Journal of Information Systems Engineering and Management
2025, 10(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Secure and Energy Efficient Routing Approach for Wireless Sensor Networks to Counter Flooding Attack

Vivek Sharma[1], Dr Devershi Pallavi Bhatt[2*]

[1]*Manipal University Jaipur, Rajasthan-303007, India. vivek.sharma@jaipur.manipal.edu*

[2*]*Manipal University Jaipur, Rajasthan-303007, India. devershipallavi.bhatt@jaipur.manipal.edu*

ARTICLE INFO

Received: 10 Oct 2024

Revised: 14 Dec 2024

Accepted: 25 Dec 2024

ABSTRACT

Wireless Sensor Networks (WSNs) are used in many applications owing to their scalability and economic efficiency, but their adhoc characteristics makes them vulnerable to security attacks such as RREQ flooding attacks. RREQ flooding attack overload the network with excessive RREQ messages resulting in network congestion and power exhaustion and interruption of standard operations. This paper presents a secure and energy-efficient routing approach that focuses on effectively mitigating the effects of flooding attacks. The proposed approach combines sophisticated algorithms into the Ad hoc On-Demand Distance Vector (AODV) routing protocol to detect and isolate malicious nodes by analyzing route request (RREQ) frequency. Nodes demonstrating abnormal behavior are identified and removed from network, significantly minimizing the effects of attacks. An energy-aware clustering technique is also included for improving energy efficiency throughout the network. This approach dynamically identifies cluster heads depending on remaining energy and distance, hence minimizing energy expenditure and extending the network's lifespan. Results from the simulation demonstrate the effectiveness of the suggested method in enhancing packet delivery ratio, decreasing energy consumption, and prolonging network lifespan, thereby attaining an optimal equilibrium between security and efficiency..

Keywords: WSN, RREQ, Flooding, Detection, Isolation, Energy Efficiency, Clustering.

INTRODUCTION

WSN comprises spatially distributed sensor nodes that collect and transfer data to a single sink. These networks are used in applications like environmental monitoring, healthcare, and military surveillance. WSNs are distinguished by their adaptability, scalability, and autonomous functionality, making them appropriate for many applications. However, these advantages come with underlying challenges, especially regarding security and energy management.

A major threat to Wireless Sensor Networks (WSNs) is flooding attacks in which malicious nodes abuse the routing protocols to produce an overwhelming number of route requests. This not only drains network resources but also induces considerable delays and packet losses, ultimately degrading the network's reliability. Traditional approaches typically concentrate exclusively on either mitigating security issues or enhancing energy efficiency, rarely handling both dimensions adequately. Energy efficiency is a critical issue in wireless sensor networks because to the limiting battery life of sensor nodes. The effective use of energy directly impacts the network's lifetime and effectiveness. Clustering techniques have been widely applied to optimize energy consumption management. However, incorporating robust security measures into these energy-efficient variants continues to be a major challenge. This paper aims to address this gap by introducing a combined methodology that improves both security and energy efficiency in WSNs.

The proposed approach tackles the vulnerabilities of the Ad hoc On-Demand Distance Vector (AODV) routing protocol by implementing mechanisms for detecting and isolating malicious nodes, while utilizing energy-aware clustering technique. This approach promises a robust and sustainable network, able to deal with flooding attacks and provide energy efficiency, hence better operational efficiency.

LITERATURE REVIEW

We have reviewed the existing literature related to our problem statement and the summary has been presented in the table given below. This review focused on the problems in the domain and the solutions suggested by the researchers as well as pros and cons of the approaches are also mentioned.

