Detection and Isolation Technique for Sinkhole Attack in WSN

Urvashi Dhaked [1], Dr. Ashok Kumar [2], Dr. Brajesh Kumar Singh [3]

[1] M. Tech.Scholar, [2] Assistant. Professor, C.S.E. Department, R.B.S. Engineering Technical Campus, Bichpuri, Agra, U.P., India, [3] Professor, C.S.E. Department, R.B.S. Engineering Technical Campus, Bichpuri, Agra, U.P., India

ABSTRACT

The WSN is a self-configuring network in which no centralized control is available. The sensing devices are considered as the nodes. These nodes have small size and low-cost. Primarily, the deployment of these networks is done in the military areas in order to monitor the activities of conflicting sides. These networks can monitor all the movement of energy. Malicious nodes can also join the network and trigger different types of active & passive attacks. The major kind of active attack is sinkhole intrusion. Such an attack allows the attacker node to spoof the identity of sink and act like sink itself. The sensor nodes focus on the transmission of information to the attacker node instead of BS. This research study suggests an algorithm to explore and segregate the attacker nodes from the network. This algorithm is designed on the basis of the identify confirmation. The NS2 (Network Simulator 2) is utilized to deploy the suggested algorithm and diverse metrics are utilized for analyzing the results.

Keywords: Sink hole, Malicious Node, Active Attack, NS2.

1. INTRODUCTION

Wireless sensor networks consist of a small, lightweight set of sensor nodes and computational components. These sensor nodes are usually less expensive, but have limited storage and processing capacity. These networks are widely distributed and deployed in potentially dangerous locations [1]. Generally, these networks measure physical factors such as weight, temperature, and moisture to monitor the system or surroundings. The battery in WSN nodes is of a lesser size than in other networks. In addition, the nodes are positioned at extremely long distances that humans are unable to reach. As a result, the use of battery within WSNs is a big concern this has an impact on the nodes' overall lifespan and, as a result, the network's deployment. Sensor nodes usually rely on a battery with a limited life and replacement due to physical restrictions is unpractical. Furthermore, a sensor network's architecture and protocol must also be scalable to any number of sensor nodes. Because reducing the amount of communication allows the battery to last longer. Low-power components in the sensing subsystem can be used to reduce energy consumption [2]. Clustering consists grouping nodes into clusters and selecting cluster heads on a regular basis. Each cluster has a cluster head, and the remaining nodes are unique to that cluster. Clustering produces a two-level order, with cluster heads forming the upper level and part nodes forming the lower level [3]. Cluster heads lose more energy than part nodes because they transmit data over longer distances on a regular basis. The LEACH protocol is the most efficient clustering protocol in a WSN. The cluster heads in the LEACH protocol are chosen at random from the network. The cluster head selects sensor nodes based on distance. The nodes closest to the cluster head will be included in the cluster. Clusters are changed at random based on energy. In each round of data transmission, the sensor node with the least energy is selected as the head of the cluster. Due to decentralized nature of the sensor network energy consumption is the major issue which degrades the network performance. The security attacks are classified into active & passive attacks. Active attacks are those that significantly reduce network performance in terms of various parameters. The passive attacks are those which don’t effects the network performance but may trigger active attack in future.

WSN has a wide range of applications. It includes health applications such as tracking the location of patients and overall patient monitoring, industrial monitoring, such as, data logging, and wastewater monitoring, structural health monitoring, which includes monitoring changes to the material and geometric properties of engineering structures such as buildings, flyovers, bridges, and roads, and military applications such as data logging and wastewater monitoring.

The rest of the section of the paper: Section. 2. goes over a research background. Section. 3 discusses research methodology for isolation of sinkhole attacks in wsn. Section. 4 is devoted to result and discussion. Finally, Section. 5 concludes this paper and makes some recommendations for further research.

