IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-6, Issue-3 E-ISSN: 2347-2693

Ad-Hoc Wireless Sensor Network Based on IEEE 802.15.4: Theoretical Review

K. Mor[1*], S. Kumar[2], D. Sharma[3]

[1*]ECE Department, University Institute of Engineering and Technology, MDU, Rohtak, Haryana, India
[2]ECE Department, University Institute of Engineering and Technology, MDU, Rohtak, Haryana, India
[3]ECE Department, University Institute of Engineering and Technology, MDU, Rohtak, Haryana, India

[*]*Corresponding Author: morkirti7@gmail.com*

Available online at: www.ijcseonline.org

Received: 20/Feb//2018, Revised: 26/Feb2018, Accepted: 19/Mar/2018, Published: 30/Mar/2018

***Abstract*—** Ad-hoc wireless sensor networks (AWSN) have become the most standard technical development in commercial and industrial applications. The use of AWSN along with Zigbee standards in Wireless Personal Area Networks (WPAN) has paved the way for effective data collections with optimum use of network resources. Zigbee Technology is designed for low cost of deployment, low complexity and low power consumption. This paper presents a comprehensive review on AWSN and its routing protocols. This paper also presents a detailed description of Zigbee technology, its various standards and enabling technologies.

***Keywords*—-** Medium access control (MAC), Personal Area Network (PAN), ZigBee Trust Center (ZTC), Zone Routing Protocol (ZRP), Optimized Link State Routing Protocol (OLSR), Temporally Ordered Routing Algorithm (TORA)**.**

I. INTRODUCTION

AWSN has become the most standard technical development in commercial and industrial applications for measuring and analyzing physical conditions (temperature, pressure) and monitoring for security purposes, smart spaces and medical systems [1]. In wireless links the losses can occur due to interference and fading of the signal during transmission over long distances. Therefore, to overcome these issues in AWSNs, the Zigbee technology developed by Zigbee Alliance is used for effective delivery of services in AWSN. The effective lifetime of the sensor nodes depends on the battery. In active sensor nodes, power consumed in maintaining topological control, data aggregation, energy balance routing and relay nodes. The use of Zigbee in AWSNs minimizes power consumption while maintaining optimal Quality of services (QoS) [2]. In this paper the various technological aspects related to AWSNs and Zigbee technology are described in Section 2 and section 3 respectively.

II. AD-HOC WIRELESS SENSOR NETWORK

AWSNs is a subset of the Ad-hoc networks and does not require any infrastructure like base station, mobile towers, etc. present in conventional communication networks. AWSN is widely used to detect events, to collect data and to transmit them to intended destination for analysis. AWSN consists of homogenous detection nodes (also called motes) which communicate with each other using RF links [3]. The sensor nodes consist of three parts: sensors (for detection), microcontrollers (for processing) and RF channels (for communication). The main characteristics of the sensor nodes are low cost, with limited computing capacity and memory exploited with limited battery power. The microcontroller used in the sensor nodes have small RAM and flash memory size but high clock speed.

The AWSN operation cycle is divided into the following phases [4]:

- Birth Phase: This is the start of an Ad-hoc wireless sensor network. This is a very energy demanding phase due to the organization, configuration and optimization. It is therefore necessary to develop initialization protocols with minimal energy consumption.
- Life stage: It is next stage that is involved in full operation mode. It carries out the detection, the notification and the transmission of data. The main objective of this phase is to maintain the predefined quality of service.

- Phase of death: This phase begins with the damage of the primary node and the lowering of the quality of service. The beginning of the death phase is different in different applications.

In [5], authors have presented a comprehensive literature survey on wireless sensor networks. They have analyzed AWSN as a combination of sensor, embedded techniques and distributed information. They have also classified Routing protocols based upon three categories which flat, hierarchical and location with main objective to increase the life time of WSN.

A. Routing Protocols used in Ad-hoc Wireless Sensor Network

Routing protocol is used by router to determine the appropriate path over which data is transmitted. Main tasks of the routing protocols are [6]:

- To learn available routes.
- Build Routing Tables.
- Make Routing decisions the shortest path.

