Approach of protocol in Wireless Sensor Network.

[1] Venugeetha Y, [1] Dr. B P Mallikarjunaswamy

[1] Research Scholar, Global Academy of Technology, Bengaluru - 560098, Karnataka, India.
venugeeta@gmail.com

[2] Professor, Department of Computer Science and Engineering, Sri Siddhartha Institute of Technology,
Maraluru, Tumkuru - 572105, Karnataka, India.
drbpmswamy@rediffmail.com

***Abstract*—** This paper discusses about the specific definition, types and topologies in a wireless sensor network. It is based on different types of system configuration the type of network is being used to connect the systems through a network. Topologies are understood according to the hop for communicating in the network. Parameters are used to analyses the network coverage, scalability, network longevity and the transmission count. Protocol also is an important understanding of different layer in the network.

Keywords*—*Topology, Protocol, System, Network.

INTRODUCTION

Network is defined as a set of computers connected together for the purpose of sharing resources. These computers on a network are called as nodes and connected via Ethernet cable or wirelessly through radio waves. There are different types of computer networks which can be characterized by their size and purpose. Size of a network can be expressed by the geographic area and the number of computers that are a part of the network. Many networks can be considered general purpose, as they are used for accessing internet to sending files to another host etc. Benefits or advantage to build up a network, are the three big facts - File Sharing, Resource Sharing, Program Sharing. Networks based on size are: PAN, LAN, MAN, WAN. Networks based on purpose are SAN, EPN and VPN.

PAN or Personal Area Network organized around an individual person within a building like office or residence can include computers, telephones, peripheral devices and other personal entertainment devices. A Local Area Network, or LAN, consists of a computer network at a single site or an individual office building. LANs can be built with relatively inexpensive hardware, such as hubs, network adapters and Ethernet cables. The smallest LAN may only use two computers, while larger LANs can accommodate thousands of computers. A LAN relies mostly on wired connections for increased speed and security, but wireless connections can also be part of a LAN. High speed and relatively low cost are the defining characteristics of LANs. If a LAN, is entirely wireless, it is referred to as a wireless local area network, or WLAN.

A metropolitan area network, or MAN, consists of a computer network across an entire city, college campus or small region. A MAN is larger than a LAN, which is typically limited to a single building or site. Depending on the configuration, this type of network can cover an area from several miles to tens of miles. A MAN is often used to connect several LANs together to form a bigger network. When this type of network is specifically designed for a college campus, it is sometimes referred to as a campus area network, or CAN. System Area Network is also known as Cluster Area Network it links high-performance computers with high-speed connections in a cluster configuration. Controller Area Network Controller Area Network or CAN protocol is a method of communication between various electronic devices like engine management systems, active suspension.

ABS, gear control, lighting control, air conditioning, airbags, central locking etc embedded in an automobile. Storage Area Network or SAN connects servers to data storage devices through a technology like Fibre Channel. A virtual private network or VPN is a special type of secured network used to provide a secure connection across a public network, such as an internet. Extranets typically use a VPN to provide a secure connection between a company and its known external users or offices.

TOPOLOGIES FOR A WIRELESS SENSOR NETWORK

While designing the network the designer has lot of choice for structuring the topologies in a WSN. Topologies of various types of single-hop and multi-hop communication are presented in Figure 1.

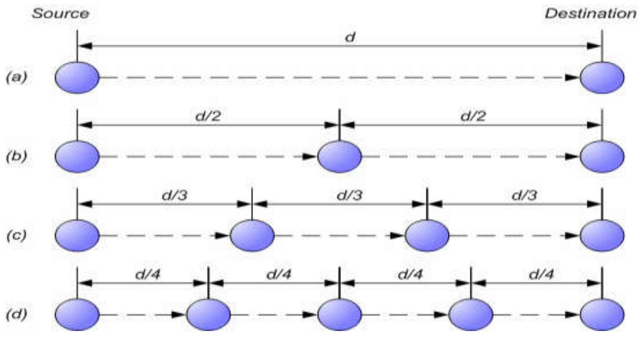

Figure1. Transmission distances for: (a) single-hop, (b) double-hop, (c) triple-hop, (d) quad-hop

Some destination could be reached with either large number of smaller hops (multi-hop) or small number of larger hops (single-hop).

A. Single hop star topology:

Single hop star topology is the simplest WSN topology. Every node communicates directly with the gateway or the data collector. The biggest limitation is the problem of scalability. The nodes that are at a large distance from the gateway will have poor quality connections with the gateway and the coverage area does not extend beyond the radio transmission range of around 30 meters in a building.

