Study and Analysis of major security attacks in WSN

A Comparative Study

Thesis submitted in partial fulfillment of requirements

for the degree of

Master of Technology in Computer Technology

of

Computer Science and Engineering Department

of

Jadavpur University

by

Prabuddha Das

Registration No. - 154190 of 2020 - 2021

Examination Roll No. -M6TCT23020

under the supervision of

Prof. (Dr.) Sarmistha Neogy

Department of Computer Science and Engineering

Jadavpur University

Kolkata, West Bengal, India

2023

Certificate from the Supervisor

This is to certify that the work embodied in this thesis entitled "**Study and Analysis of major security attacks in WSN** " has been satisfactorily completed by Prabuddha Das (Registration Number 154190 of 2020−2021; Class Roll No. 002010504025; Examination Roll No- **M6TCT23020** It is a bona-fide piece of work carried out under my supervision and guidance at Jadavpur University, Kolkata for partial fulfillment of the requirements for the awarding of the Master of Technology in Computer Technology degree of the Department of Computer Science and Engineering, Faculty of Engineering and Technology, Jadavpur University, during the academic year 2022 − 23.

……

Prof. (Dr.) Sarmistha Neogy,

Department of Computer Science and Engineering,
Jadavpur University.
(Supervisor)

Forwarded By:

Prof. Nandini Mukherjee
Head,
Department of Computer Science and Engineering,
Jadavpur University

……..

Prof. Saswati Mazumdar
DEAN,
Faculty of Engineering & Technology,
Jadavpur University

Department of Computer Science and Engineering

Faculty of Engineering And Technology

Jadavpur University, Kolkata - 700 032

Certificate of Approval

This is to certify that the thesis entitled "**Study and Analysis of major security attacks in WSN** " is a bona-fide record of work carried out by Prabuddha Das (Registration Number 154190 of 2020 − 2021; Class Roll No. 002010504025; Examination Roll No. M6TCT23020 in partial fulfillment of the requirements for the award of the degree of Master of Technology in Computer Technology in the Department of Computer Science and Engineering, Jadavpur University, during the period of September 2022 to June 2023. It is understood that by this approval, the undersigned do not necessarily endorse or approve any statement made, opinion expressed or conclusion drawn therein but approve the thesis only for the purpose of which it has been submitted.

Examiners:

……
(Signature of The Examiner)

Department of Computer Science and Engineering

Faculty of Engineering And Technology

Jadavpur University, Kolkata - 700 032

Declaration of Originality and Compliance of Academic Ethics

I hereby declare that the thesis entitled "**Study and Analysis of major security attacks in WSN**" contains literature survey and original research work by the undersigned candidate, as a part of his degree of Master of Technology in Computer Technology in the Department of Computer Science and Engineering, Jadavpur University. All information has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all materials and results that are not original to this work.

Name: Prabuddha Das

Examination Roll No.: ……

Registration No.: 154190 of 2020 − 2021

Thesis Title:

Signature of the Candidate

Table of Contents

List of Figures **6**
List of Tables **7**
Chapter Ⅰ: Introduction **8**
Ⅰ. A. The Sensor Node in WSN 10
Ⅰ. B. Characteristics of Wireless Sensor Networks 11
Ⅰ. C. Routing Challenges in WSN 12
Ⅰ. D. Organisation of the Thesis 12
Chapter Ⅱ: SECURITY IN WSN **12**
Ⅱ A. Security challenges in WSN 13
Ⅱ B. Classification of attacks at different layers 13
Ⅱ C. Security Measures in WSN 16
Chapter Ⅲ: Sybil Attack **16**
Ⅲ A. Literature Review 17
Ⅲ B. Methods to Detect and Prevent Sybil Attack 17
Ⅲ C. Protocols Affected by Sybil Attack 19
Ⅲ D. OTHER COUNTERMEASURES AGAINST SYBIL ATTACK 20
Chapter Ⅳ: Wormhole Attack: **22**
Ⅳ A.MODES OF WORMHOLE ATTACK 23
A. Packet encapsulation 23
B. Packet relay 24
C. Out-of-band channel 25
D. Protocol distortion 25
Ⅳ B. Literature Review: 26
Ⅳ C. Other COUNTERMEASURES AGAINST WORMHOLE Attacks 27
A. Location and Time based Approaches 27
B. Connectivity and Neighborhood Approaches 28
C. Graphical and Topological Information based Approaches 28
Chapter Ⅴ: Sinkhole Attack **29**
Ⅴ A. Literature Review 30
Ⅴ B. SURVEY ON VARIOUS METHODS for SINKHOLE ATTACK 31
A. Hop count based detection 31
B. Agent based detection 32
C. Cryptography based detection 33
D. Sequence number-based detection 33
Chapter Ⅵ: Conclusion and Future Scope of Work **35**
References **36**

List of Figures

Fig 1 Various Attacks in WSN ……8
Fig 2 Applications of WSN ……9
Fig 3 Components of the sensor node……10
Fig 4 Classification of attack at different layers ……12
Fig 5 Sybil Attack ……14
Fig 6 Wormhole Attack……14
Fig 7 Sybil Attack ……16
Fig 8 Countermeasures Against Sybil Attack……...20
Fig 9 Wormhole Attack……22
Fig 10 Modes of Wormhole Attack……...23
Fig 11 Sinkhole Attack……..29

List of Tables

Table 1 Methods to tackle Sybil Attacks in WSN……...18
Table 2 Protocols affected by Sybil Attacks……19
Table 3 Merits And Demerits of Defensive Techniques Against Sybil Attacks……. 21
Table 4 Different Techniques to tackle Wormhole attacks in WSN……26
Table 5 Merits and Demerits of Defensive Techniques Against WORMHOLE Attack…… 28
Table 6 Algorithms to detect sinkhole attacks in WSN…….. 33

Chapter Ⅰ: Introduction

Wireless Sensor Networks (WSNs) are networks consisting of a large number of small, low-power, and interconnected sensor nodes that collaborate to monitor and gather data from the environment. These sensor nodes can be equipped with various types of sensors to measure physical phenomena such as temperature, humidity, light, sound, motion, and more. The data collected by these nodes is then processed, aggregated, and transmitted to a central node (often called a base station or gateway) for further analysis.

During the past few years, there has been a rapidly increasing demand for wireless communication services and infrastructure. These wireless devices are reported to be susceptible to cybercriminal activities, including data forging, computer hacking, malicious attacks, and information theft and so on. Hence improvement of security in wireless communications is of utmost importance. WSNs are deployed in hostile and unattended environments.

WSN is usually deployed in a remote and unprotected area to perform monitoring and reporting tasks. Therefore, they face a higher risk of security vulnerabilities. If any of the nodes are attacked, their sensitive data and security parameters will be forged by the adversary. The adversary will launch different attacks according to the situation, such as Sybil attack, wormhole attack, Hello flood, Sinkhole shown in figure 1.

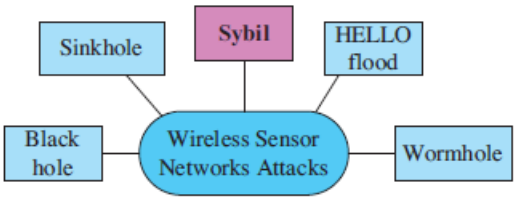

Figure 1. Various attacks in WSN.

Using the WSNs in the severe environmental monitoring work becomes a valuable research topic. And there exists lots of research about this topic.

Wireless sensor networks (WSNs) have a wide range of applications in a variety of industries and fields. Some of the most common applications of WSNs include:

- **Environmental monitoring:** WSNs can be used to monitor environmental conditions such as temperature, humidity, air quality, and soil moisture. This data can be used to track changes in the environment and to identify potential problems.
- **Home automation:** WSNs can be used to control and monitor home appliances, such as lights, thermostats, and security systems. This can help to make homes more energy-efficient and secure.
- **Industrial automation:** WSNs can be used to monitor and control industrial processes, such as manufacturing and transportation. This can help to improve efficiency and safety.
- **Military applications:** WSNs can be used for surveillance, reconnaissance, and target tracking. This can help to improve situational awareness and to make military operations more effective.
- **Agriculture:** WSNs can be used to monitor crop conditions and to manage irrigation systems. This can help to improve crop yields and reduce costs.

- **Healthcare:** WSNs can be used to monitor patients' vital signs and to collect data on their health. This data can be used to improve patient care and to prevent disease.

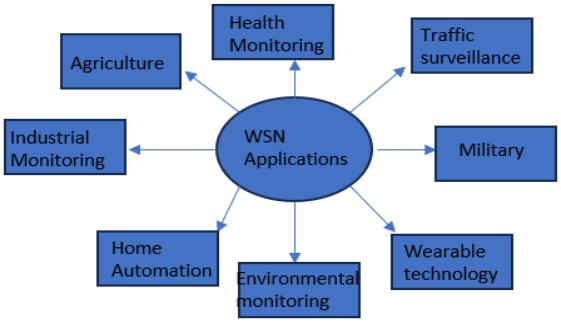

Fig 2: Applications of WSN

Ad hoc networks and wireless sensor networks differ from each other as ad hoc networks do not require any kind of infrastructure support. Sensor nodes (SNs) in WSNs have limited memory, battery supply, bandwidth and computation capability. These SNs are deployed densely in thousands of numbers. The WSNs topology changes frequently because of node mobility, joining or failure. This makes the SNs to be compromised easily by an adversary.

We propose that security design should consider the target to be secured as a whole, and not be done layer by layer. Each layer might have a different requirement as well as available resources. The lower layers are usually too weak to support any security mechanism, and therefore it might be better to delegate the problem to the higher layer with the more powerful device.

