Journal of Information Systems Engineering and Management
2025, 10(27s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Design and Implementation of Security Technique for Selective Forwarding Attack in Wsn

Hriday Banerjee [1*], Surendra Yadav [2]
[1*]*Research scholar, Department of Computer Science and Engineering, Vivekananda Global University (VGU), Jaipur – 303 012, Rajasthan, India, hriday1991.banerjee@gmail.com*
[2]*Professor, Department of Computer Science and Engineering, Vivekananda Global University (VGU), Jaipur – 303 012, Rajasthan, India*

ARTICLE INFO

Received: 21 Dec 2024

Revised: 17 Feb 2025

Accepted: 24 Feb 2025

ABSTRACT

WSN is best recognized for monitoring network processing and physical metrics continuously. Self-organizing, infrastructure-less, fault-tolerant networks provide quick, scalable, low-cost, and easy-to-implement deployments in many applications. Nodes and data security assaults can harm WSNs. As WSN security is a challenge. Nodes in harsh and changing settings make it harder for a wireless sensor network to maintain security. WSN nodes with low resources face several security risks. Most such attacks are black hole, selective forwarding, and DoS. SF is one of the most hazardous WSN assaults. SFA attacks hack legitimate nodes and selectively drop packets. Clustered WSN selective forwarding attackers are the focus of this paper. This study divides nodes by functionality into IN, CH, and MN. The suggested strategy prioritizes malicious node identification over system efficiency. As proposed, WSN efficiency is assessed by maximizing throughput by improving the network's "packet delivery ratio (PDR)" and data transfer. This paper begins with a WSN overview. The paper also covers WSN applications and clustered WSN characteristics. This publication also presents authors' past SF attack recognition works.

Keywords: WSN, Selective Forwarding Attack, Clustering, Composite Reputation Value, Inspector Node, Member Nodes, Cluster Head, Base Station, Sensor Node.

I. INTRODUCTION

A wireless sensor network, also known as a WSN, is a well-organized network in which each individual piece of wireless sensor equipment is referred to as a Sensor Node (SN), and each node is linked to one or more additional SNs. Another name for a wireless sensor network is an ad hoc network. An ad hoc network is another term that can be used to refer to a wireless sensor network. Another name for a wireless sensor network is an ad hoc network, which is just another way of saying the same thing. In its most fundamental form, a wireless sensor network, or WSN for short, is designed to gather data from the "real world." They are able to detect a wide number of various physical components, including as vibrations, pressure, temperature, and sound, and then broadcast that information throughout the network when it is required for them to do so. These types of networks make use of sensors, each of which is tasked with the responsibility of accumulating data, processing that data, and then transmitting it to a central node. These networks are useful in situations and configurations in which the use of wires would not be practicable and would be improper. In these scenarios and configurations, these networks are useful.

It is strongly urged that academics and researchers conduct research on additional concerns that are linked with WSN security vulnerabilities. This is due to the fact that wireless sensor networks are utilized in an overwhelming majority of the applications that are used in today's modern world. Every encryption network contains safeguards for authentication, authorisation, data integrity, and privacy; however, the degree to which these features are implemented varies from network to network. Authentication, authorisation, data integrity, and privacy safeguards are all included in every encryption network. WSN is afflicted by a variety of critical challenges, some of the most prominent of which include the power, the range of sensors, the number of sensors, and the installation of security systems.

One of the many diverse application subfields that are included under the umbrella term "ubiquitous computing" is wireless sensor networks (WSNs). The phrase "ubiquitous computing" refers to an overarching idea that incorporates a range of various application subfields. These networks are made up of a collection of intelligent sensor nodes that are very small in size, require very little power, and are connected to one or more base stations. There is also the possibility of there being additional base stations. After data has been gathered by SNs in a variety of settings, such as man-made environments, natural ecosystems, and battlefields, it is then transmitted to one or more BSs. These settings include man-made environments, natural ecosystems, and battlefields. These locations can range from those that were created by humans, to natural ecosystems, to even combat zones. These places can be those that were made by humans, natural ecosystems, or even war zones.

Some of these places were even constructed by humans. SNs have a restricted capability for communication, wireless bandwidth, memory, processing power, and battery power, in contrast to BS, which are outfitted with a greater number of computing resources, energy sources, and transmission channels. While SNs have a limited capacity for communication, wireless bandwidth, memory, and processing power, BS have a much greater amount of each of these. As an example, the topology of a WSN is shown in Figure 1 in its most fundamental form. This was done for the sake of clarity. Due to the fact that it acts as a communication go-between for the SNs and the end user, the base station is an exceptionally vital component of the system. [1].

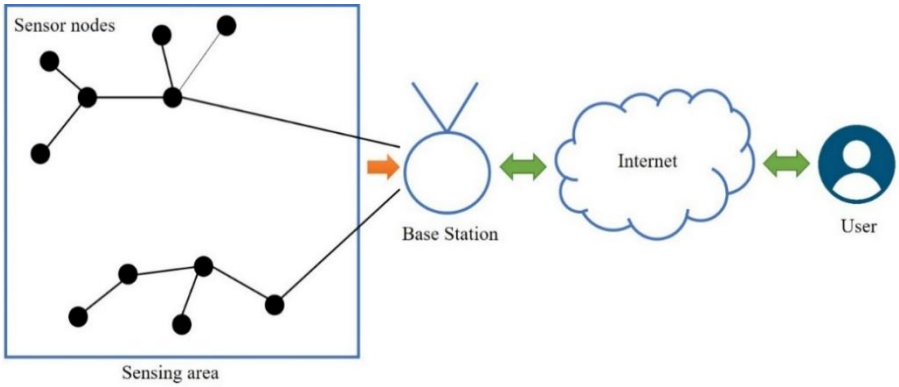

Figure 1: Wireless Sensor Networks

A self-coordinating system that is built out of a large number of small, low-cost SNs that have minimal store space, low energy consumption, and limited processing power is referred to as a wireless sensor network (WSN). Cluster-based wireless sensor networks have recently achieved extensive application in large-scale wireless data collecting networks [2, 3]. Figure 2 [4] depicts the process by which data packets are moved from the member nodes (MNs) of a cluster-based wireless sensor network to the CHs that are associated with those MNs. After that, the data packets are delivered to the CHs that are situated on the succeeding hop before they arrive at the sink node. Because of this, it is no longer necessary for each CH to explicitly transmit data with the sink node. This is because the requirement has been removed. On the one hand, there is a possibility that the SN and CH will be unable to make direct touch with one another if the channels are either too weak or the distance between them is too considerable.

On the other hand, the cost of energy necessary for multi-hop connectivity is generally cheaper than that required for direct long-distance transmission in some scenarios. This is because multi-hop connectivity involves sending data across multiple intermediate nodes. Each of the nodes in the network takes turns functioning as CHs so that there is an even distribution of power consumption across the network. This is done to ensure that there is an even distribution of power consumption across the network. Additionally, the lifetime that can be expected from the network has been extended.

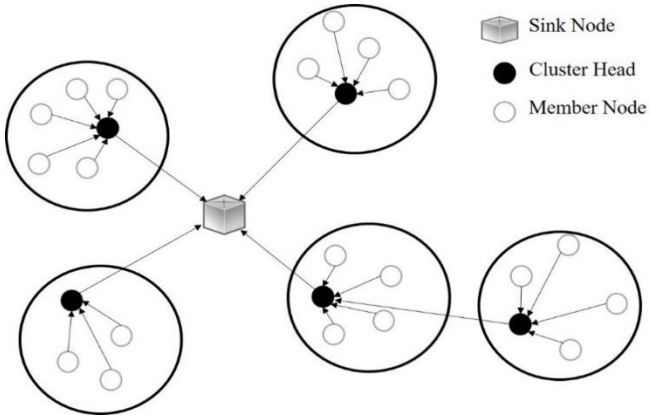

Figure 2: An example of a cluster based WSN

CHs, which play essential roles in cluster-based WSNs, are frequently the targets of a wide variety of attacks, which can come from either the inside or the outside of the network. The practice of selective forwarding, in which an adversary takes control of a CH and discards all or a portion of the data packets, is one of the most common types of assaults. Not only is there a significant decrease in quality of service (QoS) and a significant amount of data loss, but there is also a significant amount of interruption to energy-balanced routing protocols [5,6].

WSN are considered to be power-constrained networks since they have limited access to both energy and compute resources. Because of this, they are vulnerable to any attacker that possesses more power than any single node or BS, which may not be a particularly difficult undertaking for the attacker. In a typical sensor network, there could be hundreds of nodes that communicate with one another using broadcast or multicast transmission. As a result of the broadcast nature of the communication channel, WSNs are susceptible to having their security compromised. Numerous forms of assault are open to consideration within a WSN. It is possible to classify these security breaches using a variety of factors, such as the domain of the attackers or the tactics that were utilized in the attacks. SFA is one of the assaults that occurs the most frequently in clustered WSN.