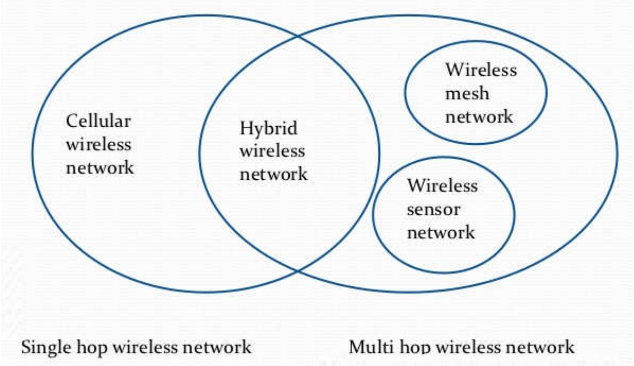
Cellular wireless network
Hybrid wireless network
Wireless mesh network
Wireless sensor network
Single hop wireless network
Multi hop wireless network

Figure2. Single hop and Multi hop wireless network.

B. Multi hop mesh and grid topology:

For covering large area, multi hop network is necessary. Here the signal goes from one sensor to the other until it reaches the gateway. The route of the signal is determined by a particular routing protocol depending upon whether the network is random or structured [1].

C. Two-tier hierarchical cluster topology:

The two-tier hierarchical cluster topology is most common architecture for larger WSNs. Here, the nodes within a specific region send their data to a local cluster head. In turn cluster heads from different regions send their collected data to the gateway. The biggest advantage is that it divides the whole network into a number of small zones within which routing of signals can be done locally.

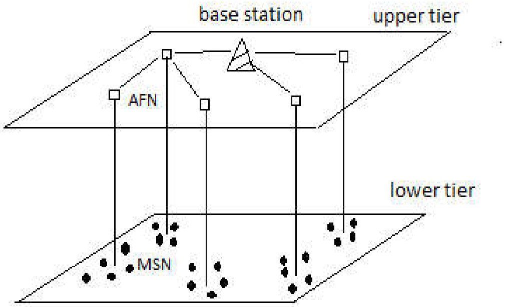

Figure 3. Two-tier Hierarchical structure

PARAMETERS FOR MEASURING THE EFFECTIVENESS OF A TOPOLOGY

A. Range and coverage:

Range is a requirement for a sensor network starting from the node to node range at a given transmission power / antenna gain and data rate, the main factors affecting are the quality and the efficiency of data transmission is through the network. The coverage requirements are eliminating dead spots in the network and the extent of coverage area in range.

B. Scalability:

Scalability is a characteristic of being able to cope up with network cells with few nodes to cells of tens of thousands of nodes as well as increasing the size of existing network by order of magnitude.

C. Expected Transmission Count (ETX):

It accounts for data loss due to medium access contention and environmental hazards and considers the number of transmissions needed to successfully transmit a packet over a link.

D. Hop Count:

The path having the minimum number of links between a given source and the destination node is hop count.

E. Power consumption/Network Longevity:

Network lifetime extension has been an important optimization objective. The position of nodes can affect the network lifetime significantly [1].

COMPONENTS OF WSN

The components of a wireless sensor network enable wireless connectivity within the network, connecting an application platform at one end of the network with one or more sensor or actuator devices in any part of the network. Finally, complete content and organizational editing before formatting. Please take note of the following items when proof reading spelling and grammar:

A. *Sensor Node*

A sensor is a device which senses the information and passes it on to mote. Sensors are typically used to measure the change in physical environmental parameters like temperature, pressure, humidity and sound.

B. *Base Station*

Different wireless sensor network are connected with base station. It consists of a microprocessor, antenna, radio board and USB interface board. For communication with wireless sensor nodes, Base station is preprogramed with low-power mesh networking software. As all the sensor nodes handover their data to base station so it is very important to deploy base station in wireless sensor network [2].

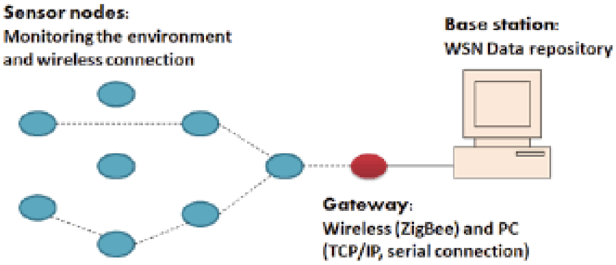
Sensor nodes:
Monitoring the environment and wireless connection
Base station:
WSN Data repository
Gateway:
Wireless (ZigBee) and PC (TCP/IP, serial connection)

Figure 4. WSN composed of sensor nodes, a base station and a remote server.

