International Journal of Advanced Technology in Engineering and Science
Vol. No.3, Issue 11, November 2015
www.ijates.com
ijates
ISSN 2348 - 7550

SURVEY ON RESPONSIBILITIES OF DIFFERENT OSI LAYERS IN WIRELESS SENSOR NETWORKS

Keshav Kaushik[1], Bharat Bhushan[2]

[1]B.tech Student , [2]Assistant Professor, Dept. of Computer Science and Engineering, HMRITM, Hamidpur, New Delhi, (India)

ABSTRACT

In computing protocol is a standard that controls connections, data transfer and communication. In simple words protocol can be defined as the rules for governing the syntax, synchronization of communication and semantics. Protocols can be implemented by hardware or software or both. For successful and secure communication and data transfer one should be aware of the protocols of wireless sensor networks. This short survey on protocols of wireless sensor networks will try to provide sufficient knowledge of wireless protocols at beginning. This short paper provides lecture notes on protocols of computing.

I. INTRODUCTION

Past few years WSN (Wireless Sensor Networks) have gained importance and research fields because of its large number of applications in world. The application of WSN ranges from environment monitoring to ecological monitoring, ocean monitoring, earth-quake monitoring and military investigations. Sensor nodes are combined to make a Sensor network. Only limited amount of data can possess on each sensor nodes. The future of WSN includes monitoring of biomedical conditions of living organisms, traffic conditions of surroundings. Combination of sensor nodes from deployed environment are compromised to make sensor networks [2]. In sensor networks sensor nodes face disability due to limited processing capabilities, storage communication and limited power. Data aggregation is process which is used to overcome the disability of limited power in sensor networks [3]. Data aggregation technique is used to reduce data in sensor environment. Thus energy of battery is conserved due to reduction of data [4]. Aggregators are the nodes used to receive signal from Sensor nodes sends aggregated or condensed reading further [5].

Wireless sensor networks is a great research area because it requires security in communication with other sensor nodes, sensor nodes for high security requires issues like data integrity, data authentication, confidentiality and key management etc. [6]. In this paper we are providing short lecture notes on protocols of wireless computing and layers of Open System Interaction model (OSI).

The OSI model is conceptual model that standardizes communication functions of telecommunication without in respect of basis of technology and internal structure. The goal is to interaction of diverse communication system with standard protocols. Network protocols are as following

Protocols of Wireless Sensor Networks

The open system interconnection model consists of 7 layers . The lowest layer or first layer of computing protocol is Physical layer The second most layer is Data link layer, The third layer is Network Layer, the fourth

layer of computing protocol is Transport Layer, the fifth most layer of computing network is Session Layer, The Sixth Layer of WSN is Presentation layer And the last, seventh layer is known as Application Layer.

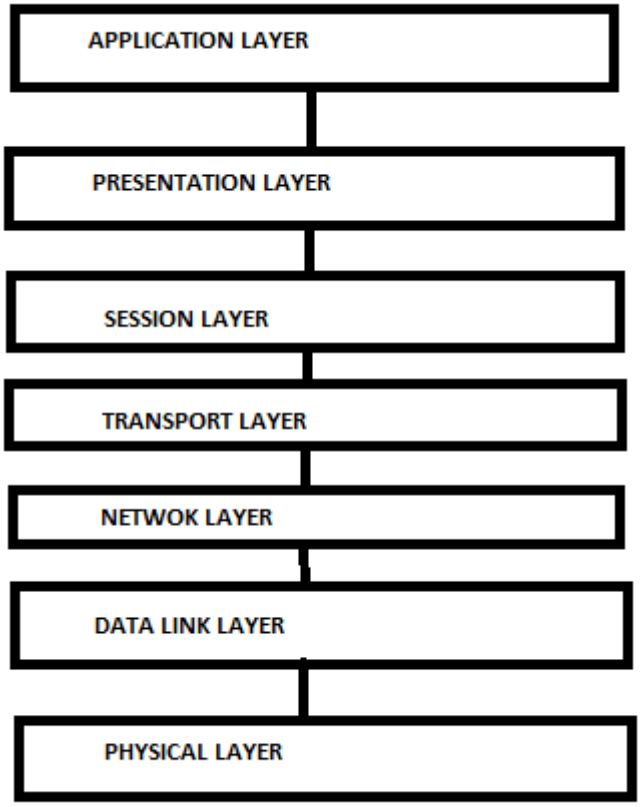

Fig. 1. The General Structure of OSI Layer

II. PHYSICAL LAYER PROTOCOL

In seven-layer Open System Interconnection system of computer networking this layer is lowest. This is also known as L1 and abbreviated by PHY. The PHY layer consists of networking hardware transmission technologies. In this fundamental layer logical data structures of higher level function network is underlined. This layer is most complex layer of Open System Interconnection System.