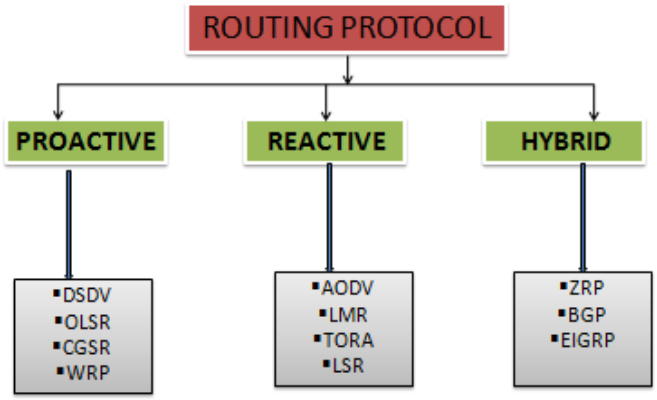

Figure 1. Routing protocols used in Ad-hoc

Each of these Routing protocol are explained in detail below.

Proactive Protocol: In these routing protocols, each node in the network maintains a routing table for all the neighboring nodes. The routing table is updated whenever there is a change in network topology. In case of change in network topology, each node sends a broadcast message to the network regarding the change [7]. Distance vector (DV) and Destination Sequenced Distance Vector (DSDV) Routing protocols are types of Proactive protocols.

Reactive protocol: These are on-demand routing protocols, in which the source node construct a path only when a request is received. It uses two way-paths from source to destination node for effective communication [8]. Ad-hoc on demand distance vector (AODV) and Label based Multipath Routing (LMR) are the examples of Reacting Protocol.

Hybrid Protocols: Hybrid protocols like Zone routing protocol and Border gateway Protocol are used to overcome the disadvantages of proactive and reactive protocols by minimizing the overhead of control message in proactive and decrease the latency problem in reactive routing protocols [9].

Table 1 describes the survey literature of different routing protocols and their metrics comparison:

Table 1. Parametric comparison of different routing protocols

Routing Protocols	Packet Loss	Packet Received	Through-put	End To End Delay
DSR,AODV & DSDV[10]	DSR have minimum packet loss	DSR have better packet received ratio	DSR is better	-
AODV, TORA, OLSR, DSDV[11]	-	AODV is better	DSDV is better	DSDV is better
DSR,AODV & DSDV[12]	DSR have minimum packet loss	AODV is better	AODV is better	AODV & DSDV outperform
AODV, ZRP, DSDV[14]	-	AODV is better	AODV is better	AODV is better
AODV, DYMO, DSR[15]	-	DYMO is better	DSR is better	DYMO is better

In [10] review of Ad-hoc routing protocols are discussed. It also includes various parametric comparisons between DSR, AODV and DSDV. DSR provides better performance among all routing protocols.
In [11], focuses on the designing of any type of wireless networks and performance analysis of different Routing protocols such as AODV, TORA, OLSR and DSDV. By comparing the performance of all routing protocols DSDV provides better performance in any Ad-hoc network by varying parameters like number of nodes.

In [12], performance analysis of reactive and pro-active routing protocols like DSR, AODV (Reactive) and DSDV (proactive) has been discussed. If we analyzed the result each protocols has its own pros and cons.

In [13], author described the performance analysis of developed prototype systems and its quality of service parameters (delay, throughput, packet loss) can be found out over line of sight and non-line of sight. In this paper author concluded that Zigbee based WSN is more suitable for low data rate applications. It also provides the analysis of multi-hop network which decreases when compared to direct transmission in terms of parameters.

The author in [14], described two protocols (i) AODV (ii) DSDV. The performance of these protocols has been analyzed in two ways (i) keeping no. of CBRs constant (ii) varying nodes from 10 to 50. The performance metrics simulated in this paper are throughput, jitter and average end to end delay. Author concluded that AODV perform better when CBR is constant and nodes varied. When applied second condition, nodes constant and CBR varied then also AODV outperform among DSDV and ZRP. Hence it is concluded that AODV is better in all conditions.