C. *Gateway*

A gateway is an interface between the application platform and the wireless nodes on the wireless sensor network. All information received from the wireless nodes is aggregated/manipulated (e.g. translation between network packet formats) by the gateway and forwarded to the application. That application may run on a local computer or a networked computer. In the reverse direction, when a command is issued by the application program to a wireless node, the gateway relays the information to the wireless sensor network. All gateways can perform protocol conversion to enable the wireless network to work with other industry or non-standard network protocols.

D. *Relay Node :*

Each relay node is considered a full-function device (FFD). They are usually called "routers," and they are used to extend network coverage area, route around obstacles and provide back-up routes in case of network congestion or device failure. In some cases, relay nodes may also be connected via analog and digital interfaces to sensors and actuators, providing the same I/O functionality of a leaf node. Base

E. *Leaf Node :*

A leaf node is considered as a reduced-function device (RFD). It is sometimes called endpoint. It is designed to provide the physical interface between the wireless sensor network and the sensor or actuator that it is wired to. Leaf nodes are usually equipped with one or more I/O connections for connecting to and communicating with analog or digital sensors or actuator devices.

F. *Sensor/Actuator :*

This is the device use for interaction with the physical system that you ultimately wish to monitor and/or control. An example is a sensor monitoring the temperature in a room and controlling the air-conditioned equipment [3].

NETWORK MODELS AND RELATED DEFINITIONS

Protocols are sets of standards that define operations and how they will be done. Without protocols there would be much confusion and there would be no standard to allow computers to communicate. Protocols are a set of defined reactions to given events. When a traffic light turns red, the defined reaction should be to stop. This is a simple form of a protocol.

Protocols are used for various purposes in the computer field. Protocols are mainly used to define networking standards although their application may extend beyond the scope of networking. Different uses of protocols include: Networking - There are different suites (or stacks) of networking protocols. The most popular include TCP/IP, IPX/XPX from Novell, NetBEUI/NetBIOS from Microsoft, AppleTalk, and SNA. Different protocols within each suite of protocols may perform different functions at different levels (see network levels in the next section). These protocols are listed by both layer and function in this documentation. The protocol stacks include:

TCP/IP
IPX/SPX
Microsoft
AppleTalk
SNA
Other - Includes OSI, DLC and SNAP.

The function of the network protocols include:

Packaging (IP)
Transport (TCP,UDP)
Network Management (ICMP, SNMP, ARP)
Host Management (RARP, BOOTP, DHCP)
Network Routing (BGP, EGP, IGP, RIP, OSPF)
Mail (SMTP)
Multicasting (IGMP)
Application (FTP, TFTP, NFS)
Security
Authentication
Encryption
Tunneling
Directory (LDAP)

Network models define a set of network layers and how they interact. The most important two are:

The TCP/IP Model - This model is sometimes called the DOD model since it was designed for the Department Of Defense. It is also called the internet model because TCP/IP is the protocol used on the internet.

OSI Network Model - The International Standards Organization (ISO) has defined a standard called the Open Systems Interconnection (OSI) reference model.

Many protocol stacks overlap the borders of the seven layer model by operating at multiple layers of the model. File Transport Protocol (FTP) and telnet both work at the application, presentation, and the session layers.

The Internet, TCP/IP, DOD Model - It has the following layers:

Link - Device driver and interface card which maps to the data link and physical layer of the OSI model. The layer corresponds to the hardware, including the device driver and interface card. The layer has data packets associated with it depending on the type of network being used such as ARCnet, Token ring or Ethernet.

Network - includes the IP, ICMP, and IGMP protocols. The network layer manages the movement of packets around. It is responsible for making sure that packages reach their destinations, and if they don't, reporting errors.

Transport - includes the TCP and UDP protocols. The transport layer is the mechanism used for two computers to exchange data with regards to software.

Application - Corresponds to the Session, Presentation and Application layers and includes FTP, Telnet, ping, Rlogin, rsh, TFTP, SMTP, SNMP, DNS, program written by user, etc. Note here to avoid confusion, that the application layer is generally referring to protocols such as FTP, telnet, ping, and other programs designed for specific purposes which are governed by a specific set of protocols defined with RFC's (Request For Comments). However a program that you may write can define its own data structure to send between your client and server program so long as the program you run on both the client and server machine understand your protocol.

A. Data Encapsulation,

When starting with protocols that work at the upper layers of the network models, each set of data is wrapped inside the next lower layer protocol, similar to wrapping letters inside an envelope. The application creates the data, then the transport layer wraps that data inside its format, then the network layer wraps the data, and finally the link (ethernet) layer encapsulates the data and transmits it. Each network layer either encapsulates the data stream with additional information, or manages data handling or come part of the connection.