There are three different kinds of SFA: an on/off attack, a grey hole attack, and a black hole attack. An on/off attack is one that occurs when a malicious node loses all of the data packets or part of them for a period of time and then functions normally the remainder of the time [7]. During a grey hole attack, a malicious node loses packets at random for no apparent reason [8]. The black hole attack is the most damaging type of SFA [9], since it causes a malicious node to lose all of the packets that it is capable of transmitting. Because the rounds and the quantity of missed packets in an SFA are both randomized, it is nearly impossible to tell whether or not the problem is caused by poor channel quality [10]. Because of this, the energy efficiency, stability, and dependability of WSNs, as well as the capability to locate an SFA, are necessary and helpful.

A. Characteristics of Clustered WSN

WSNs have a number of unique features that make them ideal for large-scale applications. The following sections outline the key features of clustered WSNs.

Data Load Management: Clustering allows for uniform network lifespan and effective data load storage. In order to transmit data from upper layers, CHs closer to the base station, face increased data loads. To deal with this issue, Cluster heads that are nearer to the BS keep fewer MNs to decrease load. The energy loss of all nodes is equal, and the duration of the system is uniform [11].

Efficient Energy Saving: Data is sent via flooding in flat networks, but data is aggregated on the Cluster head level and through multihop routing in cluster-centered networks, data transmit to the BS. In a cluster-based network, multihop routing reduces the number of propagation routes, which helps in saving energy exponentially [12].

Relay Node: When nodes fail to connect, the network is disconnected or partitioned. The relay node is applied to reconnect the partitions and reestablish the route. The relay node may be either mobile or static. A static node's initial job, on the other hand, is to locate the disjoint component and then deploy a relay node there. Mobile relay nodes, on the other hand, are a unique type of node that operates in a disjoint portion [13].

Collision Avoidance: When a single channel is considered in a sensor network, it is shared by SNs. As a result, when a various node transmits data at the same time, the network's performance reduces. This can be easily resolved in a cluster WSN, where the cluster head uses scheduling to give a special time slot to each member node [14].

Fault Tolerance: Energy depletion, interruption, delay, hardware degradation, and other factors may all impact SNs. Cluster-based protocols are ideal for certain restrictions, where nodes are not replaceable in a harsh environment. WSNs, in hostile conditions and remote areas, must be able to reconfigure themselves without human intervention. Fault tolerance techniques must be addressed during the protocol design stage to protect aggregated data. When CH fails, cluster repair and CH backup are more practical approaches for securing the whole network restoration.

B. Security Objectives of WSN

Sensor networks are distributed networks, and they all have several things in common with a traditional computer network. As a result, WSN security objectives must incorporate both standard and unique network standards, such as secrecy, integrity, data freshness, compatibility, and authentication. The below are the main security objectives of WSNs [15]:

- Time Synchronization
- Self-Organization
- Data Integrity.
- Data freshness
- Data authentication
- Data availability

II. RELATED WORK

WSN creation has often been hindered by security difficulties, particularly insider assaults [16]. The simplest insider SFA, the black hole attack, drops each packet attracted from the forwarding channel by itself [17]. Since the rogue node does not forward packets for a long time, its neighbors assume it failed and refresh the routing data. On/off attacks [18] are highly stealthy SFA in which all or part of a packet is dropped at standard intervals while nodes act normally.

According to Lu et al. [19], selective forwarding is clever; compromised nodes choose which packets to send to avoid being accused of interfering with packet quality or losing interesting packets. According to Youngho et al. [16], a multi-node collusion assault might harm the entire network. When assessing WSN security, most people can create an intrusion detection scheme (IDS) [20] using reputation value monitoring.

Ding and Liao [21] proposed a hybrid continuous strategy monitor-forward game to detect and eliminate malicious nodes between its one-hop neighbor nodes and the sending node, minimizing packet loss detection error in insecure radio channels. Examining nodes, energy-heterogeneous nodes that just record data, can prevent malevolent nodes from initiating insider assaults, according to Hu [22].

Many current algorithms based on alternative hypotheses have been presented and explored to solve the security problem, shifting the focus from hostile nodes to other helpful approaches. Shanchieh and Biru [23] estimate node reliability to limit selective forwarding. They employ modeling to investigate node forwarding behaviors to unstate SF and design a high-quality data-forwarding path.

Pitsillides and Stavrou [24] emphasize system recovery after an insider SFA. Directional antennas and blacklist-based rerouting will restore a larger, more stable, and sensitive structure.

Monitoring nodes were deployed to overhear network packets and evaluate regular node energy supply and forwarding rate [25]. After that, each node's credibility value is determined using its capacity, entropy function, and forwarding rate. Any node with low repute is an SF attacker. This method fails in mobile WSNs because the next hop always changes.

The authors employ a theory to classify SFA in [26]. They assume the other nodes stay still as the SF attacker moves. They compare neighbor node message exchange times. Malicious nodes occur when the time surpasses a threshold.

Fu et al. [27] suggested data clustering for SF attack detection. Sink nodes receive the cluster head's average forwarding rate from inspector nodes. The sink node detects suspicious locations using complex parameter clustering. This method relies on MinPts and Eps. A node is dubious if cluster head I is a noise point for k rounds. To determine cluster head i, the investigator node estimates the cumulative forwarding rate of the CH and MN.

Shreenath K N et al. presented zoning system solution [28]. WSN has different-sized areas. IDs were assigned to each zone. A localization algorithm ensured each SN's location. Every node shares energy with the BS and each other. As field leader, BS chooses the most energetic node. Cluster head receives and sends MN data to BS. All zone heads and nodes were monitored by mobile agents. The mobile agent labels a node a BH if it cannot send or receive data. The base station and zone Head will be alerted and the rogue node removed from the network.

Table 1: Comparison between various schemes for SFA

Ref. no.	Year	Author	Scheme	Special Features
[16]	2012	Youngho et al.	Virtual trust queuing	To protect against inside attackers dropping packets, improve the trust mechanism.
[26]	2012	S. K. Das, J.W. Ho, and M. Wright	Mobile malicious node detection scheme	With just a few tests, it detects mobile malicious nodes rapidly and with very low false negative and false positive rates.
[23]	2014	Biru and Shanchieh	NRE	Set up a high-quality data-forwarding route to protect from SF attacks.
[24]	2014	Pitsillides and Stavrou	Directional antennas	Rebuild a highly responsive, stronger, and highly reliable system in improving recovery in a cooperated sensor system
[25]	2014	Y. Hu, Y. Wu, and H. Wang,	Monitor node, trust mechanism	Defense against the insider attack
[19]	2015	Lu et al.	Trust queuing mechanism	Defend against both protocol-violation attacks and information-falsification.
[21]	2015	Liao and Ding	trust-based scheme	For cluster WSN, identify and separate malicious nodes. Choose more dependable CHs with appropriate residual energy and a high level of trust.
[26]	2019	Fu et al.	DCA-SF algorithm	Detect the SF attack.

III. SECURITY IN WSN

When it comes to wireless networking, security is a big issue to solve. Because of their energy and mobility limitations, WSN are vulnerable to attacks. Passive attacks and Active attacks are the 2 kinds of attacks. Passive attacks aren't able to change data because they're passive. Aside from active attacks, attacks can occur at wireless sensor network layers for example the “Application layer, Transport layer, Network layer, Link layer, and Physical layer”. In the Open system interconnection model, there is inter-process communication happens between the OSI layers. There is a risk the data will shift during an aggressive attack, which will damage the device. Modifications, network flow observation, and information disruption are all examples of data transition [29]. This kind of attack is much easier to identify than to avoid. Some DOS attacks in the OSI layers are analogous to this. The network or nodes are not affected in a passive attack, but the information is changed. It's difficult to detect a passive attack. In Figure 3 [30], layer-by-layer security attacks are discussed.

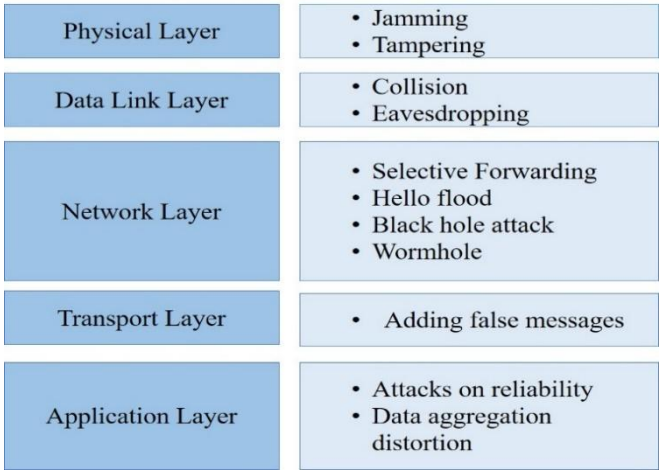

Figure 3: Layer-wise attacks in WSN

IV. CLUSTERING

Clustering is a core principle for reducing energy usage and extending the lifespan of SN in a network. Following a random deployment of SNs in the region of interest, each SN in the field attempts to form a cluster. Inside the transmission spectrum, each node only communicates with a limited number of SNs. Many of the nodes are not clustered at the start. Different types of messages, such as join, state, and Broadcast are used by each node in the clustering process.