The PHY layer defines means of transmitting bits rather than logical packets over PHY link nodes. Big stom are converted into gathered combination and converted into symbols or code wordsand converted to PHY signal which is transmitted through medium of hardware-transmission. PHY layer provides mechanical, electrical a procedural interface – transmission medium. The properties of electrical equipment's frequency to broadcast modulation scheme. Uses of PHY layer

Interfaces with data link layer, Performs encoding , transmission , reception and decoding of encoded data .Galvanic isolation, Symbol by symbol or bit by bit delivery, Modulation, Point to Multipoint configuration

The PHY layer uses ARINC818 AVIONICS Digital Bus Protocol. The PHY layer consists of following hardware equipment's.

Network adapter, Controller, Repeater, Network-Hub ,Fiber-Media Controller

Jamming is attack on PHY layer. This attacks interfere between radio signals emitting from nodes of network. This attack can be very dangerous to security of computing networks if only one similar frequency is used in whole network operations. Jamming can affect largely by injecting impertinent packets receiver will also consume energy [7].

III. DATA LINK LAYER

This layer is also known as Layer 2 because it is second most layer of Open System Interconnection model of computer networking. This layer protocol is used for transmission of data between adjacent network nodes in WAN (Wide Area Network) / between similar nodes on LAN (Local Area Network). This layer is also used for detection of errors in physical layer also provide procedural and functional means of transfer Local Area Network. This layer does not cross the boundary of Local network. Global boundaries and internetworking are high- layer functions allowing to focus on delivery. Without concern of ultimate destination, the Layer 2 is analogous to neighbourhood cop: it endeavours to arbitrate. When devices try to use medium simentanously frame the collision may occur. The Layer 2 specify how devices recovers and detect these collisions and provide solution to recover these collisions. Example of Layer 2 is PPP (point to point protocol)

3.1 SUBLAYERS of Layer 2

1. **Logical Link Control (LLC)**: - Multiplexes protocol running at the top the layer 2 provides flow control error notification. The LLC provides address & control of data link.
2. **MEDIA ACESSS CONTROL (MAC)**: - This sublayer determines who is allowed for access. Aftertimes it refers to frame structure delivery. There are Two types of MAC Distributedand counterlaized these are used to communicate between people. The Media Access Controller used for frame synchronization

IV. NETWORK LAYER

Network layer is also known as Layer 3because it is 7th layer of OSI model. This layer is responsible for packet transfer including routing from intermediate routers. Functions of Layer 3 are as follows

This layer provides procedural and functional mean of converting data different length data arranged in sequence to destination from source

Connection Model: - Connectionless Communication forex- IP is connection less communication, in datagram travel to receiver from senderdoesn't have to send an acknowledgment.

Host addressing: - Each Host in network should have a unique address. By which they determine the location of nodes. Hierarchical System is used to give unique address to each node.

The network is divided into sub parts and connects to another networks. For this specialized hosts gateways or routers to forward packets.

V. TRANSPORT LAYER

This layer is also known as Layer 4 because it is 7th layer of OSI model. Layer 4 provides host-host and end-end communication services for OSI layer components & protocols. Services like reliability, flow control, multiplexing and connection aimed DataStream support are provided by Layer 4. IP/TCP model both contains

Transport Layer IP/TCPare also known as founders of Internet. TCP (Transmission Control Protocol) is best Layer4 protocol.Connection oriented transmission is obtained by TCP. User Datagram Protocol is used by connectionless networks and used for simple messaging Transmissions