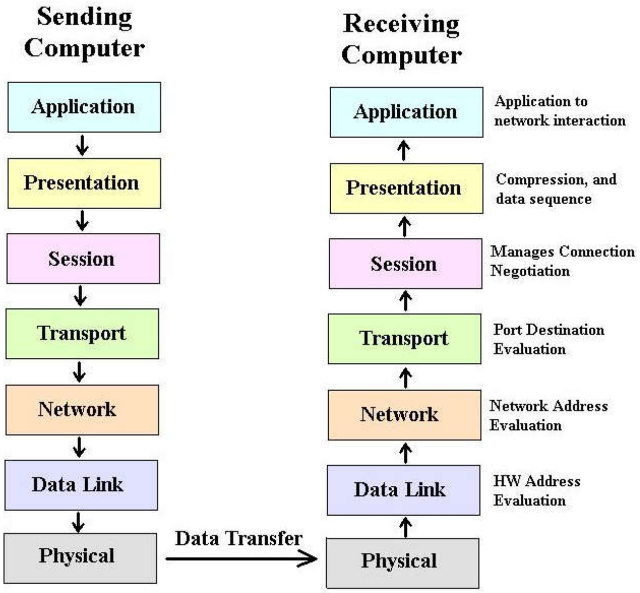

Figure 5. Network Layer Interaction

B. The OSI Network Model Standard

Each layer of a specific network model may be responsible for a different function of the network. Each layer will pass information up and down to the next subsequent layer as data is processed.

The OSI network model layers are arranged here from the lower levels starting with the physical (hardware) to the higher levels.

Physical Layer - The actual hardware.

Data Link Layer - Data transfer method (802x ethernet). Puts data in frames and ensures error free transmission. Also controls the timing of the network transmission. Adds frame type, address, and error control information. IEEE divided this layer into the two following sublayers.

Logical Link control (LLC) - Maintains the Link between two computers by establishing Service Access Points (SAPs) which are a series of interface points. IEEE 802.2.

Media Access Control (MAC) - Used to coordinate the sending of data between computers. The 802.3, 4, 5, and 12 standards apply to this layer. If you hear someone talking about the MAC address of a network card, they are referring to the hardware address of the card.

Network Layer - IP network protocol. Routes messages using the best path available.

Transport Layer - TCP, UDP. Ensures properly sequenced and error free transmission.

Session Layer - The user's interface to the network. Determines when the session is begun or opened, how long it is used, and when it is closed. Controls the transmission of data during the session. Supports security and name lookup enabling computers to locate each other.

Presentation Layer - ASCII or EBCDEC data syntax. Makes the type of data transparent to the layers around it. Used to translate date to computer specific format such as byte ordering. It may include compression. It prepares the data, either for the network or the application depending on the direction it is going.

Application Layer - Provides services software applications need. Provides the ability for user applications to interact with the network.

C. TCP/IP Networking Protocols

The TCP/IP suite of protocols is the set of protocols used to communicate across the internet. It is also widely used on many organizational networks due to its flexibility and wide array of functionality provided.

TCP/IP by Layer

Link Layer

SLIP - Serial Line Internet Protocol. This protocol places data packets into data frames in preparation for transport across network hardware media. This protocol is used for sending data across serial lines. There is no error correction, addressing or packet identification. There is no authentication or negotiation capabilities with SLIP. SLIP will only support transport of IP packets.

CSLIP - Compressed SLIP is essentially data compression of the SLIP protocol. It uses Van Jacobson compression to drastically reduce the overhead of packet overhead. This may also be used with PPP and called CPPP.

PPP - Point to Point Protocol is a form of serial line data encapsulation that is an improvement over SLIP which provides serial bi-directional communication. It is much like SLIP but can support AppleTalk, IPX, TCP/IP, and NetBEUI along with TCP/IP which is supported by SLIP. It can negotiate connection parameters such as speed along with the ability to support PAP and CHAP user authentication.

Ethernet - Ethernet is not really called a protocol. There are also many types of ethernet. The most common ethernet which is used to control the handling of data at the lowest layer of the network model is 802.3 ethernet. 802.3 ethernet provides a means of encapsulating data frames to be sent between computers. It specifies how network data collisions are handled along with hardware addressing of network cards.

Network Layer

ARP - Address Resolution Protocol enables the packaging of IP data into ethernet packages. It is the system and messaging protocol that is used to find the ethernet (hardware) address from a specific IP number. Without this protocol, the ethernet package could not be generated from the IP package, because the ethernet address could not be determined.

IP - Internet Protocol. Except for ARP and RARP all protocols' data packets will be packaged into an IP data packet. IP provides the mechanism to use software to address and manage data packets being sent to computers.

