A Survey On Attacks, Challenges and Security Mechanisms In Wireless Sensor Network

Abdul Wahid
PG Student
Department of Computer Science Engineering
National Institute of Technology Patna

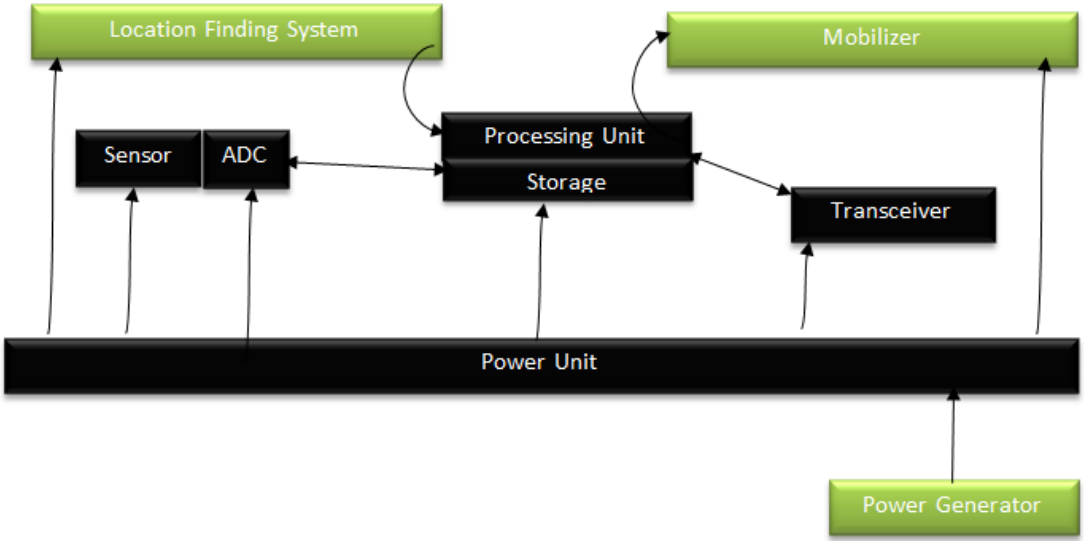
Pavan Kumar
PG Student
Department of Computer Science Engineering
National Institute of Technology Patna

Abstract

The wireless sensor network (WSN) has becomes the research area in today's worlds due to the huge number of application taking the advantage from it. Sensors are small device having memory, power and processing chip that makes it processing device. Due to its dominant nature it is used in battlefields and commercial applications such as building, traffic surveillance, habitat monitoring and smart homes and many more scenarios. Main motive behinds this paper is to introduce different types of attacks encounters during transmission or communication over the wireless sensor network and provides some ideas to overcome from these attacks. Here, we introduce security mechanisms like cryptographic key, authentication and challenges in wireless sensor network. The power computation and unsecure communication is main challenging area of wireless sensor network.
Keywords: Wireless Sensor Network, Attacks, Security Mechanism, Challenges.

I. INTRODUCTION

A wireless sensor network is composed of a large number of sensor nodes which are randomly deployed are connected through wireless medium to monitor physical or environmental conditions such as sound, vibration, pressure, temperature etc and to co-operatively pass their data to base station. Due to its rapid development it is use in various field like military, home monitoring, heath care, agriculture etc .



There are four basic components of sensor node:-
Sensing Unit, Processing Unit, Transceiver, and Power Unit.

Sensing unit contain two sub unit: sensor and analog-to-digital convertor (ADC). Sensor takes some values from real world. An analog signals produced by sensor is converted into digital signal by ADC. And these digital signal fed into the processing unit, which contain a small storage unit. After processing these data, transfer to transceiver which connects the node to network. But most important unit of sensor node is power unit who gives power to all the components (sensing unit, processing unit, and transceiver).

In this paper we discuss various types of attacks on WSN and then challenges on security in WSN and finally we discuss security mechanism in WSN.

