International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 09 | Sep -2017 www.irjet.net p-ISSN: 2395-0072

Wireless Sensor Network - An Outlook

Arockia Panimalar.S [1], Rubasri.K[2], Sruthi.K[3], Rakshitha.K.R[4]

[1] *Assistant Professor, Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Tamilnadu, India*
[2,3,4] *III BCA, Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Tamilnadu, India*

Abstract - *The headway in a decade ago in electronics & communication, computer science and information technology area has brought about the new computing and communication era, known as Wireless Sensor Networks. In the past the wired sensors were executed in constrained applications in industries. Notwithstanding, wireless usage makes the wide arrangement of sensor nodes more possible than some time recently. There has been much research with respect to the immense potential capacities of wireless sensor Networks (WSNs) in applications, for example, environmental monitoring, habitat study, military surveillance in the battlefield and home automation. With sharp declines in cost and tangible improvements in storage and processing capabilities of sensor nodes, the incorporated nearness of sensor nodes in human regular day to day existence, as the connector of the physical condition with virtual digital world, will be predominant in not so distant future. This paper reviews Wireless Sensor Network (WSN) architecture, characteristics, types, applications, issues in designing routing protocols and security threats.*

***Key Words*: Sensor Networks, Routing, Architecture, Applications, Security Threats.**

1. INTRODUCTION

A sensor network is a communication framework or gathering of specific transducers to monitor, record and react to any marvels or different areas**.** Sensing components can for the most part monitor temperature, mugginess, weight, wind bearing and speed, light force, vibration force, sound force, control line voltage, chemical concentrations, contamination levels and vital body capacities. Sensor networks communication infrastructure and protocols are distinct and challenging from late Internet based framework in light of their necessities and confinements. With the progress of technology, sensor network is implemented with small, low cost, low power, multifunctional, distributed sensors. Each sensor node has ability to perform a limited amount of processing. Be that as it may, when sensor nodes are composed with different nodes, they can play out some particular activity. Some time recently, sensor arrange was sent just for modest number of nodes, wired to a central processing station. Just, these days the concentration is going for wireless, distributed, sensing nodes.

A sensor network consists of a big number of sensor nodes that are densely positioned inside or near to the occurrence. The energy of each sensing element or energy efficiency is another issue for sensor network MANETS (Mobile Ad-hoc Networks) and sensor networks are two classes of the wireless Ad hoc networks with resource constraints. MANETS usually consist of devices that have high processing and power capabilities, mobile and can operate in coalitions. Both these wireless networks consists ad hoc nature and lack pre deployed infrastructure for computing and communication. The differences between sensor networks and ad hoc networks are identified below. The number of sensor nodes in a sensor system can be a few requests of greatness higher than the clients in an ad hoc network. Sensor nodes are densely deployed.

- Sensor nodes are prone to failures.
- The topology of a sensor network changes all the time.
- Sensor nodes chiefly utilize a broadcast communication method, though most especially ad hoc networks depend on point-to-point communications.
- Sensor nodes are restricted in control, computational abilities, and memory.
- Sensor networks are normally controlled in particular geological areas for tracking, checking and sensing.
- Sensor nodes might not have worldwide distinguishing proof (ID) because of the enormous measure of overhead and substantial number of sensors [1].

A. Three Generations of Sensor Nodes

	1980's-1990's	2000-2003	2010 Onwards
Manufacturer	Custom Contractors Eg: TRSS	Commercial: Crossbow Technology, Sensoria Corp, Ember Corp.	Dust and Other to be formed
Size	Large Shoe Box and Up	Pack of Cards to Small Shoe Box	Dust Particle
Weight	Kilograms	Grams	Negligible
Node Architecture	Separate Sensing, Processing and Communication	Integrated Sensing, Processing and Communication	Integrated Sensing, Processing and Communication

Topology	Star, Point - to-point	Peer to Peer, Client Server	Peer to Peer
Power Supply Lifetime	Hours, Days	AA Batteries, Days to Weeks	Solar, Month to Years
Deployment	Vehicle Placed or Air Drop Single Sensors	Hand Emplaced	Embedded, "Sprinkled" Left Behind

Table 1: Generations of Sensor Nodes

B. Attributes of Sensor Network

The table shows the attributes of Sensor Network:

