# Secure Wireless Sensor Network

Shrishti Sao
Bhilai Chhattisgarh

Sunil Kumar Sahu
Assistant Professor, Department of CSE
Parthivi College of Engineering & Management
Bhilai, Chhattisgarh

Umesh Kumar
Department of Computer Science & Engineering
Parthivi College of Engineering & Management
Bhilai, Chhattisgarh

***Abstract*— Today WSN (Wireless Sensor network) is most challenging field for research due to its low power processing and associated low energy.WSN is widely used in the area of remote monitoring, Sustainability, Industrial Measurements, Air/Climate Water/Soil, Indoor Monitoring, Power system, Solar, Wind Farm, Structural Monitoring, Machine Monitoring and Process Monitoring. In this paper we deal with the application and security of the wireless sensor networks and hope that work will help users to provide the security in the area of wireless sensor network.Keywords-component; formatting; style; styling; insert (key words)**

## I. INTRODUCTION

Wireless sensor networks have seen wonderful advances and operation in the past two decades. Starting from petroleum searching, mining, weather and even fight operations, all of these want sensor applications. One basis behind the growing fame of wireless sensors is that they can job in remote areas without manual interference.

Everybody needs to do is to gather the data sent by the sensors, and with certain analysis extract important information from them. Generally sensor applications engage many sensors deployed together. These sensors form a network and work together with each other to gather data and throw it to the base station. The base station acts as the control centre where the data from the sensors are gathered for additional analysis and dealing out. In a nutshell, a wireless sensor network (WSN) is a wireless network containing of spatially dispersed nodes which use sensors to monitor physical or ecological circumstances. These nodes combine with routers and gateways to create WSN System. The WSN is made of nodes which is connected to single or several sensors.

The basic components of a node are given below-

1) Sensor and actuator - A border to the physical world planned to sense the environmental parameters like pressure and temperature.
2) Controller – it is used to control dissimilar modes of operation for processing of data.
3) Memory – It is used as storage for programming data.
4) Communication –It is a device similar to antenna for transfer and receipt of data over a wireless channel.
5) Power Supply- It is a supply of energy for soft operation of a node similar to battery.

## II. LITERATURE REVIEW

**Communication Protocol**

Wireless sensor networks use layered architecture like wired network architecture [10]. Characteristics and functions of their each layer is given below in fig 2.

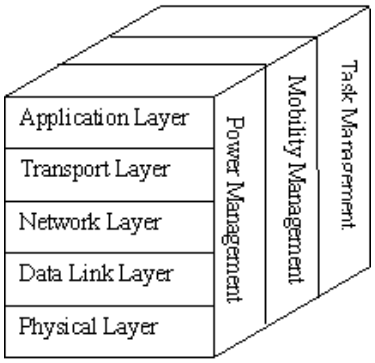


Figure 1 Layered Architecture of WSN

*A* *Physical Layer*-The objective of physical layer is to increase the reliability by reducing path loss effect and shadowing. This layer is responsible for established connection, data rate, modulation, data encryption, signal detection, frequency generation and signal detection.

*B* *Data Link Layer*-The objective of Data link layer is to insure interoperability amongst communication between nodes to nodes. This layer is responsible for error detection, multiplexing. Prevention of Collision of packets, repeated transmission etc.

*C* To secure data link layer, Karlof et al [2] proposed link layer security architecture “TinySec” for wireless sensor networks. Naveen Sastry et al[4] proposed Zigbee or the 802.15.4 standard for hardware based symmetric key encryption.

*D* Some researchers also proposed the possible use of public key cryptography [3, 9], secure code distribution [8] to create secure key during network deployment and maintenance.

*E* *Network Layer*-The objective of Network layer is to find best path for efficient routing mechanism. This layer is responsible for routing the data from node to node, node to sink, node to base station, node to cluster head and vice versa.

*F* The LEACH and PEGASIS are the protocols which describe the techniques to save the energy consumption (power of sensor) so as to improve the life of sensors. LEACH gives cluster based transmission while PEGASIS is chain protocol [5, 6]. WSN use ID based protocols and data centric protocols for routing mechanism. In WSN, each node in the network acts as a router (because they use broadcast mechanism), so as to create secure routing protocol. Encryption and decryption techniques are used for secure routing [8].

*G* *Transport Layer*-The objective of Transport Layer is to establish communication for external networks i.e. sensor network connected to the internet. This is most challenging issue in wireless sensor networks.

