Enhanced Secure Leach with Advanced Encryption Standard And Attack Detection Scheme

SAGIR IBRAHIM, AISHA IBRAHIM GIDE
Department of Computer Science, Umaru Musa Yar'adua University,
Katsina State,
NIGERIA

Abstract: - Wireless Sensor Networks (WSNs) have become widely used in a variety of applications, ranging from military surveillance to environmental monitoring, as a result of their quick development. However, WSNs are susceptible to security attacks due to their open communication channels and limited resources, which jeopardizes network dependability and data integrity. The network employs Abundant Secure LEACH protocol to create an energy-efficient system that is vulnerable to a wide range of assaults, including the HELLO flood. The proposed scheme uses Enhanced Secure-LEACH with Advanced Encryption Standard and Attack Detection (SLEAD) mechanism to protect cluster heads from sinkhole, sybil and Hello flood attacks and provide data privacy. SLEAD makes use of a unique ID for each sensor node and Advanced Encryption Standard Mechanism for the purpose of authenticating a sensor node as CH and ensure the security of data. SLEAD algorithm was implemented using Python within a Jupyter Notebook environment. The simulation result shows that SLEAD outperformed the traditional scheme in-terms of efficient energy utilization and data privacy.

Key-Words: - WSN, SLEAD, Secure-LEACH, Cluster Head (CH), Authentication.

Received: March 15, 2024. Revised: August 25, 2024. Accepted: September 16, 2024. Published: October 17, 2024.

1 Introduction

A wireless sensor network (WSN) is a network of wireless sensor devices that work in a coordinated way and communicate their readings to a base station. Each device is powered by a battery with a limited energy supply (Dionisis, 2020). Furthermore, these devices have low computation power, and limited sensing and transmission range. The energy stored in the battery of a node determines the lifespan of the node. The stored energy is used for various node operations such as sensing, processing, and communication. The batteries in sensor nodes are small and usually cannot be replaced or recharged. There are various energy harvesting methods, but they cannot eliminate the need for energy management. Hence, the most challenging job is the organization of the limited battery power by using energy-efficient hardware and software protocols for WSNs (Ju, 2021).

Wireless Sensor Networks (WSNs) are made up of spatially dispersed sensors that wirelessly transmit data to a central base station or sink while monitoring physical or environmental parameters like temperature, humidity, or motion. Due to advancements in energy-efficient designs, downsizing, and communication technologies, WSNs have undergone tremendous evolution and are now essential in a wide range of applications, such as smart cities, healthcare, military operations, and environmental monitoring (Rawat, 2021).

Sensor nodes which are able to sense, process, and send data wirelessly are the backbone of WSN operations. These nodes are commonly deployed in harsh conditions or hard-to-reach areas, making their capacity to function independently vital. Energy efficiency, data aggregation, security, and scalability as the number of nodes rises are major issues facing WSNs (Koulouras, 2020).

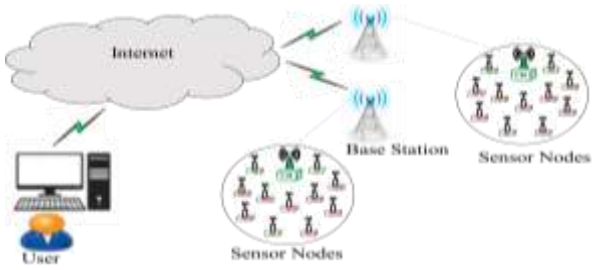

Fig. 1: Wireless Sensor Clustering (Bhatia, 2020).

1.1 Importance of securing WSN

Numerous tiny, low-power devices that connect wirelessly and gather data from their surroundings make up wireless sensor networks, or WSNs. Applications for WSNs are numerous and include smart agriculture, industrial control, environmental monitoring, and health care. WSNs must contend with a number of security issues, including scarce resources, erratic communication, changing topology, and physical attack susceptibility. In order to secure a WSN and guarantee its operation, integrity, and secrecy, it is imperative to implement a few crucial measures (Lata, 2021).

1. Data Confidentiality

WSNs often collect sensitive information such as medical data, environmental conditions, or military intelligence. If unauthorized parties intercept this data, it could result in privacy violations, security breaches, or harm to individuals or national security (Jen, 2012).

2. Data Integrity

In a WSN, data can be tampered with during transmission, leading to inaccurate or misleading information. For instance, in a military scenario, altered sensor data could result in false alarms or misinformed decisions (Gautam, 2021).

3. Availability of Network Services

WSNs must remain functional for continuous data collection and transmission. Denial of Service (DoS) attacks, such as jamming, can cripple the network by overwhelming nodes with false traffic, preventing legitimate data from being processed or transmitted (Rehman, 2022).

4. Authentication

Ensuring that only authorized devices and users can access the network is critical to preventing unauthorized data access, injecting false data, or misusing network resources. Without authentication, malicious nodes can easily infiltrate the network.

5. Energy Efficiency

Sensor nodes in WSNs have limited battery life, and security mechanisms must be efficient to avoid draining the battery quickly. Attacks like routing disruption or excessive message flooding can lead to energy exhaustion, resulting in node failure and loss of network functionality.

