International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 10 | Oct -2016 www.irjet.net p-ISSN: 2395-0072

# Wireless Sensor Networks- An Overview, Challenges and Solutions to overcome challenges.

SNEHAPIRIYA TLK

*Electronics And Communication Engineering*

*Rajalakshmi Engineering College*

*Chennai, Tamilnadu*

---

**Abstract -** *Wireless sensor networks (WSN), are otherwise called as wireless sensor and actuator networks (WSAN) are spatially distributed sensors which are capable of monitoring physical or environmental condition and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance and disaster relief operations as witnessed in recent floods in Chennai ; Also such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, smart homes, intelligent buildings( Monitoring proper ventilation, checking for earthquake stresses around the vicinity) and so on. These sensors are used in disseminating information to different required clients.*

***Key Words***: **wireless networks, sensors, applications**

## 1.INTRODUCTION

Before analyzing the challenges imposed on these networks systems, it is very essential to understand their characteristics and features. The WSN is built of nodes ; from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Sensors might vary in size from that of a giant box and range down to the size of a grain of particle or dust. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from star type to an integrated mesh type. The propagation technique established between the hops of the network can be routing type or flooding

### 1.1 Essential Characteristics:

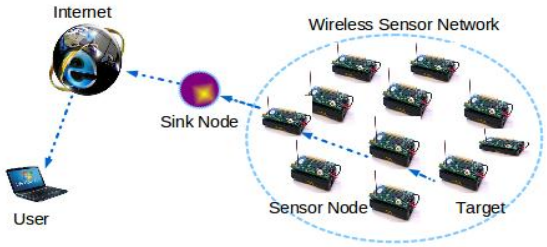
- Cross Layer Design
- Ease of Use
- Scalability- large scale deployment
- Power Consumption
- Mobility of Nodes
- Coping up with harsh environmental changes

Challenges using Traditional Layered approach:

1. Traditional layered approach cannot share different information among different layers and leads to each layer not having complete information. The traditional layered approach also, will not guarantee the optimization of the entire network.
2. This approach does not have the ability to adapt to the environmental change.
3. Due to the interference between the different users, access conflicts, fading, and the change of environment in the wireless sensor networks, traditional layered approach for wired networks is not applicable to wireless networks and thus is not feasible.

Importance of Cross Layer Designing in WSN'S:

Cross-layer optimization is an escape from the pure concept of models taught by OSI communication which consists of virtually strict boundaries between layers. The cross layer approach transports feedback dynamically via the layer boundaries to enable the compensation for .g. overload, latency or other mismatch of requirements and resources by any control input to another layer but that layer directly affected by the detected deficiency.




## 1.2 PARAMETERS FOR THE DESIGN OF A WSN

**Software**- Energy is the essential factor which will determine the life time of WSN nodes. We are aware that WSNs may be deployed in huge numbers in eclectic environments, including remote and hostile regions, where ad hoc communications are a key component. Thus for this reason, algorithms and protocols need to address the following issues:

- Increased lifespan
- Robustness and fault tolerance
- Self-configuration

**To enhance lifetime maximization:**

Energy/Power Consumption of the sensing device must be minimized and sensor nodes should be energy efficient since their limited energy resource determines their lifetime. To conserve power, wireless sensor nodes normally would power off both the radio transmitter and the radio receiver when not in use.

**Operating systems** for wireless sensor network nodes are typically less complex than general-purpose operating systems. They more strongly resemble embedded systems, for two reasons.

- Wireless sensor networks are typically deployed with a particular application in mind, rather than as a general platform.

Next, a need for low costs and low power leads most wireless sensor nodes to have low-power microcontrollers. Thus ensuring that mechanisms such as virtual memory are either unnecessary or too expensive to implement.