Sensors	**Size**: Small (eg: MEMS), large (eg: satellites, radar) **Number**: Large, Small **Type**: passive (Eg: acoustic, Video, IR), active (eg: ladar, radar) **Composition/mix:** heterogeneous, homogeneous **Spatial coverage**: sparse, dense **Deployment**: fixed, adhoc **Dynamics:** stationary, mobile
Operating Location	Adverse(battlefield), Benign (factory floor)
Sensing Entities of Interest	**Extent**: distributed, localized (eg: target tracking) **Mobility**: dynamic, static **Nature**: Cooperative (eg: air traffic control), non-cooperative (eg: military targets)
Communication	**Networking:** Wireless, Wired **Bandwidth**: Low, High
Processing Architecture	Centralized, distributed, hybrid
Energy Availability	Constrained (eg: in small sensors), unconstrained (eg: in large sensors)

2. SENSOR NETWORK ARCHITECTURE

As in fig 1, the sensor nodes are commonly scattered in sensor field. Each and every of these scattered sensor nodes are Capable of gathering data and route back data to the sink. Information is routed back to the sink through a multi hop infrastructure less route or architecture as in fig 1.

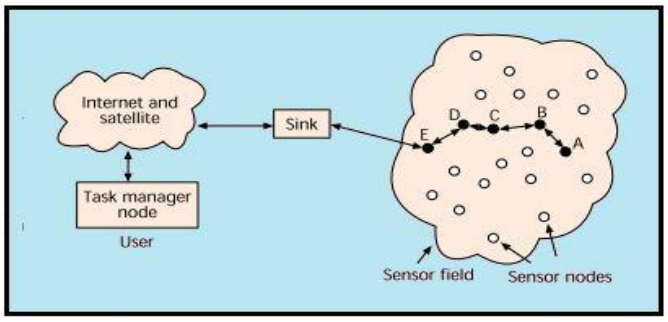

Fig 1: Sensor Network Architecture

The sink can communicate with the task manager node through Internet or Satellite technology. The pattern of sensor networks is determined by various factors, like fault tolerance, scalability, small size, robust operations, production, costs, operating environment, security, compatibility, flexibility, data aggregation, sensor network topology, hardware constraints, transmission media, quality of service (QoS), data latency and overhead and power consumption etc. In a multi hop sensor network, nodes are connected through wireless medium infrared, radio and optical[1].

3. WSN ARCHITECTURE

The architecture of WSN varies for a individual sensor node and the entire web. Vitality productivity, estimate decrease and least cost are the essential concern for sensor node architecture. The figure depicts the functional block diagram of a sensor node.

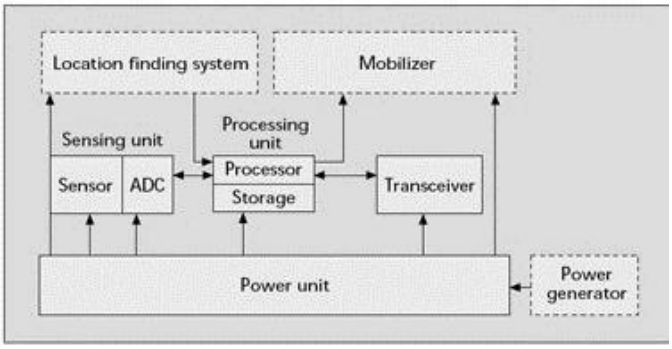

Fig 2: Block diagram of WSN

A wireless sensor node consists of 4 functional components like sensing unit, processing unit, transceiver, and power unit.

A. Sensing Unit

It consists of an array of sensors that can quantify the physical characteristics of its environment.

B. Processing Unit

A sensor node utilizes a microcontroller which performs assignments, forms data and controls the dealing with different segments in the sensor node. Since a microcontroller is portrayed by its unobtrusive value, straightforwardness to connect different gadgets, effortlessness of programming, and low power usage, they are utilized as a part of sensor nodes. Capacity prerequisites rely upon application sort.

C. Transceiver

The transceiver is used to transmit and receive messages wirelessly. The functionality of both sender and receiver are combined into a single device known as a transceiver. In WSN any node has to converse" with other guests. Nodes are constrained by limited energy. A transceiver must provide an adequate balance between a low data rate and modest energy consumption. This enables the node to live for an extended period of time.