II. SECURITY ATTACKS ON WIRELESS SENSOR NETWORK

Wireless Sensor Networks are vulnerable to various types of attacks but mainly due to the broadcast nature of the transmission medium. Figure 1 shows the various types of attacks on WSN which classified as two broad categories: (i) Active Attacks and (ii) Passive

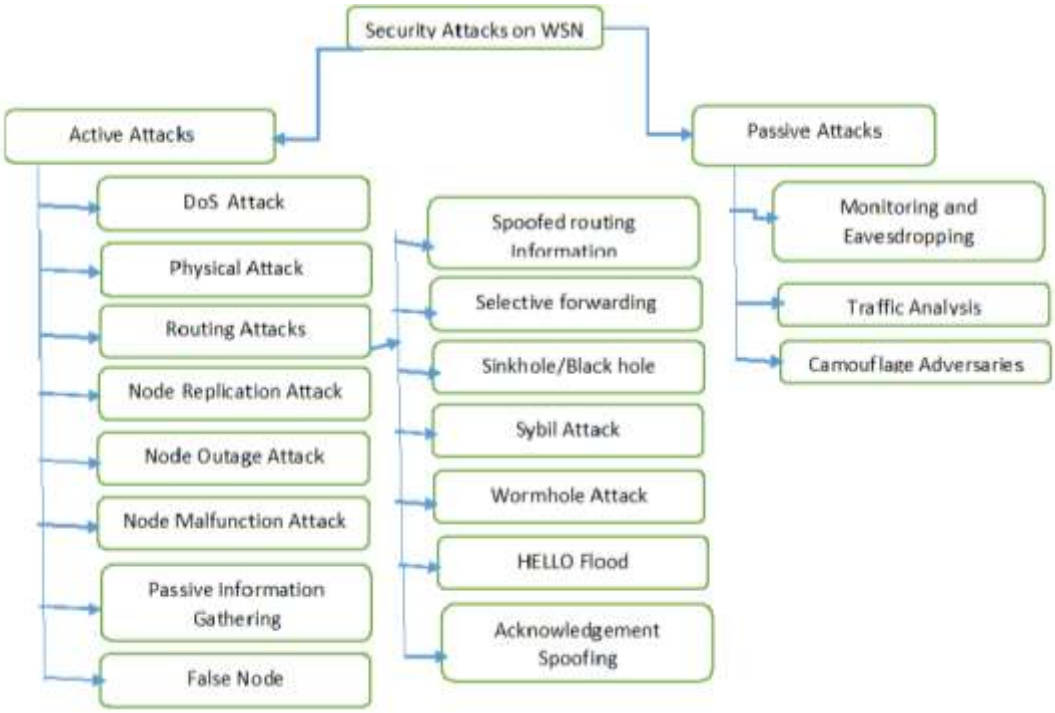


Fig. 1: Security Attacks On Wireless Sensor Network

A. Active Attacks:

In active attacks an adversary monitor, listens and introduce malicious code, steal or modify message content, or break security mechanism.

Some of the active attacks on WSN are

1) *Denial of Service (DoS) Attack*

Dos attack is an attack which either diminishes or reduces networks capability to perform task and produced by malicious action or unintentional failure of nodes. In wireless sensor network various types of Denial of Service attack occurs.

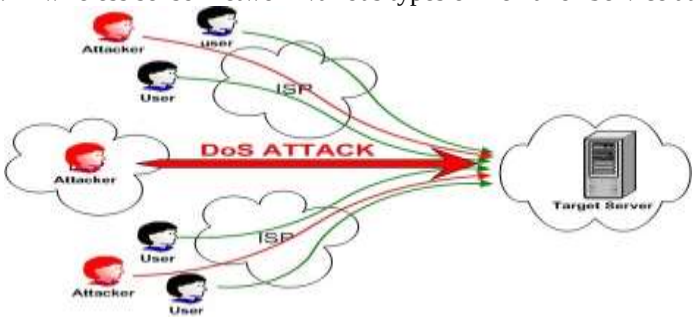


Fig 2: Demonstration of DoS Attack

In this attack, attacker may overload that server in such a way that server can't process request. For example:- Node "X" sends request to node "Y" for communication and node "Y" sends acknowledge to node "X" but node "X" keeps on sending request to "Y" continuously .As a result node "Y" is not able to communicate with any other nodes .

