International Journal of Scientific Research and Engineering Development-– Volume 4 Issue 4, July- Aug 2021

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Application of wireless Sensor Network: A Review

Swati Bareth*, Uvika kujur**

*(Loyola college kunkuri, jashpur

swatibareth62@gmail.com)

**(Loyola college kunkuri, jashpur

uvikakujur666@gmail.com)

----------**********----------

Abstract:

In this modern era Wireless Sensor Network is in high demand. Wireless Sensor Network (WSN) is a widely used advanced technology of computer Network. Wireless Sensor Network occupies a number of nodes and these nodes can communicate among themselves using radio signals. Sensor is a device that responds and detects some input from environmental situation. It is not only sensing but also processing and communicating. It is also cheap in cost as compared to other traditional network. In this article we present a survey of security issues, advantages, characteristics in Wireless Sensor Network. We also highlight layer wise attacks and defense in Wireless Sensor Network

Keyword- **WSN, sensor, node, issues, defense.**

----------**********----------

I. INTRODUCTION

Wireless Sensor Network (WSN) is self organized and self healing sensor network which is consist large number of sensor node which is working independently. Sensor node is a node in sensor network that is capable of performing processing, gather sensor information and communicating with other node in network. WSN are being used in many areas like environmental situation monitoring, defense, forest monitoring, animal monitoring, smart building, health monitoring, automobiles etc. Today's sensors can monitor temperature, pressure, humidity, soil makeup, vehicular movement, noise levels, lighting conditions, the presence or absence of certain kinds of objects or substances, mechanical stress levels on attached objects, and other properties[1].Sensing is a technique used to collect information from physical or environment objects. An object performing such type of sensing task is called sensor. a sensor is a device that translates parameters or events in the physical world into signals that can be measured and analyzed[2].Nowadays sensors are tiny and low cost and don't need more power. Many wirelesses object get their power from batteries. In this modern era Wireless Sensor Network provide most popular services in industrial and commercial field.

II. ARCHITECTURE OF WSN

Wireless Sensor Networks are heterogeneous systems containing many small devices called sensor nodes. These networks will consist of hundreds or thousands of low cost, low power and self-organizing nodes [3]

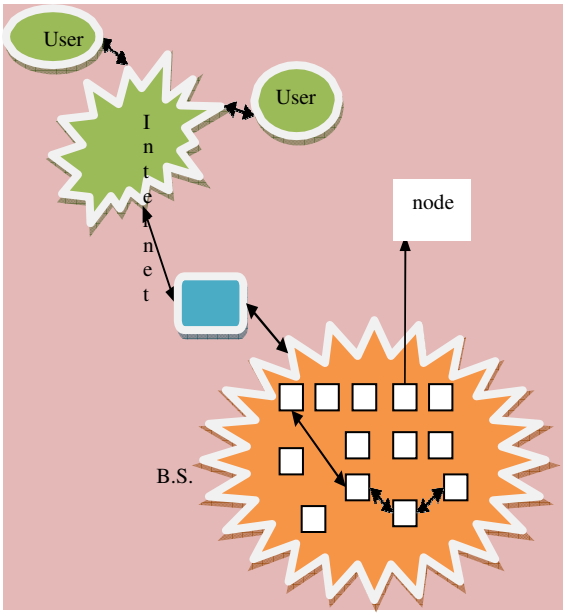


Fig:1 WSN architecture

The function of sensor node in a sensor area is to detect environmental situation or event than process and store the data and transmit it to Base Station for further processing. Base Station play very important role in wireless environment. It acts as a gateway between sensor node and users and it pass result to the user through internet.

The architecture of sensor node is shown in fig: 2. the sensor node architecture has five major components.

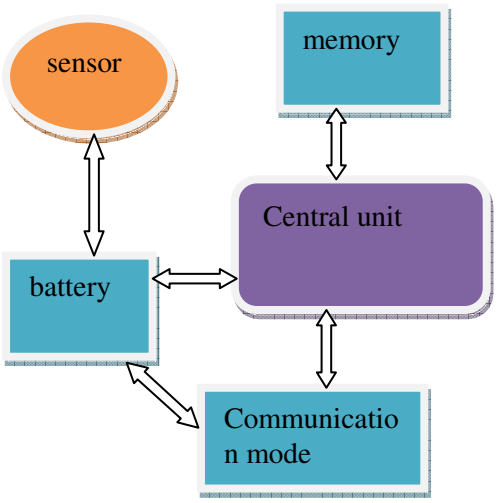


Fig: 2 Architecture of sensor node

1. Sensor: It gathers data from environment.
2. Battery: supply energy in all parts
3. Communication mode: communicate with environment
4. Microprocessor(central unit):it manage all tasks
5. Memory: store data.