In WSN there are two pairs of addresses, the MAC address and the network address. There are two MAC addresses, the 64 bits one that is assigned by the manufacturer and the 16 bits one that is only used locally.

Routes in the WSN network are discovered by on-demand methods (e.g. AODV). A source node will broadcast a route discovery message (RREQ) containing the 16 bit destination node. Each node that receives this broadcast should forward it to every other node within its listening range. Eventually the destination will receive copies of the broadcast message through different paths and a route reply (RREP) will be sent back to the source. This route must be maintained all the time, and broken path can be taken out by sending RERR (route error) messages

Ⅰ. A. The Sensor Node in WSN

A sensor node is a small device also called a mote which has a micro sensor technology and is able to perform sensing, processing and communicating with other nodes. The sensor node consists of the components as shown in Fig.a sensor, a processor, a radio transceiver and a power supply/battery.

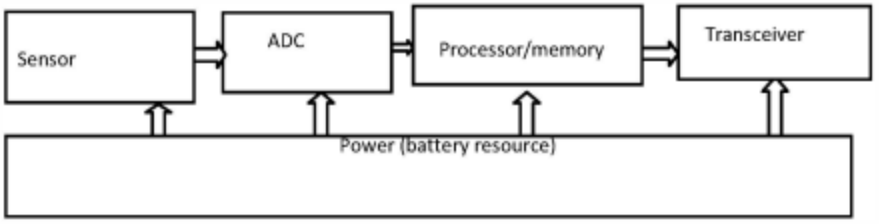

Fig 3: Components of the sensor node

- **Sensors:** Sensor nodes can have one or more sensors that can measure a variety of physical quantities, such as temperature, humidity, pressure, light, sound, and motion.
- **Microcontroller (ADC+Processor/Memory):** The microcontroller is the brain of the sensor node. It is responsible for processing the data from the sensors and communicating with other sensor nodes.
- **Radio transceiver:** The radio transceiver allows the sensor node to communicate with other sensor nodes and with a base station.
- **Power source:** Sensor nodes are typically battery-powered, so it is important to minimise power consumption.

Sensor nodes are used in a wide variety of WSN applications, such as:

- Environmental monitoring: Sensor nodes can be used to monitor environmental conditions such as temperature, humidity, air quality, and soil moisture.
- Home automation: Sensor nodes can be used to control and monitor home appliances, such as lights, thermostats, and security systems.
- Industrial automation: Sensor nodes can be used to monitor and control industrial processes, such as manufacturing and transportation.
- Military applications: Sensor nodes can be used for surveillance, reconnaissance, and target tracking.

Sensor nodes are a key component of WSNs. They provide the ability to collect data from remote and difficult-to-reach places. Sensor nodes are also relatively inexpensive and easy to deploy, which makes them ideal for a wide range of applications.

Here are some of the key challenges in designing and implementing sensor nodes:

- Power consumption: Sensor nodes are typically battery-powered, so it is important to minimise power consumption.
- Cost: Sensor nodes should be relatively inexpensive to manufacture and deploy.
- Size and weight: Sensor nodes should be small and lightweight so that they can be easily deployed in remote and difficult-to-reach places.
- Reliability: Sensor nodes should be reliable and able to operate in harsh environments.
- Security: Sensor nodes should be secure from attack.

Ⅰ. B. Characteristics of Wireless Sensor Networks

The various characteristics of WSN are as following:
• Sensor nodes are small devices having limited amounts of energy resources.
• Nodes have the risk of dying as they are energy starved devices and other environmental factors.
• There is a continuous change in the structure of the network.
• Nodes in WSN' s are not only in large amounts but also they are heterogeneous in nature in terms of memory, computation power etc.
• Due to unbound delays, there is a possibility of communication failures in these networks.

Ⅰ. C. Routing Challenges in WSN

Routing is described as the process to determine the best path to forward the data from source to destination. Routing mechanisms are very different in wireless sensor networks as compared to traditional approaches as these networks are infrastructure less networks, unreliable and energy constrained networks. There are different routing protocols including proactive, reactive, hybrid, location based and hierarchical. There are many issues which affect the design of routing protocols

- **Energy Considerations:** Energy considerations play an important role in setting up a route.
- **Data Aggregation:** Redundant data from multiple nodes must be aggregated at some point to reduce the transmissions.
- **Node capabilities:** Routing is also dependent upon the functionality of different nodes as nodes having higher functionality can lose energy early than the nodes just performing the tasks of sensing.
- **Data Delivery Models:** Routing depends upon the data delivery models with regards to route stability as in continuous model nodes send the data periodically and in case of data driven or query driven nodes send the data when some event occurs or sink node queries.
- **Node Deployment:** Routing protocol is greatly affected by how the deployment has taken place. It can be deterministic or self configurable. In case of deterministic, nodes are deployed manually and data is routed as per the predefined route and in case of self configurable network nodes are placed in ad hoc fashion, therefore selecting the efficient cluster head for route selection is a major issue in this mechanism.
- **Network Dynamics:** Routing is also affected by the factor of whether the nodes are mobile or static in nature.

Ⅰ. D. Organisation of the Thesis

This thesis deals with majorly three major attacks in Wireless Sensor Networks

1. Sybil Attack
2. Wormhole Attack
3. Sinkhole Attack

This thesis has been divided mainly into **six** chapters- beginning with the general introduction of WSNs, its characteristics, and routing challenges. **Chapter two** deals with Security in WSN, its various classification, security measures and challenges. The **third chapter** describes Sybil Attack in detail, its methods to detect and the routing protocols it affects and its critical analysis. **Chapter four** deals with Wormhole attacks, its mitigation strategies, modes and countermeasures. **Chapter five** deals with Sinkhole attacks, its survey on various methods to detect the attack and strategies to tackle it. Conclusion and future scope of the thesis is discussed in **Chapter six**.

Chapter Ⅱ: SECURITY IN WSN

Due to various resource and physical limitations including unreliable communication, collisions, latency and unattended after deployment and management by remote users, make these networks vulnerable to attacks.

Ⅱ A. Security challenges in WSN

The characteristics of the WSN that make them vulnerable to various types of attacks are discussed.

- Radio frequency: As WSN' s are configured with the radio interface at the same frequency band which makes the network open to all to attack.
- Standard routing protocols: Due to standardization of routing protocols, these protocols are known publicly. Therefore, the attacker can breach the security holes of these protocols.
- Infrastructure less networks: Due to its infrastructure less nature, it is not possible to have a continuous check on the network after deployment.
- Energy limitations: As WSN' s have starved from resources it is very difficult to have algorithms with much security required by stronger security protocols.
- Low cost networks: As WSN' s targets low cost, therefore it is unlikely to have tamper resistant hardware in these networks which leads to physical capturing of nodes.
- No security mechanisms: Most of the security mechanisms including frequency spread spectrum, anti-jamming and asymmetric cryptography are not used in these networks because of greater design

Ⅱ B. Classification of attacks at different layers

The attacks are classified on the basis of the layering model of Open System Interconnect (OSI).The classification of attacks at different layers:

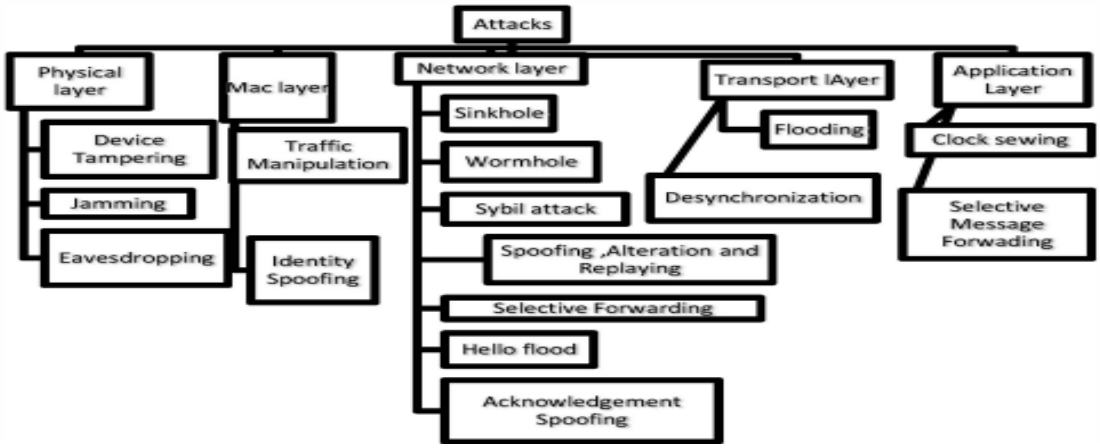

Fig 4: Classification of attack at different layers

Physical layer:

At this layer, attackers can perform non technical attacks including destroying sensor nodes and technical attacks including wiretapping etc. The various types of attacks at this layer are as follows:

- Device Tampering: Attack of this type includes the damaging of sensor nodes and their modification or by capturing the sensor nodes physically and then retrieving the confidential information.
- Eavesdropping: Eavesdropping refers to monitoring the network traffic on the communication channels without the knowledge of the sending and receiving party.
- Jamming: These types of attacks are performed by deploying a large number of nodes which can cause intense noise in the network and occupying the network channels making the transmission media unavailable for the other nodes.

MAC layer:

At this layer the attacker tries to disrupt the various coordination rules and produces the harmful traffic. They also try to spoof the identities at the MAC layer.

