# Secure Mechanism for Wireless Sensor Networks - A Review

Vani.Hiremani
Assistant Professor ,Department Of Computer Engineering
Alard College of Engg & Management,Pune,India
*vani.hiremani@gmail.com*

Monali.Madne
ME Student, Department Of Computer Engineering,
Alard College of Engg. & Management, Pune,I ndia
*monali.rupnar@rediffmail.com*

***Abstract-*** Wireless Sensor Network (WSN) is an emerging technology that is very useful for various futuristic applications both for public and military. As the use of wireless sensor networks continue to grow, so it should require effective security mechanisms. So to ensure the security of communication and data access control in WSN is paramount importance. Because sensor networks may interact with sensitive data and operate in hostile unattended environments, it is important that these security concerns should be addressed from the beginning of the system design. However because of inherent resource and computing constraints, security in sensor networks poses different challenges than traditional network security. There is currently enormous research is present in the field of wireless sensor network security. Thus, familiarity with the wireless sensor network,attack on WSN and security systems design for WSN will benefit researchers greatly. With this in mind, I survey the major topics in wireless sensor network security, and presentmany of the current attacks, and finally list their corresponding defensive measures.

**Keywords**: Sensor network security, secure communication architecture

*****

## I. INTRODUCTION

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor environmental or physical conditions, such astemperature, , pressure,sound etc. and to cooperatively pass their data through the network to a main location. Wireless Sensor Networks are heterogeneous systems containing many no of small devices called sensor nodes and actuators with general-purpose computing elements.

These networks will consist of thousands of low cost, low power and self-organizing nodes which are highly distributed either inside the system or very close to it.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors.

. These nodes consist of three main components- data processing, sensing and communication. Two other components are also there called, aggregation and base station [1]. Aggregation point's gathers data from their neighbouring nodes, integrates the collected data and then forwards it to the base station for further processing. Various applications of WSN includes ocean and wildlife monitoring ,monitoring of manufactured machinery, building safety, earthquake monitoring environmental observation , military applications ,manufacturing and logistics, and forecast systems, , health, home and office application and a variety of intelligent and smart systems

The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

Each such sensor network node has typically several parts: energy source, usually a battery ,a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors. A sensor node might vary in size. The cost of sensor nodes may vary, ranging from a few to hundreds of dollars, it depends on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as memory,energy, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network.

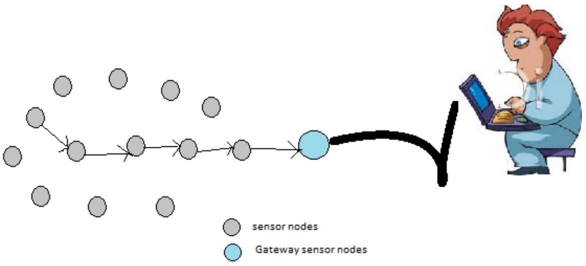

Fig.1 Wireless Sensor Network

## II. CHARACTERISTICS OF WSN

The mail characteristics of WSN are as follow

1. Ability to cope with node failures
2. Mobility of nodes
3. Dynamic network topology
4. Communication failure
5. Heterogeneity of nodes
6. Ability to withstand harsh environmental conditions
7. Easy of use
8. Unattended operation
9. Scalability to large scale of deployment

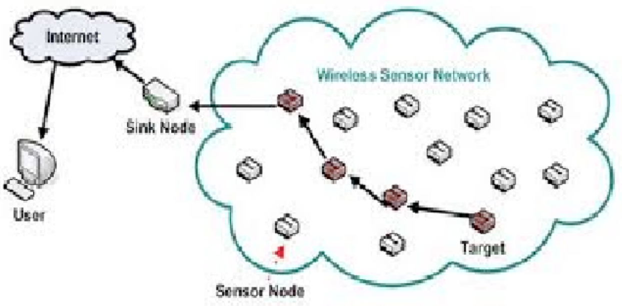

Fig.2 Characteristics of Wireless Sensor Network

## III. NEED TO SECURE WSN

1 Wirless sensor networks have many applications in homeland, military security and other areas in such area many sensor networks have mission critical tasks.

2 Security is critical for such a networks which deployed in hostile environments.

3 Most sensor networks actively monitor their surroundings and it is often easy to infer information other than the data monitored.

