University of Ibadan Journal of Science and Logics in ICT Research (UIJSLICTR)

ISSN: 2714-3627

A Journal of the Department of Computer Science, University of Ibadan, Ibadan, Nigeria

Volume 14 No. 1, June, 2025

journals.ui.edu.ng/uijslictr
http://uijslictr.org.ng/
uijslictr@gmail.com

University of Ibadan
Journal of Science and Logics in ICT Research

Performance Evaluation of MANET Protocols against Sleep Deprivation Attacks

[1] Deji-Akinpelu O. O., [2] Kuranga M. O. and [3]Osunade O. O.

Dominican University and University of Ibadan
deji-akinpelu.o@dui.edu.ng (Deji-Akinpelu O.), muhammedkuranga@gmail.com (Kuranga M.),
o.osunade@ui.edu.ng (Osunade O.)

Abstract

Mobile Ad-Hoc Networks (MANETs) are critical in many modern applications due to their flexible and decentralized nature. However, they face significant security challenges, notably Sleep Deprivation Attacks (SDAs), which can severely degrade network performance. This study evaluates the performance of three MANET routing protocols—Adaptive On-demand Distance Vector (AODV), Low Energy Adaptive Clustered Hierarchical (LEACH), and Ensemble On-demand Low Energy Adaptive Clustered Hierarchical (EO-LEACH)—under SDA conditions before and after the application of clustering techniques. Using MATLAB for simulation, the study compares protocol performance based on Packet Delivery Ratio (PDR), Average Energy Consumption, and End-to-End Delay. The findings highlight the importance of clustering in enhancing protocol resilience and efficiency, providing valuable insights for the design of more secure and robust MANETs.

Keywords: *Ensemble On-demand Low Energy Adaptive Clustered Hierarchical (EO-LEACH), On-demand Distance Vector (AODV), Low Energy Adaptive Clustered Hierarchical (LEACH), Routing protocol, Clustering techniques, Ensemble*

1. Introduction

Mobile Ad-Hoc Networks (MANETs) have garnered significant attention in recent years due to their inherent flexibility and adaptability. Unlike traditional networks, MANETs do not rely on fixed infrastructure, making them ideal for scenarios where establishing such infrastructure is impractical or impossible. Nodes in a MANET communicate directly with each other, dynamically forming and maintaining network connectivity. This characteristic makes MANETs particularly suitable for applications in military operations, disaster response, and vehicular communication systems [1].

However, the absence of a centralized control mechanism also exposes MANETs to various security threats, among which Sleep Deprivation Attacks (SDAs) are particularly detrimental. SDAs are a type of Denial-of-Service (DoS) attack that deplete the energy resources of nodes, leading to network failure. The attack forces nodes to remain active by sending constant requests, thereby consuming their battery power and rendering them inoperative [7]. This attack can be implemented by forcing the targeted node to use its vital resources, such as battery, network bandwidth, and computing power, by sending false requests for existent or non-existent destination nodes.

While clustering techniques have been proposed to improve the efficiency and security of MANETs, their specific impact on mitigating the effects of SDAs is not well understood. This study aims to evaluate the performance of three MANET protocols Adaptive On-demand Distance Vector (AODV), Low Energy Adaptive Clustered Hierarchical (LEACH), and Ensemble On-demand Low Energy Adaptive Clustered Hierarchical (EO-LEACH) under SDA conditions before and after the application of clustering techniques.

The aim of this study is to assess the effectiveness of clustering techniques in enhancing the performance and security of MANET protocols under SDA conditions. The selected protocols (AODV, LEACH, and EO-LEACH) in MATLAB.are implemented. SDA is simulated before and after applying clustering techniques. The protocols are

Deji-Akinpelu O. O., Kuranga M. O. and Osunade O. O. (2025). Performance Evaluation of MANET Protocols against Sleep Deprivation Attacks. *University of Ibadan Journal of Science and Logics in ICT Research (UIJSLICTR),* Vol. 14 No. 1, pp. 246 – 253

evaluated using metrics such as Packet Delivery Ratio (PDR), Average Energy Consumption, and End-to-End Delay.