RARP - Reverse address resolution protocol is used to allow a computer without a local permanent data storage media to determine its IP address from its ethernet address.

Transport Layer

TCP - A reliable connection oriented protocol used to control the management of application level services between computers. It is used for transport by some applications.

UDP - An unreliable connection less protocol used to control the management of application level services between computers. It is used for transport by some applications which must provide their own reliability.

ICMP - Internet control message protocol (ICMP) provides management and error reporting to help manage the process of sending data between computers. (Management). This protocol is used to report connection status back to computers that are trying to connect other computers. For example, it may report that a destination host is not reachable.

IGMP - Internet Group Management Protocol used to support multicasting. IGMP messages are used by multicast routers to track group memberships on each of its networks.

Application Layer

FTP - File Transfer Protocol allows file transfer between two computers with login required.

TFTP - Trivial File Transfer Protocol allows file transfer between two computers with no login required. It is limited, and is intended for diskless stations.

NFS - Network File System is a protocol that allows UNIX and Linux systems remotely mount each other's file systems.

SNMP - Simple Network Management Protocol is used to manage all types of network elements based on various data sent and received.

SMTP - Simple Mail Transfer Protocol is used to transport mail. Simple Mail Transport Protocol is used on the internet, it is not a transport layer protocol but is an application layer protocol.

HTTP - Hypertext Transfer Protocol is used to transport HTML pages from web servers to web browsers. The protocol used to communicate between web servers and web browser software clients.

BOOTP - Bootstrap protocol is used to assign an IP address to diskless computers and tell it what server and file to load which will provide it with an operating system.

DHCP - Dynamic host configuration protocol is a method of assigning and controlling the IP addresses of computers on a given network. It is a server based service that automatically assigns IP numbers when a computer boots. This way the IP address of a computer does not need to be assigned manually. This makes changing networks easier to manage. DHCP can perform all the functions of BOOTP.

BGP - Border Gateway Protocol. When two systems are using BGP, they establish a TCP connection, then send each other their BGP routing tables. BGP uses distance vectoring. It detects failures by sending periodic keep alive messages to its neighbors every 30 seconds. It exchanges information about reachable networks with other BGP systems including the full path of systems that are between them. Described by RFC 1267, 1268, and 1497.

EGP - Exterior Gateway Protocol is used between routers of different systems.

IGP - Interior Gateway Protocol. The name used to describe the fact that each system on the internet can choose its own routing protocol. RIP and OSPF are interior gateway protocols.

RIP - Routing Information Protocol is used to dynamically update router tables on WANs or the internet. A distance-vector algorithm is used to calculate the best route for a packet. RFC 1058, 1388 (RIP2).

OSPF - Open Shortest Path First dynamic routing protocol. A link state protocol rather than a distance vector protocol. It tests the status of its link to each of its neighbors and sends the acquired information to them.

POP3 - Post Office Protocol version 3 is used by clients to access an internet mail server to get mail. It is not a transport layer protocol.

IMAP4 - Internet Mail Access Protocol version 4 is the replacement for POP3.

Telnet is used to remotely open a session on another computer. It relies on TCP for transport and is defined by RFC854.

Bandwidth Control

BAP - Bandwidth Allocation Protocol is a bandwidth control protocol for PPP connections. It works with BACP.

BACP - Bandwidth Allocation Control Protocol.

TCP/IP by Function

Packaging and Low Level

IP - Internet Protocol. Except for ARP and RARP all protocols' data packets will be packaged into an IP data packet. IP provides the mechanism to use software to address and manage data packets being sent to computers.

SLIP - Serial Line Internet Protocol. This protocol places data packets into data frames in preparation for transport across network hardware media. This protocol is used for sending data across serial lines. There is no error correction, addressing or packet identification. There is no authentication or negotiation capabilities with SLIP. SLIP will only support transport of IP packets.

CSLIP - Compressed SLIP is essentially data compression of the SLIP protocol. It uses Van Jacobson compression to drastically reduce the overhead of packet overhead. This may also be used with PPP and called CPPP.

PPP - Point to Point Protocol is a form of serial line data encapsulation that is an improvement over SLIP which provides serial bi-directional communication. It is much like SLIP but can support AppleTalk, IPX, TCP/IP, and NetBEUI along with TCP/IP which is supported by SLIP. It can negotiate connection parameters such as speed along with the ability to support PAP and CHAP user authentication.

Ethernet - Ethernet is not really called a protocol. There are also many types of ethernet. The most common ethernet which is used to control the handling of data at the lowest layer of the network model is 802.3 ethernet. 802.3 ethernet provides a means of encapsulating data frames to be sent between computers. It specifies how network data collisions are handled along with hardware addressing of network cards.

