International Journal of Computing and Artificial Intelligence

E-ISSN: 2707-658X
P-ISSN: 2707-6571
www.computersciencejournals.com/ijcai
IJCAI 2025; 6(1): 200-207
Received: 14-01-2025
Accepted: 17-02-2025

Jagathese G Chelladurai
Research Scholar, Department of Computer Science, Mansarovar Global University Bhopal, Madhya Pradesh, India

Dr. Mona Dwivedi
Research Guide, Department of Computer Science, Mansarovar Global University Bhopal, Madhya Pradesh, India

Corresponding Author:
Jagathese G Chelladurai
Research Scholar, Department of Computer Science, Mansarovar Global University Bhopal, Madhya Pradesh, India

To detect (D) worm hole attack in wireless sensor network from various kind of attack

Jagathese G Chelladurai and Mona Dwivedi

DOI: https://www.doi.org/10.33545/27076571.2025.v6.i1c.155

Abstract
This chapter analyzes wormhole variations and their effects on wireless sensor networks. Additionally, a review of current defenses against wormhole variations such sinkholes, service denial, black holes, etc. is provided. Wormhole attacks based on sinkholes are covered in Section 1.1. Wormhole attacks based on denial of service are covered in Section 1.2. Wormhole attacks based on black holes are covered in Section 1.3. We covered current defenses against different wormhole assaults in section 1.4. presents the effects of wormhole assault variations.
The smart attack detection strategy, which is used to identify the many types of denial of service assaults in wireless ad hoc networks, has been offered as a novel method to circumvent this problem. Four different sorts of assaults may be detected using this clever attack detection technique.
Generally speaking, identifying the different harmful attack types is more crucial than identifying bad nodes. This method allows one to identify the kind of harmful assault and then create the ideal future remedy. The botnet attack, black hole assault, worm hole attack, and sink hole attack have all been identified using the smart attack detection technique. When the overflow occurs to the specific node, a botnet assault will take place.

Keywords: Wormhole attack, wireless sensor networks, worm hole, secured energy efficient technique

1. Introduction
Wormhole is an extremely risky assault since it serves as a doorway to several more attacks. An attacker can draw in traffic, examine it, discard packets, and change the contents of the packet after building the wormhole tunnel. [4] This chapter analyzes wormhole variations and their effects on wireless sensor networks. Additionally, a review of current defenses against wormhole variations such sinkholes, service denial, black holes, etc. is provided. Wormhole attacks based on sinkholes are covered in Section 1.1. Wormhole attacks based on denial of service are covered in Section 1.2. Wormhole attacks based on black holes are covered in Section 1.3. We covered current defenses against different wormhole assaults in section 1.4. presents the effects of wormhole assault variations.

1.1 Sinkhole based wormhole attack
In a [1] wormhole attack based on a sinkhole, the attacker draws traffic to it before selectively forwarding the packets. Two malicious nodes are present, one closer to the source and the other closer to the destination. One malicious node intercepts the route reply packet received by the des- tarnation node and routes it to another malicious node. This establishes a channel via malicious nodes.

1.2 Denial of service based wormhole attack
Request [5] packets are tunneled by a malicious node M1 to another malicious node M2. The malicious node M2 broadcasts to its surrounding nodes, and by way of those nodes, it is able to reach its target. Through the proper way, the surrounding nodes also get the route request. Due to the fact that it is a duplicate packet, it will be discarded by nearby nodes. As a result, it is unable to reach the desired location. Because they lack the reverse route, the nearby nodes are unable to relay the route reply packet when it is received by them from the destination.

1.3 Black hole based wormhole attack

To determine [8] the route to the destination, the source node broadcasts a route request packet. Immediately after passing via the tunnel and being intercepted by the malicious node M1, this packet is sent to the malicious node M2. M2 the malicious node sends it there. Route reply packets are sent by the destination node. The path between the source and the destination is formed through the tunnel once the source node gets this route reply packet via the tunnel. The malicious node will discard data packets delivered by the source node rather than sending them to the target. It develops a black hole assault. A hostile node intercepts a route reply packet and sends it to the target node T as part of an indirect black hole attack. It is sent to the source node by the destination node. The destination node is seen as the one hop neighbor by the source and other nearby nodes. The target node's journey to the destination is not entirely clear. As a result, packet dropping happens.

1.4 Countermeasures against variants of wormhole attacks

In [12], the authors developed a black hole assault detect ion approach based on unmanned aerial vehicles (UAVs). To determine if a node is a black hole or not, the sequential probability ratio test is performed. UAV travels through the network, stopping at each node. A node is referred to as a black hole node if messages are not received from it. Genuine nodes are considered as black hole nodes if the threshold is set too low. Black hole nodes are considered as real nodes if the threshold is set too high. In [14], authors examined a number of current black hole detection techniques. Each node in [9] monitors how its neighbors behave. Each node hears packets being sent by Based on the activity of its neighbors, the system recognizes the questionable nodes. The node notices its neighbor's improper behavior. The node is regarded as malevolent if the misbehavior entries go beyond the threshold. The following stage involves verifying all the suspect nodes. A different path is taken to deliver the verification messages to the root. Black hole attack detection in cluster-based wireless sensor networks was given by authors in [9]. All node IDs are stored in the cluster head's table. The sensor nodes must communicate the data within the timer's allotted duration. The packets won't be forwarded by the rogue node. The cluster head as a result notices it. The base station can identify a cluster head if it turns malignant. In [8], authors have simulated black hole and selective forwarding attack. For detecting the attack, the base station monitors all the sensor nodes as it has high resources compared to other sensor nodes. The detection method is also energy efficient as there is no extra burden on sensor nodes to detect the attack.