A simplest DoS attack on wireless sensor network is simply to jam a node or set of nodes. Jamming, in this case, is simply the transmission of a radio signal that interferes with the radio frequencies being used by the sensor network [1].

2) *Physical Attacks*

Sensor networks typically operate in outdoor environments. Due to its unattended and distributed nature it is highly susceptible to physical attacks. Physical attacks permanently destroy sensor nodes which may be irreversible. An attacker can extract sensitive information or change its program codes, tamper with its circuitry or may replace with a malicious node.

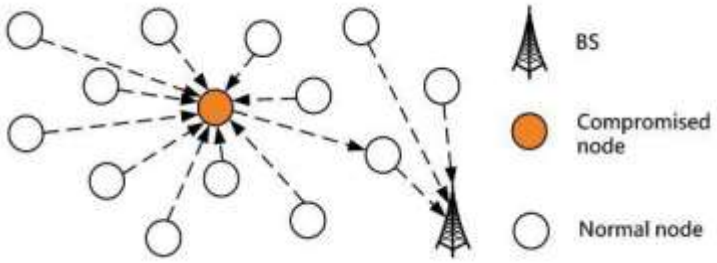


Fig. 3: Demonstration of Physical Attacks On WSN.

3) *Routing Attacks*

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 routing information

In sensor network, sensor nodes takes some values and send it to the sink or base station .While routing this information to the base station or sink an attacker may alter or spoof that routing information to disrupt traffic in network.

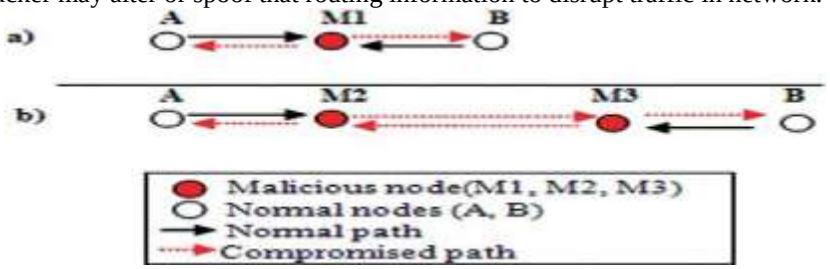


Fig. 4:-Demonstration of Spoofed Routing Information On WSN.

b) Selective packet forwarding

In wireless sensor network it is assumed that all nodes will accurately forward the entire received packet but in this attack an attacker creates malicious node which do not forward the entire message they received.

c) Sinkhole/Black hole Attack

In this type of attack, an attacker makes a compromised node look more attractive to neighbors nodes in sensor network with high resources capability (high processing power and high band width) .The result is that all surrounding nodes route their data through this compromised node and when data routes through this compromised node it is able to do anything with the packet.

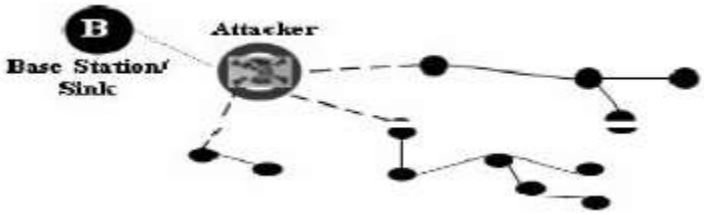


Fig. 5: Demonstration of Black Hole Atacks On WSN.

d) Sybil Attack

In wireless sensor network every sensor node might need to work together to accomplish a task.But in this attack a malicious node will appears as a set of nodes using the identities of other legitimate nodes and affect routing mechanism, distributed storage, data aggregation and send incorrect information to the network.