This study presents a novel method for assessing the effectiveness of MANET protocols when subjected to Sleep Deprivation Attacks (SDA). This study is unique in that it introduces a clustering strategy before and after Sleep Deprivation Attacks (SDA) on network nodes, which sets it apart from other studies that either use clustering or no clustering at all. This novel approach allows for a thorough examination of the influence of SDA on MANET protocols, notably AODV, LEACH, and EO-LEACH.

This work aims to provide a comprehensive understanding of how SDA impacts the selected protocols by conducting a performance assessment utilizing several network performance measures. The results of this study are vital for enhancing the efficiency and safety of Mobile Ad hoc Networks (MANETs) against SDA attacks. Additionally, the findings provide guidance on selecting the most suitable approach, whether with or without clustering, for establishing a MANET. This is crucial for ensuring dependable communication in diverse applications, such as military operations, emergency response systems, and Internet of Things (IoT) networks.

2. Related Works

Sushma *et al*. [8] examined the effectiveness of cluster-based intrusion detection systems (IDS) in mobile ad hoc networks. These systems use efficient clustering protocols to detect intrusions while minimizing resource use. However, they face challenges in maintaining stable clusters as network routes change.

Fotohi and Bari [3] introduced a countermeasure for Denial of Sleep Attacks (DoSA) in Wireless Sensor Networks (WSN) using a hybrid approach called WSN-FAHN. This technique combines Firefly and Hopfield Neural Networks (HNN) algorithms to enhance network security and extend node lifespan. By employing a mobile sink and the Firefly algorithm based on the LEACH protocol, the method addresses the issue of rapid energy depletion near fixed sinks, thereby improving overall network durability and resilience against DoSA.

Deji-Akinpelu and Osunade [2] combined the strengths of the two routing protocols, AODV and LEACH, to develop a more secured routing protocol, for the prevention of Sleep Deprivation Attack (SDA) during data transmission. The Ensemble On-demand Low Energy Adaptive Clustered Hierarchical (EO-LEACH) routing protocol minimised the impact of sleep deprivation attacks on mobile ad-hoc networks compared to the other protocol

Hemalatha *et al.* [4] examined a novel routing algorithm for efficient packet transmission in MANETs using the T-Test Procedure and Sleep and Awake Strategy. The study identified the optimal communication paths between nodes, ensuring that nodes had sufficient energy for transmission during route discovery. The T-Test procedure evaluated and selected nodes, enhancing the route discovery process. This technique, combined with the sleep and awake strategies, enabled successful packet transmission in MANETs. The algorithm was tested through network simulation and compared favorably to existing routing systems.

Khan *et al.* [5] investigated the security aspects of Mobile Ad Hoc Networks (MANETs), focusing on attack analysis and node misbehavior problems. The study provides a comprehensive analysis of MANET security concerns, discussing critical elements and applications of these networks. Attacks on MANETs are categorized by origin, behavior, involved nodes, processing power, and stacking. The research examines various node misbehaviors and their patterns, categorizing two main types of misbehavior. A significant issue identified is minimizing node misbehavior to ensure network availability and functionality. The study also explores methods for detecting nodes that misroute packets, highlighting strategies to enhance network security.

In Mohd *et. al.* [9], the authors showed an implementation of a Support Vector Machine (SVM) based intrusion detection protocol to detect denial of sleep attacks. With the model starting with 19 features and then reducing to 7 significant features, this proposed model is able to improve security of WSN’s through quick identification.

Machine learning methods can be used to detect other Denial of Service (DOS) attacks besides denial of sleep attacks as shown by Akpinar *et. al.* [10]. The authors made use of a machine learning model to develop a detection model that can identify DOS attacks. Such as in Vivekanadam [11] where the author made use of a hybrid methodology combining a Hopfield Neural Network (HNN) with a firefly algorithm to address DOS attacks (DOSA). The author also made use of the LEACH protocol as a frame works to improve efficiency and performance. With simulation, these new protocols were found to use less power to transmit data compared to cross-layer methods.