Sensor nodes generally make use of ISM band, which gives free radio, spectrum allotment and universal availability. The wireless transmission medium can be radio frequency (RF), visual communication (laser) and infrared. Lasers need line-of-sight for communication and are susceptible to atmospheric weather. But energy requirement is less for optical communication. Infrared transmission has limited broadcasting capacity, but similar to laser communication antenna is not needed. Nevertheless, in the majority of WSN applications, communication through radio is used. The license-free communication frequencies of 173, 433, 868, and 915 MHz and 2.4 GHz is ideal for wireless communication in most cases since it is not limited by line of sight. The current technology allows implementation of low-power wireless. Sensor nodes must perform in-network processing as much as possible because of the energy consumption of the transceiver which is far greater than the energy consumption of the microcontroller.

Later the appearance in 2003 of the most sensor nodes utilize transceivers for low-rate wireless personal area networks (PANs) that conform to the IEEE 802.15.4 standard presented in the twelvemonth 2003. Transceivers need extraordinary identifiers. The operational conditions of the transceiver are transmitting, accepting, lingering, and kipping. Energy consumption for transceivers out of gear mode and get mode is by and large about equivalent. Hence the transceiver is shut down and not given in the idling mode when it is not communicating; otherwise considerable amount of energy will be wasted when switching from sleep mode to transmit or receive mode.

D. Power Source

The energy needed for all components of a WSN is obtained from a power supply. Since the wireless sensor node is frequently situated in a hostile territory, changing the battery consistently can be costly and tricky. The energy use in sensor node is required for sensing, communicating and data processing. Communication of information needs more push than some other process. The primary source of energy in sensor node is from power stored in batteries or capacitors. Presence detectors are able to renew their energy from solar sources, heat differences, or pulsation [2].

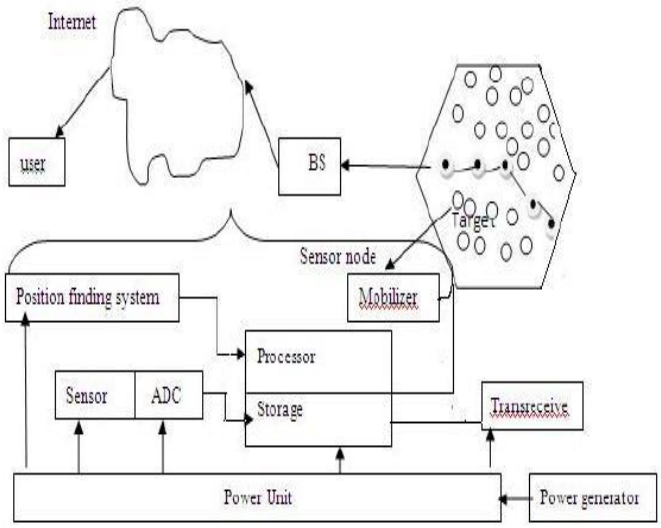

Fig 3: Sensor nodes scattered in a sensor field and components of a Sensor Node

4. CHARACTERISTICS OF WSN

The significant characteristics of a typical WSN which differ it from other wireless adhoc networks can be summarized as below:

- Limited computational capacity.
- Limited energy resources.
- Limited memory capacity.
- Frequently changing infrastructure as against adhoc networks due to mobility.
- Problem in assigning and maintaining unique global identification due to the very large number of guests present.
- Higher chances of failure of lymph glands due to harsh environment and limited energy capacity.
- More densely placed nodes.[3]

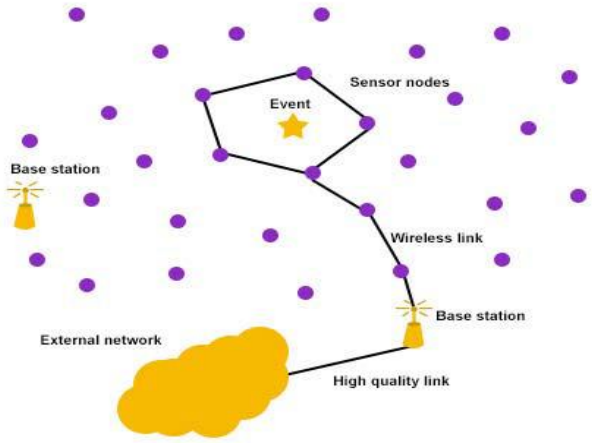

Fig 4: Wireless Sensor Network (WSN)

5. TYPES OF WIRELESS SENSOR NETWORKS

As per past research work made out five sorts of wireless sensor networks is conceivable relying on where and how sensors are introduced to monitor data. Consenting to these properties of sensor deployment, we can characterize WSNs into five essential sorts in particular, ground (terrestrial) WSN, underground WSN, aquatic (underwater) WSN, multimedia WSN, and mobile WSNs.

