# Study of Wireless Sensor Networks its Security Issue, Challenges and Security Management

Suwarna Gothane [1], Dr. M. V. Sarode[2], Dr. K. Srujan Raju[3]

[1]CMR Technical Campus, Hyderabad, India
Email: gothane.suvarna@gmail.com
[2]Jagadambha College of Engineering and Technology, Yavatmal, India
Email: mvsarode2013@gmail.com
[3]CMR Technical Campus, Hyderabad India
Email: ksrujanraju@gmail.com

**Abstract—** Wireless Sensor Network (WSN) is promising topic of technical, social, and economic importance. The sensing technology combined with processing power and wireless communication makes it rewarding for being exploited great quantity in future. The inclusion of wireless communication technology also incurs various types of security threats. Meanwhile, supplying privacy and security is an inseparable part of this technology. Without providing enough security, the promising benefits of this flourishing technology will be misused and worthless. In this paper we investigate the security related issues and challenges in wireless sensor networks. We identify the security threats, review proposed security mechanisms for wireless sensor networks. We also discuss the holistic view of security for ensuring layered and robust security in wireless sensor networks.

***Keywords—Wireless Sensor Network, Security in WSN, Security Management.***

## I. INTRODUCTION

A sensor is a device that measures a physical quantity and converts it into a signal which can be read by an today mostly electronic instrument. In a sensor network, many tiny computing nodes called sensors are scattered in an area for the purpose of sensing some data and transmitting data to nearby base stations for further processing. A sensor node, also known as a mote. Node in a wireless sensor network can perform gathering sensory information, some processing, and communicating with other connected nodes in the network. The transmission between the sensors is done by short range radio communication. The base station is assumed to be computationally well-equipped whereas the sensor nodes are resource-starved. Each of these scattered sensor nodes has the capabilities to collect data and route data back to the base station. Data are routed back to the base station by a multi-hop infrastructure-less architecture through sensor nodes.

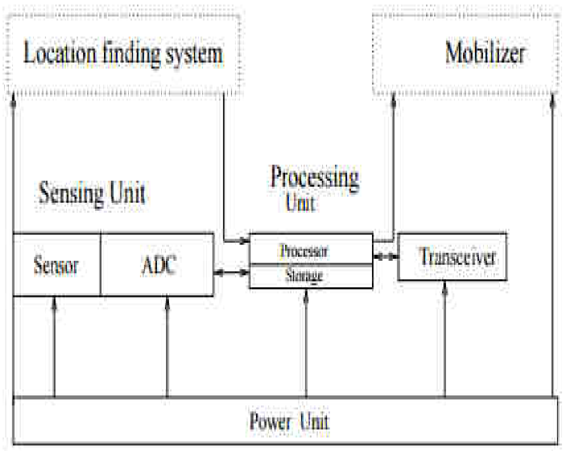

Figure: The components of a sensor node.

Due to adhoc nature and resourse limitations of sensor network providing aright key management is challenging[1].Wireless Sensor Networks (WSN) are emerging as both an important new tier in the IT ecosystem and a rich domain of active research involving hardware and system design, networking, distributed algorithms, programming models, data management, security and social factors [2], [3], [4].Application of wireless Sensor networks offer economically viable solutions for a variety of applications. For example, monitor factory instrumentation, pollution levels, freeway traffic, and the structural integrity of buildings. Other applications include climate sensing and control in office buildings and home environmental sensing systems using various sensors for temperature, light, moisture, and motion. Sensor networks are key to the creation of smart spaces, which embed information technology in every day home and work environments. Common application area covers military applications, environmental monitoring, classroom/home, health and habitat monitoring, detecting and monitoring car thefts, vehicle tracking and detection etc.

## II. SECURITY ISSUES IN WIRELESS SENSOR NETWORK

**Need of Security:**

Sensor nodes are limited in power, computation capacities as well as memory. Sensor nodes are densely deployed. Sensor nodes are prone to failures. The topology of a sensor network may change frequently. Sensor nodes do not have global identification (ID) because of the large amount of overhead and larger number of sensors. Sensor nodes mainly use broadcast communication paradigm Routing protocol plays vital role in security of Wireless sensor Network. Routing protocols are used to transfer information between the nodes. Sensor nodes can easily capture and attacker node can easily listen and change the data on channels. There is need to establish route between source to destination and transmit that information through air so any attacker hacks that information and sends incorrect information to destination node. Wireless sensor network architecture Network layer of is highly insecure and unreliable. There are various security issues in network layer of WSN.

Several issues for security are key management in Wireless Sensor Networks, user authentication in Wireless Sensor Networks, Access Control in Wireless Sensor Networks, Access Control in Wireless Body Area Sensor Networks, Key Agreement in Mobile Ad Hoc Networks, security in Vehicular Ad Hoc Networks. The number of nodes in a sensor network can be several orders of magnitude higher than the nodes in an ad hoc network.

Routing protocol routes the data from source to destination. So Energy efficient secure routing means we routes packet from source to destination in minimum energy with considering security as an extra parameter.