Table 1: Literature Survey

Reference	Technique Name	Contribution	Advantages	Limitations
Kumar Bandani, Subramanyam Makam, Prasad Kodati [1]	K-Means and AODV Routing Protocol	Proposed K-Means clustering with AODV routing to improve energy efficiency in MANETs.	Improved packet delivery ratio, reduced energy consumption.	Limited testing under high mobility conditions.
M. Atto, R.J. Mstafa, A. Alkhayyat [2]	AODV-Based Routing for Image Transmission	Improved AODV routing protocol for image transmission in mobile video sensor networks.	Enhanced image quality, extended network lifetime.	Limited to image-based applications.
Marija Malnar, Nenad Jevtic [3]	ND-AODV-PLRE	Introduced ND-AODV-PLRE for reducing routing overhead in large-scale WANETs.	Improves reliability, reduces overhead.	Limited to large-scale WANETs.
Bhattacharjya K, Alam S, De D. [4]	CUWSN Protocol for Underwater Wireless Networks	Proposed CUWSN protocol to improve energy efficiency in underwater wireless sensor networks.	Extends network lifetime, reduces energy consumption.	Limited to underwater environments.
Patra B.K., Mishra S., Patra S.K. [5]	Energy Efficient Clustering and Multipath Routing (HC-HGAPSO)	Proposed a hybrid clustering method using GA and PSO for energy-efficient routing in WSNs.	Improves throughput and network lifetime.	Limited evaluation in high-mobility networks.
Zhe Yang, Lingzhi Li, Fei Gu, Xinghong Ling, Maryam Hajiee [6]	Trust-Aware Dynamic Routing (TADR-EAODV)	Proposed a trust-aware routing algorithm for secure WSN communication using an extended AODV protocol.	Enhances security and performance under DoS attacks.	Focused on secure communication under specific attack types.
Ranjita Joon, Parul Tomar [7]	Energy-Aware Q-learning AODV (EAQ-AODV)	Developed Q-learning-based AODV protocol for energy-efficient routing in cognitive radio WSNs.	Improves end-to-end delay, network lifetime, and energy efficiency.	Q-learning may add computational complexity.
Yin H, Yang H, Shahmoradi S. [8]	Energy-Aware Trust Algorithm for AODV (EATMR)	Proposed a trust-based AODV protocol with energy-aware multipath routing for secure WSNs.	Detects malicious nodes effectively, improves network lifetime.	May struggle with high-volume attacks.
B. Wadhwa, S. S. Yadav [9]	LEACH Protocol with AODV	Improved the LEACH protocol by integrating AODV for energy-efficient data transmission in WSNs and IoT.	Increases throughput and network longevity.	Limited applicability in heterogeneous networks.
Tamizharasu S, Kalpana P. [10]	Intelligent AODV Routing with EEWCA	Proposed intelligent AODV routing using EEWCA to extend WANET network lifetime.	Reduces energy consumption, extends network lifetime.	Limited to static cluster head selection.
Jiang Y, Sun H, Yang M [11]	AODV-EOCW Protocol	Proposed a new routing protocol using combined weight metrics for improved energy and congestion management in mobile ad-hoc networks.	Reduces network congestion and end-to-end delay.	Limited testing in dynamic networks.
Chandrasekar V, Shanmugavalli V, Mahesh T.R., et al. [12]	Secure Malicious Node Detection Using Enhanced AODV	Proposed enhanced AODV for detecting and isolating malicious nodes in flying ad-hoc networks (FANETs).	Improves network security, reduces packet losses and routing overhead.	Limited testing in real-world FANET scenarios.

Rawat P, Rawat G.S., Rawat H., et al. [13]	Cluster-Based Routing for Heterogeneous Networks (CPHN)	Proposed CPHN, a cluster-based routing protocol to extend the network lifetime in heterogeneous WSNs.	Extends network lifetime, improves throughput and energy efficiency.	Limited to cluster-based architectures.
Fan Luo, Jianguo Zhou, Peng Chen, Yanming Dong, Lu Lu [14]	Optimization Algorithm for AODV-Based Unmanned Cluster Routing	Proposed MQ-AODV, a path selection algorithm for unmanned cluster routing with multiple QoS objectives.	Enhances throughput, reduces packet loss, and improves end-to-end delay.	Limited to UAV clusters.

PROPOSED SECURE AND ENERGY EFFICIENT ROUTING APPROACH

This research presents a secure and energy-efficient routing approach for WSNs, integrating the AODV protocol with enhanced security mechanisms and clustering-based analysis for detecting and isolating malicious nodes. The AODV protocol, widely used in dynamic WSN environments, is employed for its on-demand routing capabilities, which conserve energy and bandwidth. Despite its advantages, AODV is vulnerable to Route Request (RREQ) flooding attacks, necessitating additional security measures. The proposed approach incorporates modular components to enhance network security while maintaining operational efficiency and scalability.

Data Collection and Analysis

The data collection module monitors network traffic, specifically tracking RREQ packets received by each node. Analysis is performed to maintain up-to-date records of RREQ counts within a predefined time window, ensuring dynamic adaptation to changing network conditions.

Input:

RREQ_COUNT_THRESHOLD: Maximum allowable RREQ packets a node can receive in TIME_WINDOW.

