ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

SECURITY ISSUES, ATTACKS AND CHALLENGES IN WIRELESS SENSOR NETWORK

Vaishali Pahune*, Sharda Khode
Department of CSE,APGCE,Nagpur
Department of CE,BDCOE,Wardha

ABSTRACT

Wireless Sensor Networks (WSN) is an emerging technology now-a-days and has a wide range of applications such as battlefield surveillance, traffic surveillance, forest fire detection, flood detection etc. But wireless sensor networks are susceptible to a variety of potential attacks which obstructs the normal operation of the network. The wireless sensor network nature of communication is unprotected and unsafe because of deployment in hostile environment, limited resources, an automated nature and untrusted broadcast transmission media. The most of security techniques are not sufficient in WSN network and security is a vital requirement for network.

The intent of this paper is to investigate the security related issues, attacks and Challenges. The introductory section gives brief information on the WSN components and its architecture. Then it deals with some of the major security issues and challenges over wireless sensor networks (WSNs).

KEYWORDS: Attacks, challenges, Issues, wireless sensor network, security.

INTRODUCTION

Sensor networks are highly distributed networks of small, lightweight wireless nodes, deployed in large numbers to monitor the environment or system by the measurement of physical parameters such as temperature, pressure, or relative humidity. Building sensors have been made possible by the recent advances in micro-electromechanical systems (MEMS) technology. The sensor nodes are similar to that of a computer with a processing unit, limited computational power, limited memory, sensors, a communication device and a power source in form of a battery. In a typical application, a WSN is scattered in a region where it is meant to collect data through its sensor nodes. The applications of sensor networks are endless, limited only by the human imagination. WSNs have some special characteristics that distinguish them from other networks such a MANET. The characteristics, are listed as follows, that can lead to the use of WSNs in the real world:

• Sensor nodes possess extremely limited resources, such as battery life, memory space and processing capability. Routing protocols and algorithms are preferred to achieve longer sensor life.

• WSNs are self configuring and self organizing wireless networks.

• The topology of sensor network changes rapidly and randomly. Sensor nodes are continuously added and deleted from the network.

• WSNs have centralized approach in terms of network control. Data flows from sensor nodes towards a few aggregation points which further forward the data to base stations. Also base stations could broadcast query/control information to sensor nodes.Among the designs of WSNs, security is one of the significant aspects that deserve great attention, considering the tremendous application opportunities. Thus keeping in mind security constraints it presents a brief review of existing techniques for wormhole attack detection in network layer.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

WSN Architecture

In a typical WSN we see following network components –Sensor nodes (Field devices) – Each sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for

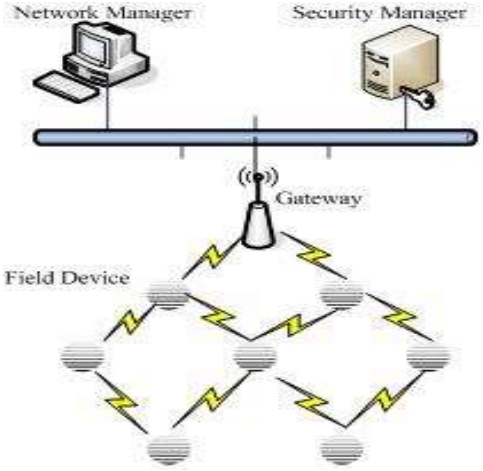
a) Interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting.

b) Gateway or Access points – A Gateway enables communication between Host application and field devices.

c) Network manager – A Network Manager is responsible for configuration of the network,scheduling communication between devices (i.e., configuring super frames), management of the routing tables and monitoring and reporting the health of the network.

d) Security manager – The Security Manager is responsible for the generation, and management of keys.

The base stations are one or more distinguished components of the WSN with much more computational, energy and communication resources. They act as a gateway between sensor nodes and the end user as they typically forward data from the WSN on to a server. Other special components in routing based networks are routers, designed to compute, calculate and distribute the routing tables. Many techniques are used to connect to the outside world including mobile phone networks,satellite phones, radio modems, high power Wi-Fi links etc. Figure 1-1 shows the architecture of WSN.