General security requirements are:

**Authentication:** Data authentication allows a receiver to verify that the data really is sent by the claimed sender. Authenticating other sensor nodes, cluster heads, and base stations before granting a limited resource or revealing information is major security requirement in wireless network sensor.

**Integrity:** Integrity refers to the ability to confirm the message has not been tampered or altered while it was on the network. An opponent is not just limited to modifying the data packet. It can change the whole packet stream by injecting additional packets. So the receiver needs to ensure that the data used in any decision-making process originates from the correct source. Integrity ensures that message or the entity under concern is not altered.

**Confidentiality:** It is the ability to hide message from a passive attacker and is the most important issue in network security. Sensor nodes may communicate highly sensitive data, such as key distribution, so it is extremely important to build a secure channel in a WSN. Moreover, sensor identities and public keys should also be encrypted to some extent to protect against traffic analysis attack. It provides privacy of the wireless communication channels to prevent eavesdropping.

**Availability:** Availability is of importance for maintaining an operational network. It is the ability of a node to make use of the resources and the network is available for the message to move on. Ensures that the desired network services are available even in the presence of denial of service attacks.

**Non-repudiation:** It is issue of preventing malicious nodes to hide their activities.

**Authorization:** It ensures that only the sensor nodes those who are authorized can be involved in providing information to network services.

**Freshness:** It ensures that data contents are recent and there no replay of any old content. This requirement is especially important when there are shared-key strategies employed in the design and need to be changed over time.

## III. SECURITY THREATS AND ATTACKS

Most of the threats and attacks in WSN are similar to the traditional network. Due to broadcasting nature of WSN it is more vulnerable. There are different types of attack [3] against the WSN. Wireless Sensor Networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Basically attacks are broadly classified in two categories i.e. active attacks and passive attacks [5].

**Denial of Service**:

The DOS attack tries to busy the available resource by the victim node by sending extra unnecessary packets.DOS attacks disrupt, destroy and also block the services network. Prevention from the DOS attack requires strong authentication and identification of traffic.

**Attack on information in transit:**

The information during transit may be altered, spoofed, replayed again. This node provides wrong information to sink node.

**Sybil attack:** In WSN Sensor nodes works by dividing their task into subtasks and redundancy of information. In this state node can represent to be more than one node is known as Sybil attack.

**Blackhole attack:**

In this type of attack a malicious node represent as black hole to attract all the traffic in the sensor network. Once malicious node inserts into the network it disturb with packet passing between them.

**Wormhole attack:**

Wormhole attack is one of the critical attacks. In this type of attack attacker records the packet at one location and tunnel those to another location. In this attack no need to compromise a sensor node.

## IV. SECURITY TECHNIQUE IN WIRELESS SENSOR NETWORKS

Security services in WSNs are needed to protect the information and resources from attacks. Security requirements in WSNs include availability, authorization, privacy, authentication, anonymity, resilience, confidentiality**,** integrity and flexibility. There are different security techniques available in WSN.

### 4.1. Cryptography Techniques:

Conventional network uses cryptography technique for security purpose. It includes techniques like symmetric cryptography, asymmetric cryptography which are mostly applicable in wired networks. Cryptography techniques [6] contain encryption and decryption methods. Cryptography techniques are not to be applied directly on wireless sensor network due to limitations of tiny sensor nodes which contain small memory, limited power battery and lack of processing. Encryption scheme requires extra energy, extra processing time. In WSN applying encryption the result is increasing delay, jitter and packet loss and one of major issue in WSN is key management problem.

**4.2. A Minimum Hop Routing Technique:** Home security [7] is an application of minimum hop routing technique. Data routing protocol [7] specially designed for a wireless home security network. Life of such a network depends entirely on the lifetime of the battery power. Protocol select as metrics parameters hop counts and battery power levels. Purpose is to conserve energy as possible in both computations and data communications. When some nodes fails or run out of battery then network will not interrupt and find the alternative path. Shao-Shan Chiang presents an energy-efficient, reliable and robust routing algorithm for wireless sensor networks. In this approach flood the packet for establishing the routing table for every node in the network this is take place before actual data transmission. Routing table contains parameters like child, parent, sibling node with identification and energy level within one hop distance. Every node having routing table based on that find best next hop node, which has highest energy level to forward the message. A system model contains base station, sink node and number of WSN nodes. Base station can be located in any space in the house. Sink node is specially designed with more memory compare to other nodes. Sink node connected to base station via wire or wireless links. A sensor deployed in the house and covers the radio range. During the communication sink node takes commands from the base station and floods the packet to the sensors nodes. A sensor node also collects the data from other sensor nodes and passes to the base station .Except sink node all nodes are battery powered. There are two phases are used one is routing table establishment and second is data routing phase. In 1st phase flooding technique is used to establish routing table. In 2nd phase routing table remains unchanged until any node failure occurs or a new node is added. Once routing table built data packets to the destination. Finally Shao-Shan Chiang presented an energy-efficient routing scheme for the wireless sensor network used in home security systems**.** System is reliable and robust. Quickly adapt change by updating the routing table and resending packet via new path. Energy consumption is very low. Security cost contains cryptography cost, monitoring cost and processing cost and which is time based.