Kumar *et al.,* [13] proposed a new security framework called the Random Number Generator with Hierarchical Intrusion Detection System (RNGHID). This new framework is developed to defend network against both the sleep deprivation and Sybil attack. With this new framework is built using a Intrusion Prevention System (IPS). This new proposed system were tested in a simulation and show that this method has an acceptable latency when mitigating DOS attacks in a single MANET. The limitation of this work are the limited generalization of the identification method in infrastructure-less networks where attacks are more adaptative.

In terms of developing dynamic approaches to aid in enhancing the security of MANETs, Mankotia *et al.,* [12] have discussed this in the paper. The authors proposed a dynamic threshold-based approached that combines monitoring mechanics that allow for detection of these accounts. This was done using set dynamic thresholds for network parameters and to constantly monitor network traffic to find black hole attacks. The main advantage of this study is that this method is focused in particular on energy depletion attacks that affect network longevity.

3. Methodology

This is experimental research, where the first step in the method approach for assessing the performance of MANET protocols against Sleep Deprivation Attacks (SDA) is the construction of three MANET protocols (AODV, LEACH, and EO-LEACH) totalling 100 nodes in a MATLAB simulation environment. Subsequently, the field dimension and sink coordinates were established for the protocols, the parameters required to compute the protocols' energy consumption were initialized, SDA was presented, and an upper bound on the total number of simulation runs was established. Prior to clustering, data was saved for comparison and a simulation was run to assess the efficacy of the chosen procedures (AODV, LEACH, and EO-LEACH). Following clustering, another simulation was performed, involving the partitioning of nodes into clusters to facilitate communication, selection of cluster gateways, and election of cluster heads.

The simulation was subsequently assessed using multiple performance metrics such as Packet Delivery Ratio (PDR), Average Energy Consumption (AEC), Throughput, and End-to-End Delay. The indicated routing protocols (AODV, LEACH, and EO-LEACH) were utilized to carry out many tests. Every experiment is specifically constructed to replicate distinct scenarios involving clustering, as well as scenarios without clustering. Additionally, some experiments involve the use of SDA, while others do not. The purpose of these experiments is to assess the performance of the procedures under diverse settings. The simulation enables the creation of comprehensive logs, which are then examined to obtain pertinent performance metrics findings.

Figure 1 displays the generic model that was designed to show the step-by-step realization of the task. This model outlines the process of conducting the experiment, starting with the initialization of the nodes and running a simulation before clustering. It includes the selection of cluster gateways, the clustering of nodes, and the selection of cluster heads. The model also incorporates the introduction of a Sleep Deprivation Attack and sets out when to evaluate using different performance metrics before showing the final result.

This research work was simulated using MATLAB's comprehensive simulation capabilities on network environments through the use of Simulink. Simulink is a MATLAB plugin that enables the modeling, simulation, and analysis of dynamic systems. It offers a visual interface for constructing block diagrams that represent the components of a system and how they interact with each other. Simulink is used to do the following:

System Initialization: Specify the system parameters, including the number of nodes, initial energy levels, communication range, and simulation time.

Node Behavior Modeling: Represent each node as a subsystem or block in Simulink.

Communication Channels and Propagation: Consider route loss, fading, and interference.

Routing and Data Exchange: Define how nodes discover neighbors, exchange control messages, and route data packets, implementing data aggregation if needed.

Performance Metrics Collection: Integrate blocks to collect performance metrics:

Packet delivery ratio (PDR).
End-to-end delay.
Average Energy Consumption (AEC).
Network lifetime.

Visualization and Analysis: Use Simulink scopes, displays, and graphs to visualize simulation results. Analyze how the MANET behaves under different scenarios.

This study employs a simulation-based approach to evaluate the performance of MANET protocols under SDA conditions. The research design involves implementing the AODV, LEACH, and EO-LEACH protocols in MATLAB and simulating their performance before and after the application of clustering techniques.

The experimental setup includes 100 nodes randomly distributed in a simulated environment. The nodes communicate using the three selected protocols, and SDAs are introduced to assess their impact on network performance. Clustering techniques are then applied, and the simulations are repeated to evaluate the improvement in performance.