Transport and Basic Functions

TCP - A reliable connection oriented protocol used to control the management of application level services between computers. It is used for transport by some applications.

UDP - An unreliable connection less protocol used to control the management of application level services between computers. It is used for transport by some applications which must provide their own reliability.

Network Management

SNMP - Simple Network Management Protocol is used to manage all types of network elements based on various data sent and received.

ICMP - Internet control message protocol provides management and error reporting to help manage the process of sending data between computers. (Management). This protocol is used to report connection status back to computers that are trying to connect other computers. For example, it may report that a destination host is not reachable. This protocol is required for basic TCP/IP operations.

ARP - Address Resolution Protocol enables the packaging of IP data into ethernet packages. It is the system and messaging protocol that is used to find the ethernet (hardware) address from a specific IP number. Without this protocol, the ethernet package could not be generated from the IP package, because the ethernet address could not be determined. Protocol is used to report connection status back to computers that are trying to connect other computers. For example, it may report that a destination host is not reachable. This protocol is required for basic TCP/IP operations.

Host Management

BOOTP - Bootstrap protocol is used to assign an IP address to diskless computers and tell it what server and file to load which will provide it with an operating system.

DHCP - Dynamic host configuration protocol is a method of assigning and controlling the IP addresses of computers on a given network. It is a server based service that automatically assigns IP numbers when a computer boots. This way the IP address of a computer does not need to be assigned manually. This makes changing networks easier to manage. DHCP can perform all the functions of BOOTP.

RARP - Reverse address resolution protocol is used to allow a computer without a local permanent data storage media to determine its IP address from its ethernet address.

Mail Protocols

SMTP - Simple Mail Transfer Protocol is used to transport mail. Simple Mail Transport Protocol is used on the internet, it is not a transport layer protocol but is an application layer protocol.

POP3 - Post Office Protocol version 3 is used by clients to access an internet mail server to get mail. It is not a transport layer protocol.

IMAP4 - Internet Mail Access Protocol version 4 is the replacement for POP3.

Multicasting Protocols

IGMP - Internet Group Management Protocol used to support multicasting. IGMP messages are used by multicast routers to track group memberships on each of its networks.

Routing Protocols

BGP - Border Gateway Protocol. When two systems are using BGP, they establish a TCP connection, then send each other their BGP routing tables. BGP uses distance vectoring. It detects failures by sending periodic keep alive messages to its neighbors every 30 seconds. It exchanges information about reachable networks with other BGP systems including the full path of systems that are between them. Described by RFC 1267, 1268, and 1497

EGP - Exterior Gateway Protocol is used between routers of different systems.

IGP - Interior Gateway Protocol. The name used to describe the fact that each system on the internet can choose its own routing protocol. RIP and OSPF are interior gateway protocols.

RIP - Routing Information Protocol is used to dynamically update router tables on WANs or the internet.

OSPF - Open Shortest Path First dynamic routing protocol. A link state protocol rather than a distance vector protocol. It tests the status of its link to each of its neighbors and sends the acquired information to them.

IPX/SPX Protocols

IPX/SPX is a routable protocol and can be used for small and large networks. It was created by Novell primarily for Novell NetWare networks, but is popular enough that it is used on products that are not from Novell.

NCP - NetWare Core Protocol provides for client/server interactions such as file and print sharing. It works at the application, presentation, and session levels.

SAP - Service Advertising Protocol packets are used by file and print servers to periodically advertise the address of the server and the services available. It works at the application, presentation, and session levels.

SPX - Sequenced Packet Exchange operates at the transport layer providing connection oriented communication on top of IPX.

IPX - Internetwork Packet Exchange supports the transport and network layers of the OSI network model provides for network addressing and routing. It provides fast, unreliable, communication with network nodes using a connection less datagram service.

Network Level	Protocols
Application	NCP SAP
Presentation	
Session	
Transport	IPX SPX
Network	
Data Link	NDIS/NIC drivers

Figure 6. IPX/SPX Protocols

Other Network Support

ODI - Open Data-link Interface operates at the data link layer allowing IPX to work with any network interface card

RIP - Routing Information Protocol is the default routing protocol for IPX/SPX networks which operates at the network layer. A distance-vector algorithm is used to calculate the best route for a packet.

MHS - Message Handling Service by Novell is used for mail on Netware networks [9].

D. AppleTalk Networking Protocols

Apple Computers have had their own set of protocols for many years. More and more operating systems today now can communicate with Apple systems using Apple networking protocols.

ADSP - AppleTalk Data Stream Protocol is used to provide data stream service for sockets. The data stream is full duplex meaning communication may be sent both directions at the same time works at the OSI network model session layer.

