# Security in wireless sensor network: A Survey

**Rekha Rani, Research Scholar, Department of Computer Science, Desh Bhagat University, Mandi Gobindgarh, India, rekha_nskalra@yahoo.co.in**

**Dr. Harmaninderjit Singh, Assistant Professor Desh Bhagat University, Mandi gobindgarh, India, jeetsinder@gmail.com**

**Abstract: - A Wireless Sensor Network (WSN) is a network created by a group of sensor nodes to sense physical environment such as light, pressure, heat etc. Wireless Sensor Network (WSN) are regarded as a revolutionary information gathering method to build the information and communication system which will greatly improve the reliability and efficiency of infrastructure systems. In these systems, wireless tiny sensor nodes are installed on application area and monitor the parameters critical to each area's efficiency based on a combination of measurements such as vibration, temperature, pressure, and power quality. Data are gathered from various nodes hence security becomes vital in WSNs. More ever in Wireless Sensor Network due to low processing power, small size memory, small power resource and due to the use of insecure wireless communication channels. Security in Wireless Sensor Network becomes a challenge. In this paper we exhibit a study of security issues in WSNs.**

***Keywords:- WSN, Security, Threats, Authentication, Encryption, Data Integrity***

## I. INTRODUCTION

"A Wireless Sensor Network (WSN) contains a mass of temperate, lightweight, battery-worked multifunctional sensor nodes". Wireless Sensor networks are equipped in field for social concern of information or checking environment for a selected area. Sensors nodes are thoroughly vigor obliged, since it isn't realistic to displace the batteries of an extensive number for sensor nodes, so that is the key test in sensor framework gets the chance to open up the life span of sensor nodes. The energy efficiency must be to outline the detecting, computing and correspondence protocols. Another issue is the safe communication between sensor node and base station. A small research work has been done in wireless sensor network security. A sensor node comprises of three units- detecting unit, microcontroller (CPU) and radio unit.

A WSNs can be installed in both inside and outside, various sensor frameworks will inclined to be passed on in open, physically slight, or even threatening circumstances where nodes work together is an unambiguous possibility that depending upon the arrangement stage. To give security in wireless sensor networks should be mixed and confirmed based confidence model to handle the issues outside the limit of cryptographic security. It is basic to keep unapproved customers from tuning in, deflecting and disappointing accumulated data by the sensor, and impelling the distinctive organization attacks against the network. A protected controlling tradition expects a significant part to deal with any strike for authentic working of the network. Purpose of the examiner is to develop the sensor with ease, low power usage and multifunctional sensor nodes. WSNs can altogether enhance structure design and process, as the earth being checked and not require the correspondence or imperativeness establishment associated with wired networks [1].

Wireless sensor network, as a developing system advances, have risen gradually recently. They can acquire a parcel of detailed and reliable information in the network circulated region anyplace; so the WSNs are generally utilized as a part of different regions like as "military protection, industry, horticulture, development and urban administration, biomedical and natural checking, open wellbeing and antiterrorism, perilous and hurtful territorial remote control", etc. [2]

## II. RELATED WORK

Andhe Dharani ,et. al [3] a analysis the vulnerabilities at major OSI layers of Wireless Sensor Networks with the related threats. they mainly focused on the security performance of clustered protocols analysis with capable resource utilization. Shipra Suman et. al[4] have classified the WSN attacks as active and passive attacks and defined these attacks. At last they conclude, WSNs are very expose to the attacks as the sensor nodes are deployed in a unfriendly and unsafe location. They have present a tabular classification of these protocols against the attack. Mohamed Lamine Messai [5]present security challenges in Wireless Sensor Networks, which different from the ad hoc networks with more severe restrictions in terms of energy, computation capabilities and communications. Shahriar Mohammadi et. al[6] Discussion WSNs' physical attacks with their characteristics, Classification and comprehensive comparison of these attacks to each other, protect against

 DOI : 10.18231/2454-9150.2019.0058 

outside attackers at layer using encryption and authentication mechanisms they also defined encryption is not enough and inefficient for inside attacks and system-class attackers. Poonam Barua et. al[7] have discuss various security threats on at different layer of Wireless Sensor Network protocol stack and outlined their Possible solution against each threats. Rajkumar et.al[8] introduced sensor networks, its related security problems, threats, risks and characteristics. S.Nithya et.al[6] discussed WSNs their risk, security, threats etc. troubles attach to it.[9]

## III. CHARACTERISTICS OF WIRELESS SENSOR NETWORKS

Characteristics keeping the utilization of traditional security scheme in WSNs are summarized below.

3.1.1. **Large Scale**. General applications of WSNs require geographical scope of huge ranges [10]. Number of nodes in WSNs may exceed several thousand [11].