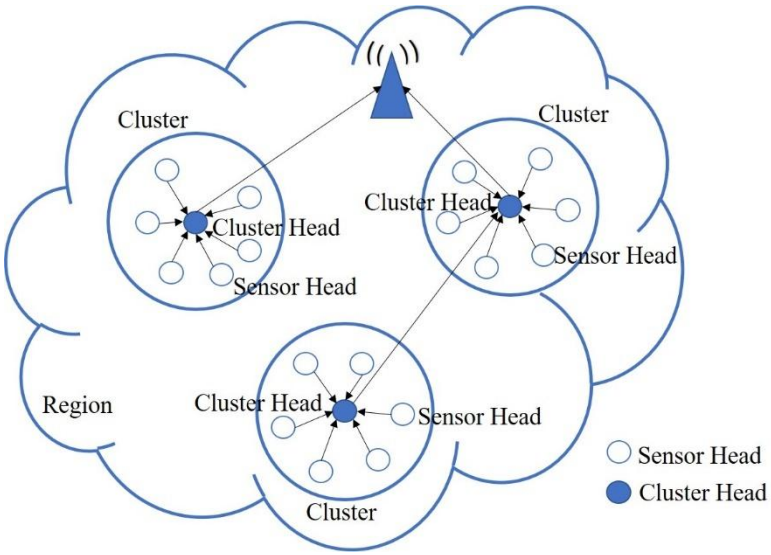

Figure 4: Clustered Networks

Each node informs the neighborhood. Latency, message volume, and energy decide if the node is a CH. The energy-rich node would delay least. Once the CH delay is through, the node can transmit a state message to its neighbors. Figure 4 shows the cluster building after other nodes make join requests [31]. CHs can create networks by binding.

The CH would send data to the sink node. Energy-efficient heterogeneous clustering is recommended for heterogeneous SNs. Clustering nodes with different sensing, energy, propagation, and other ranges is heterogeneity. EHC creates wireless sensor clusters. Distributed cluster creation and head recognition are used. Route identification with a shortest path algorithm that avoids obstacles (Figure 5) finds the shortest communication route to the sink node [31]. Creating a routing route allows CHs to link networks. The CH identifier can be changed dynamically to extend network lifespan. This dynamic cluster construction would extend network life and reduce energy use.

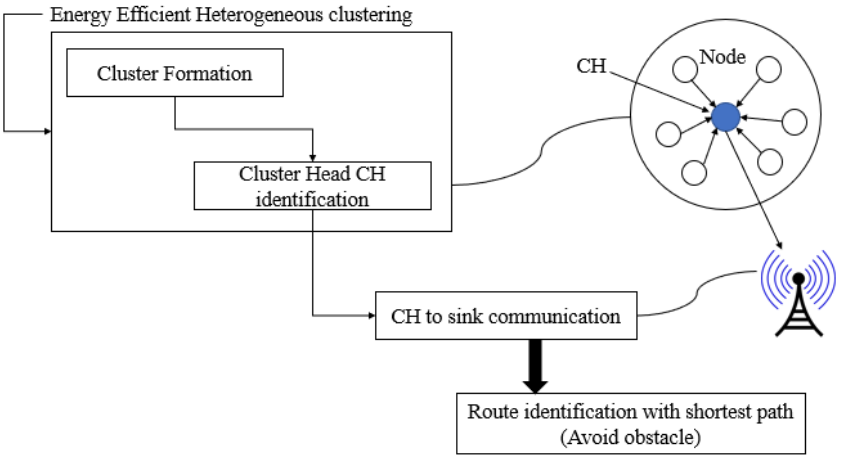

Figure 5: System Architecture

V. ROUTING PROTOCOLS IN CLUSTERED WSN

Routing performs an important part in WSN that is to be handled carefully. Routing protocols are needed for transmission of data between the SNs and BSs, to establish the connection. For a high network rate, the routing route must be the shortest and most secure. Based on different features, several routing protocols applied in the WSN vary from each other. Various routing protocols were created to assure this function and are in fact classified into 3 families as shown in figure 6.

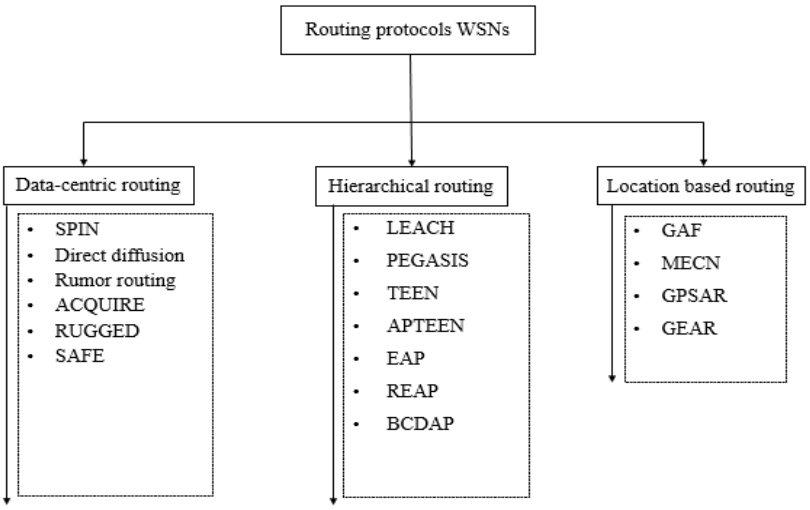

Figure 6: WSN Routing Protocols

A. Hierarchical Routing:

Clustering groups WSN nodes. The BS receives data from a cluster node specified as a CH. The energy-efficient protocol is clustering. By establishing optimal data transfer pathways, clustering nodes saves energy. Clustering extends SN life and balances node load. PEGASIS, APTEEN, TEEN, and LEACH consider the CH the most energy-hungry node and the hub for intra- and inter-cluster communication.

VI. LEACH

WSNs running in rounds use LEACH [33], a low-energy hierarchical routing protocol [34]. A LEACH round comprises two phases: setup and steady state. SNs create clusters during setup and exchange data with their CHs, who interface with the BS, during steady. Cluster heads send aggregated data to the base station. SNs consume more resources when sending base station communications than when connecting to other nodes. By running in two phases and rounds, LEACH saves resources. To cycle between sensors, LEACH randomly rotates the high-energy CH position. These features balance power consumption among all nodes, extending the network's lifespan.

A. Possible Attacks On LEACH

Attacks are nothing more than the BS's failure to receive complete and reliable sensing data, which is particularly dangerous for wireless sensor networks. BS Most stable topography-based routing protocols can withstand sinkhole attacks to a certain extent. The group of SNs keeps a constant eye on their neighbors and forwards the sensing data to a BS or destination node.

The LEACH protocol is being considered for a variety of attacks, which significantly reduces its efficiency. Then there are the main LEACH attacks, which include the following:

- SF Attack
- HELLO Flood Attack
- Sybil Attack

VII. SF ATTACK IN WSN

Several system layer attacks occur in WSNs. Refusing to route packets gives SNs multi-hop advantages. Thus, it must be ongoing [35]. A neighboring node marking a path across the rogue node would not change messages. Wagner and Karlof discovered the SFA. SFA is a Gray Hole attack.

This assault targets multi-hop communication networks most often. In multi-hop communication, route exploration sends data to the destination or sink node [36], [37]. This attack will assault a node's route exploration, and one or more nodes will send data to the sink from the same node. This procedure quickly drains the SN, skewing the network [38]. Data may loop in the network to shorten its lifespan.

Malicious nodes reduce data packet transmission or drop them in a basic SFA technique. In a basic SFA, malicious nodes prevent email transmission or loss to stop network packets. Some SFAs exist. A rogue node can crash packets to create a group or a single node in one sort of SFA. If all packets are lost, this is a black hole attack. This conduct causes a DoS attack on that node or group.

Blind Letter attacks are another SFA. This attack assures that randomly hostile nodes relay packets to neighbors of the forward-hop node. Neglecting attacks ignore reception sources and lose data. Greedy attack prioritizes just one's own packets.

Figure 7 shows the selective forwarding attack model [39]. The sinkhole attack is a popular WSN attack. In the sensor community, the SN is closer to the BS than its Neighbour node and includes nearby nodes to send information to the BS. Malicious nodes copy and transfer data to sinks [40]. As a result, the malevolent and sink nodes lose resources quickly and sometimes send data to the attacker.

Malicious nodes take corrupted paths [41]. The compromised path is low-energy, and this attack is being extensively researched.