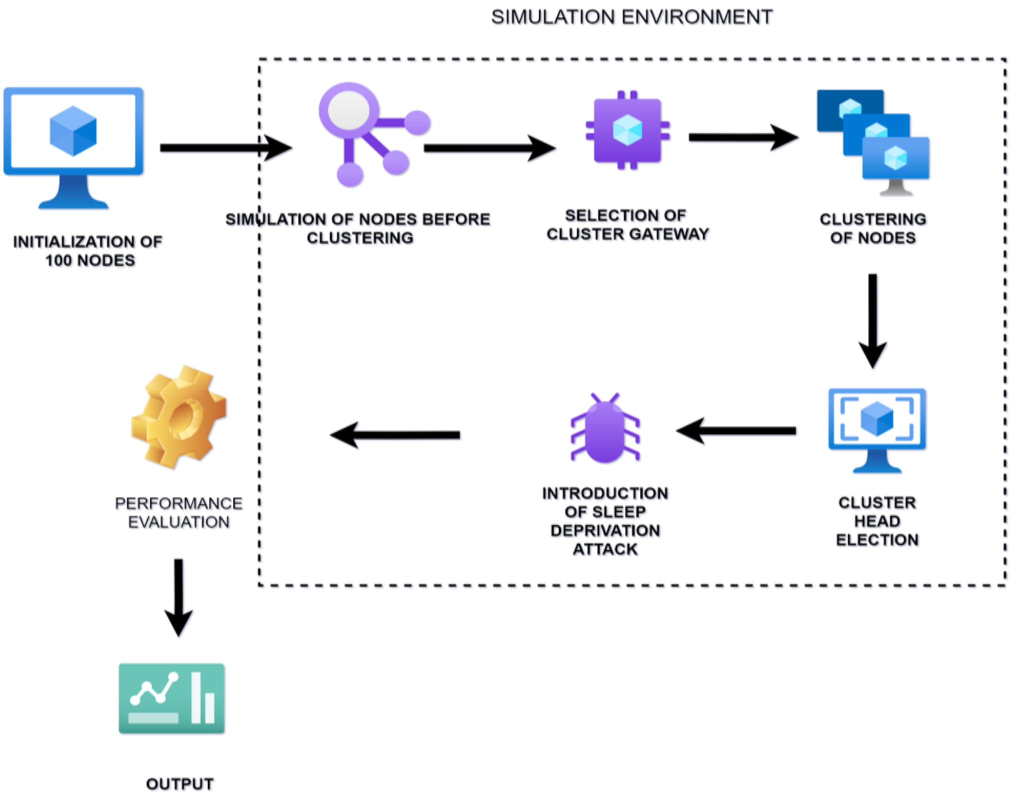
SIMULATION ENVIRONMENT
INITIALIZATION OF 100 NODES
SIMULATION OF NODES BEFORE CLUSTERING
SELECTION OF CLUSTER GATEWAY
CLUSTERING OF NODES
CLUSTER HEAD ELECTION
INTRODUCTION OF SLEEP DEPRIVATION ATTACK
PERFORMANCE EVALUATION
OUTPUT

Figure 1: Generic Model of the simulation environment

Evaluation Metrics

The evaluation of each protocol (AODV, LEACH, EO-LEACH) was evaluated based on several key metrics, including:

Packet Delivery Ratio (PDR): The ratio of successfully delivered packets to the total packets sent.

$$\text{PDR} = \frac{\text{Number of Packets Successfully Delivered}}{\text{Number of Packets Generated}}$$

Throughput: The rate of successful data delivery over the network.

$$\text{Throughput} = \frac{\text{Total Data Successfully Delivered}}{\text{Total Time}}$$

End-to-End Delay: The time taken for a packet to travel from the source to the destination.

End-to-End Delay = $\frac{1}{N}\sum_{i=1}^{N}(T_i^{Received} - T_i^{Sent})$

Average Node Energy Consumption: The average energy consumed by nodes in the network.

Average Energy Consumption = $\frac{\sum_{i=1}^{N} Ei}{N}$

Network Time: The total duration of the simulation run.

Network Lifetime = Time until the first node depletes its energy

SDA Success Rate: The effectiveness of the protocol in mitigating the impact of Sleep Deprivation Attacks.

