ABC Journals
A new domain in research publishing

Engineering International

EI

www.j-ei.us

Asian Business Consortium

ABC Research House

A Survey on Wireless Sensor Networks Architectural Model, Topology, Service and Security

Tamim Al Mahmud

Department of Computer Science and Engineering, Patuakhali Science and Technology University, Bangladesh

ABSTRACT

Recent advancement and grown up technologies has enabled the development and implementation of low-cost, energy efficient and versatile sensor networks. Sensor networks are built up with sensors that have the ability to sense fiscal or environmental property. Assumption can be made that Wireless Sensing Network (WSN) is able to sense environmental conditions at Nano and gaseous level. In this paper, first the system architecture of WSN is described. The network may maintain several architectural protocol and topologies. WSN provides some services which are maintained by layered architecture. Another important issue regarding wireless networking is the security challenges. This work guided to a concept of several security issues and discussion to overcome the challenging issues.

Keywords — Wireless Sensing Network (WSN), Network architecture, Network topology, Nano sensing nodes, WSN Services, Security and challenges.

1 INTRODUCTION

Wireless sensor network has increasingly become a research hotspot as the technology of wireless networks become gradually matured and supported by small, micro-mobile devices. WSN consists of several number of sensor nodes ranging from few tens to thousands and base station or sink node. Each node is capable of storing, processing and relaying the data that are sensed. Base station is responsible for further computation of the data. It has very spread application in many areas, such as in environmental monitoring in the military and national defence, biomedical, remote monitoring dangerous areas and so on. There are several types of traditional network topology namely peer to peer, star, tree and Mesh for development and deployment of wireless sensor networks (WSN).But these topologies are not efficient for making data transmission more reliable and efficient because of limited energy and construction limitation of nodes. In this paper we proposed a dynamic topology for WSN for better performance. Our research is focused on integration of wireless sensor networks into existing networks, mainly mobile ones, and stipulation of sensor based and/or enhanced services to remote users. Therefore, we have been working one signing an architecture that utilizes the existing infrastructure to interconnect independent wireless sensor networks and to provide data aggregation and actuator control services Sensor networks by distributed wireless technology are involved in various types of applications. Some of WSN applications

work without security which decreased Quality of Service (QoS) that caused by resource restriction. In WSN, a mass of wireless sensors are linked together via RF. The quality of working properly of the nodes in WSN application consists of comprehension, gathering and distributing information in the network. Energy is a main issue as the sensors are in general tiny. In addition wireless with restricted memory and quality of working properly given the fact that the batteries have a restricted governing power. Different types of Denial of Services attacks can affect a network or node. If attacked node continues to exchange information or ideas with its neighbours and it led to diminish all its power then the node declares as a dead node which is worst cases.

2 ARCHITECTURAL MODE

Wireless sensor network (WSN) defines to a collection of spatially autonomous sensors whose purpose is to monitor and record the fiscal situation of the external environment and organize the data at a central location. The environmental conditions that are determined by WSN are temperature, pollution levels, humidity, breeze speed and path, pressure, etc.
The WSN is consist of automatic nodes ranging from a few to several hundreds or even thousands, where one or more sensor connected to each of the node
Each of the network nodes consist of following component:

Radio transceiver: Those have connection to some internal or external antenna.
Microcontroller: A Small processing unit that interface with the sensor and an energy source, usually an alkaline battery.
Mobilizer: That helps to move the sensor node from present position and carry out defined action. The base station requires exact location of the network node which is done by location finding system because the sensor may be mobile. The size of a single sensor node can vary from shoebox-sized nodes down to devices the size of grain of dust. (Automatic WSN).

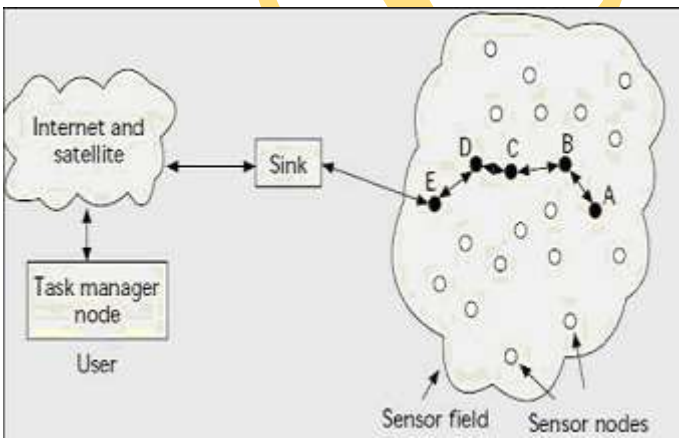


Figure: Basic Architecture of Wireless Sensor Network.