- Traffic Manipulation: Attackers try to produce the data traffic simultaneously with the legitimate users transmitted by monitoring the channel and performing various computations on protocols used at MAC layer so that collisions of the packets may take place which may degrade the network performance.
- Identity Spoofing: Attackers try to spoof the MAC identities and pretend them to be the legitimate users.

Network layer:

At this layer the attacker tries to manipulate routing information and then redirects the traffic and misleads the routing by providing false information.

- **Spoofing, Alteration and replaying the routing information:** The most common type attack on routing protocol is to manipulate the routing information which is exchanged between the sensor nodes. Attackers try to redirect the network traffic, create routing loops, replay the messages and produce the latency in the network.
- **Selective Forwarding Attacks:** In this type of attack the adversary node may deny to forward the packets or simply drops the packets. These types of attacks are more dangerous in case when the adversary node selectively forwards the packet .
- **Sinkhole Attacks:** Attackers main goal is to accomplish these types of attacks is to lure the traffic from the nodes of some particular region through a particular node called a sink node by broadcasting the message that this is the only high quality route.
- **Sybil Attack:** This is the type of attack in which a malicious node tries to have multiple identities at different locations. The Sybil attack greatly affects the techniques that provide fault tolerance in these networks including distributed storage [3], maintenance of topology [4] etc. Geographic routing protocols and location aware routing protocols are greatly affected by these attacks. Figure 3 depicts how a malicious node 'm' having similar identities representing the fake high quality route.
- **Wormhole attacks:** In this type of attack two or more nodes cooperate with each other to form a link which is a shortcut and having lower latency, basically they form a tunnel and tries to influence the nodes which are close to these tunneled nodes that these two far distant points are

very close to each other. Figure depicts the wormhole tunnel formed by two nodes 's' (source) and 'd' (destination) and all the data is then passed through this tunnel.

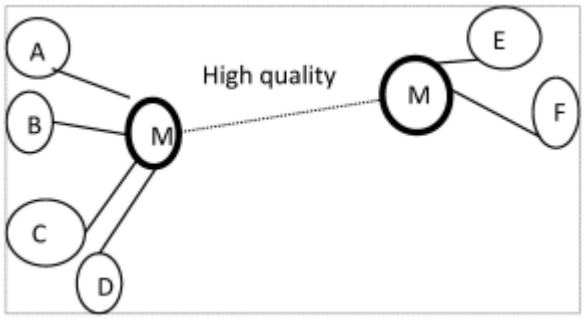

Fig 5: Sybil Attack

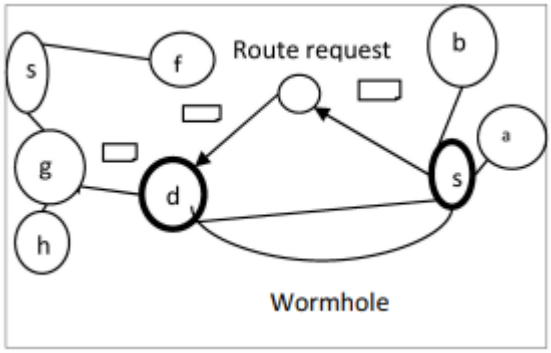

Fig 6: Wormhole Attack

- **Hello Flood attack:** Some protocols use hello packets to broadcast about themselves to their neighbors and the neighbor who receives that packet feels that it is in the range of sender [5]. The attacker may use a high energy device and influence the nodes to feel as if they all are its neighbor and attempt to use that path only.

- **Acknowledgement spoofing:** Some protocols are based on acknowledgment signals for reliability concern but attackers can spoof the acknowledgements and may influence the sending node that a weak link is strong and dead node is alive Therefore, legitimate users are not able to have the connection.
- **De-synchronization:** Here, attackers will try to waste energy by making end hosts indulge in recovering the errors which do not really exist.

Application Layer:

At this layer the attacker tries to modify the data and thus provides the wrong information to the applications.

- Clock sewing attack: These attacks are accomplished by spreading the wrong information about timing information to the sensor nodes which requires operations in synchronization.
- Selective message forwarding attack: To perform these types of attacks the attacker must understand the semantics of every unit of the message and then he forwards the messages

according to the semantics of the message only.
- Data aggregation distortion: This attack occurs when the attacker tries to modify the data collected by the sink node or by the aggregated point.

Ⅱ C. Security Measures in WSN

To protect WSNs from attack, a variety of security measures can be implemented. These measures include:

- **Authentication:** Sensor nodes can be authenticated to ensure that they are legitimate.
- **Encryption:** Data can be encrypted to prevent eavesdropping and data modification.
- **Access control:** Access to sensitive data can be restricted to authorized nodes.
- **Intrusion detection and prevention systems:** Intrusion detection systems can be used to monitor the network for suspicious activity, and intrusion prevention systems can be used to block attacks.

Researchers and engineers are constantly developing new security measures to protect WSNs from attack. However, security remains a major challenge for WSNs, and it is important to carefully consider security when designing and deploying WSNs.

Here are some specific examples of security measures that can be implemented in WSNs:

- **Symmetric key cryptography:** Symmetric key cryptography can be used to encrypt data between sensor nodes. Symmetric key cryptography is relatively efficient and easy to implement on sensor nodes.
- **Public key cryptography:** Public key cryptography can be used to authenticate sensor nodes and to establish secure communication channels. Public key cryptography is more computationally expensive than symmetric key cryptography, but it is more secure.
- **Message authentication codes (MACs):** MACs can be used to verify the authenticity of messages. MACs are relatively efficient and easy to implement on sensor nodes.
- **Routing protocols with security features:** Routing protocols can be designed with security features, such as authentication and encryption. This can help to protect the network from eavesdropping and data modification.
- **Intrusion detection systems:** Intrusion detection systems can be used to monitor the network for suspicious activity. This can help to identify and block attacks before they cause damage.

By implementing appropriate security measures, WSNs can be made more secure and resistant to attack.

Chapter Ⅲ: Sybil Attack

Ⅲ A. Literature Review

Sybil attack is a type of security threat. A threat is a set of circumstances that has the potential to cause loss or harm. It is one of the primary attacks that would facilitate the onset of many different attacks in the network. This type of attack may reduce the effectiveness of fault-tolerant schemes and pose a threat to geographic routing protocols. The Sybil attacker captures a legal node or inserts an illegal node in the network. This malicious node propagates several identifiers. The Sybil attacker forges fake identifiers or duplicates existing node identifiers in different areas of the network. Hence, a malicious node attracts a heavy and considerably disrupts routing protocols. It disturbs operations such as data aggregation, voting and reputation evaluation. A malicious node which enters the network with multiple IDs.

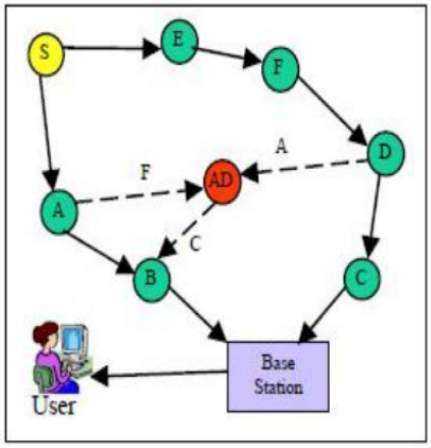

Fig 7: Sybil Attack

Fig 7 demonstrates Sybil attack in which node ‘AD’ is an adversary node, which presents multiple identities. ‘AD’ appears node ‘F’ for ‘A’, node ‘A’ for ‘D’ and node ‘C’ for ‘B’ so when node ‘B’ wants to communicate with ‘C’ it sends the message to ‘AD’. Normal functioning of the network can be disturbed by a Sybil attack.

Ⅲ B. Methods to Detect and Prevent Sybil Attack

In [1] Random Password Comparison (RPC) method is proposed to prevent Sybil attack. This method provides a facility to deploy and control the position of nodes. The algorithm generates a routing table in which the information of each node’s id, the time and a password is stored. The intermediate nodes between source and destination are identified. The intermediate node’s information is then compared with the RPC database. If the information matches then the node is considered as normal node otherwise it is considered as Sybil node. Every few seconds a random password generator generates a new password for each node and sends it to all nodes in the network. While the destination node is communicating with the source node, the destination node’s id, time delay and the random password corresponding to time delay are compared with the RPC database. If the information is matched, the source node will communicate otherwise the destination node will be considered as Sybil node. The method is dynamic and accurate. It improves data transmission in the network and also increase throughput. RPC provides more prevention than detection.

The authors have proposed a combined Compare and Match-Position Verification Method (CAM-PVM) with Message Authentication and Passing (MAP) in [2]. CAM-PVM detects and eliminates the Sybil

nodes entry in the network. To prevent the Sybil activity MAP algorithm is applied along with CAM-PVM. Base Station (BS) sends a HELLO message to each node in the network with a node creation time. This information is stored in an iNODEINFO table. For data transmission from source (S) to destination (D), it is necessary to discover the route from S to D through an N-hop intermediate node. During this process, current information of the intermediate nodes (ID, timestamp) is stored in an iROUTING table. At the time of data transmission, the iROUTING table entries are compared with the entries in the iNODEINFO table, which helps to identify the duplicate nodes with id, timestamp and the location. CAM-PVM is time consuming and cost effective. So that to prevent Sybil activity MAP algorithm is applied along with CAM-PVM. In MAP each node communicates by passing the authentication message. MAP is an effective and time consuming method.

The authors in [3] have proposed a mutual Relate and Identity Tactic (RAI) and Location Verification Technique (LVT) to prevent Sybil attack. In RAI, BS dynamically provides key value to each system in the network. When systems start interconnecting and sharing the data, each system provides their keys. If the key is not matched with the key agreed by the BS, that system is concluded as Sybil node. In LVT, the Sybil system is identified by verifying the location of the nodes. Sometimes RAI technique fails to detect the Sybil node then the further detection is carried out by LVT technique. RAI and LVT techniques can solve the Sybil attack up to 88% in the WSN.