2. RESEARCH BACKGROUND

There are the various types of active attacks which are possible in wireless sensor networks. In a wormhole attack, a malicious node creates a virtual tunnel over a low-latency link that carries a message from one network segment to another. The route of control messages is disturbed when they are tunnelled. It's a type of network-layer attack. The problem can be solved by using network monitoring and flexible routing strategies [4]. A malicious node in the network captures and reprograms a group of nodes, and instead of forwarding packets to the base station, it blocks them. Any packet entering the black hole area is intercepted by the malicious node and never makes it to its intended recipient [5]. The radio frequencies used by the sensor node are inferred in this attack. Initially, the attacker monitors to see how often the sender sends a signal to the destination node. The attacker sends out a signal that is powerful enough to disrupt the network on that frequency [6]. Sinkhole Attack**:** A scenario in which an attacker sends or reads hello packets using high transmission power to detect adjacent packets is considered a hello flood attack. This helps to create the illusion that the attacker is a neighbor of another node. This could also cause the routing protocol to be disrupted, as well as other attacks within the same network. Because of its ability to transmit packets with higher power, the malicious node is chosen as a parent node. This parent node then passes the messages that will be broadcast across the network. As a result, there is a delay in the network. The attacker broadcasts hello messages to the numerous nodes within the large WSN area. As a result, these various nodes within the network convince the attacker node to be a neighbour node. The energy is depleted as the nodes respond to all such Hello messages. Within the network, there is also a state of confusion. The malicious node will redirect all network traffic to its side, resulting in a network denial of service condition.

This section presents research works by various researchers and related to these works. A number of works in the field of protection are performed in WSN.

Roshan Singh Sachan et al. [3] explain that there are different types of attacks faced by wireless sensor networks. Wireless sensor networks are subject to a wide range of attack. There are many cases of undetectable DoS attacks and misdirection attacks. The node is mislead in such a way that it reaches any node other than the destination node. As a result of such circumstances, performance suffers. In this article, a topological analysis of a wireless network is the target of such an attack. An algorithm is proposed to aid packet throughput and delay. When it comes to performance, the tree network topology outperforms the mesh network topology.

Kavita Tandon et al. [7] introduced a number of routing and security issues in WSNs, primarily based on Sinkhole attacks. It also outlines various methods for detecting and avoiding sinkholes. Finally, the countermeasures used to counter this attack are discussed. According to the majority of the research paper, anomaly detection is a better solution when combined with an algorithm that reduces false alarms.

Annie Mathew and J.Sebastian Terence [8] In this study, they investigated sinkhole attacks and classified sinkhole detection methods based on several factors. Through this attack, we will also investigate the threats and challenges of WSN. These detection strategies were divided into four groups: hop count based detection, agent based detection, and sequence number based detection, cryptography based detection. They further suggest the benefits and drawbacks of each strategy.

PC Kala et al. [9] proposed a new method for detecting sinkhole attacks. When throughput is lower than predicted, the sensor node requests the base station's unique key. The base station computes the key using Armstrong's number. As a result, a malicious node that spoofs the base station's identity is unable to provide the unique key and is identified as a malicious node.

Wazid et al. [10] suggested using the LEACH protocol to locate sinkholes in hierarchical wireless sensor networks. They proposed two algorithms that use the sinkhole node presence algorithm to classify suspected node. Using the sinkhole node recognition algorithm, identify suspected node types as “Sinkhole message modification node**(SMD),** Sinkhole message dropping node **(SDP),** Sinkhole message delay node **(SDL)**”.

3. RESEARCH METHODOLOGY

In this work, the leach protocol is used to divide a network into fixed-size clusters with a limited no. of sensor nodes. Cluster heads are chosen based on distance & energy for each cluster.CH collects aggregated data from nodes and send it to BS. The reactive routing protocol will determine the shortest path from source to destination. There are malicious nodes in the route that are responsible for sinkhole attacks, which cause network delays. In this paper, a technique for detecting and isolating attacker node from the network those are causing sinkhole attacks in the network will be proposed.