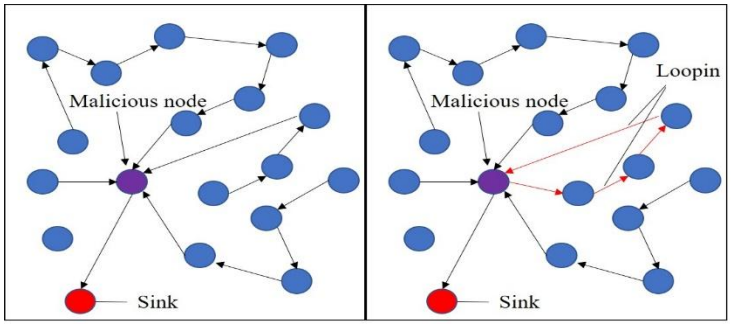

Figure 7: Selective Forwarding Attack

A. Detection Technique for Selective Forwarding Attack

Defense against SFA. Control packet collection, assault prevention, neighbor monitoring, review, and new direction. The first process tracks packets discarded, delivered, or retrieved by the BS. The second stage compares packet sequence numbers to detect BS intrusions. This is easy to spot because the BS increments packet drop counts. Control packets are inserted in the third stage when the BS requests them [42]. The BS uses control packets to identify

defamatory nodes. The BS checks control packet transfers during review. After sending damning node information, the BS submits a fresh path request without them. Existing attack research is shown in Table 2.

Table 2: Summary of existing works on attacks

S. No.	Year	Authors	Literature	Technique description
1.	2015	Mayur et al.	"Security Enhancement on LEACH Protocol From HELLO Flood Attack in WSN Using LDK Scheme" [43]	A Hello flood attack detection algorithm is proposed by updating the LEACH protocol in such a way that it operates efficiently for small networks.
2.	2015	Keerthana et al.	"A Study on Sinkhole Attack Detection using Swarm Intelligence Techniques for Wireless Sensor Networks" [44]	The particle swarm optimization strategy, also known as swarm intelligence, is a useful method for detection sink hole attacks.
3.	2016	Anand et al	"Localized DoS Attack Detection Architecture for Reliable Data Transmission Over Wireless Sensor Network" [45]	The Intrusion Detection Method (IDS) was introduced in this paper as a solution to DoS attacks.
4.	2016	Mathur et al.	"Defence against black hole and selective forwarding attacks for medical WSNs in the IoT" [46]	Mechanism suggested here is 96% effective with increased accuracy compared to the SFA.
5.	2016	Khanderiya et al.	"A Novel Approach for Detection of Sybil Attack in Wireless Sensor Networks" [47]	In this article, the AODV protocol is applied to detect Sybil attacks. Since only single node is used in the detection algorithm, this approach is energy efficient.
6.	2016	Parmar et al.	"Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol" [48]	Wormhole attacks are prevented and detected using the AOMDV and RTT protocols.
7.	2016	Takash et al.	"Poster: Detection of Wormhole Attack on Wireless Sensor Networks in Duty-Cycling Operation" [49]	The wormhole attack is detected using the time difference.
8.	2017	Devibala et al.	"Flow Based Mitigation Model for Sinkhole Attack in Wireless Sensor Networks using Time-Variant Snapshot" [50]	The approach suggested here increases network execution and decreases network overhead.

B. Countermeasures for Selective forwarding attack

The malicious node loses several packets, referred to as selected packets, during selective forwarding. The attacker has lost these packets on purpose. Dropping packets causes the network's reputation to deteriorate, as well as its performance. The following are some potential detection countermeasures for SFA:

Heterogeneous sensor head deployment: Brown et al. [51] suggest an approach that consider heterogeneous sensor networks as well as the implementation of certain low-cost sensors. The CH that shapes after sensor positioning are known as heterogeneous sensors. This data transfers to Head sensors by Low-end sensors if a packet is lost.

Head sensors run a test based on the details they've got to see if there's a vulnerable node. The test is known as the "Sequential Probability Ratio." For the identification of malicious nodes, encryption and decryption are performed at head sensors and low-end sensors, correspondingly, for security reasons.

Multi Flow Topologies: This scheme was suggested by Hung Min-Sun et al. [52] where multi flow topologies are applied to prevent the attack. The technique entails the construction of various data topologies across the network. A SN in one topology can only communicate data to other SNs in that topology. The scheme works on the premise that each topology entirely covers the sensing field, which might not be the case in some situations.

Acknowledgement based detection: In network, each node in the network is controls the detection of abnormal node in Acknowledgement dependent detection [53]. Three types of packets are used in the identification process: Alarm Packet, Report Packet, and Acknowledgment Packet. For transmission, each packet has certain predefined values. ACK_TTL, ACK_cnt, and ACK_span are the three variables. When a node receives an alert packet with a value less than ACK_span, and ACK_TTL transmits it to the SN. However, the malicious node in the network is identified by the SN.

VIII. PROBLEM FORMULATION

The work of Hai Zhou et al. (2016) is being evaluated for enhancement, where “IN (Inspector Node), MNs (Member Nodes), and CH (Cluster head)” are considered. The inspector node tracks the cluster head's transmission to secure the cluster against an SFA; the cluster head transmits packets from member nodes and other cluster heads and tests the inspector node regularly to ensure its proper operation; and the member nodes send data packets to the cluster head and check the IN's and cluster head actions using their reputation system. The author's technique's main issues include message/packet drop ratio, transmission delay, and energy efficiency.

The suggested technique improves the prior technique by making IN behave as the CH when malicious behavior is detected in the network. The suggested effort would detect and resolve harmful actions during current transmission to complete it.In this method, all nodes are separated into three types: MN, CH, and IN, with the inspector node tracking all CH and MN operations. The inspector node is trained on those standards, and the system gathers information based on the criteria, which the CH and MNs use to identify harmful behavior. After discovering the threat, the cluster head adjusts the routing protocol and member node routing to maintain data transmission.

IX. OBJECTIVES

The main objectives of research work shall be:

- To study and evaluate the domain areas study related to WSN,
- To study and evaluate the diverse types of attacks over WSN with special reference to selective forwarding attack,
- To diagnose the effect of the selective forwarding attack in the clustered network,
- To suggest a method for the recognition and diagnosis of the SFA in the clustered system,
- To evaluate the performance related comparison for proposed work and past techniques for performance parameters like delay time, packet loss, Throughput, Energy efficiency, etc.

X. RESEARCH METHODOLOGY

After going through the trouble of analyzing network safety methodologies and the existing literature, we found that cluster-based networks had a research gap. When the CH becomes corrupted and brings the network down, this is the most difficult aspect of cluster WSN. During a forwarding attack, the attacker takes control of a single node and causes data packets to be lost while they are being transmitted, creating a gaping hole in the network.

It is possible to divide the accessible nodes of a cluster network into three distinct categories: MN, CH, and IN. These node types are all interchangeable with one another. Because the cluster's radius encompasses about half of the network's transmission range, it is possible for any two nodes within the same network to communicate with one another.

The IN and CH in the network are determined by the CRV, with the highest CRV acting as the cluster head and the next node with second highest CRV value acting as the inspector node, and the computation is dependent on the forwarding rate and energy level of the nodes.

$$Val[node_{id}] = a * Pr_{id} + b * \frac{E_{else}}{E_0} \quad (1)$$

Where “a and b are specified constants with values ranging from 0<a,b<1, and a+b=1”. The original energy level of the network is E_0, and the excess energy of the nodes is Eelse. The CRV for the node is Val[nodeid], and Prid is the forwarding rate for the given node.

The cluster's radius is half the network's propagation range, allowing MNs to connect. Inspector node tracks CH and cluster head behavior to avoid malicious activities by the cluster head and other nodes. According to the composite reputation value, the cluster head has the highest value, and the inspector node has the second highest value, which is modified when the inspector node detects malicious behavior. The Inspector node watches cluster heads and other Member nodes for malicious behavior and updates the routing table if found.

The available nodes are having different part to play from which the IN is supposed to detect the activities of the cluster head node for which the IN is trained based on certain rules as under:

- Reception and delay rule: The sink must accept the entire data packets from MNs and the CH within a certain time limit, otherwise the attack will occur.
- Sub-list of Cluster Head member’s rule: If the Cluster head does not have the full list of MNs from the first packet exchanged, then an attack is suspected.
- Information loss rule: The CH transmit a control packet to the sink at the start of the communication that contains clear information about inspector node and member node, and it should be assured that the relevant data about member node is exchanged, and accessible, else malicious behaviour may occur.
- Time to react/Response time rule: After detecting the attack, the inspector node should report the cluster head and MN response rates and, if any odd symmetry is discovered, take all required actions.

CH: As previously described, in a cluster WSN, the CH performs a critical part in whole communication. The Cluster head manage the communication at levels 1 and 2, and if the cluster head is corrupted, the cluster as a whole goes down.