In [4] a Rule based Anomaly Detection System (RADS) is presented. In large scale WSNs RADS monitors and timely detects Sybil attacks. The system depends on an Ultra-Wideband (UWB) ranging based detection algorithm. The system requires no cooperation or information sharing between sensor nodes. Each node operates as an independent Anomaly based detection system (ADS) and it is responsible for detecting attacks only for itself. In rule-based detection, predefined rules are used by anomaly detectors to classify data points as anomalies or normalities. If the rules defining an anomaly are satisfied then an anomaly is declared. There are various limitations of the system, viz. The system is not compatible with old fashioned WSNs, it works on a stationary network, and Indirect Sybil attacks are not detected by the system. On the other hand, there are multiple advantages of the system, viz. RADS does not require cryptography methods, certification protocols and third-party trusted authorities, High detection accuracy and low false alarm rate are achieved by the system.

In [5] a scheme is proposed which uses the Received Signal Strength (RSS) to identify the difference between legitimate nodes and Sybil nodes. The scheme identifies Sybil identities without using third parties. Each node of the sensor network captures and stores the signal strength of the transmissions sent by the neighbouring nodes. Smallest readable RSS value is called the threshold value. When new node enters into the network and if RSS of that node is greater than the threshold, it indicates abnormal entry into the neighbourhood. In this case the identities of both nodes are checked. If it is the same then the RSS value for both nodes is checked. If it is greater than or equal to the threshold, it indicates the new node as Sybil node. High true positive, very little false positive, high level of accuracy are the advantages of the scheme.

The authors in [6] have proposed an RFID based system to prevent Sybil attack in Military Wireless Sensor Networks (MWSNs). Two types of authentication techniques are used. In the first technique RFID tags are embedded in soldiers to authenticate them and get certificates. In second technique certificates are used by soldiers to authenticate them to their neighbours. If the soldiers have two valid certificates at the same time, the Sybil attack is detected by the leaders of groups of soldiers.

Table 1: Methods to tackle Sybil Attacks in WSN

Method	Parameters	Advantages	Limitations
RPC (Random Password Combination)	Delay Time, Energy, Throughput	• Dynamic and Accurate • Improves data transmission • Increase Throughput	• Low True Positive Rate • No route repair mechanism in case of route failure • Only uses neighbor analysis to identify the node
CAM-PVM with MAP (Compare and Match-Position Verification Method with Message Authentication & Passing)	Delay time, Throughput	• CAM-PVM detects and eliminates Sybil activity. • MAP prevents Sybil activity • MAP is effective method	• Time Consuming, • Costly
RAI-LVT(Relate & Identity Tactic with Local verification Technique		• Solves Sybil Attack up to 88%	• Time Consuming
RADS-UWB (Rule based anomaly detection system on an Ultra Wide Band)	False Positive Rate	• No cryptography methods, certification protocols and third-party trusted authorities. • Communication Minimum overhead between sensor nodes • Cost-effective • No high-cost hardware • No additional base stations • high detection accuracy • Low false positive rate	• Lack of compliance with old-fashioned WSNs. • Focuses on stationary networks. • No detection of indirect Sybil attacks
RSS (Received Signal Strength)	Delay, Throughput, TPR, FPR, Packet Loss Ratio	• No centralized trusted third party • High level of accuracy • High true positive rate	• Low false positive rate • Scope: Still can be improved
RFID		• Prevents attacker from tracking the mobility of soldiers • Privacy preservation of communicating components is also taken care	• More Communication Overhead

Ⅲ C. Protocols Affected by Sybil Attack

In [7] the authors have proposed Geographical and Energy Aware Routing (GEAR) protocol. To route a packet toward the target region GEAR algorithm uses energy aware neighbor selection; i.e. it forwards the packet to the nearest neighbor to destination when at least one closer neighbor to the destination exists. When all nodes are further away; GEAR picks a next hop node that minimizes the cost value. GEAR makes forwarding decisions only based on local knowledge. To spread the packet inside the destination region Recursive Geographic forwarding or Restricted Flooding is used. There are various limitations of the GEAR [8]; viz., periodic table exchange, limited mobility and limited scalability. GEAR follows a demand driven data delivery model [9]. It faces a problem of high overhead which affects the energy efficiency [9]. On the other hand, GEAR tries to balance energy consumption and increase network lifetime.

The author in [9] has discussed Geographic Adaptive Fidelity (GAF) protocol. GAF is an energy aware location-based routing algorithm. In the GAF algorithm the entire area is divided into several square grids. GPS indicated location is used by the node to associate itself with a point in the virtual grid. It follows a virtual grid data delivery model. In each zone one node acts as master. It stays awake for a certain amount of time and is responsible for monitoring and reporting data to the sink. Other nodes in the zone can go to sleep to save energy. So the routing accuracy is not disturbed. GAF is highly scalable. GAF faces a problem of high overhead which affects the energy efficiency.

In [10] the author has discussed Greedy Perimeter Stateless Routing (GPSR) protocol. GPSR uses two phases to forward the message; greedy forwarding and face routing. In greedy forwarding each node forwards the packet to the node closest to the destination. When the closest node is found, greedy forwarding stops. This dead end is called local minima, local maxima, hole or void. When the message reaches local minima, GPSR enters into face routing or perimeter forwarding mode. Faces are the contiguous polygonal regions separated by the edges of a planar graph. Planar graph is one in which no two edges cross each other. Face routing uses two principles; the right hand rule and face change. The right hand rule moves around a face in a clockwise direction. GPSR keeps track of the points where it crosses the line which connects source S and destination D. After routing the face completely, the algorithm comes to the intersection point which is closest to the destination. The algorithm then proceeds to the next face closer to D and the same steps are repeated until it reaches the face which contains the destination. Face routing guarantees message delivery to the destination.

Table 2: Protocols Affected by Sybil Attack

Protocol	Advantages	Limitations
GEAR (Geographical and Energy Aware Routing)	• Does not use greedy algorithms to forward the packet to the destination • Balance energy consumption • Increases network lifetime	• Periodic Table exchange • No QoS • Limited Scalability • Limited Mobility • Frequent Update Messages
GPSR (Greedy Perimeter Stateless Routing)	• Performs better in case of defense techniques and sparse networks • Use piggybacking to receive updates • No extra overhead	• Not good for uniforms traffic pair • Not good for uneven traffic distribution
GAF (Geographic Adaptive Fidelity)	Highly scalable	• High overhead • No QoS

Ⅲ D. OTHER COUNTERMEASURES AGAINST SYBIL ATTACK

There are many notable techniques to defeat the Sybil attack in WSN.

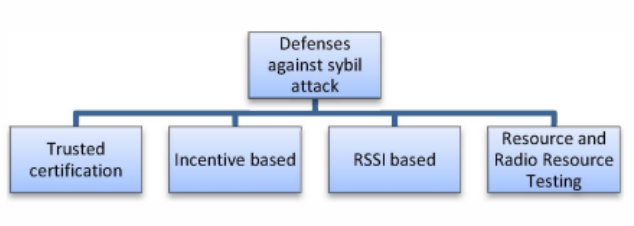

Fig 8: Countermeasures against Sybil Attack

A. Trusted Certification

Douceur [11] has proven that certification is one of the most widely used mechanisms to defeat Sybil Attack. There is a centralized CA certification authority responsible for validating the one to one correspondence between an entity and its identity. The certificate authority validates the entities by providing them with digital signatures or with some special type of hardware. The authentication usually takes place by asymmetric key cryptography having more computational overhead. There is a lot of cost applicable when these types of mechanisms are applied on large scale systems.

B. Resource Testing and Radio Resource Testing

Newsome has proposed a Resource Testing scheme where a verifier calculates the resources (energy, storage capacity, etc.) of identity, if there is the node having much more resources as compared to resource starved node then it is considered to be the attacker node. However, these verification messages may flood the network therefore these schemes are not successful. Newsome et al. has proposed the scheme 'radio resource testing' which is an extension to resource testing where every node has one radio and can transmit and receive only one channel at a time. Consider the example, where a node wants to verify about its neighbor nodes that whether they are Sybil nodes or not then the node will assign 'm' different channels to 'm' nodes and then will randomly choose the channel to hear the message and if the neighbor is legitimate then verifier will be able to listen the message. If there are' Sybil nodes then the probability to detect them is s/n.

C. Incentive-based detection

Margolin et al propose a protocol in [12] called Informant that is based on a reward scheme where economic incentives are used and it has a wide range of application areas. An entity i.e the monitor nodes rewards. The protocol offers the reward to the adversary if it reveals the entities controlled by it. An identity tells about the name of the target peer when it receives the payment in exchange.

D. RSSI (Radio Resource Strength Signaling) based scheme

Demirbas et al [13] proposed this scheme to detect Sybil attacks. This is one of the most robust schemes able to detect these attacks with accuracy. This is based on received signal strength of messages. The cooperation of one additional node and a communication message make this scheme successful but it is an unreliable scheme, generating false positive alarms as the radio signals are non isotropic i.e. not uniform. This basic strategy involved in this scheme is that the detector node receives the RSSI value from each node and its identity. Here in this case detector nodes 'd' and Sybil nodes with IDs i and j are shown. Let R_i be the value of the signal strength received from node i, the detector node starts computing the information R_i^{d1}/R_i^{d2} , $R^{d1}{}_i/R_i^{d3}$, R_i^{d1}/R_i^{d4} at time 't' and similarly computes the value for another node j, R_j^{d1}/R_j^{d2}, R_j^{d1}/R_j^{d3}, R_j^{d1}/R_j^{d3} and if the two values are same then these nodes are considered to be the Sybil node.