A) Algorithm: The following algorithm is used in this study to detect malicious nodes among a set of input nodes.

```
    Start( )
1.  Deploy the wireless sensor network with fixed no. of  nodes and in fixed area
2.  Divide entire network into fixed-size clusters and chose cluster head in each cluster
3.  Cluster head selection ()
    a.  node=0   /// Node identification
    b.  For (i=0; i<n ; i++)
        a.  If(distance & energy (a(i))<a(i+1))
        b.  Node= a(i);
            Else
            Node=0;
            End
4.  The direct route will be established from cluster head to Base station
5.  Delay =D(n)
6.  Verify secure path ()
    a.  Get coordinate of node whose id is 0
    b.  For (i=0; i<n;i++)
    c.  A(i)=a(i-1)+D(n);
    d.  End
    e.  Compute  distance between all nodes ()
        a.  Distance =(a(i+1)-a(i))^2+(a(y+1)-a(y))^2
7.  If (any nodes adjacent node !=saved information)
8.  That node will be identified as attacker node in the network

    End
```

Figure1 show how the entire network is divided into clusters of a fixed size and distributed with a limited number of sensor nodes. Location-based clustering algorithms divide the entire network into groups. Using the LEACH protocol technique, the cluster head for each cluster is selected. The LEACH protocol compares the distance & energy of each node, and the cluster head is chosen as the node with the most energy and the shortest distance from the other nodes. Data from all network nodes will be gathered and transmitted to the cluster head. The cluster head establishes a path for data transmission to the base station via other cluster heads. A route from source to destination is established using the AODV routing protocol. At each node, it stores data in the form of tables. Based on hop count and sequence number, the source node selects the best path. The best path to the destination will be chosen as the one with the fewest hops and the most sequence numbers. The data from the source nodes is sent to the path's destination nodes. The sinkhole attack is triggered by some malicious nodes in the chosen path. The node localization technique will be used by the base station to detect and isolate malicious nodes. Using the node localization approach, the base station collects information about the location of the node. The distance each of them is from the base station is also included in the data. On each hop along the established path, the distance factor causes a count delay. When the base station detects a delay, it increases the delay of the established route. With each hop, the base station counts the delay, and the nodes causing the delay to increase in the network are identified as malicious nodes in the network.

B) Flowchart

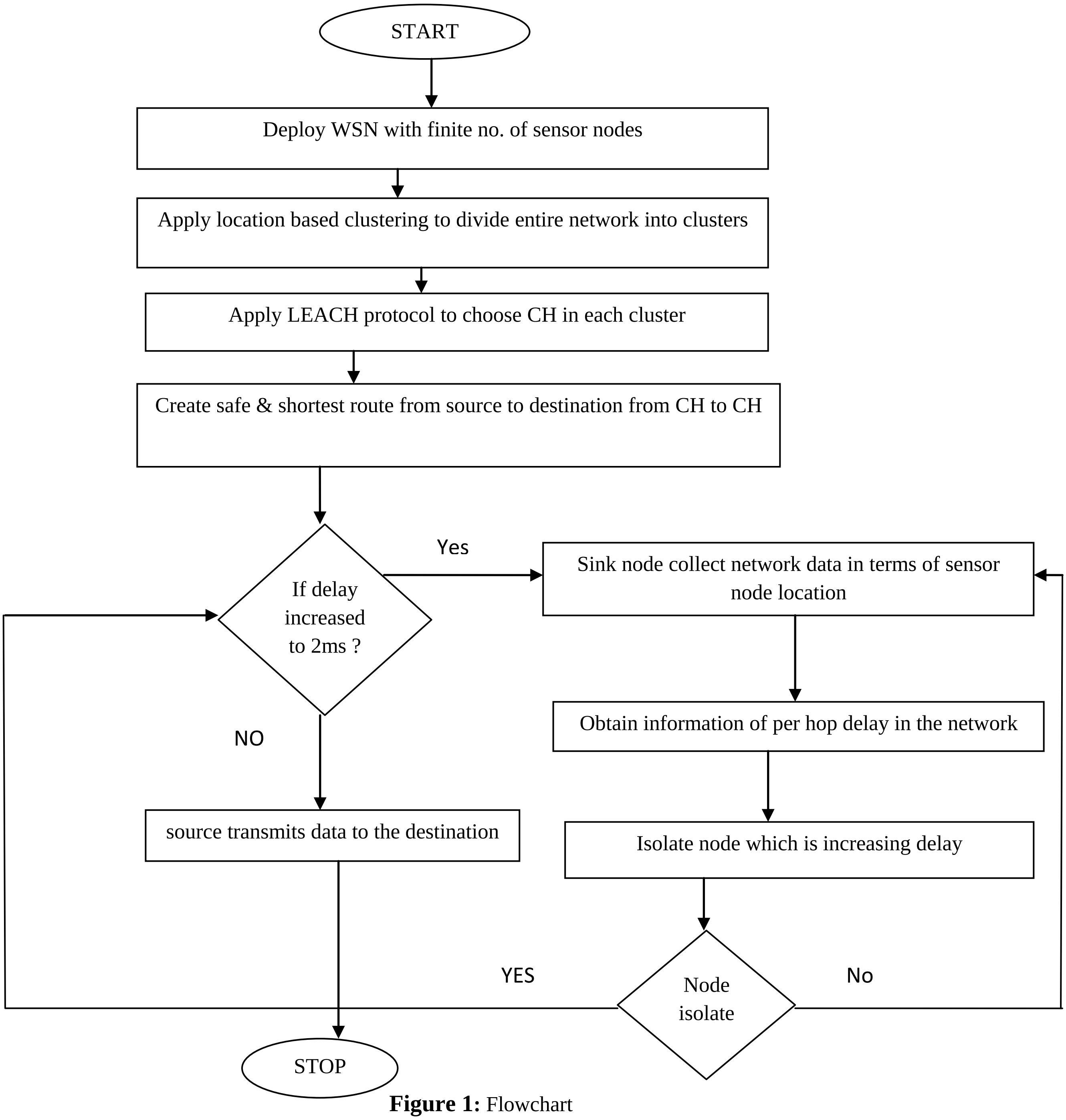
START
Deploy WSN with finite no. of sensor nodes
Apply location based clustering to divide entire network into clusters
Apply LEACH protocol to choose CH in each cluster
Create safe & shortest route from source to destination from CH to CH
If delay increased to 2ms ?
Yes
Sink node collect network data in terms of sensor node location
Obtain information of per hop delay in the network
Isolate node which is increasing delay
NO
source transmits data to the destination
YES
Node isolate
No
STOP