LITERATURE REVIEW

The paper proposes some of the security goal for Wireless Sensor Network. Further, as security being vital to the acceptance and use of sensor networks for many applications; It has made an in depth threat analysis of Wireless Sensor Network. Lastly it proposes some security mechanisms against these threats in Wireless Sensor Network[1]. , the center of attention is on physical attacks and issues in wireless sensor networks. Through this review, easily identify the purpose and capabilities of the attackers. Further, we discuss well-known approaches of security detection against physical attacks[2]. Wireless sensor networks are susceptible to a variety of potential attacks which obstructs the normal operation of the network. The security of a wireless sensor network is compromised because of the random deployment of sensor nodes in open environment, memory limitations, power limitations and unattended nature[3]. Group communications refers to either point-to multipoint (In which a packet is delivered from a group member to the other members) or multipoint-to multipoint communications (in which packets are sent from multiple members to other members simultaneously). The characteristics of different wireless networks - wireless infrastructure networks(WINs), ad hoc networks (AHNs), and wireless sensor networks (WSNs) - are vastly different in terms of group management, packet types, and resources[4].This survey paper is an attempt to analyze threats to Wireless sensor networks and to report various research efforts in studying variety of routing attacks which target the network layer. Particularly devastating attack is Wormhole attack- a Denial of Service attack, where attackers create a low-latency link between two points in the network[5].

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

SECURITY ISSUES IN WSNS

Availability*:*
The availability in wireless sensor network ensures the network services are feasible even in the subsistence of denial of service attacks. The securities protocols perform the availability of data in the network with fixate low energy and storage with reuse of code in network. In availability, a few approaches choose to adjust the code to reuse as much code as possible and make use of extra communication to achieve the same goal.

Self Organization:
The wireless sensor network has many nodes for operations and deployed in different locations and fields. In self-organization, the nodes are flexible to be self-organizing and self-healing in network. The WSN is an Ad hoc network and all nodes are independent in network and without infrastructure. This intrinsic characteristic brings a great challenge for wireless network and security, as well.

Time Synchronization:
The wireless sensor network applications rely on some type of synchronization. The nodes have two states in the network on and sleep and radio may be turn on or in sleep mode for period of time. The sensor calculates the end-to-end delay of a packet.

Secure Localization:
Wireless sensor network use location based information for identifying the position of nodes in the network. Few attacks are related with sensor location by investigating for attacks. The attackers are searching the header of packet and data for this purpose. The secure localization is an important factor during implementing security in the network.

Confidentiality:
The confidentiality is restricted data access to authorized personnel. The data should not leak across adjacent sensor network. When one node sends the highly sensitive data to the destination, it passes from many nodes in the network. For the provision of security in data, network protocols are using encryption technique with a secret key, the message is sent in encrypted for to the channel. Information should encrypt to protect from traffic analysis attack

Authenticity:
Authenticity is imperative in WSN, because an adversary can easily inject messages. The receiver node need to guarantee that data used in any decision making process originate with trusted source.The data authenticity is to ensure of identities of communication nodes. It is required in various administration tasks.

Flexibility:
The sensor network scenarios are different and depending on environmental conditions, hazards and mission because they are changing frequently .The changing mission goals frequently need sensors to be reduced from settle nodes in the network.

CHALLENGES OF SENSOR NETWORK

A wireless sensor network is a special network which has many constraint compared to a conventional computer network Security in wireless sensor networks has attracted a lot of attention in the recent years. Majority of resource constraints makes computer security more challenging task for these systems. The various challenges are discussed as follows.

Wireless nature of communication
The open nature of wireless medium is inherently less secure and thus makes it vulnerable against various kinds of malicious attacks. These attacks can be either passive or active attacks. Passive attack intends to steal information and to eavesdrop on communication within the network In active attacks, attacker modifies and injects packets into the network. This factor should be taken into consideration so that performance of the system is not significantly affected.

Ad-Hoc Deployment
Sensor nodes are deployed randomly and do not have any fixed topology. The ad-hoc nature of sensor networks

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

means no regular structure can be defined. Due to high mobility of nodes network topology is always subject to changes. Hence security mechanisms must be able to operate within this dynamic environment.

