SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V12I2P107

Volume 12 Issue 2, 54-62, February 2025

Original Article

Cluster-Based Trusted Secure Information Transmission in Wireless Sensor Networks

Hemavathi Patil[1], Vishwanath Tegampure[2]

[1]*Department of ISE, Guru Nanak Dev Engineering College, Bidar, Karnataka, India.*
[2]*Department of ECE, Bheemanna Khandre Institute of Technology, Bhalki, Karnataka, India.*

[1]*Corresponding Author : hbpatilbidar@gmail.com*

Received: 07 December 2024 Revised: 06 January 2025 Accepted: 04 February 2025 Published: 22 February 2025

Abstract - *WSN is a heterogeneous system that gives Sensor Nodes access to the communications networks to record and analyze events at many locations. There are currently a number of key managing mechanisms in place to protect communication among Sensor Nodes. At the very least, the key management technique for any secured application needs to provide safety features like trustworthiness. Diffie-Hellman Key Exchange (DHKE) is vulnerable to Man-in-the-Middle (MITM) attacks due to lack of authentication. The Diffie-Hellman with Sybil Attack Prevention method is given as a solution to this issue. The goal of this technique is to identify and remove Sybil nodes from the network in order to address the previously stated problem. Several performance parameters, including packet delivery ratio, delay, throughput, and detection rate, are considered while evaluating the proposed work's effectiveness. The results show that the proposed work is far better than the conventional techniques and has a better Sybil node detection rate.*

Keywords - *Heterogeneous systems, WSN, Key management, Sybil attack, Security, Diffie-Hellman.*

1. Introduction

Wireless Sensor Networks (WSNs) have drawn attention from all around the world recently because they offer the most affordable answers to a range of real-world issues. Because of their inexpensive installation costs, great performance, ease of deployment (no cables needed), flexibility to operate in various situations, and ease of troubleshooting, WSNs have a lot to offer. These networks comprise portable, self-contained, autonomous sensor nodes or motes. The nodes are wirelessly connected and placed at random unattended [1].

In addition to being used to automate routine chores, WSNs are a quickly evolving technology that can be employed in a wide range of hazardous and uncommon situations, such as forestry fire identification, conflict zones, agricultural activities, business sectors, medical care, marine sciences, and wildlife movements tracking [2]. WSNs require less maintenance and are very scalable and adaptable, making them perfect for real-time monitoring.

Sensor nodes, which sense and send information to the Cluster Head (CH), make up the sensor network. A CH's responsibility is to collect information, process it, and interact with other CHs so that the Base Station (BS) can use it [18]. The computing power, bandwidth, storage, and RAM available to the SNs are limited. So, maximizing the efficient utilization of these resources is WSNs' main objective. The sensing unit, processing unit, transceiver, and power unit are the four main basic parts that make up the sensor nodes [3]. WSNs have a lot more security restrictions than conventional wired networks [4]. Due to these limitations, employing the current wired network security protocols directly in WSNs is quite challenging. Therefore, before creating any energy-efficient security mechanism, it is imperative to understand the security limits. The security constraints are Resource constraints, Unreliable Communication, and Unattended operation to minimize reassembling cost, Latency and Lack of global identification [5].

Malicious nodes or attackers can readily enter WSNs owing to architectural limitations. It is anticipated that attacks on WSNs would compromise network functionality. WSNs are, hence, vulnerable to a range of attacks. Some security attacks in WSN are denial of service, black hole, warm hole, hello flood, Sybil, sink hole and selective forwarding attacks [6]. The Sybil attack prevents the network from operating normally. A malicious node in a single network can operate multiple identities simultaneously [7].

The Sybil attack scenario is shown in Figure 1. The malicious node assumes many identities for different nodes, as seen in Figure 1. In order to interact with node' E,' the message is transmitted to the malicious node, which manifests itself as node 'D' for 'B, 'C' for 'E, and 'E' for 'C'.

