International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2015): 6.391

Leach Protocol in Wireless Sensor Network

Tegendra Sahu[1], **Abhishek Badholia**[2]

Central College of Engineering and Management, Dept. of Computer Science and Engineering, Raipur, Chhattisgarh, India

Professor, Central College of Engineering and Management, Dept. of Computer Science and Engineering, Raipur, Chhattisgarh, India

Abstract: ***Wireless Sensor Network (WSN) is a network comprises of vast number of low power sensor hubs. LEACH is a less vitality versatile protocol. The primary objective of cluster based sensor systems is to minimize framework delay and reduce energy utilization. LEACH is based on clustering technique for micro sensors which can able to achieve scalable routing, energy efficient and fair routing for sensor nodes. Numerous enhancements are done in wireless sensor network. Security is exceptionally fundamental in remote sensor arrange. This paper reviews LEACH convention, their preferences, drawbacks and so forth. This paper also presents some the attacks on LEACH protocol and its consequences and effect on sensor nodes. This paper proposes a novel mechanism for dealing with WSN sensors in case of attacks using Basic Leach, M-Leach and Leach-B. The proposed mechanism outperforms the existing ones like basic leach protocol.***

Keywords: LEACH Protocol, Attacks, Wireless Sensor Networks, Routing, Security.

1. Introduction

Wireless Sensor Network includes of a huge amount of small and low cost sensor nodes which are randomly implement in an area. The sensor nodes have computational capability to carry out simple computations and transmit the needed information [1]. These nodes helps to transmit information to the sink node that calculates the whole information received from other nodes and evaluate summary information to be transmitted to the other network. These nodes of sensor can collectively monitor the physical conditions as well as environmental conditions like temperature, humidity, pressure, and sound vibrations. Such characteristics ensure a huge variety of applications for wireless sensor network such as disaster relief medical, industrial, environmental monitoring, operations, military, traffic surveillance, agriculture, infrastructure monitoring [2].

Hence, the majority of sensor nodes are implemented in hostile environment, they are susceptible to different attacks that are caused by malicious or compromised nodes in the network. The malicious nodes can alter the normal behavior of the network, tamper with the node's hardware and software, communicate false information, or drop the needed information. Therefore, the security of wireless sensor network becomes a critical problem.

1.1 Security Goals in Wireless Sensor Networks

A wireless sensor network provides some common characteristics with the traditional network and also has some unique features of its own that differentiate it from the traditional network. Hence, the security goals or needs cover both the traditional network goals as well as the goals suited solely to the wireless sensor network. The security goals are:

1) Data Confidentiality
Sensor nodes can carry sensitive information which must be hidden from the malicious nodes or attackers. If sensor nodes are not able of keeping the information confidential, then any neighboring node can interfere with the data and transmit false information. This can cause crucial hazards, especially in military applications.

Confidentiality refers of limiting data access to only the authorized users and restricts access or disclosure by the users who are unauthorized. Data confidentiality is the most essential problem that any network must address.

2) Data Authentication
Data authentication is the verification by the receiver that helps to receive information from the correct sender. In a wireless sensor network, data can not only be interfere by the malicious nodes but the whole packet stream can be modified by addition of false packets to it.

Therefore, a receiver must be able to classify if the data transmit from the correct source or not. Information validation can be completed by utilizing symmetric key cryptography where the sender and receiver communicate a mystery key or utilizing lopsided key cryptography where the data can be scrambled and decoded by utilizing open and private keys.

3) Data Availability
Data availability figures out whether the administrations of the system are accessible if there should arise an occurrence of disappointment on the other hand nearness of assaults in the system. A solitary point disappointment in the system can debilitate the accessibility of assets and different administrations. In this way, data accessibility is of prime significance and is in charge of the operation of the system.

4) Data Integrity
The data integrity in the system can control the information in the packets [3]. Information uprightness guarantees that the got information is not modified in transmit. It affirms that the information is dependable and has not been modified or changed. The system must incorporate security methods against various attacks created by malicious nodes in order to guarantee integrity of the information.