Hostile Environment

Hostile environment in which sensor nodes are deployed is another challenging factor. Due to the broadcast nature of the transmission medium, wireless sensor networks are vulnerable to various security attacks. Moreover nodes are placed in a dangerous or unguarded environment where they are not physically protected. Attackers may capture a node, physically stamper it, and extract valuable information from it. The highly hostile environment represents challenging approach for security researchers.

Resource Limitation

Adequate amount of resources are mandatory for the implementation of all security approaches. including memory, bandwidth, and energy to power the sensor. However, currently these resources are very limited in a tiny wireless sensor which poses considerable challenges to resource-hungry security mechanisms.

Limited Memory and Storage Capacity:

Sensor node is a tiny device with very small amount of memory and storage space for the code. It is necessary to limit the code size of the security algorithm in order to develop an effective security mechanism.

Power Limitation:

The use of wireless sensor networks is increasing day by day and since each node depends on energy for its activities, this has become a biggest constraint and primary requirement in wireless sensor networks. The failure of one node can destroy the entire system. Therefore, some mechanisms must be designed to conserve energy resource.

Scalability

Scalability is a major factor in wireless sensor networks. A network topology is dynamic, it changes depending upon the user requirements. All the nodes in the network area must be scalable so as to adapt themselves with changing network topology.

Unreliable Communication

Certainly, unreliable nature of communication channel is another challenging issue to sensor security. The security of the network depends heavily on a defined protocol,which in turn depends on communication.

Unreliable Transmission:

Sensor network follows packet-based routing approach for communication. Hence transmission is connectionless and therefore inherently unreliable.

Conflicts:

Although the channel is reliable, the communication may still be unreliable because of congestion of data packets. This is due to the broadcast nature of the wireless sensor network.

Latency:

Latency is defined by how much time a node takes to monitor, or sense and communicate the activity. Sensor nodes gather information, process it and send it to the base station. Latency in a network is computed based on these activities as well as how much time a sensor node takes to forward the data in heavy network traffic or in a low density network.

Unattended Operation

In certain cases, the sensor nodes are not operated and hence are left unattended for long periods of time. There are three main reasons to unattended sensor nodes.

High risk of Physical Attacks:

After deployment, sensors are usually left unattended and easy to be physically compromised. An adversary can capture one or more nodes, injects some malicious code into them to cause threats or receives information from the network. Also, an adversary can easily eaves drop the transmission or launch serious attacks. Therefore, it is not surprising that sensor networks are vulnerable to many security attacks.

Managed Remotely:

Remote management of a sensor network makes it difficult to detect physical tampering and physical maintenance issues.

***Lack of Central Coordinator*:**

A sensor network should be a distributed network. Each sensor node should operate autonomously with no central point of control in the network. In case if designed inaccurately, it will make the network organization difficult, inefficient, and weak. A sensor node left unattended for longer time is more likely to be compromised by an

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

adversary.

ATTACKS ON SENSOR NETWORKS

Wireless Sensor networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. Basically attacks are classified as active attacks and passive attacks. Figure 5.1 shows the classification of attacks under general categories and Figure 5.2 shows the attacks classification on WSN.

