# IMPLEMENTATION OF A THRESHOLD BASED TECHNIQUE FOR ISOLATION OF SINKHOLE ATTACK IN WSN

Inderpartap Singh[1], Sukhjinder Singh Gill[2]
*[1]M.Tech Student, [2]Assistant Professor*
*LALA LAJ PAT RAI INSTITUTE OF ENGINEERING AND TECNOLOGY, MOGA*

***ABSTRACT*** **-** The wireless sensor networks is the type of network in which sensor nodes sense the environmental conditions and pass sensed information to the base station. To reduce energy consumption of the network LEACH protocol is applied which divide whole network in clusters and in cluster, cluster heads are selected on the basis of energy, distance. The sink hole attack is triggered in the network which reduce network performance. The mutual authentication technique is proposed which detect malicious nodes from the network. The performance of proposed technique is tested in NS2 in terms of various parameters

***KEYWORDS*** **-** *LEACH, THRESHOLD, ATTACK, SINK HOLE*

## I. INTRODUCTION

Wireless Sensor Network is a combination of tiny light weight wireless sensors with computing elements. These sensor nodes are generally cheaper in price, with limited energy storage and limited processing capabilities. Wireless sensor network consist of large number of these sensor nodes (usually hundred or thousand of nodes). These types of networks are highly distributed and deployed in hostile environments [1]. Wireless sensor networks monitor the system or surroundings by measuring physical parameters, for example, moistness, weight and temperature. WSNs are most appropriate for applications like natural life checking, military order, shrewd interchanges, modern quality control, and perception of basic bases, brilliant structures, circulated apply autonomy, movement observing, inspecting human heart rates, and so forth. . The battery present within the nodes of WSN is of smaller size. Also the nodes are located at really far distances where human is not able to reach. So the major concern within the WSNs is the usage of battery within them. This also affects the overall lifetime of the nodes and thus the deployment of the network. The sizes of various constraints such as battery size, processors, information storing memory and so on are important within these networks. The consumption of energy is required to be advanced within the networks with the help of various optimization algorithms. Various time constraints are present within the detected and routing information sent across the WSNs. Generally sensor nodes rely on a battery with restricted lifetime, and their replacement is impractical because of physical constraints. Moreover the architecture and protocol of sensor networks must have the capacity to scale up any number of sensor nodes. Since the battery lifetime can be extended on the off chance that one figure out how to reduce the measure of communication [2]. In the sensing subsystem energy consumption can be reduced by utilizing low power components.

The clustering includes grouping nodes into clusters and choosing cluster heads periodically such that individuals from a cluster can speak with their cluster heads and these cluster heads send aggregated data received from its individuals to a base station. In every cluster has a cluster head and rest nodes are individual from that cluster. Clustering results in a two-level order in which cluster heads shape the higher level while part nodes frame the lower level [3]. Since the cluster head regularly transmit data over longer separations, they lose more energy compared to part nodes. The clustering procedure is utilized to minimize the energy consumption. The LEACH is the protocol which is the most efficient protocol for clustering in wireless sensor network. In the LEACH protocol the cluster heads are selected randomly in the network on the basis of distance and energy. The cluster head get their sensor nodes on the basis of distance. The nodes which are closest to the cluster head will comes under the cluster head. The clusters are changes randomly on the basis of energy. The sensor node

which has maximum energy will be selected as a the cluster head in each round of data transmission. Due to decentralized nature of the sensor network energy consumption is the major issue which degrades the network performance. The security attacks are broadly classified into active and passive attacks. The active attacks are those which reduce network performance to great extend in terms of various parameters. The passive attacks are those which don't effects the network performance but may trigger active attack in future. Following are the various type of active attacks which are possible in wireless sensor networks:-

I. **Worm hole Attack:** In this a malicious node, records packets at a particular location in the network and tunnels them to another location. When the control messages are routing are tunneled it create disrupted. It is a network layer attack [7]. The solution to this problem is monitoring the network and flexible routing schemes.