A. Ground (Terrestrial) WSNs

It consists of hundreds of thousands of inexpensive wireless sensor nodes deployed randomly in a given sensing area. In ad hoc deployment, sensor nodes can be omitted from a plane and randomly placed into the target area. In a dry land (terrestrial) WSN, reliable communication in a dense environment is really important. Ground (Terrestrial) Sensor nodes must be capable to effectively communicate data back to the base station. While battery control is restricted energy resource and its is primary compel on network performance and it may not be replaceable or rechargeable once more, ground(terrestrial) sensor nodes however can be outfitted with a secondary power source, for example, battery or sunlight based cell(solar). In this manner because of this it is constantly imperative for sensor nodes conserve energy. For a ground(terrestrial) WSN, energy can be safeguarded with short transmission run, multi-hop routing, disposing of data purity, in-network data aggregation, limiting postponements, and utilizing low obligation cyclic operations.

B. Underground WSNs

They are a collection of a number of sensor nodes placed inside the crust of earth or in a cave or in a mine and they are applied to monitor underground events such as volcanic conditions, etc. Additional sink or base station nodes are situated over the outside layer of earth to transmit data from the sensor nodes to the sink (base station). These kind of WSN are significantly more costly than a ground (terrestrial) WSN in terms of deployment, equipment, and care. Underground sensor nodes are all the more expensive in light of the fact that vital gear parts must be ensured solid correspondence through rocks, earth, water, and different substance dwelling inside covering. The internal condition makes remote correspondence a test because of abnormal amounts of constriction and flag misfortunes. Not at all like ground WSNs, the arrangement of an underground WSN requires cautious arranging and energy and cost contemplation. Vigor is an essential imperative in underground WSNs.

C. Aquatic (Underwater) WSNs

It comprises of various sensor nodes and vehicles deployed inside water. As inverse to ground (terrestrial) WSNs, amphibian (submerged) sensor nodes are more costly and less sensor nodes are deployed in sensing region. Autonomous aquatic (underwater) Vehicles are utilized for exploration or gathering information from sensor nodes. When contrasted with a slow deployment of sensor nodes in a ground WSN, a sparse deployment of sensor nodes is placed at sea level (underwater). Classical aquatic (underwater) wireless communications are implemented through transmission of acoustic waves.

D. Multimedia WSNs

They are combination of a number of low cost sensor nodes equipped with microphones and cameras. These sensor nodes interconnected with each other over a wireless connector for data sensing, data processing, data correlation, and data compression. Multimedia WSNs are utilized to empower monitoring and tracking of events in the form of multimedia applications.

E. Mobile WSNs

They are of a collection of moving sensor with their interaction with sensing environment. Moving sensor nodes have the mental ability to sense, compute, and communicate like non-moving nodes. Mobile WSNs are used in military and other industrial applications.[4]

6. DESIGN ISSUES OF ROUTING PROTOCOL

Routing is a process of finding a path between source and destination for data transmission.

The inherent characteristics of WSN that differentiates it from other wireless networks like mobile ad hoc networks or cellular networks makes the design of routing protocols for WSN very demanding. The routing protocols in WSN must optimize energy usage, aggregate data, data-centric and application specific. The considerable characteristics of a good routing protocol for WSN are straightforward, energy

awareness, flexibility and adaptability because of restricted energy supply, limited computation power, constrained memory and constrained transmission capacity of WSN. WSNs are planned to accomplish data communication alongside ventures to extend the life expectancy of the network. The demanding factors affecting the design of a routing protocol in WSNs are summarized as:

A. Node Deployment

In WSNs node deployment is dependent upon the purpose and environment. The operation of the routing protocols in WSNs is influenced by node deployment, particularly in the energy requirement. Clients can be deployed either manually or in a self-organizing fashion classified as manual or random deployment method respectively. Nodes deployment is also described according to the mobility of sensor nodes. If the nodes are passively moved by outside forces, they are called passive nodes. Dynamic agents can effectively search for concerned regions.

B. Network Dynamics

The coverage and connectivity of WSN is affected by the dynamic characteristics of Base Station or sensor node. As connectivity among sensor nodes change, stability and route decision becomes one of the demanding issues. If the foot station and sensor nodes are moving, the problem is more complicated.