2. Attacks on Sensor Networks

Most sensor network routing protocols are quite simple, and for this reason are sometimes even more susceptible to network attacks as compared to general ad-hoc routing protocols. Most network layer attacks against sensor networks fall into one of the following categories (Chris, 2023):

2.1 Hello flood attack

Some routing protocols in WSN require nodes to broadcast hello messages to announce themselves to their neighbors. A node which receives such a message may assume that it is within a radio range of the sender. However in some cases this assumption may be false; sometimes a laptop-class attacker broadcasting routing or other information with large enough transmission power could convince every other node in the network that the attacker is its neighbor. For example, an adversary advertising a very high quality route to the base station could cause a large number of nodes in the network to attempt to use this route. But those nodes which are sufficiently far away from the adversary would be sending the packets into oblivion. Hence the network is left in a state of confusion. Protocols which depend on localized information exchange between neighboring nodes for topology maintenance or flow control are mainly affected by this type of attack (Hamid, 2018). An attacker does not necessarily need to construct legitimate traffic in order to use the hello flood attack. It can simply re-broadcast overhead packets with enough power to be received by every other node in the network. Fig. 2 shows an attacker broadcasting hello packets with more transmission power than a base station. Fig. 3 shows that a legitimate node considers attacker as its neighbor and also as an initiator.

2.2 Sinkhole attacks

In a sinkhole attack, the attacker's goal is to lure nearly all the traffic from a particular area through a compromised node, creating a sinkhole with the adversary at the centre like black hole attack in ad hoc networks. Sinkhole attacks typically work by making a compromised node look attractive to surrounding nodes with respect to the routing algorithm (Chris, 2023).

2.3 The Sybil attack

In Sybil attack, a single node presents multiple identities to other nodes in the network. The Sybil attack can significantly reduce the effectiveness of fault-tolerant schemes such as distributed storage, multipath routing, and topology maintenance. Replicas, storage partitions and routes believed to be used by disjoint nodes could in actuality be used by one single adversary presenting multiple identities (Venkata, 2016).

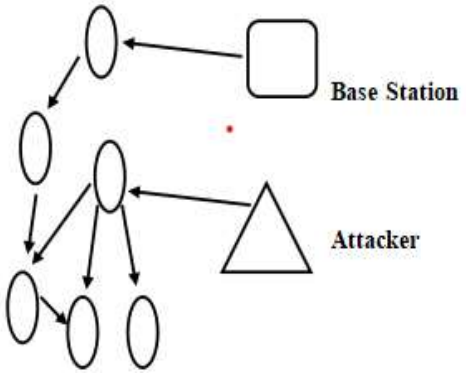

Fig. 2. Attacker broadcasting hello packets.

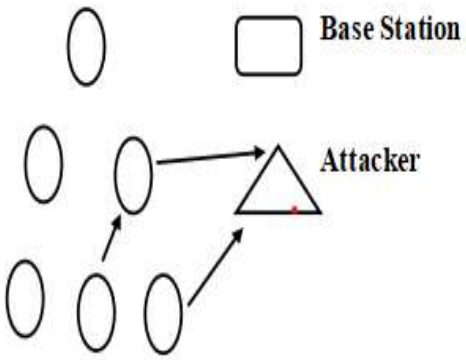

Fig. 3. The attacker is chosen as a neighbor by the sensor nodes.

3.0 Wireless Sensor Network (WSN) Clustering

Almost every application used in WSN works in an environment that is unattended and harsh. In such environments, human monitoring is not always possible. The organization of sensors is finished by controlling methods in an exceptionally huge region with the goal that specially appointed system arrangement is feasible. A huge number (hundreds or thousands) of sensors are required to cover such an enormous area and these nodes are very vitality compelled. The power delivering batteries cannot be consistently revived. Hence, it necessitates that uniquely planned vitality productive steering conventions ought to be actualized in WSN for protecting sensor organize lifetime. Therefore, it is needed that the sensor nodes in the WSN should be grouped into clusters. This is required for satisfying the objective of scalability and high energy efficiency condition in WSN so that the network exists in large scale environments. In clustered hierarchical WSN structure, each of the clusters has a fixed number of member sensor nodes. One of the member sensor nodes that control the entire cluster is called cluster head CH. The task of fusion along with aggregation is performed by CH. The clustering of sensor nodes forms a two-level hierarchy with CH on a higher level and member nodes on a lower level. The cluster members transmit data to the WSN through corresponding CH. These CH's transmit data collected from sensor nodes to the BS directly or using midway communication. The CH sends collected data to long distances so they have to spend higher energy rates. In order to balance the energy consumption of all the sensor nodes, the CH is regularly re-elected among cluster sensor nodes.