In [15], Author described that Ad hoc network and all routing protocols have been defined on the basis of their properties for Zigbee WPANs. Reactive protocols have been defined here for IEEE standard 802.15.4 Zigbee protocol. Ad hoc routing protocols have been defined on the basis of (i) Table driven, (ii) on demand (iii) Hybrid. Proactive routing protocols known as table driven and reactive known as on-demand routing protocols. Author concluded that DSR is much better in terms of traffic load and throughput than AODV (Ad-hoc on demand Distance Vector) and DYMO (Dynamic Manet on Demand). But in terms of end to end delay and average jitter it performs less as compared to both. DYMO is much better than AODV in all comparisons.

In [16], author evaluate different Mobile ad-hoc routing protocols implemented in WSN for environmental monitoring. Primary factors which described for system operation are (i) longer network life (ii) low latency. The network is assumed to be with one base station connected to a wireless wide area network, receiving the sensor measurements**.** The study focused on the impact of rapid mobility caused by the surface movements**.** Authors simulate the impact of energy constraints and random way point mobility pattern in physical layer and application layer of the nodes. According to results AODV (Ad-hoc on demand distance vector routing) provide better energy consumption.

III. ZIGBEE TECHNOLOGY

Zigbee is designed by Zigbee alliance and standardized by IEEE 802.15.4 specification is designed for the upper layer (network, security and application layer). Zigbee is used for low latency wireless personal area networks (WPAN) devices and works on 3 frequencies band with 27 channels [17]. It is designed to consume less power as compared to Bluetooth, WI-FI and WI-MAX. It provides a maximum throughput of 250 kbps in a range of 10 to 100 m. Zigbee works in frequency bands of 868MHZ, 902-924MHz and 2.4GHz. Figure 2 shows the Zigbee architecture which consists of three layers: physical layer MAC layer and upper layer (network layer, application layer)[18].

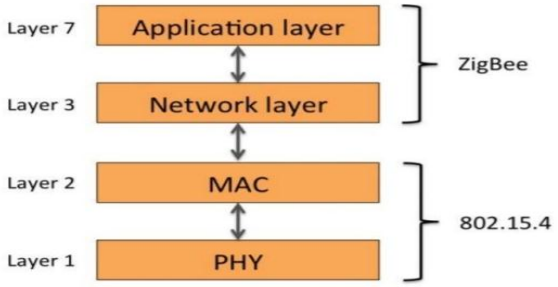

Figure 2. Architecture of Zigbee Technology

Physical Layer: Physical layer is defined in IEEE 802.15.4 standard (hardware) deals with transmission and reception of data. Table 2 shows the specified frequency band used in physical layer. Highest range Frequency band 2.4 GHz is universal license free band and is used at data rate of 250 kbps by 11 channels.

Table 2. Frequency band used in physical layer

Frequency Range	Band	Coverage	Data Rate(kbps)	Channels
2.4 GHz	ISM	Worldwide	250	11-26
902-928 MHz	ISM	America	40	1-10
866 MHz	-	Europe	20	0

MAC Layer: It is used for broadcast data or sharing a medium is required then communication. There are two broad categories of MAC protocol: Contention based (ALOHA) and Contention less. In broadcast transmission problem of collision occurs when several devices transmit data at same time. TDMA, FDMA and CDMA methods

are used to establish a proper channel and to avoid the problem of collision.

Network Layer: The main functions of network layer is congestion control, Routing , Inter-networking and deals with end to end delivery of packets.

Application Layer: It is the most important layer and acts as medium between users and other layers. The main functions of this layer are identifying communicating partners , determining resource avalibility and synchronizing the communication.

A. Frame structure of physical and Medium Access Control Layer

Figure 3 shows the frame structure for Zigbee based upon IEEE 802.15.4 design. This protocol stack provides feature for nodes to search an existing network, to form new network or to join in a network and supports the broadcast or uncast addressing mode [19].

The MAC layer program provides information regarding channel to be accessed, generates address information and appends data bytes into MAC layer data frame. The Zigbee network coordinator access each end node by pointing different arrays of destination address field sequentially.

