Library Progress International
Vol.44 No.3, Jul-Dec 2024: P.5167-5180

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

Security Based Improved LEACH Protocol For Wireless Sensor Network

Vishal More[1], Suryakant. B[2]

[1]Department of Computer Science & Engineering, Bheemanna Khandre Institute of Technology, Bhalki
[2]Department of Electronic & Comunication Engineering, Bheemanna Khandre Institute of Technology, Bhalki
[1]Department of Computer Science & Engineering, Bheemanna Khandre Institute of Technology, Bhalki
[2]Department of Electronic & Comunication Engineering, Bheemanna Khandre Institute of Technology, Bhalki

How to cite this article: Vishal. More, Suryakant. B (2024). Security based improved LEACH protocol for wireless sensor network. *Library Progress International,* 44(3), 5167-5180.

Abstract

A popular security issue in wireless sensor networks (WSN) is the denial of service (DoS). The WSNs are susceptible to several denial-of-service attacks, even though the ZigBee protocol was developed with security and reduced battery usage in consideration. This happens particularly relevant when nodes are placed in unattended environments. In WSNs, the attacker uses the flaws to execute many DoS Attacks. In this research, numerous methods for protecting against DoS attacks are discussed, and a method for detecting and fighting against both worm-hole and black-hole assaults has been proposed. The suggested technique extends network lifespan and is simpler to install, uses two-way energy (Battery and Solar powered), and is less complicated. The results show that the security based improved leach is better than conventional methods considering energy and other parameters.

Keywords: WSN SecurityWormhole & Blackhole Attack DoS LEACH

INTRODUCTION (10 PT)

Wireless Sensor Network (WSN) is emerging as a prominent among those with the greatest promising future advancements [14]. The increasing availability of microelectronics innovation and low-power wireless connectivity and processing enabled the implementation of WSN across a wide range of applications. WSN is made up of a large number of inexpensive, microscopic wireless devices known as sensors, which are also known as motes. These small autonomous devices communicate with one another to detect real-time phenomena in nature such as humidity, temperature, pressure, motion, and so on, and send them to a sink for further analysis. WSN has attracted the interest of academics in recent years due to its broad application in delivering economical options for keeping track of real-time environmental variables. Depending on the application, Sink Nodes (SNs) in WSN can be deployed predictably (positions of SNs have been determined) or randomly (positions of SNs are unknown at deployment). Random installation involves dropping SN into difficult or unsupervised environments such as a battlefield, deep woodland, flood-affected area, forest fire, and so on. Predictable deployment is used in building monitoring, tracking patients, and commercial monitoring, among other applications [15][16].Regardless of the reality that WSNs are defined by an effective combination of circulated discovering, communication and analyzing, and connection, there are numerous applications of WSNs, which provide some challenges, most notably the extreme energy limits, limited calculating power, communication accessibility, and additional space of SNs. The primary purpose of WSN is to gather and communicate data while attempting to extend the network lifetime through the use of energy-efficient approaches. There are various difficult aspects to consider while creating routing standards in WSN. These aspects must be managed effectively. Some of the significant issues in WSN are, i). Network lifetime ii). Response time iii). Scaling iv). Self-Configuration v). Coverage & Interconnection vi). Security & Privacy vii). Latency [17]. In this paper authors concentrate on security in WSN. The security of the information acquired by sensors is a major problem[18]. As a result, two main levels of security may be implemented: encryption and authentication procedures. Encryption methods encode information in order

to keep it secure from attackers. Authentication is the method or action of authenticating the identities of users. It is an effective strategy for protecting against assaults. Because of the resource constraints of WSNs, encrypting information is an expensive and infeasible option. Because the channel in WSNs is wireless, it is highly vulnerable to numerous forms of attacks. Before interacting across a network, a user must be authenticated. Traditional authentication mechanisms are inappropriate to WSNs. Authenticating protocol security features such as resistance to numerous assaults, mutual authentication, password freedom, and session key generation are all critical in WSNs. In the case of user authentication, an individual must register with the system in order to be verified by the system as a whole [19].

There are multiple types of attacks have been defined for authentication scheme like, DoS attack, impersonation attack, password guessing attacks, base station bypassing attack, stolen verifier attack insider attack etc. These attacks can be analyzed using the parameters, computation cost, communication cost and security feature. Because wireless signals are transmitted across the air, so anybody who is within the communication reach of the transmitter may get the signal, safety is a difficult issue in wireless networks. This characteristic saves energy because the transmitter can send data to all users at the same time rather than sending data to each user separately; however, this characteristic is a security bottleneck because the signals that are sent can be effortlessly captured by an intruder that is inside the transmitter's communication range, making confidentiality of data more difficult to attain. As a result, the primary emphasis of the paper is on the privacy component of security and also discusses the types of attacks and how to detect them so as to avoid the information bleaching.

In general, there are two types of attacks one is active attack and another is passive attack [20]. Active network assaults disrupt regular network interactions and alter transmission of information. Sinkhole attacks, packet dipping, IP spoofing, and so on are instances. Passive attacks gather information without interfering with network traffic. Examples include monitoring traffic, analyzing traffic, and eavesdropping. The security methods designed for WSN are divided into two main groups: i) Low level ii) High level. Key establishment, privacy and authentication protocols, secure routing, and resilient node capturing are all part of the low-level security system.Intrusion Detection System (IDS), secure data aggregation, and other high-level security mechanisms are included [21].

