iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** III **Month of publication:** March 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

A Comparative Study of Techniques Used in Detection and Prevention of Black Hole Attack in Wireless Sensor Networks

[1]*Jaspreet Kaur*, [2]*Tavleen Kaur*
[1,2]*Department of Computer Science & Engineering* SUSCET, Tangori, Mohali, Punjab, India

Abstract *This Paper reviews about the wireless sensor networks architectures, applications, characteristics, benefits, types of wireless sensor networks and attacks and their detection and prevention techniques of attacks. Wireless sensor networks are increasingly deployed in a variety of applications a like military application and medical, monitoring the climate, commercial and home application and so on .The aim of this paper is to make sensor network secure from various attacks. In black hole attack the set of nodes re-program the nodes and block the packet forwarding to the base station In this paper, we present a survey of the main types of attack at in wireless sensor network and then we review detection and prevention techniques used in wireless sensor networks. We classify these techniques of detection and prevention and comparison of these techniques is also included in this paper.*

Keywords: *WSN, Black Hole Attack, Black Hole Attack detection and prevention techniques,*

I. INTRODUCTION

A wireless sensor network (WSN) is a network made of numerous independent small sensor nodes. They are self-configuring units consisting of a battery, sensors, and a minimal amount of on-board computing power. A wireless sensor networks consist of a lightweight, un-tethered, battery-powered device, it has limited source of energy. Therefore, energy consumption is a main issue in sensor networks. When the attack is happen in this sensor networks it takes more battery power to detect the attacks.

In architecture of WSNs there are two other components, called "aggregation "and "base station" which have more resources than normal sensors. Aggregation to collects information from the sensors nodes and then forward to the base station to process gathered data, as shown in figure1. Each node is to collect data and route data back to the sink (Base Station).Protocols and algorithms with self-organization. Nodes have interacted with each other and process the sensed data. Limitations such as cost, invisible deployment and variety application domains, lead to requiring small size and limited resources (like energy, storage and processing) sensors. [2]

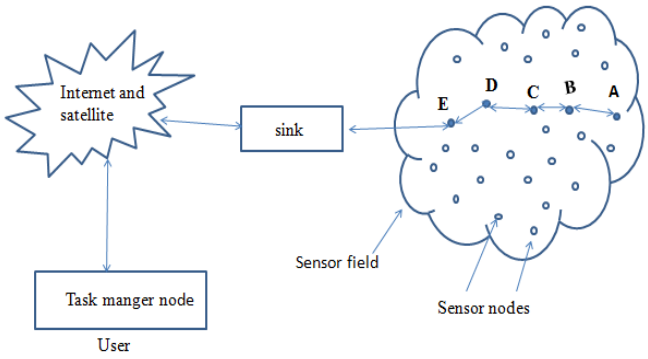


Figure1. WSN's architecture [2]

The sensor's components are: sensor unit, processing unit, Storage unit, power supply unit and wireless radio transceiver, these units are communicating to each other, as shown in figure 2The existing components on WSNs architecture are including sensor nodes (motes) transceiver is act as a base stations (access point or gateway)[2]

ISSN: 2321-9653

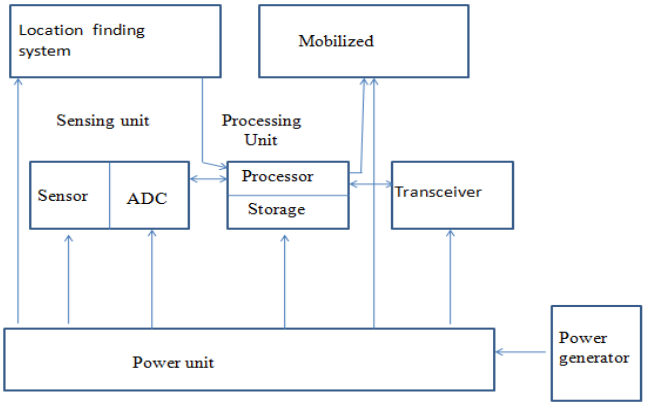


Figure2 .WSN node architecture [2]

II. CHARACTERISTICS OF WSNs [4]

The characteristics of wireless sensor networks are shown as follows:-

a. Security
b. Power supply
c. Memory space
d. Bandwidth
e. self –organized
f .Unreliable of communication
g .Ability to handle node failures
h. Mobility of nodes
i. Scalability to large scale of deployment
j .Ease of use

III. TYPES OF WIRELESS SENSOR NETWORKS [4]

There are five types of WSNs: Underground WSN, Underwater WSN, Multi-media WSN, Terrestrial WSN and Mobile WSN

A. Underground WSNs

In this we operate below the ground surface. The devices placed within a bounded open underground space like roads, tunnels and mines under dense soil.