4 Such unwanted information leakage often results in privacy breaches of the people in environment.

5 Moreover the wireless communication employed by sensor networks suffer from eavesdropping and packet injection by an adversary.

6 The above factors demands security for wireless sensor networks at design time to ensure operation safety privacy of sensitive data and privacy for people in sensor environments

7 Providing security in sensor networks is even more critical than MANETs due to the resource limitations of sensor nodes

## IV. ATTACKS ON WSN

Security is one of the major aspects of any communication system. Traditional WSNs are affected by various types of attacks. Wireless sensor networks are energy constraint networks, having limited energy and power resources. This makes them exposed enough to attack by attacker deploying on nodes more resources than any individual node or base station, which is not difficult job for the attacker. A typical sensor network may be consist of potentially hundreds of nodes which may use broadcast or multicast transmission. The broadcast transmission nature of the medium is the reason why wireless sensor networks are susceptible to security attacks. Denial of Service attack eradicates a network's range to satisfy its expected function. Following are the different types of attacks can take place on Wireless Sensor Networks

1. Data confidentiality-The principle of confidentiality specifies that only the sender and the intended recipient should be able to access the contents of a message.Confidentiality gets compromised if an unauthorized person is able to access a message.
2. Data Authentication –Authentication mechanisms help establish proof of identities. The authentication process ensures that the origin of message or document is correctly identified.
3. Data Integrity –when the contents of a message are changed after the sender sends it ,but before it reaches the intended recipient,we say that the integrity of the message is lost.
4. Data Availablity-The principle of availablity states that resources should be available to authorized parties at all times.
5. Data freshness- Data freshness ensures that the data transmitted is recent one and no previous messages have been replayed by an attacker . Data freshness can be classified into two types based on the message ordering weak and strong freshness. Weak freshness gives only partial message ordering but gives no information about delay and latency of the message. Strong freshness on the other hand, provides complete request-response pair and allows the delay estimation.
6. Self Organization - A typical WSN consist of thousands of nodes fulfilling various operations, installed at various locations. Sensor networks can be ad hoc networks, having the same flexibility and extensibility. Sensor networks crave every sensor node to be independent and capable of being drawn enough to be self-organizing to different situations
7. Flexibility - Sensor networks will be used in various area where environmental factors , hazards and mission may change frequently. Changing factors may desire sensors to be eliminated from or injected to a sensor node. Moreover, two or more than two sensor networks may be merged into one network , or a single network may be divided in two or more . Key establishment protocols must be flexible enough to render keying for all potential scenarios a sensor network may encounter.
8. Jamming- Jamming is one of the basic and destructive attacks that attempt to disturb in physical layer of the WSN network . Jamming can be of two types- intermittent jamming and constant jamming. Constant jamming affects the complete obstruct of the whole

network whereas in intermittent jamming nodes communicate data periodically but not continuously.

9. Collision-- Collision is link layer jamming attack that occurs when two nodes transfer data at the same time and with the same frequency
10. Exhaustion- This attack decreases the power resources of the node by retransmitting the message again and again even though there is no collision.
11. Homing-In this type of attack the attacker discover the network traffic at the network layer to interpret the geological area of cluster heads or base station adjoining nodes.it then implements some other attacks on these vital nodes so as to destroy them that further cause major problem in network.

## V. LITERATURE SURVEY

There are many methods has been proposed to secure wireless sensor networks . Review of these methods is presented as below:

[1] Yao-Tung Tsou and Chun-Shien Lu present a security mechanism called MoteSec-Aware which is build on network layer for wireless sensor networks with the focus on secure network protocol and data access control.In the MoteSec-Aware, a Virtual Counter Manager (VCM) with a synchronized incremental counter is Developed to detect the jamming and replay attacks based on the symmetric key cryptography using AES in OCB mode. For access control, they proposed the Key-Lock Matching (KLM) method to prevent unauthorized access.in this paper they implement MoteSec-Aware for the TelosB prototype sensor platform which running TinyOS 1.1.15, and conduct field experiments and TOSSIM-based simulations to evaluate the performance of MoteSec-Aware. The results shows that MoteSec-Aware consumes much less energy, yet achieves higher security than several state-of-the-art methods. MoteSec-Aware is an efficient network layer security system protocol which is fully implemented security mechanism that provides protection for both outside network message and inside memory data.This security system is able to achieve the two important goals of much less energy consumption and higher security than previous works.