III. KEY CHARACTERISTICS AND FEATURES OF WSN

APPLICATION

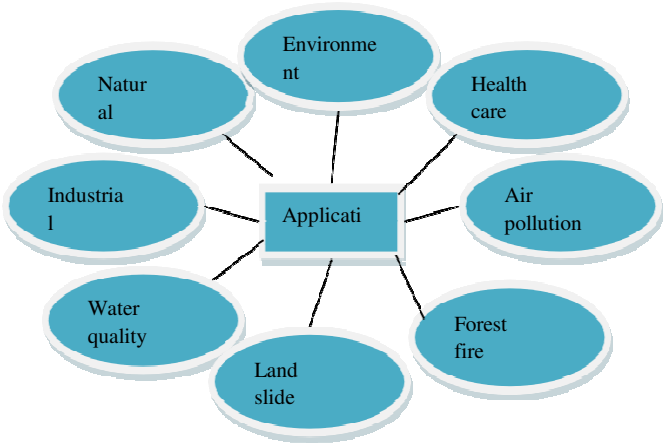
Wireless Sensor Network is helpful and useful for our society. There are various application of WSN and some wireless sensornetwork are monitoring air pollution, water quality, health care and prevent natural disaster and so on.

1. Environmental monitoring- It is common application of WSN. It allowed various physical parameters to be monitored in order to control. Ex.- in military it is use of sensors to detect enemy weapons.
2. Health care monitoring- Body sensor network systems can help people by providing health care services such as medical monitoring, memory

enhancement and communication with health care provider in emergency situation through GPRS or SMS etc .There are several types of sensor network it may be wearable, non wearable, environment embedded

3. Air pollution-air pollution serious impact on human health and environment. It requires worldwide awareness and conventional measurement. Traditional monitoring systems are costly and spatially restricted that's why it's become a challenging task. Wireless Sensor Network based system used low cost sensor and it collect air pollutant information in real time.
4. Forest fire detection-Forest fires are a natural or manmade in many parts of the world. It is mostly occure on summer season. It destroys not only forest hectares but also assets, properties. Forest fire monitoring using WSN has significance for many countries. In WSN based on cameras, fire detectors etc. this approach is aimed at detecting and verifying fire in forest.
5. Industrial monitoring-WSN technology has demonstrated for industrial, commercial and consumer applications specifically in process monitoring and control process data such as pressure, humidity, temperature, flow, level, density and vibration measurement can be collected through sensing unit and transferred wirelessly to a control system for operation and management.

Fig. 3 Application of WSN



6. Natural Disaster Prevention-Natural hazards have a variety of causes some are caused by climate like hurricanes and tornados. Others are caused by movement of tectonic plates like earthquakes and tsunamis. Wireless sensor networks utilize the technologies which can cause an for the immediate rescue operation to begin, whenever this disaster is struck.
7. Water quality monitoring-Water is important natural resources which needs constant quality monitoring for ensuring its safe use. WSN water quality control sensor responsible for sensing, data collection and process. WSN system is designed for monitoring some parameter that affect quality of water like ph, temperature etc.
8. Land slide detection-— Landslides have frequently occurred on natural slopes during periods of intense rainfall. Landslides have become one of the most significant natural hazards.

Characteristics of WSN	Advantages	Disadvantages
1. Power consumption constrainsfor nodes using batteries. 2. Deals with node failures. 3. Mobility of node. 4. Capability to withstand harshenvironmental condition. 5. Low cost 6. Simple in use 7.self organized and self healing8.cooperating	1.Enable long distance datacollection and transmission 2. It can predict natural disaster.3.protect hardware and data 4.It is flexible network so it canadopt to change 5. It has scale ability 6. useful to society 7. security	1. It is not fully secured hackers canhack the network. 2.It has short battery life 3.Communication speed is not veryfast 4. It is distracted by other wirelessdevices. 5. It can be accessed throughcentralized monitor.