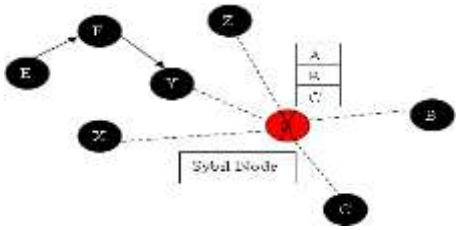


Fig. 6: Demonstration of Sybil Attacks On WSN

This incorrect information can be a variety of things [3], including position of nodes, signal strength, making a nodes that do not exist.

e) Wormhole

In this attack, attacker records the packet (or bits) at one location in the network and retransmits those packets to another location [2].

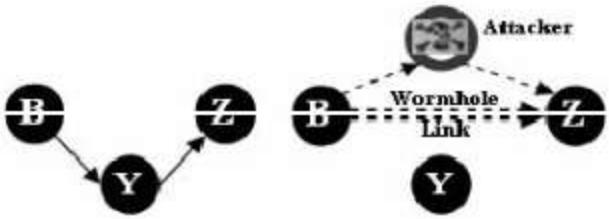


Fig. 7: Demonstration of Wormhole Attacks On WSN.

When base station or any sensor node (let us assume node B) wants to send data, then it broadcasts routing request packet to find path. When broadcast routing request packet an attacker receives those packet and sends acknowledgement to the node B. When B sends data, attacker receives those data and tunnels or retransmit to its neighbor node by hiding its own identity (retransmitting may be selective forwarding). Neighbor node will consider itself to be in the range of B, but actually it is far from node B and thus creates a wormhole.

f) Hello flood

This is simplest attack in wireless sensor network in which an attacker broadcast "HELLO" packet as a weapon with high transmission power (termed as a laptop-class attacker in [4]) to convince sensor nodes which are dispersed in large area within the wireless sensor network. The nodes sending the information to the base station, the victim nodes try to go through the attacker as they know that it is (attacker) their neighbor and result is that it is spoofed by attacker.

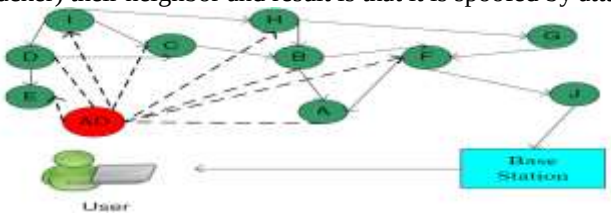


Fig. 8: Demonstration of HELLO Flood Attacks On WSN.

g) Acknowledgement spoofing

Routing algorithms used in sensor networks sometimes require acknowledgments to be used [6] [7].In this attack, an attacker may overhear packet transmitted from its neighbor nodes and spoof the acknowledgement or send false information(like send information that a node is alive when in fact it is dead) about nodes to the sending node.

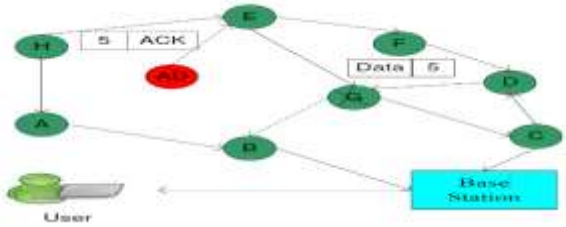


Fig. 9:Demonstration of Acknowledgement Spoofing Attacks On WSN.

4) *Node Replication Attacks*
In this attack an attacker add a sensor node to existing sensor network with copying the node ID of existing sensor node. This attack reduces the network's performances by using packet corruption or misroute the packet.

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 [5].

6) *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 [10].