II. **Black hole Attack:** In this attack malicious node captures and reprograms a set of nodes in the network and blocks the packets are received instead of forwarding them towards the base station. Any packet that enters into the black hole region is captured by the malicious node and never reaches the destination node. [8]

III. **Jamming Attack:** In this attack the radio frequencies are inferred that is used by the sensor node. Attacker monitors initially in order to verify frequency at which destination node is getting signal from the sender. Attacker transmits the signal on that frequency and powerful enough to disrupt the network 23].

IV. **Sink Hole Attack :** A scenario in which the attacker sends or replays the hello packets with the help of high transmission power for discovering the neighbor packet is said to have a hello flood attack. This helps in creating an illusion for the other nodes that the attacker is there neighboring node. This might further result in disrupting the routing protocol and causing other attacks also within the same network. The malicious node is selected as a parent node due to its ability to transmit packets with higher power. The messages that are to be broadcasted across the network are then passed through this parent node. This results in causing delay within the network. Within the huge WSN area, the hello messages are broadcasted to the numerous nodes by the attacker. The attacker node is thus convinced to be as the neighbor node by these various nodes within the network. The energy is depleted by sending reply to all such Hello messages by the nodes. There is also a confusion state caused within the network. The malicious node will redirect the whole network traffic to its side which cause denial of service condition in the network.

## II. REVIEW OF LITERATURE

Dr. G. Padmavathi et.al [2] introduced in their paper "A survey of attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", the security goals for sensor networks, various attacks in wireless sensor networks and the security mechanism related to different attacks. The paper also presented the challenges of sensor networks.

Maan younis Abdullah et al [4], review various challenges that a wireless sensor network faces due to the misdirectional attacks. This type of attack does not allow the packets to be received by the destination address. The packets are transferred to the other location. There is also another type of way of attacking the wireless networks by sending number of useless packets to the network. this acquires a lot of energy and the overall efficiency of the network reduces a lot. The latency also increases when the packets are misdirected. The intruder considers it as his main objective of not allowing the packets to be received on the other end or the destination.

Roshan Singh Sachan et al [5], discuss that there are various types of attack that the wireless sensor network faces. There are a lot of instances that have been occurring in which the detection of the attack of DoS and misdirection attacks has not been possible. The node in misled in such a way that the node reaches to any other node except for the destination node. The degradation of performance occurs due to such cases. Here in the article such an attack has been proposed on the topological analysis of the wireless network. An algorithm is proposed which will provide a help for the assistance in throughput and delaying of the packets. Better performance is observed in the tree network topology than in the mesh topology network.

Ju young Kim et.al [7] presented in their paper about the investigation of the distinctive vulnerabilities, threats and attacks for Wireless Sensor Networks. Viable administration of the threats connected with remote innovation requires a sound and through appraisal of danger given nature and advancement of an arrangement to relieve distinguished threats. An investigation to network supervisors comprehend

and evaluate the different threats connected with the utilization of remote innovation and various accessible answers for countering those threats are talked about. Remote Sensor Networks give a various chances to expanding profitability and minimizing costs.

Kalpana Sharma and M K Ghose [8] discuss the issue of security is because of the wireless nature of the sensor organizes and obliged nature of resources on the wireless sensor nodes, which implies that security models utilized for conventional wireless systems are not practical. Moreover, wireless sensor systems have an extra helplessness since nodes are regularly set in an unfriendly or risky environment where they are not physically secured. They have introduced the summery of the WSNs threats influencing diverse layers alongside their protection system. They infer that the guard system introduced just gives guidelines about the WSN security threats; the definite arrangement relies on upon the sort of application the WSN is sent for.

Roshan Singh Sachan et al [9] discuss that wireless sensor networks have faced many challenges, including the destruction of the wireless media, and the deployment of the ad hoc nature. There is a need to develop some new security systems which can prevent such attacks to occur. Misdirection attack which is a type of DoS attack is very difficult to be detected. The intruder leads the packet that has been sent from one end, to another end which in not the destination ends of the packet. There is an end-to-end delay in the transferring of the packets. The throughput of the network gets decreased. There is greater need to detect and remove the attack from the network. A cluster based intrusion and detection technique is designed. There are some parameters that are calculated by the method. These parameters provide raw information regarding the attack and the details of the packets sending and receiving information. The information is useful in detecting the origin of the attacks and traces the details. The method has helped thus, in detection of the attack and the prevention methods can be applied to it easily.