C. Energy Conservation

While creating a WSN, energy conservation factor has an outcome on the selection of routes. In many fonts, multi-hop communication conserves energy of sensor nodes compared to one hop communication and hence resulting in an increase in the life of WSN. However an issue emerges on account of the sending nodes quick energy waste in contrast with the nodes at the last layer in multi hop communication, hierarchical communication. Multi-hoping is included with critical operating cost because of network management and medium access control.

D. Error Tolerance

The sensor node failure should not influence the working of WSN. Network need to mold even when some of the sensor nodes fail.

E. Scalability

The sensors in the deployed area vary in number. Also, many sensor nodes may not be working due to power drainage and physical damage. Creating holes in the existing WSN. Design of WSN must support scalability.

F. Production Costs

The universal requirement is to keep the cost of a sensor node to be cheap.

G. Hardware Constraint

Since the requirement of WSNs is low energy, low computational capacity and low communication range, it becomes one of the important design issues related to power delivery and quality of service. All subunits of sensor nodes, that is sensed, processing, communication, power, location finding system and mobilizes, must consume very low power and be contained within a very small range. MAC layer may be designed in to synchronize the wake and sleep time with application requirement.

H. Sensor Network Topology

It must be upheld regardless of very high node density. Keeping up the topology in the mobile scenario becomes one of the important and necessary issues.

I. Environment

Nodes should be working in an inaccessible location because of the hostile environment.

J. Transmission Media

Generally, the transmission media are wireless (RF or Infrared), which is affected by fading and high fault rate and affect the operation of WSNs.

K. Data Delivery Models

Data delivery may be categorized into following: event driven, inquiry-driven, reactive, proactive, hybrid. Picking out one data delivery model is basically requirement of the application of the WSNs.

L. Quality of Service (QoS)

The application needs to deliver quality of service is dependent upon the lifetime, data consistency, energy efficiency, position knowledge and collaborative-processing. The choice of routing protocols for a particular purpose is influenced by the QoS factors.

M. Security

WSNs may communicate with sensitive data and work in disagreeable environment. Thus security concerns should be addressed to while designing the routing protocols for WSN.

N. Node Capabilities

A sensor node can be given to a particular special work such as relaying, sensing and aggregation, depending on the requirement. Absorbing all the three functionalities simultaneously on a node may result in quicker drainage of the energy at that node.

O. Data Aggregation/Fusion

In order to effectively utilize the limited energy available, computation costs, which are much smaller than the communications cost, is utilized to minimize the amount of information that actually has to be sent. Data aggregation/fusion helps in cutting down the number of communications by using some aggregate functions like suppression (eliminating duplicates), min, max and average. The clustering protocol supports in-network aggregation, which is utilized to aggregate information from various sensors and to summarize that information before communicating and passing it on to the other nodes. This increases the lifetime span of WSNs.

P. Byte Overhead

Byte overhead is the total bytes in the routing control messages which decide a routing path to the home station. The bytes transmitted along the track from the beginning node to the base station are not considered as overhead. [2]

7. WIRELESS SENSOR NETWORKS APPLICATIONS

The applications of WSNs are classified into Defense applications, forest applications, medical science applications, Domestic applications, and industrial applications:

A. Defense Applications

WSNs can be an inbuilt part of Defense command, security control, data communications, computation, intelligence, targeting systems such as (C4ISRT), surveillance and reconnaissance.

B. Forestry Applications

Some environmental applications of sensor systems incorporate tracking and reading the movements of little creatures, flying creatures and creepy crawlies, monitoring environmental conditions, earth monitoring and exploration.

C. Medical Science Applications

A portion of the health applications for sensor systems are diagnosing the patients, area locating and mobility of patients and doctor specialists in the hospital.

D. Industrial Applications

Some industrial applications of WSNs are building virtual keyboards, monitoring product quality, environmental control in office buildings, robot control, interactive toys and so on [4]

Fig 5: Wireless Sensor Network (WSN) Applications

8. SECURITY THREATS

In WSNs the security services goal is to protect resources and information from misbehavior and attack. WSN faces four basic threats, which are indicated in fig 6.