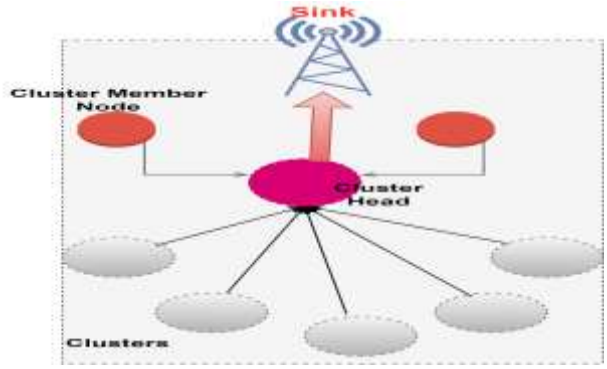

Fig. 4. WSN Clustering

3.1 Formation of Clusters and the Role of a Cluster Head in WSN

During the initialization stage, the nodes send a node-MSG message to the central station. This message contains the remaining energy and the location of the node. This information is needed for clustering by the base station. In the next step, the base station selects the cluster heads based on the available residual energy, average energy and nearness to base station. Then the base station sends a broadcast message that contains the ID of the

selected cluster heads and the corresponding relays. After the cluster heads receive this message and realize their selection as the cluster head, each cluster head broadcasts a CH-ADV message to introduce itself to the network. The remaining nodes choose a nearby cluster head based on the strength of the received CH-ADV signals and transmit a Join-MSG message. Therefore, cluster heads receive and aggregate the data from their cluster members, and then send the aggregated data to base station for decision making.

3.2 Related Works

This section briefly discusses some well-known clustering algorithms in WSN. (Mohseni et al., 2022 proposed a cluster-based routing strategy by combining the fuzzy logic system and the Capuchin search algorithm, called CEDAR. It involves two stages, namely the clustering process and intra- and extra-cluster routing. This strategy significantly cuts energy consumption through clustering the nodes in the network, and each cluster is responsible for routing the packets of the nodes in its own cluster. Additionally, the fuzzy logic system allows the nodes to adapt to the changing network conditions, and the Capuchin search algorithm ensures that the packets are routed in the most efficient way. Simulation results reveal that CEDAR is superior to comparative approaches regarding energy consumption, delay, and network lifetime. Oliveira et al., 2020 Proposed SecLEACH in which the sink authenticates the cluster head nodes and the cluster heads authenticate the joining nodes. In F-LEACH and SecLEACH, sensors are pre-assigned some keys for authentication before their deployment. However, both FLEACH and SecLEACH can prevent only external attackers from joining the cluster formation process. In other words, they cannot prevent internal attackers from declaring themselves as cluster heads and from joining in any cluster. According to (Lakshmanna et al., 2022) introduced a novel cluster-based routing protocol. The objective of this design is to ensure optimal energy utilization and network lifetime. This is achieved by developing an enhanced Archimedes optimization algorithm-driven clustering approach to facilitate the selection of CHs and establishing cluster structures. The suitability function takes into account the number of hops that the data must take to reach its destination, how far apart the nodes are from each other, and the amount of energy consumed. The teaching-learning-based optimization algorithm then uses this information to determine the best route for the data to take. As a result, the network is more efficient and reliable, leading to improved performance.

(Geetha, 2022) proposed a new energy-aware future load prediction and cluster communication strategy for sensor networks. It determines an optimal number of CHs and forecasts the incoming load on the network. It comprises two main phases: clustering with the satin bowerbird algorithm and load estimation using deep random vector functional link networks. A comprehensive analysis of the results and discussion indicates that the proposed method of regulating renewable energy usage in the snsor networks is extremely effective. Buttyan et al., 2019 proposed a cluster head election scheme which conceals the election process from external nodes using cryptographic techniques. However the concealment works for only external attackers since a compromised node can easily unveil the selection result. Moreover, the compromised node can declare itself as a CH even though it is not qualified. According to (Sabrine, 2021) LEACH is a self-organizing, adaptable clustering protocol for WSNs that uses a cluster head rotation technique to distribute energy load uniformly among the network's sensors. Sensor nodes in the target area form groups called clusters, with one node performing as the cluster head of the cluster. LEACH incorporates a random CH rotation scheme, spreading the load across multiple sensors rather than continuously draining the power from a single sensor. An elected CH broadcasts an advertisement packet to inform the neighbouring non-CH nodes about its selection. A non-CH node sends a join request message to the CH from which the strongest advertisement signal was received. After cluster formation, the CH broadcasts a transmission schedule in its cluster to allocate each cluster member one data slot in a frame. A cluster member can transmit only in its own slot. It keeps its radio OFF in the other slots. The CH collects data from all the cluster members and sends an aggregate packet to the BS directly. Sirivianos et al., 2019 proposed the SANE (Secure Aggregator Node Election) protocol in which all CH candidates in a cluster contribute to the generation of a random value and a CH is selected randomly using the random value. SANE is classified into three sub-schemes according to how to generate and distribute the random value. They are Merkle's puzzle based scheme, commitment based scheme, and seed based scheme. Moreover, LEC-MAC uses five parameters to do its job. A PT value is used to distribute CHs in