3.1.2. **Limited Resources**. Prerequisite that WSNs must be with low establishment and operation cost requires that sensor nodes ought to have straightforward equipment. Thus, operation and correspondence assets in WSNs are constrained. For instance, one of the non specific sensor types, TelosB, has 16-bit8Mhz processor, 48KB main memory, and 1024KB flash memory. Each convention must be outlined taking into account constraints in processor limit, memory and radio communication [10].

3.1.3. **Redundancy**. As a result of node repetition, every event is identified by the different sensor nodes on the network and hence builds the measure of information to be exchanged over it. In other words, repetition builds the measure of information sent to the base station and reductions the life span of the arrange [10]. To dispose of information repetition information, clustering protocol are utilized.

3.1.4. **Security**. WSN applications, for example, military systems, agriculture monitering medical monitoring systems, are exceptionally delicate in wording of security. Because of the restricted assets of the sensor nodes, conventional security instrument ts can't be utilized as a part of WSNs. Thus, the security techniques of WSNs should be planned considering restricted resources and malicious sensors [10].

## IV. SECURITY REQUIREMENTS

For secure communication, Wireless Sensor network provide some requirements. According to Woo A. ,et. al and , Sohrabi, K. et al. [12][13] availability, confidentiality, integrity and authentication. Are common security requirements of Wireless sensor network. Which is known as primary requirement [14][15] source localization, data freshness, self organization are secondary requirements of wireless sensor network which provide the security at the time of data transmission in wireless sensor network [16].

**Data Authentication:** Data authentication is a process to confirm that the sensor node is actual sensor node or falsification node. Verification is important for receiver sensor node to check verification that received data is the data is coming from an authenticated sensor node.

**Data Availability:** It means that the data or services are available for any time in the network even in case of Denial of service like attacks.

**Data Integrity:** Data integrity means, data should not be modified or altered both at the part of sender and receivered including communication. An attacker can change the data as per their need.

**Data Confidentiality:** In wireless sensor network, at the time of communication data flows in number of nodes according to routing algorithm so there is many chances to use data by the attackers [17]. So encryption techniques are used to provide data confidentiality.

**Self-Organization:** [16] Wireless sensor network is a unstructured network mostly in hostile location in which infrastructure are not fixed so it a great challenge to maintain security in Wireless Sensor Network. There is necessity of each node having different situations properties individually, self organizing, self maintaining and self healing properties.

**Source Localization:** For data transmission some applications use location information of the sink node. It is important to give security to the location information. Non-secured data can be controlled by the malicious node by sending false signal strengths or replaying signals.

**Data Freshness:** It means that all messages transmitted in the network fresh and new. For communicating with fresh data, it is necessary to avoid old data replaying by each node.

## V. THREATS AND ATTACKS IN WSNS

### A. Performer-Oriented Attacks

There are two types of Performer oriented attacks [18] [19].

#### Outside Attacks

Outside attacks may cause passive extra bogus packets so that to resource extortion and to produce congestion.

#### Inside Attacks

Inside attackers mostly destroy or disturb the network as the attacker can catch the knowledge about the encryption and decryption security codes and can be modified, change routing, change packet data, etc.

### B. Goal-Oriented Attacks

#### Passive Attacks

A sort of attacks an attacker is mainly interested in monitoring the unencrypted traffic and communication so that to gain the encryption keys and sensitive information

 DOI : 10.18231/2454-9150.2019.0058 

used in other types of attack as well as decrypt the weak encrypted traffic [20].