Scalability, like that of other forms of communication systems, is the most crucial architectural aspect of sensor networks. When employing a single-tier network, the gateway commonly becomes overwhelmed as sensor density grows. Due to overloading, such communication lag is conceivable, and event monitoring becomes extremely challenging. If the network grows in size, just one gateway design is incapable of processing communication.Some routing systems have used network clustering to enable the system to be able to cope with the increased load required to cover the huge sensor network. The primary motivation for designing hierarchical networking is to efficiently manage energy consumption associated with sensor nodes at greater levels by involving them through multi-hop communication to form a cluster [22].

A sensor node's lifespan is determined by the sources of energy that are accessible and its energy usage. Furthermore, because of the sensor nodes' tiny size, increasing battery capacity doesn't seem viable. In the end, the problem may be solved by lowering the energy utilized by the sensor nodes. The goal of this effort is to find and measure energy-saving solutions in WSN. A crucial precondition for carrying out this task is the development of a technique for assessing energy usage across individual WSN nodes and the entire network throughout its entirety.WSNs could be attacked from both inside and outside the network. Outsiders in cryptographically safeguarded networks are not given proof of identity or key to demonstrate that they're actually network members, but insiders have. Insiders can occasionally prove trustworthy since their identities might have been stolen or obtained certificates from trusted nodes in the network. The BS is believed to be genuine. The paper concentrates on the DOS types of attacks especially on wormhole and Blackhole attacks.

The rest of the paper has been organized as follows, section 2 depicts related work, section 3 describes proposed work, section 4 explains the results and discussion and finally section 5 concludes the paper.

1. RELATED WORK

In article [1], authors suggested a stable and secure LEACH (SS-LEACH), for enhancing the stability of CH and energy efficiency as it considers the nodes' consumed energy ratio (CER) for CH selection and random number generation, here after the proposed LEACH is named as CER-LEACH. In addition, it aims to prevent the previously elected CH node and it will get another chance in the current round. This method correlates the

threshold used in traditional LEACH with the energy consumption ratio of each node. Further, it also introduces a hybrid reputation-based data transmission (HRDT) scheme for secure data transmission. With the proposed CER-LEACH protocol, WSNs achieves better performance in terms of secured communication, network lifetime, and energy consumption based on the analysis of simulation results

Node to node trust-based procedures for secure routing in MANET were suggested by the author, according to [2]. Mobile Ad-Hoc networks are multi-hop networks that depend on dynamic infrastructure because their nodes are typically mobile and need a signal for communication. Due to its benefits of being flexible, quick to start up, affordable, and durable, Mobile Ad-Hoc Network (MANET) is becoming more and more well-known. However, it has drawbacks including a short wireless range, unpredictable routes, packet loss, heterogeneous devices, and a low battery life. Because of this, MANET is more susceptible to security assaults than infrastructure-based wired networks. Wormhole attacks are among the most harmful since they have a significant impact on routing. In order to offer secure routing, it is important to isolate hostile nodes in MANETs without incurring significant overheads. hostile node identification alone is insufficient. The suggested approach makes advantage of aggregated N2N trust to identify wormhole source malicious nodes and isolate them in order to prevent routing from being intercepted by them. As a result, the system delivers secure data traffic routing with increased throughput.

Transmission Range based Method (TRM), which determines the transmission range using local neighborhood data, is the extremely effective wormhole detection method that the author presented, according to [3]. Without the use of additional hardware or clock synchronizations, the suggested solution is based on the transmission range and utilizes the local neighborhood information check. Numerous simulations are run using various mobility models. The suggested method may effectively and efficiently identify wormhole attacks in WSNs, according to simulation results.

The author [4] talked about different Mobile Ad-hoc Network attacks. Due to the wireless nature of communication, WSNs are unstable since any attacker wishing to steal the data may do so by introducing rogue nodes into the network. Attackers may do this by initiating many types of attacks, including wormhole, flood, and grey hole. Finding the shortest path between a source and a destination node is often the aim of routing protocols. The hop count is a metric that is used to determine the distance traveled. One of the numerous above-described methods, the wormhole attack, is dangerous since it creates a tunnel by ignoring a few nodes in between them. The tunnel automatically reduces the hop length, creating a direct path between the source and destination nodes. This article gives a succinct outline of the techniques or tactics for recognizing and fending off wormhole attacks. WSNs are more susceptible to several forms of attacks because of their remote wireless nature and human unsupervised environment, and intruders may visit these networks on purpose or accidentally. In article [5], the author put out the secure LEACH protocol as a way to identify network intrusions as well as wormhole and black hole attacks. With the use of several base stations and a key, this detection method attempts to stop assaults on wireless sensor networks employing the LEACH protocolThe LEACH technique is utilized, which significantly reduces energy use. As a result, overhead is decreased and data delivery is improved. Since several base stations are used, data is supplied 100% of the time. Since LEACH protocol is employed, it ensures extra energy power supply for a long period of time.

This guarantees that the packet delivery ratio has increased, extending the network's lifespan. More security is provided for the individual nodes, however increasing node security requires more energy, which shortens the network's lifespan.The assaults on mobile ad hoc networks (MANETs) were explored in this paper [6]. Decentralized networks that can interact without pre-existing infrastructure are referred to as mobile ad hoc networks (MANETs). Due to their use of open medium access and dynamically changing network topology, MANETs are susceptible to numerous attacks, including the Sybil attack, rushing attack, jellyfish attack, wormhole attack (WHA), byzantine attack, selfishness attack, and network partition attack. Worm hole attacks are among them, and they are the most frequent and harmful attacks that seriously impair network performance and interfere with routing protocols. In this research [6], the attacks on mobile ad hoc networks (MANETs) were examined. Mobile ad hoc networks (MANETs) are decentralized networks that are capable of interacting without the use of established infrastructure. In addition to the Sybil attack, rushing assault, jellyfish attack, wormhole attack (WHA), byzantine attack, selfishness attack, and network partition attack, MANETs are also vulnerable to the Sybil attack, wormhole attack (WHA), and jellyfish attack due to their usage of open medium access and dynamically changing network topology. Worm hole attacks are one of them; they are the most prevalent and harmful assaults that drastically affect network performance and obstruct routing protocols.

