A Review on Wireless Sensor Networks

Mrs. Monali.Rupnar[1], Ms. Pooja Shinde[2]

[12]*Lecturer , Department Of Computer Engineering*

Dr. D. Y. Patil, School of Engineering Pune, India

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 as temperature, , 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) sensor. 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 severalparts: 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.

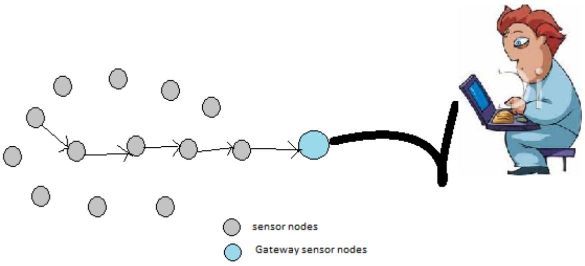

Fig.1 Wireless Sensor Network

II. DESIGN ISSUES OF ROUTING PROTOCOLS IN WSN

Routing protocols in Wireless Sensor Network are responsible for searching energy saving routes in the networks, in order to make communication reliable and efficient .the main aim of routing protocol design is extending the network life time by keeping the sensors alive as much as possible .there are some challenging points which are crucial in designing routing protocols these are as follows:

Node deployment: Deployment is application specific and affects performance of routing protocols.it can be manual in which nodes are manually placed and data is routed through predestined paths .this choice is not good for harsh environments. On the other hand in random deployment the nodes are scattered arbitrarily .this method is useful if the application is related to event detection.

Energy Consumption: Since the sensor nodes have limited energy resources, so there is a need to design routing protocols that can accommodate the tradeoff between energy optimization and accuracy.

Nature of Nodes: In wireless Sensor network nodes are of two types homogeneous and heterogeneous. Homogeneous nodes have same capabilities such as range of transmission, battery life and processing capacity while heterogeneous nodes have different capabilities.
Scalability: The number of nodes deployed in the field may be variable i.e. few to thousands. Routing protocols required to be able to work with massive amount of nodes .when the number of nodes is extensive, it is in feasible that each node maintain a global knowledge of network topology.

III. CHARACTERISTICS OF WSN

As compared to the traditional wireless communication networks such as mobile ad hoc network (MANET) and cellular systems, WSN have the following unique characteristics Dense sensor node deployment: Sensor nodes are usually densely deployed and can be huge in number than that in a MANET.
Nodes powered by Battery: Nodes are usually powered by battery and are deployed in a harsh environment where it is very difficult to change or recharge the batteries.
Severe energy, computation, and storage constraints: Sensors nodes are having highly limited Energy back up , computation, and storage capacity .
Self-configuration: Sensor nodes are usually randomly deployed and automatically configure themselves into a communication network.
Unreliable sensor nodes: Since sensor nodes are prone to physical damages or failures due to its deployment in harsh or hostile environment.
Data redundancy: In most sensor network application, sensor nodes are densely deployed in a region of interest and collaborate to complete a common sensing task. Thus, the data sensed by sensor nodes typically have a certain level of redundancy.
Application specific: A sensor network is usually designed for a specific application. The design requirements of a network change with its application.
Many-to-one traffic pattern: In most sensor network applications, the data sensed by sensor nodes flow from multiple source sensor nodes to a particular sink, exhibiting a many-to-one traffic pattern.
Frequent topology change: Network topology changes continuously due to the node failures, damage, addition, energy depletion, or channel fading.

IV. NEED TO SECURE WSN

1. Conflicting between minimization of resource consumption and maximization of security level.
2. Advanced anti-jamming techniques are impossible due to its complex design and high energy consumption.
3. Most current standard security protocols do not scale to a large number of participants.
4. Encryption requires extra processing, memory and battery power.
5. Secure asymmetric key needs more computations.
6. Most existing time synchronization schemes are vulnerable to several attacks.