TABLE 3. Merits And Demerits of Defensive Techniques Against Sybil Attacks

Techniques	**Methodology**	**Merits**	**Demerits**
Trusted Certification	Based on certificate authority	No resource Overhead	Expensive when applicable to large scale networks
Resource and radio resource testing	Based on calculation of residual resources	No bandwidth overhead	Minimal defense provided and cannot thwart Sybil attacks completely
Incentive Based	Based on rewards	No special hardware and clock synchronisation	May encourage Sybil Attackers to have economic benefits in order to receive economic benefits in return
Radio Resource strength Signalling	Based on radio signal strength	Robust technique, few false positive results	Not reliable

Chapter Ⅳ: Wormhole Attack:

A wormhole attack is a sophisticated form of network-layer attack that can compromise the security and integrity of wireless communication protocols in various types of networks, including ad hoc and sensor networks. In this type of attack, malicious nodes create a virtual tunnel or shortcut between two distant locations within the network. This tunnel enables data packets to be transmitted between these two points much more quickly than they would through normal network routes.

The key characteristic of a wormhole attack is that it bypasses the regular network routing mechanisms, allowing an attacker to potentially eavesdrop on, modify, or disrupt communication between nodes that are not in direct communication range of each other. The malicious nodes at the ends of the wormhole tunnel can collude to exchange data quickly and without the knowledge of other nodes in the network, leading to potential security breaches and the compromise of network protocols.

Wormhole attacks can have severe consequences, such as undermining network security mechanisms like authentication and encryption, disrupting network connectivity, and causing data integrity violations. Detecting and preventing wormhole attacks is challenging due to the hidden nature of the attack and the fact that it can exploit vulnerabilities at the network layer, which can be harder to address compared to higher-layer attacks.

To protect against manifestation of wormhole attack however the routing data is categorized, validated or scrambled. The neighbor node doesn't have to know about the routing protocol or bargain with the sensor node. Fig 2 shows the wormhole attack where A and B are the malicious node and making a tunnel by which data packets are transferred from A to B.

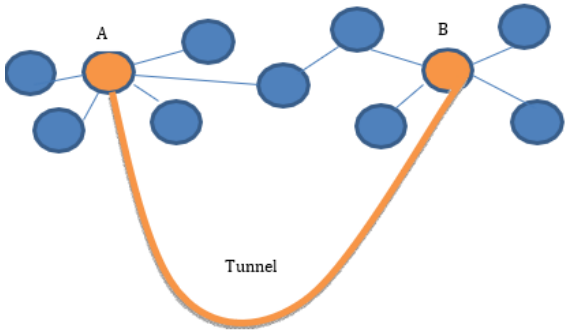

Fig 9: Wormhole Attack

Ⅳ A.Modes of Wormhole Attack

This section explains in detail about the number of ways in which wormhole attack could be performed in wireless sensor networks. There are many ways for this and some of them are discussed in this section and they are classified in fig 9.

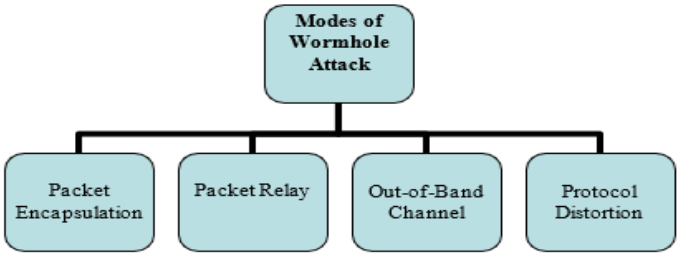

Fig 10: Modes of Wormhole Attack

A. Packet encapsulation

There are two or more than two nodes to perform packet encapsulation. Data is compressed between these malicious nodes. By doing this, it prevents hop count increments. This is the simplest mode to launch wormhole attack.The goal of packet encapsulation in wormhole attacks is to bypass security measures that are designed to prevent the forwarding of packets between malicious nodes. By encapsulating packets, the attackers can make it appear as if the packets are coming from legitimate nodes, which can trick the security measures into allowing the packets to pass through.Here is an example of how packet encapsulation can be used in a wormhole attack:

1. Node A wants to send a packet to Node C.
2. Node A encapsulates the packet inside a packet that is addressed to Node B.
3. Node A sends the encapsulated packet to Node B.
4. Node B forwards the encapsulated packet to Node C.

When Node C receives the encapsulated packet, it removes the outer packet and sees that the inner packet is addressed to it. Node C then processes the inner packet as if it had come directly from Node A.Packet encapsulation can be a very effective way to bypass security measures in WSNs. However, there are a number of techniques that can be used to detect and prevent wormhole attacks. These techniques include:

- Using hash chains to verify the authenticity of packets.
- Using routing protocols that are resistant to wormhole attacks.
- Using intrusion detection systems to monitor for suspicious traffic patterns.

B. Packet relay

In this type of mode any number of nodes, either one or many affected nodes can launch the attack. This mode of attack is referred to as “relay-based attack” in the literature. Packet relay is a technique used in wormhole attacks in wireless sensor networks (WSNs) to forward packets between two malicious nodes that are not directly connected. In a packet relay attack, the malicious nodes first capture packets from the network. They then relay these packets to each other, creating a virtual tunnel between them. This tunnel allows the attackers to forward packets between them without having to go through the rest of the network.Packet relay attacks are a more sophisticated type of wormhole attack than packet encapsulation attacks. This is because they do not require the attackers to modify the contents of the packets. Instead, they simply forward the packets as-is. This makes them more difficult to detect and prevent.

Here is an example of how packet relay can be used in a wormhole attack:

1. Node A wants to send a packet to Node C.

2. Node A captures the packet.
3. Node A relays the packet to Node B.
4. Node B relays the packet to Node C.

When Node C receives the packet, it believes that it came directly from Node A. This is because the packet has not been modified in any way.Packet relay attacks can be very difficult to detect and prevent. However, there are a number of techniques that can be used to mitigate their impact. These techniques include:

- Using time-to-live (TTL) values to limit the number of times a packet can be forwarded.
- Using routing protocols that are resistant to packet relay attacks.
- Using intrusion detection systems to monitor for suspicious traffic patterns.

C. Out-of-band channel

It needs only one affected sensor that has high transmission power which affects the packets to follow route passing from it. There are more chances to detect the presence of malicious nodes in it. Out-of-band channels can be very effective in wormhole attacks. This is because they allow the malicious nodes to communicate without being limited by the constraints of the main network channel. For example, the out-of-band channel can be used to send large amounts of data, or to send data quickly.Here is an example of how an out-of-band channel can be used in a wormhole attack:

1. The malicious nodes establish an out-of-band channel.
2. The malicious nodes use the out-of-band channel to coordinate their attack.
3. The malicious nodes use the main network channel to forward packets between them.

When the legitimate nodes in the network see the packets being forwarded, they believe that the packets are coming from the legitimate nodes that are directly connected. However, in reality, the packets are coming from the malicious nodes that are communicating over the out-of-band channel.Out-of-band channels can be very difficult to detect and prevent. This is because the malicious nodes can use a variety of methods to hide their communication. However, there are a number of techniques that can be used to mitigate the impact of out-of-band channels. These techniques include:

- Using intrusion detection systems to monitor for suspicious traffic patterns.
- Using routing protocols that are resistant to wormhole attacks.
- Using cryptography to encrypt traffic.

D. Protocol distortion

Here, an affected node attempts to invite traffic by altering the routing protocol. This mode doesn't influence the routing a lot and hence creates less harm. It is referred to as a “rushing attack” in literature. Protocol distortion can be a very effective way to launch wormhole attacks. This is because it is difficult for the legitimate nodes to detect and prevent. The malicious nodes can use a variety of methods to hide their false routing information, such as encryption or compression.Here is an example of how protocol distortion can be used in a wormhole attack:

1. The malicious nodes inject false routing information into the network.
2. The legitimate nodes update their routing tables based on the false information.
3. The malicious nodes use the updated routing tables to forward packets between them.

When the legitimate nodes see the packets being forwarded, they believe that the packets are coming from the legitimate nodes that are directly connected. However, in reality, the packets are coming from the malicious nodes that are communicating over the virtual tunnel.Protocol distortion can be very difficult to detect and prevent. However, there are a number of techniques that can be used to mitigate its impact. These techniques include:

- Using routing protocols that are resistant to protocol distortion attacks.
- Using intrusion detection systems to monitor for suspicious traffic patterns.
- Using cryptography to encrypt routing information.

IV **B. Literature Review:**

Wireless Sensor Network is a very emerging and vast area. Sensors transmit the sensed data over the network. Sybil, Sinkhole, Jamming, Wormhole are the various attacks performed in WSN. In a wormhole attack, there are pairs of malicious nodes, one node receives the data and tunnels to the other. There are various techniques for detection of wormholes and prevention of wormholes. The brief survey of such methods is presented below:

Yurong Xu et al.[14] described the distributed wormhole attack detection which is detected by distortion done by malicious nodes. It uses WGDD and width to detect distortion. This technique does not need any extra hardware and any kind of anchor node. The main benefit of the technique is that it provides the geographical detail of the sensor, which is used to counter the attack.

Parmar Amish et al [15] integrated AOMDV routing protocol with Round Trip Time (RTT). It calculates the RTT of every route of the network and calculates the threshold. Various other parameters are also calculated.