*H* *Application Layer*-The objective of Application Layer is to present final output by ensuring smooth information flow to lower layers. This layer is responsible for data collection, management and processing of the data through the application software for getting reliable results.

*I* SPINS (Security Protocols in sensor Networks)[9] provides data authentication, replay protection, semantic security and low overhead. SPIN has two secure building blocks SNEP and µTESLA. SNEP provides baseline security primitives: Data Confidentiality, two party data authentication and data freshness. µTESLA provides authentication broadcast for severely resource constrained environments. Localized Encryption and Authentication Protocol (LEAP)[9] is a key management protocol for sensor networks. It provides multiple keying mechanisms (Group Key, Cluster Key, Pairwise Shared Key) in this regard.

Some attacks are given in table 1.

Table1: WSN layers, Attacks and the existing protocols.

| WSN Layer | Types of attacks | Existing protocols |
|---|---|---|
| Physical Layer | Denial of service attack | |
| Data Link Layer | Denial of service attack | Link Layer security protocol (TinySec, PEGASIS, LEACH) |
| Network Layer | Denial of service attack, Wormholes, Sinkholes, Sybil attacks. | Routing protocols (ID based, data-centric) |
| Transport Layer | Denial of service attack | |
| Application Layer | Malicious Node | Aggregation scheme |

## III. APPLICATION OF WSN

There is some important application of Wireless Sensor Network-

1. Area Monitoring: It is a general application of WSNs. Here the WSN is deployed over a area where a number of event is to be monitored. A army example is the utilize of sensors to finding opponent intrusion. When the sensors spot the event being monitored, the event is reported to one of the stand stations. Similarly, wireless sensor networks may use a choice of sensors to sense the presence/absence of vehicles ranging from motorcycles to train cars.
2. Environmental Monitoring: Wireless sensor networks have been deployed in several states to monitor the attention of unsafe gases for people. It can also be used to decrease the temperature and moisture levels inside greenhouses.
3. Medical Application: Sensor networks may also be largely used in fitness care centers. In some current hospital sensor networks are planned to supervise patient physiological data, to decrease the drug administration path and monitor patients and doctors inside the hospital.
4. Structural monitoring**:** Wireless sensors are used to monitor the society within large buildings and communications like tower, underground architecture, crowd area etc.
5. Traffic Monitoring: The sensor node has a built-in magneto-resistive sensor that measures changes in the Earth's magnetic field caused by the survival or passing of a vehicle in the nearness of the node. By insertion of two nodes some area apart in the way of traffic, specific individual vehicle speeds can be measured and reported.
6. Habitat Monitoring: The close connection with its instant physical surroundings allows each sensor to give localized measurements and full report which is difficult to obtain through conventional instrumentation.

Below fig shows some application areas of WSN.

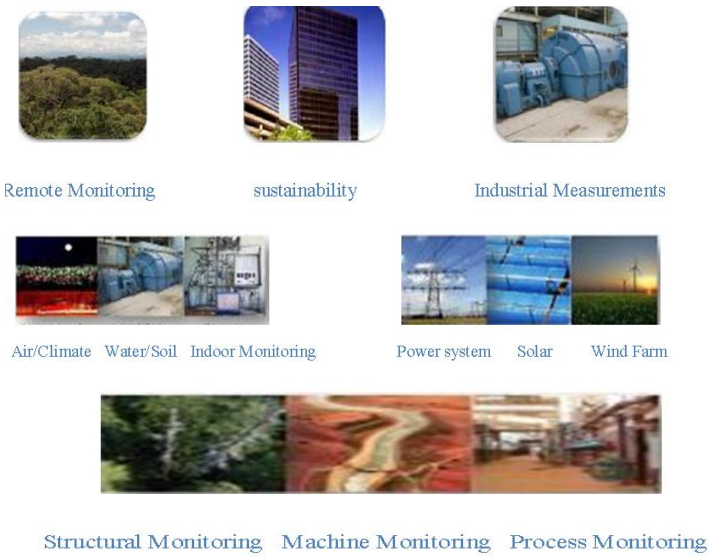


Figure 2 WSN Application Areas

**Sensor Network application classes**

A *Environmental data collection*- At the network level, the environmental data collection application is eminent by having a huge number of nodes incessantly sensing and transmitting information back to a set of connected base stations which accumulate the information using traditional methods. These networks usually need very low data rates and strongly long lifetimes. In typical usage situation, the nodes would be evenly dispersed over an outside surroundings. The distance among neighbour nodes will be least yet the distance across the whole network will be realistic.