2. Impact of variants of wormhole

In NS2, the wormhole variations are emulated. Throughput and PDF are the variables that are measured. Both metrics are measured both in the absence of an assault and when one is present [12]. The ratio of packets delivered from the source to those delivered to the destination is known as the packet delivery fraction. The quantity of data packets transferred from the source node to the destination node per interval of time is referred to as throughput. The PDF and throughput findings for several wormhole attack variations are displayed in Tables.

Table 1: PDF and throughput for sinkhole based wormhole attack

	KBPS		PDF (Per)	
No of Nodes	**Without Attacks**	**With Attacks**	**Without Attacks**	**With Attack**
60	84	72.15	99.70	85.14
80	84.75	72.90	99.76	85.90
100	85.10	73.20	99.78	86.10

3. Wormhole detection in static WSN

A synchronized [11] clock, directional antenna, GPS, and fingerprinting device are only a few of the additional hardware requirements for some of the wormhole detection methods described in the literature. Some methods rely on a cryptographic system where the sensor node needs both the public and private keys for secure communication. Some methods spread a group of investigator nodes around the network to keep an eye on the network topology. The detection methods now in use are resource-intensive. Sensor nodes are constrained by resources. A simple method with high detection accuracy and little overhead must be created. In this chapter, we suggested a neighborhood-based wormhole detection method for static WSNs.

The suggested strategy is laid forth in Section 3.1. We demonstrated in Section 4 that two real neighbor nodes always have the same one hop neighbors. The experimental setup and network situation are presented in Section 3.1. Results and performance evaluation of the suggested The wormhole attack approach described in Section 3.2 has the ability to drop and manipulate packets. Nodes that are malicious can examine the traffic. Malicious nodes do not engage in the network for a brief initial period. Every node communicates a greeting with each of its neighbors. Any node that gets the hello message sends the reply message right away. Every node creates a list of its neighbors in this manner.

3.1 Experimental setup and network scenario

This part [15] provides a thorough explanation of the whole assessment technique, as well as the simulation environment and network scenario. In many scientific fields where experimental approaches are impractical and analytical methods are appropriate, simulation has shown to be a useful tool. The well-known NS2 simulator [12] was selected to perform performance analysis of our suggested solutions presented in this thesis primarily because it is a simulation tool that has been successfully used in numerous prior research studies, and the results have been validated and verified in [13, 3].

3.2 Results and performance analysis of proposed approach under wormhole attack

NAV denotes the average number of neighbors. NT denotes the total number of nodes. SID is a representation of ID size. The cost of storage needed to keep track of the neighbors is SIDNAV. The needed storage cost is SIDNAV in order to store the neighbors' neighbor list. The overall cost of storage

required for each node is equal to (SIDNAV + SIDNAV NAV). The storage cost for each node is 440 bytes if the ID size is 4 bytes and the average number of neighbors is 10. The proposed protocol requires extremely little memory, making it suitable for wireless sensor networks with limited resources. Below are the simulation results for the suggested strategy using the network situation described in Table.

