WIRELESS SENSOR NETWORKS AND APPLICATIONS

Sai Krishna Kovi
Department of computer science
Frostburg state university
Frostburg, MD
Skosgi0@frostburg.edu

Pavankumar Jangam
Department of computer science
Frostburg state university
Frostburg, MD
pjangam0@frostburg.edu

Sai Kumar Goud Kosgi
Department of computer science
Frostburg state university
Frostburg, MD
Skosgi0@frostburg.edu

Abstract

Wireless sensor network is rapidly growing technologies in recent times. These sensor networks can be used in various applications like military, environment, health, automotive, home and other applications. Sensor nodes with wireless interface can communicate with each other to form a network. Each sensor node uses protocol stack to communicate with each other. Sensor networks are small and low-cost. Sensor networks protocol stack consists of application layer, transport layer, network layer, data link layer, physical layer and cross-layer protocols. This survey paper will cover up with types of sensors, sensor architecture and protocol stack, applications, security and their counter measures.

Introduction

Wireless sensor network is a major area of research in recent years. It consists of compact devices called sensor nodes. These sensor nodes are very small which consists of limited processing and computing resources [3]. It has a group of sensors which are used to scan differential environmental conditions to organize and collect the data to some location. It measures and select number of physical conditions like temperature, pressure, humidity, sound, direction and speed, chemical components, vibrations and pollutant levels etc., with the growth in technology, sensor network is executed with small, low power, low cost, multi-functional distributed sensors [2]. Sensor nodes can sense, measure and gather information from different environment and they can transmit the sensed data to the user [3].

A sensor network consists of more number of sensor nodes; these nodes are to be engineered or pre-determined for their position [1]. Each sensor node has a capability to perform limited amount of efficiency [2]. Main power source in a sensor node is battery, solar cells are used as secondary power to power up the batteries [3]. A sensor network consists of large number of sensor nodes that are densely located near or inside of the occurrence [2]. The basic components of sensor nodes are power source, memory storage, processor, transceiver, gps. Processor performs tasks like processing data and control the functions of other components in the sensor node. Transceiver receives command from the base station and transmits data to computer or station [2]. It is a combination of both radio transceiver and receiver, wireless transmission media has a possible choice they are radio frequency (RF), optical communication (laser) and infrared. There are two types of memory: user memory is used to store personal data or application related, program memory identification of data if it is present. In power source power is stored in batteries or in capacitors, both rechargeable or un-rechargeable batteries are main source of power supply for sensor nodes.

Wireless sensor networks consist of two types of sensor nodes: structured and unstructured. In unstructured (ad hoc) mode, the sensor nodes are distributed randomly to the target area that are dropped from the plan [7]. In structured or pre-planned mode considers optimal placement, grid placement, 2D and 3D placement models [7]. The advantage of structured node is fewer node is deployed with low network maintenance and management cost [4].

Many applications are developed using sensor networks, most of them are custom made with basic architecture and standardization in protocols that can be used for communication [8]. Some of the applications are: military, environmental, biomedical, automotive, home application. In military surveillance and target tracking, WSN help in intrusion identification and detection [4]. To forecast disasters before they occur, sensor nodes are used to sense and detect the environment conditions [4]. Diagnostics, integrated monitoring of a patient is done using bio-medical WSN.

There are two types of security we have they have wired and wireless security. Wired sensor network security is better to control and maintain some software's like firewalls. In wireless sensor network signals are transmitted through the air so, there is more chances of getting hacked and manipulated. In WSN security is important issue, due to satellite features and various limitations it becomes significantly challenging to design security for some networks [4]. In this paper, we discuss about the security issue and challenges for the WSN. This paper structured as follows: Section 2 gives the different types of sensor networks. Section 3 we explain about the system architecture and protocol stack. Section 4 we explain about the applications of sensor networks. Section 5 explains of different types of securities in WSN. Section 5 we conclude our paper.

Types of sensor network

Wireless sensor networks are developed on land, underwater and underground. According to the environment in the sensor network, it faces different challenges and constraints [4]. There are different types of sensor networks they are [4], [6]: terrestrial WSN, underground WSN, underwater WSN, multi-media WSN, mobile WSN.

Terrestrial WSN: Terrestrial WSNs consists of hundreds or thousands of wireless sensor nodes, these nodes are positioned into structured and unstructured nodes; either in ad hoc or pre-planned manner [6]. In unstructured (ad hoc) mode, the sensor nodes are distributed randomly to the target area that are dropped from the plan [6]. In structured or pre-planned mode considers optimal placement, grid placement, 2D and 3D placement models.

Sensor node must communicate successfully with base station in terrestrial WSN; the battery power is limited may not be rechargeable, however the battery is equipped with secondary power cells as solar cells [4], [6]. It is necessary for solar cells to conserve energy. The energy conservation of terrestrial WSNs is achieved by using multi-hop optimal routing, short transmission range, eliminating data redundancy, in-network data aggregation, minimizing delay and using low-duty cycle operation [4].

Underground WSN: Underground WSN consists of underground sensor nodes connected wirelessly, communicated through the soil and it is used to detect and monitor underground situation [8]. Transmission of information from sensor node to the base station is done by sink node [6]. In terms of equipment, development and maintenance underground WSN are costlier than terrestrial WSN [4], [6]. They are very difficult to recharge; the sensor battery nodes have a limited battery life and difficult to recharge. Underground sensor nodes are much expensive since genuine components must be selected for reliable communication through soil, rocks, water and other mineral contents [6]. To increase network lifetime underground WSN should plan energy and cost efficient [4].

Underwater WSN: underwater WSN consists of number of sensor nodes and vehicles which are deployed under the water [4]. Compared to terrestrial WSNs, underwater sensor nodes are more cost and less dense [6]. Sensor failure, bandwidth and long propagation delay are big challenges for the acoustic communication in underwater WSN. Underwater WSN cannot be recharge or replaced because they have limited battery. Underwater sensor node has many potential applications they are [7]: seismic monitoring, equipment monitoring and control and flocks of underwater robots. Developing efficient underwater communication and networking techniques involves energy conservation issue for underwater WSNs.

Multi-media WSN: Multi-media WSNs are used to enable monitor and track events in the form of multimedia [4]. It interconnects smart devices that permits retrieving video, audio, still images and scalar sensor data [8]. Camera and microphone are the low-cost sensor nodes equipped by the multimedia WSNs [6]. Data compression, data retrieving and correlation sensor nodes are interconnected with each other with wireless connection. The challenges with the multimedia WSN include high energy consumption, high bandwidth requirements, quality of services(Qos), data processing and compression techniques and cross-layer design [4], [6]. Video stream needs high bandwidth to deliver the content. So, energy consumption is high for high data rate [4]. Processing and delivery of process improved by cross-layer interaction among the layers.