*Rajendra et al. [16]*described a detection technique for wormhole attack with high transmission power mode. RSSI has been used for detection of attacks. It uses the inbuilt circuitry within the sensor nodes. There is no need for any extra hardware for detection. This method effectively recognizes the malicious node.

Rupinder et al.[17] provided a new method named as Wormhole Resistant Hybrid Technique (WRHT). This is an optimistic attack detection technique. This is a dual attack detection technique. It ensures that no wormhole attack is untreated. The most important feature of this technique is detecting all type of attacks in the network.
Mohammad et al. [18] described a new technique that uses artificial neural networks for wireless sensor networks. This is the best technique for a uniform distributed network, but the main objective of this technique is to find a wormhole in a constant and variant environment. This technique also has less computation overhead. The main objective of this technique is to detect wormhole attack in any distribution

Table 4: Different Techniques to tackle Wormhole attacks in WSN

Author	Technique	Description	Advantage	Disadvantage	Remarks
Yurong Xu et al.	WGDD	This algorithm spots wormhole attacks by hop counting process.	It detects wormhole attack in any type irregular network. Accuracy is very high in this technique. Less error detection gauges the estimated area of wormhole attack.	Slower than the three hop degrees.	For large number of nodes, detection rate of the wormhole attack is 100% and for shorter wormholes are 80%.
Yih-Chun et al.	Packet leashes	This detection algorithm joins two kinds of packet leashes, one is temporal and other one is geographical with TIK protocol.	Large and lengthy computation is low, use of TIK protocol. Outcome of this is s instant confirmation of received data packets.	This technique only works in wireless data transfer. For temporal: clock strongly in-time. For geographical: nodes should be aware of location.	Transmission range reduced to 6.2m for the geographical leash.
Parmar et al.	Ad-hoc on demand multipath distance vector (AOMDV)	It uses Round Trip Time (RTT) to spot wormhole attack.	It provides less computational overheads on the system.	It pre-assumes that the sensor node is static and does not think about the dynamic node.	The throughput is 286.4 bits/second for usually 45 nodes end to end is 80.8036 seconds.
Zaw Tun et al.	Round Trip Time (RTT)	RTT and the neighboring hub used in this algorithm in presence of AODV.	Negligible overhead on the system, less use of energy.	This only works for similar static and symmetric systems.	The detection rate is 100% for nodes less than 50.
Mostefa et al.	Wormhole attack detection using sinalgo simulator	It uses moveable node technique to distinguish between malicious node and normal node.	Improve the period by Improving packet delivery rate. It takes energy to maintain the reliability of the system.	Does not work in mobile sensor node, and also other network attack also not covered.	Energy utilization increases by 28% in the affected network area for 200 nodes in 800 milli-seconds.
Rupinder et al.	Wormhole resistant hybrid technique (WRHT)	This method calculates the probability of occurrence of wormhole attack in the system with the help of Delphi and Watchdog scheme.	This technique does not need any extra hardware and it detects wormhole very efficiently.	The Delphi and Watchdog scheme decrease the performance of the system.	Accuracy for 500 node is 0.98.

Mohammad et al.	Artificial Neural Network (ANN)	A moveable detector node is deployed in the sensor field. It collects training and testing data from the sensor nodes.	A machine learning algorithm is used for the detection of residual energy.	Computation overhead is very high and very long process	Accuracy is perfectly achieved.
Rajendra et al.	High Transmissio n Power	This method detects an attack on the basis of transmission power of a malicious node.	Affected nodes have RSSI characteristics by which an attack is detected. No requirement of extra hardware.	Dependency on too many parameters.	Simulation is done on 5 to 100 sensor nodes for the perfect accuracy.

Ⅳ C. Other COUNTERMEASURES AGAINST WORMHOLE Attacks

A. Location and Time based Approaches

- Jakob Eriksson et.al [19] proposed a concept of TrueLink based on the verification of two nodes. Verification of nodes takes place in authentication and rendezvous phases. In the rendezvous phase, the two nodes share nonce so that only immediate neighbors can respond in time. In the authentication phase, the nodes sign the transmit message to mutually authenticate themselves. The major advantage of this scheme is that it can be deployed with a minimal number of resources.
- Hu and Evans [20] proposed a scheme based on some special hardware called directional antennas. By verifying the direction of packets that they are coming from the authenticated neighbors. The information regarding the direction of the packet of set of neighbors is expected to be to the correct node. The drawback of this approach is the requirement of special hardware and it can only detect wormholes where fake neighbors are present.

B. Connectivity and Neighborhood Approaches

- Gupta et.al [21] presented an approach where the destination itself detects the presence of a wormhole by counting the difference of number of hops between the one hop away nodes. This scheme involves that for route discovery RREQ packets are sent by source to destination and each node replies with RREP, before sending the packet to the destination it makes packets called hound packets by signing the message digest with its own private key.
- Vani and Rao [22] proposed a scheme known as WARRDP (Wormhole Avoidance route Reply decision packet) which uses the anomaly detection, hop count and neighbor list method for detection and removal of wormhole. The basic principle of this scheme is to make it possible for the nodes neighbor to the wormhole node to detect that the wormhole nodes have high competition in path discovery. Path discovery takes place by nodes not selecting their immediate neighbors but selecting the route having higher threshold.

C. Graphical and Topological Information based Approaches

- Wang and Bhargava [23] proposed a scheme MDS-VOW (Multi Dimensional-Scaling Visualization of Wormhole) having a central controller for detection of wormholes. The major advantage of this scheme is that it does not require any special hardware but is very less effective in sparse networks.

- Alzer et al [24] proposed a scheme based on the social theory of diffusion of innovations to detect and prevent wormhole detection. It is implemented in five stages which are knowledge, persuasion, decision, implementation and confirmation. This is a decentralized scheme using network monitor elements to monitor parameters such as transmission power, the total number of packets etc.

Table 5: Merits and Demerits of Defensive Techniques Against WORMHOLE Attack

Techniques	**Methodology**	**Merits**	**Demerits**
Location & Time	Based on tight time synchronization and shared secret keys	Low false detections	High computational and bandwidth overhead
Connectivity and neighborhood	Based on hop count and neighbour list	No need of special hardware	High false alarm rates
Graphical and topological information	Based on addition of special monitor nodes	Computation and bandwidth overhead is less No need of time synchronizations	Special nodes with high power are required

Chapter Ⅴ: Sinkhole Attack

Sinkhole attack advertises routing paths to the base stations, making itself a normal node misguiding the neighbor nodes that cause threats to the network. The malicious nodes create a hole in the routing path that can damage the regular operations of the network. The sinkhole attack uses a compromised node with fewer hops to advertise the route to the destination. This misuse of routing information misguides the legitimate node and attracts the node closer. Figure 10 cluster B illustrates the scenario of a sinkhole attack for attracting and capturing packets from the neighbor nodes. The sinkhole attack utilizes a secret tunnel for attracting nodes and capturing packets. The malicious node then deceived and sent packets to the base station

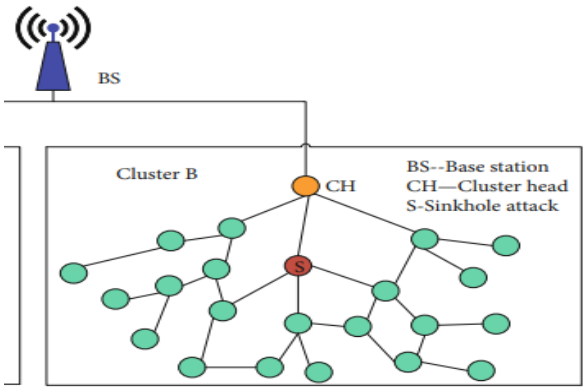

Fig 11: Sinkhole Attack

Ⅴ A. Literature Review

A sinkhole attack involves a malicious node or attacker luring legitimate nodes' traffic towards itself by pretending to be a trustworthy sink node. This can disrupt the normal functioning of the network and compromise the integrity and confidentiality of the data being transmitted. Here's how a sinkhole attack typically works:

Placement of Malicious Node: The attacker strategically places a malicious node in the network, often closer to legitimate nodes than the real sink node.

Advertisement of False Information: The malicious node advertises itself as the legitimate sink node by broadcasting fake routing advertisements with lower hop counts or better signal strength, making nearby nodes consider it as a more optimal choice for routing data.

Traffic Diversion: The legitimate sensor nodes, following the false routing information, start sending their data packets to the malicious node instead of the actual sink node.

Data Interception: The malicious node intercepts the data packets, potentially modifying or capturing sensitive information before forwarding the modified data to the real sink node. This could compromise the accuracy and reliability of the collected data.

Disruption of Network Communication: By redirecting traffic to itself, the attacker can disrupt the normal flow of data in the WSN, causing delays, loss of data, and potential network congestion.

Preventing and Mitigating Sinkhole Attacks in WSNs:

Secure Node Deployment: Ensuring the physical security of sensor nodes during deployment can prevent unauthorized nodes from being introduced into the network.

Cryptographic Techniques: Implementing encryption and authentication mechanisms can help nodes verify the identity of the sink node and ensure data integrity.

Intrusion Detection Systems (IDS): Deploying IDS can help identify and raise alarms when suspicious behavior, such as nodes suddenly advertising lower hop counts, is detected.

Location-Based Trust: Nodes can rely on location information to determine the credibility of routing advertisements. Nodes closer to the legitimate sink node might be more trusted.

Multi-hop Verification: Instead of blindly following the advertised routing information, nodes can verify the information from multiple neighboring nodes to make more informed routing decisions.