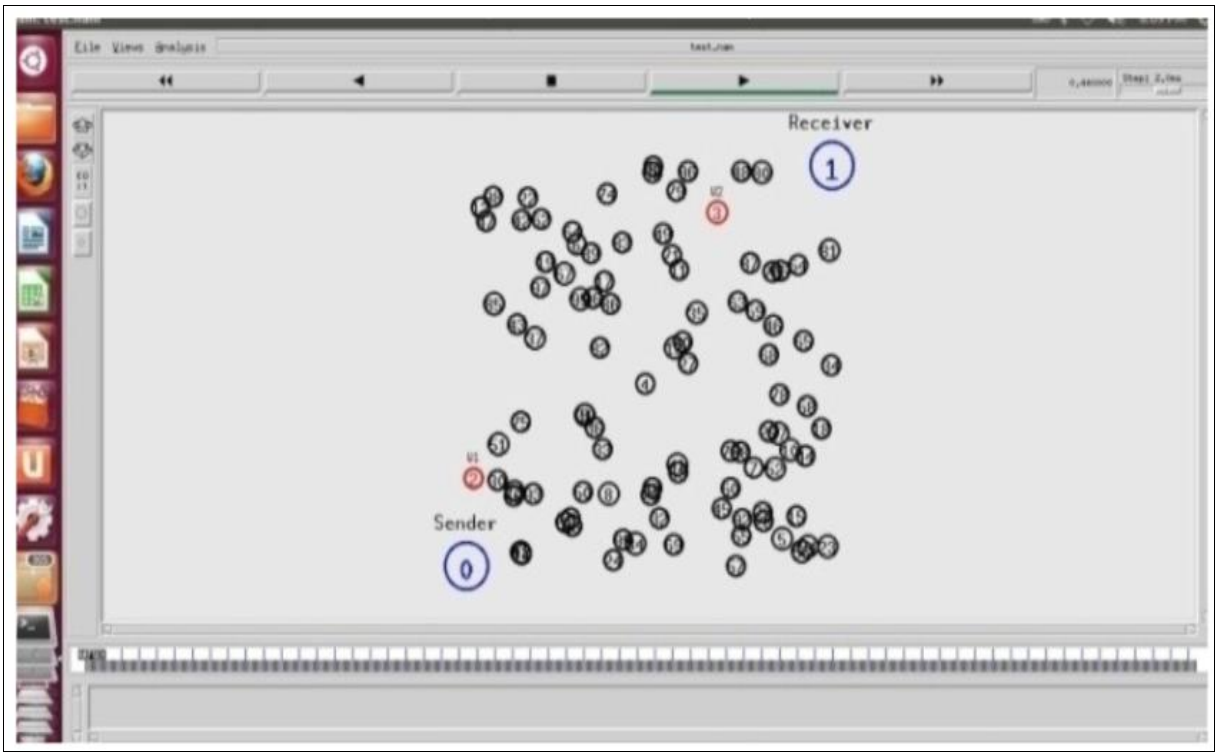

Fig 3.2: WA in dense network

The wormhole assault on the dense network is depicted in Figure 3.2. For dense networks, throughput (in KBPS) and PDF (in percentage) are measured. In a dense network, the PDF count is 99.78 (without an attack), 56 (with an attack), and 98.10 (with an assault) (after applying proposed approach). In the absence of an assault, throughput counts are 86 KBPS, 54 KBPS, and 84.70 KBPS (after applying proposed approach).

3.2 Wormhole Attack in Sparse Network: In a sparse network, the wormhole assault is depicted in Figure 3.3 Throughput (in KBPS) and PDF (in percentage) are measured. In a sparse network, the PDF count is 98.50 without an attack, 54.60 with an attack present, and 96.30 after an assault (after applying proposed approach). In the absence of an assault, throughput counts are 83.40 KBPS, 52.70 KBPS, and 82.10 KBPS (after applying proposed approach). When there is an assault, packet delivery ratio and throughput both drastically drop. Both the packet delivery ratio and throughput significantly increased after using the suggested approach.

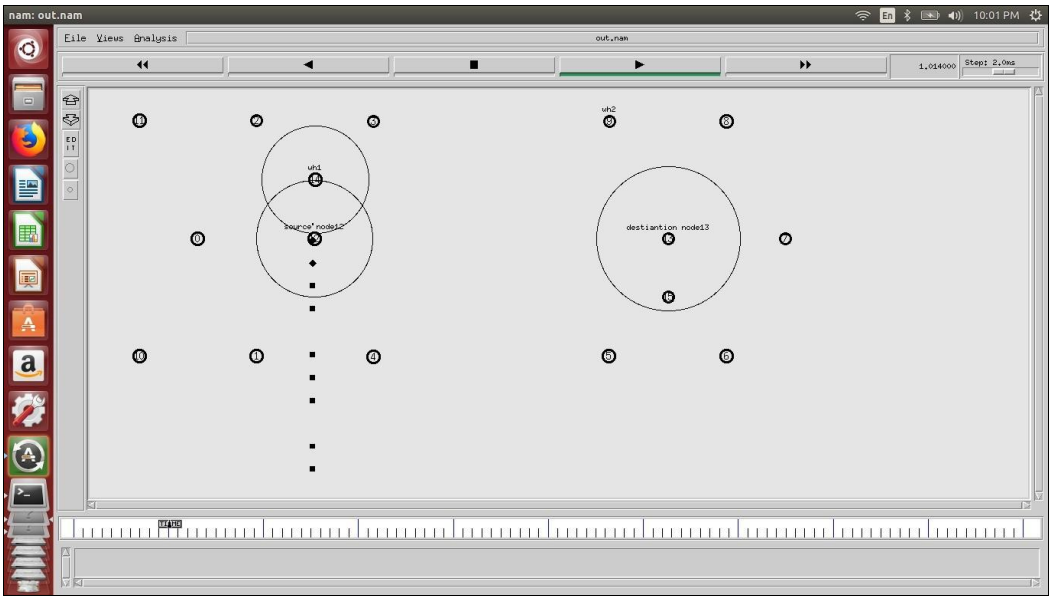

Fig 3.3: Wormhole attack (WA) in dense network

3.3 Detection Accuracy

Table 3.4 shows the detection accuracy of the P worm [14], RTT Based MDS [12], and our suggested technique for 1 pair of an attacker node. Our suggested technique consistently maintains detection accuracy between 0.97 and 0.99, whereas P worm detection accuracy drops to 0.80 to 0.91 and RTT Based MDS detection accuracy drops to 0.93 to 0.98.