Mobile WSN: Mobile WSNs consists of set of sensor that can be moved on their own and can be interacted with the physical environment, sensor nodes can move from one place to another place [4]. Mobile nodes can communicate, compute and sense. Mobile nodes can organize itself and change its position in the network [6]. Mobile WSNs can start with initial state and nodes will spread out to gather information [6]. Mobile nodes when they are within the range can communicate with each other and transfer the gathered information [4], [6]. These networks can be easily interfaced with the environment. The challenges with the mobile WSN are [4]: deployment, self-organization, localization, energy, navigation and control, coverage, maintenance and data process. Applications for mobile WSN are environment monitoring, target tracking, search and rescue and real-time monitoring of hazardous [6]. These mobile networks are versatile compared with other static sensor network systems.

Sensor Network Communication Architecture:

Sensor Network Communication Architecture consists of sensor nodes, sensor field, internet and user as shown in the figure below [1].

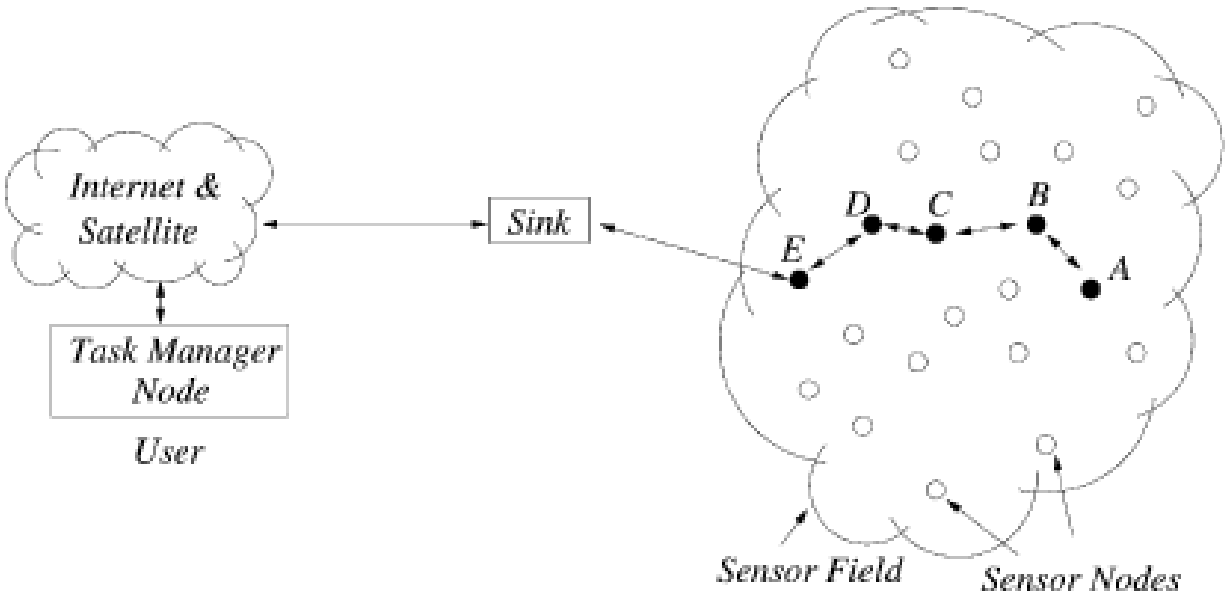


Fig1. Sensor network communication architecture

Nodes in a sensor network works as battery in most situations, each sensor node has the capability to collect data and route data back to the sink and to the end user. A network may consist of hundreds or thousands of nodes, depending upon the application. Data are routed back through the sink to the end user by a Multi-hop infrastructure-less architecture [1]. The sink will communicate task manager node via internet & satellite [2]. To achieve more network lifetime, sensor nodes must tailor their activities in an energy efficient way so scarce energy reverses are used very efficiently [1]. Each sensor node uses protocol stack to communicate with one another and to sink. In terms of communication and effective work across multiple sensor nodes, protocol stack must work energy efficiently.

Protocol stack integrate power and routing awareness, communicates power efficiently through wireless medium, integrates data and networking protocols and promotes cooperative effects of sensor nodes [1], [2]. The sensor network protocol stack is shown in the figure below. Protocol consists of physical layer, data link layer, network layer, transport layer application layer, power management plan, mobility management plan and task management plan [1].

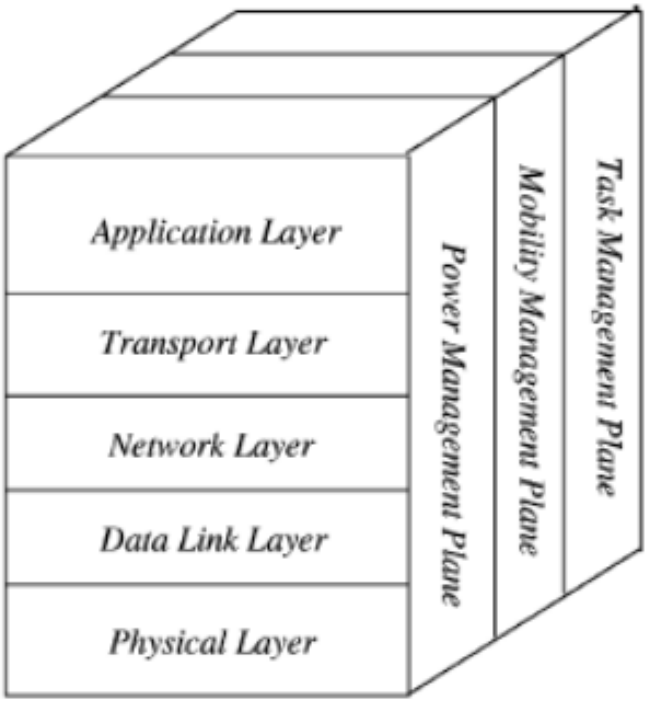


Fig2.different layers in a wireless sensor network

Application Layer: It is responsible to provide software for different applications that translate the data in a predictable form or send queries to get certain information and to maintain traffic management. There are three application layer protocols they are: Sensor Management Protocol (SMP), Task Assignment and Data Advertisement Protocol (TADAP), and Sensor Query and Data Dissemination Protocol (SQDDP) [1].

1. **Sensor Management Protocol**

System administrators interact with sensor networks using SMP protocol [2]. An application layer management protocol makes hardware and software of the lower layers transparent to the sensor network management applications [1]. SMP needs to access the nodes by using location-based naming and attributes-based addressing. Therefore, the software will perform the following administrative task [1].

- Introducing the rules related to data aggregation, attribute-based naming and clustering to the sensor nodes.
- Exchanging data related to the location finding algorithm's.
- Time synchronization of the sensor nodes.
- Moving sensor nodes.
- Turning sensor nodes on and off.
- Querying the sensor nodes network configuration and the status of the nodes, and reconfiguring the sensor network.
- Authentication, key distribution and security in data communications.

The description of some of the task are given in [3].

2. **Task Assignment and Data Advertisement Protocol**

One of the important operation of sensor network is interest dissemination and user send their interest to a sensor node, a subset on whole network or a node [2]. Another one is the advertisement of available data where the sensor nodes advertise the available data to the users and the user question the data in which they are interested [1], [2].

3. **Sensor Query and Data Dissemination Protocol**

The protocol provides user interface for the applications to issues questions, respond questions and collect incoming replies [1]. Queries are not supplied for the nodes instead; location or attributes-based naming is preferred [2].