V. 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.

VI. LITERATURE SURVEY

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

Yao-Tung Tsou and Chun-Shien [1]This paper describes the security protocol for WSN which is Motesec-Aware .Design of this protocol is base on existing security primitive AES, which has been proven to be the most suitable block cipher for the WSNs under consideration. They present a Virtual Counter Manager (VCM) with synchronized incremental counters and explore the Key-Lock Matching (KLM) method to, respectively, resist the replay/jamming attacks and achieve memory data access control. On the other hand, since sensors in the network, particularly those with limited resources, may suffer from DoS attacks, their previous work, called Constrained Function based Authentication (CFA), is employed with proper modification to resist DoS attacks. They denote the process of executing CFA in the AES with Offset Codebook Mode (OCB) mode as AES-OCFA. In this paper, AES-OCFA is the approach proposed to achieve the goal of secure network protocol. On the other hand, Memory Data Access Control Policy (MDACP) is presented to achieve the goal of data access control. To defend against unauthorized users in accessing data, They investigate the Key-Lock Matching (KLM) method to define access rights in each node because of its characteristic in needing low computation overhead. In KLM, each user is associated with a key (e.g., a prime number) and each file is associated with a lock value. For each file, there are some corresponding locks, which can be extracted from prime factorization. Through simple computations on the basis of keys and locks, protected memory data can be accessed. Here, data access control is designed exclusively for function nodes.

Aashima singl,Ratika Sachdeva [2] Describes types of wireless sensor network, its characteristics and attacks on it. Security is an important requirement and complicates enough to set up in different domains of WSN. also s various dimensions of security (availability, integrity, confidentiality and authenticity) that are being directed by different physical attacks is discussed. Characteristics of WSN are compact size, physical security, power, memory space, bandwidth, unreliable communication. Types of sensor networks are first Terrestrial WSNs In these nodes are distributed in a given area either in an ad hoc manner or in pre-planned manner, second Underground WSNs In these sensor nodes are buried underground or in a cave or mine that monitors the underground conditions. Sink nodes are deployed above the ground to forward the gathered information from the sensor nodes to the base statio, third Underwater WSNs in these, sensor nodes and vehicles are located underwater. Autonomous vehicles are used for gathering the data from the sensor nodes, and fourth Multimedia WSNs in these low cost sensor nodes are equipped with cameras and microphones. These nodes are located in a pre-planned manner to guarantee coverage. Issues in these networks are demand of high bandwidth, high energy consumption, quality of service provisioning, data processing.

Security is one of the major aspects of any system the DoS attacks on different layers of networks are Dos attacks on the physical layer, Dos attacks on the network layer, Dos attacks on the link layer, Dos attacks on the transport layer, Dos attacks on the application layer.

Data confidentiality, Data integrity, data authentication these are the security concern in WSN.Black hole attack,flooding,Sybil attack, selective forwarding, worm hole, hello flood attack, data freshness, self organization, time synchronization, secure localization, flexibility, robustness and survivability,jamming,collision these are the some attacks can take place in WSN.

Edvin prem kumar [3] Presents An overview of the broad spectrum of applications of WSN has been given in this paper. The application of WSNXthe areas of biomedical, intelligent parking, healthcare applications, environmental, industrial, and militaryapplications have been briefed. These interesting applications are possible due to the flexibility, fault tolerance,low cost and rapid deployment characteristics of sensor networks. Though wireless sensor networks are constrained by scalability, cost, topology change and power consumption, new technologies are being devised to overcome these and to make sensor networks an integral part of our lives. A review on the various research issues involved in the WSN applications has been outlined. Research on these issues will lead to promising results, making WSN based applications very popular. The application of WSNs is not limited to the areas mentioned in this paper. The future prospects of WSN applications are highly promising to revolutionize our everyday lives.

.

[4] This paper presents and analyzes a variety of regular deployment topologies, including circular and star deployments as well as deployments in square, triangular, and hexagonal grids. In this paper, they focus on optimal strategies for placing sensor units. Individual sensor units must be placed close enough to each other that wireless communication is possible, and must be arranged so they form a network to relay data back to data collection points. In addition, nodes can be prone to failure due to events such as loss of power, operating system bugs, and equipment glitches. It is important that the network provide reliable communication that can survive node outages. A second constraint is that units must be placed so as to observe events of interest. Finally, financial or other considerations usually limit the number of units that can be deployed to study a given Area.

VII. CONCLUSION

In this paper, I present a brief survey on wireless sensor network, its characteristics ,need for security, Attacks on WSN. Then I present the literature survey on various security techniques for WSN . Security is an important requirement and complicates enough to set up in different parts of WSN. Developing such a security mechanism and making it efficient this 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,tecniques 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] Aashima single,Ratika Sachdeva,"Review On Security Issues And Attacks In Wireless Sensor Networks",IJARCSSE,Vol 3,Issue 4,2013

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

[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.

[10] Edvin Prem Kumar Gilbert, Baskaran Kaliaperumal,"Research Issues in Wireless Sensor NetworkApplications: A Survey"