The attacks on mobile ad hoc networks (MANETs) were looked at in this study [6]. Decentralized networks with the ability to communicate without the aid of pre-existing infrastructure are known as mobile ad hoc networks (MANETs). Due to their use of open medium access and dynamically changing network topology, MANETs are also susceptible to the Sybil attack, wormhole attack (WHA), and jellyfish attack in addition to the rushing assault, jellyfish attack, wormhole attack (WHA), byzantine attack, selfishness attack, and network partition attack. One of them is a worm hole attack; it is one of the most common and dangerous assaults that seriously degrades network performance and obstructs routing protocols.

In this study [6], the assaults on mobile ad hoc networks (MANETs) were examined. The term "mobile ad hoc networks" (MANETs) refers to decentralized networks that can interact without the assistance of pre-existing infrastructure. MANETs are vulnerable to the Sybil attack, wormhole attack (WHA), and jellyfish attack in addition to the rushing assault, jellyfish attack, wormhole attack (WHA), byzantine attack, selfishness attack, and network partition attack because they use open medium access and have dynamically changing network topology. One of them is a worm hole attack, which is among the most frequent and deadly attacks and severely impairs network performance and interferes with routing protocols.

The attacks on mobile ad hoc networks (MANETs) were looked at in this study [6]. Decentralized networks that may communicate without the aid of pre-existing infrastructure are referred to as "mobile ad hoc networks" (MANETs). Due to their use of open medium access and dynamically changing network topology, MANETs are susceptible to the Sybil attack, wormhole attack (WHA), and jellyfish attack in addition to the rushing assault, jellyfish attack, wormhole attack (WHA), byzantine attack, selfishness attack, and network partition attack. A worm hole attack is one of them; it's one of the deadliest and most common types of attacks, substantially reduces network performance, and messes with routing protocols.

In article [10] author propose a novel technique for detecting black-hole attacks in WSNs using multiple base stations and check agents to detects and prevents black hole attacks in WSNs. If there is a chance of black hole attack in the network. The proposed solution forces every node in the network to maintain a list of neighboring nodes. Moreover, it uses Dijkstra's algorithm to establish the routing path and a check agent to examine the nodes routing through multiple base stations. Otherwise, routing is done through the nearest base station only, in order to reduce energy consumption in WSNs. Also, author demonstrated that check agents have an important factor in black hole attacks detection in WSNs by decreasing the complexity of the messages and reducing network overhead. Data delivery is ensured due to the use of multiple base stations.

In article [11] the author proposed an Enhanced Detection and Prevention Mechanism for Black hole Attack (EDPMBA) Trust Model to save the assurance from single and helpful black hole attack. The trust model reports a successful and secure instrument for identification of single and cooperative black hole attack and gives a protected routing path from sensor node till base station. This method continues acting mischievously node from being a piece of a system correspondence process before real black hole identification system is started. Simulation results shows better performance of EDPMBA as far as delay and PDR which is the basic prerequisite in WSN

In paragraph [12], In the sensor network, clusters are made using the K mean clustering approach. The formation of the clusters ensures that the sensor nodes within each cluster pass detected data to the relevant cluster head rather than straight to the sink node. The attacker enters the passageway to interact with the packets flowing between them when it receives a request for a route from the destination node. It then constructs a reply for the short route. If a black hole node exists in the network, it will cause the network's energy to be used up more quickly while also reducing performance by keeping an eye on the bogus reply packets that the nodes send out, the black hole node can be located and eliminated from the network. As a result, the sensor nodes' battery usage will be lower, and the sensor network's performance will improve.

The author [13], proposed a cryptographic cluster-based communication technique for preventing the network from attackers. In addition of that the clustering schemes are help to improve the performance of network in most optimum manners. For securing the network the cluster network includes the Blackhole and Grayhole attack for detection and prevention. The implementation of the proposed secure technique is performed using the AODV

2. PROPOSED WORK

This section depicts the system architecture of the proposed work along with working and algorithms used for detecting Blackhole and Wormhole attacks. The proposed work also gives the key based methodology to restrict Blackhole and Wormhole attacks.

3.1. System Architecture

LEACH is intriguing since it dynamically and occasionally organizes the nodes in the cluster. It renders relying on long-term node-to-node trust connections to protect the protocol challenging. It is a critical component in adding security to WSNs. Applying security to WSNs is very difficult since they are embedded. Because of a shortage of resources, current approaches for conventional and various other networks are inapplicable to sensor networks.

Although public keying is conceivable in sensor networks, effective solutions can only be found by adjusting network architecture.

After the clusters are formed and the TDMA schedule is established, nodes begin transmitting data, assuming that all nodes have data to broadcast. These nodes receive the data and deliver it to the CH within the allowed delivery period as shown in figure 1. The lowest quantity of energy needed for transmission is determined by the received intensity of the CH. Every non-Cluster Head's radio can be switched off till the nodes' assigned time to broadcast expires. This reduces the loss of energy. This does not apply to CH; the CH must maintain its receiving switched on in order to receive every bit of information from the cluster's nodes. Because the base station is situated far away, the combination signal is an energetic signal that is transmitted to the base station. The information in these packets are sent by the CHs utilizing CSMA, an established spreading algorithm. Following a certain amount of time, the following round starts off with a new node becoming the CH for this particular round and notifying all the others of the decision.