Sensor Query and Tasking Language (SQTL) [2], [1] is an application proposed to provides even a large set of services. SQTL supports three types of events, they are defined by: receive, every and expire. Receive means sensor nodes generates events when the sensor node receive message; every defines events occur periodically due to timer time-out; expire defines events occurred when time is expired [2] [1].

Transport Layer: The function of the transport layer is to provide reliability and quality of the data at source and the sink. For different applications, this layer should provide variable packet reliability [4]. There are two types of approach for packet recovery they are hop-by-hop and end to end [4]. Transport layer is needed when the system is planned to access through internet or external networks [1]. TCP connections are created between sensor node and sink, communication between user and sink is done via internet or satellite by UDP or TCP [2]. Transport layer need to handle differently for the factors such as power consumption and scalability, and characteristics like data-centric routing.

Network Layer: The major function of this layer is routing; it handles routing of data across network from source point to destination point [4]. By meeting these protocol constraints such as limited energy, communication bandwidth, memory and consumption capabilities can prolong the networks lifetime [4]. Energy efficient route, data centric routing and data aggregation are some of the important tasks performed by network layer which provide internetworking with external networks such as internet and command and control systems [2].

Data Link Layer: This layer is responsible for multiplexing data streams, data frame detection, error control and MAC, ensures reliability of point-to-point or point-to-multiple point [1]. MAC should have the following attributes they are energy efficiency, bandwidth utilization, frame synchronization, flow control, error control and scalable to node density for data communication [4]. Wireless multi-hop sensor network must achieve two goals: 1) Creation of network infrastructure: MAC should establish communication links for the data transfer which gives the sensor network self-organizing ability, since thousands of sensor nodes may be densely scattered in a sensor field. 2) the second is effectively and fairly share communication resources between sensor nodes.

Physical Layer: This layer is responsible for frequency selection, signal detection, modulation, carrier frequency generation and data encryption [1]. It interacts with the MAC layer, performing transmission, reception and modulation. Error rate at physical layer is more and time varying in a wireless transmission, to detect and correct errors MAC layer will interact with physical layer [4].

Power Management Plan: How a sensor node uses its power is managed by power management plan [1]. If sensor power level is low, it stops participating in routing and broadcast the low power status to the neighbor [2]. To get duplicate messages sensor node may turn off its receiving message from neighbors [2].

Mobility Management Plan: Movements of sensor nodes are registered and detected by mobility management plan [2], [5]. Results route back to the user is maintained. So, that the sensor node can maintain records that balance their task usage and power.

Task Management Plan: It balances and schedule the sensing tasks to a specific region [5]. This task management plan is required for route data in a mobile sensor network, sensor node can work together in power efficient way and share resources between sensor nodes [2].

APPLICATIONS OF WIRELESS SENSOR NETWORKS

Overview:

Wireless sensor networks are widely used in controlling and monitoring different physical environments. The introduction of wireless sensors has reduced the physical presence of humans in monitoring several situations. Currently most of the sensors are compact, advanced and highly cost effective, which improved the availability of these sensors to anyone. People can easily buy these sensors and use to measure a variety of situations like temperature, motion, distance, acceleration, location, etc. [10]

Wireless sensor networks can be implemented in automation of various application like [11]

- Defense
- Environmental monitoring
- Logistics
- Human-centric applications
- Robotics.

WSN consists of sensor nodes that are responsible for collecting and processing the information and communicate with each other. These nodes are also called as mote which can be integrated with different devices, collect data from their environment and store the data for feature use. They form a network of sensors that are connected through Wi-Fi networks, Ethernet cables, Bluetooth, infrared and other means of connections [12]. These wireless devices connected to sensors communicate with each other on a real-time basis.

Wireless sensor networks are one of the best systems for gathering information to develop highly efficient and reliable systems. The data collected is transmitted to an individual or software application that analysis the data and take appropriate actions. Wireless sensor networks are flexible, cost effective and easy to implement which makes the sensor networks to develop innovative applications in different fields.

Technically wireless sensor networks can be implemented in any major application area. With the increased use of the wireless sensors at industrial level a lot of data is collected from different sources by the devices and processing all the data is one of the major constraint. Research is being carried out in developing technologies to overcome these the data processing limitations. WSN are going to be an integral part of the human lives in a lot of aspects and it's important to overcome the all the limiting factors that are existing.

To understand the applications of wireless sensor networks we should understand the different types of sensors and their application.

Classification of sensors.

Sensor Category	Parameter	Field-Readiness	Scalability
Physical	Temperature	High	High
	Moisture Content	High	High
	Flow rate, Flow velocity	High	Med-High
	Pressure	High	High
	Light Transmission (Turb)	High	High
Chemical	Dissolved Oxygen	High	High
	Electrical Conductivity	High	High
	pH	High	High
	Oxydation Reduction Potential	Medium	High
	Major Ionic Species (Cl-, Na+)	Low–Medium	High
	Nutrientsa (Nitrate, Ammonium)	Low–Medium	Low–High
	Heavy metals	Low	Low
	Small Organic Compounds	Low	Low
	Large Organic Compounds	Low	Low
Biological	Microorganisms	Low	Low
	Biologically active contaminants	Low	Low

Table1.classification of sensors

Image ref: APPLICATIONS OF WIRELESS SENSOR NETWORKS Antoine Bagula, University of Capetown.[13]

Here we can see the different categories of sensors, parameters, field readiness and scalability. If you look in to the categories, there are different kinds of sensors that can literally be used in a whole lot of applications and depending on the user requirement and compatibility of the device, these sensors can be configured with multiple devices and connected to a network to collect the data and report the information to the user to let them know the current situations.

Readiness for field deployment: measures maturity for field deployment in terms of economic and engineering efficiency. [13]

Scalability: A sensors scalability to distributed environmental monitoring tasks require that the sensors be small and inexpensive enough to scale up to man distributed systems. [13]

Cost: Sensors are deployed in thousands. It is expected that cost will drop but current generation sensors are still expensive to allow wide development. [13]

Applications of wireless sensor networks in Defense Surveillance:

The concept of wireless sensor networks is developed for the requirements in the defense sector to reduce the human involvement and automation of military applications.