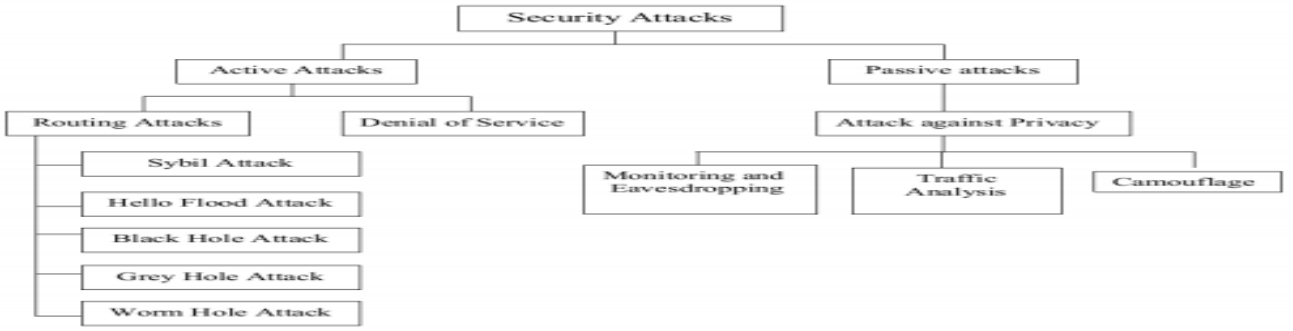
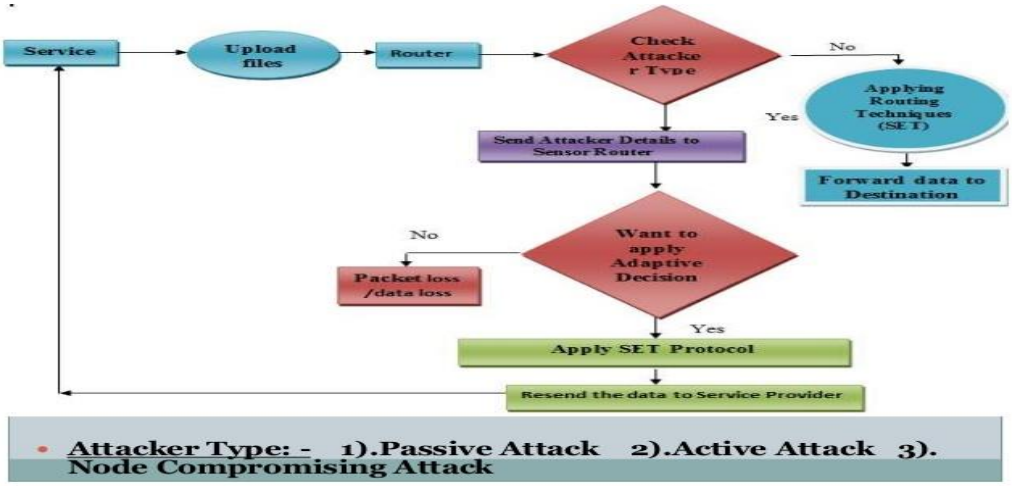



Fig. Security Attacks [4]

**Active Attacks**

An attacker gets the sensitive information `and alter it so that it may be of no use for the other or make it according to their own desire [21].




**C. Layer-Oriented Attacks**

This section identifies the vulnerabilities and threats in each Open Systems Interconnection (OSI) layer.

| OSI Layer | Types of Attack |
|---|---|
| Physical layer | Jamming, Tampering |
| Data link layer | Collision, Eavesdropping, Resource exhaustion, Traffic analysis |
| Network layer | Spoofing, black hole/ Sink holes, Sybil attacks, Denial-of-service (DoS), Wormholes Flooding, Hello Flood Attack |
| Transport layer | Injects false messages, Energy drain attacks |
| Application layer | False data injections, Attacks on reliability |

**Fig. Types of network layer attacks [22]**

**Physical Layer Attacks**

Jamming of the communication channel and node capturing is one of the major issues in physical layer attacks in WSNs [23]. This sort of attacks is too difficult to control as in this an attacker can jam the entire communication channel by sending high energy signals in the appropriate territory, which result Denial-of-Service to this layer.

**Data Link Layer Attacks**

As this layer protocols provide a framework how to access shared channel. An attacker sends a NAKC to the sender node so it can retransmit the data so that the energy of the node is wasted, or may deduct the sensitive data even if the data is cannot be decrypted [23].

**Network Layer Attacks**

DoS, sinkhole attacks Spoofed, Transformed, or Reiterated Routing Information are the most direct attacks against a routing protocol in any network are Network Layer attacks.

**Transport Layer Attacks**

An attacker may repeatedly engage the legitimate nodes with itself so that their resources are exhausted.

 DOI : 10.18231/2454-9150.2019.0058 

**Application Layer Attacks**

An attacker might devastate network nodes, causing network to forward huge volumes of traffic to a base station. This attack devours network bandwidth and sinks nodes energy.

## VI. CONCLUSION

Security is the big challenge in the sensor network. WSN are utilized today as a part of antagonistic situations, shopping centers, doctor's facilities, house machines and armed forces to do various types of employments, which make its security level to swing from low to high. Sensor nodes exchanges data with different nodes regularly in very short intervals using wireless link and in communication an attacker can affected the data. So security is the big challenge in the sensor network. In the paper we have discuss various Characteristics, security requirements of Wireless Sensor Networks. We have also discuss various attacks that are possible in WSNs. However, lots of open issues still remaining to be explored.

## REFERENCES

[1] D. Estrin et al., *"Instrumenting the World with Wireless Sensor Networks,"* Proc. Int'l. Conf. Acoustics, Speech and Signal Processing, Salt Lake City, UT, May 2001.

[2] Parli B. Hari, Dr. Shailendra Narayan Singh*," Security Issues in Wireless Sensor Networks: Current Research and Challenges"* 978-1-5090-0673-1/16/$31.00 ©2016 IEEE.

[3] Andhe Dhar, Manjuprasad, Shantharam Nayak, Vijayalakshmi *"Performance Analysis of Cluster Based Protocols in Sensor Networks and their Vulnerabilities"* International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 4, April 2015 ISSN (Print): 2320-9798.