B. Underwater WSNs

They consist of a number of sensor nodes. Underwater WSNs can be used to temperature gradients (thermo cines), monitoring ocean currents and weather , biological ,forecast monitoring and other possible application .In this it has limited bandwidth**.**

C. Multimedia WSNs

They must provide relatively low end-to-end delay and jitter and high throughput while being energy efficient. Multi-media WSNs have been proposed to enable tracking and monitoring of events in the form of multimedia such as video, sounds and image. It has of low cost sensor nodes.

D. Terrestrial WSNs

They consist of thousands of wireless sensor nodes in a given area, either in a pre-planned (according to the requirement) or in an ad hoc manner. In this the battery power is limited and cannot be recharged again and again

E. Mobile WSNs

The Applications include environment monitoring, target tracking, search and real-time monitoring of material. security is main feature. It has more channel capacity

IV. BENEFITS OF WIRELESS MEASURMENT

- Less installation cost
- Low Maintenance cost
- Less downloading time need
- Unreliable communications
- Easily access data almost anywhere and anytime
- Increase Efficiency

V. APPLICATIONS OF WIRELESS SENSOR NEWORKS

ISSN: 2321-9653

The sensor networks have been used in the high-end applications. A short list of applications as follows.

A. *Military applications*:

Monitoring land (good for framing), Monitoring equipment, Military-theater or battlefield surveillance, Targeting, aircrafts Battle damage assessment, Nuclear, biological, chemical attack detection, area monitoring

*B .Environmental applications***:**

Microclimates, Forest fire detection, Flood detection and Precision agriculture, pollution control, landslide detection and check water quality, earthquake observation and more

*c. Health applications***:**

Remote monitoring of physiological data, Tracking and monitoring doctor and patients inside a hospital, Drug administration, and more

*d. Home applications***:**

Home automation, Instrumented environment, automated meter reading, home using electrical machines and more

e. Commercial applications:

Environmental control in industrial and office buildings, Inventory, traffic control Vehicle tracking and detection.

VI. Security in WSN

Security is the major issues in wireless sensor networks. WSNs are affected by various types of attacks. These attacks can be categorized as:

- Attacks on authentication
- Silent attacks on service
- Attacks on network

There are mainly two types of attacks

A. Active Attacks

Active attacks are those attacks which are performed by the malicious nodes. It involves some modification of data stream or creating the false stream.

The following attacks are active in nature

- Routing Attacks in Sensor Networks
- Denial of Service Attacks
- Node Subversion
- Node Malfunction
- Node Outage
- physical Attacks
- Message corruption
- False Node
- Node Replication Attacks
- Information gathering

B.Passive Attack

In passive attacks the attacker does not disturb the routing protocol. Passive attack is in nature of eavesdropping on, or monitoring of transmission. Passive attacks are very difficult to detect because they do not involve any modification of data

ATTACKS IN WIRELESS SENSOR NETWORKS **[3]**

The Sensor networks are self-organizing networks which, once deployed, are expected to run autonomously. Attacks are harmful for the networks the destroyed the system and has great effect on database. In some cases lost data is recoverable. Major attacks on sensor networks are as follow:

Some of active attacks on routing

- *Jamming*

Jamming is one of the basic attacks in which it uses to interfere with the radio frequencies of the sensor nodes. A few jamming node can put a considerable amount of the nodes

ISSN: 2321-9653

out of order. Jamming can be of two types of constant jamming and intermittent jamming. Constant jamming complete affects on whole network whereas in intermittent jamming nodes are not communicating continuously

- *Tampering*

A Tampering attack is attack which damage a sensor nodes and replaces the entire node or part of its hardware

- *Worm Holes Attack*

Worm hole attack which records the packets which is send to the one location in the networks In these attacks the tunnels messages received in one part of the network over a low latency link, and another part of the network where the messages are replayed. It is leading to quick exhaustion of the energy resources.