## III. PROPOSED METHODOLOGY

The wireless sensor network is much vulnerable to various type of security attack due to decentralized nature of the network. The sink hole attack is the active type of attack in which malicious node spoof the identification of the sink. The cluster heads transmit the data to the malicious node instead of base station. The sink hole attack is the denial of service type of attack which reduce network performance in terms of various parameters. The algorithm is been proposed in this paper which detect and isolate malicious nodes from the network. The proposed technique is based on the mutual authentication mechanism. The base station has unique identification which is the complex Armstrong number. The base station will localize the node location and assign the unique number to each node in the network. The cluster head before transmitting the data to the base station will ask their identification. The malicious node will not able to present the identification number of the base station to the cluster head. The cluster head will apply multipath routing to isolate malicious node in the network.

### 3.1. Proposed Algorithm

Input : Network with finite number of sensor nodes

Output : Detection of malicious node

1. Deploy wireless sensor network with the finite number of sensor nodes

2. Divide the network into fixed size cluster and select cluster head in each cluster based on distance, energy

3. Apply node localization ()

   I. Base station send ICMP message to each node in the network
   II. The nodes will reply back the hello message on the basis of received message , base station judge location of the sensor node

4. Assign Unique Number ()
   I. The base station generate unique number for each node in the network
   II. The generate number is the unique Armstrong number which is complex in nature and difficult to break
   III. The base station will also send its unique number of each node in the network

5. Mutual Authentication ()
   I. The cluster head ask unique identification number of base station
   II. If ( Base station fails to present unique number)
   III. Destination node detected as malicious node
   IV. Else

V. Authentication complete
VI. Data transmission starts in the network

## IV. RESULTS AND DISCUSSION

The proposed algorithm is based on mutual authentication for the detection of malicious nodes in the network. The NS2 is the simulator which is used to test the performance of proposed algorithm by taking simulation parameters described in the table 1

| Parameters | Values |
|---|---|
| Antenna type | Omi-directional |
| Channel | Wireless channel |
| Queue type | Priority queue |
| Number of nodes | 28 |
| Area | 800*800 meters |
| Frequency | 2.4 GHZ |
| Range | 18 meter |

Table 1: Simulation parameters

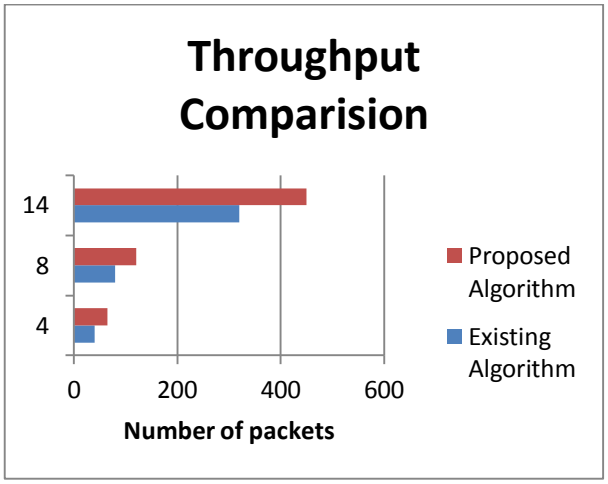


Fig 1: Throughput Comparison

The throughput of the proposed and existing algorithm is compared and it is been analyzed that due to isolation of sink hole attack in the network, throughput will be increased at steady rate

| Time | Existing per hop delay Algo | Proposed threshold Algo |
|---|---|---|
| 4 second | 68 packets | 76 packets |
| 8 second | 140 packets | 172 packets |
| 14 second | 260 packets | 420 packets |