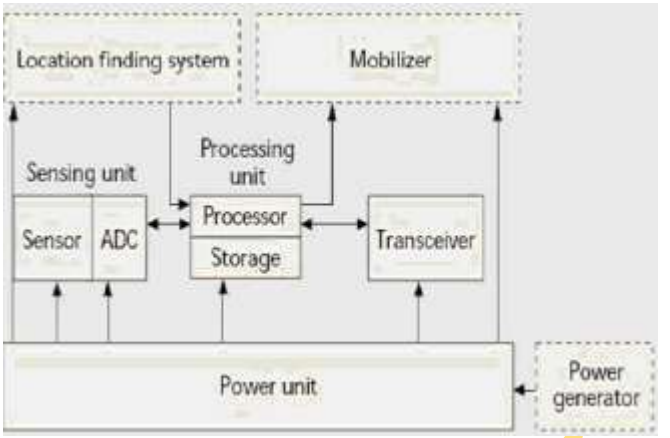


Figure 3. Components of a Sensor Node

3 TOPOLOGY

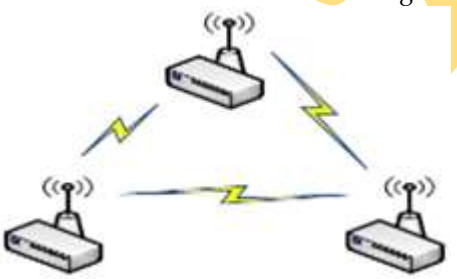
In communication networks, topology refers to the description of arrangement of network nodes and the communication link among nodes.
There are four basic WSN topologies as follows:

A. Peer to Peer
B. Star
C. Tree and
D. Mesh

We here simply discuss these four types of topologies.

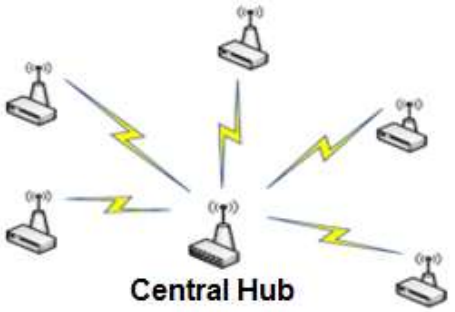
A. Peer-to-Peer

Networks allow communication among nodes without aid of central communication hub. It provides communication among network nodes directly. The two communicating nodes can act as client and server interchangeably.



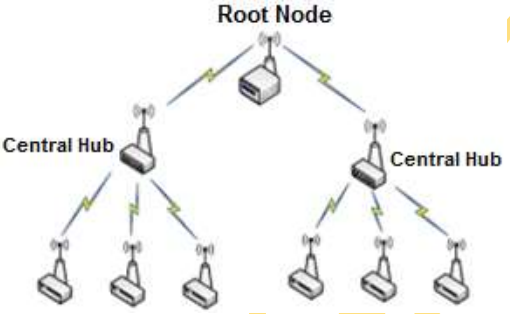
B. Star networks

Allow communication through a central communications hub without direct communication with one another. Centralized hub is responsible for all communication among nodes of the WSN. In this network topology hub acts as a server while nodes perform action as a client.



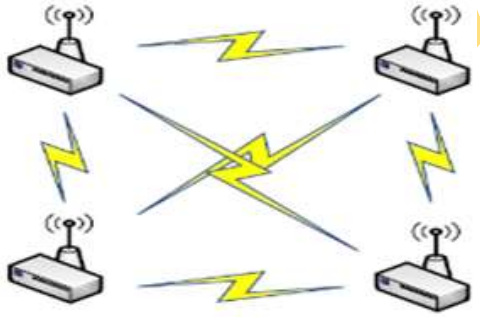
C. Tree networks

Are a combination of Star network and Peer to Peer network. It uses a central hub that refers to the Root node of the network. Next level from the Root node is the h Central hub that constructs the Star topology.



D. Mesh networks

Is the most complex type of network that provides node to node transfer of data to make successful transmission. The network to be self-healing it must maintain these properties. Data routed from node to node until it reaches its destination node.



4 WHY DYNAMIC TOPOLOGY

Wireless Sensor nodes are energy constraint device. It consumes more power and energy in each transmission. So we must interconnect the network nodes in such a way that consumes less power and energy. If we use the above network topologies then nodes can't efficiently transmit data due their limited energy. So we now propose Dynamic topology that provide energy efficient data transmission.