Figure 1: Flowchart

4. RESULT & DISCUSSION

The proposed algorithm was simulated using network simulator (NS2) & various parameters, like energy consumption, throughput, and packet loss, are analysed in the results. The NS2 is a simulator based on events and X graphs are used for network performance analysis. NS2 was created with the C++ programming language and OTcl. The different parameter values used for the simulation are as seen in simulation table.

Table 1: Simulation Table

Parameter	**Value**
Terrain Area	800m * 800m
Antenna Type	Omni directional
Routing Protocol	AODV
Data Payload	512 Bytes/Packet
Pause Time	2 second
Number of nodes	37
Application Traffic	CBR

4.1 Performance Parameter

Number of quantitative metric are responsible for the evaluations of the performances of the routing protocols for wireless sensor network. Four quantitative metrics have been used in this work.

Throughput

Throughput is a measurement of the number of packets received per unit time.

$$Throughput = \frac{Total\ Data\ packets\ received\ at\ destination}{Simulation\ time} \quad ....(1)$$

Packet Delivery Ratio

The proportion of successfully received packets to total packets transmitted is referred to as PDR. The congestion in the network takes place due to the retransmissions takes place.

$$Packet\ Delivery\ Ratio = \frac{Total\ Data\ packets\ received}{Total\ data\ packets\ sent} \quad .....(2)$$

Average End-to-End Delay

E2E delay is calculated by adding the delay to each successful data packet delivery and then dividing it by the total number of successful data packets received.

$$Average\ End\ to\ End\ Delay = \frac{\sum(Time\ Received - Time\ sent)}{Total\ Data\ Packets\ Received} \quad .....(3)$$

<u>Overhead</u>

Diverse protocols are utilized to accomplish diverse tasks according to their enlarged size due to the scalability of the ad hoc networks. The increased size of the network leads to improve the quantity of routing traffic. The routing overhead is a significant measure. Overhead is the total amount of routing algorithm transmitted across the network. Routing overhead is available with regard to bits per second or packets per second. Overhead is occurred due to the route error packet and network jamming.

