have a standards-based wireless platform optimized for the unique needs of remote monitoring and control applications, including simplicity, reliability, low-cost and low-power”.

The target networks encompass a wide range of devices with low data rates in the Industrial, Scientific and Medical (ISM) radio bands, with building-automation controls like intruder/fire alarms, thermostats and remote (wireless) switches, video/audio remote controls likely to be the most popular applications. So far sensor and control devices have been marketed as proprietary items for want of a standard. With acceptance and implementation of ZigBee, interoperability will be enabled in multi-purpose, self-organizing mesh networks

2. ZIGBEE CHARACTERISTICS

The focus of network applications under the IEEE 802.15.4 / ZigBee standard include the features of low power consumption, needed for only two major modes (Tx/Rx or Sleep), high density of nodes per network, low costs and simple implementation.

These features are enabled by the following characteristics,

• *2.4GHz and 868/915 MHz dual PHY modes*. This represents three license-free bands: 2.4-2.4835 GHz, 868-870 MHz and 902-928 MHz. The number of channels allotted to each frequency band is fixed at sixteen (numbered 11-26), one (numbered 0) and ten (numbered 1-10) respectively. The higher frequency band is applicable worldwide, and the lower band in the areas of North America, Europe, Australia and New Zealand .

• Low power consumption, with battery life ranging from months to years. Considering the number of devices with remotes in use at present, it is easy to see that more numbers of batteries need to be provisioned every so often, entailing regular (as well as timely), recurring expenditure. In the ZigBee standard, longer battery life is achievable by either of two means: continuous network connection and slow but sure battery drain, or intermittent connection and even slower battery drain.

• Maximum data rates allowed for each of these frequency bands are fixed as 250 kbps @2.4 GHz, 40 kbps @ 915 MHz, and 20 kbps @868 MHz.

• High throughput and low latency for low duty-cycle applications (<0.1%)

• Channel access using Carrier Sense Multiple Access with Collision Avoidance (CSMA - CA)

• Addressing space of up to 64 bit IEEE address devices, 65,535 networks

• 50m typical range

• Fully reliable “hand-shaked” data transfer protocol.

• Different topologies as illustrated below: star, peer-to-peer, mesh

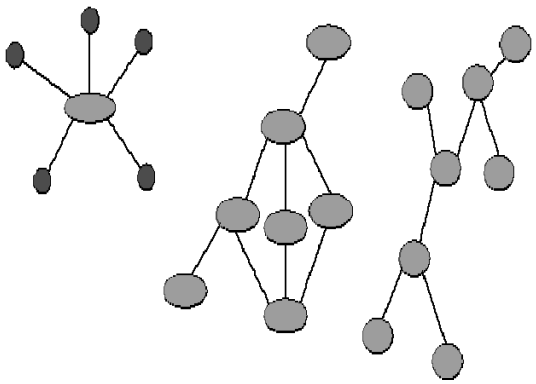

Figure 1: ZigBee Topologies

3. TRAFFIC TYPES

ZigBee/IEEE 802.15.4 addresses three typical traffic types. IEEE 802.15.4 MAC can accommodate all the types.

1. Data is *periodic*. The application dictates the rate, and the sensor activates, checks for data and deactivates.

2. Data is *intermittent*. The application, or other stimulus, determines the rate, as in the case of say smoke detectors. The device needs to connect to the network only when communication is necessitated. This type enables optimum saving on energy.

3. Data is *repetitive*, and the rate is fixed a priori. Depending on allotted time slots, called GTS (guaranteed time slot), devices operate for fixed durations.

ZigBee employs either of two modes, beacon or non-beacon to enable the to-and-fro data traffic. Beacon mode is used when the coordinator runs on batteries and thus offers maximum power savings, whereas the non-beacon mode finds favour when the coordinator is mains-powered.

In the beacon mode, a device watches out for the coordinator's beacon that gets transmitted at periodically, locks on and looks for messages addressed to it. If message transmission is complete, the coordinator dictates a schedule for the next beacon so that the device ‘goes to sleep'; in fact, the coordinator itself switches to sleep mode.

While using the beacon mode, all the devices in a mesh network know when to communicate with each other. In this mode, necessarily, the timing circuits have to be quite accurate, or wake up sooner to be sure not to miss the beacon. This in turn means an increase in power consumption by the coordinator's receiver, entailing an optimal increase in costs.