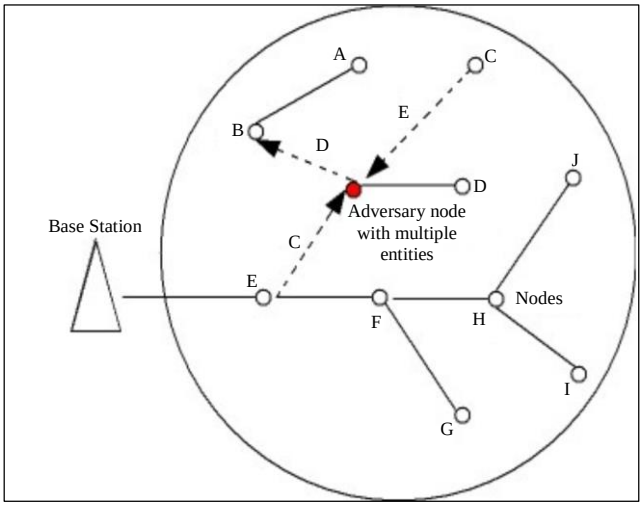

Fig. 1 Sybil attack

For Sensor Nodes, security is the main priority because they are susceptible to malicious attacks. These Sensor Nodes may monitor, process, and transmit data to BS placed remotely in certain geographic areas. Attackers might receive access to private information while it's being transferred across an unsecured Wi-Fi connection. The process of choosing a path for information transfer between source nodes and BS is known as routing. The network layer is mostly used to configure the routing path for incoming data.

WSN routing protocols can differ depending on the application. Multi-hop data transfer is used in WSNs due to the high density and constrained communication range of SNs. It is observed that the source node frequently cannot establish a direct connection with the sink, unlike in multi-hop organizations. Every SN has a single channel that it may use to transmit data, and it can quickly switch to another path if a connection fails during network operation because of hardware failure, SN energy depletion, or any other external event.

In order to achieve multiple loop independence and link discontinuous routes, the Ad-hoc On-demand Multipath Distance Vector (AOMDV) routing method is employed [8]. For contesting link failure, it finds many pathways between the source node and the BS in a single route finding. The existing method for identifying the Sybil nodes lags behind proper identification methodology, with lower identification accuracy.

The main objective of the research is to prevent the Sybil attack in the sensor network using improved Diffie-Hellman Key Exchange, where some weights are added to find the accurate Sybil attacked node so that such nodes can be eliminated from the network, avoiding any data being transmitted from such nodes. The paper uses an enhanced Diffie-Hellman Key Exchange algorithm to check whether any node in the cluster is misbehaving or injecting false information into the network. Such nodes will be adverse to the network's overall operation and affect overall operation. The method proposed here uses two methods: first, the formation of trust-worth nodes and second, secure communication. The first method ensures that the node being utilized in the network is trusted and that information can be exchanged. The second method ensures that link security is secure, i.e., data transfer from one node to another, and no other can access the transmitted information.

The rest of the paper has been organized as follows: section 2 gives the literature review, section 3 describes the proposed work, section 4 explains the result and analysis of the proposed work, and finally, section 5 concludes the paper.

2. Literature Review

This section provides the recent works on secure communication in WSN by preventing Sybil and other security attacks.

In [9], the author mentioned that WSNs are extremely important for protecting networks. Numerous researchers have demonstrated very significant assaults of various sorts in wireless sensor networks up to this point. The Sybil attack is a massively disruptive attack on a sensor network in which a large number of falsified identities are used to obtain unauthorized access to the network. In WSN, identifying the Sybil, Sinkhole, and Wormhole attacks during multicasting is a major task.

A Sybil attack is essentially defined as a node impersonating another node. In addition to causing data loss, communication to an unauthorized node puts the network at risk. The Random Password Comparison technique currently in use only employs a methodology to analyze neighbors in order to verify node identities. To address this issue, a survey on a Sybil attack was conducted. The survey suggests using Message Authentication and Passing (MAP) in conjunction with Compare and Match-Position Verification Method (CAM-PVM) to identify, remove, and ultimately stop Sybil nodes from joining the network. The suggested solution provides security for wireless sensor networks by addressing both unicasting and multicasting threats.

In [10], authors took routing security into consideration for WSN. There have been several suggested sensor network routing protocols, but neither of them has been created with security in mind. They introduced two classes of novel attacks against sensor networks-sinkholes and HELLO floods-analyzed the security of each of the major sensor network routing protocols and suggested security goals for routing in sensor networks. They have also demonstrated how assaults against ad-hoc and peer-to-peer networks can be tailored into effective attacks against sensor networks. The authors outline devastating attacks on each of them and offer defense strategies and architectural considerations.

In [11], the authors explain that WSNs have proliferated recently in various fields, including the military, agriculture, surveillance, etc. WSNs are absolutely necessary for protecting networks. However, several researchers have discovered horrible critical assaults of various types in these networks. A Sybil attack is one of those where a legitimate node is changed into a replica node with a distinct personality by utilizing an identical ID. Stated differently, a Sybil attack happens when a base station or sensor node adopts several identities by altering its IP address, MAC address, and other identifying details. Voting, data aggregation, and reputation are among the primary routing protocols and functions impacted by this attack. This article presents a precise and dynamic strategy for detecting and preventing Sybil attacks. This technique will advance data transmission in the network and improve performance by integrating the Message Authentication and Passing method (MAP) with Random Password Comparison (RPC).