The proposed protocol is meant to reduce energy usage while yet maintaining a secure network. The proposed scenario describing wormhole and Blackhole is as shown in figure 2. This improved LEACH procedure is divided into two phases: setup and steady state. A CH is chosen and created to be the Head for one cycle according to the amount of energy in the nodes. To the SN, all nodes submit their leftover energy and desire in becoming the CH. If the nodes have more energy and more nodes coverage, they are promoted to CH. The first responsibility of the CH is to build a cluster with adjacent surrounding nodes. The CH broadcasts an acknowledgment in addition to the advertising message to build a cluster. The message being promoted is issued by all CHs, and the CHs choose to depend on the signal intensity detected by the nodes. An individual non-Cluster Head node might get two separate Cluster Head messages. It selects the signal with the highest intensity. A member node that wishes to become a CH sends a willingness to participate message to the CH. likewise; all non-Cluster Head nodes communicate their eagerness to join through their corresponding CHs.

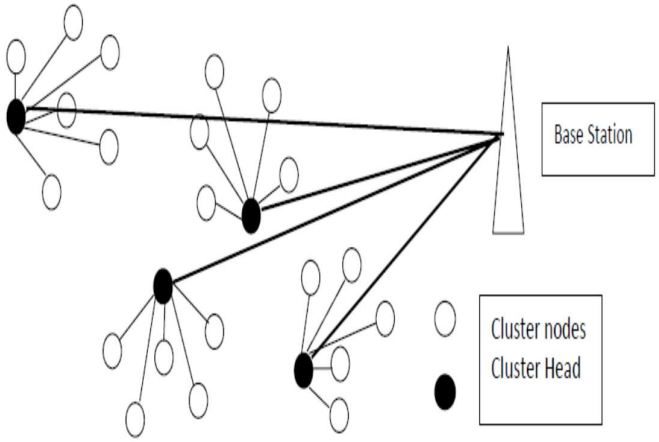

Figure 1: System Architecture

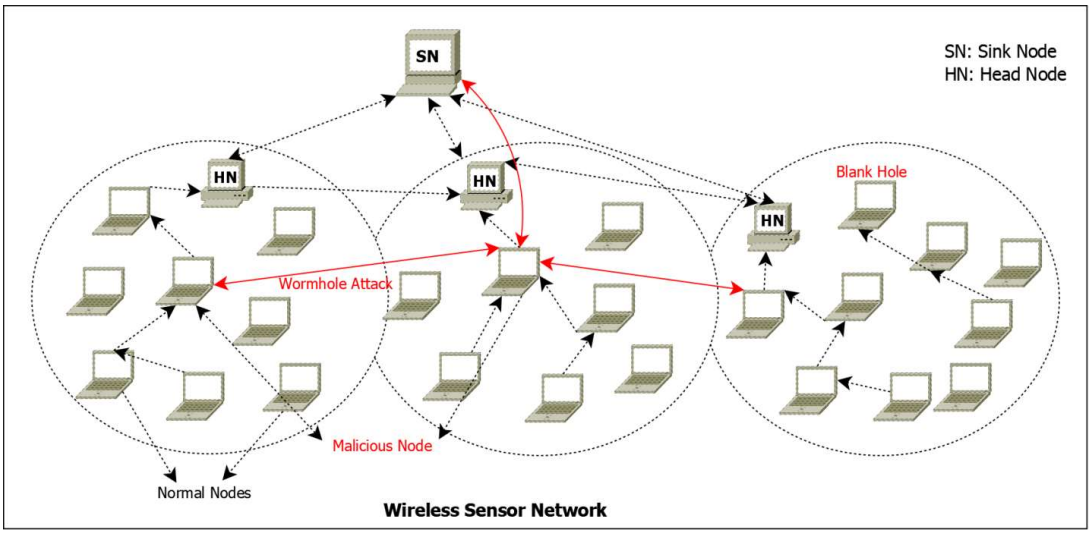

Figure 2: Proposed Scenario

One of these nodes is chosen as the CH, and the connected node joins the given cluster. All of the CH nodes can join any of the CHs. The login details are distributed to the participating nodes by the CH from the BS/SN. The SN has a collection of keys that are produced at random through a random generating technique. Keys are produced and given out at random to membership nodes; every node in all clusters is assigned a key. Nodes communicate their information and keys to the CH throughout information transfer. The information is delivered to the CH, who then confirms that it is from an authorized cluster member. The information received is from an unauthorized node if the CH receives information and a key that don't match the created key. A node of this type that has the geographical coordinates it obtained is removed from the cluster and the network as a whole. Information is still being sent till the start of the following round.

The SN, which has access to a pool of keys, is the entity that generates keys at random. All the keys are gathered by the CH and sent to the SN. After collecting all the keys, the SN checks to see whether any are duplicates or mismatched. If someone remains, it indicates that there is an intrusion into the network; otherwise, the nodes are clear of any intrusion. Additionally, if the total amount of keys and nodes is exactly the same as the period before, there isn't a new intrusion in the WSNs. A node replica threat is conceivable if there is duplicate information or a key incompatibility. Lastly, the CH is informed of the total number of nodes, their availability for use, and details like how much energy they have. The CH gathers all information from non-Cluster Heads, and all CHs submit information about their nodes to the SN. By providing this data, it is possible to calculate the nodes' energy levels and count the number of failing nodes.