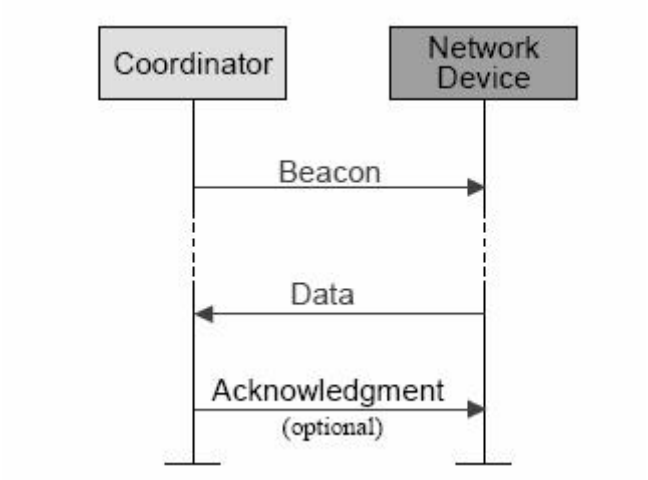

*Figure 2: Beacon Network Communication [*Source:www.zigbee.org/en/resources]

The non-beacon mode will be included in a system where devices are ‘asleep' nearly always, as in smoke detectors and burglar alarms. The devices wake up and confirm their continued presence in the network at random intervals.

On detection of activity, the sensors ‘spring to attention', as it were, and transmit to the ever-waiting coordinator's receiver (since it is mains-powered). However, there is the remotest of chances that a sensor finds the channel busy, in which case the receiver unfortunately would ‘miss a call'.

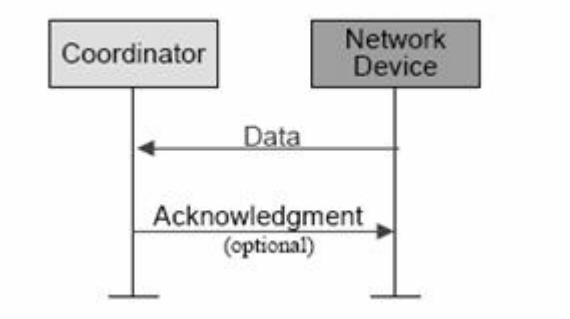

*Figure 3: Non-Beacon Network Communication [*Source:www.zigbee.org/en/resources]

4. ARCHITECTURE

ZigBee is a home-area network designed specifically to replace the proliferation of individual remote controls. ZigBee was created to satisfy the market's need for a cost-effective, standards-based wireless network that supports low data rates, low power consumption, security, and reliability. To address this need, the ZigBee Alliance, an industry working group (www.zigbee.org), is developing standardized application software on top of the IEEE 802.15.4 wireless standard. The alliance is working closely with the IEEE to ensure an integrated, complete, and interoperable network for the market. For example, the working group will provide interoperability certification testing of 802.15.4 systems that include the ZigBee software layer.

The ZigBee Alliance will also serve as the official test and certification group for ZigBee devices. ZigBee is the only standards-based technology that addresses the needs of most remote monitoring and control and sensory network applications.

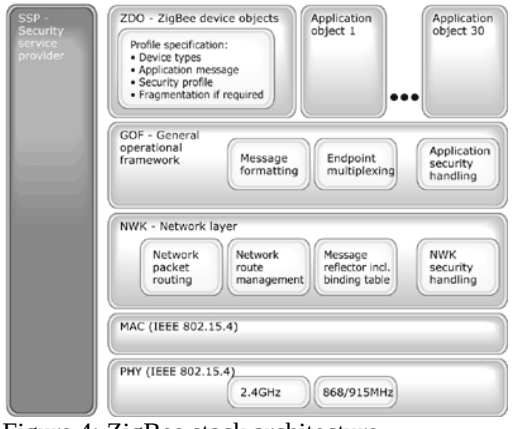

Figure 4: ZigBee stack architecture

It may be helpful to think of IEEE 802.15.4 as the physical radio and ZigBee as the logical network and application software. Following the standard Open Systems Interconnection (OSI) reference model, ZigBee's protocol stack is structured in layers. The first two layers, physical (PHY) and media access (MAC), are defined by the IEEE 802.15.4 standard. The layers above them are defined by the ZigBee Alliance. The IEEE working group passed the first draft of PHY and MAC in 2003.

ZigBee-compliant products operate in unlicensed bands worldwide, including 2.4GHz (global), 902 to 928MHz (Americas), and 868MHz (Europe). Raw data throughput rates of 250Kbps can be achieved at 2.4GHz (16 channels), 40Kbps at 915MHz (10 channels), and 20Kbps at 868MHz (1 channel). The transmission distance is expected to range from 10 to 75m, depending on power output and environmental characteristics. Like Wi-Fi, Zigbee uses direct-sequence spread spectrum in the 2.4GHz band, with offset-quadrature phase-shift keying modulation. Channel width is 2MHz with 5MHz channel spacing. The 868 and 900MHz bands also use direct-sequence spread spectrum but with binary-phase-shift keying modulation.

5. FRAME STRUCTURE

Figure 5 illustrates the four basic frame types defined in 802.15.4: data, ACK, MAC command, and beacon.