Table 3.4: Accuracy analysis

No of Nodes	P Worm	RTT Base MDS	Approach
14	0.80	0.93	0.97
25	0.82	0.95	0.98
50	0.86	0.96	0.99
100	0.91	0.98	0.99

In a dense network, the suggested approach achieves a detection accuracy of 99 percent. All false positives have been eliminated. When a wormhole is launched for a short distance, false negatives happen. No formula-based threshold computation has been discovered. Hop count is represented by threshold here. Based on a trade-off between the false positives and detection rate, the appropriate value is chosen. With =1 or =2, we can find brief wormholes, but the number of false positives will rise. To disrupt the routing process, a wormhole attack is launched between two distantly placed nodes. Short wormholes are not discovered, despite the fact that the false positives are decreased by =4 or =5. Therefore, the threshold value chosen is 3, which will decrease false positives and boost detection accuracy. According to Fig. 3.4 is the ideal number for the trade-off between false positives and detection rate.

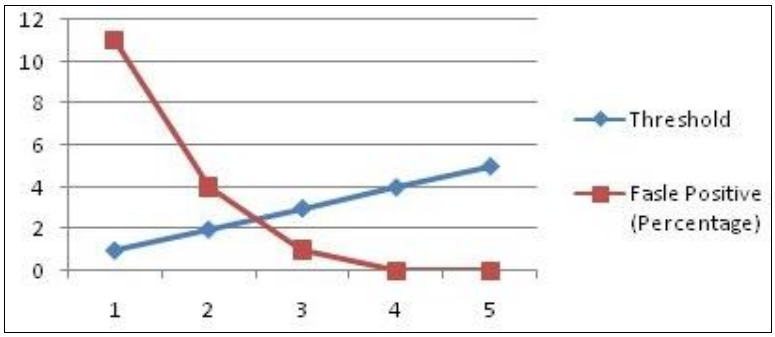

Fig 3.4: False positive with varying threshold value

In today's world, security is crucial in every industry, including wireless ad hoc networks. Due to the wireless medium's high degree of mobility, third parties can readily access the data and cause disruptions at both the source and the destination. The smart attack detection strategy, which is used to identify the many types of denial of service assaults in wireless ad hoc networks, has been offered as a novel method to circumvent this problem. Four different sorts of assaults may be detected using this clever attack detection technique.

[2] Generally speaking, identifying the different harmful attack types is more crucial than identifying bad nodes. This method allows one to identify the kind of harmful assault and then create the ideal future remedy. The botnet attack, black hole assault, worm hole attack, and sink hole attack have all been identified using the smart attack detection technique. When the overflow occurs to the specific node, a botnet assault will take place. When any intermediary node prevents the transfer of data to the target, a black hole attack will happen. When one of the attacking nodes disrupts the adjacent nodes, a wormhole attack will happen. Sinkhole attacks happen if an attacker node repeatedly bothers a neighboring node.

Table 3.5: Protection of WSN from Various Kinds of Attacks

Name of attack	Attacker type	Security attributes
Denial of Service (DOS)	Malicious, Active, Insider, Network	Availability
Black hole	Passive, Outsider	Availability
Malware	Malicious Insider	Availability
Sinkhole	Insider, Network Attack	Availability
Wormhole (or) Tunneling	Outsider, Malicious, Monitoring Attack	Availability

4. Protection of WSN from various kinds of attacks

Wireless [9] Sensor Networks (WSNs) are proving to be a promising technology in a variety of fields, including healthcare, industrial monitoring, environmental data recording, automobile, military applications, home automation, fire detection, and many more. This is due to the ease of use of features like small and low cost sensors deployment. In WSNs, a base station typically serves as the central coordinator and links and manages all of the other sensor nodes (SNs). The WSN is connected to the outside world through internet access, and the base station serves as the node that gathers data and facilitates further communication. Energy and electricity are a significant barrier to WSN operation. The majority of the energy used by WSNs goes toward communicating the detected data. Security is a crucial problem as well.

Routing among [10] the nodes is the aspect of WSN operation that causes the greatest consideration, and the reason for this is due to its adhoc setup and scalability features. Routing protocols in WSNs may be roughly categorized into three groups: location-based protocols, hierarchical protocols, and flat network protocols. Contrary to location-based protocols, which deliver data to a specific site based on position information rather than the whole network, all nodes in flat networks have the same capacity for sensing and routing data.