VI. SESSION LAYER

The session Layer is also known as Layer5 because this layer is 5th layer of 7 layer OSI model. The mechanism for closing, opening & managing Session between application process sessions communication consists permanent dialogue. Environment make use of Remote Procedure Calls. In case of loss in data this protocol tries to recover data. If the connection is not in use then for larger time then it close and reopen it. Examples of Session layer

- SCP (session control protocol)
- ZIP (Zone Information Protocol)

VII. PRESENTATION LAYER

This Layer is also known as Layer6 because this is 6th layer of the OSI model. Formatting and delivering information is responsibility of 6th layer of OSI model to application layer or Layer 7 for further processing and display. The presentation layer consists of following parts

MULTIPLEXER & DEMULTIPLEXER, ENCODER & DECODER, ENCRYTPTION & DECRYPTION, ANIMATION MULTIPLEXER: - A multiplexer is an electronic device selects one either digital or analog input and forward that input into one singleline. The multiplexer consists of 2*m input where m are select lines. The use of multiplexer is used to increase quantity of data to be sent.With the help of multiplexer we can reduce bandwidth of the signal. Another name of multiplexer is dataselectors.

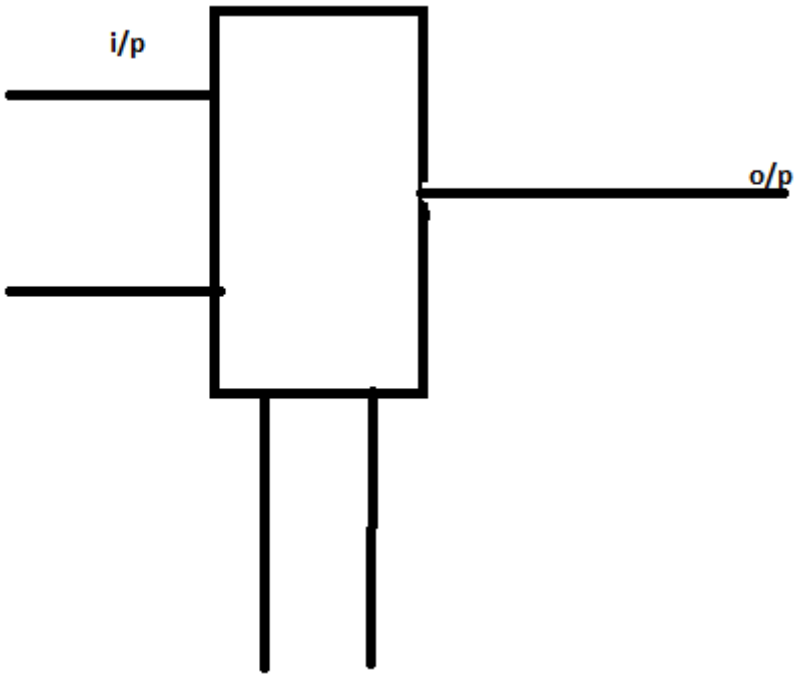

Fig. 2. The General Structure of Multiplexer

DEMUILTIPLEXER:-This device take 1 line input and convert it into many lines.

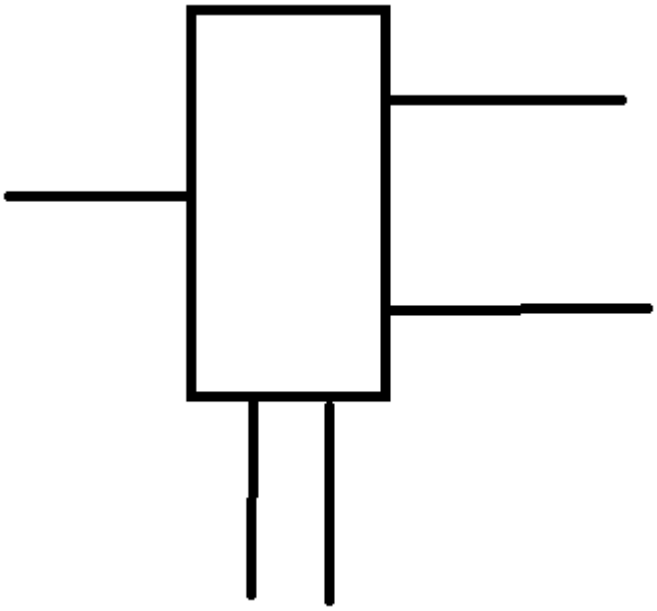

Fig. 3. The General Structure of Demultiplexer

DECODER: - decoder have m input and 2 *m mtimes. Decoders are used to convert coded data into uncoded data. The input of decoder in in binary form but in coded binary form and the decoder will convert in encoded binary data.

