# The Technique for Sinkhole Attack Detection in Wireless Sensor Networks

Roli Tripathi[1], Sameer Asthana[2], Pooja Tripathi[3]
[1]*Research Scholar,* [23]*Assistant Professor*
[12]*United College of Engineering and Research, Greater Noida*
[3]*Buddha Institute of Technology, Gorakhpur*

***Abstract:*** The wireless sensor network is the decentralized type of network in which sensor nodes can join or leave the network when they want. Due to self configuring of the network, malicious nodes enter the networks which are responsible to trigger various types of active and passive attacks. The misdirectional attack is the active type of attack which increase delay in the network. The available malicious hub will trigger the attack. In order to recognize and disengage malicious nodes a novel strategy is proposed in this work. The sinkhole attack is triggered by the malicious node which floods the false identification messages in the network. In this work, authentication technique is proposed which detect malicious nodes from the network. The performance of proposed technique is tested in NS2 and it is been analyzed that performance is improved in terms of various parameters.

***Keywords:*** sinkhole, active attacks, leach, wsn, ids, ns2, dos

## I. INTRODUCTION

A combination of tiny light weight wireless sensor makes a Wireless Sensor Network. The limited storage of energy and limited capabilities of processing of sensor nodes make it cheaper in price. 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. Wireless sensor networks monitor the system or surroundings by measuring physical parameters, for example, moistness, weight and temperature. There are two types of sensors nodes in Wireless Sensor networks, sensor node and a Sink node. A large number of sensor nodes are there in Wireless Sensor Networks which collects or sense the data and transmit it to the sink through multiple hops. The sink can use that data locally or globally using internet [1]. The Wireless Sensor Network can screen an assortment of conditions in the distinctive environment like temperature, pressure, noise, movements, stress and so forth. So based on these conditions in which wireless sensor networks can be utilized we have a wide assortment of applications of these wireless sensor networks. Wireless sensor networks are usually installed at unprotected and bitter environments where security is an essential issue [2]. In such unprotected environments wireless sensor networks are open to many physical as well as logical attacks. Security of Wireless sensor network is very important as such types of networks are generally causing alerts which require sudden attention [3]. False alerts generated by the wireless sensor networks may lead to unwanted actions. There are number of attacks which have been faced in wireless sensor network. In Worm hole Attack, packet is recorded at a particular location in the network by a malicious node. After that they get tunnel to another location. The disruption is created in this when tunneling and routing take place in control messages [4]. The network layer is mainly affected by this attack. By monitoring the network and using flexible routing scheme this problem can be prevented. Black hole Attack occurs when a set of nodes in the network are reprogrammed after being captured by the attack malicious node. It will not forward that packet to the base station instead of that it will block the packets. Malicious node captures the packet that enters in the region of black hole and then that packet never reaches the destination node. In Jamming attack the radio frequency used by the sensor node is get inferred. At which destination node is getting signal from the sensor is verify by attacker [5]. By monitoring and finding that frequency the attacker transmit signal on that particular frequency which is very powerful that network can be disrupted by it. In Collision Attack, the attacker will find frequency and then send data on that same frequency which will occur in collision of packets and data need to be retransmitted again. Misdirection attack is the most popular denial of service attack. This attack can be performed in different ways. A malicious node could deny a substantial course to a specific node in this way denying service to the destination. A scenario in which the attacker sends or replays the hello packets with the help of high trans-mission power for discovering the neighbor packet is said to have a hello flood attack [6]. 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 [7]. 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.