7) *Passive Information Gathering*
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 nodes and destroy them [8] [9]. Besides the locations of sensor nodes, an adversary can observe the application specific content of messages including message IDs, timestamps and other fields.

8) *False Node*
A false node attack is an attack in which attacker add a malicious node in wireless sensor network that feeds false data or prevents the passage of accurate data. Most of the attacks in wireless sensor network caused by false information.

B. Passive Attacks:-
In passive attacks an attacker monitor and analyze traffic through which data are transfer and it does not change or modify the data like an active attacks. The aim of this attack is to obtain information that is being transmitted.

Some of the common passive attacks on WSN are

1) *Monitor and Eavesdropping*
This attack is most common and easiest attack on privacy. In this attack an adversary snoop the data, by snooping those data an adversary easily understands message 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.

2) *Traffic Analysis*
Traffic analysis is a passive attack on wireless sensor network on privacy. In this attack an adversary analyze traffic that can identify activities in a wireless sensor network and also identify some sensor nodes that plays an important role in wireless sensor network. This attack may create Denial of Service (Dos) attack and also attack on those node which plays an important role.

3) *Camouflage Adversaries*
It is also a passive attack on wireless sensor network on privacy. In this attack an adversary either inserts a sensor node or compromises a sensor node in wireless sensor network. This camouflaged node attracts the packets from other nodes and may misroute those packet where privacy analysis perform.

III. CHALLENGES FOR WIRELESS SENSOR NETWORK SECURITY

A. Power Limitation
Energy is the biggest constraint on wireless sensor node. Most of the sensor node uses battery and lifetime of battery is limited (from days to years). The consumption of energy in WSN can be categorized as:-

(1) Energy for microprocessor computation.

(2) Energy for transducer.
(3) Energy for communication among sensor nodes.

If we apply higher security level mechanism in WSN, it consumes more energy. So that it is very challenging issue for securing wireless sensor network.

B. Limited Memory

A sensor node has limited storage capacity. The storage capacity of a sensor node is restricted by the requirement of size and cost of the sensor node. Memory in sensor node mainly contains flash memory and RAM. Flash memory is used for storing code of downloaded application and RAM used for storing sensor data and intermediate computations.

Name of Sensor node	*Dot*	*Eyes*	*Mice2*	*Imote*	*KMote*
Flash Memory	*16KB*	*60KB*	*128KB*	*512KB*	*48KB*
RAM	*1KB*	*2KB*	*4KB*	*64KB*	*10KB*

This is not enough space to run complicated algorithm to secure WSN.

C. Ad-hoc Deployment

Due to ad-hoc deployment of sensor nodes in WSN various types of attack may occur (like Tampering). In ad-hoc deployment node may be dropped by airdrop due to this sensor node may fail to perform task or may an attacker attack on that node.

D. Hostile Environment

The hostile environment is the challenging factor of WSN in which sensor nodes function. *Motes* face the possibility of destruction or capture by the attacker. Since in hostile environment, an attacker may easily capture a node and extract the important information or change the information of a node. An attacker may also physical access of the node and replace the sensor node by malicious node. The highly hostile environment is the challenging factor of the wireless sensor network.