AEP - AppleTalk echo protocol uses echoes to tell if a computer, or node, is available. It also measures the time it takes for etches to travel from the source computer (node) to the destination and back works at the OSI network model transport layer.

AFP - AppleTalk Filing protocol makes network files appear local by managing file sharing at the presentation layer. This protocol is build to top of ASP. AFP supports communication between different types of computers. Works at the OSI network model application and presentation layers.

AppleShare - Works at the application layer to provide services.

ARUP - AppleTalk update routing is a newer version of RTMP.

ASP - AppleTalk Session Protocol opens, maintains, and closes transactions during a session, while ADSP provides a full-duplex, byte-stream service between any two sockets on an AppleTalk Internet works at the OSI network model session layer.

ATP - AppleTalk Transaction Protocol provides a Transport Layer connection between computers. This protocol guarantees reliability by directing the transaction process and binding the request and response works at the OSI network model transport layer.

DDP - Datagram Delivery Protocol is a routable protocol that provides for data packet (datagram) transportation. It operates at the network layer of the OSI network model which is the same level the IP protocol in TCP/IP operates at works at the OSI network model network layer.

LAP - Link-Access Protocol is a set of data link layer protocols that support LocalTalk (LLAP), EtherTalk (ELAP), TokenTalk (TLAP), and FDDITalk. The LAP manager determines which LAP to connect for the correct upper level protocol.

NBP - Name-binding protocol translates addresses into user friendly three part names works at the OSI network model transport layer.

PAP - Printer Access Protocol is a connection oriented service for managing information between workstations and printers. It is used to send print requests to printers.

RTMP - Routing Table Maintenance Protocol is used to update routers with information about network status and address tables. The whole address table is sent across the network. This protocol sends its information as broadcasts across the network every 10 seconds works at the OSI network model transport layer.

ZIP - Zone Information Protocol is used by AppleTalk routers co create a Zone Information Table (ZIT). The ZIT has a list of zone names which are associated with network numbers. This list is displayed in the Apple System's file chooser works at the OSI network model session layer.

Network Level	**Protocols**			
Application	AFP	AppleShare		
Presentation				
Session	ADSP	ASP	ZIP	
Transport	AEP	ATP	NBP	RTMP
Network	DDP			
Data Link	LAP protocols			

Figure 7. AppleTalk Networking Protocols

E. SNA Networking Protocols

System Network Architecture (SNA) by IBM is a suite of protocols mainly used with IBM mainframe and AS/400 computers.

APPC - Advanced Peer-to-Peer Communications provides peer to peer services at the transport and session layer. Part of the System Network Architecture (SNA) suite of protocols.

APPN - Advanced Peer-to-Peer networking supports the computer connections at the network and transport layers. Part of the System Network Architecture (SNA) suite of protocols.

F. Other Protocols

DLC - Data Link Control. This protocol operates at the data link layer and is designed for communications between Hewlett-Packard network printers and IBM mainframe computers. This protocol is not routable.

OSI - Open Systems Interconnect. A suite of protocols developed by the International Standards Organization (ISO) which corresponds with the layers of the OSI model. These protocols provide a number of application protocols for various functions. The OSI protocol stack may be used to connect large systems. OSI is a routable transport protocol.

Mail Protocols

MIME - Multipurpose Internet Mail Extension is the protocol that defines the way files are attached to SMTP messages.

X.400 - International Telecommunication Union standard defines transfer protocols for sending mail between mail servers.Directory Protocols

LDAP - Lightweight Directory Access Protocol is a standard for directory services with additional features that enhance its capabilities being added. LDAP may allow for consolidation of directory lists to be consolidated. An LDAP server provides the directory services and other LDAP functions.

X.500 - This is a recommendation outlining how an organization can share objects and names on a large network. It is hierarchical similar to DNS, defining domains consisting of organizations, divisions, departments, and workgroups. The domains provide information about the users and available resources on that domain, This X.500 system is like a directory. Its recommendation comes from the International Telegraph and Telephone Consultative Committee (CCITT).

G. Microsoft Protocols

Microsoft developed a suite of protocols around NetBIOS using NetBEUI for transport. The primary advantage of this protocol is that it is easy to configure and Microsoft claims that it runs faster. Microsoft has been switching to a wider use of TCP/IP in recent years, probably in support of larger organizational networks.

NetBIOS - Network Basic Input / Output allows browsing of network resources and handles basic functions of a Windows network. Two way acknowledged data transfer is used. It is a Microsoft protocol used to support Microsoft Networking. Works at the session layer. Controls the sessions between computers and maintains connections.