After operation, the nodes must first find out the topology of the network and estimate most favourable routing methods. Now it may then be used to route the information to a middle group points. But it is not required to set up the nodes for optimal routing strategies on their own in green monitoring applications. Instead, it may be probable to calculate the best routing topology exterior of the network and then communicate the required information to the nodes as required which is probable because the physical topology of the network is moderately constant.

B *Security Monitoring*- Our second set of sensor network application is security monitoring. Security monitoring networks are built of nodes which are located at set locations throughout an environment that constantly control one or more sensors to spot an anomaly. Dissimilarity between security monitoring and ecological monitoring is that security networks do not gather any data or information. This become to a important impact on the best network architecture. Every node repeatedly check the position of its sensors but it only transmit a data report when there will be a security contravention. The instant and reliable message conversation among the alarm messages is the system's major requirement. These are the report generated by exception networks.

Additionally, it is vital that it is validated that each node is still present and working. If a node is disabled, it will stand for a security violation that must be reported. Basically for security monitoring, the network should be created so that nodes are responsible for ruling the position of each other. We have one move towards where each node is assigned to peer that will report if a node does not work. The best topology of a security monitoring network will seem quite different from that of a data group network.

Once detected, a security violation should be communicated to the linked station straight away. The latency of the information communication crossways the network to the base station has a strict impact on application presentation. Generally most of users demand that alarm conditions should be reported within seconds of discovery. So that the network nodes should be able to react readily to requests from their neighbours to forward data.

C *Node tracking scenarios* -A third usage situation commonly analyzed for wireless sensor networks is the tracing of a tagged object through a area of space guarded by a sensor network. There are a variety of conditions where one would like to mark out the location of important assets. Current control systems try to road objects by recording the last checkpoint which an object passed through. But, these conventional systems it is not simply possible to determine the object's present location. For example, UPS tracks every shipment by scanning it with a barcode whenever it passes through a routing mechanism.

## IV. ATTACKS ON WSN AND THEIR MITIGATION

There are some kinds of attacks in WSN, let's see one by one in detail.

A *Denial of service*-After this type of attack, the resultant resources are become unavailable to their intended users. As an example node X sends request to node Y for communication and node Y sends acknowledge to node X but X keeps on sending request to Y continuously. Due to this result Y is unable to communicate with any other nodes in the network and thus becomes unavailable to all of them in that network.

This type of attacks may be prevented by identification mechanisms powerful authentication and.

B *Attack of information in transit*- In wireless sensor networks usually each node reports changes to a cluster head or base station only for data above some threshold. Information in transit may be altered, replayed, spoofed, again or vanished. In this type of attack attacker has large communication range high processing power and.

Attack of information in transit may be prevented by data aggregation and authentication techniques.

C *Sybil attack*- In this attack the attacker gets illegally multiple identities on one node. By this, the attacker mostly affects the routing mechanism.

These types of attacks are generally prevented by validation techniques.

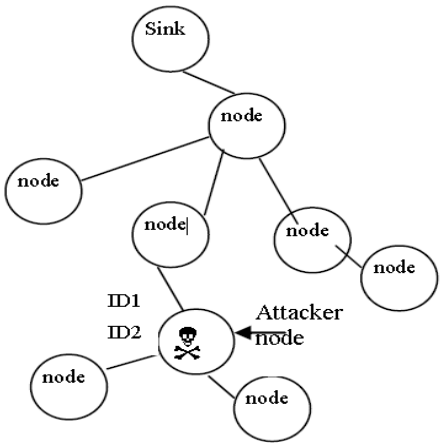


Figure 3 Sybil Attack

D *Black hole/ Sinkhole Attack*:- In Black hole/Sinkhole attack, generally attacker places himself in a network with high capability resources by which it always creates

shortest path. As a result, all data passes through attacker's node.

*E* *'Hello flood' Attack*- Basically Hello flood is one of the simplest attacks in WSN, i.e in which attacker broadcasts HELLO packets with high transmission power to sender or receiver. The receiver node receiving the messages and assume that the sender node is nearest to them and sends packets by this node. Due to this attack, congestion may occur in the network. This is a specific type of DOS. To avoid such kinds of attacks, Blocking techniques are used.

*F* *Wormhole Attack*-In Wormhole type of attack, tunnelling mechanism is used by the attacker to establish himself between sender and receiver by confusing the routing protocol.