In [20], author discussed about two critical factors for WSN (i) energy consumption (ii) network life time using IEEE 802.15.4 standard for low data rate Wireless Personal Area Networks (WPANs). The superframe structure of Medium Access Control layer (MAC) in IEEE 802.15.4 allows devices to access channels in a Contention Access Period (CAP) or Collision Free Period (CFP). In MAC layer Beacon based synchronization procedure is used. IEEE 802.15.4 networks use two modes for data transfer which is beacon and non beacon: Beacon mode act as sleep mode in order to overcome the energy consumption whereas Non-beacon mode acts as acknowledgement mode to enhance the communication reliability.

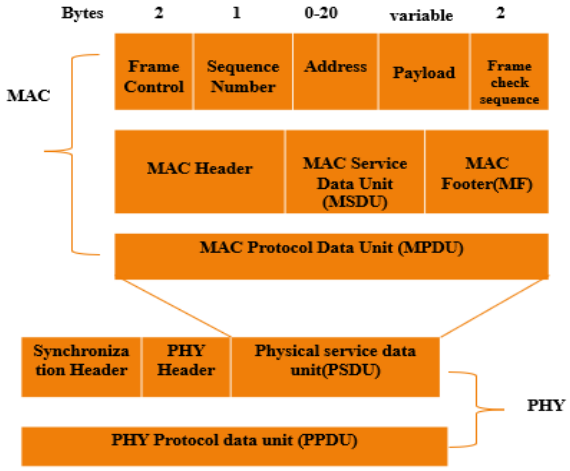

Figure 3. Frame structure of Zigbee Layers

The data transfer occurs in two ways: Beacon mode and non-beacon mode. In non beacon mode the network is always in active mode and constantly monitors the arrival of data hence consumes more power. It works in asleep mode, because at any time any mote can get up and communicate. Beacon mode works in sleep mode because, in the absence of a data message from the terminals, the routers and coordinators go into sleep mode [21]. Sometimes the coordinator gets up and transfers the data to the system routers. The main benefit of beacon mode is the reduction of work cycles and prolonged use of the battery. Periodic (sensor data), intermittent (light switches) and repetitive these types of data are managed by beacon mode and non-beacon [22].

IV. SECURITY SERVICES IN ZIGBEE

Key establishment, key transport, frame protection and device authorization are the main services used by Zigbee Network for security purposes. The Zigbee security architecture includes three layer security mechanism of protocol stack: Application, MAC and Network. MAC layer decide their security itself, but application and network layer decide the level of safety to apply. The Advanced Encryption Standard (AES) in Zigbee design uses a key size of 128 bits. The main keys used in Zigbee are Master, Network and Link [23].

The network key is a general key used for key update purposes by all nodes of a network. Link key also known as secret session keys are used for communication between two devices. The approach by which master, link, and network keys are generated, stored, processed, and sent to devices calculates the efficiency and overall security of the entire network. Zigbee Trust Center (ZTC) is the vital part of the Zigbee security architecture and it concern about the

whole Zigbee network. The main task of ZTC are Trust management, network management, configuration management, and to collect and allocate the keys of Zigbee devices.

In [24], author has described the applications of WSN for providing security in military, hospitals and weather departments. Authors have used WSN as two motes (nodes)(i) Crossbow "MICAz" mote (ii) Berkeley's "MICA2" mote. For enhancing security levels in WSN, the authors used two cryptographic schemes using asymmetric key and symmetric key. After simulations the authors concluded that symmetric key schemes are better than asymmetric key schemes in providing greater degree of security while improving end to end delay.

In [25], Zigbee security architecture, security services, security model, security components, security keys and the Trust Centre, security measures of each layers have been described. The authors deeply studied and analyzed the security mechanism of Zigbee to further improve the security schemes and describe different methodology for improvement.

In [26], Author described security structure of Zigbee wireless network and its layers. Moreover, it also defined the authentication and encryption in Zigbee technology and proposes opinions for network security protection, solves the confidentiality integrity and access control problem in network communication.

V. CONCLUSION

This paper presents a theoretical review of AWSN routing protocols and Zigbee application for WPAN. Finally, concluded that WPAN using Zigbee application has many advantages including low cost, low power consumption, longer battery life, greater range and high reliability in mesh networking. This paper will help researchers to get information related to Zigbee technology at a single platform and help them to pursue their research in an efficient and effective manner.