E. Wireless Medium

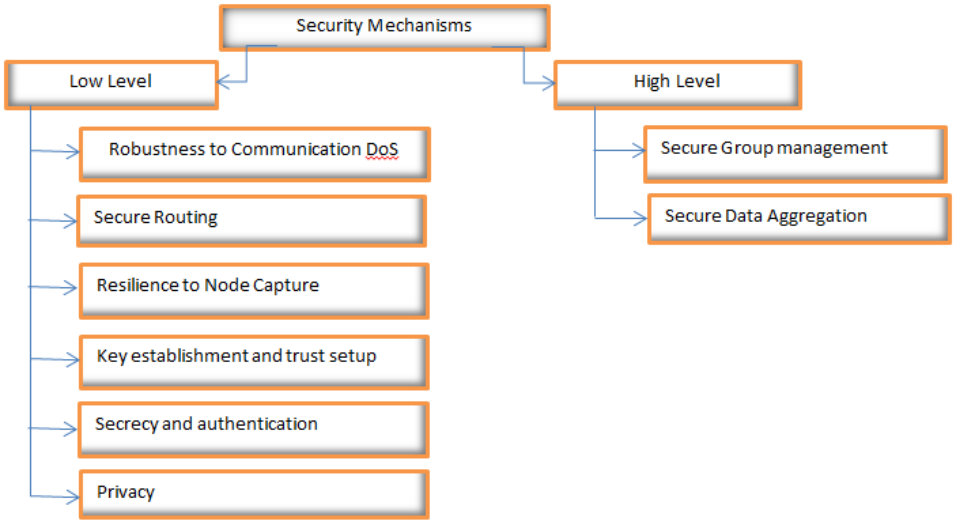
Wireless medium is not much more secure because of its broadcasting nature. An attacker can easily intercept, change and alter any transmission. In Wireless medium an attacker easily track the node and replace that node by malicious one. This is the really challenging field of sensor network.

F. Immense Scale

The proposed scale of the sensor networks shows a significant challenge for security mechanism. The network has thousands of the nodes; to scale the security is a challenging factor of the WSN. Security mechanisms must be scalable for the large network while maintaining high *computation and communication efficiency*.

IV. SECURITY MECHANISMS

The main motive behinds the security mechanisms is to detect, prevent, and recover from the security attacks and also provides a pseudo idea to protect from different kind of security attacks. Many different types of security schemes can be invented to encounter different types of attacks. Based on this we can divides the security mechanisms into two parts Low level and High level.



A. Low Level Security Mechanisms

1) *Robustness to communication denial of service*
An attacker attempts to disrupt the operations of the networks. Means, if a node have the huge power and broadcast a high energy signals. If the broadcasted node have highly transmission rate then the entire communication system channel could be jammed.

2) *Secure routing*
To Route the packet, is a crucial service for enabling the communication in sensor network. The Routing protocols we have till now, unfortunately suffer from many security vulnerabilities. An attacker can be launch the DoS (Denial of Services) attack on the routing protocol, preventing communication just by broadcasting a packet with high transmission rate and could be jammed the entire communication network. An attacker may inject malicious routing information into the network, resulting in routing inconsistencies. We can protect the communication network from above attacks by using authentication but some routing protocols are susceptible to replay by the attacker of legitimate routing messages. [11]

3) *Resilience to Node Capture*
Resiliency against node capture is one of the most challenging issues in sensor networks. In most of the application, sensor nodes are to be placed on many locations that are easily accessible to the attackers. By this attacker can capture the sensor node and extract the cryptographic secrets, change their programs and may replace them with malicious nodes under the control of the attacker. *Tamper-resistant packaging* may be a defense but it is expensive so current technology does not provides the high security.

4) *Key establishment and trust setup*
The establishment of cryptographic keys is the primary requirement to setting up the sensor network. As we know, the sensors have the limited computational power and the public key cryptography primitives are too expensive. The way of communication of sensor network differ from traditional networks, sensor networks needs to establish a key and set up with their neighbors. The disadvantage of this mechanism is that the attacker may compromise and most of the node could be reconstruct the complete key pool and easily break the security scheme.

5) *Secrecy and authentication*
The sensor network application needs to protect against modification, eavesdropping and alteration of packet. To overcome with this, Cryptography is the standard defense approach. In the contest of cryptography, we can set up a centrally server which provides the unique id with key to each sensor node of the wireless network and whenever any sensor node wants to transmit the data over the network, first send to the server and then server further transmit the packet to the appropriate node. But problem of this approach is that if the server fails then the entire network leads to be failed. The earliest sensor networks are likely to use link layer cryptography, because this approach provides the greatest ease of deployment among currently available network cryptographic approaches [12].