- *Hello Flood Attack*

Hello flood attack is attack in which HELLO message is send by anther neighboring node within radio transmission range. It gives illusion to the malicious node. When the nodes will send message to the base station, then it passes through the malicious node and this node provides the shortest route to the base station as an illusion. When the information reaches the attacker, the victim is betrayed by it. This leads to data congestion and data flow in the network.

- *Spoofed, altered or replayed routing information*

This is the attack which is directly attack on the network. By spoofing, altering or replaying routing information the attacker can complicate the network and create routing loops, attracting or repelling traffic, generating false error message, shortening or extending services router or partitioning the network shortening or extending services router or partitioning the network which increases end-to-end latency and effect on speed on network.

- Selective Forwarding

This layer is attack on network layer. This is selective and forwarding In sensor networks This layer is attacks on network layer. In sensor networks the nodes are forward received messages but some compromised node refused to forward packets, however neighbors node start using connect to another route.

- *The Sybil Attack*

This layer is attacks on network layer. A malicious node presents multiple identities to the network. This attack is to geographic routing protocols appears to be in multiple locations at once.

- *Black Hole Attack*

A black hole attack is an attack that is adversary on a subset of the sensor nodes in the network. The adversary captures these nodes and re-programs them so that they do not transmit any data packets, namely the pack supposed to forward. Wireless Sensor Networks (WSNs) are many attacks from which Black hole is one of them. Black hole attack is one of the security threats in wireless sensor networks. There is an increasing threat of attacks on the wireless sensor networks. A black hole is a just like as Denial of Service (DoS) attack which is very difficult to detect and remove . In black hole attack, an intruder captures and re-programs a set of nodes in the network to block the packets they receive instead of forwarding them towards the base station.

- *Denial of services*

DOS attack is the simplest attack. . Sending extra packets which destroy the network. In wireless sensor networks, the different types of DoS attacks is can be performed on layers At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack resynchronization .

- *Node Subversion*

ISSN: 2321-9653

It is attack which Capture anode information which includes the disclosure to cryptographic keys and compromise the whole sensor network with it.

Some of Passive Attacks

- *Attacks against Privacy*

The information from sensor networks is collected through direct site surveillance. In privacy problem because they make large volumes of information easily available through remote access .The more common attacks against sensor privacy are as follows as:

1) Monitor and Eavesdropping:

The most common attack to privacy is to analysis sensor network When the traffic conveys to the control information about the sensor network configuration, which contains each detailed information. Which is easily accessible through the location server, the eavesdropping can act effectively against the protection for privacy.

1) Traffic Analysis:

When the messages transferred are encrypted, it still has a high possibility to analysis the pattern of communication. It causes malicious harm to the sensor network.

2) *Camouflage Adversaries***:**

The nodes which are hide in the sensor network are copy to the normal node which attract the packets and then misguide the route packets.

V. TECHNIQUES USED FOR DETECTION AND PREVENTION OF BLACK HOLE ATTACKS

The following techniques used for detection and prevention for black hole attack as shown in following table 8.1

Techniques	**Description**	**Problem**

ISSN: 2321-9653

Exponential Trust Based [4]	• A Streak counter is store the consecutive number of packets dropped and a trust factor is maintained for each node. The trust factor drops exponentially with each consecutive packet dropped which helps in detecting the malicious node. • In this technique, we maintain a table in the memory which stores the trust factor of each node. This uses a streak counter which keeps a record of count of consecutive packets dropped. This method show a decrease in the number of packets dropped before the node being detected as a malicious node. • The trust factor of a node is calculated by this formula 100(x^n	Fault tolerance of the network is very less
REWARD (receive, watch, redirect) [5]	• It is stand for (receive, watch, redirect) which is link with replication • The algorithm for finding out the single black holes or group of malicious nodes. The routing technique is used for network nodes and their transmit power supply. • REWARD forwards packets by using geographic location of router. The data base keeps records for suspicious node • The algorithm has two types of messages which are MISS and • SAMBA, MISS (material for intersection of suspicious sets) message helps to identify malicious nodes SAMBA (suspicious area, mark a black-hole attack) it help to detect physical space and provides locations of detected black hole attacks, it has counter which count each node before transmission SAMBA messages will decline its efficiency. • REWARD allows to security feature and lifetime performance.	. REWARD is more suitable with dense networks where is easier to find neighboring nodes scaling the distance .