5 PROPOSED DYNAMIC TOPOLOGY

We proposed that there will be a central node and some supporting node same to the central node whose energy, transmitting power, efficiency all are same to the central node and greater than other sensing nodes.

At particular time a particular node will active and collecting sensing node information. After activating for a particular time it may transmit signal to the router and continuously losing its energy. A mechanism is provided after each transmission at central node to check their energy level .Nodes is randomly hand over the mechanism of selecting route this process node .Repeating until all the nodes are damage or transmit information

Then all other nodes are constructing a tree topology with the selecting central node. After selecting central node all other node are construct tree topology with the central node (fig 5).

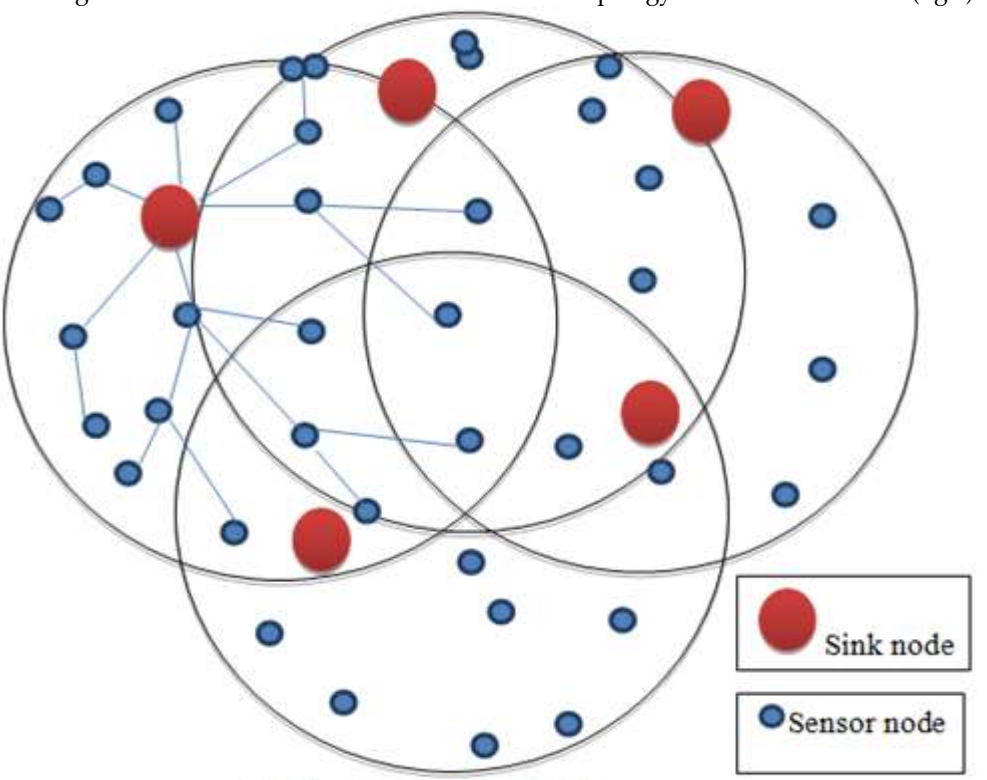


Fig5: Tree topology based on our thinking

The nodes are transmitting information to the central node and it transmits to the router. Sensing node transmit signal to the root node. The root node covers an area supporting by its sensor node. Once the root will damage which serve for transmitting the enter network is not disconnected yet. But root node automatically hand over its mechanism to the other root node which will inactive/sleep moment before and collect/gather information coming from sensing node. Sensing node connect/communicate with each other by knowing its neighbour .The discovery of the neighbour nodes (parent and children) is done by the exchange of advertisement control messages (ADVERT). The first node that starts sending advertisement messages is the sink node (root node describe above). The advertisements are broadcast messages that advertise specific children tree positions. The

advertisements are sent in the downstream slot of the epoch. When a node (not the sink) is firstly switched on it initialize during the first epoch and sets all the slots of the node in"scan mode" so that to receive advertisements.