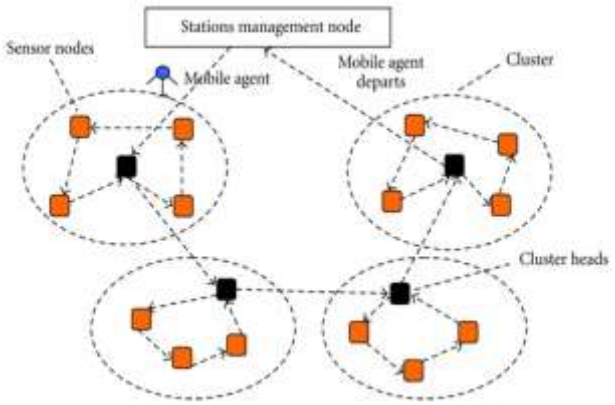

Figure 1: Shows the wireless sensor networks arrangement

2. Attacks in WSN and its Counter Measures

This section of review paper deals with various attacks on WSN. There are various layer like Physical, Network, Transport on which attacks by attacker are made. They are described below.

A. Physical Layer
- Attack: Jamming
- Protection: Mode Changing

B. Link Layer
- Attack: Collision
- Protection: Error Correcting Code

C. Network Layer

Table 1: Shows various Network Layer Attacks

Attacks	Protection
Sink Hole	Redundancy Checking
Sybil	Monitoring of Authentication
Wormhole	Probing
Acknowledgement Flooding	Link Verification

D. Transport Layer
- Attack: Flooding
- Protection: User Authentication

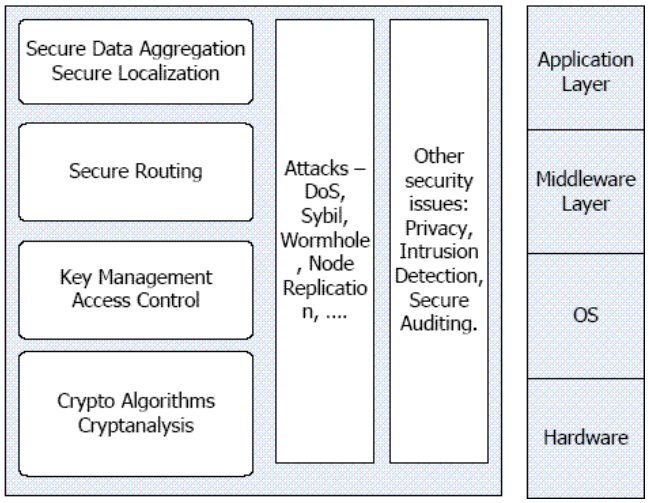

Figure 2: Security Architecture of WSN

3. Literature Survey

1) SecLEACHon the security of clustered sensor networks

L. B. Oliveria et al. [4] Clustered sensor networks have been shown to increase system throughput, decrease system delay, and save energy. While those with rotating cluster heads, such as LEACH, have also advantages in terms of security, the dynamic nature of their communication makes most existing security solutions inadequate for them. In this paper, author shows how random key pre distribution, widely studied in the context of flat networks, can be used to secure communication in hierarchical (cluster-based) protocols such as LEACH. To our knowledge, it is the first work that investigates random key pre distribution as applied to hierarchical WSNs.

Method Used: F-LEACH

Strength: FLEACH provides authenticity, integrity, confidentiality and freshness to node-to-node communication.

Limitation: it is vulnerable to node capturing attack.

2) Cluster based secure routing protocol for WSN

R. Srinath et al. [5]. This protocol is based on LEACH protocol; named Authentication Confidentiality cluster based secure routing protocol. It uses both public key (in digital signature) and private key cryptography.

Method Used: improved LEACH

Strength: This protocol deals with interior adversary or compromised node.

Limitation: high computational requirement (use of public key cryptography), it is not efficient for the WSNs.

3) Detection of HELLO flood Attack on LEACH Protocol Revisited

Shikha Magotra et. al. [6] present the new non cryptographic approach EBDS (Energy based detection scheme) which detect the attacker by calculating the energy of nodes. As we know when attacker starts dropping the packets its energy starts decreasing and it becomes the low energy node when compare with other nodes.