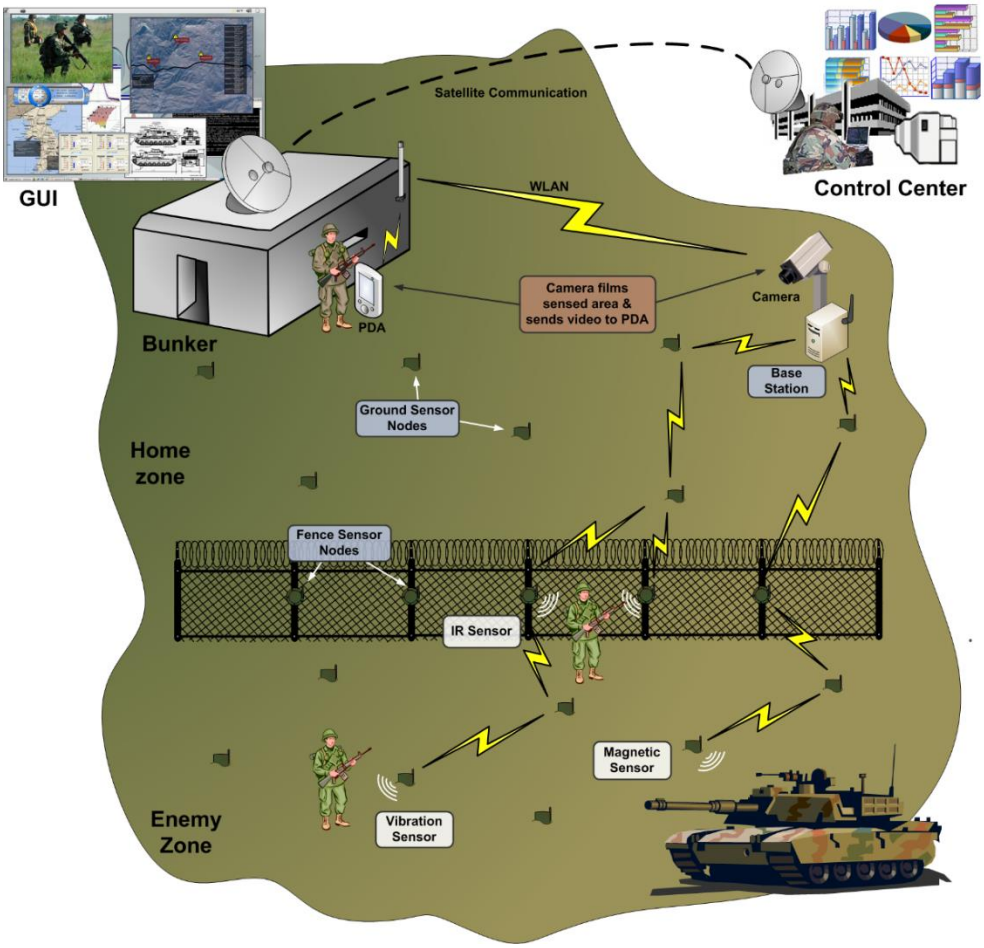


Fig3.Applications of WSN in Defense

There is huge potential for wireless sensor networks in the fields of security and surveillance. In military applications motes are mainly used in border surveillance, tracking and classification of enemy activities.

One of the important application of motes is motion detection using proximity sensors which can be used to monitor land mines that are considered dangerous for a human being to access. At present combat drones that are also known as unmanned combat aerial vehicles are popular in attacking the enemy base with no onboard pilot and real-time human control reduces the loss of human life. WSN applications can also be used in the regular operations like homeland security, border patrol, property protection etc. [11]

Wireless sensor networks in Robotic Applications:

Now a day there is advanced development in robotics. Robots are equipped with multiple sensors that can solve different problems humans face every day [11]. Wireless sensors play an important role in these robots by gathering the information, processing and providing output to the user. Robomote one of the kind of robot developed by USC renter for Robotics and Embedded systems to promote research in large scale sensor networks.

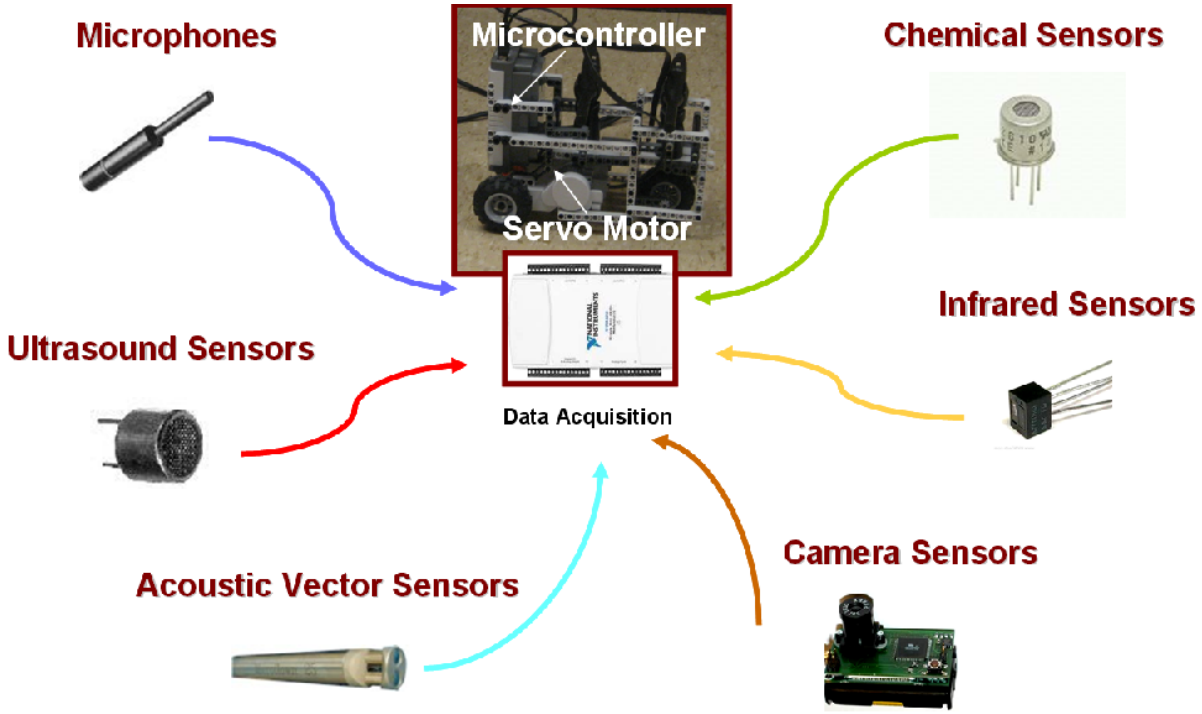


Fig4. Examples of robotic sensors

Examples of a robotic sensor are as following

- Microphones
- Ultrasound sensors
- Acoustic vector sensors
- Camera sensors
- Infrared sensors
- Chemical sensors

Each of these sensors have an individual functionality that perform various operations also can easily be integrated with other devices. These sensors are easy to produce and cost efficient. They can be programmed to perform certain actions with a particular time frame that help people to easily trace different actions and situations.

Monitoring the Environment using wireless sensor networks:

Environmental monitoring is one of the obvious applications of wireless sensor networks. For instance,

Air monitoring:

A good example for air monitoring is using air quality sensors for measuring the level of air pollution in major cities to let the people know the level of pollution and take proper measures to control air pollution.

Water monitoring:

A lot of government agencies are involved in monitoring the national waters to determine the water quality, finding problems like water pollution and pollution control efforts and responding to emergencies.

Some of the popular Example of Environmental monitoring are:

- Great Duck (bird observation on Grate Duck island)
- ZebraNet (studying wild life tracking systems)
- Glacier (glacier monitoring)
- Herding (cattle herding)
- Bathymetry
- Ocean (ocean water monitoring)
- Cold Chain (cold chain monitoring)
- Avalanche (rescue of avalanche victims)

Concept of Smart cities:

Many governments are bringing up the concept of smart cities that involves developing selected cities as smart cities. The objective of a smart city is meet the following objectives.

- Digitalizing the data in various government departments and government services.
- Developing smart infrastructure including smart roads, bridges and buildings installed with internet of things.
- Controlling the atmospheric pollution with is of the major threat to the health
- Organization of traffic in major parts of the city and control traffic mismanagement.
- Proper health care system using smart patient monitoring and hospital management.

Logistics Distribution architecture for Wireless network sensors:

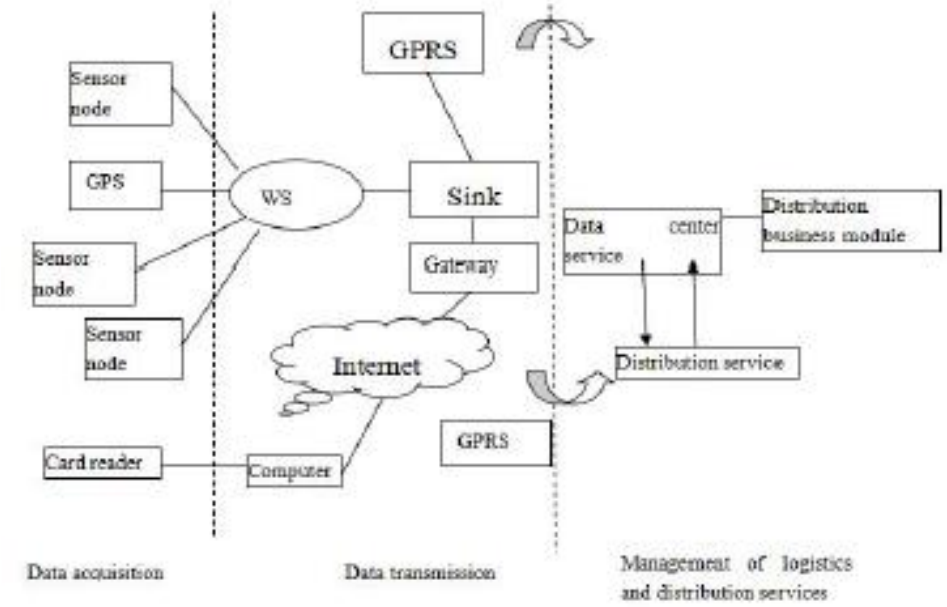


Fig5.Distribution architecture for WSN[18]

Wireless system Network architecture

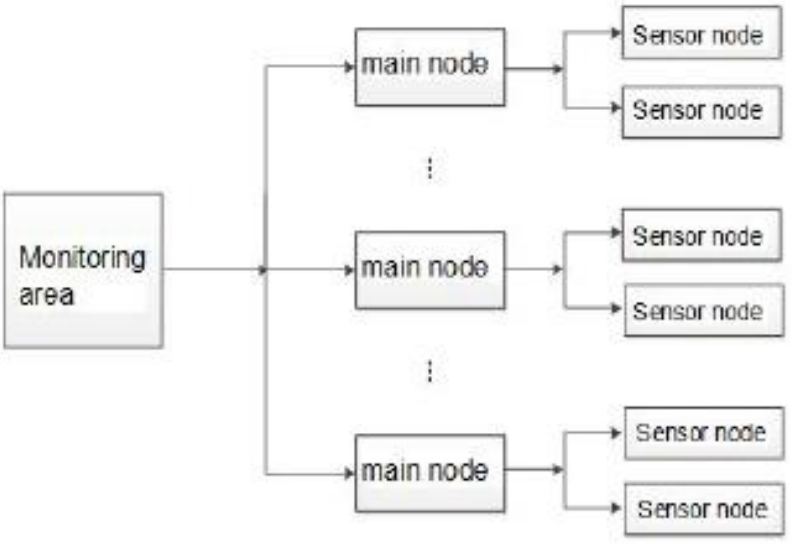
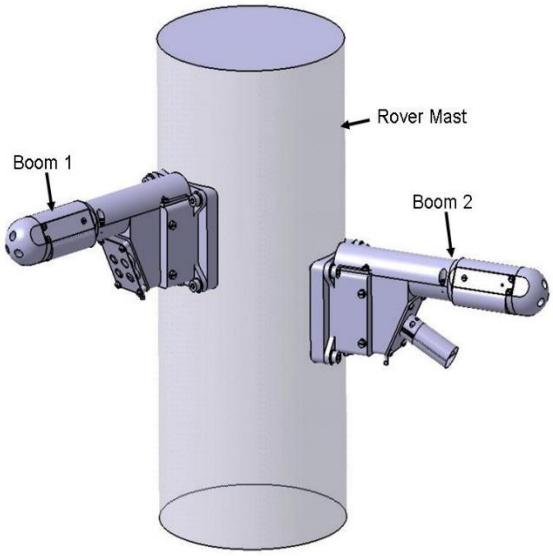


Fig6. WSN system architecture [18]

Wireless sensors in Space Research:

Curiosity is a robotic rover that is exploring mars to study the Martian atmosphere, surface, atmospheric pressure, humidity, ultraviolent radiation around the rover.

Rover Environmental Monitoring Station(REMS): [15]



Two small booms on the rover mast will record the horizontal and vertical components of wind speed to characterize air flow near the Martian surface from breezes, dust devils, and dust storms. A sensor inside the rover's electronic box will be exposed to the atmosphere through a small opening and will measure changes in pressure caused by different meteorological events such as dust devils, atmospheric tides, and cold and warm fronts. A small filter will shield the sensor against dust contamination. [15]

A suite of infrared sensors on one of the booms (Boom 1) will measure the intensity of infrared radiation emitted by the ground, which will provide an estimate of ground temperature. These data will provide the basis for computing ground temperature. A sensor on the other boom (Boom 2) will track atmospheric humidity. Both booms will carry sensors for measuring air temperature. [15]

This information shows how advanced the wireless sensor networks can be used to study the interplanetary atmospheres. These developments can make huge differences in space research and development of sustainable life on earth.

Security in WSN:

The WSN is an emerging new technology now a day due to its excellent capability in controlling environments and its numerous applications is making them to reach greater heights. There is lot of difference between wireless sensor networks and wired sensor networks. Coming to security of wired sensor networks it is good in a way and can be maintained by using some software's like firewall etc. But it's not same in the case of wireless sensor networks. The security of WSN's Is weak because the signals transmitted from WSN's is through air and can be easily manipulated or disturbed. But by following some techniques such as encryption we can manage to some extent. In this paper we are going to discuss about WSN's security vulnerabilities why they are caused and what are the counter measures to protect wireless sensor network from threats [21][22].