NetBEUI - NetBIOS Extended User Interface. Microsoft Protocol used to support Microsoft Networking. Provides data transportation. It is not a routable transport protocol which is why NBT exists on large networks to use routable TCP protocol on large networks. This protocol may sometimes be called the NetBIOS frame (NBF) protocol. Works at the Transport and Network layers. NetBEUI - The main protocol used for networking in the windows environment. NetBIOS Extended User Interface works at the transport layer and provides data transportation. It is not a routable transport protocol[9].

SMB - Microsoft Protocol used to support Microsoft Networking by providing redirector client to server communication. Works at the presentation layer.

Network Level	Protocols
Application	Redirector
Presentation	SMB
Session	NetBIOS
Transport	NetBEUI
Network	
Data Link	NDIS/NIC drivers

Figure 8. Microsoft Protocols

Other Network Support

NBT - NetBIOS over TCP/IP refers to NetBIOS being transported by TCP/IP rather than NetBEUI defined by RFC 1002.

Redirector - Directs requests for network resources to the appropriate server and makes network resources seem to be local resources.

NDIS and NIC driver - NDIS allows several adapter drivers to use any number of transport protocols. The NIC driver is the driver software for the network card.

H. Authentication Protocols

Authentication protocols are listed and described below.

CHAP - Challenge Handshake Authentication Protocol is a three way handshake protocol which is considered more secure than PAP.

EAP - Extensible Authentication Protocol is used between a dial-in client and server to determine what authentication protocol will be used.

PAP - Password Authentication Protocol is a two way handshake protocol designed for use with PPP. Authentication Protocol Password Authentication Protocol is a plain text password used on older SLIP systems. It is not secure.

SPAP - Shiva PAP. Only NT RAS server supports this for clients dialing in.

DES - Data Encryption Standard for older clients and servers.

RADIUS - Remote Authentication Dial-In User Service used to authenticate users dialing in remotely to servers in an organization's network.

S/Key - A onetime password system, secure against replays RFC 2289.

TACACS - Offers authentication, accounting, and authorization.

MS-CHAP (MD4) - Uses a Microsoft version of RSA message digest 4 challenge and reply protocol. It only works on Microsoft systems and enables data encryption. Selecting this authentication method causes all data to be encrypted.

SKID - SKID2 and SKID3 are vulnerable to a man in the middle attack.

I. Encryption Protocols

Encryption protocols are listed and described below.

CIPE - Crypto IP Encapsulation.

SSL - Secure sockets layer.

J. Tunneling Protocols

IPIP tunneling - Tunneling IP packets in IP packets.

IPSec - Internet protocol security, developed by IETF, implemented at layer 3. it is a collection of security measures that address data privacy, integrity, authentication, and key management, in addition to tunneling does not cover key management.

L2F - Layer2 Forwarding, works at the link layer of the OSI model. It has no encryption. It is being replaced by L2TP.

L2TP - Layer2 Tunneling Protocol. (RFC 2661) Combines features of L2F and PPTP and works at the link layer. No encryption or key management is included in specifications. It uses IPSec for encryption.

PPTP - Point-to-Point Tunneling Protocol (RFC 2637) works at the link layer. No encryption or key management included in specifications. A VPN tunneling Protocol used to send secure communications from point to point.

Socks - handled at the application layer.

CONCLUSION

A wireless sensor network enable various parameters to analyze the network with hop count, longevity, ETX etc. Wwireless connectivity within the network can be understood by the components in WSN along with the topology used for connectivity. The protocols of the OSI layer used in WSN plays an important role about its functionality while connecting the base station with the hop count etc. One needs to understand the functions of a network like tcp or udp etc. Based on the function of the network, protocols can be understood and worked on at a particular layer of the network.

References

[1] *Gurwinder Kaur 1 and Rachit Mohan Garg 2 "ENERGY EFFICIENT TOPOLOGIES FOR WIRELESS SENSOR NETWORKS," DOI: 10.5121/IJDPS.2012.3516*

[2] *Yogesh Kumar Fulara, "SOME ASPECTS OF WIRELESS SENSOR NETWORKS," DOI : 10.5121/ijans.2015.5102.*

[3] *J. Cecílio, P. Furtado, Wireless Sensors in Heterogeneous Networked Systems, Computer Communications and Networks, DOI 10.1007/978-3-319-09280-5_2 © Springer International Publishing Switzerland 2014.*

[4] *K. Elissa, "Title of paper if known," unpublished.*

[5] *R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.*

[6] *Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740-741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].*

[7] *M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.*

[8] *Christoph Lenzen, Roger Wattenhofer, "Distributed Algorithms for Sensor Networks",*

[9] *http://www.comptechdoc.org/independent/networking/*