the network uniformly. The PT value ensures that no region in the target area is crowded with CHs. An MCS value is used to prevent clusters from growing too big. A TE value is used to ensure that low-energy nodes do not become CHs. If the RE of a node is less than the TE, it is not allowed to participate in the CH selection process. A DE value is used to minimize the transmission of redundant data. Sensor nodes located more than DE meters away from the event are not allowed to report the event. A VP is also used, such as ES-MAC and EE-MAC, to reduce idle listening in CHs (Babu, 2022). Quadrant Q-LEACH algorithm, as one of the developed protocols of LEACH. This protocol divides the network environment into regions, where CHs are selected. Although the proposed protocol has relative improvement compared to the LEACH protocol, it has some disadvantages: in each region, CH selection is based on the initial LEACH. In other words, CH is selected randomly and based on the threshold formula, so that residual energy of the nodes is not considered. As a result, problems of LEACH remain in CH selection and data transfer (Ali, 2021& Deepa, 2022). Modified Cluster head selection algorithm was proposed. In LEACH Sensor nodes are organized into clusters. Each cluster has cluster head and member nodes, cluster heads in each cluster are selected randomly. The main disadvantage of LEACH is that if a sensor node with less residual energy is selected as cluster head would die quickly, ultimately the whole cluster would become non-functional. LEACH performs local processing to reduce the amount of data being transmitted to base station (BS), therefore reducing energy consumption and improving network lifetime (Rawat, 2021& Faheem Khan, 2020). Multi-tier Multi-hop Routing in LEACH (MMR LEACH) Protocol was proposed. This protocol uses CH layering in the network by selecting two CHs. The BS divides the entire network into several multi-tiers. The main CH is responsible for collecting, compressing, and transmitting data to the BS as well as selecting the vice CH based on the residual energy. In the process of data transmission, the vice CH acts as an interface between the main CHs of the network bottom layers and the BS. This protocol operates in three phases of clustering with two CHs, cluster layering by BS, and scheduling (Hou, 2022 & Aghera, 2021).

4. Authenticated Cluster Head (CH) Selection using AES cryptographic Methods

In wireless sensor networks (WSNs), clustering is a popular energy-saving technique. However, the effectiveness of this method greatly depends on choosing the appropriate cluster head (CH). Because there is more data to communicate between cluster members and the sink node, improper CH selection might result in high energy use. Using Advanced Encryption Standard (AES) cryptography, this study provides a unique cluster head selection method that addresses energy efficiency and network lifespan (Yuvaraja1, 2024). The proposed approach employs AES for cluster head authentication, guaranteeing that only authorized nodes are capable of functioning as CHs and protecting the network from unauthorized access. In comparison to asymmetric cryptography, AES also makes key management simpler, which makes it more appropriate for WSNs with limited resources. This method enhances energy consumption while improving security, which eventually enhances WSN lifetime and overall performance.

4.1 Requirements for secure CH selection

The signal strength, which sensor nodes utilize to broadcast hello messages, is the primary factor that determines which cluster head (CH) to choose. Higher battery reserve nodes are able to provide stronger signals and have a higher chance of developing into CHs. To increase their chances of being chosen as CH, malicious nodes frequently take advantage of this by broadcasting a stronger Hello message while having a significant power backup. In order to prevent this, malicious nodes are often kept from being selected by the use of a combination of random values and signal strength in CH selection (Singh, 2021). An attacker can still alter these conditions in spite of these protections, which underlines the necessity for a more reliable CH authentication mechanism. The CH selection procedure can incorporate AES (Advanced Encryption Standard) to safeguard this system. The network could make sure that only trusted nodes—rather than compromised or malicious ones—are selected as cluster heads by employing AES to authenticate the cluster heads. By adding an extra layer of security and preventing hackers from taking advantage of power or signal-based weaknesses in the selection process, this cryptographic method makes the WSN more dependable and safe.

4.2 Proposed SLEAD protocol for CH authentication using AES cryptographic Method

For Wireless Sensor Networks (WSNs), the SLEAD (Secure LEACH) protocol is an enhancement on the traditional LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol. It is intended to improve energy efficiency and security during cluster head (CH) selection and communication. The Advanced Encryption Standard (AES) cryptographic techniques are integrated into this protocol to enable secure and verified cluster head selection. The proposed SLEAD protocol's steps are outlined as follows:

1) Node initialization

Sensor nodes with limited energy resources and unique node identities are placed throughout a designated area. Nodes are sensitive of their starting energy levels and locations (or closeness to other nodes).

2) Formation of Clusters:

Depending on how close together nodes are, they are organized into clusters. Every node assesses its energy levels, distance from other nodes, and node degree (that is, the quantity of neighboring nodes) to determine if it is suitable to become a Cluster Head (CH).

3) Cluster Head Designation:

The objective of the dynamic and energy-efficient CH selection process is to lower network wide energy usage. The protocol assesses the proximity and energy of each node. Nodes voluntarily sign up to become CHs, however in order to verify that they are legitimate under the proposed SLEAD protocol, the node must additionally go through an authentication process.

4) CH's AES-Based Authentication:

During the CH selection process, the proposed protocol incorporates AES-based cryptography to ensure safe communication between nodes and the CH. Upon becoming a CH, a node generates a 16-byte AES key hashed using MD5 or another hashing technique, based on its node ID. All communication between the CH and other cluster members is encrypted using the AES key, ensuring that the information is safe, verified, and protected from malicious attempts like eavesdropping and data tampering. In order to verify that only valid CHs are permitted, each node authenticates the CH by confirming its AES-encrypted communications, so ensuring that the only CHs authorized to collect and send data are those that are legitimate.