In [12], the author described that a WSN is particularly useful in military and civilian applications in critical places like battlefields, and it is crucial to enhance security in these networks. This has the potential to enhance life quality in a number of ways. However, it is to be used in other contexts, like implementation, for reasons of protection. The likelihood of coming into contact with several infections and hacking attempts is very high. For the security of information, unauthorized access points must be identified. Malicious assaults on these networks, such as the Sybil Attack, result in a security breach when they pose as a node that simultaneously proclaims many bogus identities. Because of this, legitimate nodes are misled, and they mistakenly believe that each of those IDs represents an individual node. In an integrated wired/wireless context, the authors suggested a machine learning approach that uses acquired raw traffic information to identify approved and illegitimate APs and identify Sybil attacks.

In [13], the authors described that the WSNs are prone to several attack vectors. The Sybil attack is particularly dangerous among them as it may create a large number of bogus nodes and introduce bogus data into the network. They are harmful to a number of FSU operations, including resource allocation fairly and data pooling. Consequently, it is essential to defend against and identify Sybil's assaults. Network performance is significantly impacted by the Sybil attack, but it will clearly improve if it is discovered. In this paper, the authors examined a novel approach that uses random keys to identify Sybil assaults. Signs indicating a weak relationship between the group of false nodes and the group of normal nodes are employed in the suggested strategy. Signs indicating a weak relationship among the group of false nodes and the group of normal nodes are employed in the suggested strategy. The study outcomes demonstrate that the suggested strategy may identify a fake node with modest energy and a probability of over 90 percent.

In [14] author explained that one of the biggest problems with WSNs is network communication security. In contrast to heterogeneous wireless sensor networks, traditional wireless sensor networks have seen much discussion of the key distribution challenge. Through the introduction of high-resource capacity sensor nodes into the network, heterogeneous WSNs have optimized network capabilities and created new security prospects. This research proposes an effective dynamic key management and authentication strategy for heterogeneous wireless sensor networks. The major goal is to maximize the security level while offering a single lightweight protocol for both key establishment and authentication. Because the key distribution method generates dynamic keys based on previous information rather than requiring a secure channel or sharing phase, it is more secure, energy-efficient, and memory-efficient.

In [16], the authors mentioned that the information travels across a typically open wireless channel, wherein malicious attackers might obtain vital information; data security is a significant concern in WSNs. While the current data security systems have complicated security procedures with significant computations and responses that influence the network lifetime, the sensors in WSNs are devices with restricted resources. Additionally, the Diffie-Hellman technique is used for key generation and exchange in many current systems, including safe encryption algorithms. However, Diffie-Hellman is extremely susceptible to attacks called Man-in-the-Middle attacks. Utilizing an improved version of Diffie-Hellman, the paper presents an information safety method with faster reaction times and less processing. By creating a hash of every value sent over the network, the Diffie-Hellman algorithm has been altered to protect it from assaults.

In [17], the authors described that the Diffie-Hellman key exchange, which encrypts and decrypts medical information, is used to accomplish key management and safe transfer for routing. This improves the throughput and delivery ratio while facilitating the safe and efficient transfer of information from the source to the destination.

3. Proposed Work

This section depicts the proposed work. The proposed scenario and its workflow will be discussed here, along with the algorithms that have been designed to prevent the Sybil attack in cluster-based WSN by key generation technique in the modified DH method. Figure 2 depicts the proposed system environment. The nodes are randomly localized, and clusters are created.

The Cluster Head (CH) is elected by considering the distance between the node and the Sink Node (SN). The CH node informs all the nodes in the cluster about its current status and location. The nodes in the cluster pass the information to CH using multipath routing [15], and CH sends the final information to SN. Some external nodes may interrupt the

operation during the node transactions and harm the overall network. The DHKE method has been used in the proposed work.

If DHKE is used without node authentication, it is susceptible to MITM attacks. The proposed Diffie-Hellman with Sybil Attack Prevention technique creates a network of reliable nodes to identify and reduce Sybil nodes to solve this issue. After that, modified-DH is utilized for key creation and key exchange as validation in order to provide safe and incorrect-free communication amongst interacting nodes.