REFERENCES

[1] R. Gupta, H. Aggarwal, "*Ad-hoc routing protocol "review paper*", Journal of Global Research in Computer Science, ISSN:2229-371X, Volume 4, No. 5, pp.26-29, 2013

[2] S.K. Kurmi, N.K. Saluja, S. Patel, "*Performance Analysis of Quality of Service Evaluation in IEEE 802.15.4 Wireless Sensor Networks*", International Journal of Engineering Sciences & Research Technology, ISSN: 2277-9655, pp.3516-3522, 2013.

[3] D. Sharma, "*An overview of Wireless Sensor Networks*", International Journal of All Research Education and Scientific Methods (IJARESM), Volume 3, Issue 4 ISSN: 2455-6211, pp.29-33, 2015.

[4] J. Balen, D. Zagar, G. Martinovic, "*Quality of Service in Wireless Sensor Networks: A Survey and Related Patents*", Recent Patents on Computer Science, ISSN: 1874-4796, Vol. 4, No. 3, pp.188-202, 2011.

[5] Reena, S. Phulre, R. Pandit, "*Wireless sensor network and its routing protocol: A survey paper*", International Journal of Computer Science and Mobile Computing (IJCSMC) , ISSN: 2320-088X, Vol. 2, Issue. 6, June 2013, pp.60 – 64, 2013.

[6] M. Abuhmida, K.R. Krishnan, "*Performance Evaluation of Mobile Ad-hoc Routing Protocols on Wireless Sensor Networks for Environmental Monitoring*", 17th UKSIM-AMSS International Conference on Modeling and Simulation, 978-1-4799-8713-9/15,DOI 10.1109/UKSim.2015.60, pp.544-548, 2015.

[7] S.R. Biradar, H.H.D. Sharma, K. Shrama, S.K. Sarkar, " *Performance Comparison of Reactive Routing Protocols of MANETs using Group Mobility Model*", International Conference on Signal Processing Systems (IEEE), pp.192-195, 2009.

[8] A.A.A. Radwan, T.M. Mahmoud, E.H. Houssein E.H, " *Evaluation comparison of some ad hoc networks routing protocols*", Egyptian Informatics Journal, doi:10.1016/j.eij.2011.04.001, pp.95–106, 2011.

[9] H.D. Trung, W. Benjapolakul, P.M. Duc, "*Performance evaluation and comparison of different ad hoc routing protocols*", Elsevier Comput Commun; pp.2478–96, 2007.

[10] M. Gupta, S. Kumar, "*Performance Evaluation of DSR, AODV And DSDV Routing Protocol for Wireless Adhoc Network*", IEEE International Conference on Computational Intelligence & Communication Technology, DOI 10.1109/CICT.2015.95, pp.416-421, 2015.

[11] R. Kumar, P. Singh, "*Performance analysis of AODV, TORA, OLSR and DSDV Routing Protocols using NS2 Simulation*", International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753, pp.416-421, 2015.

[12] S.S. Tyagi, R.K. Chauhan, "*Performance Analysis of Proactive and Reactive Routing Protocols for Ad hoc Networks*", International Journal of Computer Applications (0975 – 8887).Volume 1 – No. 14, pp.27-30, 2010.

[13] H. Fitriawan, M. Susanto, A.S. Arifin, D. Mausa, A. Trisanto, "*ZigBee Based Wireless Sensor Networks and Performance Analysis in Various Environments*", 15th Intl. Conf. QiR: Intl. Symp. Elec. and Com. Eng, pp.272-275, 2017.

[14] Preeti, S. Bishnoi, "Wireless Sensor Network based AODV and DSDV Routing Protocols using Qualnet", International Journal of Enhanced Research in Science, Technology & Engineering, ISSN: 2319-7463, Vol. 5 Issue 6, pp.194-200, 2016.

[15] Narmada, S. Rao, "Comparison of Routing Protocols for Zigbee WPANs Performance", International journal of computer science issues (IJCSI), ISSN: 1694-0814, vol 8, pp. 394-402.