Need for security in WSN's:

As we already know that wireless sensor networks transmit through air and can be easily manipulated by attackers so we need lot of security in protecting the information without out being manipulated or changed. Apart from its applications and uses WSN's are to be timely monitored and taken care of. WSN security always seeks the following parameters they are

1. Confidentiality

2. Integrity

3. Authentication

4. Availability

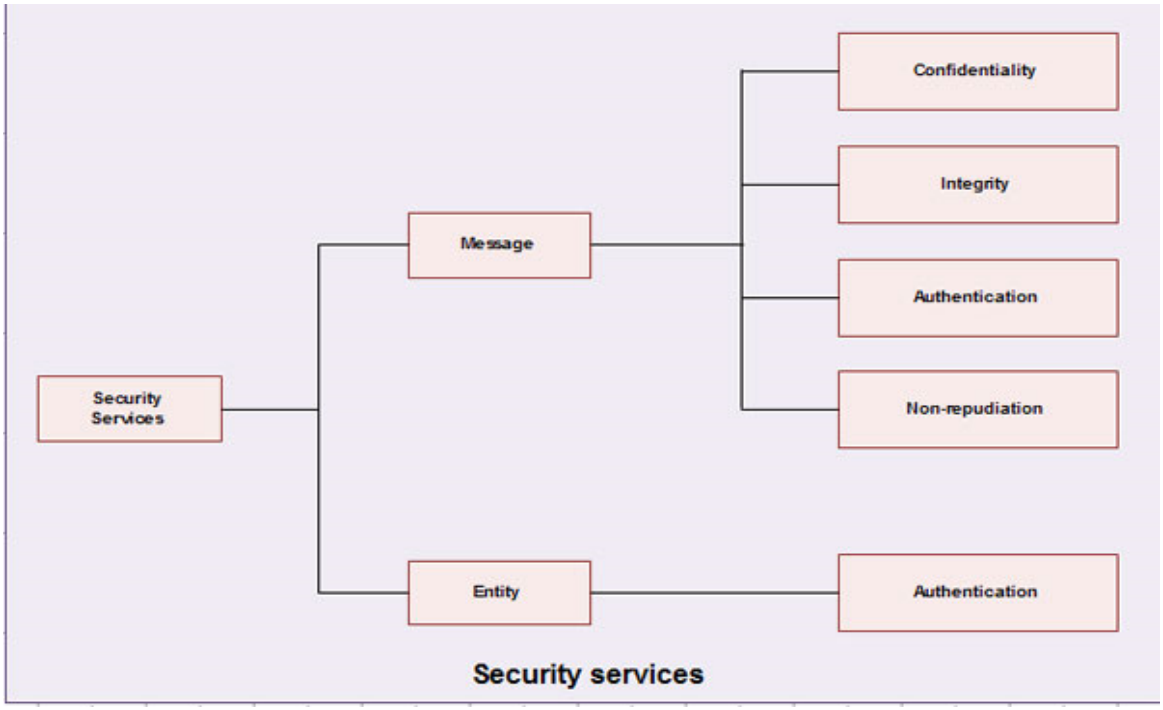


Fig8. Security services

1. **Confidentiality:**
   Confidentiality refers to whether the message is reached to authorized user. That means the wireless sensor networks shouldn't leak any information to unauthorized nodes [27].

2. **Integrity:**
   Integrity refers to the protection against injections or modification of messages. For every wireless sensor network, there should be integrity where it guarantees that data is not modified [27].

3. **Authentication:**
   By providing authentication only legitimate users can modify the messages and it determines whether the message is from original node which it claims to be and checks for the reliability of the messages [27].

4. **Availability:**
   Availability determines whether a node can use the resources which are available and to check whether the network is available for the messages to move on [27].

The WSN security is to be considered as most important aspect when compared to other networks because the communications occur through air using radio frequencies and WSN's have their own peculiarities such as

1.Limitations of energy resources

2.Deployment in an open environment where chances of getting attacked are higher

3.They maintain a close relation with physical environment and people [21].

- **security vulnerabilities related to wsn are as follows:**

- **Denial of service attack**

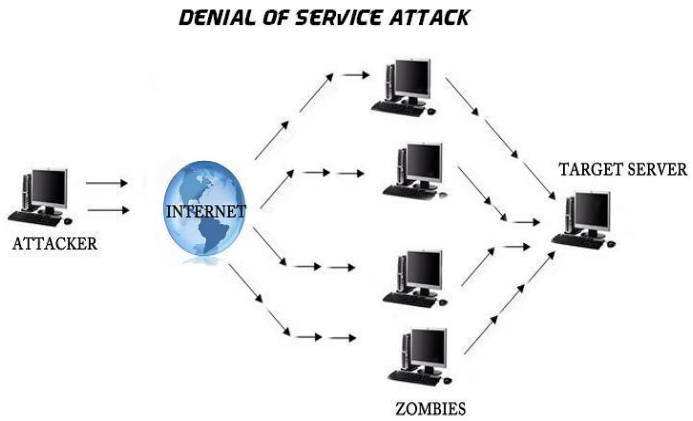


Fig9. Denial of Service Attack

In this attack the attacker makes the network and its resources unavailable for its user's. This is mainly caused by sending high energy messages or by over flooding messages or requests to the network which we are connected to [21]. This will mainly cause the network to temporarily unavailable for the user and it's a bad remark for the service provider in other words this condition is also called as jamming [21]. whenever we type a url in the browser that means we are sending a request to access that site to the site's server. If the attacker sends many messages or requests, then the server could be unable to process these many requests and denies our request. These attacks mainly depend on abusing of protocols such as extensible authentication protocol(eap) [22]. sometimes the attacker may send many spam messages and request and consume our space and eventually we are unable to get legitimate messages in return. Denial of service attacks can be performed at different layers. i.e. at physical layer, link layer and transportation layer at the physical layer the Denial of Service attacks could be jamming and tampering [23], at link layer dos may be in the form of collision, exhaustion, and at network layer the dos may be neglecting, misdirection, black holes and at transport layer this attack can occur due to malicious flooding attacks and resynchronizations [23].

- **Data aggregation attack:**

As WSN networks are used to send data to users, sometimes they are designed to send aggregated data rather than sending raw data of multitudinous volume. The collection of data and performing required operations are done by aggregator node. But this aggregator node may be a target to attackers as it has got entire information from other nodes. Attack may happen by way of sending false data to aggregator node, or attack on aggregator node physically or attacking aggregator node through some other attacks like DoS[21].

- **Traffic analysis attack**

In this attacker tries to find out traffic flow with in WSN and tries to influence the data. This attack is possible when attacker deduces topology of WSN network. This attack is possible in two ways rate monitoring and time correlated[30].

In rate monitoring attacker uses the concept of the closer the node to base station, the more packets it sends. In time correlation attack, the attacker monitors the time when a node sends data to base station and thus in any one of the above two ways attacker deduces the path to the base station[30].

- **Routing attacks:**

There are number of attacks that fall under routing attacks. Routing attacks is a kind of denial of service type attacks where router which is supposed to be relay packets instead It discards them.

The following attacks comes under routing attacks

- Black Hole Attack
- Selective forwarding attack:
- Wormhole attack
- Sinkhole attack

1) <u>Black hole Attack:</u>

Black hole effect occurs whenever a node falsifies the information related to router and if forces the data to pass by itself, after that it leads to an imaginary black hole in the network where nothing will be transferred [25]. Or whenever a malicious node, drops down the packets which was received from a neighbor node thereby resulting the packets not to get to its destination [26].

2) <u>Selective forwarding attack:</u>This attack is also by the malicious nodes inside the network. This type of attacks occurs whenever a malicious node drops packets on selected node instead pf passing them then this occurs [21]. Here in this attack a node plays the role of router and malicious nodes instead of forwarding certain messages they simply drop them on a selected node which meets the criteria [25].