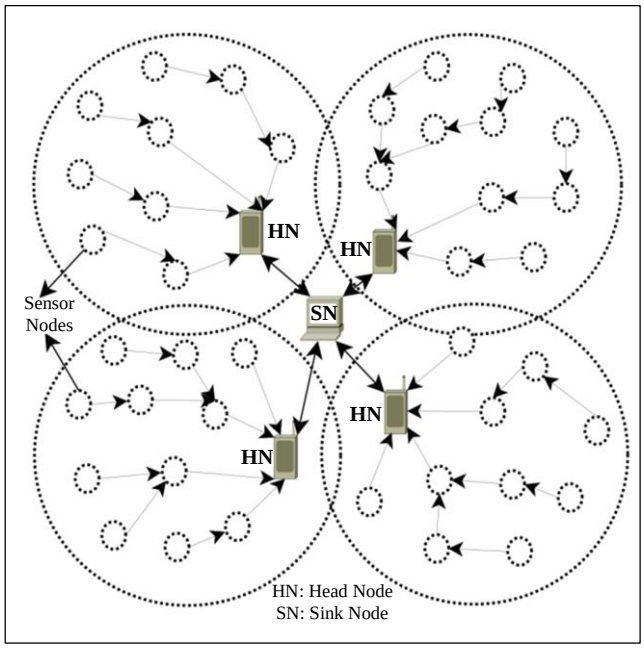

Fig. 2 Proposed system environment

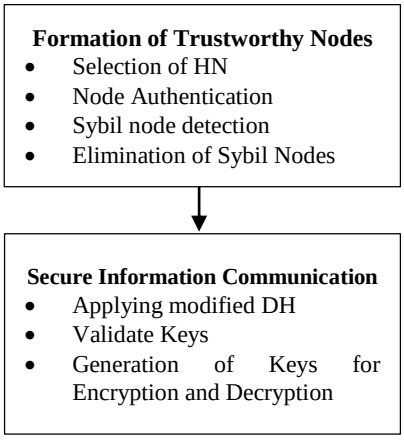

Fig. 3 Proposed workflow

The proposed approach functions as follows: initially, it establishes a network of trustworthy nodes that locates and eliminates Sybil nodes from the system. Then, during key creation and exchange, modified DH is utilized as validation. The workflow of the proposed work is shown in Figure 3.

3.1. Mathematical Model

3.1.1. Modified Diffie–Hellman Key Exchange (DHKE) Model

When transferring information over an open network, the Diffie-Hellman method is employed to create a shared secret that may be utilized for secure communication. The elliptic curve is usually utilized to produce points and obtain the secret key using the parameters. The main purpose of the Diffie-Hellman algorithm is as a key exchange mechanism. Two parties can determine a shared secret key via this interactive protocol by exchanging messages. The primary foundation for the Diffie-Hellman algorithm's security is the complexity involved in calculating the discrete logarithms. We shall simply take into account four variables in the method's mathematical model: two private values, r and s, one prime, D, and H (a primitive root of D).

Both D and H are openly accessible numbers. Users create a key and publicly exchange it after selecting the private values r and s. After receiving the key, the other party produces a secret key, giving them the identical secret key to encrypt. Finally, Key_r = $Node2Key^r$ mod D and Key_s = $Node1Key^s$ mod D is the final key formation for the modified DHKE model. A detailed explanation is provided below:

Table 1. Modified DHKE model explanation

X	Y
Public Keys = D, H	Public Keys = D, H
Private Key = r	Private Key = s
Key generated = $y=H^r \bmod D$	Key generated = $z=H^s \bmod D$
The created keys are exchanged.	
Key received = z	key received = y
Generated Secret Key = $k_r = x^r \bmod D$	Generated Secret Key = $k_s = y^s \bmod D$
Algebraically, it can be shown that $k_r=k_s$	
Users now encrypt using a symmetric secret key	

The example for the Diffie-Hellman model is as follows,

1. X and Y obtain public numbers D = 23, H = 9
2. X selected a private key r = 4 and Y selected a private key s = 3
3. X and Y compute public values
4. X: y = (9^4 mod 23) = (6561 mod 23) = 6
5. Y: z = (9^3 mod 23) = (729 mod 23) = 16
6. X and Y swap public numbers
7. X receives public key z =16 and
8. Y receives public key y = 6
9. X and Y compute symmetric keys
10. Alice: kr = z^r mod D = 65536 mod 23 = 9
11. Bob: ks = y^s mod D = 216 mod 23 = 9
12. 9 is the shared secret.