[16] M. Singh, S.N. Thakur, "*Comparison of DSDV, DSR and ZRP Routing Protocols in MANETs*". International Journal of Computer Applications (0975 – 8887) Volume 108 – No. 13, 2014.

[17] K. Kaushal, T. Kaur, J. Kaur, "*Zigbee based Wireless Sensor Networks*", International Journal of Computer Science and Information Technologies, ISSN: 0975-9646, Vol. 5 (6), pp 7752-7755, 2014.

[18] G. Singh, R. Bhardwaj, K. Singh, S. Mehla, "*ZigBee: A Review*", International Journal of Computer Science and Information Technologies (IJCST), ISSN: 2229-4333 (Print), Vol. 3, No 1, pp.328-332, 2012.

[19] Amol B.Suryawanshi, Baljit Kaur Saini, "Survey on Various Routing Protocols in Ad-hoc Networks", International Journal of Scientific Research in Network Security and Communication, Vol.5, Issue.3, pp.174-178, 2017.

[20] K.M. Mohan, C. Bagavathi, K. Shalini, "*A power efficient Mac protocol for quality of service evaluation in wireless sensor networks*", International Journal of Innovative Research in Electrical, Electronics, Instrumentation And Control Engineering, ISSN: 2321-2004, Vol.2, pp.2154-2159, 2014.

[21] Surender, P. Samundiswary, "*Performance Analysis of Node Mobility in Beacon and Non-Beacon enabled IEEE 802.15.4 based Wireless Sensor Network*", International Journal of Computer Applications (0975 – 8887) Volume 76– No.12, pp 32-35, 2013.

[22] S.K. Guha, P.Y. Nabhiraj, T.K. Bhaumik, C. Mallik, "*Design and implementation of an IEEE 802.15.4 / Zigbee based Star Network for data Acquisition and Monitoring*", Proceedings of PCaPAC2012, Kolkata, India, ISBN 978-3-95450-124-3, pp.160-162, 2012.

[23] Ishita Chakraborty, Prodipto Das, "*Data Fusion in Wireless Sensor Network-A Survey*", International Journal of Scientific Research in Network Security and Communication, Vol.5, Issue.6, pp.9-15, 2017.

[24] sB. Fan, "*Analysis on the Security Architecture of ZigBee Based on IEEE 802.15.4*", IEEE 13th International Symposium on Autonomous Decentralized Systems, DOI 10.1109/ISADS.2017.23, pp.241-246, 2017.

[25] M. Qianqian, B. Kejin, "*Security Analysis for Wireless Networks Based on ZigBee*", International Forum on Information Technology and Applications, DOI 10.1109/IFITA.2009.439, pp.158-160, 2009.

[26] J. Sen, "*A Survey on Wireless Sensor Network Security*", International Journal of Communication Networks and Information Security, ISSN: 2073-607X (Online) vol. 1, pp.55-78, 2009.

Authors Profile

Mrs. Kirti pursed Bachelor of Technology from N.C. Institute of Technology in year 2016 and currently pursuing Master of Technology from University Institute of Engineering &Technology (UIET), MDU and Rohtak, India.

Col (Dr.) Suresh Kumar has served in Corps of Signals (Indian Army) After taking PMR, joined as teaching faculty in UIET, MDU Rohtak, in Department of ECE in October 2008.He did his B.Tech from CME Pune and MCTE Mhow in 1999 from JNU New Delhi in Electronics and Communication Engineering. He did his PhD. In ECE in 2011 on the title "CONTROL SPILL OVER OF TRANSMITTED POWER IN CDMA CELLULAR COMMUNICATION NETWORKS IN BORDER AREAS FOR DEFENCE FORCES". His area of specialization is wireless and Optical communication. He has guided 06 PhD. Thesis(04 awarded and 02 pursuing) and 24 M Tech students dissertations. He has published 85 papers in International Journals and international/national conf proceedings in India and abroad.

Mr Deepak Sharma is a PhD Research Scholar in Department of Electronics and Communication Engineering, UIET, MDU Rohtak. His research Interest areas include heterogeneous wireless networks, MANETs and optical networks. He has published 35 research papers in International journals and in International/National Conference proceedings.