SDA_SDR = $\frac{N_{Successful}}{N_{Total}}$ $X\ 100\%$

Total Data Transfer: The amount of data transmitted across the network.

4. Results and Discussion

The performance of the selected routing protocols, (AODV, LEACH, and EO-LEACH) were evaluated using metrics such as Packet Delivery Ratio, End-To-End Delay, Throughput, Network Time, and Average Energy Consumption.

Table 1: Performance metrics summary for each protocol (AODV, LEACH, EO-LEACH) without Clustering

Protocol	Network Time (s)	Total Data Transfer (bytes)	End-to-End Delay (s)	Average Node Energy Consumption	Throughput (bytes/s)	Packet Delivery Ratio (%)
AODV	2.13	1536	0.18	-	8.533	94.9
LEACH	2.14	1065	1.02	0.2	8.044	94.3
EO-LEACH	2.11	1862	0.25	0.1	8.743	95.2

Table 2: Performance metrics summary for each protocol (AODV, LEACH, EO-LEACH) with Clustering

Protocol	Network Time (s)	Total Data Transfer (MB)	End-to-End Delay (s)	Average Node Energy Consumption (J)	Throughput (Mbps)	PDR (%)
AODV	1500	300	1.2s	1.2	6	94.7
LEACH	1800	250	1.5s	1.4	5	93.5
EO-LEACH	1600	275	1.1s	1.2	5.5	92.2

Table 3: Performance comparison of Adaptive On-demand Distance Vector (AODV) protocol before and after clustering.

Protocol	Nodes	Clustering	Network Time (s)	Total Data Transfer	End-to-End Delay (s)	Avg Node Energy Consumed	Throughput	SDA Success Rate	Packet Delivery Ratio (PDR) %
AODV	100	No	2.13	1536	0.18	-	8.533byte	N/A	94.9
AODV	100	Yes	1500	300 Mb	1.2	1.2	6Mbps	0.85	94.7

The implementation of this research work was done with MATLAB using Simulink extension to perform the simulation and to access the outputs.

The evaluation of each protocol without clustering yielded insightful results. For Adaptive On-demand Distance Vector (AODV), the network exhibited efficient routing with low end-to-end delay and high throughput. Low Energy Adaptive Clustered Hierarchical (LEACH) demonstrated energy-efficient clustering, leading to reduced average node energy consumption. Ensemble On-demand Low Energy Adaptive Clustered Hierarchical (EO-LEACH), leveraging the strengths of both AODV and LEACH, achieved a balance between energy efficiency and routing performance.

The table 1 shows the result of AODV, LEACH, and EO-LEACH protocols without clustering, showcasing their performance using performance metrics like Network Time, Total Data Transfer, End-to-End delay, Throughput, Average Energy Consumption, Packet Delivery Ratio.

Without clustering, Introducing Sleep Deprivation Attacks into the network significantly impacted the performance of all three protocols. Without clustering, AODV had the best End-to-End delay time of (0.18), and EO-LEACH comes immediately after with (0.25) and whereas LEACH had (1.02). Without clustering, EO-LEACH tends to outperform the other protocols AODV, and LEACH, showcasing its strength derived from combining the two protocols (AODV and LEACH) to create by demonstrating the best Network Time (2.11), compared to AODV (2.13) and LEACH (2.14). EO-LEACH also boast of the best Total Data Transfer of (1862) while AODV and LEACH had (1536) and (1065) respectively. EO-LEACH showed a low Average Energy Consumption of (0.1) and LEACH had (0.2). EO-LEACH has the best Packet Delivery Ratio of the three protocols without clustering with (95.2) coming second to this is AODV with (94.9) and LEACH had (94.3).

AODV experienced reduced performance due to route disruptions caused by SDA. LEACH suffered from cluster destabilization and increased energy consumption, leading to degraded performance metrics. EO-LEACH demonstrated resilience to SDA, leveraging its adaptive clustering and on-demand routing capabilities to mitigate the impact of attacks.