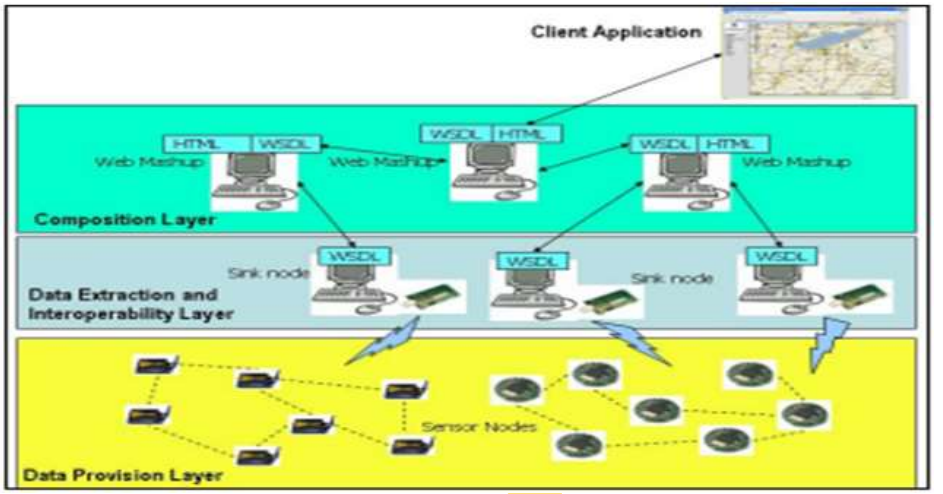
6 WSN AS A SERVICE

WSN mainly provide two types of Services as follows:
Information Provider: Wireless sensor network is first of all provide service as a sensor information provider that offers some fixed sensor information defined by the type of available sensor in the network.
Actuation Services: Each WSN provides actuation service that performs some computation or action on the data collected by the sensor and produced the desired output
WSN can be classified in two types based on class of target application that uses the services provided by WSN as follows:
Proactive: Sensor nodes sporadically sense the surroundings and transmit engrossed data to the application.
Reactive: Sensor nodes react to sudden change in the network immediately.

7 ARCHITECTURE OF WSN AS A SERVICE

Here we propose a WSN architecture that acts as service provides. It consist of four layer namely
Layer 1: Data Provision Layer
Layer 2: Data Extraction and Interoperability Layer
Layer 3: Composition Layer
Layer 4: Application Layer

Data Provision Layer:
Data provision layer composed of sensor nodes of the network. These nodes are responsible for sensing the external environment and collecting information about surroundings. Sensor nodes can perform only few operations on the sensed information like computation of average, maximum, minimum, etc
Data Extraction and Interoperability Layer:
This layer consists of sink node which has high energy than sensor node of the low layer. Data collected by multiple sensor nodes of different WSN of the previous layer are extracted in this layer for further operation. It also provides a common interface for accessing the information.
Composition Layer:
This layer consists of Web Mishaps. Data extracted from different WSN by previous layer are combined by this layer and provides value-added services to the client application. This layer collects data from previous layer through the use of common interface.
Application Layer:
Application layer is consisting of client application that use the services provided by WSN. It can perform additional computation to these services for efficient and better performance.



8 SECURITY

Attack and Attacker: an attempt to get illegal access to information, services defined as Attacks. Attacks are produced by attackers. They are also known as introducers.
There are mainly two board types of attacks
Active attack Attacker try to modify or falsify the data transmitted through network. This attack is easily notified.
Passive attack Attacker only observes the data without any modification or falsification of data. It is more dangerous than active attack because it is not so easy to detect.

9 ATTACKS IN WIRELESS SENSOR NETWORKS

Denial of Service: In WSN, a denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is defined as an attempt to provide a resist to access machine or network resource by intended user making these machine or network resources unavailable. In WSN, various kinds of DoS attacks performed in distinct layers. At physical layer the Denial-of-service attacks could be tampering and jamming, at data link layer, collision, unfairness, at network layer, homing, misdirection, black holes and at transport layer this attack can be done by DE synchronization malicious flooding. The techniques to protect DoS attacks include pushback, payment for network resources, identification of traffic, strong authentication.

Attacks on Information in transit : In WSN, sensors monitor the Changes of specific or values or parameters are monitored by sensors and inform to the sink node in according to the requirement. The information in transit may be spoofed, altered, or vanished, replayed again while sensor sending the report. As wireless sensor communication is attack to eavesdropping, attacker can monitor the traffic flow and get into action to intercept, interrupt, modify or fabricate [22] packets thus, provide false information to the sinks nodes. Since sensor nodes normally have a short range of communication and limited resource, an attacker with greater processing power and larger transmission range can attack several sensors nodes.