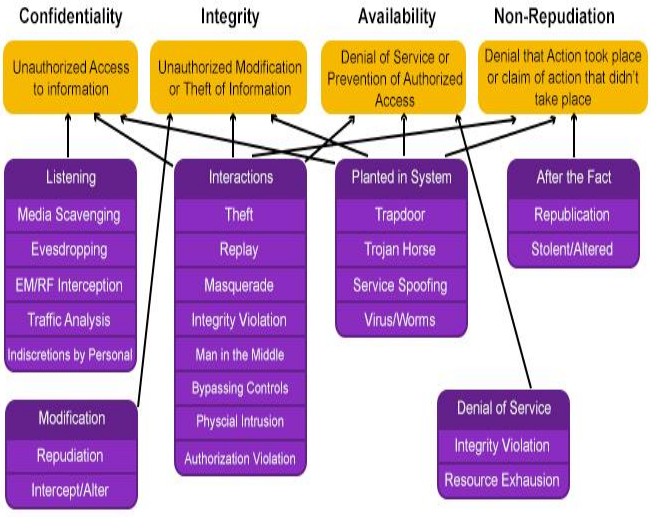

Fig 6: Four Basic Threats

A. Confidentiality

It makes certain that only desired recipients can understand the given message. Confidentiality and security countermeasures are mentioned in fig. 7.

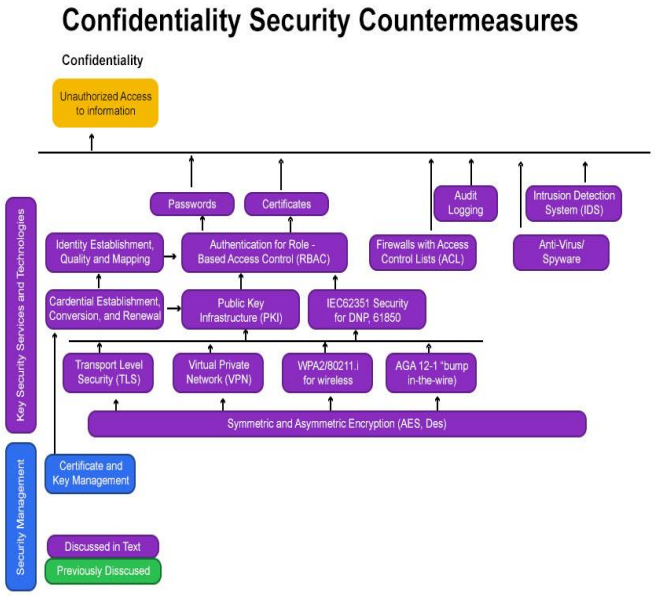

Fig 7: Confidentiality Security & Countermeasures

B. Integrity

It makes sure that the message is not altered by intermediate nodes, which are malicious when it is sent to another node in a net. Countermeasures for threats on integrity are demonstrated in fig. 8.

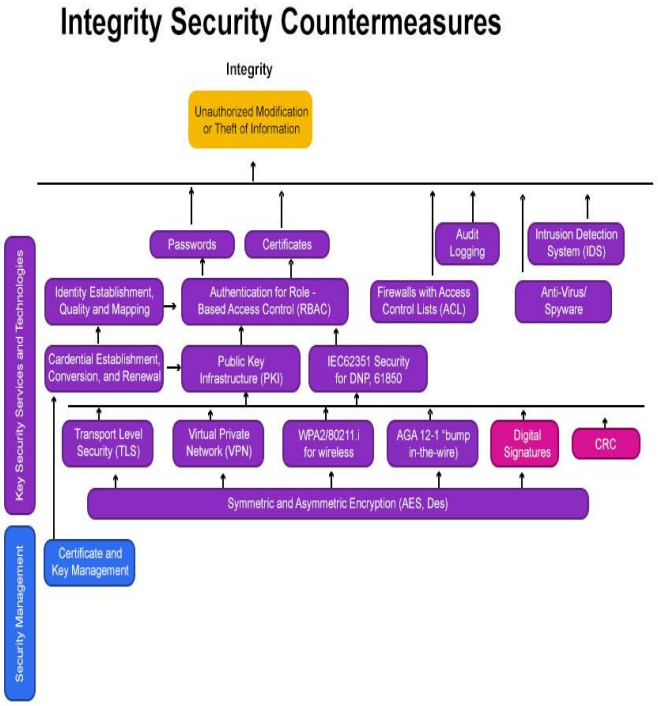

Fig 8: Integrity Security & Countermeasures

C. Availability

It makes sure that the services of network are available which are desired even under attacks such as DoS(denial-of-service). Security countermeasures for availability threats are shown in fig. 9.