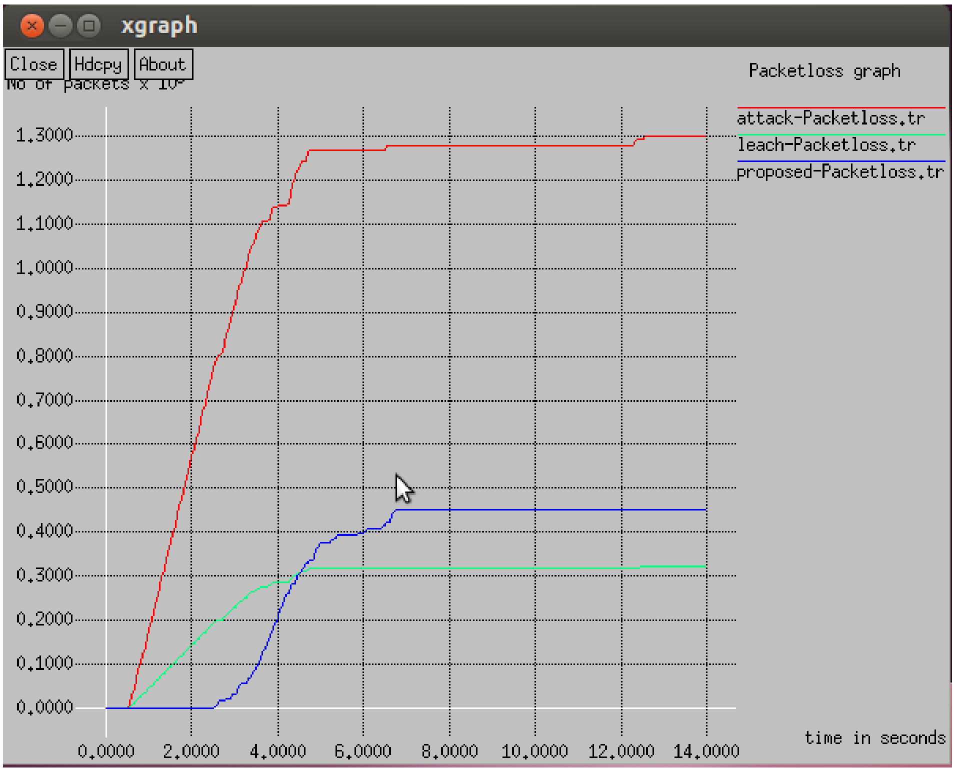

Figure 2: Packet loss comparison

In above Figure 2, X-axis show time and y axis shows packets. Attack, leach, and proposed technique are compared in terms of packetloss. The red line depicts the packet loss when sinkhole attacks occur. The green line in the LEACH protocol represents packet loss, while the blue line represents packetloss when an attack is isolated. After the sinkhole attack is isolated, the LEACH protocol has the greatest effect and reduces packet loss in the network.