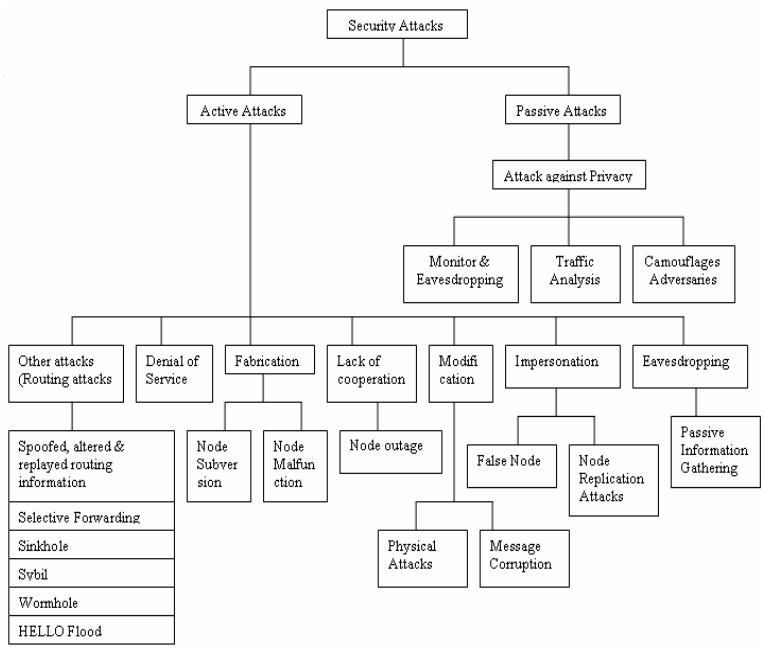


Figure 5.1. General Classification of Security Attacks

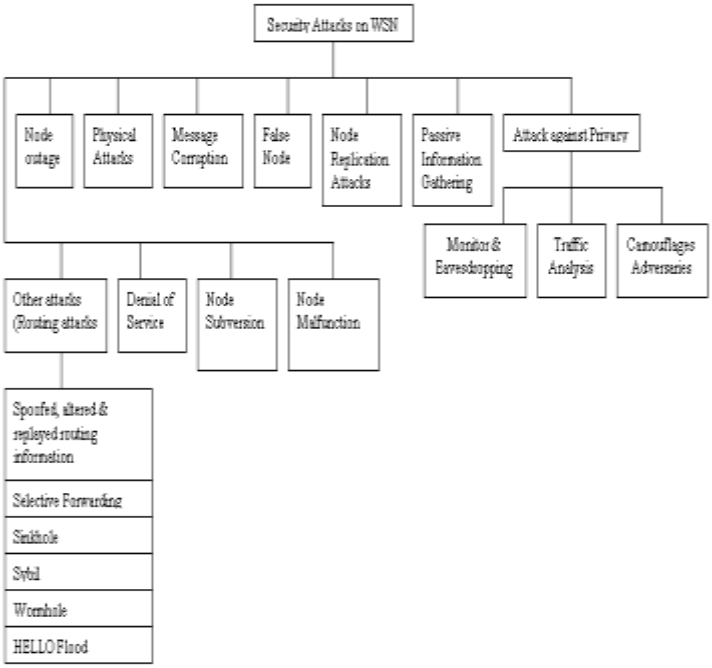


Figure 5.2. Classification of Security Attacks on WSN

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

Passive Attacks

The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. The Attacks against privacy is passive in nature.

1) Attacks against Privacy

The main privacy problem is not that sensor networks enable the collection of information. In fact, much information from sensor networks could probably be collected through direct site surveillance. Rather, sensor networks intensify the privacy problem because they make large volumes of information easily available through remote access. Hence, adversaries need not be physically present to maintain surveillance. They can gather information at low-risk in anonymous manner. Some of the more common attacks against sensor privacy are:

• Monitor and Eavesdropping: This is the most common attack to privacy. By snooping to the data, the adversary could easily discover the communication contents. When the traffic conveys the control information about the sensor network configuration, which contains potentially more detailed information than accessible through the location server, the eavesdropping can act effectively against the privacy protection.

• Traffic Analysis: Even when the messages transferred are encrypted, it still leaves a high possibility analysis of the communication patterns. Sensor activities can potentially reveal enough information to enable an adversary to cause malicious harm to the sensor network.

• Camouflage Adversaries: One can insert their node or compromise the nodes to hide in the sensor network. After that these nodes can copy as a normal node to attract the packets, then misroute the packets, conducting the privacy analysis.

5.2 Active Attacks

The unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are known as active attack. The following attacks are active in nature.

1. Routing Attacks in Sensor Networks
2. Denial of Service Attacks
3. Node Subversion
4. Node Malfunction
5. Node Outage
6. Physical Attacks
7. Message Corruption
8. False Node
9. Node Replication Attacks

1) Routing Attacks in Sensor Networks:

The attacks which act on the network layer are called routing attacks. The following are the attacks that happen while routing the messages.

a) Spoofed, altered and replayed routing information

• An unprotected ad hoc routing is vulnerable to these types of attacks, as every node acts as a router, and can therefore directly affect routing information.