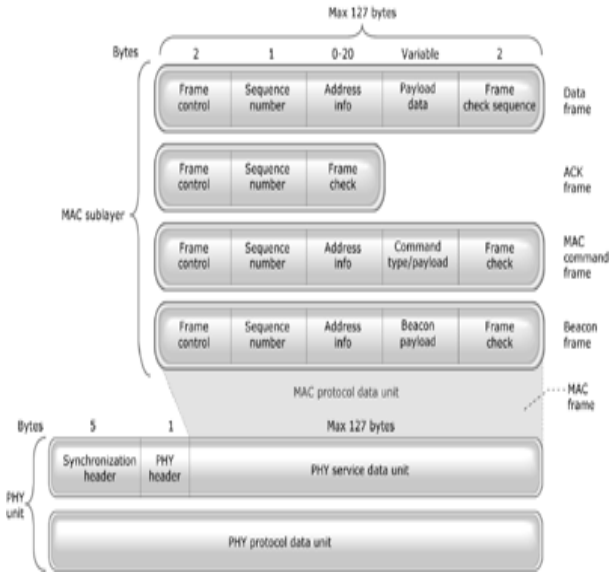

Figure5: The four basic frame types defined in 802.15.4: Data, ACK, MAC command, and beacon

The *data frame* provides a payload of up to 104 bytes. The frame is numbered to ensure that all packets are tracked. A frame-check sequence ensures that packets are received without error. This frame structure improves reliability in difficult conditions.

Another important structure for 802.15.4 is the *acknowledgment (ACK) frame*. It provides feedback from the receiver to the sender confirming that the packet was received without error. The device takes advantage of specified "quiet time" between frames to send a short packet immediately after the data-packet transmission.

A *MAC command frame* provides the mechanism for remote control and configuration of client nodes. A centralized network manager uses MAC to configure individual clients' command frames no matter how large the network.

Finally, the *beacon frame* wakes up client devices, which listen for their address and go back to sleep if they don't receive it. Beacons are important for mesh and cluster-tree networks to keep all the nodes synchronized without requiring those nodes to consume precious battery energy by listening for long periods of time.

6. CHANNEL ACCESS, ADDRESSING

Two channel-access mechanisms are implemented in 802.15.4. For a non"beacon network, a standard ALOHA CSMA-CA (carrier-sense medium-access with collision avoidance) communicates with positive acknowledgement for successfully received packets. In a beacon-enabled network, a superframe structure is used to control channel access. The superframe is set up by the network coordinator to transmit beacons at predetermined intervals (multiples of 15.38ms, up to 252s) and provides 16 equal-width time slots between beacons for contention-free channel access in each time slot. The structure guarantees dedicated bandwidth and low latency. Channel access in each time slot is contention-based. However, the network coordinator can dedicate up to seven guaranteed time slots per beacon interval for quality of service.

Device addresses employ 64-bit IEEE and optional 16-bit short addressing. The address field within the MAC can contain both source and destination address information (needed for peer-to-peer operation). This dual address information is used in mesh networks to prevent a single point of failure within the network.

7. DEVICE TYPES

These devices have 64-bit IEEE addresses, with option to enable shorter addresses to reduce packet size, and work in either of two addressing modes – star and peer-to-peer.

ZigBee networks use three device types:

- The *network coordinator* maintains overall network knowledge. It's the most sophisticated of the three types and requires the most memory and computing power.
- The *full function device (FFD)* supports all 802.15.4 functions and features specified by the standard. It can function as a network coordinator. Additional memory and computing power make it ideal for network router functions or it could be used in network-edge devices (where the network touches the real world).
- The *reduced function device (RFD)* carries limited (as specified by the standard) functionality to lower cost and complexity. It's generally found in network-edge devices.

8. SECURITY

Security and data integrity are key benefits of the ZigBee technology. ZigBee leverages the security model of the IEEE 802.15.4 MAC sublayer which specifies four security services:

- access control—the device maintains a list of trusted devices within the network
- data encryption, which uses symmetric key 128-bit advanced encryption standard
- frame integrity to protect data from being modified by parties without cryptographic keys
- sequential freshness to reject data frames that have been replayed—the network controller compares the freshness value with the last known value from the device

and rejects it if the freshness value has not been updated to a new value

The actual security implementation is specified by the implementer using a standardized toolbox of ZigBee security software.