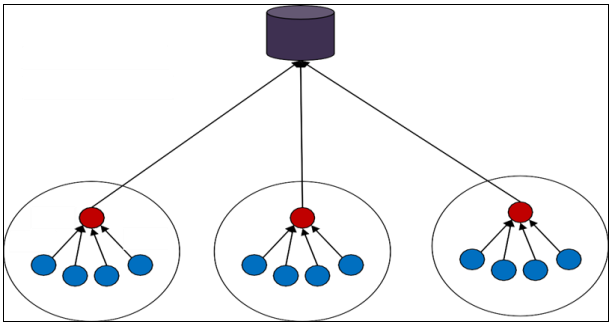

Fig 4: Normal data flow in WSN with three clusters and a base station

The goal of hierarchical protocols is to reduce the energy needed by individual nodes for data routing to base stations. Clustering, in which the WSN is separated into several clusters as illustrated in Figure 4, is one of the finest options. A cluster head election is conducted for each individual cluster in order to choose the person who will be in charge of gathering data from the cluster's sensor nodes and transmitting it to the sink node. There are several different selection criteria for cluster heads. Selecting a node with more energy or residual energy is the method that is most frequently utilized. The main goal is to decrease the amount of data transfers in order to prolong the lifespan of WSNs. Communication in clustering may be separated into two phases: both intra-cluster and inter-cluster communication Intra Cluster Communication: The transfer of information from sensor nodes inside a cluster to the cluster head. Depending on the number of nodes and the region chosen for a cluster, communication between sensor nodes and the cluster head may occur in a single hop or multichip. Inter-cluster communication: In this sort of communication, the cluster head sends the base station aggregated data gathered from the cluster's sensor nodes. Since cluster heads directly connect with the base station, single hop communication is typically used in inter-cluster communication. When more energy efficiency is needed, multichip transmission may be used in specific situations.

4.1 Black hole attack in Wsn

This is one of the most recent attacks where the attacking node decodes itself and claims to have the shortest path. Following such notice, the remaining nodes forward the data to the attacking node for onward transmission. After receiving the data packets, the attacking node removes them, depriving the requesting node of the most fundamental service. The most energy-efficient method of transmitting sensed data to sink node is through the cluster-based structure of WSN. Black hole nodes in cluster-based WSNs advertise that they have the maximum energy and ideal distance to the base station to increase their appeal as candidates for cluster heads. Black hole nodes start discarding data packets meant for base stations once they become CHs, which has a significant impact on quality of service characteristics.

5. Detection and prevention methodology for black hole attack in WSN

For the [7] identification and prevention of black hole attacks in WSNs, a novel approach called Secured Energy Efficient Technique (SEET) is proposed. In SEET, a brand-new notion called an associate cluster head (ACH) is presented in an effort to save energy and defend against black hole assault. Figure 5.2 depicts a typical data flow with the presence of ACH in a cluster-based WSN. a WSN with a base station, three clusters, and nodes. There are four sensor nodes in each cluster (SN1, SN2, SN3, and SN4), three cluster heads (CH1, CH2, and CH3), and two associate cluster heads (ACH1, ACH2, and ACH3). After gathering the data in each cluster, the sensor nodes send it to the ACH for that cluster. After receiving the data from the sensor nodes, the ACH aggregates it and sends it to the appropriate CH.

In contrast [14] to LEACH, CH and ACH share the tasks of CH, and it also optimizes the communication distance between CH and SNs, which results in an extension of CH's life. Data flow under a black hole attack. Sink node is not getting any data from CH1, despite CH1 receiving data from ACH1. When ACH1 does not hear back from BS within a predetermined amount of time, it checks the status of CH1 and notifies BS of that state. BS needs to take more action. Because blocking a lot of data increases the efficacy of an attack, CHs always have a higher chance of becoming a black hole node. Black hole attacks have a significant influence on WSN performance, particularly on throughput and end-to-end latency.

5.1 Performance evaluation of seet

Using [12] the NS-2 network simulator, the performance of WSN under black hole attack has been assessed. A 1000 m by 1000 m flat area serves as the simulation area. CBR is the program used to simulate the data flow in WSN. Three clusters, including CH and ACH, each include n/3 sensor nodes as part of the simulation scenario. The utilized sink node/BS is a fully functional device with no energy restrictions, in contrast to the other nodes in the WSN which have restricted power/energy. One CH is used as a black hole in the simulation. The suggested method defends against black hole attacks on WSN. The following are the several performance measures that were taken into account while evaluating SEET's performance:

- **Energy:** To evaluate energy consumption, different parameters like average energy consumption in each round or remaining energy after each round are being used. In this paper the average residual energy of network is calculated after each round.
- **Network Lifetime (NL):** NL is defined as the time until battery power of all nodes drain out.
- **Throughput:** Throughput is defined as the rate of successful message delivered from one device to another over a communication channel. In this paper throughput is calculated between CHs as source and BS as destination. The simulation of SEET has been carried out for different network scenarios under black hole attack. The detailed analyzation with above described metrics is discussed below.