Table 2 shows the results of the AODV, LEACH, and EO-LEACH protocols with clustering, showcasing their performance using performance metrics like Network Time, Total Data Transfer, End-to-End delay, Throughput, Average Energy Consumption, Packet Delivery Ratio.

With clustering, AODV outperforms EO-LEACH and LEACH in terms of Total Data Transfer (300Mb) with EO-LEACH coming second with (275Mb) and LEACH having (250Mb). AODV also had the best throughput of the three protocols boasting (6Mbps) and EO-LEACH coming second with (5.5Mbps), LEACH had (5Mbps). AODV also has the best Packet Delivery Ratio with (94.7%) and LEACH coming second with (93.5%) with EO-LEACH having (92.2%). AODV also boosts the best Network Time of (1500) with LEACH and EO-LEACH having (1800) and (1600) respectively.

EO-LEACH also performs significantly well with clustering having the best End-to-End Delay time of (1.1s) in comparison to AODV (1.2s) and LEACH (1.5s), EO-LEACH also has a very good Average Energy Consumption rate of (1.2J) sharing this with AODV (1.2J) while LEACH had (1.4J).
With clustering, AODV demonstrated the best performance in mitigating SDA attacks among the three protocols (AODV, LEACH, EO-LEACH). Also, EO-LEACH performs remarkably well with clustering as it also showcased a high performance in mitigating SDA attacks.

Table 3 shows the comparison of a selected MANET protocol Adaptive On-demand Distance Vector (AODV), before and after clustering has been done on the nodes.

AODV shows a great increase in Total Data Transferred (300Mb), compared to (1536) before clustering, the throughput rose to (6Mbps) after clustering than (8.533 bytes) before clustering. It can also be noted that AODV Network Time goes up to (1500s) after clustering than (2.13s) before clustering, this is due to the increment in the data transferred over the protocol. A high End-to-End Delay of (1.2s) after clustering and (0.18s) before clustering was also noted, and this occurred due to route disruption and packet loss. Packet Delivery Ratio remains relatively close but lower (94.7%) after clustering than (94.9%) before clustering even with more data being transferred and delivered showing that Clustering improves the MANET protocols in leveraging against SDA attacks.

AODV performs better after clustering than before clustering because the nodes can communicate more effectively and packets are sent faster over the network. It can be noted that AODV performed better after clustering was done than it performed before the nodes were clustered.

LEACH has a great leap in Total Data Transferred (250Mb), compared to (1065) before clustering, the throughput also increases to (5Mbps) after clustering than (8.044 bytes) before clustering. LEACH Network Time goes up to (1800s) after clustering than (2.14s) before clustering, this is due to cluster destabilization caused by SDA. A high End-to-End Delay of (1.5s) after clustering and (1.02s) before clustering was also noted due to disrupted cluster communication and reorganization delays. Packet Delivery Ratio was lower (93.5%) after clustering than (94.3%) before clustering due to increased packet loss within clusters.

Low Energy Adaptive Clustered Hierarchical (LEACH) technique after Clustering shows that with more data being transferred and delivered Clustering improves the performance of MANET protocols against SDA attacks

Ensemble On-demand Low Energy Adaptive Clustered Hierarchical (EO-LEACH) technique after Clustering accomplished an increase in Total Data Transferred (275Mb), compared to (1862) before clustering, the throughput increased from (8.743 bytes) before clustering to (5.5 Mbps) after clustering. The Network Time of EO-LEACH goes up from (2.11s) before clustering to (1600s) after clustering due to the increment in the data transferred over the protocol. End-to-End Delay of (0.25s) before clustering increases to (1.1s) after clustering was also noted due to adaptive routing. Packet Delivery Ratio decreased from (95.2%) before clustering to (92.2%) after clustering due to packet loss during transmission and retransmission of data over the protocol.

EO-LEACH performs better after clustering than before clustering because the nodes can communicate more effectively and packets are sent faster over the network. It can be noted that AODV performed better after clustering was done than it performed before the nodes were clustered.

With clustering, EO-LEACH performs better in terms of energy consumption, packet delivery ratio, and SDA resilience, by leveraging the adaptability of AODV and the energy efficiency of LEACH, EO-LEACH achieves a balance between performance and resilience in the presence of SDA.