The usual security techniques are unable to be directly applied in WSNs because of their numerous restrictions. Given that the WSN deployment region may include public areas where an intruder might directly seize control of the sensor nodes and steal all the data. Additionally, some nodes might perish from energy problems or new nodes could join the network. Denials of service assaults, which are perpetrated by an attacker by focusing on the routing method, are among the main issues. These assaults might be the result of malicious action or unintended node failure. In this type of attack, a targeted node's resources are depleted by receiving needless messages that are not authorized or intended for that node. DoS attacks target not just hostile nodes but also situations that undercut the network's capacity to deliver services. There are certainly many kinds of DOS assaults that malicious nodes might use to harm the network, render it unsafe for communication, and obstruct the network's normal operation. Black hole and wormhole attacks, two common assaults on the network layer, will be the major topics of this paper.

3.2 Identification of Blackhole

An assault that records nodes and modifies them so they are unable to send any information in packets is known as a "black hole attack." In the black hole attack, the node presents itself as a genuine node and offers an unauthorized path to the target node. This attack's objective is to intercept packets. The traffic starts passing via the target node when the source node chooses a routing that includes the attacker node. This node starts dropping

packets in chunks or at random. Once a black hole assault is launched, further attacks can follow.
There are no issues with the transfer among the CH and participating nodes. Each of the nodes which are getting additional packets is recognized in order to determine whether the wormhole exists in the network's infrastructure. To find out whether there is an assault, every node is watched. In this case, LEACH uses links between source nodes, the cluster's CH, and the SN. It is broadcast from the SN to the cluster's CH and then to the target node. Presuming that the network just uses single-hop communication and doesn't make use of multi-hop communication.
If a node transmits to CH, the next node, SN will receive the signal if CH is the sending node. If a node p transmits y bits of data, q nodes get y bits of data or data that is almost y bits in size. The q node is an attacker if it doesn't send any data to the subsequent hop. A wormhole attacker is present when node p sends node q'y' bits of information while node q sends no data at all.If node q transfers data to the subsequent hop and communication proceeds without any problems, there has been no possibility of network assault.
Algorithm for detection of Blackhole attack
The technique is employed in nodes whenever transmission of information fails to determine whether or not an intruder is existing. There is no threat or intrusion if the information has been received. The node waits for time t + ty if the information fails to arrive after a typical waiting period of t, wherein ty is a variable amount of time that varies based on the information that was sent. Even if the period of waiting is finished and the information has still not come, the node might have failed or the awaiting interval would be prolonged by another time period of ty. As a result, information may be delayed or, in the case when the node didn't get anything, information may have been taken during an intrusion.
When a source launches a wormhole attack, the target only receives 0 packets while the source sends y packets. The packet delivery ratio becomes infinity here.

Detection of Blackhole attack

START
Each node that is getting more packets is identified.
for(Np =1; Npi<= n;N++)
Consider the node p transmits data to a neighbor q and then s and so on
if (Np forwards to Nq) here q=p+1 always q=CH, p=member node
then
p transmits y bit information q receives y bit information.
Nq transmits 0 bit information
Np is a Wormhole attacker.
Else
Nq is not a wormhole attacker node.
End if
End for
END

Next algorithm gives how to detect the intruder,

Detection of an intruder in the system

```
START
In nodes during which delivery is unsuccessful
for( p to s)
if (information entrance ==1 )
then
no intruder or risk
else if (no arrival reply information)
then
if(wait time >= Threshold waiting time)
then
node malfunction
else
wait for a reply
else if (no information arrival)
then
Intruder node noticed
else
wait for a reply
end if
```

3.3 Identification of Wormhole attacks

The technique is used to determine whether or not an intruder exists in the network. Through an intermediary SN and the appropriate CH, the non-Cluster HN from a cluster transmits information to another non-Cluster HN. if the message that's being transferred was sent from the source node but was not received. Either the node fails or an intruder is found.

If the anticipated recipient node receives information following the Tx interval, there was either an overhead delay or another problem. The anticipated node might have failed if it didn't get any messages. If more information hasn't come in, attacks are to blame.

When the communication is in advancement, a data packet of size a bits is broadcast, followed by an interval of Ta, a message of size b bits gets delivered, or when a node anticipates delivering in node E and a node actually gives in node F, the attack may be determined to be a wormhole attack. The discovered node in this instance is a wormhole attacker node. With the aid of this method, the legitimacy of each node is determined.

Algorithm for wormhole attack

```
Pneumonic: Tx: Transmitted, Dx: Delivered
START
IF(Tx msg==1)
Dx msg==0
Node malfunction or Assault noticed.
IF (Dx msg==1 after time Ta=T+T(n)
Delay (due to node malfunction or owing to overhead)
Else
Attack detected.
IF (Tx msg=a)
Delivered Message =c after time delay Ta=T+T(n)
Anticipated node to deliver = E
Node delivered =F
Wormhole attack detected.
End if
```

3.4 Avoiding wormhole attacks

An attacker is sandwiched in the network between two separate points and controls the wormhole attacks. The attacker nodes or harmful nodes can interrupt the communication among CHs and draw traffic to themselves. Into

wormhole attacks, an attacker's node steals data from a trustworthy node and subsequently tunnels the information via a minimal latency link and broadcasts within a specific area of the network. This sent information may be changed, replayed, or sent in its original form. When information is transferred via a network from one node to another, it must hop through several nodes before it ultimately reaches its destination. In such circumstances, the nodes absorb information by hiding close to any other node and tunneling them to a node that is extremely distant. The cluster-based strategy is the method used, and the improved LEACH protocol is applied.The CH is one of the clusters that the LEACH algorithm divides a set of nodes into. This means that the CH and the SN are the most exposed to intrusions.The target nodes and CH both vary often being attacked in this method. The network is completely secure when the CH and SN are secured. In this approach, many SN are employed, and the new CH is chosen following each round. Attacks are decreased when numerous base stations are used.