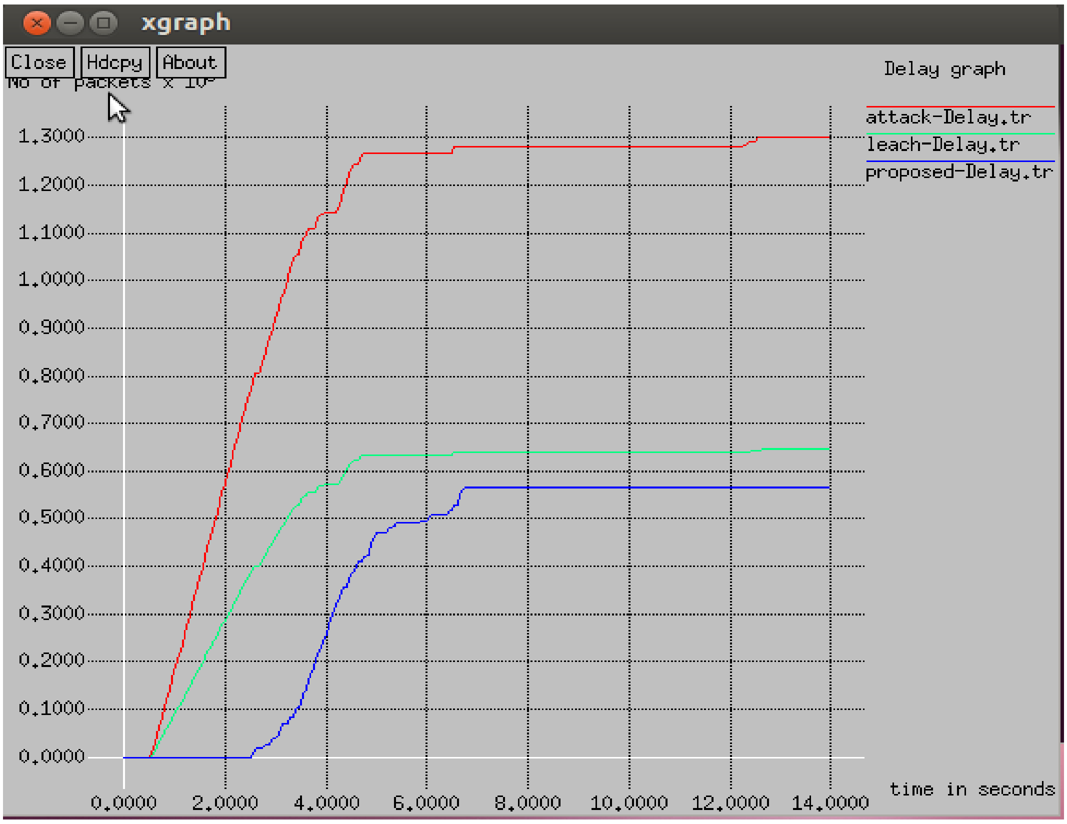

Figure 3: Delay Comparison

In above Figure 3, X-axis show time and y axis shows packets. Attack, leach, and proposed technique are compared in terms of delay. The red line depicts the network delay when sinkhole attacks occur. The green line in the LEACH protocol represents network delay, while the blue line represents network delay when an attack is isolated. The attack scenario has the greatest delay, whereas the proposed scenario has a shorter delay due to the attack being isolated in the network.