• Create routing loops
• Extend or shorten service routes
• Generate false error messages
• Increase end-to-end latency

b) Selective Forwarding

A malicious node can selectively drop only certain packets. Especially effective if combined with an attack that gathers much traffic via the node. In sensor networks it is assumed that nodes faithfully forward received messages. But some compromised node might refuse to forward packets, however neighbors might start using another route.

c) Sinkhole Attack

Attracting traffic to a specific node in called sinkhole attack. In this attack, the adversary's goal is to attract nearly all the traffic from a particular area through a compromised node. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes.

d) Sybil Attacks

A single node duplicates itself and presented in the multiple locations. The Sybil attack targets fault tolerant schemes such as distributed storage, multipath routing and topology maintenance. In a Sybil attack, a single node presents multiple identities to other nodes in the network. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

e) Wormholes Attacks

In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them to another location, and retransmits them into the network.

f) HELLO flood attacks

An attacker sends or replays a routing protocol's HELLO packets from one node to another with more energy. This attack uses HELLO packets as a weapon to convince the sensors in WSN. In this type of attack an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes that are isolated in a large area within aWSN. The sensors are thus influenced that the adversary is their neighbor. As a result, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker.

2) Denial of Service

Denial of Service (DoS) is produced by the unintentional failure of nodes or malicious action. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion and unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and de-synchronization. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic.

3) Node Subversion

Capture of a node may reveal its information including disclosure of cryptographic keys and thus compromise the whole sensor network. A particular sensor might be captured, and information (key) stored on it might be obtained by an adversary.

4) Node Malfunction

A malfunctioning node will generate inaccurate data that could expose the integrity of sensor network especially if it is a data-aggregating node such as a cluster leader.

5) Node Outage

Node outage is the situation that occurs when a node stops its function. In the case where a cluster leader stops functioning, the sensor network protocols should be robust
enough to mitigate the effects of node outages by providing an alternate route.

6) Physical Attacks

Sensor networks typically operate in hostile outdoor environments. In such environments, the small form factor of the sensors, coupled with the unattended and distributed nature of their deployment make them highly susceptible to physical attacks, i.e., threats due to physical node destructions. Unlike many other attacks mentioned above, physical attacks destroy sensors permanently, so the lossesare irreversible. For instance, attackers can extract cryptographic secrets, tamper with the associated circuitry,modify programming in the sensors, or replace them with malicious sensors under the control of the attacker.

7) Message Corruption

Any modification of the content of a message by an attacker compromises its integrity.

8) False Node

A false node involves the addition of a node by an adversary and causes the injection of malicious data. An intruder might add a node to the system that feeds false data or prevents the passage of true data. Insertion of malicious node is one of the most dangerous attacks that can occur. Malicious code injected in the network could spread to all nodes, potentially destroying the whole network, or even worse, taking over the network on behalf of an adversary.

9) Node Replication Attacks

Conceptually, a node replication attack is quite simple; an attacker seeks to add a node to an existing sensor network by copying the nodeID of an existing sensor node. A node replicated in this approach can severely disrupt a sensor network's performance. Packets can be corrupted or even misrouted. This can result in a disconnected network, false sensor readings, etc. If an attacker can gain physical access to the entire network he can copy cryptographic keys to the replicated sensor nodes. By inserting the replicated nodes at specific network points, the attacker could easily manipulate a specific segment of the network, perhaps by disconnecting it altogether.

10) Passive Information Gathering

An adversary with powerful resources can collect information from the sensor networks if it is not encrypted.An intruder with an appropriately powerful receiver and well-designed antenna can easily pick off the data stream.Interception of the messages containing the physical locations of sensor nodes allows an attacker to locate the

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

nodes and destroy them. Besides the locations of sensor nodes, an adversary can observe the application specific content of messages including message IDs, timestamps and other fields. To minimize the threats of passive information gathering, strong encryption techniques needs to be used.This section explained about the attacks and their classification that widely happens on wireless sensor networks. The next section discusses about the security mechanisms that are used to handle the attacks.z

APPLICATIONS OF WSN

Following are some of salient areas of applications of WSN:

Military Applications

Sensor nodes admit battlefield surveillance ,monitoring, and also lets in guiding systems of intelligent missiles and sensing of attack by weapons of mass wipeout.