Method Used: LEACH and RSS

Strength: Efficient for finding RSS value and distance between nodes and cluster head to find malicious node.

Limitation: Where the non CH nodes are located closely to the adversary node.

4) A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management

C.Wang et. al. [7] investigate adding security to cluster-based routing protocols for wireless sensor networks which consisted of sensor nodes with severely limited resources, and propose a security solution for LEACH, a protocol in which the clusters are formed dynamically and periodically. Our solution uses improved random pair-wise keys (RPK) scheme, an optimized security scheme that relys on symmetric-key methods; is lightweight and preserves the core of the original LEACH. Simulations show that security of RLEACH has been improved, with less energy consumption and lighter overhead.

Method Used: SLEACH, LEACH

Strength: a light weight and optimized security scheme that rely on symmetric-key methods.
Limitation: SLEACH cannot prevent to crowd the time slot schedule of a cluster, causing DoS attack or simply lowering the throughput of the CH and does not guarantee data confidentiality. It protects only outsider attack.

5) Hello Flood Attack and its Countermeasures in Wireless Sensor Networks

Virendra Pal Singh et al. [8] proposed a technique in the paper Signal Strength based HELLO Flood Attack Detection and Prevention in Wireless Sensor Networks using AODV protocol. They have used a threshold for RSS i.e. fixed signal strength for sensor nodes, and the RSS of the each received HELLO packet is compared to this threshold.
Method Used: AODV protocol
Data Source: Text Document
Strength: ADOV protocol effectively stops flooding attack.
Limitation: Nodes which are significantly far from adversary will wrongly categorize the adversary as 'Friend'.

4. Related Work

Setup Phase

In this stage, the hubs are introduced in the zone to be observed. After the hubs get moved to their positions, the procedure of cluster arrangement is performed. Groups uniformly disperse the energy all through the system. The groups are framed by isolating the system as per the separation secured. The hubs falling in a particular region go have a place with a group.

Cluster Head Selection

After the underlying set-up is finished; the CH race is to be finished. For introductory choice of CH, irregular hubs are picked in each CH. These hubs go about as 'Initiators'. The initiator hubs request that each part hub give its energy status. Once the energy levels of all hubs detailed; the initiator hub sort down the rest part hubs as indicated by diminishing level of their comparing energy levels. The hub with most extreme energy level is picked as CH.

Communication Phase

After CH get chose, the correspondence procedure begins. The hubs sense information. This detected information is gathered by CH for information accumulation process. To report this information to the Sink hub, the Multi-bounce way is taken after. The Multi-bounce way is characterized as the CHs of different bunch falling while in transit to the BS. The Multi-jump has turned out to be immensely vitality effective approach, particularly to implement wide zone WSNs.

CH Rotation Phase

At the point when a series of correspondence finishes, the CH revolution process is completed as if there should arise an occurrence of straightforward LEACH and B-LEACH. In proposed M-LEACH, the following hub in the arranged rundown is chosen as new group. Putting away the vitality levels in beginning disposes of the overhead of contrasting vitality levels of all hubs unfailingly. After the race of the following round CHs, the entire correspondence process happens as delineated in Figure 1.