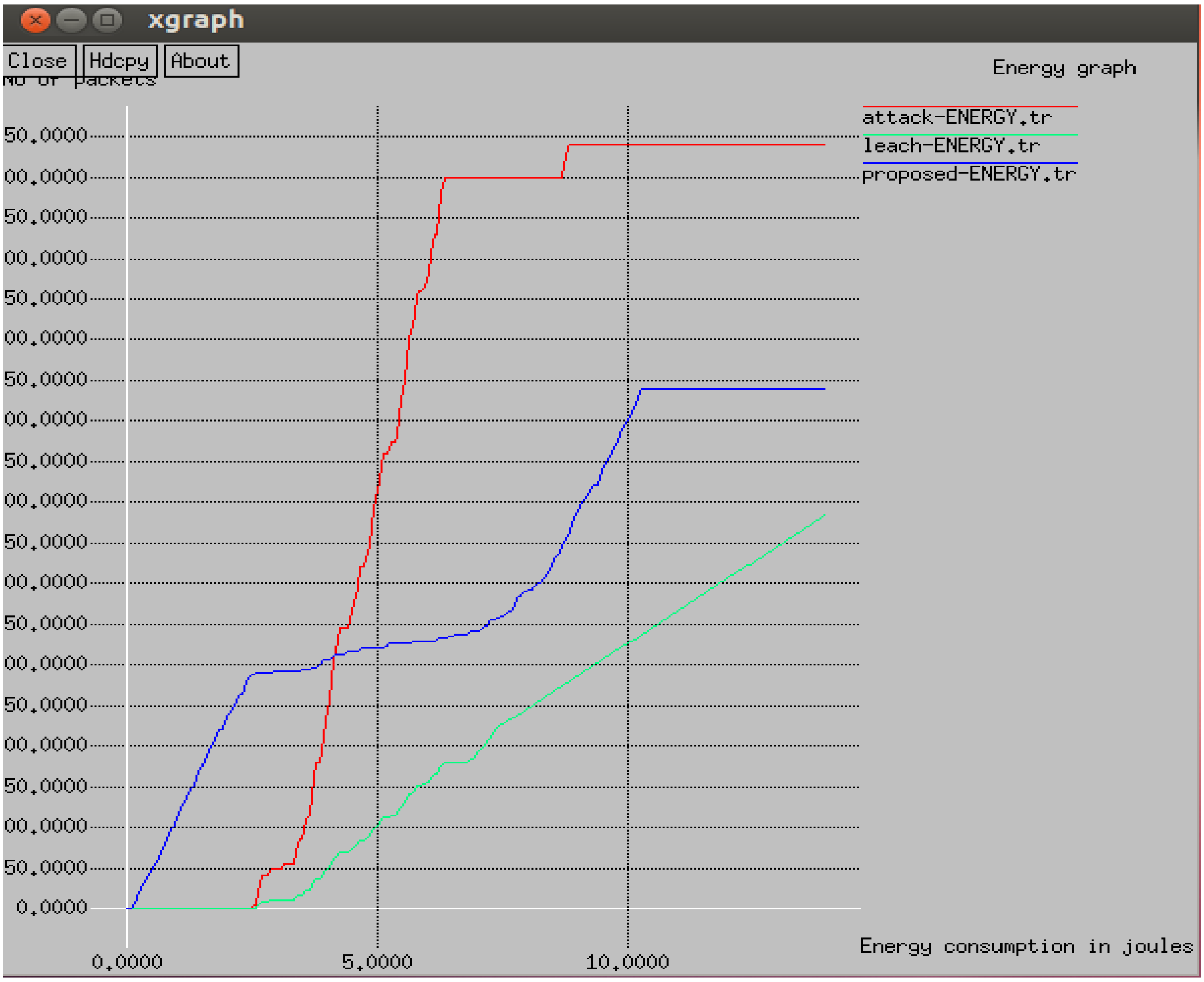

Figure 4: Energy Comparison

In above Figure 4, X-axis depicts time, while the Y-axis depicts energy con-sumption in joules. The red line depicts the network's energy con-sumption when sinkhole attacks occur. The green line indicates energy consumption in the Leach protocol, while blue line indicates energy consumption when the attack is isolated from the network. It has been determined that after the isolation of the attack, energy consumption is reduced.