Medical Application

Sensors can be wear by patient which wil highly useful in patient diagnosis and monitoring .Sensor devices will monitor the patient's physiological data such as heart rate, temperature, etc.

Environmental Applications

It includes Flood Detection, Precision Agriculture, traffic, Wild fire etc.

Industrial Applications

It includes industrial sensing and diagnostics. For example appliances, factory, supply chains etc.

Infrastructure Protection Application

It includes power grids monitoring, water distribution monitoring etc.routing of sensor networks is based on connectionless protocols and thus inherently.

CONCLUSION

The deployment of sensor nodes in an unattended environment makes the networks vulnerable. Wireless sensor networks are increasingly being used in military, environmental, health and commercial applications Security in Wireless Sensor Network is vital to the acceptance and use of sensor networks. In particular, Wireless Sensor Network product in industry will not get acceptance unless there is a full proof security to the network. . This paper summarizes the attacks and their classifications in wireless sensor networks . This will hopefully motivate future researchers to come up with smarter and more robust security mechanisms and make their network safer.

ACKNOWLEDGEMENTS

Making of paper needs co-operation of number of people. I therefor making it my primary duty to thanks all those who had helped me through this venture. It is my immense pleasure to express my gratitude to prof. R.S. Mangrulkar sir as guide who provide me constructive and positive feedback durig the preparation of this paper.

REFERENCES

1. Vikash Kumar, Anshu Jain,P N Barwal " Wireless Sensor Networks: Security Issues, Challenges and Solutions "International Journal of Information & Computation Technology, Vol. 4, Number 8 (2014), pp. 859-868.
2. Raja Anwar, Majid Bakhtiari, Anazida Zainal, Abdul Hanan Abdullah and Kashif Naseer Qureshi "Security Issues and Attacks in Wireless Sensor Network"World Applied Sciences Journal 30 (10): 1224-1227, 2014 .
3. Deepali Virmani, Ankita Soni, Shringarica Chandel, Manas Hemrajani " Routing Attacks in Wireless Sensor Networks:A Survey,International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014.
4. K.Venkatraman, J.Vijay Daniel, G.Murugaboopathi "Various Attacks in Wireless Sensor Network:Survey" International Journal of Soft Computing and Engineering, Vol.3,Issue-1, March 2013.
5. Priya Maidamwar, Nekita Chavhan "A Survey on Security Issues to DetectWormhole Attack In Wireless Sensor Network",International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 4, October 2012.
6. Md Abdul Azeem, Dr.Khaleel-ur-Rahman khan, A.V.Pramod" Security Architecture Framework and Secure Routing.Protocols in Wireless Sensor Networks -Survey", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.4, November 2011.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

7. Gursewak Singh, Rajni Bedi," A Survey of Various Attacks and Their Security Mechanisms in Wireless Sensor Network", International Journal of Emerging Science and Engineering (IJESE), Volume-2, Issue-8, June 2014.
8. Shio Kumar Singh, M P Singh , and D K Singh, "A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks", International Journal of ComputerTrends and Technology- May to June Issue 2011.
9. Dr. Banta Singh Jangra, Vijeta Kumawat, "A Survey on Security Mechanisms and Attacks in Wireless Sensor Networks", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 3, Sep 2012.
10. C K Marigowda1, Manjunath Shingadi,"Security Vulnerability Issues InWireless Sensor Networks: A Short Survey", International Journal of Advanced Research in Computer and Communication Engineering,Vol.2, Issue 7, July2013
11. Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security,Vol. 4, 2009.
12. Kalpana Sharma, M K Ghose, "Wireless Sensor Networks: An Overview on its Security Threats", IJCA Special Issue on "Mobile Ad-hoc Networks"MANETs, 2010.