ISSN: 2321-9653

Techniques	Description	Problems
TBESP Algorithm (Topology Based Efficient Service Prediction) Algorithm [6]	• TBESP is stand for Topology Based Efficient Service Prediction (TBESP) algorithm • It used to choose the best topology as per the network service requirement under black hole attack. This algorithm is used to analysis the performance of two WSN's topologies. Tree and Mesh. • By using this topology we able to choose the best topology which is easily detect and remove the black hole attacks from wireless sensor networks • WSN prone to black hole attack and requires time efficient network service for information exchange then Tree Topology is to be chosen. • If it requires throughput efficient service in the network then Mesh topology is used.	This only used for choosing the two topology are Tree and Mesh as per the required in wireless sensor network under black hole attack.
Virtual Edge Based Coverage Hole Detection Algorithm in Wireless Sensor Networks [7]	• The locations of each node in randomly in wireless sensor networks • An improved hole detection algorithm is based on the Boolean sensing model. The algorithm screens out hole-boundary nodes by using the Voronoi Diagram. • Voronoi diagram which is a fast and easy to detect black hole But it can only express the holes locations with vertexes of Voronoi polygons, rather than describe locations and shapes of holes accurately • The location information of coverage holes, is introduce a new method called Virtual Edge to calculate boundary nodes. • The algorithm used to get the more accurate result for location, shape and area information of coverage of black holes attacks.	The error is difficult to handle
Energy Efficient Intrusion Detection System for Black Hole Attacks in WSN [8]	• Black hole attacks target sensors routing protocols which is impact on hierarchical routing protocols. Several solutions for security is used but the most complex solutions is energy in efficient. • A hierarchical energy efficient intrusion detection system is to protect sensor network from black hole attacks. • It is simple and based on comparison of control packets between sensor node and base station. By using this technique we get better result. • The alarm packet which contains identifier of node table is maintained in this • LEACH protocol is used to maintain the network in a cluster based topology.	Attacker node is to select the cluster head again and again which leads to more attack on black hole