## 2. CHOICE OF TECHNOLOGY TO IMPLEMENT WSN'S

Recent technological advances have enabled delivery of the features like, data reliability, low latency in and less power changes pertaining to battery life etc in many markets. Several Technologies present are,

- Satellite, Cellular, Wi-Fi and other IEEE standards which help design WSN networks over a long run.

LIMITATIONS OF THESE TECHNOLOGIES:

Satellite and cellular work well for many applications, but they have the highest energy cost per packet. Data plan charges can also be prohibitive, although this is likely to change as carriers develop billing models appropriate for relatively sparse data flow.

Also to mention, it would be difficult for a satellite or cell phone (i.e., usage of cellular technology) signal to make its way out of a heavily obstructed structure, and the sensors generally do not have the capability of moving from side to side
Consider an application of sending information at a very low data rate (i.e., one data packet per day) with good connectivity; in that case satellite or cellular technology would actually make a lot of sense.

**ALTERNATIVE TECHNOLOGY SOLUTION**

- Wi Fi (IEEE 802.11b, g) sensors are now very widely available. The energy cost for a Wi-Fi packet is much lower than cellular technology costs incurred, and there are no recurring fees for data. Connectivity and coverage remain important concerns, as the density of access points necessary for reliable communication with a fixed sensor is typically higher than that necessary for mobile humans with gadgets.

With reference to the OSI layer model, the 802.15.4 standard defines a physical layer (PHY) and medium access control (MAC) layer for short range, low-power operation that is well suited for wireless sensor networks. The radio is relatively low data rate (up to 250 kbps); the packets are short (< 128 bytes) and low energy. This can be cited with an example that is, sending a few bytes of sensor data, with routing, cryptography, and other headers, takes under1 ms.

## PERFORMANCE METRICS – GOALS TO BE MET

The predominant goal or requirement as a performance metric would be, ideally how fast you get the data and also the costs incurred for this data transmission. Ideally designed to operate or work at environments where there are link-layer packet delivery ratios (PDR) down to about 50 percent.

- The system must meet a minimum reliability goal. For industrial applications, the target is typically to receive at least 99.9 percent of the generated data,

as missing data would then trigger alarm conditions.

- Second, the system must support a certain throughput, which is the number of sensor data packets per second.

- Third, these data packets are only useful if received within a maximum latency period. Many processes rely on fresh data updates for control, stale data may have no utility.

- Last but not the least, many systems must operate in challenging environments that include wide temperature ranges and intrinsic safety restrictions.

Adding to these metric requirements, comes in to the picture the cost of ownership and flexibility constraints. The cost of ownership encompasses several areas: product development, installation hardware and providing power over the lifetime of the installation.

Wireless technologies have reduced installation costs dramatically compared to wired solutions, but battery-powered wireless devices may require battery changes over the lifetime of the network.

Solutions with deterministic scheduling, such as Time-Division Multiple Access (TDMA), can help separate high current events as much as possible to reduce the capacitor size requirement.

**Scalability and Flexibility:**
Networks must scale from small to large numbers of sensors and from low to high density. To be robust across diverse wireless environments, resource provisioning should ensure that devices reliably communicate with moderate interference and that the networks survive the loss of individual devices.

Additional resources, which include more wireless links, more neighbors for each device, or more signal amplification, improve reliability and latency. All these additions come at increased power costs that can be minimized with dynamic allocation.

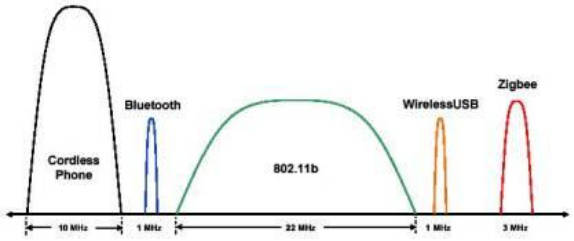
## CHALLENGES IMPOSED ON WSN'S

1. The wireless channel is unreliable in nature, and a number of phenomena can prevent a transmitted packet from reaching a receiver. One such phenomenon is interference. When two independent transmitters transmit over the same channel such that their signals overlap, they may corrupt each other's signal at a receiver's radio. This requires the transmitter to re-transmit, at the cost of additional time and energy.