Sybil Attack: In most cases, the sensors node in a wireless sensor network might require to work together to complete a task, hence attackers can use distribution of sub-task and

redundancy of information. In such a situation, a node can claim to be two or more node using the identities of other authorized nodes (Figure 1).In this attack where such a node counterfeit the identities of two or more node is the Sybil attack [23], [24]

Black hole/Sinkhole Attack: By this attack, a spiteful node acts as a black hole [25] to attract all the traffic in the sensor network. In a flooding based protocol, for routing the attacker listens to requests then replies to the target nodes in which it contains the greater quality or shortest path to the base station.

Hello Flood Attack: This kind of attack uses HELLO packets as a keyword to persuade the sensors in Wireless Sensor Network. In this kind of attack an attacker with a high radio communication (termed as a laptop-class attacker in [26]) range and processing power sends HELLO packets to several number of sensor nodes which are spread in a large area within a Wireless Sensor Network. The sensors are therefore convinced that the adversary is their neighbor. Accordingly, while transfer the information to the sink node or base station, the attack nodes try to go through the attacker as they learn that it is their neighbor and are ultimately spoofed by the attacker.

Wormhole Attack: Wormhole attack [27] is a critical attack in which the attacker records the packets (or bits) at one location in the network and tunnels those to another position. The tunneling or re-broadcasting of bits could be done selectively. Wormhole attack is an important threat to WSN, because; this sort of attack does not need mutual agreement a sensor node in the WSN rather, it could be accomplished even at the initial phase when the sensors begin to invent the neighboring information.

Network Security Services: Network security can provide one of the five services as shown in Figure. These four network security services are related to the message exchanged using the network: message confidentiality, no repudiation, authentication integrity. Authentication or identification is provided by these services.

Message Confidentiality: Message confidentiality or privacy means that the sender and the receiver expect confidentiality. The intended receiver is sensed by message which is transmitted. To all others, the message must be garbage. When a customer communicates with his/her bank, she expects that the communication is totally confidential.

Message Integrity: Message integrity means that the data must arrive at the receiver exactly as they were sent. There must be no hangs during the transmission, neither accidentally or maliciously. As more and more monetary exchanges occur over the Internet, integrity is crucial. For example, it would be disastrous if a request for transferring $100 changed to a request for $10,000 or $100,000. The integrity of the message must be preserved in a secure communication.

Message Authentication: Message authentication is a service beyond message integrity. In message authentication the receiver needs to be sure of the sender's identity and that an imposter has not sent the message.

Message No repudiation: Message no repudiation means that a sender must not be able to deny sending a message that is send. The receiver is responsible for proof. For example, when a client sends a message to exchange money from one account to another account, the bank must have proof that the customer actually requested this transaction.

Entity Authentication: In entity authentication (or user identification) the entity or user is verified prior to access to the resource of system (files, for example). For example, an employee who needs to access her university resources needs to be authenticated during the logging process. This is to protect the interests of the university and the employee.

10 CONCLUSIONS

Wireless Sensor Networks have great impact on every spheres of life beginning from healthcare ending to the homeland security. Environmental protection is also a great use. In this paper we have discussed about the core concepts of Wireless Sensor Network (WSN). This paper also provides knowledge about wireless Sensing Nodes and the network architecture which follows different topologies to form an efficient network in a nutshell. As the security challenges are great issues, this paper also serves a basic idea with respect to network security. Wireless Sensing Networks have enormous services that are also described in this paper. Further research is to be considered to build up other network performance and its criteria such as service quality issues with high energy efficiency and integrated security.

REFERENCES

FLEXChip Signal Processor (MC68175/D), Motorola, 1996.

J. Breckling, Ed., *The Analysis of Directional Time Series: Applications to Wind Speed and Direction*, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.

J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.

Karnik, "Performance of TCP congestion control with rate feedback: TCP/ABR and rate adaptive TCP/IP," M. Eng. thesis, Indian Institute of Science, Bangalore, India, Jan. 1999.

M. Shell. (2002) IEEEtran homepage on CTAN. [Online]. Available: http://www.ctan.org/tex-archive/macros/latex/contrib/supported/IEEEtran/

M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in *Proc. ECOC'00*, 2000, paper 11.3.4, p. 109.

R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, "High-speed digital-to-RF converter," U.S. Patent 5 668 842, Sept. 16, 1997.

S. M. Metev and V. P. Veiko, *Laser Assisted Microtechnology*, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," *IEEE Electron Device Lett.*, vol. 20, pp. 569–571, Nov. 1999.

Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997.