3.2. Algorithms

3.2.1. Diffie-Hellman with Sybil Attack Prevention

In Diffie-Hellman with Sybil Attack Prevention, N sensor nodes are initially dispersed randomly throughout the network. Afterwards, each sensor node is given an ID. The base station does the topological verification. Send the fake messages to each sensor node in the next phase. The network's attacker nodes discard the messages and use all of their energy. Thus, the least message drop sensor nodes are chosen to be trusted nodes. Header nodes, often referred to as cluster heads, are chosen from trustworthy nodes in order to lessen the workload on the BS.

The density of sensor nodes in the network determines the number of header nodes. Joining their closest header node are the remaining trustworthy nodes. The ID and energy value of every member node are sent to the HNs. Each member node's energy value is compared to the threshold value by HNs. A threshold value indicates insufficient energy in the Sensor Node to send data packets to the intended location. The node is identified as a Sybil node and is disconnected from the network if the power value is below the threshold. Use modified DH between communication parties for safe and error-free data transfer after eliminating all Sybil nodes from the network. The algorithm steps are as follows,

Nomenclature: SN: Sensor Nodes, BS: Base Station, HN: Head Node, bpvalue: Battery Power Value, HP: Hello Packet, TV: Topology Verification

1. N numbers of Sensor Nodes are randomly positioned in the network.
2. Assign ID's to each SN.
   for i =1 to N
   SNi ← Location (rand (x), rand (y))
   ID (SNi← i)
   end loop
3. All of the SNs get Hello packets from the BS, and responsive nodes reply to the BS to validate the topology.
   for i= 1 to N
   BS (HP) → SNi
   SNi (TV) →BS
   end loop
4. Deliver dummy packets to every SN. The trustworthy nodes are those that have the least packet drop.
   for i= 1 to N
   Send (dummyinformationP) → SNi
   T* ← minimum packets drop (SNi)
   end loop
5. From among the trustworthy nodes, HNs (H1, H2,...Hn) are chosen, and the remaining trusted nodes connect to the closest HN. Here, n is the HN count.
6. The ID and BP values of each member node are sent to the HNs.
   m1k (ID, BPvalue)→H1
   m2k (ID, HPvalue)→ H2
   Here k is the count of member nodes for each HN
7. HNs contrast each member node's power value with the threshold value. The node is identified as a Sybil node and is disconnected from the network if the power value is below the threshold.
   If (bpvalue(SNi) < threshold) then
   Si ← SNi Blocked as Sybil Node
   Update neighbour list of Header nodes
   Hi ← remove node (SNi(ID), SNi(x), SNi(y))
   end if

3.2.2. Key Generation in Modified-Diffie–Hellman

1. The R and S are chosen by two communicating nodes, accordingly.
2. Calculate h (R) and h (S)
   a) Convert R and S values to binary form.
   b) Count the Number of 1's in R and S, respectively.
3. A private number chosen by both nodes is never shared over the network. Random selections are made for private numbers.
4. Step 2 is used by both nodes to compute the hash map of private numbers.
5. Now generate the key in a fashion that Node1Key = S^a mod R and Node2Key =S^b mod R
   a) Node1Key and Node2Key values convert to binary.
   b) Count the number of 1's in Node1Key and the same for Node2Key.
6. Interchange the keys and the hash map produced in step 5 (Node1Key with Node2 and Node2Key with Node1).
7. Received keys are (Node1 = Node2Key) and (Node2 = Node1Key) along with the hash map.
8. Using steps 5.a and 5.b, the receiving node computes the hash map once more.
9. Use the value that was acquired to create the official key after using the hash map to validate both keys. The keys are deemed compromised in the event that the receiver's counter-check is unsuccessful.
10. Key_a = $Node2Key^a$ mod R and Key_b = $Node1Key^b$ mod R.
11. Therefore, Key_a= Key_b. The generated key is used by both nodes for encryption and decryption.

These improved algorithms provide a more robust defense against Sybil attacks in WSNs.

4. Result and Analysis

The NS2 program simulates the network model with a 200 m × 200 m network size and a variety of nodes. The many parameters utilized in the simulation are shown in Table 2. A range of quality of service metrics, including PDR, throughput, and latency, are employed to assess WSN effectiveness. The NS2 simulator is used to evaluate five distinct situations with variable numbers of sensor nodes (20, 40, 60, 85, and 100). Information is sent via multipath routing from Sensor Node to CH and CH to BS using the AOMDV routing protocol.

Table 2. Simulation parameters

S. No	Parameters	Values
1	Area	200x200
2	Nodes	20,40,60,80,100
3	Routing Protocol	AOMDV
4	Simulation Time	1000s
5	Network Interface	wirelessPhy
6	Propagation Model	TwoRay
7	Node Energy	2 Joules

Packet Delivery Ratio: It reports the number of packets that reach their target. Energy limitations, node failures, and interference can all result in packet loss in WSNs. Ineffective implementation of Diffie-Hellman may raise overhead and cause packet loss.