[4] Shipra Suman, Shubhangi "*A Survey On Comparison Of Secure Routing Protocols in Wireless Sensor Networks*" International Journal of Wireless Communications and Networking Technologies Volume 5, No.3, April – May 2016 ISSN 2319 – 6629.

[5] Mohamed-Lamine Messai *"Classification of Attacks in Wireless Sensor Networks"* International Congress on Telecommunication and Application APRIL 2014.

[6] Dr. Shahriar Mohammadi1 and Hossein Jadidoleslamy *"A COMPARISON OF PHYSICAL ATTACKS ON WIRELESS SENSOR NETWORKS"* International Journal of Peer to Peer Networks Vol.2, No.2, April 2011

[7] Ms. Poonam Baru , Mr. Sanjeev Indora "*Overview of Security Threats in WSN "* International Journal of Computer Science and Mobile Computing A Monthly Journal of Computer Science and Information Technology ISSN 2320–088X IJCSMC, Vol. 2, Issue. 7, July 2013, pg.422 – 426

[8] Rajkumar, Sunitha K R, Dr.H.G.Chandrakanth, "A *Survey on Security Attacks in Wireless Sensor Network"*International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue4, July-August 2012, pp.1684-1691.

[9] S .Nithya, Dr.C.Gomathy *"An Investigation on Security Attacks in Wireless Sensor Network"* International Journal of Pure and Applied Mathematics Volume 119 ,2018, pages 927-935 ISSN: 1314-3395 (on-line version).

[10] M. Meghdadi, S. Ozdemir, and I. Guler, *"Security in wireless sensor networks: problems and solutions,"* International Journal of Information Technologies, vol. 1, pp. 35–40, 2008.

[11] D. W. Carman, P. S. Krus, and B. J. Matt, *"Constraints and approaches for distributed sensor network security,"* Tech. Rep. 00-010, NAI Labs, Network Associates, Inc., Glenwood, Md, USA, 2000.

[12]. Woo, A. and Culler, D., *"A Transmission Control Scheme for Media Access in Sensor Networks"*, Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking, MobiCom, Rome, Italy, 2001.

[13]. Sohrabi, K., Gao, J., Ailawadhi, V., and Pottie, G. J., *"Protocols for Self-Organization of a Wireless Sensor Network"*, IEEE Personal Communications, pp. 16-27, 2000.

[14]. W. Xu, W. Trappe, and Y. Zhang, *"Channel Surfing: Defending Wireless Sensor Networks from Interference",* in Proc. Of Information Processing in Sensor Networks, 2007.

[15]. Khan, F., & Nakagawa, K. (2012). "*Performance Improvement in Cognitive Radio Sensor Networks"*. in the Institute of Electronics, Information and Communication Engineers (IEICE) , 8.

[16]. Parno, B., Perrig, A. and Gligor V., *"Distributed Detection of Node Replication Attacks in Sensor Networks",* Security and Privacy, 2005 IEEE Symposium , DOI: 10.1109/SP.2005.8.

[17]. Khan, F., Bashir, F., & Nakagawa, K. (2012). "*Dual Head Clustering Scheme in Wireless Sensor Networks"*. in the IEEE International Conference on Emerging Technologies (pp. 1-8). Islamabad: IEEE Islamabad.

[18]. W. Xu et al., *"The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks,"* MobiHoc '05: Proc. 6th ACM Int. Symp. Mobile Ad Hoc Net. and Comp., pp. 46–57, 2005.

[19]. Shih, E., Cho, S., Ickes, N., Min, R., Sinha, A., Wang, A. &Chandrakasan, A., *"Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks",* Proceedings of the 7th Annual International Conference on Mobile Computing and Networking, Rome, Italy, pp. 272-287.

[20]. Chris Karlof and David Wagner, *"Secure routing in wireless sensor networks: attacks and countermeasures,"* Ad Hoc Networks Journal, Vol.1, Issue 2-3, pp. 293-315, 2003.

[21]. Yan Sun, Zhu Han, and K. J. Ray Liu, *"Defense of Trust Management Vulnerabilities in Distributed Networks,"* IEEE Communications Magazine, Vol 46, Issue 2, pp.112-119, 2008.

[22] Manjuprasad B, Andhe Dharani," Necessitate for Security in Wireless Sensor Network and its Challenges", International Journal of Research in Computer Applications & Information Technology, ISSN Online: 2347- 5099, Volume 1, Issue 1, pp. 21-25, July-September, 2013.

[23]. David R. Raymond and Scott F. Midkiff, *"Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses"*, IEEE Pervasive Computing, Vol. 7, No. 1, pp. 74-81, 2008.

 DOI : 10.18231/2454-9150.2019.0058 