5) Data Transmission and Aggregation:

Following a successful authentication process, the CH gathers information from all of the cluster's nodes. Then, in order to minimize transmissions and increase network longevity, the CH securely sends the aggregated data over the AES-encrypted communication channel to the base station (sink).

6) Re-authentication of the Dynamic CH:

To maintain a balance in the nodes' energy usage, the CH role is alternated on frequently. A new node must go through the same AES-based verification procedure to confirm its authenticity and identity before it can take on the function of CH.

4.3 Flowchart and operation stages of SLEAD Protocol

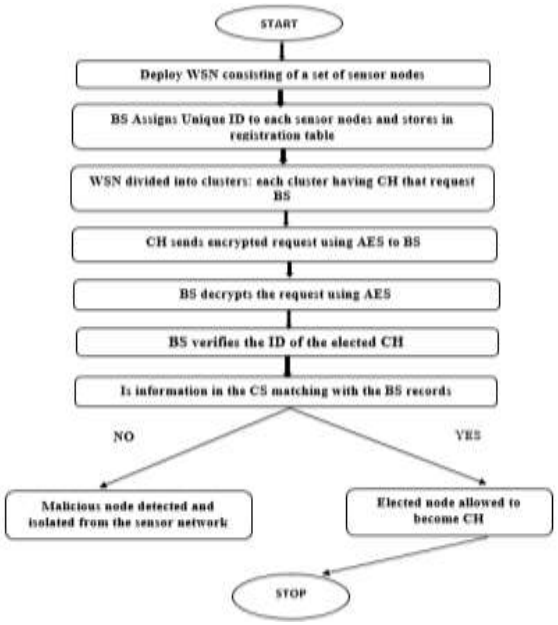

Fig 5: Enhanced HFS-LEACH (SLEAD) FLOWCHART with AES

5. Simulation and Results

In this simulation, the Enhanced HFS-LEACH (SLEAD) algorithm was implemented using Python within a Jupyter Notebook environment. In addition to the 50 randomly placed sensor nodes, three

malicious nodes were added to the network to simulate common network attacks: the reply attack, sinkhole attack, and HELLO flood. For secure communication, each node even the malicious ones were assigned a unique AES key that was created using the node ID's MD5 hash. The network's performance under both normal and attack situations was assessed using a number of metrics in the simulation. These included energy consumption, latency, overhead, throughput, and packet delivery ratio (PDR). Matplotlib was used to generate visualizations of node deployment and the effects of attacks on the network, showing the node placement and distribution of attackers.

5.1 Network Visualization and Deployment of Wireless Sensor Networks

In a wireless sensor network (WSN), the figure 6 shows the network under attack with the initial sensor node deployment. The “Initial Network Deployment” diagram on the left illustrates the random distribution of sensor nodes (shown by colorful circles) over an 800x800 m region. These nodes distributed equally throughout the network and perform normally. A HELLO flood node (red 'X'), a Reply attack node (purple diamond), and a Sinkhole node (orange square) are three examples of malicious nodes that have been added to the same network in the right plot, which is named "Network with Attacks". These malicious nodes seek to attack network security and interfere with communication. The graphic comparison highlights the importance of strong security measures, as the AES-based encryption employed in the Enhanced HFS-LEACH (SLEAD) algorithm, to safeguard against such attacks while ensuring the network’s efficiency and reliability.

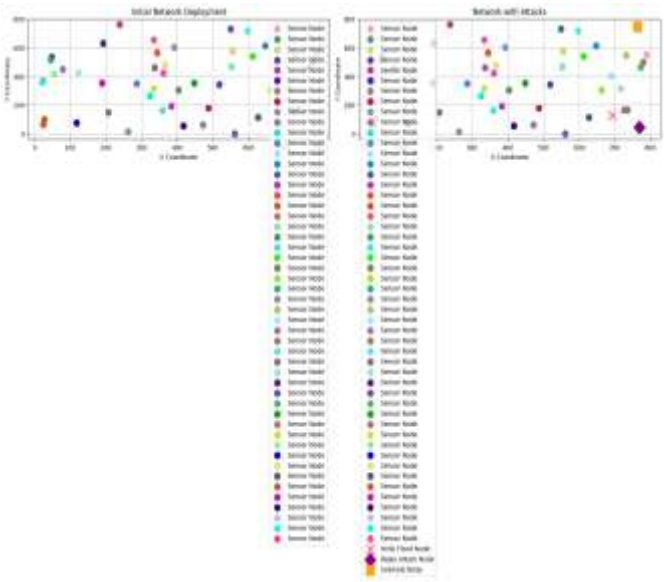

Fig 6: Visualization of Initial Sensor Node Deployment and Network Under Attack in Wireless Sensor Network.

5.2.1 Throughput

By ensuring that only legitimate cluster heads (CHs) were selected, the Enhanced HFS-LEACH (SLEAD) algorithm improved the throughput overall. The system successfully prevented malicious nodes, like those launching HELLO flood attacks, from taking control of data transmission by using AES-based authentication for CH selection. This preventive technique resulted in better packet transmission rates across the network, ensuring network reliability despite attack attempts. The total number of packets successfully delivered to the destination divided by the simulation's total time is known as throughput. Throughput is calculated as (total packets sent to the destination) / (simulation time). Figure 3.1 illustrates Enhanced HFS-LEACH (SLEAD) throughput while maintaining an attack and without an attack.