**Types of Interference:**

- Interference can come from the same network if the underlying medium access technology does not schedule contention-free communications. This is particularly problematic if the two transmitters can hear the receiver, but not hearing each other and hence called Hidden Terminal Problem. This can be resolved by back off mechanisms which would eliminate collisions.

- Interference can also come from another network operating in the same radio space, or from a different radio technology using the same frequency band. The latter, known as "external" interference, is especially present in unlicensed bands such as the 2.400 to 2.485 GHz spectrum.




***Interference Levels depicted as explained above***

## 2. SECURITY CONCERNS

**A. Data Integrity**
Data integrity in sensor networks is needed to ensure the reliability of the data. It ensures that data packets received by destination is exactly the same with transferred by the sender and any one in the middle cannot alter that packet. The techniques like message digest and MAC are applied to maintain integrity of the data. By providing data integrity we are able to solve the Data integrity attacks. Data integrity is achieved by means of authentication the data content.

**B. Data Confidentiality**

Confidentiality is to protect data during communication in a network to be understood other then intended recipient. Cryptography techniques are used to provide confidentiality. Data confidentiality is the most important issue in all network security. Every network with any security focus will typically address this problem first Data confidentiality of the network means that data transfer between sender and receiver will be totally secure and no third person can access it(neither read nor write) .Confidentiality can be achieved by using cryptography: symmetric or asymmetric key can be used to protect the data.

**C. Data Availability**

Availability ensures that the services are always available in the network even under the attack such as Denial of Service attack (Dos). The researchers proposed different mechanisms to achieve this goal. Availability is of primary importance for maintaining an operational network. Data Availability determines whether a node has the ability to use the resources and whether the network is available for the messages to communicate. Availability ensures that sensor nodes are active in the network to fulfill the functionality of the network.

**D. Data Authentication**

Data Authentication of a sensor node ensures the receiver that the data has not been modified during the transmission. Data authentication is achieved through symmetric or asymmetric mechanisms where sending and receiving nodes share secret keys. In asymmetric cryptographic communication digital signatures are used to check the authentication of any message or user while in symmetric key, MAC (Message Authentication Code) are used for authentication purpose.

Understanding the above described challenges it is important to be cognizant of the different attacks imposed on WSN's.

- **Black Hole Attack**: Also known as sink holes attack occurring at the network layer algorithm. This results maximum traffic to flow towards these fake nodes.
- **Flooding:** Flooding also occurs at the network layer. This may result into effusion of the memory and energy resources of the node being bombarded.
- **Wormhole attack:** In the wormhole attack, pair of awful nodes firstly discovers a wormhole at the network layer. These packets are then replayed locally. This creates a fake scenario that the original sender is only one or two nodes away from the remote location. This may cause congestion and retransmission of packets squandering the energy of innocent nodes.

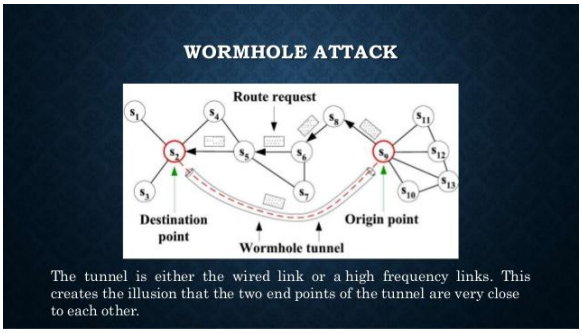


Fig: Wormhole attack

## 3. POWER MANAGEMNET ISSUES

Low-cost deployment is one acclaimed advantage of sensor networks. Limited processor bandwidth and small memory are two arguable constraints in sensor networks, which will disappear with the development of fabrication techniques. However, the energy constraint is unlikely to be solved soon due to slow progress in developing battery capacity.