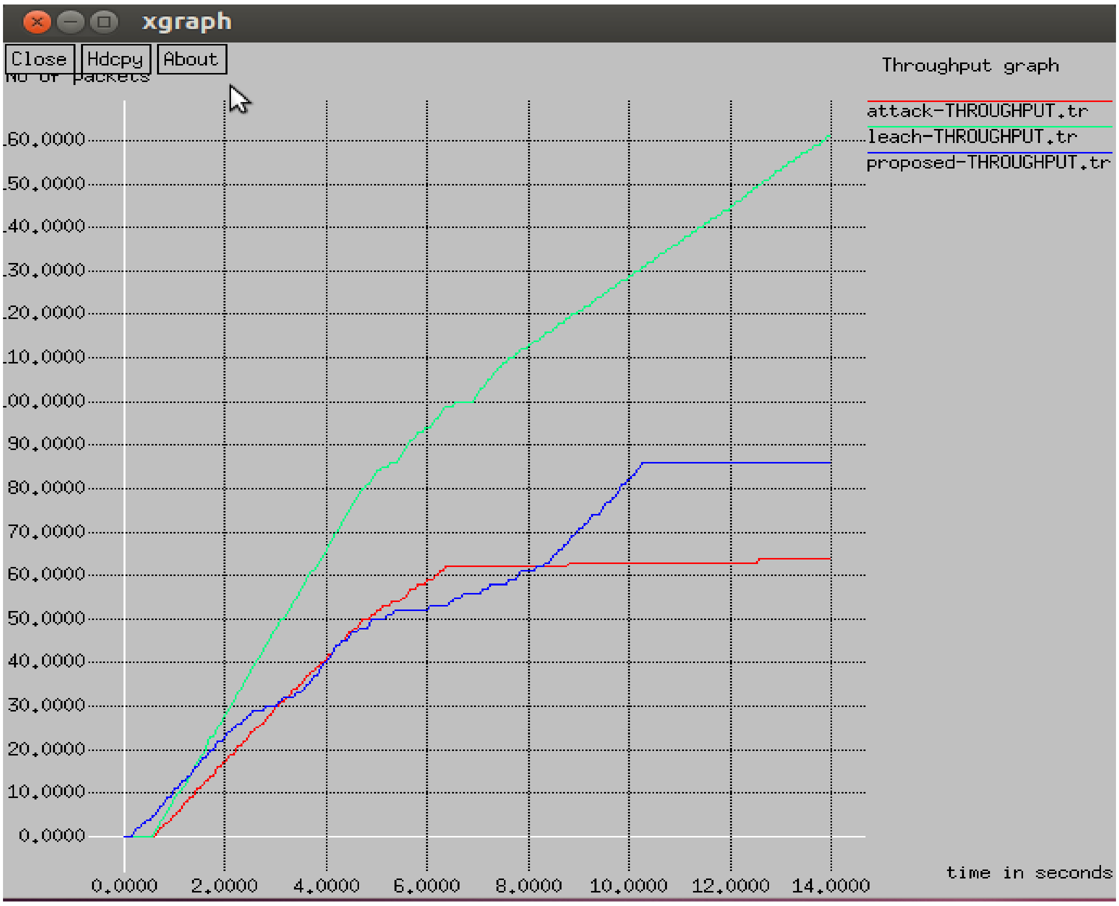

Figure 5: Throughput Comparison

In above Figure 5, X-axis show time and y axis shows packets. Comparisons are shown in terms of throughput between Attack, Leach, and the proposed scenario. The red line represents the throughput when sinkhole attacks on the network are triggered. The green line indicates the throughput in leach while blue line represent network throughput in proposed scenario when attack is isolate. It has been determined that after an attack is isolated, network throughput increases at a consistent rate.

5. CONCLUSION

Sensor nodes in wireless sensor networks detect environmental conditions and send the information to a base station. The sensor nodes' battery life is limited due to their small size. Malicious nodes may join wireless sensor networks because they are self-configuring networks. A network misdirection attack is being launched by these malicious nodes. It is concluded that sinkhole attack spoof the identification of the malicious nodes which affect network performance. The impact of sink hole attack is shown in the form of throughput, packet loss and energy consumption. A method for detecting and isolating malicious nodes from networks is proposed in this work. The proposed method is relies on node-localization, with the base station analyzing hop delay. A malicious node in the network will be identified as one that can increase the maximum delay times. It is determined that the network's energy consumption is reduced, throughput is increased, and network delay is reduced.

REFERENCES

[1] Baviskar, B.R. and Patil, V.N. (2014), “Black hole attacks mitigation and prevention in wireless sensor network”, International Journal of Innovative Research in Advanced Engineering (IJIRAE), Volume 1, Issue 4, pp. 167-169.

[2] Dr. G. Padmavathi, Mrs. D. Shanmugapriya (2009), “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, pp. 1-9.

[3] G.H. Raghunandan, B.N. Lakshmi (2011), “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 (2008), “Wireless Sensor Networks Misdirection Attacker Challenges and Solutions”, IEEE 978-1-4244-2184- 8/08/ ,2008.

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

[6] Dhulkar, R., Pokharkar, A. and Mrs. Pise, R. (2015), “Survey on different attacks in Wireless Sensor Networks and their prevention system”.

[7] Kavita Tandon (2016), “Sinkhole Attacks in Wireless Sensor Network Routing: A Survey”, Research Journal of Computer and Information Technology Sciences, IEEE, Vol. 4(8), pp. 4-7.

[8] A. Mathew and J. S. Terence (2017), “A survey on various detection techniques of sinkhole attacks in WSN,‖ in 2017 International Conference on Communication and Signal Processing (ICCSP), Chennai, pp. 1115–1119.

[9] Prakash C Kala, Arun Prakash Agrawal, Rishi Rajan Sharma (2020), “A Novel Approach for Isolation of Sinkhole Attack in Wireless Sensor networks” 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence).

[10] Wazid, Mohammad & Das, Ashok Kumar & Kumari, Saru & Khan, Khurram. Design of sinkhole node detection mechanism for hierarchical wireless sensor networks. Security and Communication Networks. 9. 10.1002/sec.1652, (2016).