ENCODER: - This is an electronic device and which have its extensive property in graphics display, data manipulation which is required in Layer 6. These devices are used to convert simple binary no. into binary code.

ENCRYPTION:- encryption is process for encoding messages and information in an way in which only authorised persons are allowed to see. The encryptor denies message content it interceptorencoder does not prevent itself from interception. To encrypt code we require cryptography techsnique

Decryption: - In this process the encrypted data is converted in an non-coded information. The decoder also uses a technique of cryptography.

ANIMTION: - a process of creating illusion of shape and motion by rap[id display technique in a sequence of static images. Animation can be recorded on analogue media or flipbook, motion picture and other.

VIII. APPLICATION LAYER

This layer is at the top of the OSI model layer segment and known as Layer 7 This layer interface methods used by host in an communication network. The application layer have its application in both of computing networking in TCP/IP. The application layer is used to communicate protocol process-process across the intent protocol of computing networking.

APPLICATION LAYER PROTOCOLs: -

Remote login to hosts : telnet, File Transfer Protocol, Simple mail Transfer Protocol, Domain Name system, BOOTP, SNMP (simple network management protocol),CMOT (Common management Information Protocol over TCP)

IX. SYSTEM ARCHITECTURE

Non-communication and Communication objects are divided conceptually in OSI AP (application process). AE (application entity) is Communication object of an Application Process. An Application Entity Consists of one/more Application Service Elements (ASE) as basic sub-objects. Authors implementation Client system in following figure. To support a-synchronous mode operations the MMS-APand MMS-AE implemented as different UNIX processes.

An Application Entity contain User elements and a set Application Service Elements. An MMSAE contains 2 ASE, ACSE. User element uses ASE to completely successful the communication objectives. Messaging Module, high level service provider and AE manager are components of user elements of MMSAE.

Application Program written by AD (application Developer) is MMS application process. MMSAP requires MMSAPI to access MMS services. The communication between MMSAE andMMSAP is supported by SVR4 spipe (stream pipe), full duplex and bidirectional connection.

MMSAP activates MMSAE which starts daemon process. AE belongs to only one AP, MMSAE provides services to MMSAP which activates it. AE can be activated multiples as needed based on AP.