5.2.2 Packet Delivery Ratio (PDR)

Using the Enhanced HFS-LEACH (SLEAD) algorithm resulted in a significant increase in the packet delivery ratio. The approach improved the successful delivery of packets to their intended destination by using AES cryptography to secure the CH selection process. This confirmed that legitimate nodes were in charge of routing data. In situations with active attacks, where rogue nodes would often prevent data flow, this gain was particularly

noticeable. PDR is defined as (packets received/packets generated) * 100. Figure 3.1 illustrates Enhanced HFS-LEACH (SLEAD) packet delivery ratio (PDR) while maintaining an attack and without an attack.

5.2.3 Delay

Due to the additional processing steps required for AES encryption and CH authentication, the Enhanced HFS-LEACH (SLEAD) technique introduced a slight spike in delay. However, considering the increased security benefits, this increase was minor and reasonable. The average time between packet generation and successful delivery was used to calculate the delay, and although it was greater than in an unsecured network, it was still within reasonable limits for most WSN applications. Delay is calculated as Delay = ∑ (received time – send time) / ∑ (number of connections). Figure 3.1 illustrates Enhanced HFS-LEACH (SLEAD) delay while maintaining an attack and without an attack.

5.2.4 Overhead

When the Enhanced HFS-LEACH (SLEAD) approach was implemented, the simulation demonstrated a reduction in network overhead. Malicious nodes flooded the network with control messages in situations without AES authentication, greatly increasing the overhead. Even in spite of threats, the Enhanced HFS-LEACH (SLEAD) method decreased unnecessary communication and overhead by authenticating CHs using AES. Figure 3.1 illustrates Enhanced HFS-LEACH (SLEAD) overhead while maintaining an attack and without an attack.

5.2.5 Energy Consumption

By preventing malicious nodes from turning into CHs, AES cryptography helped the network preserve energy. Since they were not required to react to communication triggered by an attack, legitimate sensor nodes were able to function more effectively under normal circumstances. Consequently, the overall energy usage was optimized, resulting in an extended lifespan for the network. The level of strength utilization is calculated as follows: Initial energy − current energy = Energy consumption. Figure 7. illustrates Enhanced HFS-LEACH (SLEAD) energy consumption while maintaining an attack and without an attack.

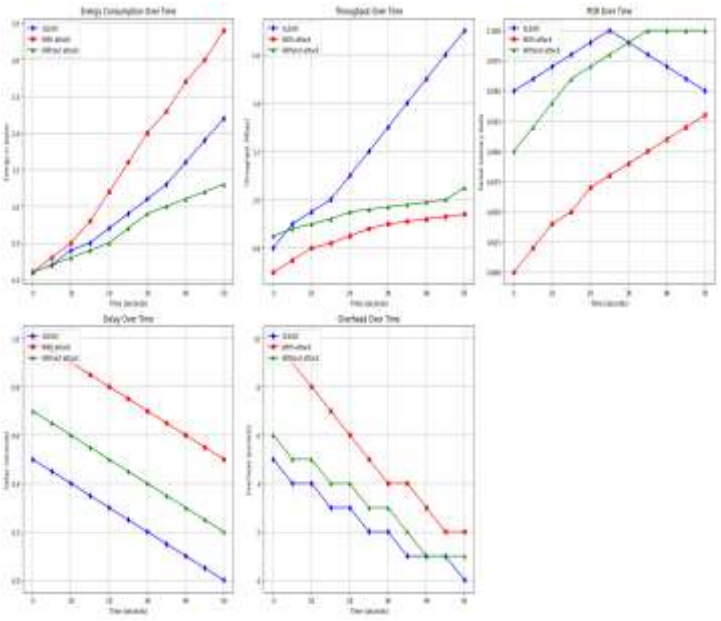

Fig 7. Figures illustrating simulation results

In conclusion, the simulation results demonstrated that by using AES-based authentication for CH selection, the Enhanced HFS-LEACH (SLEAD) method effectively reduced a range of attacks and enhanced network performance. With significant improvements in throughput, packet delivery, and energy conservation, the small rise in the processing latency was worth the trade-off.

5.3 Comparison with Existing Technique

When the HFS-LEACH and SLEAD protocols are compared, it becomes evident that SLEAD uses more energy during the simulation. The energy consumption graph shows that SLEAD uses less energy than HFS-LEACH, which is important for prolonging the life of the network, particularly in wireless sensor networks (WSNs). When energy conservation is a primary concern, SLEAD is an effective option considering its energy efficiency advantage. When it comes to network performance, SLEAD significantly outperforms HFS-LEACH in terms of throughput and packet delivery ratio (PDR). Figure 8. illustrates Performance Comparison of HFS-LEACH and SLEAD Protocols in Wireless Sensor Networks (WSN).