MN: MNs are in charge of data transfer and collection, as well as updating themselves with different energy needs and other network-related requirements. Member node are used to determine each node's CRV value, which is then used to describe the IN and CH. The complete working framework of the proposed system is us under:

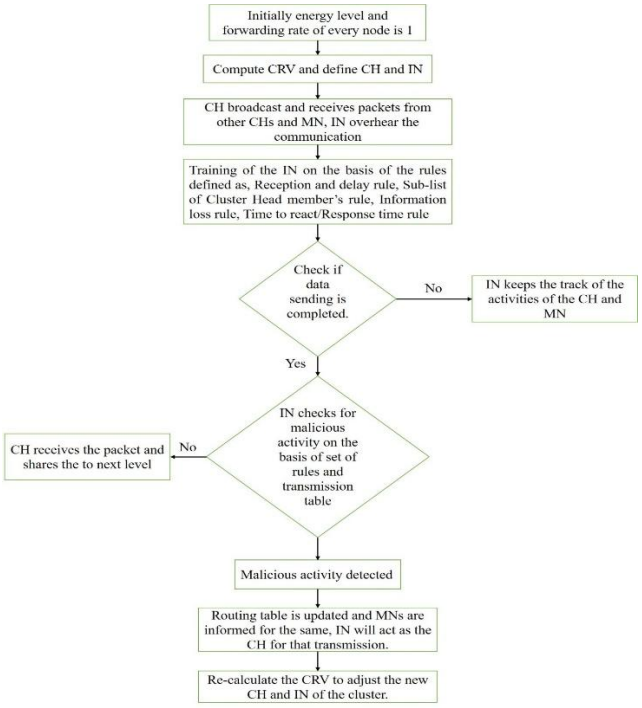

Figure 8: Proposed Methodology

XI. IMPLEMENTATION

In this model, a network is built in simulation, with a huge number of nodes and a cluster. The work shown here is for the recognition and resolution of a SF attack in a cluster-based WSN. The entire methodology is modelled in the MATLAB tool, and the work is supported centered on specific implementation-connected parameters such as energy consumption, throughput, packet delivery ratio, and how cluster head and inspector nodes are chosen.

Result 1: In the proposed methodology 2 cluster modules were taken as shown in figure 9. Here, at first stage all the nodes were defined.

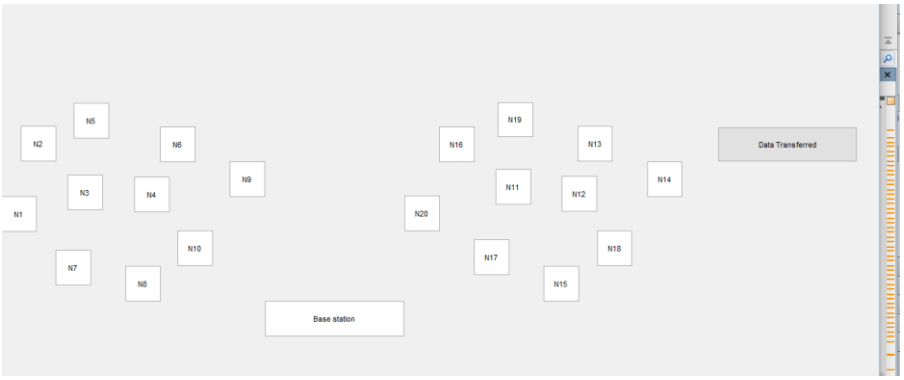

Figure 9: Node initialization

Result 2: In the proposed methodology 2 cluster modules were taken as shown in figure 10. Here, at first stage all nodes initially having value "1".

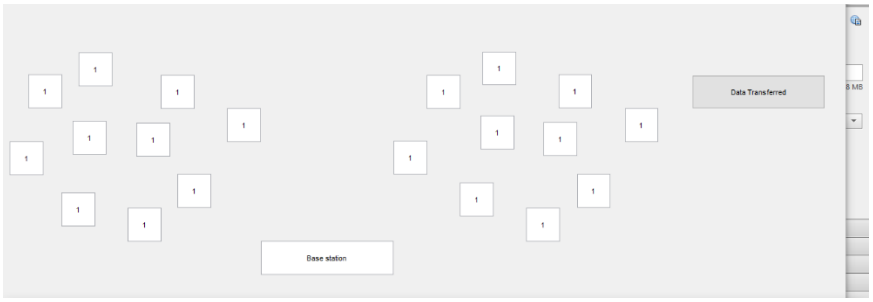

Figure 10: Nodes with initial values

Result 3: The suggested approach divides the whole set of nodes into three categories: member nodes (MNs), cluster heads (CH), and inspector nodes (IN). A single node is designated as the cluster head in each cluster, and it is responsible for all communication both inside and outside the cluster. With the aid of a learning process, the Inspector node is intended to listen in on every communication in the cluster and be accountable for the MNs' and CH's harmful behaviour. The rest of the nodes in the cluster are called member nodes. In a network, IN and CH node selected by computing CRV value of each node as shown in this result. Figure 11 represent the computed CRV value of each node for identification of CH and IN node.

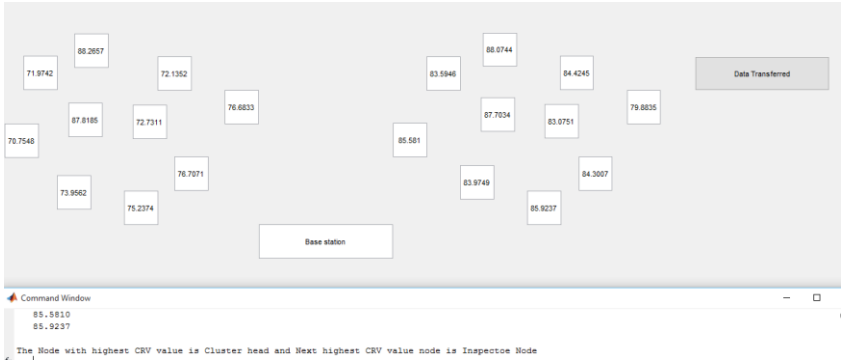

Figure 11: Nodes and their respective CRV value

Result 4: IN is anticipated to overhear the full transmission through CH or from any of the MNs in the current situation and recognize CH if no harmful behavior is observed based on the training criteria, which helps IN detect malicious activity. Figure 12 shows that the inspector node (IN) has the 2nd highest CRV value and CH is the maximum. The first cluster has CH and CRV values of 88.2657 and 87.8185, while the second cluster has CH at 88.0704 and IN at 87.7034.

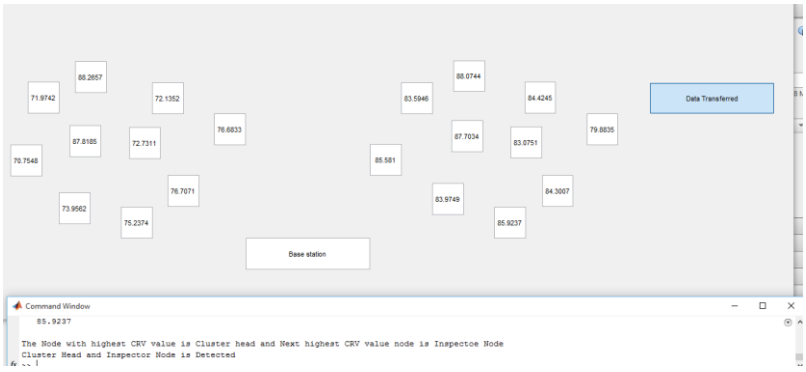

Figure 12: Decided CH node and IN node

Result 5: In figure 13 source and destination are allocated in both clusters from where data is transferred and received. In cluster 1 node with CRV value 70.7548 is source and node with CRV value 76.6833 is considered as destination. In cluster 2 node with CRV value 85.581 is source and node with CRV value 79.8835 is considered as destination.

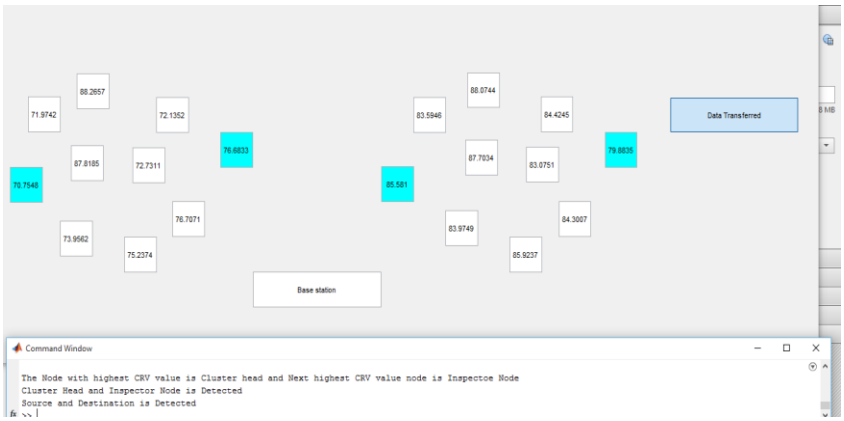

Figure 13: Selection of source and destination node

Result 6: In the figure 14 the training of IN is done on the basis of defined rule such as reception and delay rule, Sub-list of cluster head and members rule, information loss rule, time to react/response time rule.