5. Conclusion

This study evaluated the performance of three MANET protocols—AODV, LEACH, and EO-LEACH—under Sleep Deprivation Attack (SDA) conditions before and after the application of clustering techniques. The findings indicated that clustering significantly improved the resilience and performance of the protocols, highlighting its importance in enhancing MANET security and efficiency.

Clustering techniques played a crucial role in mitigating the impact of SDAs on MANET protocols. By organizing the network into clusters, the routing overhead reduced, and the network became more resilient to attacks. The study demonstrated that clustering did not only enhance network performance but also provided a robust defense mechanism against SDAs.
Future research would explore the integration of other security measures with clustering techniques to further enhance MANET resilience against a broader range of attacks. Additionally, the development of adaptive clustering algorithms that dynamically adjust to changing network conditions could provide further improvements in performance and security.

References

[1] Ahmed, I., and Upadhyay, R. (2021). Performance Analysis of MANET Routing Protocols. *International Journal of Computer Applications*, 176(30), 24-29.

[2] Deji-Akinpelu. O. and Osunade. O. (2022). *Development of an Ensemble Routing Protocol to Minimise Sleep Deprivation Attacks in Mobile Ad-hoc Networks [PhD Dissertation, University of Ibadan]*.

[3] Fotohi, R., and Firoozi Bari, S. (2020). A novel countermeasure technique to protect WSN against denial-of-sleep attacks using firefly and Hopfield neural network (HNN) algorithms. *The Journal of Supercomputing*, *76*(9), 6860-6886.

[4] Hemalatha, S., Pallathadka, H., and Chinhewadi, R. P. (2023). Novel Routing Algorithm for Efficient Packet Transmission in MANET using T–Test Procedure and Sleep and Awake Strategy. *Int J Med Net*, *1*(1), 92-100.

[5] Khan, S. A., Anwar, S. M., and Jeon, G. (2017). Software Defined Networking in Mobile Ad Hoc Networks: An Overview. IEEE Access, 5, 2139–2151.

[6] Reddy, B., & Dhananjaya, B. (2022). A Comprehensive Review on Mobile Ad-Hoc Networks. *Wireless Communications and Mobile Computing*, 2022, 1-12.

[7] Srinivasan, K. (2018). Security Challenges in Mobile Ad-Hoc Networks. *International Journal of Security and Networks*, 13(4), 221-232.

[8] Sushma, T. (2021). A review of the cluster based mobile adhoc network intrusion detection system. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(2), 2070-2076.

[9]]Mohd, N., Singh, A., & Bhadauria, H. S. (2020). A Novel SVM Based IDS for Distributed Denial of Sleep Strike in Wireless Sensor Networks. Wireless Personal Communications, 111(3), 1999–2022. https://doi.org/10.1007/s11277-019-06969-9

[10] Akpinar, H. N. M., Duran, S., Eser, R. I., & Dogru, S. (2024). Detection of DoS Attacks in WSNs by using Machine Learning Models. 2024 8th International Artificial Intelligence and Data Processing Symposium (IDAP), 1–8. https://ieeexplore.ieee.org/abstract/document/10710944/

[11] Vivekanadam, B. (2020). A novel hybrid HNN and firefly algorithm to overcome denial of sleep attack on wireless sensor nodes. Journal of Ubiquitous Computing and Communication Technologies (UCCT), 2(04), 223–227.

[12] Mankotia, V., Sunkaria, R.K. and Gurung, S. (2024). DTAM: A Dynamic Threshold and Monitoring Based Technique to Protoect Mobile Ad-hoc Network from Black-Hole and Flooding Attacks Wireless Personal Communications. 134(3), 1469-1490. https://doi.org.10.1007s11277-024-10856-0

{13} Kumar, A., Dhabliya., Agarwal, P., Aneja, N., Dadheech, P., Jamal, S. S. and Antwi, O. A. (2022). Cyber-Internet Sesurity Framework to Computer Energy-Related Attacks on the Interneet of Things with Machine Learning Techniques, Computational Intelligence and Neuroscience.1-13, https://doi.org. 10.1155.2022.8803686