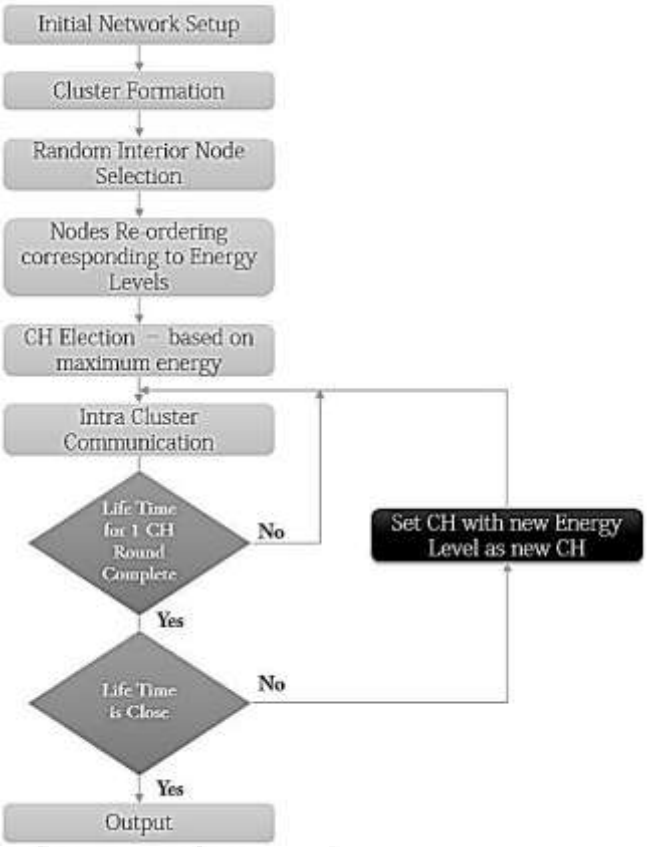

Figure 1: Shows the proposed system architecture

Table 1: Network Deployment Parameter

SNO	Parameter	Values
1	Field Dimension – Nodes Setup	X = 200 m and Y = 200 m (m = meters)
2	Number of Nodes in Field	10
3	Optimal Election Probability of a node to become cluster head	P = 0.1
4	Initial Energy	Et = 50 Eo = 0.5
5	Data Aggregation Energy	EDA = 5*0.000000001
6	Maximum Number of Rounds	2500

5. Simulation Results and Analysis

We have implemented the following steps to get a clear understanding and analysis of the attack:

- Examine normal LEACH under various network parameters as above.
- Examine the LEACH with Black Hole attack under same network parameters.
- Detect the black hole node using below descried algorithm.

1) Performance Metrics

a) Packet delivery ratio

The ratio of the number of delivered data packet to the destination and the total number of packet sent to the destination. This illustrates the level of delivered data to the destination.
Packet delivery ratio= ∑Number of packet receive/ ∑Number of packet sent (Packets dropped+ packets received)

b) Throughput

Throughput can be defined as the number of bits successfully received through a network per unit of time.

Throughput = ∑number of bits received/Time

c) Remaining energy

It is defined as the residual energy of the node after sending data to the base station during the network lifetime.

2) Type Comparison

There are several leach we are used for alive nodes, packet send and energy consumption show in the figure