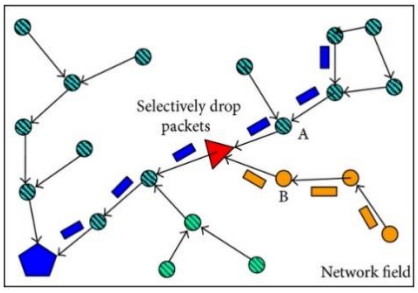


Fig10.selective forwarding attack

3) <u>Worm hole attack:</u>

In this effect the attacker tries to change the path of the network by creating a path which appears as best one. This type of attacks unleashes the other type of attacks such as black hole attack.

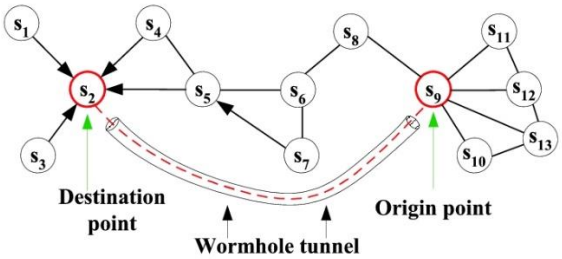


Fig11.wormhole attack

4) **Sink hole attack:**

This attack is occurred inside the network were an attacker falsifies information inside the node and performs the attack. In this attack mainly the node which is compromised attracts lot of traffic from the neighboring nodes and displays false routing updates.

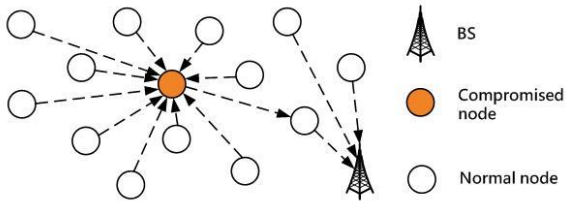


Fig12.Sinkhole attack

- **Ad-hoc networks:**

Ad-hoc networks are the networks which are the peer to peer networks wireless computers with no access points. ad hock networks are always open for attacks [22]. generally, encryption and authentication helps in providing security for ad-hoc networks.

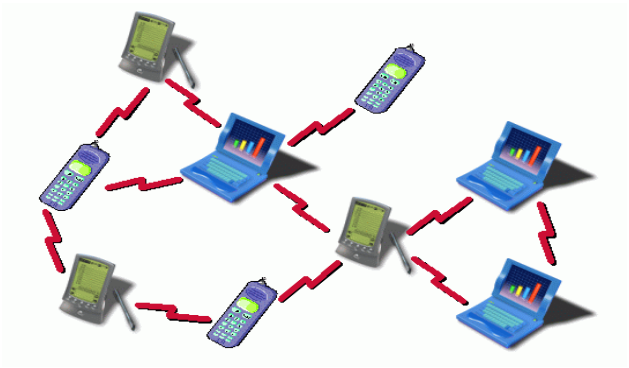


Fig 13. Ad-hoc networks

- **Sybil attack:**

Sybil attack is a type of security attack where a system is diverted by forging or presenting multiple identities which all are false [23]. This attack is named after a book Sybil which was written on

a woman who suffered from multiple personality disorder. Sybil attacks are mainly used against routing algorithms and maintenance of topology [27].

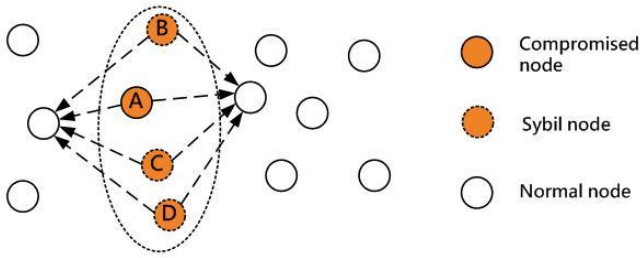


Fig14.Sybil attack

- **Counter measures for security attacks:**

I. **Counter Measures for Denial of Service :**

DoS can be counteracted by way of identifying the problematic areas i.e. where signals from other devices persists and analyzing the genuineness of those signals. Change of wireless access points if required. We can also use spread spectrum to handle jamming of signals. Spread spectrum is the technique of using messages with more bandwidth than the original message without losing the signal. This will prevent jamming [21].

II. **Counter Measures for Data Aggregation attack**:

It can be counter attacked through data encryption. A Secure –Enhanced Data Aggregation based on Elliptic Curve Cryptography (SEDA-ECC) is proposed for WSNs. In this the aggregation tree is divided into sub trees. Finally, Base Station verifies the aggregated result generated by sub trees [21].

III. **Counter Measures for Traffic analysis attack has two ways**:

Rate monitoring attack can be tackled by way of random forwarding of packets to non-parent nodes. So, attacker may not deduce base station. Time correlated attack can be tackled by way of making a node generate spurious packet when it neighbor node is sending packet to base station. So attacker is confused about the whereabouts of Base Station.

IV. Counter Measures for Selective Forwarding attack:

With the use of Encryption and analysis of application level traffic Making attacker confused about different types of traffic thus forcing the attacker to forward all traffic or none. use of Multipath routing can counter selective forwarding attacks [29]

V. Sybil attack counter measures:

As this attack happens by masquerading the identity of the node that attacker has compromised, this can be counter acted by way of cryptography. Sharing a unique key between every node and trusted base station. Two nodes can then use protocols like Needham-Schroder to verify others identity and establish a shared key [23].to tackle Sybil attacks techniques like radio resource technique are used [21]. By using identity certificates also, we can prevent this attack [29].

VI. Counter Measures to Warm Hole & Sink Hole attack:

These are very hard to identify when these attacks happen together. Geographic routing protocols are resistant to these attacks. These protocols construct a topology using local interactions and information without contacting base station [29].

Conclusion:

Wireless sensor networks are developing rapidly and are setting new standards in gathering data form multiple sources and processing the information. Motes play an important role in exchanging the processed information and communicate with other devices. These sensors are easy to produce and cost effective. Most of the times WSN operate automatically and communicate within a short range.

One of the major constraint for wireless sensor networks is energy consumption. Powering up all the sensors is often difficult and limits exploring all the possible benefits of the sensor networks. Research and development in energy management is required to improve the feasibility and better design of wireless sensor networks. Wireless sensor networks are more vulnerable to security attacks compared to wired networks. Security is another important area that needs to be improved.

The implementation of wireless sensor network is not just limited to computing devices these sensors can be used in every aspect of our daily life. In future more research is needed for expanding the application areas of wireless sensor networks. If we can overcome the design constraints in the application of wireless sensor networks and other limiting factors like energy efficiency and security, Wireless sensor network technologies are invincible.