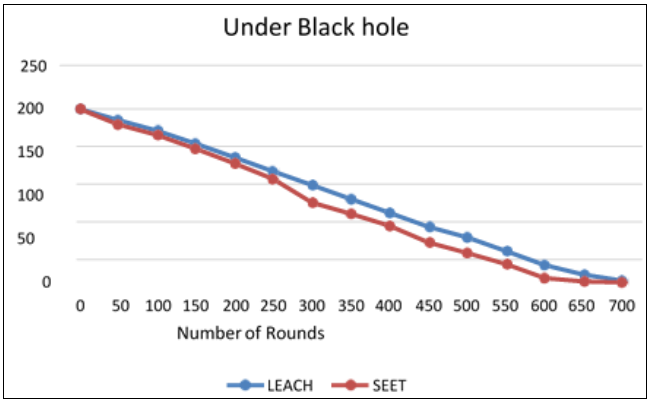

Fig 5.1: Comparison of Remaining Energy between LEACH and SEET under Black Hole Attack

Figure 5.1 details the effect of the black hole on the nodes' remaining energy as the number of rounds increases. Because black hole CH suppresses packets received from ACH, network under black hole attack uses less energy than SEET. As a result, CH and base station are unable to communicate. Because the energy of the black hole node steadily diminishes, Figure 5.4 shows that a specific energy level essentially stays the same throughout the course of the previous several cycles. Black hole nodes solely use their energy for internal processing and data reception. Following are some justifications for SEET performance.
compares the leftover energy in LEACH and SEET on a cluster level. A black hole assault has invaded cluster C1 at this location. The differences in the residual energy of C1, C2, and C3 are displayed in experimental results. In LEACH, C1 has more energy left over than C2 or C3, however in SEET, energy levels are about the same throughout all clusters. Because CH of C1 is a black hole node, the findings graphically shown in figure 5.5 show that energy of C1 across all rounds is high in C1. Black hole CH dumps all data after receiving it from ACH; there is no contact at CH; instead, it sends the data to BS. The majority of the energy is used up while CH and BS are exchanging data.

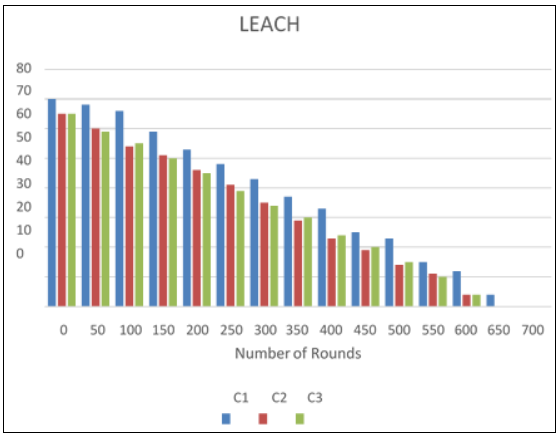

Fig 5.2: Cluster wise Remaining Energy of LEACH Under Black Hole Attack

On the other hand, as seen in Figure 5.2, SEET quickly identifies the block hole attack and maintains the regular operation of WSN. Up to the 700th round, all three clusters are still in operation.

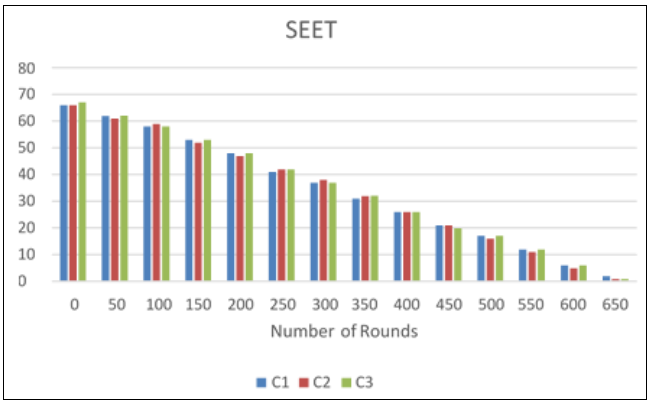

Fig 5.3: Cluster wise Remaining Energy Under Black Hole Attack

6. Network Lifetime

The number of living nodes (NL) in the network is used in Table 6 to characterize network longevity. The network life period will be longer if more nodes survive till the final round. LEACH has a longer network lifespan than SEET.

Table 6: Comparison of Network Lifetime between LEACH and SEET

Number of rounds	Number of Alive Nodes	
	LEACH	SEET
0	100	100
50	100	100
100	100	100
150	100	100
200	95	90
250	80	72
300	65	58
350	47	40
400	35	27
450	22	13
500	14	5
550	9	3
600	5	1
650	2	1
700	2	0

The lifespan of a network is shown in Figure 6.0. When a black hole attack occurs, NL is higher than it would be in a situation without a black hole. The majority of the cluster's energy is used for communication between CH and BS. The battery consumption of the black hole node is extremely low compared to other CHs since the black hole CH does not communicate with the target BS. Thus, under a black hole assault, network lifespan greatly rises. which function as regular nodes as a black hole in the cluster, CH in C1 uses less energy than the cluster heads in C2 and C3.