## V. CONCLUSION

Wireless sensor networks have seen wonderful operation in the field of petroleum searching, mining, weather and even fight operations; all of these want sensor applications. WSN is most challenging research area; this paper gives overview of wireless sensor networks, their application and security issues and their corresponding solutions. We hope that this work will help users and research scholar in the field of wireless network to secure Wireless Sensor Network.

## REFERENCES

[1] Gunnar Gaubat, Jens-Peter Kaps, Berk Sunar, "Public Key Cryptography in Sensor networks- Revisited", Book Series Lecture Notes in Computer Science Pages 2-18, 11 january 2005.

[2] Jan Steffan, Ludger Fiege, Mariano Cilia Alejandro Buchman,"Scoping in Wireless Sensor Networks", 2nd workshop on middleware for pervasive and Ad-Hoc Computing Toronto, Canada,2004 ACM 1-58113-951-9.

[3] Chris karlof, Naveen Sastry, David Wanger, "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks", Proceedings of the 2nd international conference on Embedded networked sensor systems,November 3-5, 2004, pages 162- 172,Baltimore, Maryland, USA. ISBN:1-58113-879-2.

[4] Al-Sakib Khan Pathan, hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", Feb 20-22, 2006 ICACT2006.

[5] Woo Kwon Koo, Hwaseong Lee, Yong Ho kim, Dong Hoon Lee, "Implementation and Analysis of New Lightweight Cryptographic Algorithm Suitable for Wireless Sensor Networks", International Conference on Information Security and Assurance,2008.

[6] M. Ding, D. Chen, K. Xing, and X. Cheng. Localized fault-tolerant event boundary detection in sensor networks. In Proceedings of IEEE INFOCOM 2005,2005.

[7] F. Koushanfar, M. Potkonjak, and A. Sangiovanni-Vincentelli. Fault-tolerance in sensor networks.In Handbook of Sensor Networks. CRCpress, 2004.

[8] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehaviour in mobile ad hoc networks. In MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking, pages 255–265, New York, NY, USA, 2000. ACM Press.

[9] Perrig, R. Szewczyk, V. Wen, D. E. Culler, andJ. D. Tygar. SPINS: security protocols for sensor netowrks. In Mobile Computing and Networking, pages 189–199, 2001.

[10] Abhishek Pandey, R. C. Tripathi A Survey on Wireless Sensor Networks

Security International Journal of Computer Applications (0975 – 8887)

Volume 3 – No.2, June 2010

[11] K. Akkaya, M. Younis, "A Survey of Routing Protocols in Wireless Sensor Networks," Elsevier, Ad Hoc Network Journal, 3 (3): 325- 349, 2005.

[12] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "A Survey on Sensor Networks," IEEE Communications Magazine, 40(8): 102-114, 2002.

[13] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless Sensor Networks: A Survey," Computer Networks, 38(4): 393-422, 2002.

[14] C.Y. Chong, S.P. Kumar, B.A. Hamilton "Sensor Networks: Evolution, Opportunities, and Challenges," Proceedings of IEEE,

91(8):1247-1256, 2003.

[15] W. Du, R. Wang, and P. Ning, "An Efficient Scheme for Authenticating Public KeysSensor Networks," MobiHoc '05 Proc. 6th ACM Int'l. Symp. Mobile Ad Hoc Net. and Comp., New York:ACM Press, pp. 58–67, 2005.

[16] C.P. Fleeger, Security in computing, 3rd edition, Prentice-Hall Inc. NJ. 2003.

[17] A. Perrig et al., "SPINS: Security Protocols for Sensor Networks," Wireless Networks, vol. 8, no. 5, pp. 521–34, Sept. 2002.

[18] K. Dasgupta, K. Kalpakis, and P. Namjoshi. "An Efficient Clustering-based Heuristic for Data Gathering and Aggregation in Sensor Networks". Wireless Communications and Networking (WCNC 2003). IEEE, Volume: 3, pp.16-20, March 2003.

[19] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. First IEEE Int'l. Wksp. Sensor Network Protocols and Applications, , pp. 113–27, May 2003.

[20] J. Newsome et al., "The Sybil Attack in Sensor Networks Analysis and Defenses," IPSN '04: Proc. IEEE Int'l. Conf. Info. Processing in Sensor Networks, Apr. 2004.

[21] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks," Proc. IEEE INFOCOM 2003, Apr. 2003.

[22] D. K. Goldenberg, J. Lin, A. S. Morse, B. E. Rosen, and Y. R. Yang. Towards mobility as a network control primitive. In Proceedings of the 5th ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc 2004, Roppongi Hills, Tokyo, Japan, May 24–26, 2004, pp. 163–174