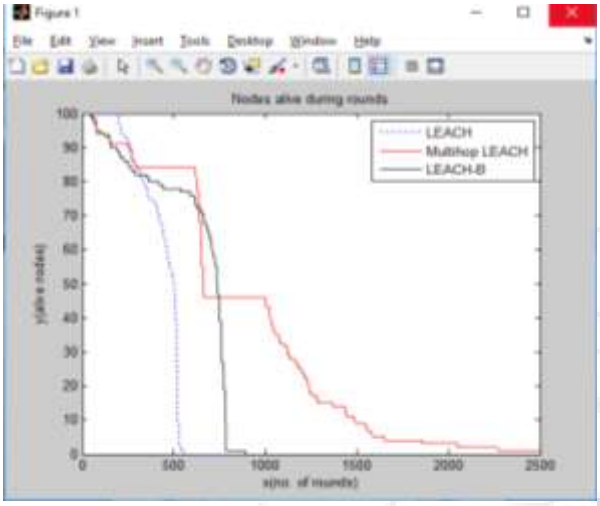

Figure 2: Nodes alive during nodes

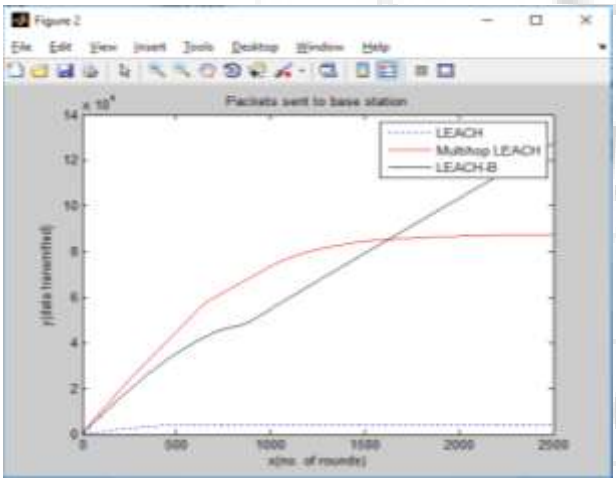

Figure 3: Packet send to Base Station

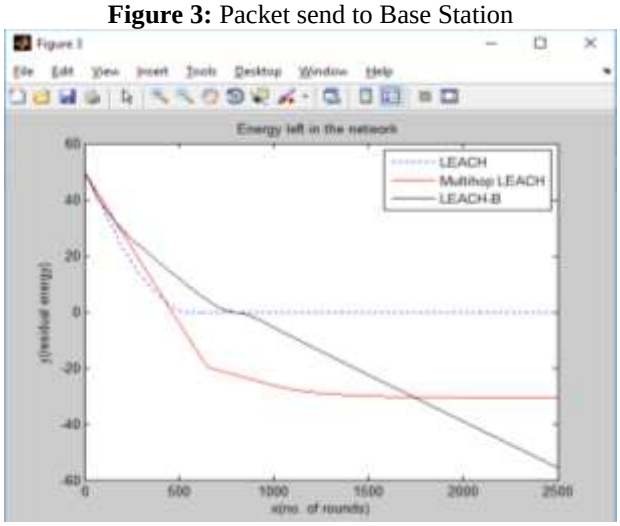

Figure 4: Energy left in the network

3) Performance Metrics of basic leach with and without attack

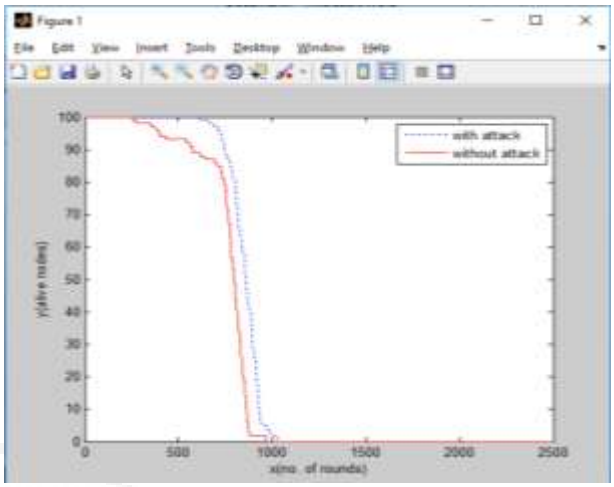

Figure 5: Alive nodes in basic leach with and without attack

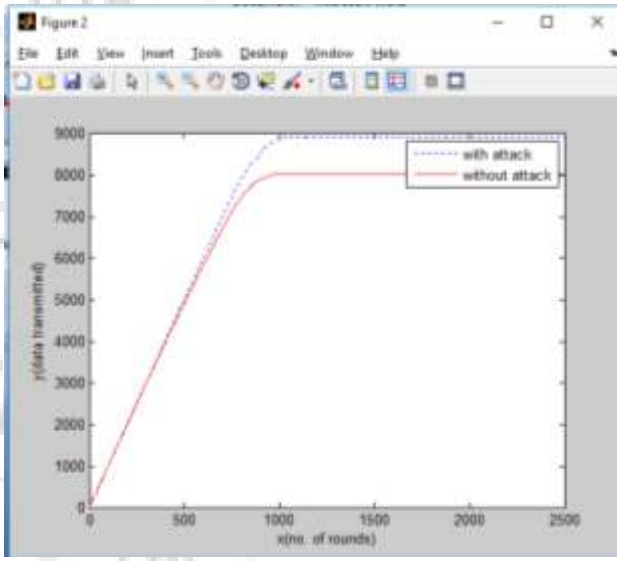

Figure 6: Data transimision of basic leach with and without attack

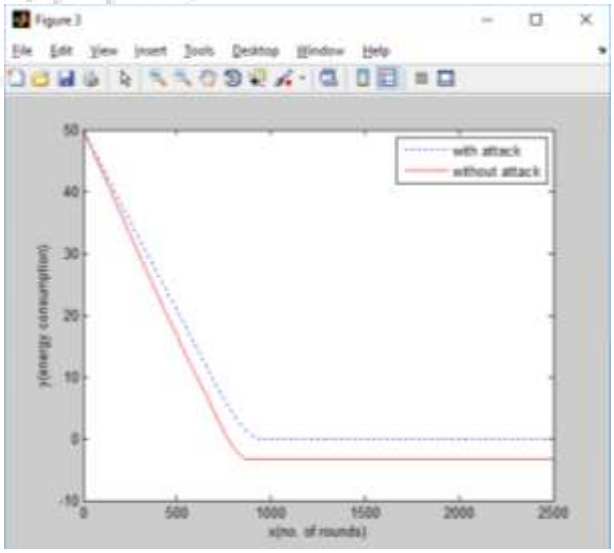

Figure 7: Energyconsumption of basic leach with and without attack

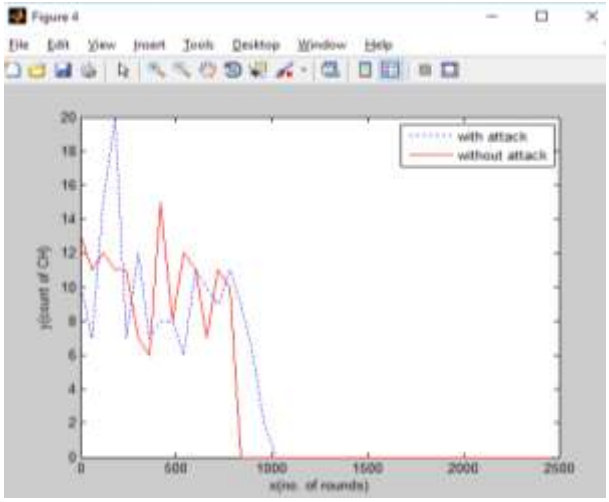

Figure 8: Count of CH in basic leach with and without attack

4) Performance Analysis for LEACH in Different types of Attack

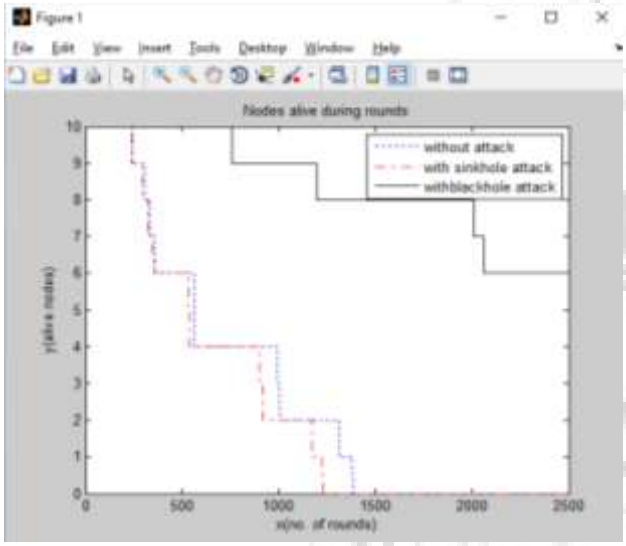

Figure 9: Alive nodes in different Attack

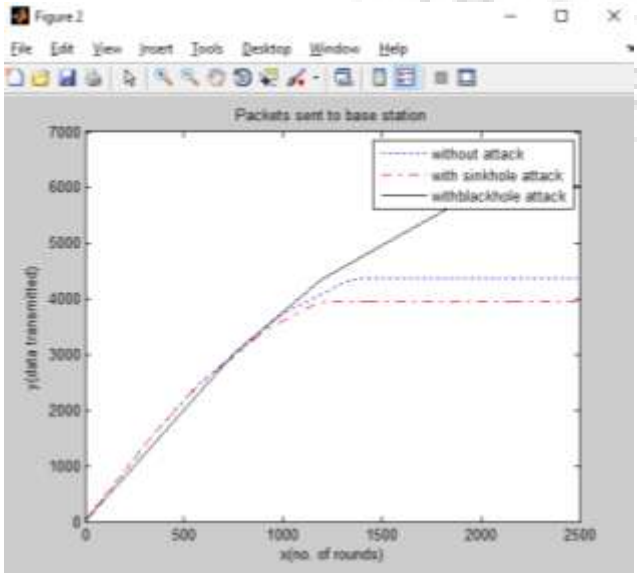

Figure 9: Data Transmission in different Attack

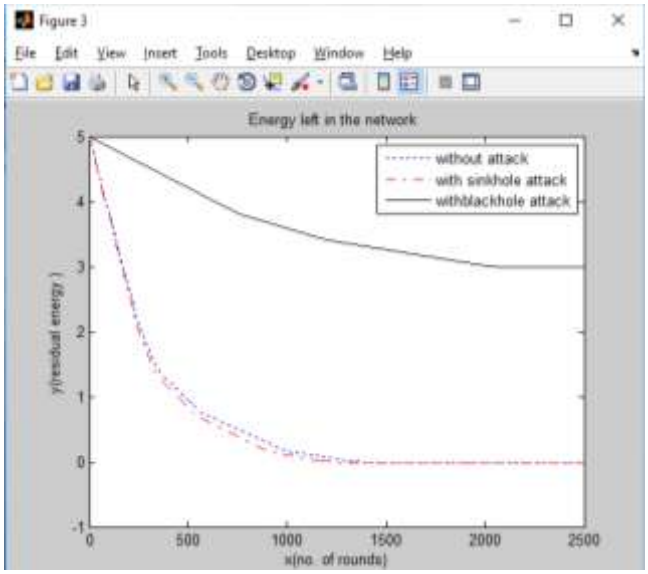

Figure 9: Erergy in different Attack

6. Conclusion