The following table-1 shows the Wireless technology comparison chart,

Standard	Bandwidth	Power Consumption	Protocol Stack Size	Stronghold	Applications
Wi-Fi	Up to 54Mbps	400+mA TX, standby 20mA	100+KB	High data rate	Internet browsing, PC networking, file transfers
Bluetooth	1Mbps	40mA TX, standby 0.2mA	~100+KB	Interoperability, cable replacement	Wireless USB, handset, headset
ZigBee	250kbps	30mA TX, standby 3#&956;A	4"32KB	Long battery life, low cost	Remote control, battery-operated products, sensors

Table 1 Wireless technology comparison chart

9. CONLUSION

It is likely that ZigBee will increasingly play an important 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 (for limited capability end devices, the stack size is as low as 4 KB). 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, mainly, extremely low power consumption for (long) 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 highly sought after in many networks that are characterized by numerous nodes consuming minimum power and enjoying long battery lives. ZigBee technology is designed to best suit these applications, for the reason that it enables reduced costs of development and very fast market adoption.

REFERENCES

[1] ZigBee Alliance,ZigBee Specification.Version 1.0 ZigBee Document 053474r06, December 14th, 2004.

[2] P. Kinney, ZigBee Technology: Wireless Control that Simply Works, White Paper dated 2 October 2003.

[3] Behrouz A. Frouzan, “Data Communication”, Third Edition, Tata McGraw-Hill Publishing company Limited, 2004, Pp 19-110.

[4] Andrew S. Tenenbaum, “Computer Networks”, Fourth Edition Pearson Publication Limited, 2003, Pp 21-89.

[5] William Stalling, “Wireless Communication and Networks”, Fourth Edition, Pearson Publication Limited, 2004, Pp 39-118.

[6] 802.15.4, Part 15.4: Wireless Medium Access Control(MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LRWPANs).

[7] Sheng-Fu Su, The Design and Implementation of the ZigBee Protocol Driver in Linux, White Paper dated 26 July 2005.

[8] Jacob Munk-Stander,Implementing a ZigBee Protocol Stack and Light Sensor in TinyOS,White Paper dated October 2005.

[9] Freescale Semiconductor,ZigBee Implementer’s Guide ;Document Number:F8W-2004-0007,May 23, 2005

[10] Weiser, M. (1991). The Computer for the 21st Century. *Scientific America*, September 1991. 94-104.

[11] Kahn, J.M., Katz, R.H., Pister, K.S.J. (1999). Next century Challenges: Mobile Networking for "Smart Dust" Proceedings of the 5th Annual ACM International Conference on Mobile Computing and Networking (MobiCom)

[12] 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

[13] *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.

[14] *ZigBee Specification v1.0*, ZigBee Alliance, December 14th, 2004.

[15] Tanenbaum, A. S., Gamage, C., & Crispo, B. (2006). Taking sensor networks from the lab to the jungle.Computer, 39(8), 98-100.

[16] 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. Paper presented at the Proceedings of the 3rd ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor and Ubiquitous Networks, Terromolinos, Spain. 48-57.

[17] Gorbis, M., & Pescovitz, D. (2006). IEEE fellow's survey: Bursting tech bubbles before they balloon. *IEEE Spectrum*, 43(9), 50-55.

[18] Tseng, Y., & Pan, M. (2006). Quick convergecast in ZigBee/IEEE 802.15.4 tree-based wireless sensor networks. *MobiWac '06: Proceedings of the international workshop on Mobility management and wireless access*, 2006, 60-66.

[19] Ran, P., Sun, M., Zou, Y. (2006). ZigBee routing selection strategy based on data services and energy-balanced ZigBee routing. *APSCC '06*, December 2006, 400-404.

[20] Chen, B., Wu, M., Yao, S., & Binbin, N. (2006). ZigBee technology and its application on wireless meterreading system. *Industrial Informatics, 2006 IEEE International Conference on*, August 2006, 1257-1260.

[21] Schlessman, J., Shim, J., Kim, I., Baek, Y. C., & Wolf, W. (2006). Low power, low cost, wireless camera sensor nodes for human detection. *Proceedings of the 4th International Conference on Embedded Networked Sensor Systems*, October 2006, 363-364.

[22] Jiang, Y., Cao, J., & Du, Y. (2006). Unmanned air vehicle landing based on Zigbee and vision guidance. *WCICA 2006*, 2, 10310 - 10314.

[23] James Kurose & Keith W. Ross, "Computer Networks", Fourth Edition, Pearson Publication Limited, 2004,Pp 49-98.

[24] M. Gerla, C. R. Lin. "Adaptive Clustering for Mobile Wireless Networks". : IEEE Journal on Selected Areas in Communications, Vol.15 N.7.

[25] Singh', Sanjay, Kumar, Dhurandher'. "Weight Based Adaptive Clustering in Wireless Ad Hoc Networks". : School of Computer & Systems Sciences, Jawaharlal Nehru University, India.

[26] http://www.zigbee.org/en/documents/zigbeeoverview4.pdf

[27] http://www.palowireless.com/zigbee/tutorials.asp

[28] http://www.zigbee.org/en/resources