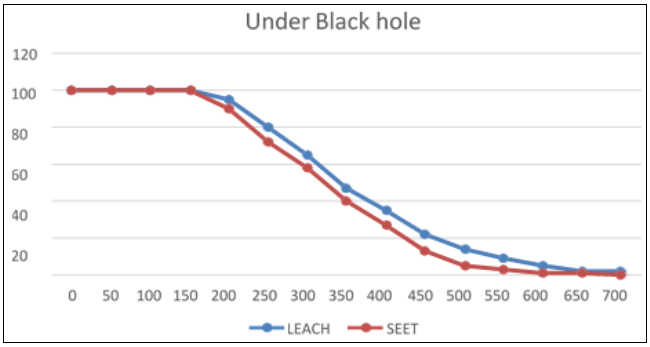

Fig 6: Comparison of Network Lifetime between LEACH and SEET under Black Hole Attack In

C1 containing with malicious CH survives for more time than C2 and C3 by dropping all data CH1 saves its energy that increase the life time of C1. in Figure 6.0 in C1 cluster head CH1 is a black hole node and consumes less energy as compare to CH2 and CH3. So, life time of C1 is extended up to 700 rounds while network lifetime of C2 and C3 restricted to 600th round.

6.1 Throughput Evaluation

As more rounds are played, the network's throughput declines, as seen in Figure 6.0. Early rounds saw every sensor node active, able to perceive objects and transmit information to the BS through ACH and CH. After 50 cycles, sensor nodes begin to fail and generate less data overall. Throughput thus declines. Because a black hole CH erases all of a cluster's data, performance under a black hole attack is significantly lower than it would be otherwise. As a result, instead of three clusters, BS is now only getting data from two clusters. Cluster-wise throughput in each round under a black hole, analyzes SEET performance and demonstrates how WSN is completely insulated from black holes; all three clusters transfer data to BS. SEET can communicate all information gathered from clusters. Nodes as ACH forwarded all data to BS again after the black hole CH dropped them. Therefore, even in the event of a black hole assault, there is no data loss.

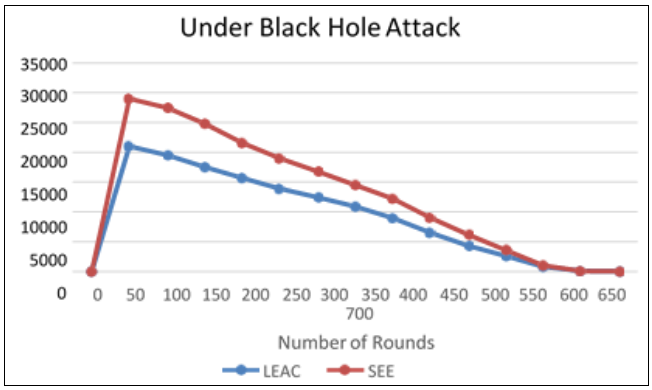

Fig 6.1: Throughput of WSN

Comparison of throughput between LEACH and SEET under black hole attack is illustrated in Figure 6.1. It is very much clear that throughput of SEET under black hole attack is much higher than the LEACH.

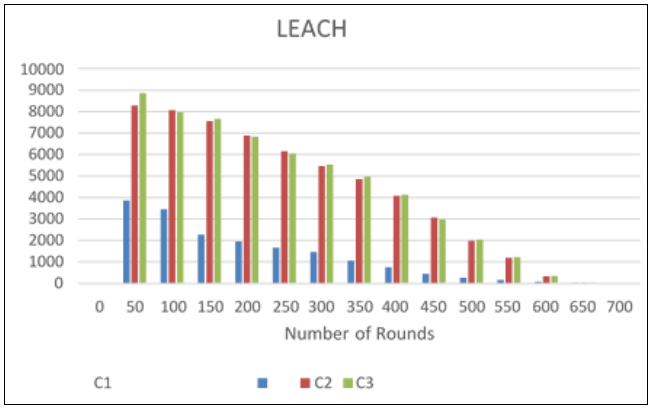

Fig 6.2: Cluster wise Throughput of LEACH under Black hole

Throughput is specified cluster-wise and represented in Figures 6.1 and 6.2 for LEACH and SEET, respectively. A black hole node is CH1 of C1 in Figure 6.2. As a result, throughput is significantly reduced because only control information is sent to BS. The throughput in all three clusters is roughly the same, as seen in SEET Figure 6.2 due to the fact that SEET effectively locates and replaces black hole cluster heads without affecting network performance. When there are changes in the input variables, sensitivity analysis aids in result prediction. The goal of the sensitivity analysis is to pinpoint the entities for which minor adjustments result in a significant shift in the output measure of the model. The decision-maker may have a good understanding of how the chosen optimal solution will respond to changes in the input values of the parameters with the use of sensitivity analysis. The most often used sensitivity analysis techniques include regression analysis, correlation analysis, and factorial experimental design. The most straightforward approach is to change the value of one input characteristic at a time while keeping the other input parameters fixed.