Routing Protocol Enhancements: Developing secure and robust routing protocols that are resistant to sinkhole attacks can significantly improve network security.

Dynamic Key Management: Regularly updating encryption keys and managing them dynamically can make it harder for attackers to decrypt intercepted data.

Behavioral Analysis: Monitoring nodes' behavior for sudden changes or deviations from their normal patterns can help detect sinkhole attacks.

Ⅴ B. SURVEY ON VARIOUS METHODS for SINKHOLE ATTACK

The detection of sinkhole attacks is mainly classified into four categories, namely mobile agent-based detection, hop count-based detection, sequence number-based detection, cryptography-based detection and energy consumption-based detection. We learned about various classifications of sinkhole detection methods merits, demerits and performance metrics of each paper.

(A) Hop count-based detection
(B) Agent based detection
(C) Cryptography based detection
(D) Sequence number-based detection

A. Hop count based detection

In hop count based detection techniques the sinkhole has been identified by using various algorithms. The fake hop count has been identified using different techniques to prevent the sinkhole attack in WSN.

1) ***Detecting Sinkhole Attacks in Wireless Sensor Network Using Hop Count****:* Md. Ibrahim Abdullah et al. [25] proposed a mechanism for sinkhole attacks which detect the malicious nodes using hop count. Thus, the main advantage is that without requiring any discussion with the base station, the node can detect the malicious node. So here the base station is placed

outside the network and it keeps the records of all the node id. The record is updated if any node misplaces or is deployed. So, a perfect quality route was provided to the base station to launch an attack. By some localization measures the location of nodes is maintained in a base station. It helps the nodes from recognizing the base stations wrongly. Thus, in this technique a neighbour database construction will be done and it has the details of base station and sensor nodes with a detailed description of id and hop count. To detect sinkhole each node has a sorting algorithm and it takes the lowest hop count value and its id and thus calculates the average hop count. It calculates the difference between average and lowest hop count. If the difference is greater than a threshold value, it is an anomaly. It is also identified as a suspicious node for all the nodes that have minimum value.

2) ***Sinkhole Attack Detection Based on Redundancy Mechanism in Wireless Sensor Networks:*** Fang-Jiao Zhang et al. proposed a sinkhole attack detection based on redundancy mechanism in WSN. A multipath selection happened in WSN,
The path establishment consists of route request, route reply and route establishment. A node in the network transmits the request to the various other nodes through broadcast message and all nodes receive it. The packet contains the field name, path to record information, a collection of nodes the packet passes etc. Thus, the neighbour node updates the neighbour list until the route request reaches the destination. When the node first receives the route request packet, it would save the sending node as a parent node, and add their own identity to the field-Path in route request packet, and then transmit the packet. Thus, the node receives the reply packet and sends a reply to its parent node. Thus, by using Dijkstra algorithm the multipath problem increases as the distance to the sink increases in [26]. By using selective forwarding methods, the increase of the distance to the sink will not help the compromised nodes to attract traffic. Thus, using the resilient approach, the sinkhole attack has been detected with higher performance.

B. Agent based detection

In mobile agent-based detection techniques the sinkhole has been identified by using various techniques. The monitor node collects the various details about the agents and through that the sinkhole is detected.

1) ***A Secure Routing Algorithm Against Sinkhole Attacks***

For Mobile Wireless Sensor Networks: A secure routing algorithm against sinkhole attack for mobile wireless sensor networks has been developed by Liping Teng et al. [27] for mobile wireless sensor networks (MWSN) based on a mobile agent through the routing algorithm for data packets. Mobile agents are made to communicate with each other with a respective counter added to it. Thus, these counters increment a value when it visits a node. If two agents visit the node, the agent with the higher counter has been updated. These agents contain the id, program and agent packets. Mobile agent reaches one node, compare the counter stored in the agent packet with counters of other nodes; the data information with a bigger counter is updated. Then the agent will copy the information of the updated node of the cache. A matrix table will be created about the details of all the nodes. When the data packets need to be sent, a path is selected according to the routing algorithm. A routing algorithm for data packets is also being developed that checks the connection between node A and node B. If T (A, B) =0 then no connection is established. Otherwise, it establishes a connection and finds the hop count as zero. Thus, a routing algorithm created by every node can communicate with each other so easily without any problems. So, by using agents the overheads have been reduced and the information reaches the destination in an efficient way.

2) ***A Leader Based Monitoring Approach for Sinkhole Attack in Wireless Sensor Network:*** Udaya Suriya Rajkumar et al. [28] proposed a leader-based monitoring approach in wireless sensor network for sinkhole attack. So, a Leader Based Intrusion Detection System (LBIDS) is proposed and a leader randomly selected in a group and while constructing a node it has to register with the cluster heads. At the time of data transmission, a leader selects the node with highest energy. A table has been created with the id and location of each node there; whenever it goes for transmission the leader will choose the nodes with highest energy with the residual energy. Whenever the node begins a connection in the network, the clusters check and verify the table. Same way an algorithm for malicious node is also been created for the detection of suspicious region for that IDS algorithm is been checked, in the network a node checks its content in the table such as its id
and procedure otherwise change the path thus we can avoid the malicious behaviour also by checking the IDS of LBIDS. An agent is set with a counter value added to it and if the agent disperses the node, the counter value will be uploaded. The counter identifies the frequency visited by the agent and if two agents have the same counter value the bigger counter will be updated. Another way to detect the sinkhole is by using the equation TAB = (R-d) (R>d) /v Where A and B are neighbouring nodes within the transmission range R, with the distance d and V is the average speed. So, the leader-based method proved the detection of sinkhole and its removal by using a mobile agent.

C. Cryptography based detection

In cryptography-based detection techniques the sinkhole is been identified by using various cryptographic techniques. The various cryptographic methods are identified and through that the sinkhole has been detected.

1) ***Intrusion Detection System against Sinkhole Attack in Wireless Sensor Networks with Mobile Sink:*** Mohamed Guardroom et al. proposed an Intrusion Detection System (IDS) against sinkhole attack in wireless sensor networks with mobile sink. Thus, through a flat grid cell the detection area is divided to detect the attack. Thereby the authors differentiate between real and false sink nodes by using signature-based techniques. Thus, by using signature-based techniques the false mobile sink node has been detected. Cell leaders activate their IDS only when a sinkhole event occurs. This permits to reduce the number of nodes running their IDS and minimize energy consumption in terms of detection rate, efficiency, and energy consumption, the proposed IDS shows high performance.

2) ***To Detect and Overcome Sinkhole Attack in Mobile Ad-Hoc Network:*** Vivek Tank et al. proposed a cryptographic technique such as digital signature and hash function along with AODV routing protocol to prevent attack in sinkhole in MANET. Since the MANET is prone to environmental problems, security is the main problem regarding sequence numbers. Thus, every time the user sends a request the reply message can be identified using the Source, Destination and Sequence number. Thus, by using digital signature and hash chain the security is maintained. For maintaining the identity of each packet, the digital signature was used. Hash chain is used to authenticate the hop count of RREQ/RREP messages. After checking this, the sequence number has been determined by the current and previous one thereby finding out the duplicate sequence number compared to security techniques. The packet is forwarded if it has a digital number and hash chain or unique sequence number otherwise the packet dropping can be done.

D. Sequence number-based detection

In these detection techniques the sinkhole has been identified by using sequence numbers. The monitor node collects the various details about the network and through that the sinkhole is detected.

1) ***Identification of Contamination Zones for Sinkhole Detection in MANETS:*** Leovigildo Sánchez-Casado et al. proposed a detection methodology for identification of contamination zone for sinkhole attack in MANET. The nodes in the dynamic region communicate to each other using a multi hop strategy. So, a behavioural based detection system has been proposed for the existence of contamination zones. So, a two-phase collaborative detection scheme for the sinkhole attack is produced. The pre detection process is the first approach for reducing the overheads, only after an alarm rings the next approach happens thereby collecting the neighbour details and detecting the malicious neighbour. The existence of a contamination border has been identified by the nodes in the contamination zone; it forwards the traffic through a sinkhole node. So, the node in the non-contamination zone sends a message to the neighbour in the contamination zone, and gets a reply as false information. So, it can be detected by having a sequence number greater than other nodes as we considered the sinkhole. Thus, the sequence number is compared and thereby it detects the malicious nodes and this method helps to reduce the fake reply being sent by the nodes. The results obtained highly reduce the attack and it achieves the detection process.

2) ***Detection and Isolation of Sinkhole Attack from AODV Routing Protocol in MANET:*** Shashi Pratap Singh Tomar et al. presents mechanism of detection and isolation of sinkhole attack in MANET by using ad hoc on demand routing protocol for the sinkhole attack. This routing protocol has various phases. In the first phase the source node broadcasts various route requests to its neighbour by sending route request and obtain shortest route in terms of long life or energy efficiency. In the next phase the route table was updated and stored the details of the source and destination, sequence number and hop count. This led to the route inquiry phase which evaluated the current and previous request with sequence number. Thus, the malicious node is assumed if the value of sequence number is larger than packet drop. In the next phase they compared the threshold value with sequence number, this may be based on the cumulative sequence number of packets successfully received/transmitted by the destination and source node. The packet will be malicious if the value of threshold is larger than the confirmed value. The shortest path has been taken from source to destination. If the value is less than or equal to threshold, the last phase is analysed and compared with the near values. They establish multiple paths between source node to destination node to prevent sinkhole attack. Hence the load balancing power aware rate has been achieved and rate-based congestion techniques helps in other routing protocols with high density and speed of nodes in MANET.