When keys are distributed inside a cluster, 50% of the nodes possess one key while the remaining half possesses a different key. For a cluster, Completely SN assigns two unique credentials. Similarly to that, each cluster receives two unique keys. The CH gets a key from the SN. A single-bit key is supplied for each CH. Additionally; the BS gives all of the non-CH nodes their keys directly. The key that is supplied to CH is also given to each CHs in turn. This is used to verify whether or not the CH is real.

Two distinct keys are given to each node. The first key is used by the CH node to determine if the younger nodes are malicious, while the other key is used by the CH nodes to figure out whether or not the CH is real. A collection of keys that the CH nodes acquired from the BS are first randomly distributed across each of its membership nodes. In all, it contains two sets of keys. Before transferring data, each nCH node verifies its kindness. The SN transmits the keys together with its node IDs to collect information.

The master CH who possesses the information about each of the nodes' keys. The CH asks the nCH for the keys prior to accepting the information. The key generated by nCH and the key that is that exists in the CH databases is then compared. The CH gets the information when both are identical. The CH reports to the BS with the nCH ID if the keys are different. The CH are unable to predict each of the nodes' keys even if it is compromised. As a result, the CH may be identified as an unauthorized node and quickly stopped. The multiple nCH nodes can communicate securely using this type of key generation approach. The SN is the next potential target for assaults. In this case, a third party is added to the extensive network to keep an eye on the SN. Taking into account that the system has many SN.

3.5 Key based wormhole and Blackhole prevention

It uses the improved LEACH protocol to divide the network's traffic into clusters. In the upcoming rounds, one of the many nodes that each CH owns is anticipated to succeed the current CH. The information is gathered and combined by all non-Cluster Heads. The data is subsequently transmitted from the CH to the SN, which ultimately transmits it to the target node. The nodes which are accessible in this situation with all the gathered data are the CH and the SN. Such nodes are vulnerable to assaults because they contain data. If the assailants gain access to these nodes, they may quickly launch an assault on these nodes. At each cycle, a bit is included in the transmission information in order to prevent these assaults and manage the scenario with any problems. The Base Station transmits a one-bit message to every node, including the CH, after every cycle to verify the network for any assaults. The key in this one-bit communication was chosen at random. To facilitate communication, several keys of a single bit in size are given to each node.

In a cluster, 50% of the randomly chosen nodes are given one set of keys, while the remaining half are given keys that are identical. The CH is given two separate sets of privileges for a cluster by the SN. A pair of keys must be given by the CH to each of their separate clusters. The CH is prepared to collect data once the transmission of information from the Non-Cluster Head to the CH starts. Before transferring data, nodes request the key from the CH for verification. The owning key and the new key obtained from the CH are both verified for politeness by all nodes. According to the immediate data received by the SN, it determines whether or not the own key and the new key are identical.

$$\Pi = [SN1, SN2, SN3, SN4], n - 1\ to\ 4 \quad (1)$$

Example, if one SN fails or found malicious then such SN will be removed from the group.

$$\Pi new = \Pi - \Pi(n) \quad (2)$$

where the nth node is the harmful node. Now the new Base Stations are

$$\Pi new = [SN1, SN2, SN4] \quad (3)$$

As a result, there are no attackers on the network. Therefore, the check procedure is completed each and every

time. It is ensured that both the SN and the nodes are safe from assaults.
The network may now transmit data among nodes without experiencing any issues or losing messages due to improved security. In other words, the nodes interact with their neighbors while protecting their sensor and information nodes.

The lifespan of the network is lowered to greater levels due to the continual usage of these nodes and the inclusion of security, which causes the nodes to run out of energy. The energy loss caused by the power shortage poses a serious problem, and in order to increase the node's lifespan it requires a longer outside power supply. The depletion of energy on the other end can be charged and matched with the energy generated by the solar panel on the opposite side if the node is connected to a solar-powered energy source.

4. RESULTS AND DISCUSSION

This section describes the results and discussion of the proposed work. The simulation was carried out through the network simulator, and the outcomes are displayed as follows; the sensor region is 200*200 long. There are 100 nodes altogether, all of which are battery- and solar-powered. The total SN is four and is located s meters from the center. Two SN are separated by 2s meters, and the other simulation parameters are listed in the Table 1.

TABLE 1: Simulation Parameters

Simulation region:	100*100
Total Nodes:	100
Packet size:	4000 bits
Node Energy:	3 joules
Cluster Head proportion:	p=6%
No of SNs:	4

4.1 Remaining Energy

The network's remaining power after p rounds is depicted in a graph. In contrast to the standard LEACH without any intruders (Malicious node) termed as LEACH-M and the LEACH protocol-used system with an intruder or assailant in the sensor network, the amount of energy consumed in the source node and the target node appears to be greater in the proposed Secured improved LEACH method.

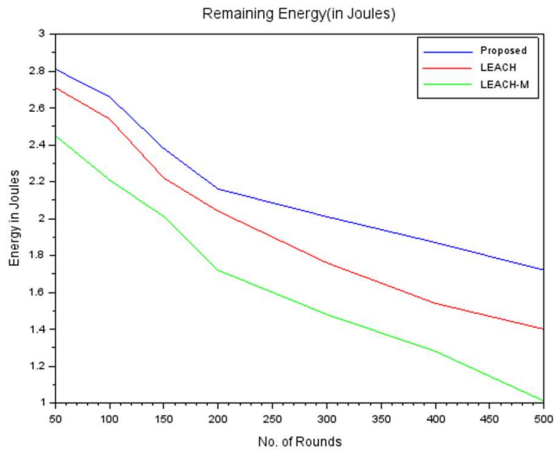

Figure3: Remaining Energy

4.2 Packet Delivery Ratio

The proportion of the information packets sent from the sending node to those that were received. The graph compares the sent and received messages/bits. PDR= (No. of Messages received/No. of Messages Transmitted) *100