As shown in Figures 6.1 and 6.3, when the number of black hole cluster heads is increased from one to two, as in the case of LEACH, the performance of the WSN in terms of throughput is substantially reduced since data from two cluster heads is rejected by malevolent cluster heads. While the black hole cluster head drops the data packets rather than transmitting them, this has little impact on the remaining energy and network lifespan. In contrast, SEET effectively manages the rise in black hole cluster heads since only a 1% to 2% change is shown in the amount of energy left over, the network lifespan, and the throughput of WSN.

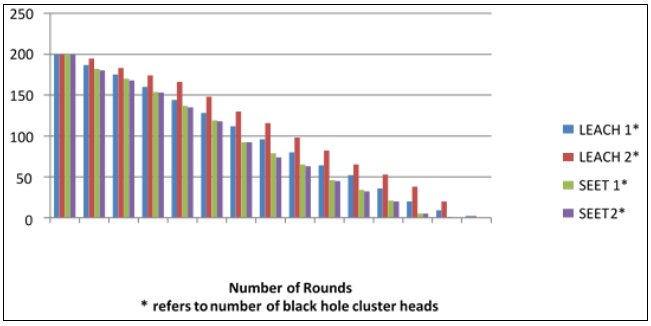

Fig 6.3: Effect on remaining energy with change in number of black hole cluster heads

7. Conclusion

In order to protect and improve the functionality of WSN, a Secured Energy Efficient Technique (SEET) is provided in this chapter. To extend the life of WSN and safeguard against malicious attack, an enhanced cluster topology and cluster head selection criteria are proposed. The results of the simulation are examined in terms of node energy remaining, network longevity, and throughput for the entire network as well as for each cluster separately.

While the observations from the acquired findings are summarized, it is discovered that the residual energy of the nodes and NL is large in the case of LEACH because there is no data communication from the cluster when the black hole CH is present. It is believed that all sensor nodes are stationary. Additionally, it is presumable that every node safely builds neighbor information for a brief initial phase during which no malicious nodes are present. High-speed tunnel is created by two malicious nodes. One malicious node is at one location, while a second malicious node is in a different location. A malicious node draws traffic from one place and tunnels it to another node in a different location.

8. References

1. Manap Z, Ali BM, Ng CK, Noordin NK, Salt A. A review on hierarchical routing protocols for wireless sensor networks. Wireless Pers Commun. 2013 Sep;72(2):1077-1104.
2. Ahmed M, Huang X, Sharma D, Cui H. Wireless sensor network: characteristics and architectures. In: World Academy of Science, Engineering and Technology; Penang, Malaysia; 2012. p. 660-3. Vol 72.
3. Singh SK, Singh MP, Singh DK. A survey on network security and attack defense mechanism for wireless sensor networks. Int J Comput Trends Technol. 2011 Jun;1(2):1-9.
4. Svilen I, Andre H, Georg L. Experimental validation of the NS-2 wireless model using simulation, emulation and real network. In: Proceedings of Kommunikation in Verteilten Systemen 15, ITG/GI Fachtagung; Bern, Schweiz; 2007 Feb.
5. Kaur R, Grover A. Performance analysis of AODV, DSR and OLSR routing protocols in WSN. Int J Comput Appl. 2017 Jul;170(1).
6. Aggarwal A, Gandhi S, Chaubey N. Performance analysis of AODV, DSDV and DSR in MANETS. Int J Distrib Parallel Syst. 2011 Nov;2(6).
7. Mhala NN, Choudhari NK. An implementation possibilities for AODV routing protocols in real world. Int J Distrib Parallel Syst. 2010 Nov;1(2).
8. Kumar P, Thakurta G, Guin R, Bandyopadhyay S. An efficient approach for detecting wormhole attacks in AODV routing protocol. Advances in Intelligent Systems and Computing. Springer; 2018. p. 217-227.
9. Zhang YY, Li XZ, Liu YA. The detection and defence of DoS attack for wireless sensor network. J China Univ Posts Telecommun. 2012 Oct;19:52-56.
10. Mansouri D, Mokddad L, Ben-othman J, Loualalen M. Preventing denial of service attacks in wireless sensor networks. IEEE Mobile and Wireless Networking Symposium; 2015.
11. Joby PP, Sengottuvelan P. A localised clustering scheme to detect attacks in wireless sensor network. Int J Electron Secur Digit Forensics. 2015;7(3).
12. Gunasekaran M, Periakaruppan S. A hybrid protection approaches for denial of service (DoS) attacks in wireless sensor networks. Int J Electron. 2017.
13. Fouchal S, Mansouri D, Mokdad L, Louallalen M. Recursive-clustering-based approach for denial of service (DoS) attacks in wireless sensors networks. Int J Commun Syst. 2015;28:309-324.
14. Mazur K, Ksiezopolski B, Nielek R. Multilevel modeling of distributed denial of service attacks in wireless sensor networks. J Sensors. 2016;2016:5017248.
15. Oo KK, Ye KZ, Tun H, Lin KZ, Portnov EM. Enhancement of preventing application layer based on DDOS attacks by using hidden semi-Markov model. 9th Int Conf Genetic Evol Comput; 2015 Aug 26-28.