TIME_WINDOW: Duration for temporal analysis.

k: Number of clusters for K-Means Clustering.

current_time: Current time in the simulation or system.

Initialization:

Initialize NodeRREQCount to store RREQ counts for each node.

Initialize NodeRREQTimestamps to store timestamps of received RREQ packets.

Threshold-Based Detection and Temporal Analysis

A threshold-based detection mechanism identifies nodes exceeding the maximum allowable RREQ count (RREQ_COUNT_THRESHOLD) within the specified time window, flagging them for further scrutiny using temporal analysis.

for each RREQ packet received do:

Update RREQ Counts:

If node_id not in NodeRREQCount:

Initialize NodeRREQCount[node_id] = 0 and NodeRREQTimestamps[node_id] = [].

Increment NodeRREQCount[node_id] by 1.

Append the current timestamp to NodeRREQTimestamps[node_id].

Update NodeRREQCount[node_id] to the length of the updated timestamps.

For each node:

Identify nodes exhibiting suspicious behaviour (e.g., exceeding RREQ_COUNT_THRESHOLD).

Node Isolation Decision and Response

For each suspicious node do:

Confirm Malicious Behaviour:

Analyse the RREQ Count and Temporal Data.

If confirmed malicious:

Proceed to isolate the node.

Nodes confirmed as malicious are isolated by updating routing tables to exclude them and notifying neighboring nodes to avoid communication with these nodes. This response ensures prompt isolation while preserving network integrity and minimizing disruptions for legitimate nodes.

- Update routing tables to exclude malicious nodes.
- Inform neighboring nodes to propagate isolation.

Clustering with K-Means

To enhance energy efficiency, K-Means clustering is applied to group nodes based on energy level of nodes and the distance of nodes from central node.

Apply K-Means Clustering to group nodes into k clusters:

Input: Nodes: List of nodes with coordinates (x, y), k: Number of clusters.

Repeat for the specified number of iterations:

a. Assign nodes to the nearest cluster head:

i. For each node:

- Calculate the Euclidean distance to each cluster head.

- Identify the cluster head with the smallest distance.

- Assign the node to the cluster corresponding to this cluster head.

Update cluster head:

i. For each cluster:

- Calculate the remaining energy of all nodes in the cluster.

- Update the cluster head to the highest remaining energy node.

Return the final clusters and cluster heads.

By integrating threshold based detection, temporal analysis and K-Means clustering, the approach achieves high detection accuracy, energy efficiency, adaptability to dynamic environments, and scalability for larger networks. The methodology is particularly suited for applications in Mobile Ad Hoc Networks, IoT networks, and WSNs, where security and energy efficiency are critical.

IMPLEMENTATION DETAILS

1. Network Topology and Node Distribution

- Number of Nodes: The network consists of 100 nodes arranged in a flat grid topology over an area of 3168x500 units.
- Node Clustering: Nodes are organized into clusters, with one node in each cluster designated as the cluster head (CH).
    - Cluster Heads: These are nodes selected dynamically based on their energy levels, ensuring that the highest-energy nodes become cluster heads. This selection reduces the risk of early node depletion and prolongs the network's operational lifetime.

2. Traffic and Data Transmission

- UDP Traffic: All nodes generate UDP traffic periodically, representing typical sensor data in WSNs. This traffic is sent to their respective cluster heads.

- Data Aggregation and Forwarding:
    - Cluster heads aggregate data from the nodes in their cluster to reduce redundancy.
    - The aggregated data is then forwarded to a central base station for analysis.
- Periodic Traffic Generation: Ensures a consistent flow of data, allowing analysis of network performance under steady-state conditions.

The simulation setup represents a wireless sensor network (WSN) configured to study the behavior and performance of a clustered network where energy efficiency and hierarchical communication are critical. Here's a detailed explanation of the setup:

1. Network Topology and Node Distribution

- Number of Nodes: The network consists of 100 nodes arranged in a flat grid topology over an area of 3168x500 units.
- Node Clustering: Nodes are organized into clusters, with one node in each cluster designated as the cluster head (CH).
    - Cluster Heads: These are nodes selected dynamically based on their energy levels, ensuring that the highest-energy nodes become cluster heads. This selection reduces the risk of early node depletion and prolongs the network's operational lifetime.