## II. LITERATURE REVIEW

Leena Rani et al (2015) presented that when there is a change in the network topology, there is a change in the energy efficiency and the fault tolerance protocols. The maintenance of both of the parameters is very important and so the various methods have been proposed which can prevent the attacks to happen. The main degradation of energy occurs due to the attacks that are caused by the intruders. The misdirection attack, a type of DoS attack has caused a lot of problems as it is difficult to be detected. Approaches like cluster based approach are explained in this article which will prevent the energy from being destroyed. Through this the maintenance of the throughput is also done. The article has proposed various such methods which will help in prevention of all the attacks and will help maintain the network secure [8]. Ruchita Dhulkar, et al (2015) explained in this article about the security of the wireless sensor networks. There are many attacks which are dangerous for the performance of the network like black hole, jamming, wormhole etc. Misdirection is most dangerous routing attacks network. In this paper they proposed a technique to detect malicious node to work network member in the data routing [9]. Hossein Jadidoleslamy, et al (2011) intended for wireless sensor networks and explained how various attacks can be configured. There are many attacks which are vulnerable to the network. In this paper they explain the launching procedure of detecting attack using MintROUTE Protocol. MintRoute is the most widely utilized directing protocol as a part of sensor network organizations, utilizing the link quality metric to assemble the relating routing tree. Experimental results show that proposed technique is better than existing in terms of accuracy and throughput [10]. Jin Qi et.al (2013) presented that wireless Sensor Network is a heterogeneous system combining tiny sensors with general purpose computing elements. There are many routing protocol which are used in sensor network are efficient to detect attacks. There are many attacks which can be easily triggered in sensor network. Among them misdirectional attack is the most destructive attack for these networks. It degrades the performance of the network due to packet loss. This paper discussed a mechanism to initiate the attack at wireless sensor networks. They do experiments to verify the result of the proposed technique [11]. Chun-Hsin Wang et al (2010) explained that due to replying spoof routing information the malicious nodes become immediate nodes of routing paths. Then by selfish nodes the data packets might be stolen, customized and can be drop. There is need to modify the protocols as the unnecessary data is consumed because of the affected bandwidth. In this paper, the authors have proposed a new to detect malicious nodes. Without changing or including directing protocols, just few sets of detection nodes are required, which can recognize and disconnect malicious nodes. From the simulation results it has been seen that by one pair of detection nodes the delivery rate of packets improve to 17%. There is also increase of 0.1 KB/s in each node average extra overhead [12]. Yi Zhing Zang et.al (2012) designed a novel message for observation mechanism (MoM) to detect and defense the DoS attack. To identify the frequency and content attack similarity function is utilized by MoM. This all process is based on the spatial temporal correlation. Further to isolate the malicious node the rekey and reroute countermeasures are adopted by MoM. The analysis based on security is done in this paper. The results of this analysis show that the energy consumption can also be reduced by using their scheme along with the detection and defense of DoS attack [13].

## III. RESEARCH METHODOLOGY

The network performance is reduces by the malicious node. As the malicious nodes causes various types of active and passive attack by entering in the network. One of the active types of attack is sinkhole attack in this attacker node flood the network with the rough packets and sensor nodes keep on busy to send route reply packets. In network to isolate malicious nodes to enter a mutual authentication based technique will be proposed in this work. The proposed techniques works in the steps described below:-

Step 1: The network is deployed with the finite number of sensor nodes

Step 2: While loop is executed for each node in the network

Step 2.1 Base station gather node location with node localization procedure

Step 2.2 The base station assign the unique arm strong number of each node in the network

Step 2.3 The base station assign unique ID to each node in the network

While End

Step 3: Cluster heads process initiated in the network

Step 3.1 Volunteer node are selected in the network to be selected as the cluster head