Adding on, the untended nature of sensor nodes and hazardous sensing environments preclude battery replacement as a feasible solution. On the other hand, the surveillance nature of many sensor network applications requires a long lifetime; therefore, it is a very important research issue to provide a form of energy-efficient surveillance service for a geographic area.

Much of the current research around the globe focuses on how to provide full or partial sensing coverage in the context of energy conservation. In such an approach, nodes are put into a dormant state as long as their neighbors can provide sensing coverage for them. These solutions regard the sensing coverage to a certain geographic area as binary, either it provides coverage or not.

## Solutions to overcome the imminent challenges:

Routing access restriction

False routing information detection.

As stated previously, one technology well suited for solving the WSN problem is IEEE 802.15.4. Such 802.15.4 radios offer low-power, low data rate PHYs in several unlicensed frequency bands, the 2.4 GHz ISM band, available worldwide. The 2.4 GHz band spread spectrum PHYs provide immunity to noise – a particularly important feature for a low-energy device designed to operate in a potentially crowded, unlicensed band.

This flexible solution leads to another technology that is the ZIGBEE protocol, and forms unsynchronized single-channel networks, and the Wireless HART protocol, which uses it to form time synchronized multichannel networks.

## FUTURE IN THE DOMAIN OF WSN'S

**Some of the Active Research Areas**

The security issues posed by sensor networks are a rich field for research problems.

1. Designing routing protocols having built in security features.

2. A new symmetric key cryptography for sensor networks.

3. Designing secure data aggregation protocols, designing intrusion detection systems and security systems for multimedia sensors.

4. Mobiles as Wireless Sensors

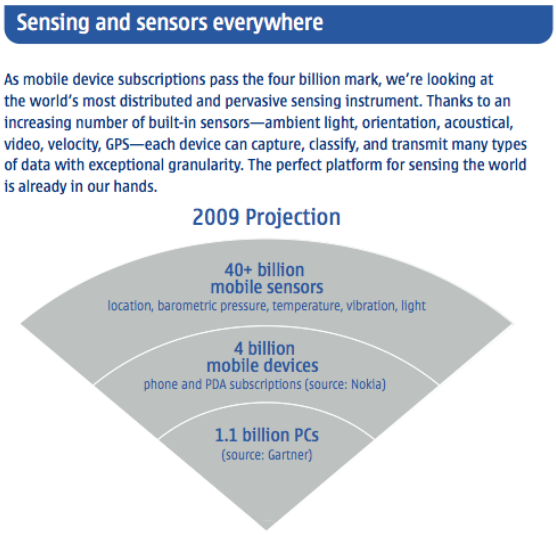



Fig: Future Goals

## 3. CONCLUSIONS

Wireless Sensor Networks have created a exceedingly wide range of challenges that still needs to be addressed. In this paper we have identified and analyzed comprehensive list of issues associated with Wireless Sensor Networks. We have also discussed some of the popular protocols implementing these issues in part or as a whole technique. The importance of wireless sensor networks on our day to day life can be preferably compared to what Internet has done to us. This field is definitely providing to g us tremendous opportunity to change the way we perceive the world today.
Multichannel time-synchronized mesh networks based on 802.15.4 radios address many of the challenges involved in building flexible, reliable, low-power wireless sensor networks. There are a growing number of new applications that are utilizing these types of sensor networks to reduce costs and provide enhanced services around the world.

## REFERENCES

[1] J.Hill,M.Horton,R.Kling and L.Krishnamurthy,"The Platforms EnablingWireless Sensor Networks", Communications of the ACM, June2004/Vol 47.No.6

[2] D.Puccinelli and M.Haenggi,"Wireless Sensor Networks: Applicationsand Challenges of Ubiquitous Sensing", IEEE Circuits and SystemsMagazine, Volume 5, Issue 3, 2005, pp: 19:31].