IV. LAYER WISE ATTACKS AND DEFENSE IN WSN

WSN Layer	Attacks	Defense
PhysicalLayer	• Denial of Attacks	Priority message
	• Jamming	Spread Spectrum, mode change, Region mappingLower duty cycle
	• Tampering	Tamper proofing, Hiding
Data Link Layer	• Collision	Error correction code
	• Exhaustion	Rate Limitation
	• Unfairness	Small frame
NetworkLayer	• Hello Flood	Cryptography
	• Acknowledgementproofing	Bidirectional link Verification
	• Wormhole	Authentication , Link layer encryption
	• Sybil	Authentication, Encryption
	• Sinkhole	Authentication, Identification
	• Spoofed, altered routinginformation	Counter, Timestamps
	• Selective Forwarding	Multiple path
TransportLayer	• Flooding	Solving a Puzzle
	• Desynchronization	Packet Authentication
ApplicationLayer	• Sensory Overload • Path based	Sensor Sensitivity Authentication

1. **Physical Layer**- The physical layer is the first layer of the Open System Interconnection Model (OSI Model). The physical layer deals with bit-level transmission between different devices and supports electrical or mechanical interfaces connecting to the physical medium for synchronized communication.
    1. A Denial of Service attack makes a computer system or some other resource unavailable to legitimate users. For example if A send request to B and B send acknowledgement to A but A continuously sending request such that B is not available to communicate with others. Aim to block traffic that they identify as illegitimate and allow traffic that they identify as legitimate
    2. Jamming- Jamming in Wireless network is defined as disturbance of existing wireless communication by decreasing the signal to noise ratio at receiver's side. Jamming can both store and disrupt wireless
    3. Tampering- In this attack attacker extract sensitive information such as cryptographic keys and nodes may be altered or replaced by attackers.
    Tamper proofing physical packaging is one of the solutions. In tampering hide the memory content to prevent data.

2. **Data Link Layer**- It is second layer
4. layer is layer 3. The network layer is responsible for packet forwarding including routing through intermediate routers. Function of network layer is host addressing, of OSI model. This layer is protocol layer that transfer data between adjacent network nodes in WSN. It has two sub layer data link layer (DLL) and media access control (MAC). A main service of 1.DLL is encapsulation of data packets into frames 2. Frame synchronization 3. Error control 4. Flow control.
    1. Collision- When two nodes transmit data simultaneously on same frequency channel than collision occurs and collision change the content of package. Defense against collision is error correction code or use checksum method which corrects the error bit.
    2. Exhaustion- Attacker interrupts the channel by continuously transmitting something over it. This method keeps busy the channel and authorized users can't access or send data packet at the end starvation occurs.Rate limitation helps to ignore continues request and also save to exhaustion of energy during transmission.
    3. Unfairness-Attackers can degrade instead of preventing access to a service outright for gaining an advantage like other node miss there transmission deadline in real time Using small frame reduce the effect of these attacks.

3. **Network Layer** - the network

message forwarding.

1. Hello Flood- An attacker may use a high-powered transmitter to deceive a large area of nodes and it makes node to believe that

malicious nodes are neighbor node because attackers create illusion at the end unauthorized user access the channel.Cryptography is the solution of these types of attack.

2. Wormhole- The attackers keep eye on communication between two node then it replays information between the motes located far away physically by giving an illusion that they are very close to each other.[9] Using authentication or encryption we reduce this type of attacks
3. Selective Forwarding-An attacker may create malicious nodes which selectively forward only certain message and simply drop others [10]. Malicious node may send the messages to the wrong path so that it can create unfaithful routing information in the network. When malicious nodes may selectively forward packets to subsequent node and put the rest at the end we loss the important data. If all packets are dropped and none is forward than this attack is called black hole. Defense of Selective Forwarding is to use multiple paths for transmitting data.
4. Sybil- A single node copies itself and is presented in more than one location.
5. Attacker makes a malicious node which is more attractive to original node by forging routing information at the end the original node choose these nodes. This type of attack causes selective forwarding to be very
2. are reached a maximum limit Solution of this problem is to

simple because all traffic from a large area in the network will flow through the adversary's node.Using Authentication and identification we solve these types of attacks.

6. Acknowledgement Proofing- The acknowledgements of overheard packets can be spoofed by an adversary for particular nodes for providing false information to the neighboring nodes. Ex A send signal to B and not available the D send Acknowledgement instead of B after that communication establish between A and D now D can modify all the packet send by A.
7. Spoof, Altered or replayed Routing Information- Attacker may spoof, alter or replay routing information in network

5. **Transport Layer-** This layer provides host to host communication service for application t provides services such as connection-oriented communication, reliability, flow control, and multiplexing. The best-known transport protocol of the Internet protocol suite is the Transmission (TCP). It is used for connection- oriented transmissions, whereas the connectionless User Datagram Protocol (UDP) is used for simpler messaging transmissions [13].
   1. Flooding- Occurs when the attacker sends large number of request for establishing connection until the resources required by each connection

require each connecting client to evidence its dedication to

the connection by solving a puzzle [5].