Table 2: Comparison of Throughput

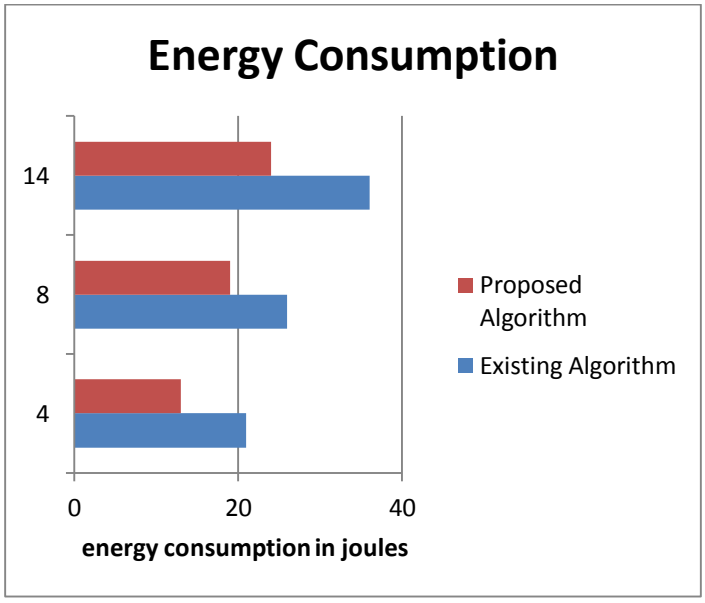


Fig 2: Energy Consumption Comparison

As shown in figure 2, the energy consumption of proposed algorithm is compared with the existing algorithm. It is been analyzed that energy consumption of the proposed algorithm is less due to isolation of sink hole attack in the network

| Time | Existing per hop delay Algo | Proposed threshold Algo |
|---|---|---|
| 4 second | 21 joules | 16 joules |
| 8 second | 26 joules | 19 joules |
| 14 second | 38 joules | 24 joules |

Table 3: Comparison of Energy Consumption

## V. CONCLUSION

In this paper, it is been concluded that due to decentralized nature of the wireless sensor network various type of active and passive attacks are possible in the network. The LEACH protocol is applied in the network which will cluster the whole network into fixed size cluster and cluster heads are selected in the cluster. The technique is been proposed in this paper, which isolate malicious nodes from the network which are responsible to trigger sink hole attack in the network. The proposed technique is implemented in NS2 and it is been

analyzed that network performance is increased at steady rate when proposed technique is applied in the network.

## VI. REFERENCES


[1]. Juby Joseph, Vinodh P Vijayan," Misdirection Attack in WSN Due to Selfish Nodes; Detection and Suppression using Longer Path Protocol", 2014 Vol.4

[2]. 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, No. 1 & 2, 2009, pp. 1-9

[3]. G.H. Raghunandan, B.N. Lakshmi, "A Comparative Analysis of Routing Techniques for Wireless Sensor Networks", Proceedings of the National Conference on Innovations in Emerging Technology, IEEE 2011.

[4]. Maan younis Abdullah, Gui Wei Hua, Naif Alsharabi, **"**Wireless Sensor Networks Misdirection Attacker Challenges and Solutions", 2008 IEEE 978-1-4244-2184-8/08/

[5]. Roshan Singh Sachan, Mohammad Wazid, D.P. Singh, Avita Kata and R.H. Goudar, **"**Misdirection Attack in WSN: Topological Analysis and an Algorithm for Delay and Throughput Prediction", 2012 IEEE 978-1-4673-4603-0/12/

[6]. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci. "Wireless Sensor Networks: A survey" Broadband and Wireless Networking Laboratory, School of Electrical and Computer Engineering, Georgia institute of Technology, Atlanta, GA 30332, USA Received 12 December 2001; accepted 20 December 2001, pp . 392-422.

[7]. Ju young Kim, Ronnie D. Caytiles, Kyung Jung Kim, "A Review of the Vulnerabilities and Attacks for Wireless Sensor Networks" Journal of Security Engineering, 2014, pp.241-250

[8]. Kalpana Sharma and M K Ghose, "Wireless Sensor Networks: An Overview on its Security Threats" IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010, pp.42-45

[9]. Roshan Singh Sachan, Mohammad Wazid, Avita Katal, D P Singh, R H Goudar ," A Cluster Based Intrusion Detection and Prevention Technique for Misdirection Attack inside WSN", 2013 IEEE 978-1-4673-4866-9/13/

[10]. LV Shaohe, Wang Xiaodong, Zhao Xing," Detecting the Sybil Attack Cooperatively in Wireless Sensor Networks", Computational Intelligence and Security 2008, CIS '08 International Conference on Volume 1Suzhou, pp.442-446, IEEE 2000