2. Traffic and Data Transmission

- UDP Traffic: All nodes generate UDP traffic periodically, representing typical sensor data in WSNs. This traffic is sent to their respective cluster heads.
- Data Aggregation and Forwarding:
    - Cluster heads aggregate data from the nodes in their cluster to reduce redundancy.
    - The aggregated data is then forwarded to a central base station for analysis.
- Periodic Traffic Generation: Ensures a consistent flow of data, allowing analysis of network performance under steady-state conditions.

3. Routing Protocol

- AODV Protocol: The Ad hoc On-Demand Distance Vector (AODV) routing protocol is used for routing decisions. AODV is well-suited for dynamic networks like WSNs due to its ability to establish routes on-demand and maintain efficient communication paths.

4. Wireless Communication and Physical Layer Configuration

- MAC Protocol: The 802.11 MAC protocol is used, providing a reliable framework for wireless communication.
- Antenna Type: OmniAntenna is employed for uniform signal transmission and reception in all directions.
- Propagation Model: The TwoRayGround propagation model is used to simulate signal transmission characteristics, considering ground reflection and direct line-of-sight components.

The simulation setup represents a wireless sensor network (WSN) configured to study the behavior and performance of a clustered network where energy efficiency and hierarchical communication are critical. Here's a detailed explanation of the setup:

1. Network Topology and Node Distribution

- Number of Nodes: The network consists of 100 nodes arranged in a flat grid topology over an area of 3168x500 units.
- Node Clustering: Nodes are organized into clusters, with one node in each cluster designated as the cluster head (CH).

- Cluster Heads: These are nodes selected dynamically based on their energy levels, ensuring that the highest-energy nodes become cluster heads. This selection reduces the risk of early node depletion and prolongs the network's operational lifetime.

2. Traffic and Data Transmission

- UDP Traffic: All nodes generate UDP traffic periodically, representing typical sensor data in WSNs. This traffic is sent to their respective cluster heads.
- Data Aggregation and Forwarding:
  - Cluster heads aggregate data from the nodes in their cluster to reduce redundancy.
  - The aggregated data is then forwarded to a central base station for analysis.
- Periodic Traffic Generation: Ensures a consistent flow of data, allowing analysis of network performance under steady-state conditions.

3. Routing Protocol

- AODV Protocol: The Ad hoc On-Demand Distance Vector (AODV) routing protocol is used for routing decisions. AODV is well-suited for dynamic networks like WSNs due to its ability to establish routes on-demand and maintain efficient communication paths.

4. Wireless Communication and Physical Layer Configuration

- MAC Protocol: The 802.11 MAC protocol is used, providing a reliable framework for wireless communication.
- Antenna Type: OmniAntenna is employed for uniform signal transmission and reception in all directions.
- Propagation Model: The TwoRayGround propagation model is used to simulate signal transmission characteristics, considering ground reflection and direct line-of-sight components.

5. Energy Management

- Default Energy Model: Each node starts with 10 units of energy. This setup allows studying energy consumption patterns and evaluating the network's energy efficiency.
- Cluster Heads: By assigning high-energy nodes as cluster heads, the system optimizes energy use and minimizes the likelihood of early energy depletion.

6. Simulation Duration and Output

- Simulation Time: The simulation runs for 50 seconds, during which all network operations (traffic generation, routing, and data transmission) are executed.
- Output Data:
  - Trace Files (pro.tr and pro.nam): Used to log network activity and enable performance analysis.
  - Performance Metrics: Metrics like energy consumption, packet delivery ratio, latency, and throughput can be extracted from the trace files for evaluation.

This setup provides a realistic and comprehensive framework for testing WSN protocols and strategies, especially those focused on energy efficiency, clustering, and hierarchical communication.

RESULTS & DISCUSSION

After implementation of the above setup, we found the results which are explained in this section.

Figure 1 shows the Throughput: Normal AODV: Achieves the highest throughput at 461.61, indicating efficient data delivery in the absence of attacks. AODV with Flooding: Drops significantly to 84.69, reflecting the impact of RREQ flooding attacks, which overwhelm the network. Proposed Method: Recovers throughput to 355.26, showing substantial improvement over the flooding scenario, though not matching the normal AODV due to additional overhead in detection and mitigation processes.