[2] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar proposed a protocol optimized for resource constrained environments and wireless communication. They proposed a protocol SPINS .SPINS have two major blocks SNEP and µTESLA.SNEP provides Data confidentiality, data freshness, and two party data authentication. Particularly in wireless network difficult problem is to provide efficient broadcast authentication, which is an important mechanism for sensor networks. µTESLA this is a new protocol which provides that authenticated broadcast for severely resource constrained environments. they implemented the above protocol and show that they are practical even on minimam hardware.additionaly they demonstrate that this suite can be further used for building higher level protocols

[3]C Karlof ,N sastry and D Wagner introduce TinySec, the first fully-implemented link layer security architecture for wireless sensor networks. In their design, they leverage recent lessons learned from design vulnerabilities in security protocols for other wireless networks such as 802.11b and GSM. Conventional security protocols tend to be conservative in their security guarantees, With small memories, weak processors, limited energy, sensor networks cannot afford this luxury. TinySec addresses these extreme resource constraints with careful design;they explore the tradeoffs among different cryptographic primitives and use the inherent sensor network limitations to their advantage when choosing parameters to find a sweet spot for security, packet overhead, and resource requirements. TinySec is portable to a variety of hardware and radio platforms. Their experimental results on a 36 node distributed sensor network application clearly demonstrate that software
based link layer protocols are feasible and efficient, adding less than 10% energy, latency, and bandwidth overhead.

[4]M luk,G Mezzeour,A perrig and V gligor proposed a protocol MiniSec is a secure network layer that achieves best of both things: High security and low energy consumption . MiniSec has two operating modes, one is for single-source communication, and another is for multi-source broadcast communication. The latter does not require per-sender state for replay protection and thus scales to large networks. They present a publicly available implementation of MiniSec for the Telos platform, and experimental results demonstrate low energy utilization. Battery power is the main resource to conserve in current wireless sensor networks. Researchers have proposed several approaches for securing communication that optimize either for high level of security or for low energy utilization. MiniSec, offers a high level of security while requiring much less energy than the previous approaches.

## V. CONCLUSION

In this paper, I Represent a brief survey on wireless sensor network, its characteristics ,need for security, Attacks on WSN. Then I represent the literature survey on various security techniques for WSN. Security is an important

ISBN: 978-93-82307-27-3

requirement and complicates enough to set up in different parts of WSN. , developing such a security mechanism and making it efficient represents a great research challenge. Again, ensuring Reliable security in wireless sensor network is a major research issue. Many of today's proposed security systems are based on specific network models in future though the security schemes become well-established for each individual layer, combining all the these mechanisms together for making them work in a unit will incur a hard research challenge.

## REFERENCES

[1] Yao-Tung Tsou,Chun-Shien Lu "Motesec-Aware:A practical Secure Mechanism for Wireless Sensor Networks"IEEE TRANSACTIONS on wireless communication,vol 12 No 6 JUNE 2013

[2] A.perrig,R Szewczyk V. Wen, D. culler, J .D. Tygar ,"SPINS:security protocols for sensor networks."International conference on mobile computing and networking ,pp 189-199

[3] Chris Karlof,Naveen Sastry,David Wagner "TinySec-A link layer security architecture for wireless sensor networks "International conference on embedded networked sensor systems pp 162-175

[4] Mark luk ,Ghita Mezzour,Adrian Perrig,Virgil Gligor,"Minisec:A secure sensor network communication architecture"

[5] Ashima single,Ratika Sachdeva "Review on security issues and attacks in wireless sensor networks" International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 4, April 2013

[6] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary "Wireless Sensor Network Security: A Survey"

[7] Yazeed Al-Obaisat, Robin Braun "On Wireless Sensor Networks: Architectures, Protocols, Applications, and Management"

[8] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong "Security in Wireless Sensor Networks: Issues and Challenges"

[9] MIHAELA CARDEI, DING-ZHU DU "ImprovingWireless Sensor Network Lifetime through PowerAware Organization" Wireless Networks 11, 333–340, 2005