6) *Privacy*
Like other traditional networks, the sensor networks have also force privacy concerns. Initially the sensor networks are deployed for legitimate purpose might subsequently be used in unanticipated ways. Providing awareness of the presence of sensor node sand data acquisition is particularly important.

B. High Level Security Mechanisms

1) *Secure Group management*
Every node in wireless sensor network has the limited computational and communication capabilities. All the activities in a network like data aggregation and analysis of data can be performed by the group of nodes. In actual the nodes as comparing of the group may change continuously and quickly. The key services are also be performed by the group. That's why the secure protocol for group of nodes are to be needed, to securely admit new group members and provide the secure communication to newly admitted member within the group. The outcome of group key is transmitted to the base station. It is ensured that the output is authenticated and coming from authorized group. The group key must be managed by the group members and protects from outside member (nodes) or unauthorized nodes.

2) *Secure Data Aggregation*
The fine grain sensing is the advantage over the wireless sensor network which is provided by the dense sets of nodes. The data sensed by the different nodes in the network must be aggregated to avoid the huge amount of traffic back to the base station. Suppose a system may average the temperature of the geographic region, combine sensor values to compute the velocity and location of s moving object, or aggregate the data to avoid the false alarms in real-world event detection. The aggregation may

done on more than one place of the network, it is depend on the architecture of the wireless sensor network and all location of the WSN must be secured.

V. Conclusion

In this paper we surveyed on existing attacks on wireless sensor network. We have also covered the security mechanism and challenges in WSN. In Security attack we describe all the attack which is passive in nature or active in nature. In challenges for WSN security we describe some challenges due to limited resources, unreliable communication and unattended operation. And in security mechanism part we describe how to detect prevent and recover from security attacks. This paper helps the readers to have better view of attacks, security mechanism and challenges in WSN.

References

[1] A. D. Wood and J. A. Stankovic. Denial of service in sensor networks. Computer, 35(10):54–62, 2002.
[2] Hu, Y.-C., Perrig, A., and Johnson, D.B., "Packet leashes: a defense against wormhole attacks in wireless networks", Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE INFOCOM 2003, Vol. 3, 30 March-3 April 2003, pp. 1976 – 1986
[3] Adrian Perrig, John Stankovic, and David Wagner, (2004) "Security in wireless sensor networks", Commun.ACM,47(6):53-57.
[4] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", AdHoc Networks (elsevier), Page: 299-302, year 2003
[5] Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong, "Security in wireless sensor networks: issues and challenges" Advanced Communication Technology (ICACT), Page(s):6, year 2006
[6] Yong Wang, Garhan Attebury, and Byrav Ramamurthy "A survey of security issues in wireless sensor networks" 2nd quarter 2006, volume 8, NO. 2 IEEE communication surveys
[7] Jaydip Sen "A survey on wireless sensor networks security" International Journal of Communication Networks and Information Security (IJCNIS) Vol. 1, No. 2, August 2009
[8] Al-Sakib khan Pathan et.al,(2006) "Security in wireless sensor networks: Issues and challenges" in feb.20- 22,2006,ICACT2006,ISBN 89-5519-129-4 pp(1043-1048)
[9] C. Karlof and D. Wagner, (2003). "Secure routing in wireless sensor networks:Attacks and countermeasures," AdHoc Networks Journal, vol. 1, no. 2–3,pp. 293–315, September
[10] Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong, "Security in wireless sensor networks: issues and challenges" Advanced Communication Technology (ICACT), Page(s):6, year 2006
[11] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks" (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009
[12] Vikash Kumar, Anshu Jain and P N Barwal, Wireless Sensor Networks: Security Issues, Challenges and Solutions, International Journal of Information & Computation Technology.ISSN 0974-2239 Volume 4, Number 8 (2014), pp. 859-868.