3. Desynchronization- It refers to disconnection of established connection. The malicious node requires constant sending of requests for establishing connection from one or both nodes between which the connection is established. This way the established connection desynchronizes, and besides that,additional power is wasted on responding to the malicious node [11]

   Solution of this kind of attack is to use only authenticate packet when exchange packet between two sensor node.

6. **Application Layer-** An application layer is an abstraction layer that specifies the shared communications protocols and interface methods used by hosts in a communications network.[1]The application layer abstraction is used in both of the standard models of computer networking: the Internet Protocol Suite (TCP/IP) and the OSI model. It provide various services like telnet, ftp, tftp, smtp, dns etc.[12]

   1. Sensory Overload- Occurs when the attacker tries to overload the node by stimulating sensors which increase data traffic rate. We use Sensor sensitivity to overcome this type of attacks.
   1. Path Based-attack occurs when the attacker injects altered packets to end to end communication between two nodes. These packets are forward from base station that's why it consumes network bandwidth and energy of the node[11].Solution of this problem is to require good authentication.

SECURITY REQUIREMENT

Sensor network have to fulfill all requirement for providing a secured communication network. In WSN required securities are data confidentiality, integrity, data authentication, data freshness etc.

1. Data Confidentiality- Data should not be disclosed to any third party. Secrete data exchanged and store in WSN must not be reveal to the third party person.. data confidentiality is very necessary for WSN. In this method it encrypts data and use shared key so that only authorized receivers can get sensitive data. That's way it is very necessary in WSN.
2. Integrity- Data integrity ensures that the message will not be altered during communication. It also ensures data received at destination node must be same as that sent by the source node. It is very important in context of secured data.
3. Data Authentication-In data authentication sensor node ensures the receivers data has not been modified during transmission and also ensure the attackers cannot change w hole packet by injecting additional packets and also allow a receiver to verify that the data really sent by authorized sender. If it is not present than many unauthorized user access our sensitive data.
4. Data Freshness- Data freshness

checks that the data is new and updated. Because it's possible the attackers can resend the copy of old measurement data or a previous data. So it is able to detect and discard old data.

5. Attacks-WSN bears various types of attacks and also prevents sensitive data from attackers.
6. Availability- The availability of nodes is available in network when they need to fulfill the functionality of network. Attackers attempt to ruin this property[6]
7. Scalability- It is an important issue because network topology of WSN is dynamic in nature that is new node can be added for extending the network size.

V. CONCLUSION

In this paper we explain about WSN features and application scenarios. In this paper our main strategy is against attackers who act against secure network. They drain off energy of node and also stole sensitive data. This report studies various aspects associated with layer wise attacks and also study various defense mechanism that exist in WSN and these defense mechanisms are very important in future for upcoming researches. It also guide to develop new security schemes for WSN.

VI. REFRENCES

[1] Pathan S.K.,Lee H.W. and Hong C.S , Security in Wireless Sensor Network: Issues and Challenges, ICACT ,ISBN 89-5519-129-4,FEB 2006.

[2]Mohammad A.E, Elrazik S., and El-bakry H.M., Challenges in Wireless SensorNetwork,IJAR .

[3]Singla A.and Sachdeva R. , Review on Security Issues and Attacks in Wireless Sensor Network,, International journal of Advanced Research in Computer Science and Engineering(IJARCSE) VOL-3 ISSUE-4, APRIL 2013.

[4]https://www.google.co.in/search?q=characteristics+of+wireless+sensor+network&[20/11/2019].

[5] https://www.elprocus.com/architecture-of-wireless-sensor-network-and-applications/[20/11/2019] [5] https://journals.sagepub.com/doi/full/10.1155/2014/303501[23/11/2019]

[6] Rehana J. , Security of Wireless Sensor Network ,TKKT -110.5190 seminar on internetworking 2009.

[7] Singh G. Security Attacks and Defenses Mechanism in Wireless Sensor Network: A Survey, IJISET, VOL-3, ISSUE-4, April 2016

[8] https://en.wikipedia.org/wiki/[27/11/2019]

[9]Chawla H.,Kaur H, and Kaur C. , Review on Security Issues in Wireless Sensor Network, International Journal of Current Engineering and Technology, Vol-6, june-2016.

[10] Wang Y. , Ramamurthy B and Attebury G. , A Survey of Security Issues in Wireless Sensor Networks, IEEE Communications Surveys and Tutorials, Vol-8, No.2 , 2006.

[11] file:///C:/Documents%20and%20Settings/compaq/Desktop/cyber/wireless/attak2.htm[19/11/2019]

[12] https://en.wikipedia.org/wiki/Application_layer[28/11/2019]

[13] https://en.wikipedia.org/wiki/Transport_layer[28/11/2019]