In the wireless sensor networks, the system hubs are utilized for sensing the data from the different sorts of non-reachable zones. In MWSNs the fundamental risk in the system is security. Different sorts of attack happened in systems. Attack happen in WSN is clone attack which is otherwise called replica attack. In this attack the hub duplicate the id of the other hub and demonstrate its forecasts at various areas. A replica hub can make a black hole or wormhole attack which can be used by attacker in various ways. This attack can transmit false data to all true legitimate hubs.

Primary issue in this is to identify the hub having clone attack, since every single hub has same id and areas at various positions on same interim of time. This issue has likewise been emerging in bunches in which groups repeat and the primary issue emerges when group head duplicate. This paper reviews various methods and protection techniques through which attacks are minimized or completely stopped.

References

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: A survey, Computer Networks”, pp. 393-422, 2000.
[2] A.S.K. Pathan, H.W. Lee, C.S. Hong, “Security in Wireless Sensor Networks: Issues and Challenges”, Communications, IEEE Transaction , Feb 2006.
[3] G. Padmavathi, D. Shanmugapriya,“A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks”, International Journal. Computer Science and Information Security, vol. 4, 2009.
[4] M. A. Vilaa H. C. Wong M. Bern R. Dahab L. B. Oliveira, A. Ferreira and A. A. F. Loureiro “SecLEACHon the security of clustered sensor networks,” vol.87, pp.2882-2895, December 2007.
[5] A. V. Reddy R. Srinath and R. Srinivasan “Cluster based secure routing protocol for wsn,” Third

International Conference on Networking and Services, pp.45, Washington, DC, USA, 2007.
[6] Shikha Magotra, Krishan kumar "Detection of HELLO flood Attack on LEACH Protocol," IEEE International Symposium on Network Computing and Applications, pp.145-154, Washington, DC, USA,2014.
[7] C.Wang K. Zhang and C.Wang "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," 4th International Conference on Wireless Communications, Networking and Mobile Computing, 2008.
[8] Virendra Pal Singh "Hello Flood Attack and its Countermeasures in Wireless Sensor Networks," IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 11, May 2010.