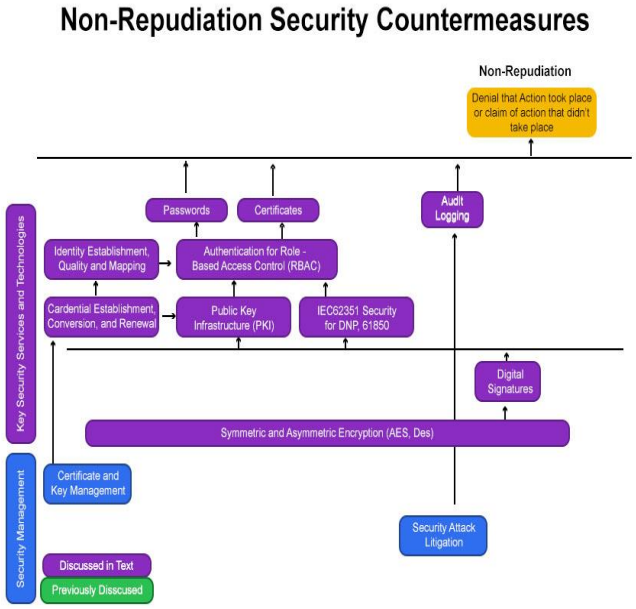

Fig 9: Availability Security & Countermeasures

D. Non-Repudiation

Non-Repudiation refers to the facility to ensure that a person cannot negate the authenticity of their signature. Countermeasures for Non-repudiation threats are shown in fig. 10.

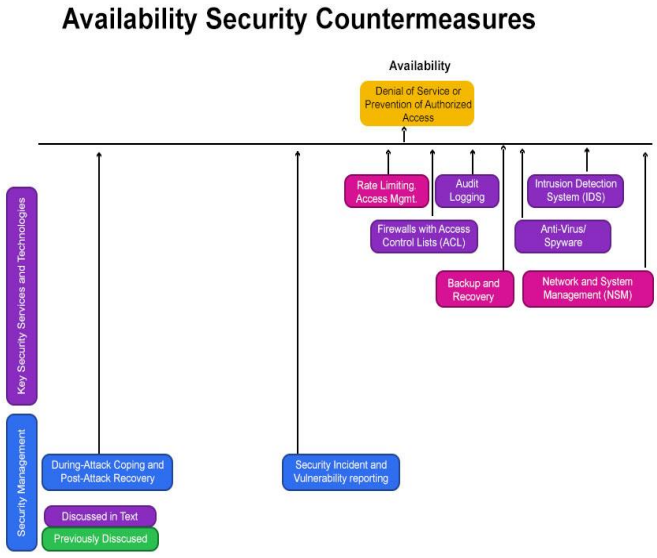

Fig 10:Non-Repudiation Security &Countermeasures

9. CONCLUSION

Wireless Sensor Networks are one of the emerging areas in research area. Wireless sensor networks have a remarkable feature to monitor the environmental and physical phenomenon such are temperature, force per unit area and humidity. In this paper, we talked about a few parts of wireless sensor networks and furthermore examined different types of WSNs, their characteristics, applications, issues in designing routing protocols and security threats. The routing protocols in WSN have turned out to be a standout amongst the most essential research zones and displayed special difficulties contrasted with traditional data routing in wired networks. The essential point behind the routing protocol design is to keep the sensors working for quite a while, therefore expanding the network lifetime and many routing protocols have been proposed for sensor networks.

10. REFERENCES

1] Kazi Chandrima Rahman" A Survey on Sensor Network", VOLUME 01, ISSUE 01, MANUSCRIPT CODE: 100715, ISSN 2218-5224 (ONLINE)

[2]Shabbir Hasan1, Md. Zair Hussain2, R. K. Singh3 "A Survey of Wireless Sensor Network" (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 3, March 2013)

[3]Amit Rathee, Randeep Singh, Abhishilpa Nandini "Wireless Sensor Network- Challenges and Possibilities" Volume 140 – No.2, April 2016 ,ISSN: (0975 – 8887)

[4]Pardeep Kaur, Vinay Bhardwaj" Wireless Sensor Networks: A Survey" Volume 5, Issue 5, May 2015 ISSN: 2277 128X

[5] Furrakh Shahzad1, Maruf Pasha2, Arslan Ahmad2" A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures" Vol. 14, No. 12, December 2016, ISSN 1947-5500