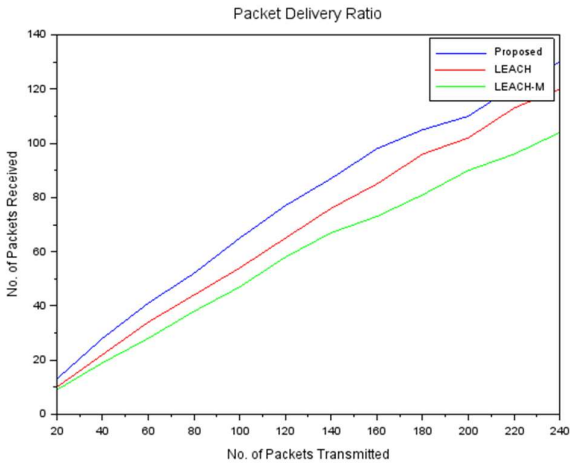

Figure4: Packet Delivery Ratio

A graph showing the number of active nodes over time is shown. As contrasted to the LEACH protocol, the proposed Secured LEACH performs quite well. The overall number of deceased nodes drops, PDR grows, while control overhead rises as the nodes become solar-aware and security is introduced.

4.3 PDR Vs Time and PDR Vs Network Density

The PDR against time is explained in Figure. The suggested improved LEACH performs significantly better than the original LEACH and LEACH with Intruder.

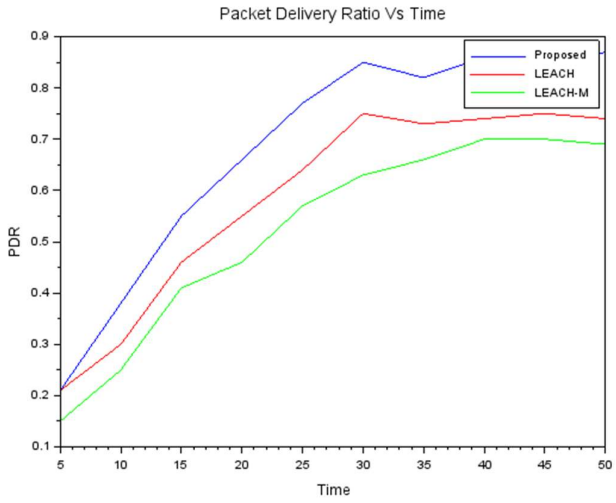

Figure5: PDR Vs Time

The PDR is shown against the network density. As the total amount of nodes rises in the Secured improved LEACH method, an increasing amount of packets get delivered compared to LEACH, and LEACH with Intruder performance is very poor. In the Figure, the network's density is shown.

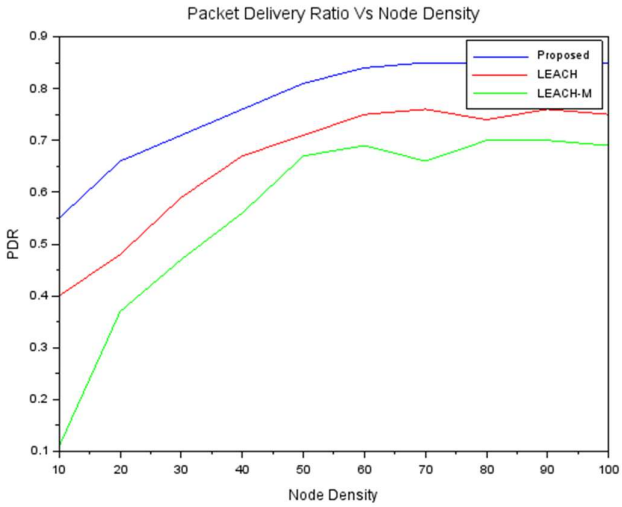

Figure 6: PDR Vs Node Density

5.CONCLUSION

One of the key components of the wireless sensor network is security. The majority of network resources are exploited through denial-of-service attacks. Wormhole and black hole attacks are challenging to recognize and counter. The mechanism for effectively detecting and defending against wormhole and black hole attacks is proposed in this research. It also includes an updated leach version that uses less energy. As a result, the nodes' batteries will last longer, contributing to an extended network lifetime. The results show that, when energy, PDR, and node density parameters are taken into account, the proposed approach performs much better than traditional methods. Additionally, this approach may be expanded to counter additional denial-of-service threats.

ACKNOWLEDGEMENTS (10 PT)

I would like to thank Visvesvaraya Technological University, Belagavi for providing therequired facility to complete my Ph.D within stipulated time and also i would like to thanks Dr.Sangamesh Kalyane, Professor BKIT Bhalki, for supporting me to bring this paper successful.

REFERENCES

[1]. Ravi Kumar Sanapala, Srineevasa Rao Duggirala, "A Secure LEACH Protocol for Efficient CH Selection andSecure Data Communication in WSNs", International Journal of Computer Network and Information Security(IJCNIS), Vol.14, No.5, pp.82-93, 2022. DOI:10.5815/ijcnis.2022.05.07

[2]. Nisha Sharma, Mukesh Kumar Gupta, Durga Prasad Sharma, M. K. Banerjee,"Improved N2n Trust Based Mechanism To Mitigate The Effect Of Wormhole In Dynamic Source Routing Protocol ",Journal of Theoretical and Applied Information Technology,31st January , Vol.100. No 2, 2022.

[3]. Guowei Wu, Xiaojie Chen, Lin Yao, Youngjun Lee, and Kangbin Yim," An Efficient Wormhole Attack Detection Method in Wireless Sensor Networks," Computer Science and Information Systems, Volume 11, Issue 3,pp. 1127-1141,2014.