It is the ratio of the total number of packets transmitted from the source node to the BS to the total number of packets received by the BS. A maximum number of data packets arriving at the destination is needed. Actually, the BS won't get any of the data packets that the source node produces. This is because network nodes that have been hacked or connection failures may cause certain data packets to be lost. Network efficiency will rise with PDR maximization.

Delay: The duration of a packet's journey from its origin to its final destination. Delay is essential for critical tasks in WSNs. Delays may be triggered by Diffie-Hellman's computational expenses, particularly if it is not optimized.

It is described as the amount of time needed for data packets to travel from their source to their destination. It is dependent on the network's congestion and hop count. Reducing latency guarantees the prompt delivery of data packets and allows the network to function as a real-time network.

Throughput: How much information is successfully sent in a certain length of time. Throughput in WSNs is frequently constrained by energy and bandwidth issues. Because of the processing cost, Diffie-Hellman might lower performance if it is done incorrectly.

It is expressed as the quantity of data packets received by the BS per second. It can be expressed in Mbps and fluctuate in bandwidth as a result of many problems, including jitter, packet loss, delay, etc. The throughput is reduced when information packets are retransmitted. The result scenarios are as follows:

4.1. Diffie–Hellman without Attack Prevention

Because DHKE doesn't offer authentication between nodes during transmission, it is susceptible to MITM attacks. As presented in Table 3, this scenario assesses WSN QoS parameters with DH in the absence of attack mitigation.

Table 3. Diffie–Hellman without attack prevention

Nodes	PDR	Delay (ms)	Throughput (Mbps)
20	89.1	0.06123	0.362
40	87.6	0.06184	0.264
60	86.2	0.06211	0.227
80	83.8	0.06245	0.142
100	81.1	0.06314	0.113

4.2. Diffie-Hellman with Attack Prevention

Table 4 displays our evaluation of the suggested Diffie-Hellman with Sybil Attack Prevention's QoS parameters and detection rate in this situation.

Table 4. Diffie-Hellman with attack prevention

Nodes	PDR	Delay (ms)	Throughput (Mbps)	Detection Rate (%)
20	98	0.00421	0.421	97.1
40	97.6	0.00446	0.386	95.4
60	95.9	0.005245	0.321	94.2
80	94.2	0.005674	0.274	92.5
100	92.1	0.006211	0.221	90.1

Figures 4, 5, and 6 compare the QoS characteristics (PDR, latency, and throughput) of the DH without Attack Prevention with the proposed technique.

The number of malicious nodes grows along with the number of sensor nodes in the network, affecting data delivery and causing packet loss. Before implementing DH, the proposed approach monitors and eliminates the harmful nodes from the network.

Diffie-Hellman with Sybil attack prevention performs better in terms of PDR, throughput, and delay, as seen in Figures 4, 5, and 6. When compared to DH without an attack mitigation method, Diffie-Hellman with Sybil Attack Prevention allows for node authentication and the early detection of attacks, which increases the quantity of packets that the BS can securely receive with less time.