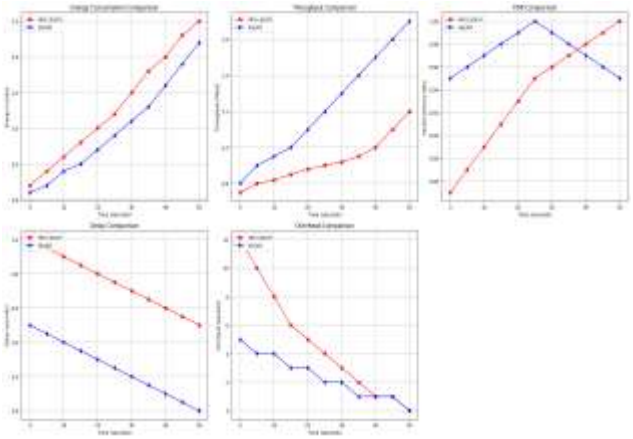

Fig 8: Performance Comparison of HFS-LEACH and SLEAD Protocols in WSN

SLEAD is effective in reducing overhead and communication delays. According to the delay comparison, SLEAD continuously has reduced latency, which improves data transfer. SLEAD's total efficiency is also enhanced by maintaining a substantially lower overhead throughout the simulation, which results in decreased processing and communication costs. Because of these characteristics, SLEAD is more suited for situations where low overhead and speedy data delivery are crucial.

6. Conclusion

Given an emphasis on energy efficiency and secure communication, the proposed SLEAD protocol improves upon traditional cluster-based routing algorithms in Wireless Sensor Networks (WSNs). By implementing AES cryptographic methods for Cluster Head (CH) authentication, this improvement guarantees secure communication and addresses issues such as packet loss and energy usage. SLEAD is perfect for resource-constrained WSN situations since it uses AES to simplify key management while providing strong security in comparison to asymmetric cryptographic techniques. In order to preserve network integrity and data security, the AES integration prevents unauthorized nodes from assuming CH roles. Plotting the results shows that proposed algorithm performs better than the existing HFS-LEACH in a number of crucial areas. It is more effective in energy-constrained scenarios because it exhibits noticeably lower energy consumption, reduced communication overhead, and lower latency. This is essential for increasing the network's lifespan, which is a primary goal of WSNs. SLEAD has a better throughput and Packet Delivery Ratio (PDR), reduced overhead and faster data transmission (lower delay) which demonstrate that it is suitable for real-time applications where speed and limited processing are critical.

Future studies on the SLEAD protocol could focus on improving its adaptability and security. While AES offers robust encryption for cluster head authentication, exploring hybrid cryptographic techniques that integrate symmetric and asymmetric methods could enhance security even more without sacrificing efficiency. The protocol may become more secure by using lightweight machine learning models, which may also allow for the real-time detection of possible anomalies or attacks. Furthermore, by taking into account variables like node energy levels, traffic patterns, and mobility, improvements in adaptive Cluster Head (CH) selection techniques such as integrating machine learning for real-time decision-making can maximize network performance.

References:

[1]. Aghera, K., Pambhar, H., & Tada, N. (2021). MMR-LEACH:Multi-tier multi-hop routing in LEACH protocol. In Proceedings of international conference on communication and networks.Berlin: Springer.

[2]. Ali, H.; Tariq, U.U.; Hussain, M.; Lu, L.; (2021). Panneerselvam, J.; Zhai, X.J. ARSH-FATI: A Novel Metaheuristic for Cluster Head Selection in Wireless Sensor Networks. IEEE Syst. J., 15, 2386–2397.

[3]. B. Geetha, P. S. Kumar, B. S. Bama, S. Neelakandan, C. Dutta, and D. V. Babu, "Green energy aware and cluster based communication for future load prediction in IoT," Sustainable Energy Technologies and Assessments, vol. 52, p. 102244, 2022.

[4]. Babu, P.R.; Debasis, K. A Low Energy Consuming MAC Protocol forWireless Sensor Networks. In Proceedings of the 2022 2nd International Conference on Artificial Intelligence and Signal Processing (AISP), Vijayawada, India, 12–14 February 2022; pp. 1–5.

[5]. Bhatia, T., et al. (2020). A genetic algorithm-based distance aware routing protocol for wireless sensor networks. Computers& Electrical Engineering, 56, 441-455.

[6]. Buttyan Zahoor el Houssaini, D.; Kammoun, I.; Kanoun, O. Precision irrigation: An IoT-enabled wireless sensor network for smart irrigation systems. In Women in Precision Agriculture;

Springer: Cham, Switzerland, 2019; pp. 107–120.

[7]. Chris, Ameh, Saboor, S. (2023). An Energy-Efficient Cluster Head Selection and Secure Data Transmission in WSN using Spider Monkey Optimized Algorithm and Advanced Hybrid Cryptographic with Security. Category: STEM (Science, Technology, Engineering and Mathematics), doi: 11.53802/sctconf3254891, 16.