Step 3.2 : Volunteer node send its unique ID, arm strong number to base station

Step 3.3 If loop executed

Step 3.3.1 All information matched

the node is selected as cluster head

Else

Node gets isolated

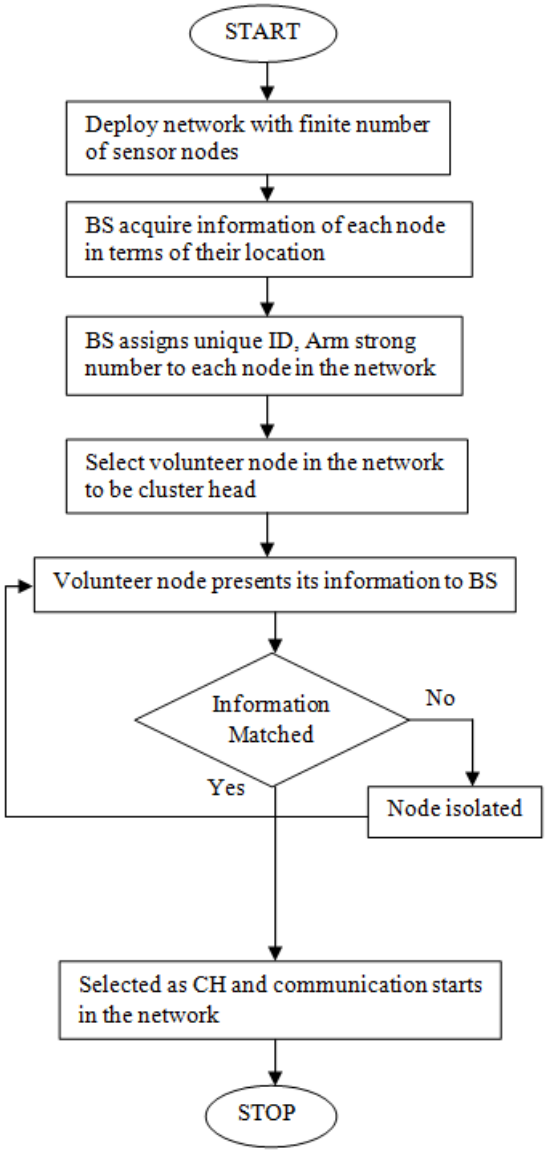


Fig.1: Proposed Flowchart

## IV. EXPERIMENTAL RESULTS

The proposed research work is implemented in NS2 and the results are evaluated in terms of packetloss, throughput and energy consumption.

As shown in figure 2, the value of the basic leach, leach protocol under the impact of sinkhole attack and proposed technique is compared in terms of packetloss. It is been analyzed that LEACH protocol is maximum effect and packetloss is reduced in the network after isolation of sinkhole attack.

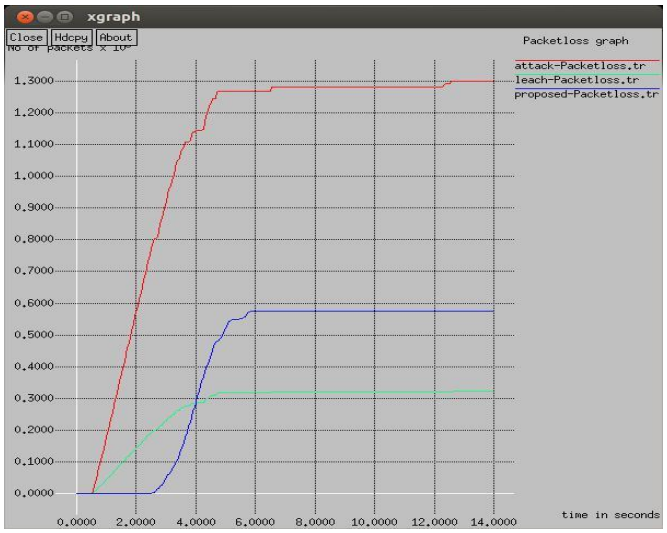


Fig.2: Packet loss comparison

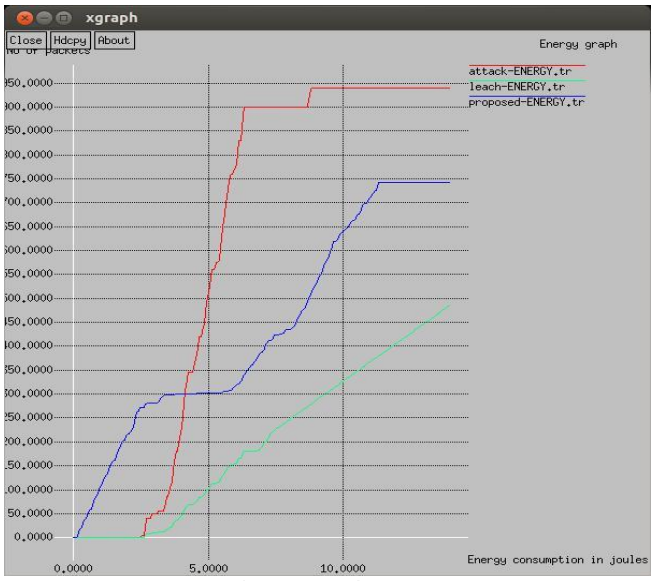


Fig.3: Energy Comparison

As shown in the figure 3, the energy consumption of the proposed technique, LEACH protocol and LEACH protocol under the impact of sinkhole attack is compared and it is been analyzed that energy consumption is reduced after the attack isolation.

As shown in the figure 4, the throughput of the proposed, LEACH protocol and LEACH protocol under impact of sinkhole attack is shown and it is been analyzed that network throughput is increased at steady rate after attack isolation.