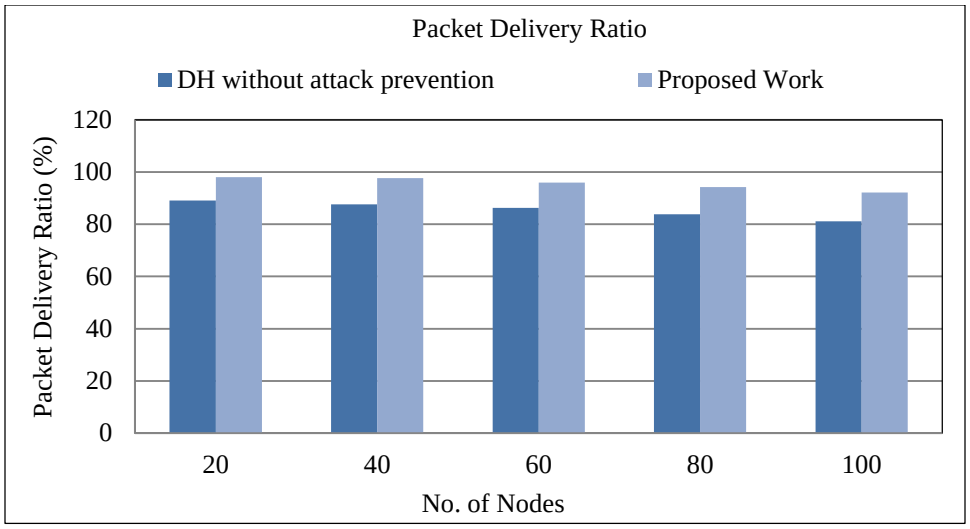

Fig. 4 Packet Delivery Ratio of DH without attack prevention and proposed work

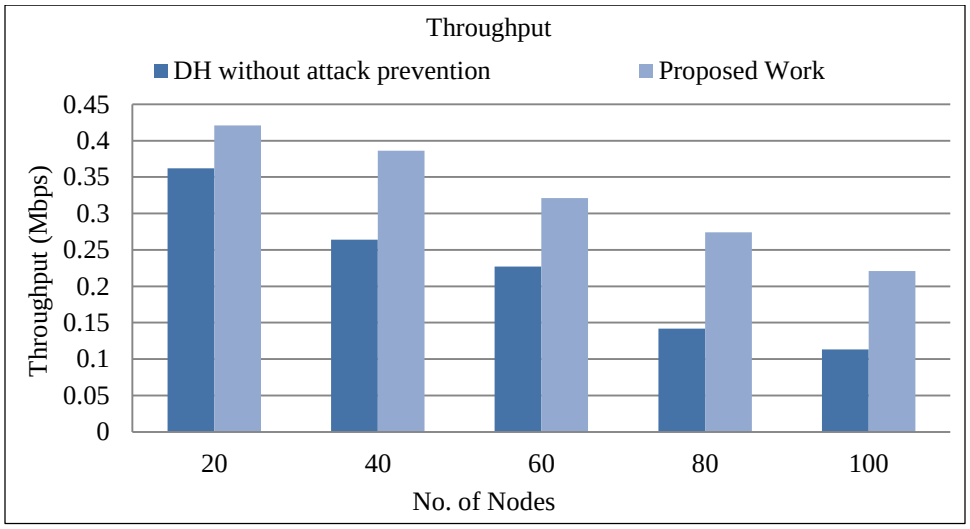

Fig. 5 Throughput of DH without attack prevention and proposed work

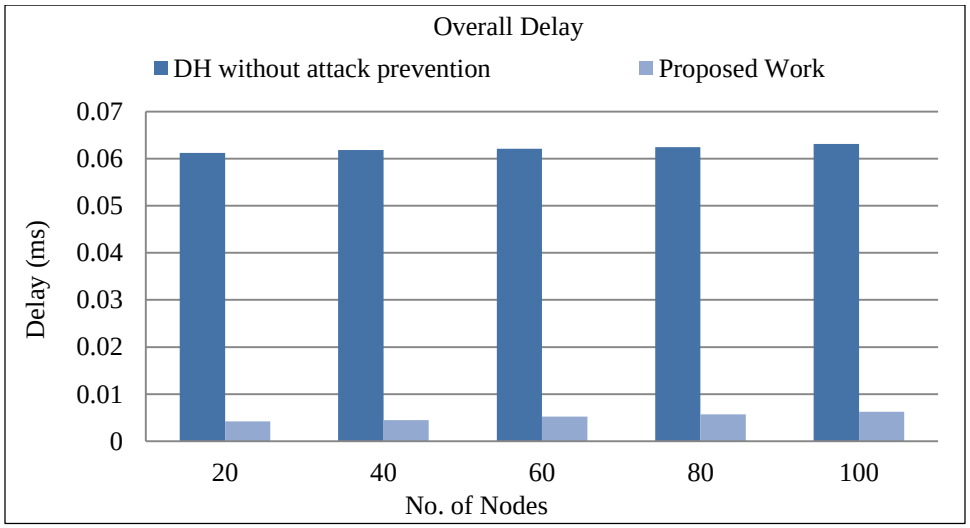

Fig. 6 Overall delay of DH without attack prevention and proposed work

5. Conclusion

Since information travels across an inevitably exposed wireless channel, where fraudulent attackers might gain access to sensitive information, information safety is a major problem in WSNs. Single-route routing is quite popular in WSNs. However, it has two drawbacks: if a single path node is compromised, there is no other way to transport the data to the destination securely, and connection failure causes data loss in the network. Multiple pathways are established using AOMDV. Since DHKE doesn't offer authentication for nodes to use when communicating, MITM attacks may easily target DHKE. In order to solve this issue, the suggested Diffie-Hellman with Sybil attack prevention paradigm first establishes a network of trustworthy nodes before using modified DH to secure data transmission throughout the network. This paradigm is appropriate for early-stage detection and mitigation of Sybil attacks against WSNs. Since the Sybil nodes are found during the first phase of route discovery, the network may proceed with its transmission without worrying about being attacked. The findings show that, in terms of detection rate, the proposed approach, Diffie-Hellman with Sybil attack prevention, performs better than the current methods, RPC, CAM-PVM, and MAP, in that order. Data analysis and simulation findings showed that in comparison to ECC, Diffie-Hellman with Sybil attack prevention offers shorter delay and greater throughput. Further, the work can be improved by considering location-based approaches, improved Sybil attack detection mechanisms, lightweight cryptography and enhanced energy-efficient approaches, which further boost the work with greater throughput, less delay and greater packet delivery ratio.