Table 6: Algorithms to detect sinkhole attacks in WSN

Algorithm	Description	Merits	Demerits
Hop count-based detection	This algorithm uses the number of hops between a node and the base station to detect sinkholes. If a node has a significantly lower hop count than its neighbors, it is considered to be a sinkhole.	Simple to implement and requires low computational resources.	Not very reliable, as the hop count can be manipulated by the attacker.
Link quality indicator	This algorithm uses the	More reliable than hop	Requires more

(LQI)-based detection	LQI, which is a measure of the signal strength between two nodes, to detect sinkholes. If a node has a significantly higher LQI than its neighbors, it is considered to be a sinkhole.	count-based detection.	computational resources.
Received signal strength indicator (RSSI)-based detection	This algorithm uses the RSSI, which is a measure of the power of the signal received by a node, to detect sinkholes. If a node has a significantly higher RSSI than its neighbors, it is considered to be a sinkhole.	More reliable than hop count-based detection.	Requires more computational resources.
Trust-based detection	This algorithm uses a trust value to determine whether a node is malicious. The trust value is calculated based on factors such as the node's behavior, its reputation, and its interactions with other nodes.	Can be very effective in detecting sinkholes.	Requires more computational resources and a well-defined trust model.
Intrusion detection system (IDS)-based detection	This algorithm uses an IDS to detect sinkholes. The IDS monitors the network for suspicious activity, such as a node sending a large number of routing packets or a node having a high packet drop rate.	Can be very effective in detecting sinkholes, even if they are sophisticated.	Requires more computational resources and a well-configured IDS.

Chapter VI: Conclusion and Future Scope of Work

With the emerging technology, WSN is an interesting topic of research having a wide variety of applications. Routing faces a lot of challenges in WSN and because of the open wireless nature of these networks there are a lot of security issues. Therefore, different types of attacks are possible on these networks. Classification of attacks has been studied at different layers on the OSI (Open Systems Interconnection) model. Also, the different mitigation techniques of the severe attacks including Wormhole, Sybil and Sinkhole attacks are also studied. The advantages and limitations of these proposed schemes are also considered. Although several detection mechanisms have been proposed by various researchers, there is still no efficient method which can overcome most attacks with energy efficient manner and complete accuracy.

The future scope involves having the integrated detection and prevention scheme to avoid most of the attacks at the network layer, having less computation and bandwidth overhead, more energy efficient and having better quality of service parameters. Security is a major challenge for WSNs. Researchers are developing new security protocols and techniques to protect WSNs from attack. Secure WSNs will be essential for many applications, such as critical infrastructure monitoring, defense, healthcare and IOT.

In this thesis I performed a survey on the three known attacks in WSN namely Sybil, Wormhole and Sinkhole attacks and compiled various mitigation strategies to tackle each of them. I believe that this survey has the potential to make a significant contribution to the field of WSNs. I encourage further research to improve the security and performance of WSNs in real world applications.

References

[1] Singh, Shio Kumar, M. P. Singh, and D. K. Singh, “A survey on network security and attack defense mechanism for wireless sensor networks,” international journal of computer trends and technology 1, no. 2, pp. 9-17, 2011
[2] Amuthavalli, R., and RS Bhuvaneswaran, "Detection and prevention of sybil attack in wireless sensor network employing random password comparison method," journal of theoretical & applied information technology 67, no. 1, 2014.
[3] Dhamodharan, Udaya Suriya raj kumar, and Rajamani Vayanaperumal, "Detecting and preventing sybil attacks in wireless sensor networks using message authentication and passing method," the scientific world journal 2015
[4] Dhanalakshmi, T. G., N. Bharathi, and M. Monisha, "Safety concerns of sybil attack in WSN," in science engineering and management research (icsemr), international conference on, pp. 1-4, IEEE, 2014.
[5] Sarigiannidis, Panagiotis, Eirini Karapistoli, and Anastasios A. Economides, "Detecting sybil attacks in wireless sensor networks using UWB ranging-based information," expert systems with applications 42, pp. 7560- 7572, no. 21, 2015
[6] Sujatha, V., and Ea Mary Anita, "Detection of sybil attack in wireless sensor network," 2015.
[7] Triki, Bayrem, S. Rekhis, and Noureddine Boudriga, "An RFID based system for the detection of sybil attack in military wireless sensor networks," in computer applications and information systems (wccais), world congress on, pp. 1- 2. IEEE, 2014.
[8] Yu, Yan, Ramesh Govindan, and Deborah Estrin, “Geographical and energy aware routing: a recursive data dissemination protocol for wireless sensor network,” Technical report ucla/csd-tr-01-0023, ucla computer science department, 2001
[9] Pantazis, Nikolaos, Stefanos A. Nikolidakis, and Dimitrios D. Vergados, "Energy-efficient routing protocols in wireless sensor networks: a survey," communications surveys & tutorials,IEEE 15,pp. 551-591, no. 2, 2013
[10] Roychowdhury, Sinchan, and Chiranjib Patra, "Geographic adaptive fidelity and geographic energy aware routing in ad hoc routing," in international conference, vol. 1, pp. 309-31, 2010.
[11] J Douceur, J. S. Donath, "The Sybil attack", in Proceedings of ACM IPDPS, pp. 251-260, 2002
[12] A.Margolin, N. Boris, and L.B.Neil, "Informant: Detecting Sybils using incentives", In Proceedings of Financial Cryptography (FC), Springer, pp. 192-207,2007
[13] M.Demirbas, Y.Song, "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks", In Proceedings of the International Symposium on World of Wireless, Mobile and Multimedia Networks, pp. 564 - 570,2006.
[14] Youran Xu Guanling, James Ford and Fillia Makedon, “Detecting Wormhole attack in wireless sensor networks”, International Federation for Information Processing, Volume 25, Springer
[15] Parmar Amisha ,V.B.Vaghela, “Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol”, 7th International Conference on Communication, Computing and Virtualization, 2016, pp. 700-707
[16] Rajendra Kumar Dwivedi, Prachi Sharma, Rakesh Kumar, “A Scheme for Detection of High Transmission Power Based Wormhole Attack in WSN”, 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), 2018, pp.1-6
[17] Rupinder Singh, Jatinder Singh, and Ravinder Singh, “WRHT: A Hybrid Technique for Detection of Wormhole Attack in Wireless Sensor Networks”, Hindawi Publishing Corporation Mobile Information Systems, vol. 2016, Article ID 8354930, pp. 1-13
[18] Mohammad Nurul Afsar Shaon and Ken Ferens, “Wireless Sensor Network Wormhole Detection using an Artificial Neural Network”, Int. Conf. Wireless Networks, ICWN'15, pp. 115-120
[19] J. Eriksson, S.V.Krishnamurthy and M.Faloutsos," TrueLink: A Practical Counter measure to the Wormhole Attack in Wireless Networks", in 14lh IEEE International Conference on Network Protocols, pp.75-84, 2006

[20] L.Huand and D.Evans, "Using Directional Antennas to Prevent Wormhole Attacks", in Network and Distributed System Security Symposium (NDSS), 2004.
[21] S.Gupta, S.Kar and S.Dharmaraja, "WHOP: Wormhole Attack Detection Protocol using Hound Packet", in IEEE International Conference of Innovations in Information Technology, pp.226-231, 2011
[22] A.Vani and D.Sreenivasa Rao, "WARDP", in International Journal on Computer Science and Engineering (UCSE), Vol. 3, no. 6, pp. 2377-2384,2011
[23] Dhara Buch and Devesh linwala, “Detection of wormhole attacks in wireless sensor network”, Proc. of Int. Con! on Advances in Recent Technologies in Communication and Computing, 2011 pp. 1-8
[24] W.Wang and B.Bhargava, "Visualization of wormholes in sensor networks", in Proceedings of the 3'd ACM workshop on Wireless security, pp.51-60, 2004.
[25] Md. Ibrahim Abdullah, Mohammad Muntasir Rahman and Mukul Chandra Roy, “Detecting sinkhole attack in WSN using hop count,” I. J. Computer Network and Information Security, 3, 50-56, Feb(2015).
[26] Mamta Patel, Prof. Mohammed Bakhtawar Ahmed, “Sinkhole Attack Detection Based On Redundancy Mechanism In Wireless Sensor Networks,” Ijsdr, Volume 1, Issue 6, 2016
[27] Liping Teng, “SeRA: A Secure Routing Algorithm against Sinkhole Attacks for Mobile Wireless Sensor Networks,” Second International Conference on Computer Modeling and Simulation, 978-0-7695-3941-6, 2010.
[28]] Udaya Suriya Rajkumar and Rajamani Vayanaperumal, “A Leader Based Monitoring Approach For Sinkhole Attack In Wireless Sensor Network,” Journal of Computer Science 9 (9): 1106-1116, July(2013).
[29]Svarika Goyal;Tarunpreet Bhatia;A.K. Verma “Wormhole and Sybil Attack in WSN: A Review” 20152nd International Conference on Computing for Sustainable Global Development (INDIACom)
[30]Annie Mathew; J. Sebastian Terence “A Survey on Various Detection Techniques of Sinkhole Attacks in WSN” 2017 International Conference on Communication and Signal Processing (ICCSP)
[31] Shehnaz T. Patel; Nital H. Mistry “A Review: Sybil Attack Detection Techniques in WSN” 2017 4th International Conference on Electronics and Communication Systems (ICECS)
[32]Mohit Kumar Verma;Rajendra Kumar Dwivedi”A Survey on Wormhole Attack Detection and Prevention Techniques in Wireless Sensor Networks”2020 International Conference on Electrical and Electronics Engineering (ICE3)