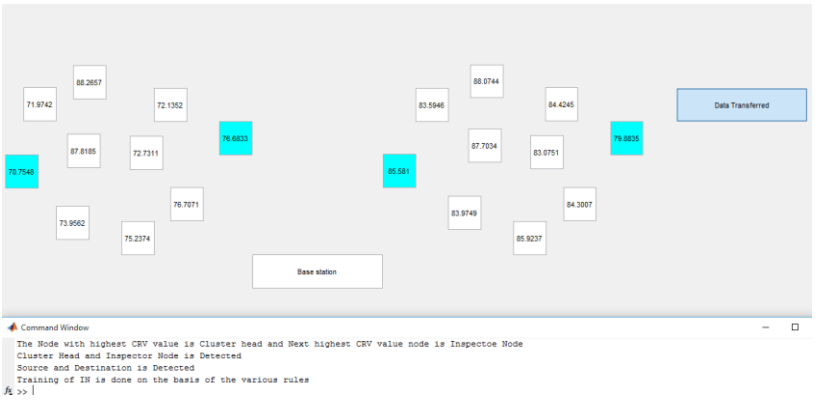

Figure 14: Training of IN

Result 7: In figure 15 the complete data transfer is done without any interruption. During the transmission process there is no malicious activity detected. Here in the given condition data is transferred from source of cluster 1 to destination of cluster 2.

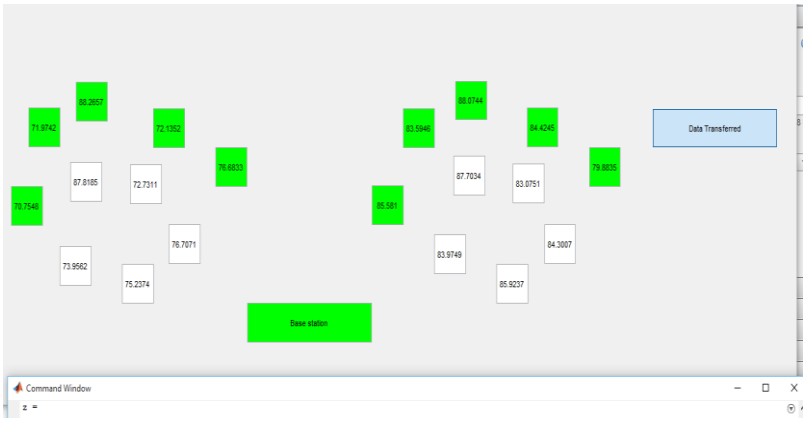

Figure 15: transmission without malicious activity

Result 8: In figure 16 malicious activity is detected and CH is found as malicious in cluster 1 in the path that is decided for the data transmission.

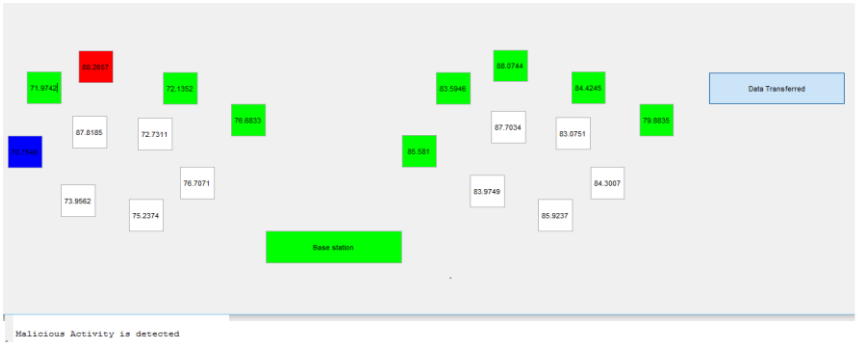

Figure 16: CH detected as malicious

Result 9: In the figure 17 the next optimum path is selected for the data trasnmission as the previous path is having malicious activinty then this path is used and there is no malicious activity detected during the transmission of the data.

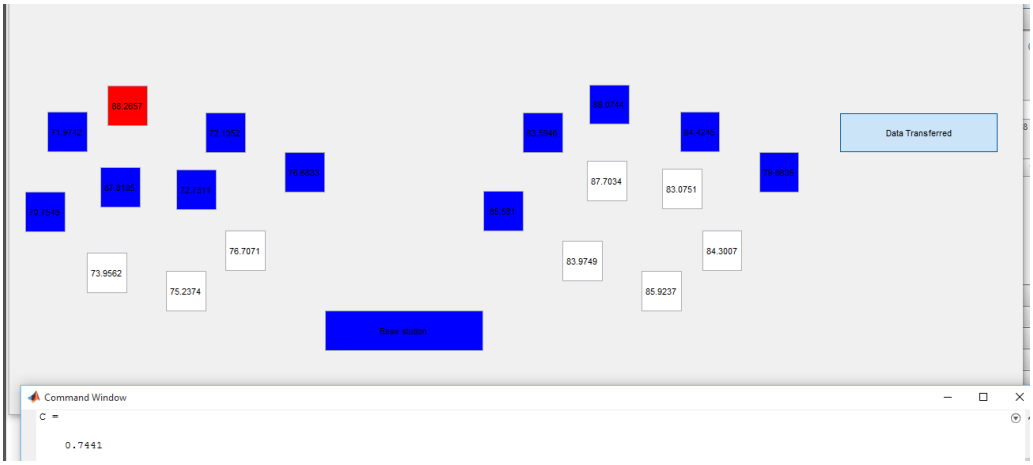

Figure 17: Data transmission through next path

Result 10: The figure 18 shows that the trasnmission of data is successfully done from the another selected path with no malicious activity has been found.

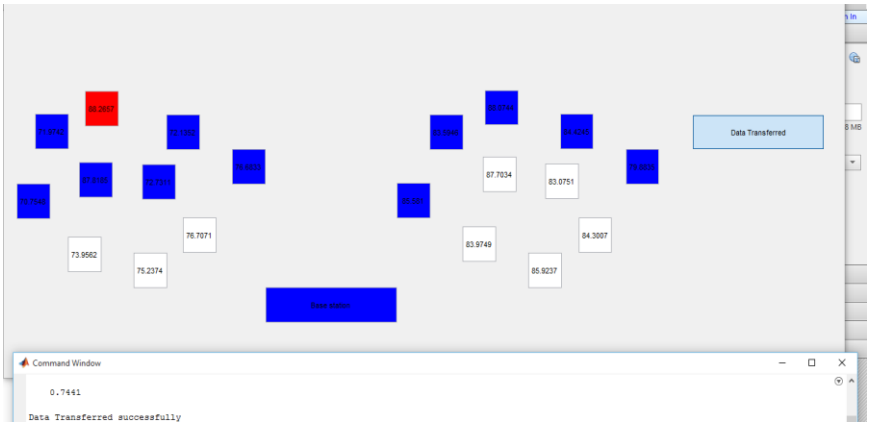

Figure 18: Data transferred successfully

Result 11: Figure 19 represent the energy consumption of the WSN network in existing system [54] in blue color and proposed system is shown in red color. This result proves that the proposed design is more energy efficient than the existing result.

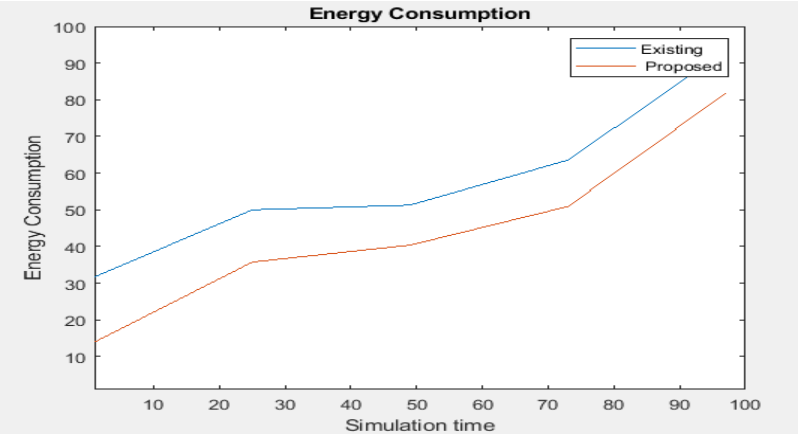

Figure 19: Energy Consumption

Result 12: Throughput is the rate at which packet is sent through the network from node1 to node 2. In figure 20, orange line shows the proposed throughput which contains 90 as maximum value and blue line shows the existing Throughput which contains 85 as maximum value.