References

[1] Farah Kandah, Jesse Whitehead, and Peyton Ball, "Towards Trusted and Energy-Efficient Data Collection in Unattended Wireless Sensor Networks," *Wireless Networks*, vol. 26, no. 7, pp. 5455-5471, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] Ahmad Ali et al., "A Comprehensive Survey on Real-Time Applications of WSN," *Future Internet*, vol. 9, no. 4, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[3] Ala' Khalifeh et al., "Microcontroller Unit-Based Wireless Sensor Network Nodes: A Review," *Sensors*, vol. 22, no. 22, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] Rajwinder Kaur, and Jasminder Kaur Sandhu, "A Study on Security Attacks in Wireless Sensor Network," *International Conference on Advance Computing and Innovative Technologies in Engineering*, Greater Noida, India, pp. 850-855, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] Apip Miptahudin, Titiek Suryani, and Wirawan Wirawan, "Wireless Sensor Network Based Monitoring System: Implementation, Constraints, and Solution," *JOIV: International Journal on Informatics Visualization*, vol. 6, no. 4, pp. 778-783, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Zainab Alansari et al., "A Systematic Review of Routing Attacks Detection in Wireless Sensor Networks," *PeerJ Computer Science*, vol. 8, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Arthanareeswaran Angappan et al., "Novel Sybil Attack Detection Using RSSI and Neighbour Information to Ensure Secure Communication in WSN," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 6567-6578, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] Yousif Hardan Sulaiman et al., "Hybrid Security in AOMDV Routing Protocol with Improved Salp Swarm Algorithm in Wireless Sensor Network," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 5, pp. 2866-2875, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Udaya Suriya Raj Kumar Dhamodharan, and Rajamani Vayanaperumal, "Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method," *The Scientific World Journal*, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[10] Chris Karlof, and David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *Ad Hoc Networks*, vol. 1, no. 2-3, pp. 293-315, 2003. [CrossRef] [Google Scholar] [Publisher Link]

[11] Jlassi Wadii, Haddad Rim, and Bouallegue Ridha, "Detecting and Preventing Sybil Attacks in Wireless Sensor Networks," *IEEE 19th Mediterranean Microwave Symposium*, Hammamet, Tunisia, pp. 1-5, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[12] Mandala Mounica, R. Vijayasaraswathi, and R. Vasavi, "Detecting Sybil Attack in Wireless Sensor Networks Using Machine Learning Algorithms," *IOP Conference Series: Materials Science and Engineering*, vol. 1042, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] Zhukabayeva T.K., Mardenov E.M., and Abdildaeva A.A., "Sybil Attack Detection in Wireless Sensor Networks," *IEEE 14th International Conference on Application of Information and Communication Technologies*, Tashkent, Uzbekistan, pp. 1-6, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[14] Samir Athmani, Azeddine Bilami, and Djallel Eddine Boubiche, "EDAK: An Efficient Dynamic Authentication and Key Management Mechanism for Heterogeneous WSNs," *Future Generation Computer Systems*, vol. 92, pp. 789-799, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[15] Shilpa Chaudhari, "A Survey on Multipath Routing Techniques in Wireless Sensor Networks," *International Journal of Networking and Virtual Organisations*, vol. 24, no. 3, pp. 267-328, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[16] Shahwar Ali et al., "An Efficient Cryptographic Technique Using Modified Diffie-Hellman in Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, vol. 16, no. 6, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[17] A. Jenice Prabhu, and D. Hevin Rajesh, "Authentication of WSN for Secured Medical Data Transmission Using Diffie Hellman Algorithm," *Computer Systems Science & Engineering*, vol. 45, no. 3, pp. 2363-2376, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[18] Prashant Sangulagi, A.V. Sutagundar, and S.S. Manvi, "Agent Based Information Aggregation and Routing in WSN," *Computer Networks and Information Technologies*, pp. 449-451, 2011. [CrossRef] [Google Scholar] [Publisher Link]