[8]. Deepa, S., Marimuthu, C., & Dhanvanthri, V. (2022). Enhanced Q-LEACH routing protocol for wireless sensor networks. ARPNJournal of Engineering and Applied Sciences, 10(9), 4036-4041. Elements.Statistics and Simulation, 391-402. https://doi.org/10.1007/978-3-319-76035-3_28

[9]. Dionisis,Tariq, Abubakar, Mahmood.; Hussain, J.; Mu, W.; (2020). Panneerselvam, K.; Bhai, X.J. ASHRAF-SADI: A Novel Metaheuristic for Cluster Head Selection in Wireless Sensor Networks. IEEE Syst. J., 15, 2386–2397

[10]. Faheem Khan (2020). Routing Techniques in Wireless Sensor Networks: Wireless Sensor Networks for Condition Monitoring in the Railway Industry.

[11]. Gautam, Tantawy, Chauhan, S. (2021), Clustering protocols in wireless sensor network: A survey, classification, issues, and future directions. Computer. Sci. Rev. 42, 100578.

[12]. Hamid,Chambhar, H., & Tada, N. (2018). O-LEACH,MMR-LEACH:Multi-tier multi-hop routing in LEACH protocol. In Proceedings of international conference on communication and networks.Berlin: Springer.

[13]. Hou, J.; Qiao, J.H.; Han, X.L. (2022). Energy-Saving Clustering Routing Protocol for Wireless Sensor Networks Using Fuzzy Inference. IEEE Sens. J. 22, 2845–2857.

[14]. Jen, Taureed, Venkata, Deen (2012). A genetic algorithm-based distance aware routing protocol for wireless sensor networks. Computers& Electrical Engineering, 66, 542-541.

[15]. JU, Khareem, Taoreed, L.B.; Khaleed, M.; Du, W.; (2021). Pannyselvam, J.; Zhai, X.J. ARSH-FATI: A Novel Metaheuristic for Cluster Head Selection in Wireless Sensor Networks. IEEE Syst. J., 15, 2386–2397

[16]. K. Lakshmanna, N. Subramani, Y. Alotaibi, S. Alghamdi, O. I. Khalafand, and A. K. Nanda, "Improved metaheuristic-driven energy-aware cluster-based routing scheme for IoT-assisted wireless sensor networks," Sustainability, vol. 14, no. 13, p. 7712, 2022.

[17]. Koulouras, Saleem, Tariq, B, S, U.; Hasheem, N.; Zu, G.; (2020). Panneerselvam, J.; Zhai, X.J. ARSH-FATI: A Novel Metaheuristic for Cluster Head Selection in Wireless Sensor Networks. IEEE Syst. J., 15, 2386–2397

[18]. Lata, Sabir, Chandoo, Pambhar, H., & Sada, M. (2021). SEC-LEACH,MMR-LEACH:Multi-tier multi-hop routing in LEACH protocol. In Proceedings of international conference on communication and networks. Berlin: Springer.

[19]. L. B. Oliveira, H.C. Wong, M. W. Bern, R. Dahab, and A.A. Loureiro, "SecLEACH-a random key distribution solution for securing clustered sensor networks," Proc. Of 5th IEEE Int'l Symp. On Network Computing and Applications, Cambridge, Massachusetts, USA, Jul. 24-26, 2020

[20]. L. Buttyan and T. Holczer, "Private Cluster Head Election in Wireless Sensor Networks," Proc. of the Fifth IEEE Int'l Workshop on Wireless and Sensor Network Security (WSN '09), IEEE, pp. 1048-1053, 2019

[21]. M. Mohseni, F. Amirghafouri, and B. Pourghebleh, "CEDAR: A cluster-based energy-aware data aggregation routing protocol in the internet of things using capuchin search algorithm and fuzzy logic," Peer-to-Peer Networking and Applications, pp. 1-21, 2022.

[22]. M. Sirivianos et al., "Non-manipulable Aggregator Node Election Protocols for Wireless Sensor Networks," Proc. of Int'l Sympo. on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt '07), Cyprus, pp. 1-10, Apr. 2019

[23]. M. Yuvaraja1 , S. S. (2024). An Energy-Efficient Cluster Head Selection and Secure Data Transmission in WSN using Spider Monkey Optimized Algorithm and Hybrid Cryptographic with Security. Category: STEM (Science, Technology, Engineering and Mathematics), doi: 10.56294/sctconf2024650, 13.

[24]. Rawat, P.; Chauhan, S. (2021), Clustering protocols in wireless sensor network: A survey, classification, issues, and future directions. Computer. Sci. Rev. 40, 100396.

[25]. Rehman, Chandrakasan,Chauhan, S. (2022), Clustering protocols in wireless sensor network: A survey, classification, issues, and future directions. Computer. Sci. Rev. 40, 101620.

[26]. Sabrine, K.; el Houssaini, D.; Kammoun, I.; Kanoun, O. Precision irrigation: An IoT-enabled

wireless sensor network for smart irrigation systems. In Women in Precision Agriculture; Springer: Cham, Switzerland, 2021; pp. 107–129.

[27]. Singh, R., Singh, R., & Kaur, P. (January 2021,). Securing Cluster Head in Wireless Sensor Network for Internet of Things. International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 10, (Issue. 1,), pg.49 – 60.

[28]. Venkata, Taureed., et al. (2016). A genetic algorithm-based distance aware routing protocol for wireless sensor networks. Computers& Electrical Engineering, 56, 451-450.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.