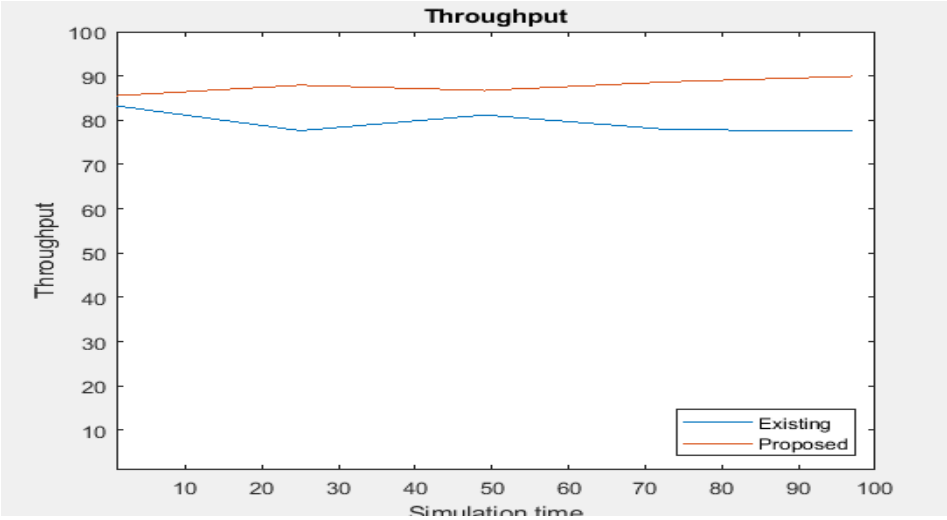

Figure 20: Throughput

Result 13: PDR is specified as the quantitative connection among the supply packets produced and the packets obtained at the destination. To calculate the proper results, divide the total number of packets at the destination by the total number of packets generated at the source node, then multiply the result by the percentage given below. As illustrated in Figure 21, the PDR is the proportion of total packets delivered to total packets sent from source to destination nodes in the network.

$$PDR= (td/ts)* 100 \quad (2)$$

where, "P D R is the packet delivery ratio, td is the total number of packets at the destination, and ts is the total number of packets generated at the source code". In figure 16 the blue line shows the proposed Packet Delivery Ratio which contains 95 as maximum value and orange line shows the existing Packet Delivery Ratio which contains 85 as maximum value.

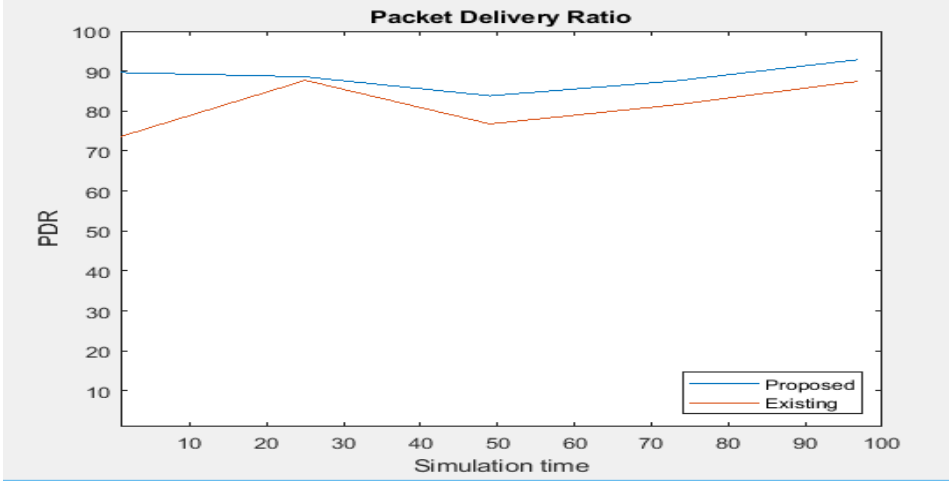

Figure 21: Packet Delivery Ratio

A. Performance Analysis

The given comparative study in table 3 is done with proposed work and already existing work [54].

Table 3: comparative study of Performance Parameters

Parameters	Simulated Result			
	Proposed Result		Existed Result	
	Min. Value (approx.)	Max. Value (approx.)	Min. Value (approx.)	Max. Value (approx.)
Energy Consumption	15	80	30	90
Throughput	85	90	78	80
Packet delivery ratio	89	95	72	85

XII. CONCLUSION AND FUTURE SCOPE

The use of wireless technology in place of wired networks in communication is becoming increasingly common. WSNs, on the other hand, are swiftly becoming a popular area of research within the realm of wireless networks, and many innovations are beginning to embrace them. WSNs are networks that are easy to set up, intelligent, relatively small, and inexpensive. Sensor systems have limitations when it comes to the amount of battery power, memory, and processing capacity they can use. According to the findings of the research, WSN can be used to a number of different

uses in this paper. WSNs are vulnerable to many different kinds of attacks due to the fact that they function as open networks with limited resources at each node.

They are also more susceptible to dangers as a result of the open and dispersed structure of the networks as well as the limited resources of the individual nodes. The first section of the study provided a high-level summary of the properties as well as the design of wireless sensor networks (WSNs). The paper then moves on to analyze the SF attack and the countermeasures that can be taken against it in clustered WSNs. In addition, various machine learning strategies for protecting clustered WSNs are presented in this article as well.

Because wireless networks are more susceptible to attacks, there is an undeniable need to develop protection measures that are dependable and more effective in order to make wireless networks more stable and guarantee that the data maintained within those networks is handled in a manner that is completely secure and secret. The findings of the simulation reveal a selective forwarding attack in WSN. The energy consumption in WSN architecture, throughput, and packet delivery ratio are also examined, and a comparison is made with previously obtained results.

As a consequence of this, new approaches ought to be developed while taking into consideration the computing, energy, and processing power of clustered WSN nodes. Because they have a variety of drawbacks, the approaches that are currently being used will also need to be modified. In the not-too-distant future, wireless sensor networks will be established nearly everywhere, which will make it necessary to make significant efforts to lessen the risk of SFA attack.

XIII. CONFLICT OF INTEREST STATEMENT

None of the authors have a conflict of interest to disclose

REFRENCES

[1] Naik, Anil S., and R. Murugan. "Security attacks and energy efficiency in wireless sensor networks: A survey." International Journal of Applied Engineering Research 13, no. 1 (2018): 107-112.
[2] Zhou, Haibo, Yuanming Wu, Yanqi Hu, and Guangzhong Xie. "A novel stable selection and reliable transmission protocol for clustered heterogeneous wireless sensor networks." Computer communications 33, no. 15 (2010): 1843-1849.
[3] Yinghong, Liu, Wu Yuanming, and Chang Jianyu. "The Diffusion Clustering Scheme and Hybrid Energy Balanced Routing Protocol (DCRP) in Multi-hop Wireless Sensor Networks." Adhoc & Sensor Wireless Networks 43 (2019).
[4] Fu, Hao, Yinghong Liu, Zhe Dong, and Yuanming Wu. "A data clustering algorithm for detecting selective forwarding attack in cluster-based wireless sensor networks." Sensors 20, no. 1 (2020): 23.
[5] Yuanming, Wu. "An energy-balanced loop-free routing protocol for distributed wireless sensor networks." International Journal of Sensor Networks 23, no. 2 (2017): 123-131.
[6] Liu, Yinghong, and Yuanming Wu. "A key pre-distribution scheme based on sub-regions for multi-hop wireless sensor networks." Wireless Personal Communications 109, no. 2 (2019): 1161-1180.
[7] Chae, Younghun, Lisa Cingiser DiPippo, and Yan Lindsay Sun. "Trust management for defending on-off attacks." IEEE Transactions on Parallel and Distributed Systems 26, no. 4 (2014): 1178-1191.
[8] Lu, Zhuo, Yalin E. Sagduyu, and Jason H. Li. "Queuing the trust: Secure backpressure algorithm against insider threats in wireless networks." In 2015 IEEE Conference on Computer Communications (INFOCOM), pp. 253-261. IEEE, 2015.
[9] Gulhane, Gaurav, and Nikita Mahajan. "Performance evaluation of wireless sensor network under black hole attack." Int. J. Comput. Technol 1 (2014): 92-96.
[10] Zhou, Hai, Yuanming Wu, Li Feng, and Daolei Liu. "A security mechanism for cluster-based WSN against selective forwarding." Sensors 16, no. 9 (2016): 1537.
[11] He, Jing, Shouling Ji, Yi Pan, and Yingshu Li. "Greedy construction of load-balanced virtual backbones in wireless sensor networks." Wireless Communications and Mobile Computing 14, no. 7 (2014): 673-688.
[12] Maraiya, Kiran, Kamal Kant, and Nitin Gupta. "Wireless sensor network: a review on data aggregation." International Journal of Scientific & Engineering Research 2, no. 4 (2011): 1-6.
[13] Lee, Sookyoung, Mohamed Younis, and Meejeong Lee. "Connectivity restoration in a partitioned wireless sensor network with assured fault tolerance." Ad Hoc Networks 24 (2015): 1-19.