### 4.3. Steiner Based Secure Multicast Routing Protocol

Multicast protocols for WSNs focus on how to deliver data packets, but none of them take the security into account. When WSN is working in the battle area or some hospital field, the security is one of the key questions in sensor networks [8]. In particular, the data transmitted between nodes should have three great characteristics: confidentiality, integrity and authentication. In order to satisfy security requirements and control of energy consumption, Steiner-based Hierarchical Secure Multicast Routing Protocol (SHSMRP) for wireless sensor network combines the idea of Steiner tree and cluster network topology, which is scalable and energy efficient for large group communications in WSN. Furthermore, the protocol adopts secure communication mechanism to ensure the data integrity, security and verifiability[8].

This protocol includes the following five phases:

1) Nodes information gathering phase
2) Steiner tree construction phase
3) Steiner sub-trees distribution phase
4) Data delivery phase
5) Steiner tree maintenance phase

A. Nodes information gathering phase

In order to join the network, each node first gets location information by some location services, and then sends the join message to source node S including the location information. The source node should verify each node in order to prevent the malicious node to join in the network. The authentication of each node is checked by pre-shared key.

B. Steiner tree construction phase: The source node S begins to construct Steiner tree as soon as nodes information is obtained. Due to the limited number of receivers in one multicast packet, the Steiner tree should be partitioned into several subtrees to meet the requirement of limitation of one multicast packet. Each Steiner sub-trees can be called as multicast group in this way.

C. Steiner sub-trees distribution phase: After the Steiner tree divided into several sub-trees, source node S should broadcast topology structure of each sub-tree. And after each node receives the information of topology, it analysis the data packets of topology structure to obtain the role information about itself in WSN. For the security reasons, the sensor node should unicast the node-state information table before broadcasting the topology of Steiner sub-tree.

D. Data delivery phase: When the source node wants to transmit any request, it should firstly determine the region of multicasting. Then the source node selects the related Steiner sub-trees which are in the geographical scope from local database. Taking a Steiner sub-1tree as unit, the source node transmits multicast data using unicast technology. After the multicast packet reaches the root node of the sub-tree, CHs in the sub-tree forward the multicast packet in accordance with the order of CHs' Height Value. Simultaneously, if the CH detects that it is the destination, it first validate the timestamp T and the value of HMAC in the received message.

Secondly, each CH who is the destination of multicasting broadcasts the content of multicast packet Each MN in the cluster also checks T and value of HMAC. If the inequality Clock holds and computing result is equal to HMAC in the received message, MNs accept the content of multicast packet.

E. Steiner tree maintains phase:

In this phase the maintenance of Steiner tree is done. The joining or leaving of new node in the tree is done. The main task of Steiner tree maintains is re-keying for each node in the network.

## V. CONCLUSION AND FUTURE SCOPE

Security challenge focus open architecture of WSN is biggest challenge of security. Defence against attacker is difficult task in Wireless Sensor nodes.WSN nodes deployed randomly in environment. Major challenge for employing any efficient security scheme in WSN is created by the size of sensors, the processing power, limited memory and type of task expected by the sensors. Battery power limitation is another challenge.

Sensor networks applications are being research and deployed all over the world. With the rise of these applications, implications will arise too. In this paper we tried to raise the concerns of major social implications like privacy and security. Without taking care of these issues, the necessary growth and development will face major obstacles in coming future. Here in this paper we analyze security issues and its management in WSN.

In future proper coordination between different government agencies, research institutes and manufactures is necessary to overcome these obstacles and have smooth implementation. In future common public should also be made aware of the benefits and implications.

## REFERENCES

[1] Tanveer Zia and Albert Zomaya, "A Secure Triple-Key Management Scheme for Wireless Sensor Networks", IEEE Infocom, DOI: 10.1109,April, 2006

[2] I.F.Su.W, Sankarasubramaniam, Y.E Cayirci, "Wireless Sensor Networks: A Survey", Computer Networks, 38, 2002, pp. 393-422.

[3] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.

[4] Dai, S, Jing, X, and Li, L, "Research and analysis on routing protocols for wireless sensor networks", Proc. International Conference on Communications, Circuits and Systems, Volume 1, 27-30 May, 2005, pp. 407-411.

[5] N. Krishna Murthy, R. Selvam "Security Issues in wireless sensor network", IJARCSSE,Vol.6,Issue 3,March 2016,pp.233-237.

[6] Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", Feb. 20-22, ICACT, 2006.

[7] Shan Chiang, Chih-Hung Huang, and Kuang-Chiung Chang "A Minimum Hop Routing Protocol for Home Security Systems Using Wireless Sensor Networks" IEEE Transactions on Consumer Electronics, Vol. 53, No.4, October 2007.

[8] Rong Fan, Jian Chen, Jian-Qing Fu and Ling-Di Ping, "A Steiner-Based Secure Multicast Routing Protocol for Wireless Sensor Network", Second International Conference on Future Networks, 2010.