[4]. Deepak Badgujar , Lokendra Jat," Review of Wormhole Attack on Mobile Ad-hoc Network", International Journal of Scientific Research & Engineering Trends, Volume 8, Issue 4, , ISSN (Online): 2395-566X ,-Aug-2022.

[5]. R.M. Dilip Charaan, R. Ramesh and E. Uma," Detection and Prevention of Wormhole Attacks in Leach Protocol for Wireless Sensor Networks",Asian Journal of Information Technology , Volume:16Issue:1pp.69 –76,2017.

[6].Gupta, Chitvan, Singh, Laxman and Tiwari, Rajdev. "Wormhole attack detection techniques in ad-hoc network: A systematic review" Open Computer Science, vol. 12, no. 1, pp. 260-288. 2022.

[7]. Bin TIAN , Qi LI , Yi-xian YANG , Dong LI , Yang XIN ," TA ranging based scheme for detecting the wormhole attack in wireless sensor networks", The Journal of China Universities of Posts and

Telecommunications", Volume 19, Supplement 1, Pages 6-10 ,June 2012.
[8]. K. P. Sampoornam, S. Saranya, G. K. Mohanapriya, P. Sandhiya Devi and S. Dhaarani,"Analysis of LEACH Routing Protocol in Wireless Sensor Network with Wormhole Attack", in proc.ThirdInternational Conference on Intelligent Communication Technologies and Virtual Mobile Networks(ICICV), Tirunelveli, India, pp. 147-152,2021.
[9]. Bindu Rani,Harkesh Sehrawat", Blackhole Attack Detection And Prevention In Wireless Sensor Networks: A Study ",Journal of Emerging Technologies and Innovative Research (JETIR),Volume 5, Issue 3,pp:461-465, March 2018.
[10]. Detecting Black-Hole Attacks in WSNs using Multiple Base Stations and Check Agents",inproc.Future Technologies Conference San Francisco, United States, pp. 6-7 December 2016.
[11]. Ganesh R. Pathak, M.S. Godwin Premi, Suhas H. Patil ,"A Trust Model for Security Against Black Hole Attack in Hierarchical Cluster Based Wireless SensorNetwork",International Journal of RecentTechnology and Engineering (IJRTE), ISSN: 2277-3878, Volume-8 Issue-4,pp-12645-12650, November 2019.
[12]. Kalaiselvan. K , Gurpreet Singh ,"Detection and Isolation of Black Hole Attack in Wireless SensorNetworks", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue-5,pp. 3516-3524, May 2015.
[13]. OjashviShivwanshi, Rahul Patel, Preetika Saxena"," Cluster Based Secure WSN against the Blackhole and Grayhole Attack", International Journal of Computer Science and Information Technologies, Vol. 6 (6), pp. 5470-5472, 2015
[14]. Faris, Mohammed, Mohd Nazri Mahmud, Mohd Fadzli Mohd Salleh, and Alhamzah Alnoor. "Wireless sensor network security: A recent review based on state-of-the-art works." International Journal of Engineering Business Management 15 (2023): 18479790231157220.
[15]. Kandris, D., Nakas, C., Vomvas, D., &Koulouras, G. (2020). Applications of wireless sensor networks: an up- to-date survey. Applied system innovation, 3(1), 14.
[16]. Huanan, Zhang, Xing Suping, and Wang Jiannan. "Security and application of wireless sensor network." Procedia Computer Science 183 (2021): 486-492.
[17]. Jebi, R. Christal, and S. Baulkani. "Mitigation of coverage and connectivity issues in wireless sensor network by multi-objective randomized grasshopper optimization based selective activation scheme." Sustainable Computing: Informatics and Systems 35 (2022): 100728.
[18]. Luqman, Mohammad, and Arman Rasool Faridi. "Security in wireless sensor network: a current look." In 2022 9th International conference on computing for sustainable global development (INDIACom), pp. 385-391. IEEE, 2022.
[19]. Tropea, Mauro, Mattia Giovanni Spina, Floriano De Rango, and Antonio Francesco Gentile. "Security in wireless sensor networks: A cryptography performance analysis at mac layer." Future Internet 14, no. 5 (2022): 145.
[20]. Xia, Zhengxin, Zhe Wei, and Huan Zhang. "Review on Security Issues and Applications of Trust Mechanism in Wireless Sensor Networks." Computational Intelligence and Neuroscience 2022 (2022).
[21]. Barati, Hamid. "A hierarchical key management method for wireless sensor networks." Microprocessors and Microsystems 90 (2022): 104489.
[22]. Tyagi, Lalit Kumar, Anoop Kumar, C. K. Jha, Ashok Kumar Rai, and Vipul Narayan. "Energy Efficient Routing Protocol Using Next Cluster Head Selection Process in Two-Level Hierarchy for Wireless Sensor Network." Journal of Pharmaceutical Negative Results (2022): 4772-4783.

BIOGRAPHIES OF AUTHORS

	**Vishal More** DOB:22.10.1982. Completed B.E from SRTU Nanded in 2006, and M.tech from RVC Bangalore in 2009, currently working as a assistant professor in the department of CSE BKIT, Bhalki since from april 2009. Email: vishal.more1@gmail.com
	**Dr. B. Suryakanth Chandrappa** DOB:01.04.1965Experienced Professor with a demonstrated history of working in the higher education industry. Strong education professional with a Doctor of Philosophy - PhD focused in Microwave communication (Microstrip Antenna) . Working as Professor in ECE Department BKIT, Bhalki, affiliated to VTU, Belagavi. Email: bsuryakanth3413@gmail.com