[14] Lee, Sang Hyuk, Soobin Lee, Heecheol Song, and Hwang Soo Lee. "Gradual cluster head election for high network connectivity in large-scale sensor networks." In 13th International Conference on Advanced Communication Technology (ICACT2011), pp. 168-172. IEEE, 2011.
[15] Kumar, Raj, and Kirti Walia. "Wireless Sensor Networks: A Study on Security Goals and Issues."
[16] Cho, Youngho, Gang Qu, and Yuanming Wu. "Insider threats against trust mechanism with watchdog and defending approaches in wireless sensor networks." In 2012 IEEE symposium on security and privacy workshops, pp. 134-141. IEEE, 2012.
[17] Gulhane, Gaurav, and Nikita Mahajan. "Performance evaluation of wireless sensor network under black hole attack." Int. J. Comput. Technol 1 (2014): 92-96.
[18] Chae, Younghun, Lisa Cingiser DiPippo, and Yan Lindsay Sun. "Trust management for defending on-off attacks." IEEE Transactions on Parallel and Distributed Systems 26, no. 4 (2014): 1178-1191.
[19] Lu, Zhuo, Yalin E. Sagduyu, and Jason H. Li. "Queuing the trust: Secure backpressure algorithm against insider threats in wireless networks." In 2015 IEEE Conference on Computer Communications (INFOCOM), pp. 253-261. IEEE, 2015.
[20] Butun, Ismail, Salvatore D. Morgera, and Ravi Sankar. "A survey of intrusion detection systems in wireless sensor networks." IEEE communications surveys & tutorials 16, no. 1 (2013): 266-282.
[21] Liao, Hongmei, and Shifei Ding. "Mixed and continuous strategy monitor-forward game based selective forwarding solution in WSN." International Journal of Distributed Sensor Networks 11, no. 11 (2015): 359780.
[22] Hu, Yu, Yuanming Wu, and Hongshuai Wang. "Detection of insider selective forwarding attack based on monitor node and trust mechanism in wsn." Wireless Sensor Network 6, no. 11 (2014): 237.
[23] Cui, Biru, and Shanchieh Jay Yang. "NRE: Suppress selective forwarding attacks in wireless sensor networks." In 2014 IEEE Conference on Communications and Network Security, pp. 229-237. IEEE, 2014.
[24] Stavrou, Eliana, and Andreas Pitsillides. "Recovering from the selective forwarding attack in WSNs-enhancing the recovery benefits of blacklisting and rerouting using directional antennas." In 2014 International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 299-303. IEEE, 2014.
[25] Hu, Yu, Yuanming Wu, and Hongshuai Wang. "Detection of insider selective forwarding attack based on monitor node and trust mechanism in wsn." Wireless Sensor Network 6, no. 11 (2014): 237.
[26] Ho, Jun-Won, Matthew Wright, and Sajal K. Das. "Distributed detection of mobile malicious node attacks in wireless sensor networks." Ad Hoc Networks 10, no. 3 (2012): 512-523.
[27] Fu, Hao, Yinghong Liu, Zhe Dong, and Yuanming Wu. "A data clustering algorithm for detecting selective forwarding attack in cluster-based wireless sensor networks." Sensors 20, no. 1 (2020): 23.
[28] Dr. Shreenath K N, Manasa V M "Black Hole Attack detection in Zone based WSN" International Journal on Recent and Innovation Trends in Computing and Communication, pp 148–151, Volume:5, Issue:4, April 2017
[29] Anand, C., and R. K. Gnanamurthy. "Localized DoS attack detection architecture for reliable data transmission over wireless sensor network." Wireless Personal Communications 90, no. 2 (2016): 847-859.
[30] Nagireddy, Vyshnavi, and Pritee Parwekar. "Attacks in Wireless Sensor Networks." In Smart Intelligent Computing and Applications, pp. 439-447. Springer, Singapore, 2019.
[31] Elma, K. Johny, and S. Meenakshi. "Energy efficient clustering for lifetime maximization and routing in WSN." International Journal of Applied Engineering Research 13, no. 1 (2018): 337-343.
[32] Mundada, Monica R., Savan Kiran, Shivanand Khobanna, Raja Nahusha Varsha, and Seira Ann George. "A study on energy efficient routing protocols in wireless sensor networks." International Journal of Distributed and Parallel Systems (IJDPS) 3, no. 3 (2012): 311.
[33] Krontiris, Ioannis, Thanassis Giannetsos, and Tassos Dimitriou. "Launching a sinkhole attack in wireless sensor networks; the intruder side." In 2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, pp. 526-531. IEEE, 2008.
[34] Newsome, James, Elaine Shi, Dawn Song, and Adrian Perrig. "The sybil attack in sensor networks: analysis & defenses." In Third international symposium on information processing in sensor networks, 2004. IPSN 2004, pp. 259-268. IEEE, 2004.
[35] Bysani, Leela Krishna, and Ashok Kumar Turuk. "A survey on selective forwarding attack in wireless sensor networks." In 2011 International Conference on Devices and Communications (ICDeCom), pp. 1-5. IEEE, 2011.
[36] Ren, Ju, Yaoxue Zhang, Kuan Zhang, and Xuemin Shen. "Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks." IEEE Transactions on Wireless Communications 15, no. 5 (2016): 3718-3731.

[37] Yaseen, Qussai, Firas Albalas, Yaser Jararwah, and Mahmoud Al-Ayyoub. "Leveraging fog computing and software defined systems for selective forwarding attacks detection in mobile wireless sensor networks." Transactions on Emerging Telecommunications Technologies 29, no. 4 (2018): e3183.
[38] Lim, Sunho, and Lauren Huie. "Hop-by-Hop cooperative detection of selective forwarding attacks in energy harvesting wireless sensor networks." In 2015 International Conference on Computing, Networking and Communications (ICNC), pp. 315-319. IEEE, 2015.
[39] Vignesh Ramamoorthy, H., and R. Gunavathi. "Survey on Discovery Practices of Black Hole Attack in Wireless Sensor Networks."
[40] Han, Guangjie, Jinfang Jiang, Ning Sun, and Lei Shu. "Secure communication for underwater acoustic sensor networks." IEEE communications magazine 53, no. 8 (2015): 54-60.
[41] Shuai, Xiang. "Research on sinkhole attack and intrusion detection method in GPSR geographic routing protocol." Electronic Test 12 (2016): 85.
[42] Mathur, Avijit, Thomas Newe, and Muzaffar Rao. "Defence against black hole and selective forwarding attacks for medical WSNs in the IoT." Sensors 16, no. 1 (2016): 118.
[43] Mayur, S., and H. D. Ranjith. "Security enhancement on LEACH protocol from HELLO flood attack in WSN using LDK scheme." International Journal of Innovative Research in Science, Engineering and Technology 4, no. 3 (2015).
[44] Keerthana, G., and G. Padmavathi. "A study on sinkhole attack detection using swarm intelligence techniques for wireless sensor networks." IRACST Int. J. Comput. Sci. Inf. Technol. Secur.(IJCSITS) 5, no. 5 (2015).
[45] Anand, C., and R. K. Gnanamurthy. "Localized DoS attack detection architecture for reliable data transmission over wireless sensor network." Wireless Personal Communications 90, no. 2 (2016): 847-859.
[46] Mathur, Avijit, Thomas Newe, and Muzaffar Rao. "Defence against black hole and selective forwarding attacks for medical WSNs in the IoT." Sensors 16, no. 1 (2016): 118.
[47] Khanderiya, Mirali, and Mital Panchal. "A Novel Approach for Detection of Sybil Attack in Wireless Sensor Networks." IJSRSET 2, no. 3 (2016): 113-117.
[48] Amish, Parmar, and V. B. Vaghela. "Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol." Procedia computer science 79 (2016): 700-707.
[49] Amish, Parmar, and V. B. Vaghela. "Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol." Procedia computer science 79 (2016): 700-707.
[50] Devibala, Kannan, Saminathan Balamurali, Ayyanar Ayyasamy, and Maruthavanan Archana. "Flow based mitigation model for sinkhole attack in wireless sensor networks using time-variant snapshot." International Journal of Advances in Computer and Electronics Engineering 2, no. 05 (2017): 14-21.
[51] Brown, Jeremy, and Xiaojiang Du. "Detection of selective forwarding attacks in heterogeneous sensor networks." In 2008 IEEE International Conference on Communications, pp. 1583-1587. IEEE, 2008.
[52] Sun, Hung-Min, Chien-Ming Chen, and Ying-Chu Hsiao. "An efficient countermeasure to the selective forwarding attack in wireless sensor networks." In TENCON 2007-2007 IEEE Region 10 Conference, pp. 1-4. IEEE, 2007.
[53] Singh, Moutushi, Rupayan Das, Mrinal Kanti Sarkar, Koushik Majumder, and Subir Kumar Sarkar. "KT3F: A Key-Based Two-Tier Trust Management Filtering Scheme for Intrusion Detection in Wireless Sensor Network." In Proceedings of the Second International Conference on Computer and Communication Technologies, pp. 679-690. Springer, New Delhi, 2016.
[54] Kamble, Swapnil B., and Vivek V. Jog. "Efficient key management for dynamic wireless sensor network." In 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), pp. 583-586. IEEE, 2017.