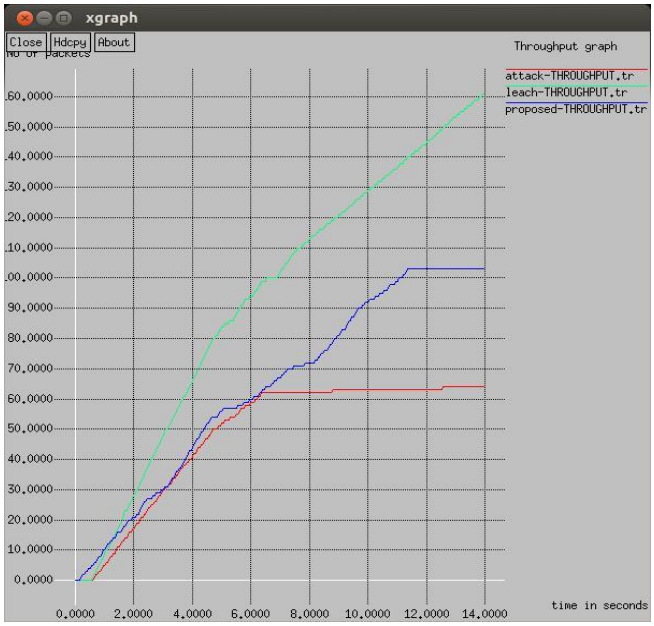

Fig.4: Throughput Comparisons

## V. CONCLUSION

In this paper, it is been concluded that LEACH protocol is the most efficient protocol to reduce energy consumption of wireless sensor network. The technique of mutual authentication is been proposed which detect and isolate malicious nodes from the network. The performance of proposed technique is been analyzed in terms of packet loss which is reduced to 15 %, network energy consumption is reduced to 18 percent and network throughput is increased to 25 percent. The technique is proposed in this paper which can identify and separate the malicious nodes from the network. On the basis of threshold mechanisms the base station analyzed the delay per hop within the network. The malicious node is identified on the basis of the delay such that the node that contributes maximum delay will be recognized as malicious node. This helps in minimizing the energy consumption of the network along with the increment in throughput and reduction of delay within the network.

## VI. REFERENCES

[1]. Michael Collins, Simon Dobson, Paddy Nixon," Securing Wireless Sensor Networks: Intro-ducing ASLAN - A Secure Lightweight Architecture for WSNs", 2009 International Journal on Advances in Internet Technology, Vol. 2 No.

[2]. R Sowmya, Mrs. Shoba. M," DETECTION AND PREVENTION OF MISDIRECTION ATTACK BY THIRD PARTY MONITORING IN WSN", 2000 International Journal of Re-search in Science & Engineering Volume: 1 Special Issue: 2

[3]. Dr. ShahriarMohammadi and HosseinJadidoleslamy," A COMPARISON OF LINK LAYER ATTACKS ON WIRELESS SENSOR NETWORKS", 2011, GRAPH-HOC, Vol.3, No.1

[4]. Megha Joshi, Saumil Patel," CENTRALIZED SIGNATURE BASED APPROACH FOR WIRELESS SENSOR NETWORK USING RSA ALGORITHM", 2015 International Journal for Technological Research In Engineering Volume 2, Issue 8

[5]. C. Anand, R. K. Gnanamurthy," Localized DoS Attack Detection Architecture for Reliable Data Transmission Over Wireless Sensor Network", 2016 Springer Science + Business Media New York

[6]. Omar Said and AlaaElnashar," Scaling of wireless sensor network intrusion detection prob-ability: 3D sensors, 3D intruders, and 3D environments", 2015 Springer

[7]. Suparna Biswas, SubhajitAdhikari," A Survey of Security Attacks, Defenses and Security Mechanisms in Wireless Sensor Network", 2015 International Journal of Computer Applications (0975 – 8887) Volume 131 – No.17

[8]. Leena Rani, Er. Veena Rani," A Novel Study on Data Flow Routing with Energy Optimization under Different Attacks in WSN", 2015

[9]. Ruchita Dhulkar, Ajit Pokharkar, Mrs. Rohini Pise," Survey on different attacks in Wireless Sensor Networks and their prevention system**",** 2015

[10]. Hossein Jadidoleslamy," A HIERARCHICAL INTRUSION DETECTION ARCHITECTURE FOR WIRELESS SENSOR NETWORKS", 2011 Vol.3, No.5

[11]. Chun-Hsin Wang and Yang-Tang Li, "Active Black Holes Detection in Ad-Hoc Wireless Networks", IEEE, 2013

[12]. R Sowmya, Mrs. Shoba. M, "DETECTION AND PREVENTION OF MISDIRECTION ATTACK BY THIRD PARTY MONITORING IN WSN", 2010, International Journal of Research In Science & Engineering, Volume: 1 Special Issue: 2

[13]. Yi-Ying ZHANG, Xiang-zhen LI, Yuan-an LIU, "The detection and defense of DoS attack for wireless sensor network", Elsevier Journal of China Universities of Posts and Telecommunications, Vol19, pp. 52-56, Oct-2012.