Table 8.1 Techniques used for detection and prevention of Black Hole Attack

ISSN: 2321-9653

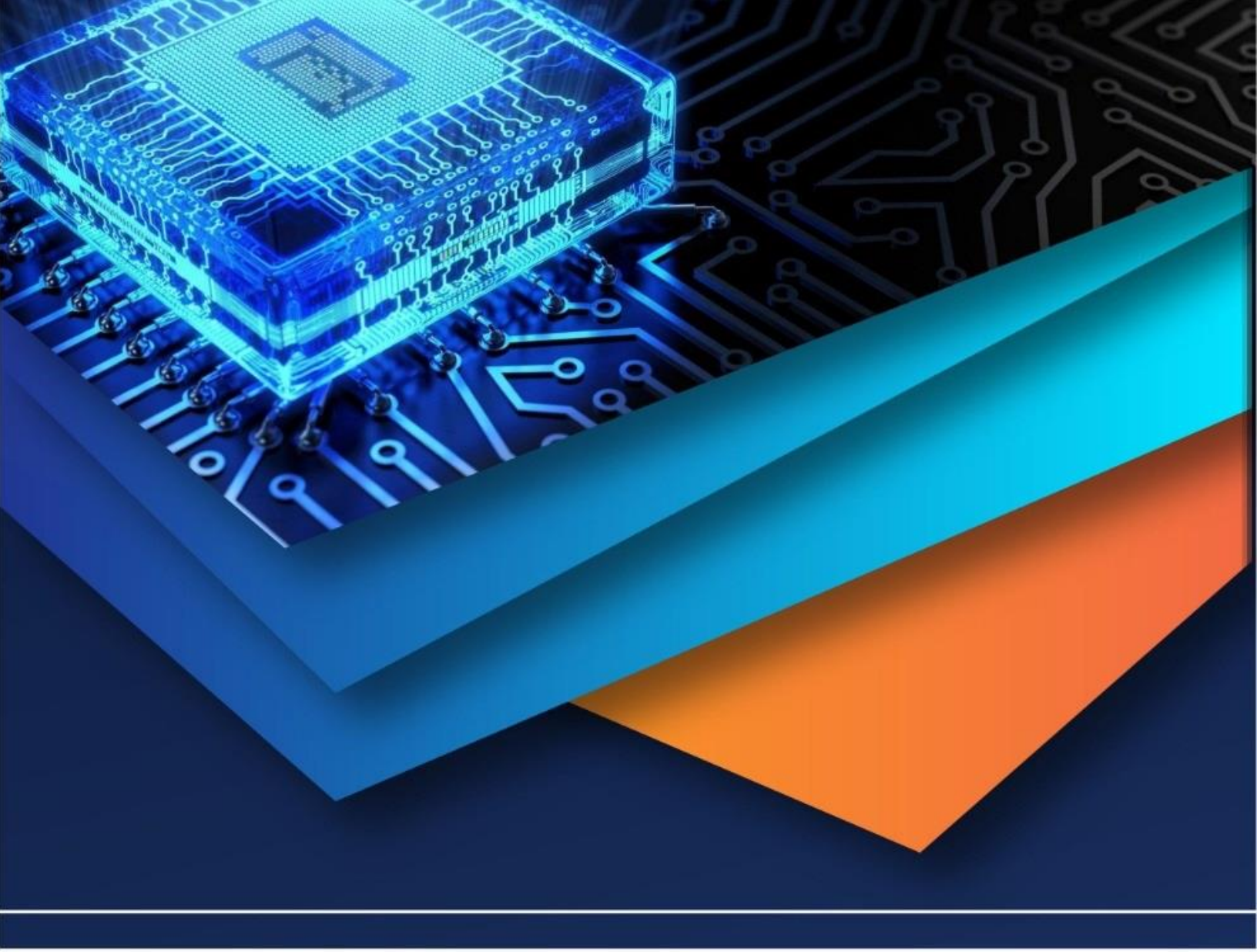
VI. CONCLUSION

In this we have a brief survey on wireless sensor network, characteristics, types of WSNs benefits and its application Then we discussed about the security in sensor networks, various attacks in wireless sensor networks and techniques used for detecting and prevention of black hole attacks on wireless sensor networks. Security is an important requirement

and complicates enough to set up in different domains of Wireless sensor networks. From this comparative study we get an overview of the techniques used for detection and prevention of black hole attack.

REFERENCE

1. www.visualsoftindia.com/journal.html
2. K. Sharma and M. K. Ghose; Wireless Sensor Networks: An Overview on its Security Threats; IJCA, Special Issue on *"Mobile Ad-hoc Networks*" MANETs; CSE Department, SMIT, Sikkim, India; 2010.
3. Aashima Singla, and Ratika Sachdeva *Student Masters of Technology,Department of CSE Sri Guru Granth Sahib World University Fatehgarh sahib, Punjab, India" Review on Security Issues and Attacks in Wireless Sensor Networks" 2013*
4. Dr. Deepali Virmani 1, Manas Hemrajani 2, Shringarica Chandel3 *Bhagwan Parshuram Institute of Technology,* "*Exponential Trust Based Mechanism to Detect Black Hole attack in Wireless Sensor Network"*
5. Zdravko Karakehayov University of Southern Denmark and Mads Clausen Institute Grundtvigs Alle *"Using REWARD to detect team black-hole attacks in wireless sensor networks*"
6. Mohammad Wazid, *Student Member, IEEE,* Avita Katal, *Student Member, IEEE* and R H Goudar "*TBESP Algorithm for Wireless Sensor Network under Black hole Attack" 2013*
7. Yunzhou Zhang1,2, Xiaohua Zhang1, Zeyu Wang1, Honglei Liu College of Information Science and Engineering , Shenyang SIASUNG Robot & Automation Northeastern University Company, Ltd. Shenyang, P.R.China *"Virtual Edge Based Coverage Hole Detection Algorithm in Wireless Sensor Networks" IEEE 2013*
8. Samir Athmani1, Djallel Eddine Boubiche2 and Azeddine Bilami Computer Sciences Department. M'Sila University. Computer Sciences Department. UHL Batna. *"Hierarchical Energy Efficient Intrusion Detection System for Black Hole Attacks in WSNs*" IEEE 2013
9. www.en.wikipedia.org/wiki/ Wireless sensor network



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY