JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Leach Protocol Performance Evolution with Reference of Sinkhole Attack

Mr. Sachin Vishwakarma, Mr. Rajneesh Pachouri, Mr. Anurag Jain
Research Scholar, Assistant Professor, Assistant Professor
Computer Science and Engineering,
Adina Institute Of Science And Technology, Sagar, India

Abstract: Researchers' interest in Wireless Sensor Networks (WSNs) has increased because of the wide range of possible applications. A WSN essentially consists of a collection of sensor nodes that are powered by a tiny battery integrated into each node. A crucial component of wireless sensor networks is security. LEACH is the most well-known cluster-based routing protocol, and it is utilized in WSNs. The sinkhole attack is the most harmful routing attack that may be used against this protocol. LEACH employs a centralized clustering method and has the same steady-state phase as LEACH. Most wireless sensor networks employ a many-to-one communication strategy for data collecting. Sensor network attacks that are effective include jamming, DOS attacks, sinkhole attacks, and black-hole attacks. One of the most destructive routing attacks is the sinkhole attack. The challenge with the sinkhole attack is that a sphere of influence is created when a subverted node or malicious node broadcasts the desirable routing information and compels networks to route data towards it. Therefore, a sinkhole attack results in decreased network performance. In this study, we'll assess the LEACH Protocol's effectiveness in sinkholeand non-sinkhole-attacked networks. To carry out the planned work, we will use MATLAB, and we'll build a performance graph to assess how the LEACH protocol performed.

IndexTerms - Sinkhole Attack, Wireless Sensor Network (WSN), low energy adaptive clustering hierarchy (LEACH), Cluster Head (CH), Secure Low Energy Adaptive Clustering Hierarchy (SLEACH)

I. INTRODUCTION

Small sensors are deployed in a wireless sense network (WSN) to sense physical characteristics and transfer data to a central station known as sink nodes or base station. The most crucial feature of WSN is how sensors are efficiently placed while keeping the required detection performance. [1]. the nodes may be stationary or moving. They are unsure of their position in existence. They could be homogenous or non-homogeneous. The data is sent ahead to a sink that can use it locally or is linked to other networks, most commonly via multiple hops relaying. [2]. WSNs have gain popularity as a low-cost alternative for data collecting and measurement. WSNs provide a number of benefits, including ease of deployment, which is facilitated by the use of routing protocols that automatically establish the network. If WSNs are to be utilised to control critical infrastructure, such as water delivery, the network's security must be protected from malicious attacks [3].A wireless network (WSN) is made up of base stations and nodes (wireless sensors). These networks monitor physical conditions such as sound, pressure, and temperature, and send data to a central point over the network. WSN is used to understand, analyse, store, and collect the data. [4]. Below figure 1.1 shows how components in WSN works.

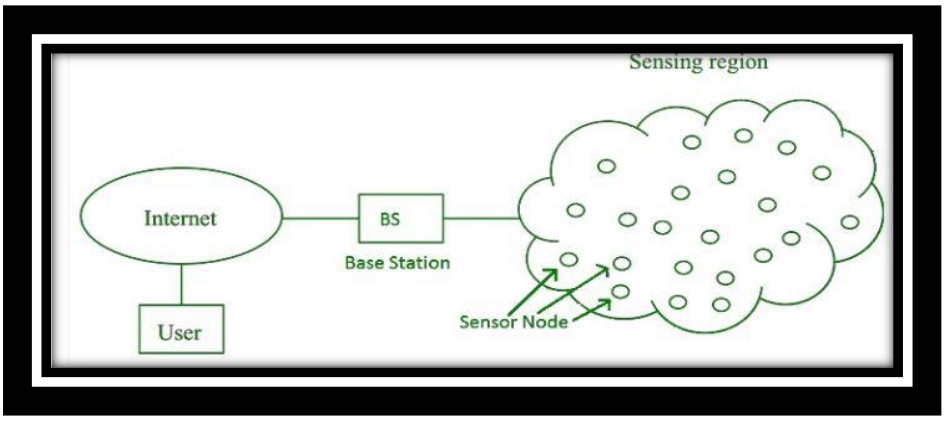

Figure 1 Wireless Sensor Network Components and working

Definition of Wireless Sensor Networks

A mote, also known as a wireless sensor node, is a computational system that consists of a sensing device, CPU, transceiver, memory, and power source. The sensing devices sense the surroundings and collect data that represents the physical circumstances that are being monitored. The sensor data is supplied to a local processor for preliminary processing before being forwarded to the base station for further processing through multi-hop wireless communication. Motes are configured with the needed operating parameters and security credentials before being deployed. In order to acquire precise and synchronised data, a large number of sensor nodes are typically scattered across the region of interest and form a wireless crowd [6].Due to its self-organization, data dynamics, anti-interference, and anti-damage features, it has a wide range of applications in a variety of industries, including military, agricultural, aviation, and medicine. During the WSN research phase, location awareness, networking, data fusion, and energy management are all essential tactics that must be thoroughly investigated. Wireless Sensor Networks are a resource-constrained system that places a premium on security. The LEACH protocol is one of the most well-known cluster-based routing

systems. WSN researchers are now working on routing algorithms and security challenges. Hierarchical protocols are defined to reduce energy use and save time by aggregating data to the Base Station's transmissions. LEACH is the most widely used routing protocol that employs cluster-based routing to reduce energy consumption [27]. WSN is important in fields like computer science and electronics, among others. WSNs are a type of ad-hoc network that can be used in inaccessible or hostile environments. Because of its unattended deployment technique, the network is more vulnerable to a range of threats. Vulnerability can be activated in a variety of ways, both inside and outside[7]. The network is more exposed to a variety of threats due to its unmanaged deployment method. Vulnerability can be triggered in a number of ways, both inside and externally. [3]. It has a wide range of applications in a variety of fields, including military, agriculture, aviation, and medicine, due to its self-organization, data dynamics, anti-interference, and anti-damage characteristics. Location awareness, networking, data fusion, and energy management are all critical strategies that require extensive investigation during the WSN research phase [26].

COMPONENTS

1. Sensors: Sensors are utilized in a WSN to capture environmental variables and collect data. Sensor signals are translated to electrical signals.

2. Radio Nodes: These take data from the sensors and transmit it to the WLAN access point. It includes a microcontroller, transceiver, external memory, and power source.

3. WLAN Access Point: This device accepts data wirelessly transmitted by radio nodes, which is generally over the internet.

4. Evaluation Software: The data collected by the WLAN Access Point is analyses by Evaluation Software, which then sends the report to the users for further processing..

WSN ARCHITECTURE

The transmission of sensor data to the centre through multi-hop transmission is the basis for the general operation of wireless sensor networks. This transmission has to be both secure and fast. Wireless sensor network architecture follows the OSI architecture Model. The WSN has five layers and three cross layers in its construction. In most sensor n/w applications, we need five layers: application, transport, n/w, data link, and physical layer. Power management, mobility management, and task management are the three cross planes. These WSN layers are used to complete the network and make the sensors operate together in order to increase the network's overall efficiency. The final node to communicate with the base station is the sink node. The sensor node's sensed data is processed, and the data is passed to the neighboring node. The data is then sent to the sink node, which then sends it to the centre via the base station [16].If WSNs are to be utilized to monitor important infrastructure like water delivery, the integrity of the WSN must be guaranteed be safe from cyber-threats. The WSN routing protocols could be hacked. Susceptible routing assaults, which can wreak havoc on the internet's connectivity network. The sinkhole attack prevents the base station from collecting complete and precise sensing data, resulting in a significant danger to wireless communications. Networks of sensors In fact, this occurs as a result of the unprotected environment. The use of wireless networks, the placement of sensors in open spaces, and so on as well as the insufficient computing and battery power. This technique has two primary components: a secure and low-overhead algorithm and an efficient identification algorithm. The first is a secure and low-overhead base station algorithm that can collect data network flow data from the area that was attacked. The second is the one is a route pattern analysis algorithm; while the other is a routing pattern analysis algorithm determine who the intruder is [3].

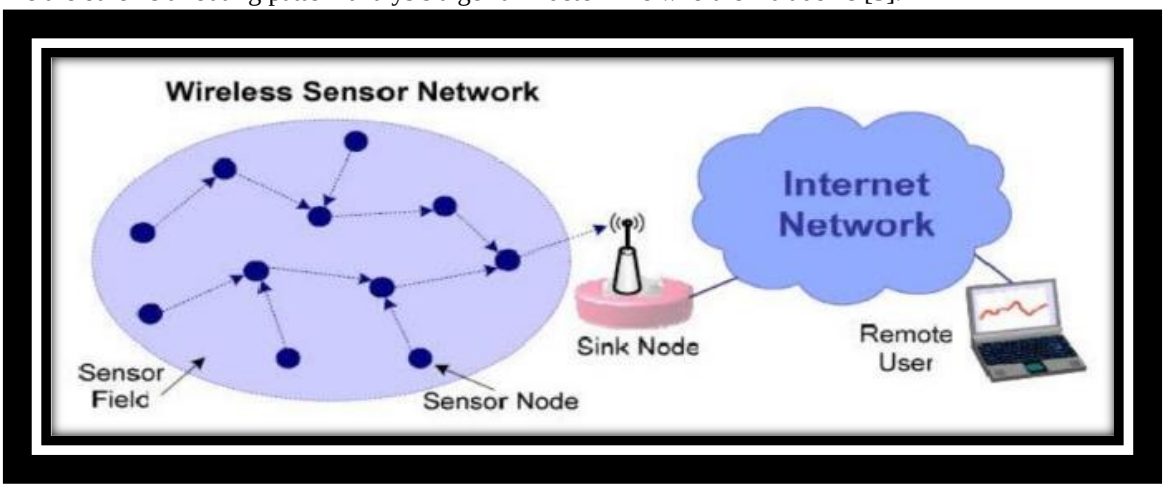

Figure 2 Wireless Sensor Networks Architecture.

SINKHOLE ATTACK :

A sink node is a node that leaks into the network and collects all data packets. This exploit puts all network traffic at risk. The Sinkhole attack can change the packet flow direction by initiating the selective forwarding attack. It increases the appeal of a risky node to its neighbours. It has the ability to create the ideal conditions for a Wormhole attack. To put it another way, the Sinkhole attack prevents messages from being sent in a given area by informing neighbors' that it is a sink node [16].

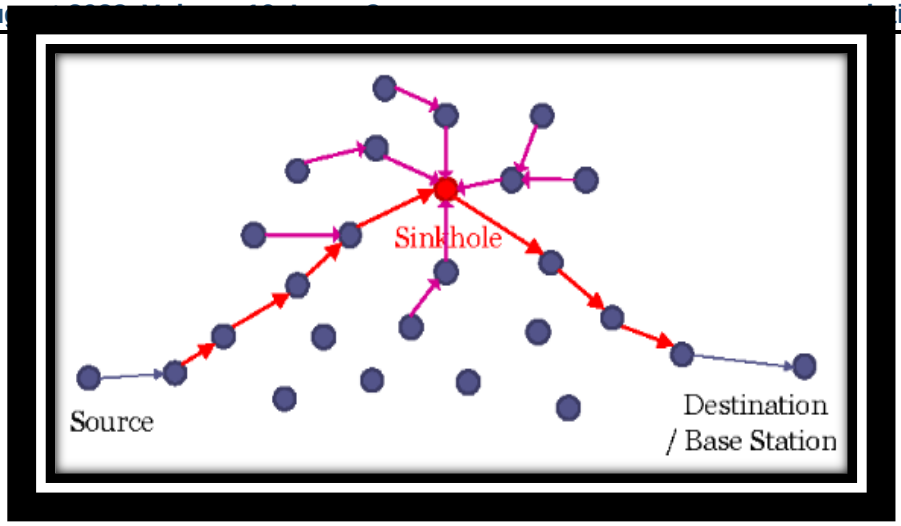

Figure 3 Sinkhole Attack. Sybil Attack:

The Sybil assault is a massively disruptive attack on a sensor network in which a large number of authentic identities are replaced with falsified identities in order to gain unauthorised access to a network.. A node is a sort of assault in which many IDs are used. As a result, an opponent may be present in multiple locations at once. The Sybil assault greatly reduces the efficacy of fault tolerant systems. Because a node can have different IDs, location information can be changed [16]. The Sybil node tries to connect with surrounding nodes by using the identity of a normal node, however this is unlawful because a single node gives numerous identities in the area to other nodes in the network. A Sybil node can be created as a new identity or as a legal identity that is pilfering. As a result, it is regarded as an additional entity of a misbehaving node. The network becomes jumbled as a result of this, and it collapses.It makes effective techniques like authentication, multipath routing, and topology preservation more difficult to implement. It can trigger the selective forwarding attack by guaranteeing that the nodes are misbehaving. [22].

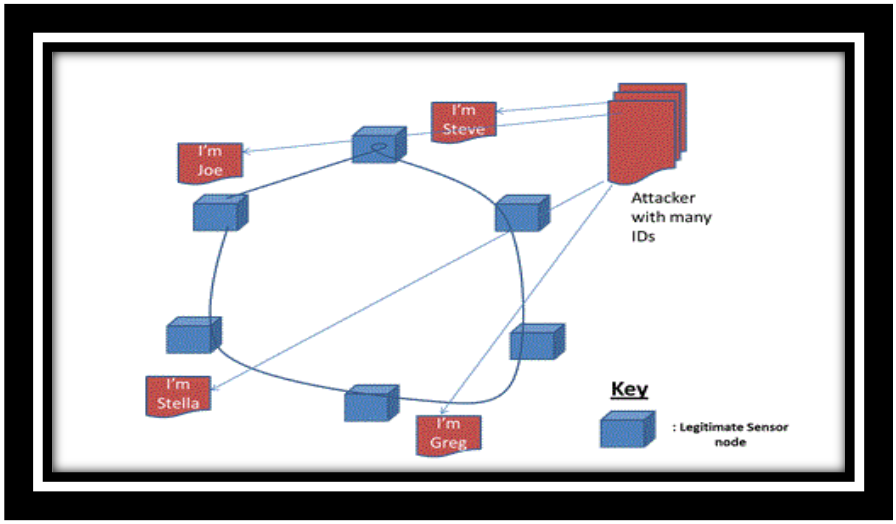

Figure 4 Sybil Attack

TECHNOLOGIES RELATED TO WIRELESS SENSOR NETWORK

The focus of this article is on two main WSN technologies: location awareness and data fusion. To begin, the most important techniques, technological obstacles, and future advances in location awareness technology are thoroughly covered. In addition, the data fusion level and essential algorithms are addressed, as well as their benefits and limitations, and the data fusion technology's potential progress is anticipated. [22].

Location awareness of WSN: Location awareness could offer positioning functions comparable to the global positioning system, even though it would operate indoors (GPS). For multi-agent wireless networks, location knowledge is critical because it allows agents to receive precise observation messages, ensuring the significance of the observed data. Agent interactions with the outside world or with neighbouring nodes are therefore accomplished [22].

Data fusion of WSN: A wireless sensor network is made up of a number of sensor nodes that are distributed across the space. It is unavoidable to have asynchronous clocks, observations, and information transfer delays. As a result, when homogeneous or heterogeneous sensor nodes collaborate to fulfil the same task, a large amount of data is processed. To be more specific, specialised algorithms are used to evaluate and fuse the data with the goal of removing duplicate data from the network, refilling missing data with redundant messages, and lowering network data traffic. Data fusion technology is a type of information integration and analysis technology used in wireless network [22].

II. LITERATURE REVIEW

Hoon Kim and Sang-wook Han [1]

A deployment plan for large-scale WSNs has been presented that meets the average detection probability requirements. The proposed methodology, unlike the uniform deployment method, considers the local event incidence rate information when distributing sensors. There has been presented an ideal problem for selecting the number of sensors for each local location that minimises the overall number of sensors while meeting the requirements for average detection probability, as well as an algorithm for choosing the best solution.

Ankit Solanki Sarvajanik and Niteen B. Patel [2]

Because the majority of wireless sensor networks are battery-powered, one of the most important considerations is energy efficiency. The designer must choose a routing system that uses the fewest resources when creating the wireless sensor network. The suggested protocol enhances the network's lifetime by 40 percent to 75 percent parameters by properly configuring the network, according to simulation results. In each round, the constructed algorithm assumes that each node will transmit a single piece of data.

Ahmad Salehi S., M.A. Razzaque, Parisa Naraei, Ali Farrokhtala [3]

Because of its low cost, self-organization, and ease of use, the demand for wireless sensor networks (WSNs) is growing by the day. WSNs have a number of advantages, one of which is their ease of deployment. If WSNs are to be used to monitor important infrastructure, such as water and healthcare monitoring, the integrity of the WSN must be maintained so that hostile assaults can be avoided. In general, routing methods used in WSNs are vulnerable to routing attacks, which can degrade network connectivity.

Manpreet kaur, Amarvir Singh [4]

At the network layer, a sinkhole attack occurs. It's a spin-off of the black hole attack. It also reduces the number of shows held by the organisation. The remote sensor network was deployed in a set zone and with a fixed number of hubs; the network was decentralised. With the help of the AODV routing protocol, we set up the path from the source to the destination after sending the remote sensor network. The source node floods the network with route request packets for path establishment to the destination, while the destination's nearby nodes respond with route reply packets to the source node. We choose the optimum way among the various paths for transmitting the packets from the source to the destination after receiving the route request and route reply packets. The harmful hub that is currently in the way of triggering a sinkhole assault and changing the postponement between the source and the objective. The presence of the evil hub is detected by calculating the postponement per bounce for each hub that exists in the way**.**

Fang-Jiao Zhanga,b , Li-Dong Zhaia [5]

Sybil, selective forwarding, Sinkhole Wormhole, and HELLO FLOOD are all attacks that wireless sensor networks are vulnerable to. The sinkhole attack, which is the focus of this study, is a semi-regular attack. The hubs attacked guarantee that they will be able to provide a single-jump, high-quality path to the base station, which will then pull in the neighbouring hubs to adjust the first course. Furthermore, bundles sent from the base station are discarded or forwarded to the sinkhole attacker, causing serious harm to the network's heap adjusting. It's cleverly combined with other attacks, amplifying the network's damage.

Asaduzzaman and Hyung Yun Kong [6]

Remote sensor networks are self-coordinated networks, which means they don't have a central control station like a passageway. WSNs have a key component called grouping-based steering, which allows them to take advantage of some of the benefits of cell-based remote organisations. We divide the entire sensor network into varying numbers of clusters, select a CH for each cluster, and then localise the network's coordination and control. LEACH is a centralized clustering-based technology for wireless sensor networks that saves energy. The LEACH protocol works in a round-robin fashion. Each round of the LEACH protocol contains three phases: advertisement, cluster set-up, and steady-state.

S.Ranjeeth Kumar, A.Umamakeswari [7]

Wireless sensor networks require a little amount of resources. In addition, the LEACH Protocol uses fewer resources. The LEACH technique is divided into two phases: setup and steady state. If we wish to form a cluster, the cluster head with the highest probability and energy level is chosen during the setup phase. The node sends the data to its cluster head in its assigned slot during the steady-state phase. The CH collects and aggregates data from the nodes before sending it to the Base Station. Because the cluster head node in the LEACH protocol is not authenticated, the protocol is not secure. The cluster head now sends the data transmission time slot to its member nodes.

Changlong Chen, Min Song, and George Hsieh [8]

We looked at how wireless sensor networks work and how difficult it is to build compromised node detection systems. In wireless sensor networks, a statistical GRS-based technique for detecting rogue nodes has been presented. The difference in CPU utilisation of each node is determined by the base station monitoring CPU usage of each node during a defined time interval.

Liping Teng and Yongping Zhang [9]

In wireless sensor networks, a sinkhole attack is a severe concern. It could cause a system failure in terms of network availability, rendering the sensor hub unable to send and receive data.

Prakash kala, Arun Prakash Agrawal, Rishi Rajan Sharma [10]

Wireless sensor network also uses AODV protocol. In AODV, the source node sends the route request to the adjacent nodes. The path from source to destination is selected on the basis of hop count and sequence number. If the hop count is minimum then that path is selected. During communication, the intruders hacked the identification of base station and sensor node sends the data to malicious node instead of base station. This is the major problem in AODV protocol. To remove these problem we can use some others protocol such as LEACH, S-LEACH etc.

Nazli Siasi, Adel Aldalbahi, Mohammed A. Jasim [11]

Network security problems almost always cause packet loss and latency in a mobile network. The mobile nodes' packet fall, tunnelling delay analysis, and other node behaviour are insufficient for determining their wormhole sinkhole features. As a result, a mechanism is offered for detecting and minimising node collusion, as well as preventing wormholes and sinkholes. The memory effective node collusion approach, which aids in detecting illegal cooperation among nodes and informs neighbours of the evidence, is used to identify sinkhole attacks.

III. LEACH PROTOCOL

LEACH (Low Energy Adaptive Clustering Hierarchy) is a TDMA-based MAC technology. The primary purpose of this protocol is to increase the life of wireless sensor networks by lowering the energy required to construct and maintain Cluster Heads. The necessity for network protocols like LEACH originates from the fact that when a node's battery dies, it becomes unusable. This protocol allows us to extend the lifetime of the node, allowing them to perform only the bare minimum of data transmission tasks. The LEACH treatment is broken down into multiple rounds, each of which comprises two phases: Set-up and Steady [23].

Setup Phase: A CH will be one of the distributed nodes, receiving messages from the Base Station and transmitting them to all non-CH nodes [24]. The primary purpose of the Set-up process is to build clusters and pick the cluster head for each cluster by choosing the sensor node with the greatest energy [23]. The setup process is divided into three stages: Task Ordination (TO), Cluster Configuration, and Scheduling. In the TO stage, each node is believed to be a Normal Node (NN). The percentage of current CHs (which fluctuates from 5% to 10%), the number of nodes previously classified as CH, and the energy level are used to determine which nodes become CHs. For CH selection, only nodes with an energy value equal to or greater than the average of all nodes' energy will be considered.

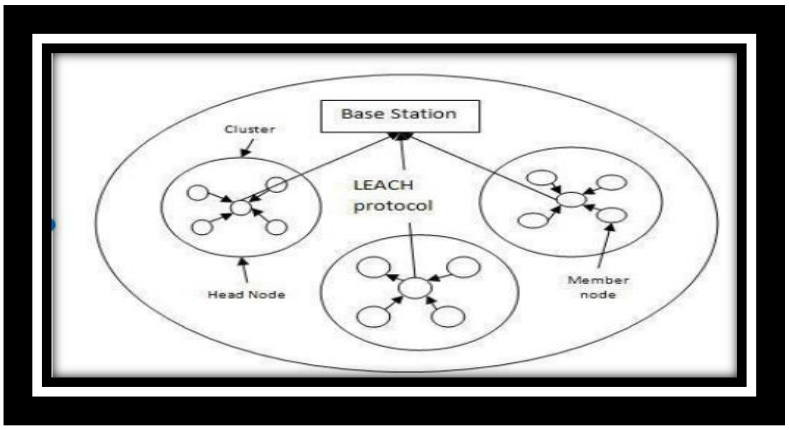

Figure 5 Setup Phase in LEACH

Steady state: Non-CHs send data to CH, who then aggregates the data and sends it to the sink node. The steady phase lasts a little longer than the setup phase. When data is transmitted between nodes, the cluster-head is preserved.

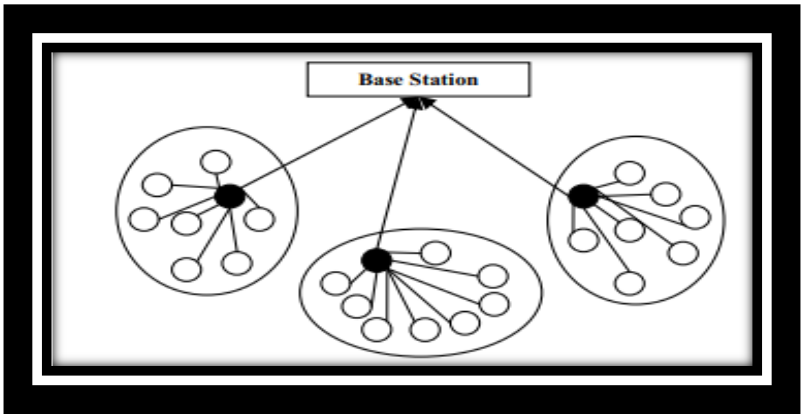

Figure 6 Steady Phase in LEACH

LEACH PROTOCOL IN SINKHOLE ATTACK

A sinkhole attack is a type of active attack in which a compromised node channels all traffic through it. The compromised node attracts the attention of the other nodes by setting a high value for the routing metric. As a result, the attacker obtains all of the packets and can carry out additional attacks including selective routing, packet manipulation, or packet falling. The infected node uses a different metric to attract the packet to itself depending on the routing protocol. For example, if the Mint route protocol is used, the compromised node will advertise that it has a better connection quality, enticing packets. Fake packets can also be transmitted to sensor nodes, in addition to metrics, to include the compromised node in the packet flow direction.

IV. PROBLEM DEFINITION

The purpose of this work is to perform a comprehensive review of the literature on security classification. We'll look at a range of wireless sensor network issues in this study. We're seeking to fix three primary problems: sinkhole attack, Sybil attack, and wormhole attack. Wireless sensor networks are widely used networks, but when their performance degrades, they constitute a serious security threat. When wsn confronts a sinkhole attack in a network, the main concern is efficiency. When a sinkhole attack occurs, nodes' energy consumption increases and their efficiency declines. The figure 9 shows how the sinkhole attack takes place in network.

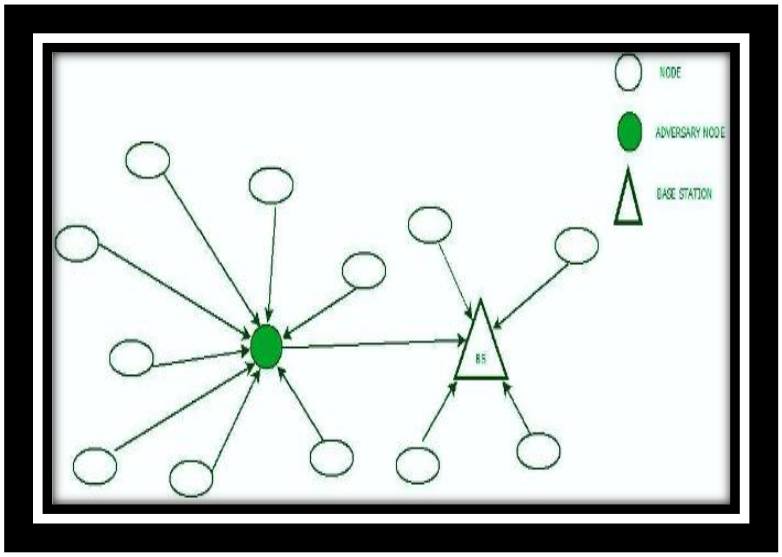

Figure 7 Sinkole attack in WSN

Sinkhole attacks are carried either via hacking into a network node or introducing a fake network node. The malicious node advertises to be the shortest route to the base station and attempts to divert traffic away from other nodes. This attracts not only the nodes closest to the sinkhole, but also the nodes closest to the base station. The invader node or sinkhole can then simply alter the data, jeopardizing the security of the network. Sinkhole attacks can come from both the inside and the outside of the network. In the first scenario, the invader might use a bugged node to launch the attack, while in the second; the invader might use it to establish a direct connection to the base station, persuading other nodes to send traffic through it. The goal of this study is to figure out how to provide maximum security in wireless sensor networks, which has been a long-standing open question. A method is being developed in particular to achieve core security objectives in WSNs, which vary depending on the WSN application. As a result, no single security approach can be demonstrated to be the best fit due to the wide range of security objectives. Starting with a study of the security threats to a WSN, and then going on to the application, ranking security objectives should be done with care. We start by generating a comprehensive list of security threats, which we then categories' and associate with the security assessment framework analytically. It allows security technologies to be tested in real time before being accepted by WSNs. Security is one of the WSN's most critical challenges for reasons including data confidentiality, communication continuity, and protection from malicious users. The proposed authentication approaches are used to verify that Nodes are aware of one another and can communicate effectively with one another.

V. PROPOSED METHODOLOGY

As a result of our observations of the prior strategy's failures and shortcomings in terms of quality and success. Our work exemplifies a cutting-edge solution that is both efficient and effective. In this test, we simply examine how well a LEACH protocol performs in sinkhole and non-sinkhole attacks. Out of all the nodes, a cluster node is chosen as the best. A cluster is in charge of keeping track of all of the nodes. All of the cluster nodes are connected to the base station. Below is a description of the proposed algorithm:

Define Network Size.

- Select compromise node.
- Assign initial energy to each node.
- Start rounds to select CH applying LEACH protocol.
- Calculate alive node, energy consumption, and CH and data transmission after each node.
- Apply sinkhole attack to a network.
- Repeat step 5.
- Draw plots for step 5 and 7.
- Compare the performance of LEACH protocol with and without attack.

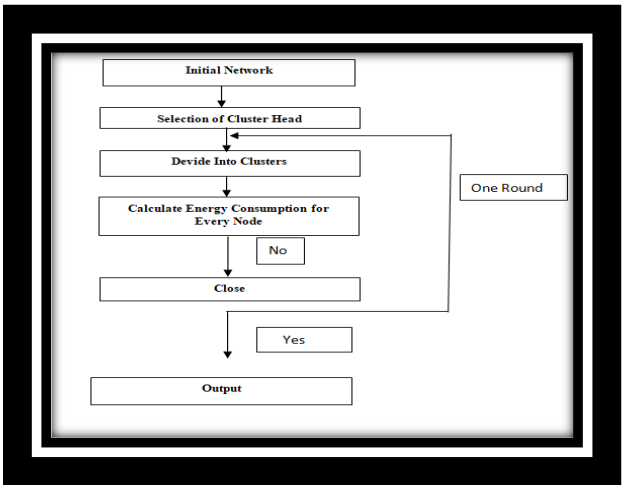

Figure 5 : Flowchart of proposed algorithm

VI. SIMULATION & RESULT ANALYSIS

Wireless sensor networks are those networks which completely rely on batteries. If any sensor consumes more energy the battry dies and sensors stop working. To increase the performance of WSNs when there is no attack we can use LEACH protocol. As we also know that WSNs are prone to many attack. If WSNs encounter sinkhole attack, then the output of network degrades because it consumes more energy due to which the sensors dies early and stop working.

Performance Measures: The graph which is given below shows the performance of LEACH protocol in wireless sensor networks with sinkhole attack and without sinkhole attack. When sinkhole attack start attacking on any network, the compromise node attract all the information of cluster head and advertise false routing which cause more data transmission and consume more energy due to which efficiency decreases. In this section, we utilize MATLAB to test the suggested algorithm's performance. The detection time and false positive rate are two basic performance measures rate. The false negative rate is not taken into account because simulations were carried out until all malicious nodes had been eliminated.

PROCESS BY PROCESS SCREENSHOT AND DESCRIPTION FOR THAT:

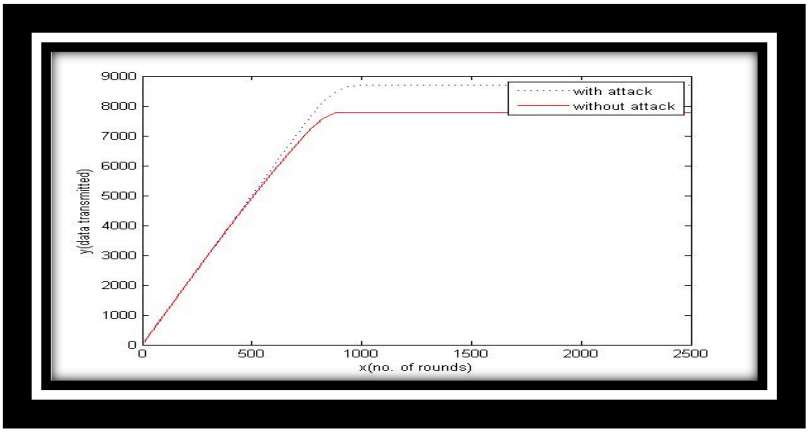

Figure 9 Graph between data transmission and number of rounds

The fig 9. shows the complete framework between data transmission and number of rounds. The amount of data transmitted during a sinkhole attack is lower than in a network that is not under attack.

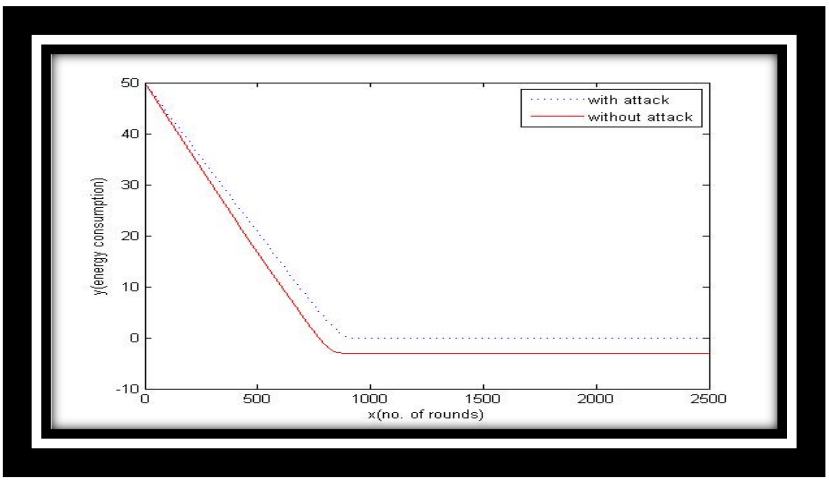

Figure 10 Graph of Energy consumption and number of rounds.

Fig 10 shows the comparisons between energy consumption with sinkhole attack and without sinkhole attack. The dotted line shows that energy consumption in sinkhole attacked network and the red line shows the energy consumption without attacked network. When a certain number of rounds are completed, the cluster head changes in each round. When a sinkhole attack occurs, the compromising node attracts all of the information, resulting in increased energy consumption; however, when a non-sinkhole attack occurs, it consumes less energy and produces more efficient output.

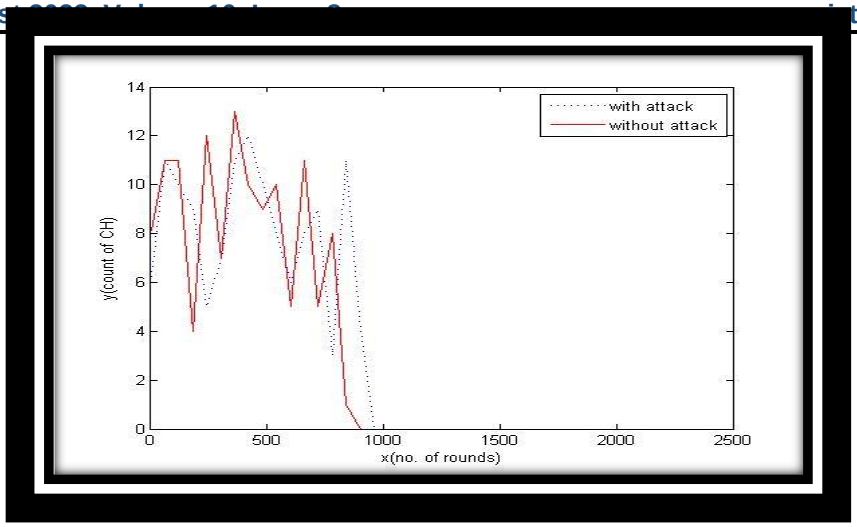

Figure 11 Graph between count of CH and number of round

The figure 11 shows the computation of cluster head value for each round. In each round we get new cluster head and also in each round we discard dead nodes and list out the alive node for next round. Sinkhole attacks damage network throughput by discarding packets and reduce LEACH protocol efficiency.

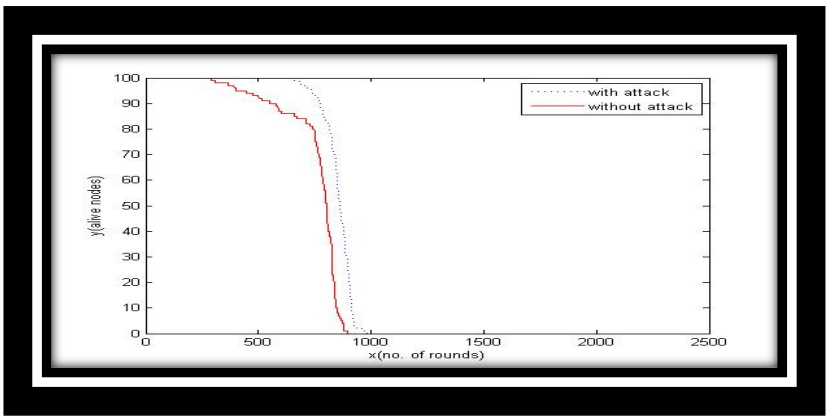

Figure 12 Graph between alive node and number of rounds

The Fig 12 shows the comparision of alive nodes w.r.t number of rounds.In this graph the red line shows more alive nodes w.r.t number of rounds (around 1000 rounds) in non-sinkhole attack as energy consumption is less and the dotted line shows less alive node w.r.t number of nodes in sinkhole attack because energy consumption is very high so more number of nodes dies (around 1000 rounds).

Energy Consumption: Energy consumption means how much energy is used by a node to complete a task. If energy taken by node is less than it is efficient. Energy consumption and modelling are significant considerations in the design and implementation of Wireless Sensor Networks (WSNs), since they allow designers to optimise energy usage in WSN nodes. The first step in reducing energy consumption in WSNs is to have a good understanding of the causes of energy usage. In wireless sensor networks, energy is a finite resource. Indeed, lowering power consumption is critical for extending the life of low-power sensor networks. Wireless sensor networks are made up of small, self-contained devices that can communicate wirelessly. Minimizing power consumption is one of the most important concerns to address in order to maximise the usefulness of the technology in real-world applications. As a result, for the evaluation of wireless sensor networks, an appropriate power model is necessary. The energy is used to calculate the sensor node's lifetime. Sensor node parameters are measured. Given the increase of research in this field over the last few years, the broad range of applications that could be aided by such a technology According to the proposed model, the expected lifetime of a battery-powered sensor node can be greatly enhanced. In the table present below is a statistical comparison of the values which are retrived as time taken by the different process algorithm, throughput and other parameter can be observe.

Table 1 statistical comparison

Parameters	Existing work	Proposed Work
Simulator	**NS2-2.35**	**MATLAB 2021**
Number of nodes	**37**	**100**
Antenna type	**Omni-directional**	**Omni-directional**

Plots	Energy consumption vs number of packet loss	Energy Consumption vs Number of rounds
Rounds in selected CH	Unknown	2500

The above table represents the number of data values from the data and algorithm is Performed.

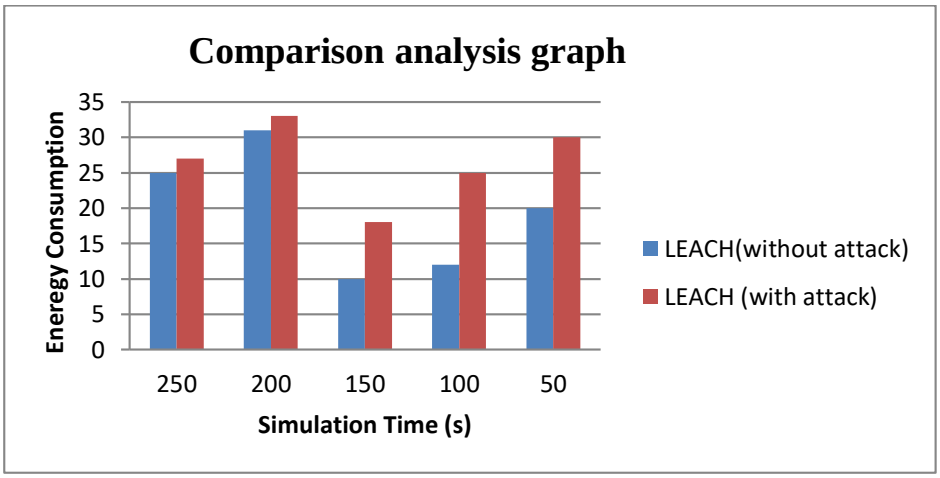

Figure 63 Comparison of Line graph for technique analysis

In the above graph drawn x axis as data from which post were extracted for the query processing for specified dataset and line graph is printed using the chart library provided by the Microsoft and further analysis can easility performed The graph representation shows the efficiency of our proposed algorithm work and it outperform the low forcasting value.

VII. CONCLUSION & FUTURE WORK

In this article a sinkhole attack in remote sensor organization be investigated. Wireless sensor networks are one of the significant technologies nowadays. It is also one of the most important IoT applications. Wireless sensor networks are a new form of networked system with limited computation and energy resources and an ad hoc operational environment. Wireless sensor network security has gotten a lot of attention in recent years. The severe energy restrictions of wireless sensor networks, as well as the demanding deployment conditions, make computer security more difficult than it is for traditional networks. WSNs are utilised to collect data in this era. The information could be about a defence or military system, the environment, weather forecasting etc. It may simply be utilised to acquire information due to its compact size. However, because of its tiny size, it is inefficient if energy use is high. When energy consumption rises, numerous attacks on WSNs, such as sinkhole attacks and wormhole attacks, occur. To protect the WSNs, LEACH (Low energy adaptive cluster head) protocol is used. In this article, we will compare the efficiency of the LEACH protocol when there is a SA and when there isn't. LEACH protocol is a type of hierarchical protocol which randomly selects the cluster head. This protocol always tries to equalizes the energy consumption.

This Work suggested that a sinkhole attack in a wireless sensor network be investigated. Wireless sensor networks are networks in which protection plays an important role in the organization's presentation. Sinkhole attacks degrade organisation execution by falling bundles and lowering filter convention efficiency. We may expect the calculation to rise continuously and broadly in our future work, where there are still various issues. In the meantime, we'll focus on improving the re-external enactment's appearance. We can clearly see from the graph of LEACH protocol that when a SA occurs on any node, the energy intake of is more .So, if we desire to save a Wireless sensors network then in future we can use other protocol such as M-LEACH. The multi level LEACH protocol is basically a efficient level protocol used im wireless sensors network. In M-LEACH, CHs are selected first, and these CHs send broadcast messages that they are the CHs to the nodes. This protocol increases the lifetime of network as compared to LEACH protocol. Apart from this we can also use a hierarchical type of protocol i.e. DD LEACH Protocol.At the first level LEACH protocol is used and after that DD LEACH Protocol is used. We can also increase number of nodes as in base paper 37 nodes are selected and in proposed model 100 nodes are selected. In this proposed model 2500 rounds are selected and in future number of rounds can also be increases.

REFERENCES

[1].Hoon Kim, Member, and Sang-wook Han, An Efficient Sensor Deployment Scheme for Large-Scale Wireless Sensor Networks, In IEEE communications letters, VOL. 19, NO. 1 January 2015 IEEE, pages

[2].Ankit Solanki Sarvajanik College of Engineering and Technology, Niteen B. Patel Sarvajanik College of Engineering and Technology, 4th ICCCNT IEEE-2013, pages

[3]. Ahmad Salehi S., M.A. Razzaque, Parisa Naraei, Ali Farrokhtala, “A Survey on Detection of Sinkhole Attack in Wireless Sensor Network”, In International Conference on Space Science and Communication Melaka, Malaysia e 2013 IEEE, pages

[4].Manpreet kaur, Amarvir singh, "Detection and Mitigation of Sinkhole Attack in wireless sensor network", In 2016 International Conference on Micro-Electronics and Telecommunication Engineering.
[5].Fang-Jiao Zhanga,b , Li-Dong Zhaia, Jin-Cui Yangb, , Xiang Cuic, Sinkhole attack detection based on redundancy mechanism in wireless sensor networks, In Procedia Computer Science 31 (2014) 711 – 720.
[6].Asaduzzaman and Hyung Yun Kong, A Survey on Detection of Sinkhole Attack in Wireless Sensor Network, In journal of communications and networks, VOL. 12, No. 4, August 2010.
[7]. S.Ranjeeth Kumar , A.Umamakeswari, SSLEACH: Specification based Secure LEACH Protocol for Wireless Sensor Networks, In School of Computing, Sastra University, Thanjavur,India IEEE WiSPNET 2016 conference.
[8]. Changlong Chen, Min Song, and George Hsieh, "Intrusion Detection of Sinkhole Attacks In Large-scale Wireless Sensor Networks", In George Hsieh is with the Department of Computer Science, Norfolk State University, Norfolk, VA 23504, USA 2010 IEEE.
[9]. Liping Teng and Yongping Zhang, "SeRA: A Secure Routing Algorithm against Sinkhole Attacks for Mobile Wireless Sensor Networks", In 2010 Second International Conference on Computer Modeling and Simulation Department of Computer Science and Technology China University of Mining and Technology Xuzhou, China.
[10]. Prakash kala, Arun Prakash Agrawal, Rishi Rajan Sharma, "A novel approach for isolation of sinkhole attack in wireless sensor network", In 10th International Conference on Cloud Computing, Data Science & Engineering 2020 IEEE.
[11]. Nazli Siasi, Adel Aldalbahi, Mohammed A. Jasim, "Reliable Transmission Scheme Against Security Attacks in Wireless Sensor Networks", In Department of Electrical Engineering, University of South Florida, Tampa, FL, USA 2019 IEEE.
[12]. Deepali S. Patil1 Shailaja C. Patil2, "A Novel Algorithm for Detecting Node Clone Attack in Wireless Sensor Networks", In Department of Electronics and Telecommunication Engineering, Rajarshi Shahu College of Engineering, Pune University 2017 IEEE.
[13]. Divya Bharti, Neha Nainta, Prof. Himanshu Monga," Performance Analysis of Wireless Sensor Networks under adverse scenario of attack", 6th International Conference on Signal Processing and Integrated Networks (SPIN)2019 IEEE.
[14]. Arya, Dr. Binu G S, Cross Layer Approach For Detection and Prevention Of Sinkhole Attack Using A Mobile Agent, 2nd International Conference on Communication and Electronics Systems 2017 IEEE.
[15]. D. Sasirekha, Dr. N. Radha, Secure And Attack Aware Routing In Mobile Ad Hoc Networks Against Wormhole And Sinkhole Attacks, In 2nd International Conference on Communication and Electronics Systems 2017 IEEE.
[16]. Aykut Karakaya and SedatAkleylek, A Survey on Security Threats and Authentication Approaches in Wireless Sensor Networks, In Internet and Network Technology Program, Department of Computer Technology, Bulent Ecevit University Zonguldak, TURKEY 2018 IEEE.
[17]. Yan-Xiao Li, Lian-Qin and Qian-Liang, Research On Wireless Sensor Network Security, In 2010 International Conference on Computational Intelligence and Security 2010 IEEE.
[18]. Adnan Ashraf and Abdul Rauf, A Model for Classifying Threats and Framework Association in Wireless Sensor Networks, In Research Scholar CREST Group.
[19]. Akshat Tyagi, Juhi Kushwah and Monica Bhalla, Threat to security of Wireless sensor network, In Amity University Uttar Pradesh 2017 IEEE.
[20]. Yang Xiaomei and Ma K, Evolution of Wireless Sensor Network Security, In College of Computer and Information Three Gorges University Yichang, Hubei, China.
[21]. Abdulaziz Abdullah Alsahli, Hameed U/lah Khan, Security Challenges of Wireless Sensors Devices, In Department ofInformation Systems, College of Computer and Information Sciences King Saud University, Riyadh Kingdom of Saudi Arabia 2014 IEEE.
[22]. Hong Tao ZHANG, Key Technologies of Wireless Sensor Networks, In First International Conference on Advanced Algorithms and Control Engineering.
[23]. Sibo Liu, Liaojun Pang†, Qingqi Pei, Hua Ma, Qingquan Peng, In Fifth International Conference on Information Assurance and Security Xidian University Xi'an, China.
[24]. Walid Elgenaidi, Thomas Newe, Eoin O'Connell, Daniel Toal, Gerard Dooly and Joseph Coleman, Tenth International Conference on Sensing Technology Limerick, Ireland 2016.
[25]. Jiann-Liang Chen1 , Yin-Fu Lai1 , Hsi-Feng Lu1,2 and Quan-Cheng Kuo1, In Department of Computer Science & Information Engineering, National Dong Hwa University 2008 IEEE.