References:

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: A survey,” *Computer Networks*, vol. 38, pp. 393-422, 2002.
[2] Kazi , R., *A Survey on Sensor Network*. JCIT, vol.1, issue 1. 2010
[3]Yick, Jennifier, Bishwanth Mukherjee, and Dipak Ghosal. "Wireless Sensor Network Survey." *Wireless Sensor Network Survey*. N.p., n.d. Web. 29 Oct. 2016.
[4] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J.D. Tygar, SPINS: security protocols for sensor networks, Proceedings of ACM MobiCom’01, Rome, Italy, 2001, pp. 189–199.
[5] Edwin Prem Kumar Gilbert, Baskaran Kaliaperumal, and Elijah Blessing Rajsingh. "Research Issues in Wireless Sensor Network Applications: A Survey." - Volume 2 Number 5 (Sep. 2012). N.p., n.d. Web. 04 Nov. 2016.
[6] Maraiya, Kiran, Kamal Kant, and Nitin Gupta. "Application Based Study on Wireless Sensor Network." International Journal of Computer Applications21.8 (2011): 9-15. Web.
[7] Heidemann, John, Wei Ye, Jack Wills, Affan Syed, and Yuan Li. "Research Challenges and Clustering." Underwater Acoustic Sensor Networks (2010): 1. Web.
[8]Yu, Xiaoqing, Petu Wu, Wenting Han, and Zenglin Zhang. "Overview of Wireless Underground Sensor Networks for Agriculture." N.p., 28 Feb. 2012. Web.

[9] Akyildiz, Ian F., Tommaso Melodia, and Kaushik R. Chowdhury. "Wireless Multimedia Sensor Networks." *Akyildiz/Wireless Sensor Networks Wireless Sensor Networks*(2010): 349-97. Web.

[10] Internet of Things: Wireless Sensor Networks This White Paper has been prepared by the Wireless Sensor Networks project team, in the IEC Market Strategy Board. The project team includes:Dr. Kang Lee, Project Partner, NIST Mr. Peter Lanctot, IEC Dr. Fan Jianbin, SGCC Dr. Hu Hao, SGCC Dr. Bruce Chow, Corning Incorporated Mr. Jean-Pierre Desbenoit, Schneider Electric Mr. Guido Stephan, Siemens Mr. Li Hui, Siemens Mr. Xue Guodong, Haier Mr. Simon Chen, SAP Mr. Daniel Faulk, SAP Mr. Tomas Kaiser, SAP Mr. Hiroki Satoh, Hitachi Prof. Ouyang Jinsong, ITEI China Mr. Wang Linkun, ITEI China Ms. Wang Shou, ITEI China Dr. Zhen Yan, Nari Group Corporation Dr. Sun Junping, China-EPRI Prof. Yu Haibin, SIA Dr. Zeng Peng, SIA Dr. Li Dong, SIA Dr. Wang Qin, University of Science and Technology, Beijing

[11] A Survey of Applications of Wireless Sensors and Wireless Sensor Networks

Th. Arampatzis, J. Lygeros, *Senior Member, IEEE,* and S. Manesis, *Member, IEE.*

[12] Wireless sensor network survey Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal *

Department of Computer Science, University of California, Davis, CA 95616, United States

[13] APPLICATIONS OF WIRELESS SENSOR NETWORKS Antoine Bagula, University of Capetown.

[14] Wireless Sensor Networks and Applications: a Survey Carlos F. García-Hernández†, Pablo H. Ibargüengoytia-González†, Joaquín García-Hernández†, and Jesús A. Pérez-Díaz*. †Electric Research Institute,(IIE), ITESM, Cuernavaca Campus, Mexico

[15] "Rover Environmental Monitoring Station (REMS)." NASA. NASA, n.d. Web. 05 Nov. 2016.
[16] A Survey of Applications of Wireless Sensorsand Wireless Sensor Networks
Th. Arampatzis, J. Lygeros, *Senior Member, IEEE,* and S. Manesis, *Member, IEEE*

[17] A Survey of Robotic Applications in Wireless Sensor Networks. Sam Shue. Electrical and Computer Engineering , University of North Carolina at Charlotte, Charlotte, NC James M. Conrad Electrical and Computer Engineering, University of North Carolina , Charlotte, NC
[18] Applications of wireless sensor network in the field of production and distribution.
Song Chuanzhen, Economic Management Institute, Shandong Women' University, Jinan, China
[19] Commercial Wireless Sensor Networks: Technical and Business Issues Vassileios Tsetsos, George Alyfantis, Tilemahos Hasiotis, Odysseas Sekkas, and Stathes Hadjiefthymiades *Communication Networks Laboratory, University of Athens, Dept. of Informatics and Telecommunications, Panepistimiopolis, Ilissia, Athens, Greece*
[20] Integration of Mobile, Big Data, Sensors,and Social Media:Impact on Daily Life and Business Mario GASTALDI*Evonue Digital, 16 Gold Coast Complex, Kalimaye Rd,Flic en Flac – Black River, 90508 Mauritius.*

[21] V. Ekong and U. Ekong, "A SURVEY OF SECURITY VULNERABILITIES IN WIRELESS SENSOR NETWORKS," *Nigerian Journal of Technology*, vol. 35, no. 2, p. 392, Apr. 2016.

[22] Min-kyu Choi1, Rosslin John Robles, Chang-hwa Hong, and Tai-hoon Kim. "Wireless Network Security: Vulnerabilities, Threats and Countermeasures." *Http://www.sersc.org/journals/IJMUE/vol3_no3_2008/8.pdf*.

[23] Gurudatt Kulkarni, Rupali Shelk, Kiran Gaikwad, Vikas Solanke, Sangita Gujar, and Prasad Khatawkar. " WIRELESS SENSOR NETWORK SECURITY THREATS In." *IEEE Xplore* -. N.p., n.d. Web. 29 Oct. 2016.

[24] Zheng Yue-Feng, Han Jia-Yu, Chen Zhuo-Ran, and Li Zheng. "A Novel Based-node Level Security Strategy in Wireless Sensor Network." 2012 International Conference on Information Management, Innovation Management and Industrial Engineering, n.d. Web.
[25] Mohamed-Lamine Messai. "Classification of Attacks in Wireless Sensor Networks." International Congress on Telecommunication and Application'14 University of A.MIRA Bejaia, Algeria, 23-24 APRIL 2014, n.d. Web.

[26] Daniel E. Burgner, and Luay A. Wahsheh. "Security of Wireless Sensor Networks." 2011 Eighth International Conference on Information Technology: New Generations, n.d. Web.
[27] Tanveer Zia, and Albert Y. Zomaya. "Security Issues and Countermeasures in Wireless Sensor Networks." Boukerche/Networks Algorithms and Protocols for Wireless Sensor Networks (2008): 479-502. Web.

[28] Di Ma, and Gene Tsudik. "Ma, Di, and Gene Tsudik. "Security and Privacy in Emerging Wireless Networks [Invited Paper." IEEE Wireless Communications 17.5 (2010): 12-21. Web." (n.d.): n. pag. Web

[29] Reema Sandhu. "Attacks in Wireless Sensor Networks and Security Measures." IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.6, No 2, Mar-Apr 2016 (n.d.): n. pag. Web.

[30] Kaushal, Kanchan, and Taranvir Kaur. "A Survey on Attacks of WSN and Their Security Mechanisms." International Journal of Computer Applications IJCA 118.18 (2015): 1-4. Web.