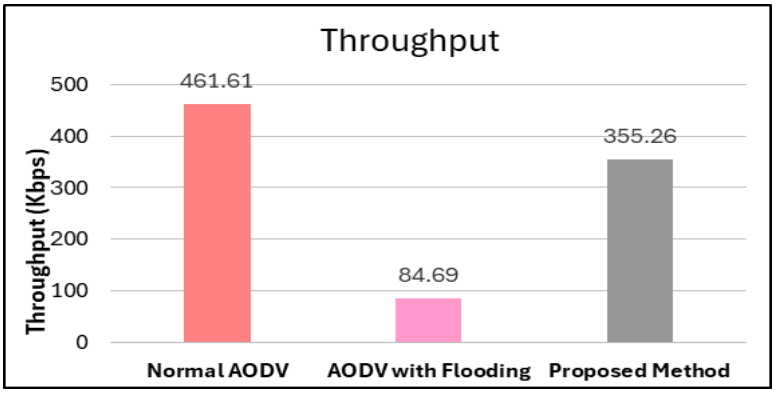

Figure 1: Throughput

Figure 2 shows the Packet Delivery Ratio (PDR): Normal AODV: PDR is 21.73, which serves as a baseline. AODV with Flooding: Drastically reduced to 3.99, signifying severe degradation in network performance caused by malicious activity. Proposed Method: Improves to 16.73, demonstrating effectiveness in mitigating attacks and restoring delivery efficiency.

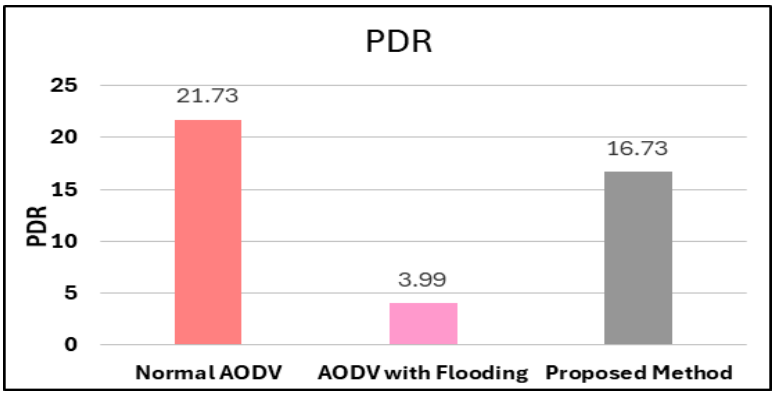

Figure 2: Packet Delivery Ratio (PDR)

Figure 3 shows the End-to-End (ETE) Delay: Normal AODV: The delay is the highest at 1952.54, potentially due to natural routing overhead without disruptions. AODV with Flooding: Reduced to 1393.95, as the network struggles to deliver fewer packets amid the attack. Proposed Method: Delay further drops to 1096.82, suggesting better routing efficiency and reduced congestion in handling malicious nodes.

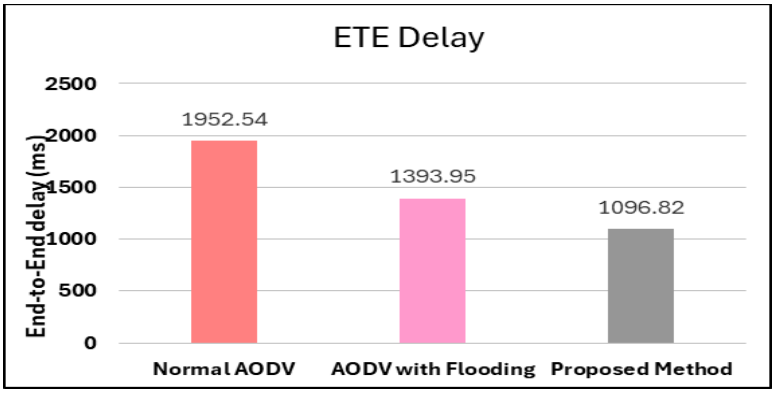

Figure 3: End-to-End (ETE) Delay

Figure 4 shows the Average Remaining Energy: Normal AODV: Average Remaining Energy 0.883297 energy units, indicating efficient operation in attack-free conditions. AODV with Flooding: Energy usage increases to 1.058203, reflecting wasted resources due to malicious activity. Proposed Method: Shows slightly higher energy usage at 1.092207, attributed to additional computations for intrusion detection and malicious node isolation.

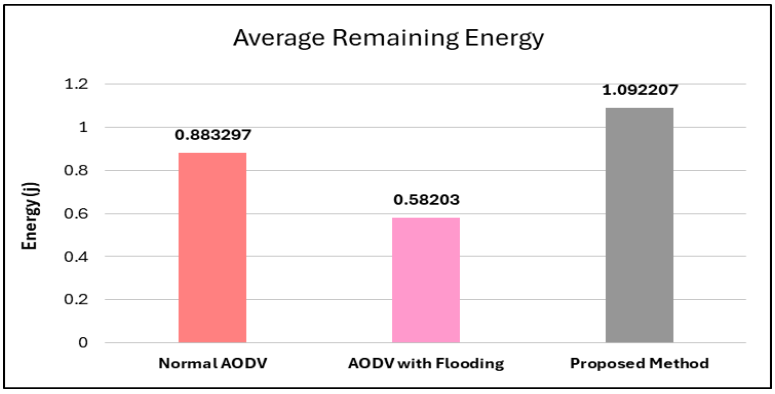

Figure 4: Average Remaining Energy

Figure 5 shows the Normalized Routing Load (NRL): Normal AODV: Maintains a low routing load of 5.05. AODV with Flooding: Jumps to 27.54, highlighting the disruptive impact of flooding attacks that increase routing overhead. Proposed Method: Reduces the load to 6.56, close to normal AODV levels, emphasizing improved control over the network under attack.

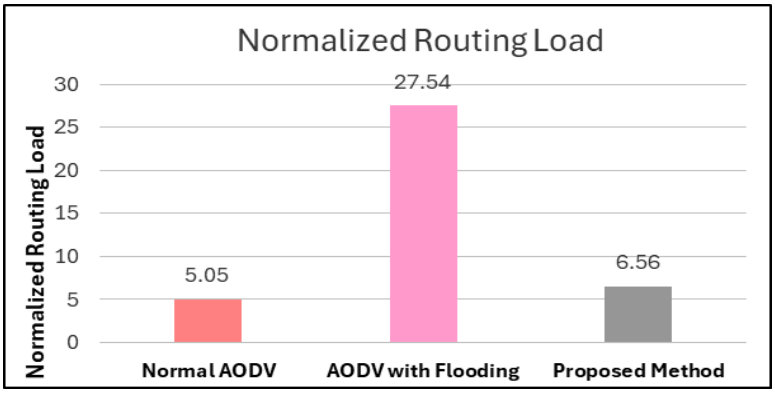

Figure 5: Normalized Routing Load

Significant recovery in throughput and PDR compared to the flooded scenario, indicating effective mitigation was achieved. Substantial reduction in NRL was there showing the ability to control excessive routing overhead caused by the attack. The lower ETE delay compared to both attack and normal scenarios suggesting optimized routing efficiency.

Table 2: Analysis of performance metrics

Metric	Throughput	PDR	ETE Delay	Energy	Normalized Routing Load
Normal AODV	461.61	21.73	1952.54	0.883297	5.05
AODV with Flooding	84.69	3.99	1393.95	0.58203	27.54
Proposed Method	355.26	16.73	1096.82	1.092207	6.56

Energy Consumption: The method slightly increases residual energy compared to the flooded scenario, which results in an increase of lifetime of energy-constrained WSNs.
Throughput and PDR: Though improved, these metrics are still below normal AODV, pointing to room for optimization in detection accuracy and response mechanisms.
Key Trade-Offs: The proposed method trades off slight increases in remaining energy for significant performance gains in throughput, PDR, and routing load. The balance between detection efficiency and energy overhead is critical for maintaining long-term network capabilities.

CONCLUSION & FUTURE SCOPE

This research introduces a safe routing method for WSNs that uses the AODV protocol to prevent RREQ flooding attacks. The method efficiently detects flooding assaults by monitoring RREQ count and temporal analysis, identifying nodes with unusually high RREQ packet frequencies and isolating them from the network. Simulation

results show significant enhancements in end-to-end delay, throughput, packet delivery ratio, average remaining energy, and normalized routing load when compared to the regular AODV protocol without security provisions. This approach improves the security of WSNs as well as guarantees efficient energy usage and consistent network performance. Future research directions may include investigating the scalability of the proposed approach in larger and more dynamic network environments with different topologies and clustering, refining the detection algorithm to minimize computational burden, and expanding the approach to mitigate other network attacks.

REFERENCES

[1] Kumar, Bandani & Subramanyam, Makam & Prasad, Kodati. (2019). An Energy Efficient Clustering Using K-Means and AODV Routing Protocol in Ad-hoc Networks. International Journal of Intelligent Engineering and Systems. 12. 125-134. 10.22266/ijies2019.0430.13

[2] M. Atto, R. J. Mstafa and A. Alkhayyat, "Improving AODV Routing Protocol for Image Transmission Over Mobile Video Sensor Networks," in IEEE Access, vol. 8, pp. 169396-169407, 2020, doi: 10.1109/ACCESS.2020.3024093

[3] Marija Malnar and Nenad Jevtic. 2022. An improvement of AODV protocol for the overhead reduction in scalable dynamic wireless ad hoc networks. Wirel. Netw. 28, 3 (Apr 2022), 1039–1051. https://doi.org/10.1007/s11276-022-02890-5

[4] Bhattacharjya, K., Alam, S. & De, D. CUWSN: energy efficient routing protocol selection for cluster based underwater wireless sensor network. Microsyst Technol 28, 543–559 (2022). https://doi.org/10.1007/s00542-019-04583-0

[5] Patra, B.K., Mishra, S., Patra, S.K. (2022). Energy Efficient Clustering and Optimal Multipath Routing Using Hybrid Metaheuristic Protocol in Wireless Sensor Network. In: Kaiser, M.S., Bandyopadhyay, A., Ray, K., Singh, R., Nagar, V. (eds) Proceedings ofTrends in Electronics and Health Informatics. Lecture Notes in Networks and Systems, vol 376. Springer, Singapore. https://doi.org/10.1007/978-981-16-8826-3_47

[6] Zhe Yang, Lingzhi Li, Fei Gu, Xinghong Ling, Maryam Hajiee, TADR-EAODV: A trust-aware dynamic routing algorithm based on extended AODV protocol for secure communications in wireless sensor networks, Internet of Things, Volume 20, 2022, 100627, ISSN 2542-605, https://doi.org/10.1016/j.iot.2022.100627

[7] Ranjita Joon and Parul Tomar. 2022. Energy Aware Q-learning AODV (EAQ-AODV) routing for cognitive radio sensor networks. J. King Saud Univ. Comput. Inf. Sci. 34, 9 (Oct 2022), 6989–7000. https://doi.org/10.1016/j.jksuci.2022.03.021

[8] Yin, H., Yang, H. & Shahmoradi, S. EATMR: an energy-aware trust algorithm based the AODV protocol and multi-path routing approach in wireless sensor networks. Telecommun Syst 81, 1–19 (2022). https://doi.org/10.1007/s11235-022-00915-0

[9] B. Wadhwa and S. S. Yadav, "Leach Protocol with AODV based Data Transmission in Wireless Sensor Networks and IoT Applications," 2023 2nd International Conference for Innovation in Technology (INOCON), Bangalore, India, 2023, pp. 1-7, doi: 10.1109/INOCON5975.2023.10101152

[10] Tamizharasu, S., Kalpana, P. An intelligent AODV routing with energy efficient weight based clustering algorithm (EEWCA) in wireless Ad hoc network (WANET). Wireless Netw 29, 2703–2716 (2023). https://doi.org/10.1007/s11276-023-03321-9

[11] Jiang Y, Sun H, Yang M. AODV-EOCW: An Energy-Optimized Combined Weighting AODV Protocol for Mobile Ad Hoc Networks. Sensors. 2023; 23(15):6759. https://doi.org/10.3390/s23156759

[12] Chandrasekar, V., Shanmugavalli, V., Mahesh, T.R. et al. Secure malicious node detection in flying ad-hoc networks using enhanced AODV algorithm. Sci Rep 14, 7818 (2024). https://doi.org/10.1038/s41598-024-57480-6

[13] Rawat, P., Rawat, G.S., Rawat, H. et al. Energy-efficient cluster-based routing protocol for heterogeneous wireless sensor network. Ann. Telecommun. (2024). https://doi.org/10.1007/s12243-024-01015-7

[14] Fan Luo, Jianguo Zhou, Peng Chen, Yanming Dong, and Lu Lu. 2024. Optimization Algorithm for AODV-Based Unmanned Cluster Routing with Multiple QoS Objectives. In Proceedings of the 2024 11th International Conference on Wireless Communication and Sensor Networks (icWCSN '24). Association for Computing Machinery, New York, NY, USA, 80–88. https://doi.org/10.1145/3657529.3657536