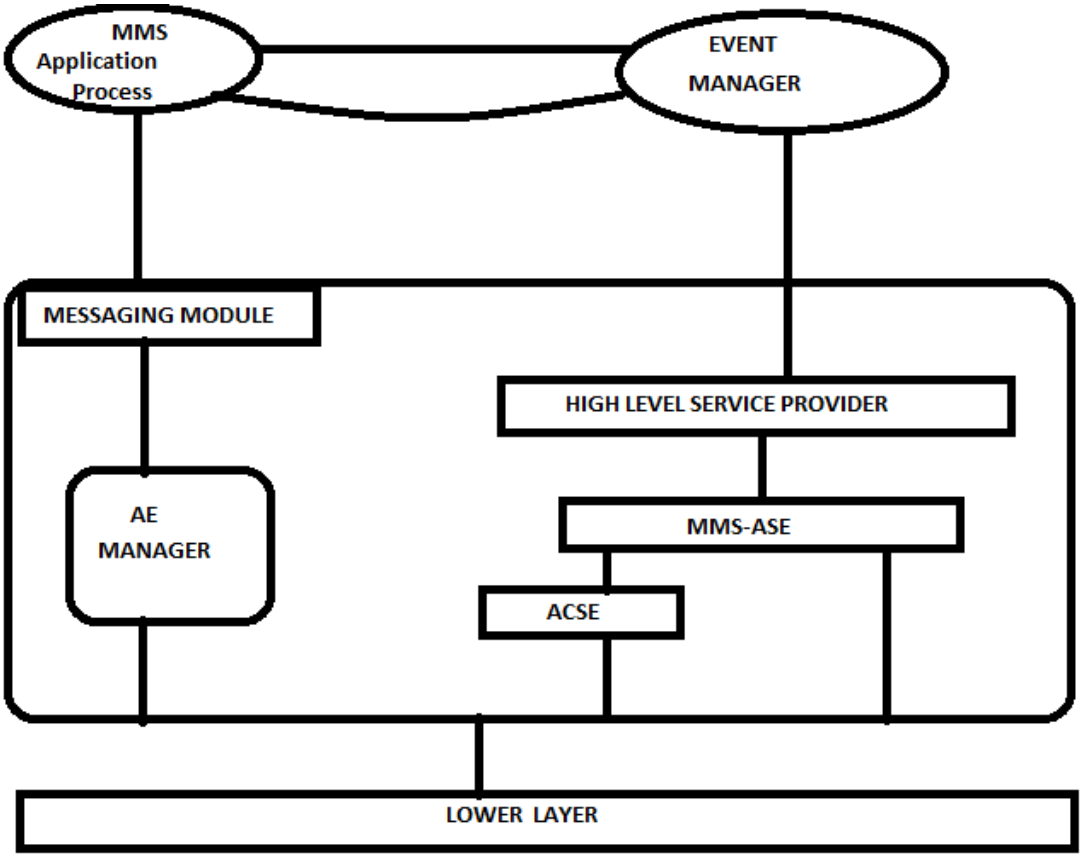

Fig. 4. The General Structure of Implementation of Protocols

X. SENERAL LAYER FUNCTIONS

The layering concept requires certain functions to be performed. Layer management is an example of functions. Following are the important functions –

Connection establishment, Connection release, Connection identification, ID and parameter exchange, Service data unit transfer, Expedited service data unit transfer, Layer management, (N) address to (N-1) address mapping, Service data unit mapping to protocol data unit mapping

XI. CONCLUSION

This paper provides short lecture notes on wireless protocols, and explaining the importance of OSI model protocols in wireless sensor networks and wireless computing. The paper also states it's importance in security issues where application of wireless sensor networks are used. The application of WSN like military aspects require very high secure data processing so it require protocols of WSN for safer and secure data communication.

REFRENCES

[1] Bharat Bhushan, Sandeep Verma, Amit Kumar Rai "A secure Concealed Data aggregation for multiple applications in wireless sensor networks", 'IJERM April 2014'

[2] I. Akyildiz, W.su, Y. Sankarasubramaniam and, E Cayirci, "A survey on sensor networks" ,'IEEE Comm. Magazine'

[3] R.Min, A.Chandrakasan, "Energy-Efficient communication for ad-hoc Wireless sensor networks", '35th Asilomar Conference Signals'

[4] B. Przydatek, D. songA. Perrig,"SIA: secure information aggregation in Sensor networks", '1st International conf. Embedded network system 2003 '

[5] R.Chandramouli, s Bapatla and K>P subbalakshmi."Battery Power- aware encryption., ACM transactions on information and system security"

[6] J. giaro, M. Schneider , D. Westhoff,"CDA concealed data aggregation in WSN" 'Proceedings of ACM workshop'

[7] Hero Modaares, RosliSaalleh, AmirhosseinMoravejosharieh, "Overview of Security Issues In Wireless Sernsor Networks" 'IEEE 2011 3rd international conf. on computaionalinteelligence, modelling & Simulation'

[8] D. Westhoff, J. Giaro and M.acharya, Concealed data aggregation for reverse multicast traffic in sensor networks: Encryption key distribution and routing adaption, IEEE trans. Mobile computing vol5 Oct 2006.

[9] C.dWesthoff, B.Lamparter, and A. Weimerskirch, on digital signaturesin ad hoc networks, J.Eur Trans telecom vol16.

[10] R. Watro, D.kong, S.cuti, C.Gardiner, C.lynn, and P.kruus, Sensor networks with public key technology, in proc 2ndacm workshop security adhoc sensor network 2004.

[11] C.karlof, D.Wanger, Secure routing in wireless sensor networks: attacks and countermeasures, in the proc IEEE int Workshop Sensor network protocols may 2003.

[12] C.castelluccia, E. Mykeltun and G.tsudik, efficient aggregation of encrypted data in wireless sensor networks, Mobile and Ubiquitous systems: networking and services 2005.