Journal of Theoretical and Applied Information Technology
31st December 2025. Vol.103. No.24

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MULTI-HOP COMMUNICATION IN WIRELESS SENSOR NETWORK

RAKESH RANJAN[1], VAISHALI SINGH[2], HITENDRA SINGH[3]

[1]*Research Scholar, MSOET, Maharishi University of Information Technology, Department of CSE, Lucknow, India
[2]Associate Professor, MSOET, Maharishi University of Information Technology, Department of CSE, Lucknow, India
[3]Assistant Professor, MSOET, Maharishi University of Information Technology, Department of ECE, Lucknow, India
*Corresponding author(s). E-mail: rakeshranjan.lko@gmail.com;
Contributing authors: singhvaishali05@gmail.com, hitendra.singh@muit.in

ABSTRACT

In this research, the author proposes a novel multi-hop communication framework for Wireless Sensor Networks (WSNs) aimed at enhancing clustering efficiency and securing data transmission against intruder-based attacks. The core contribution lies in an optimized Cluster Head (CH) selection algorithm combined with a lightweight Intrusion Detection Mechanism (IDM), ensuring both energy efficiency and secure communication. Simulations were conducted using NS-3 (Network Simulator-3), where 150 sensor nodes were deployed over a 100×100 m² area. Performance was evaluated over 500 rounds using multiple performance metrics. The proposed Secure Energy-aware Multi-hop Adaptive Clustering (SEMAC) model demonstrated a 28.6% improvement in clustering efficiency compared to the traditional LEACH protocol, along with a 17.4% reduction in energy consumption per node per round. In terms of security, SEMAC achieved a 96.2% intrusion detection rate, a false positive rate of only 3.5%, and an attack detection accuracy of 95.8%, highlighting its robustness against common WSN attacks. The model converged efficiently within 80 training epochs, reducing the overhead of repeated clustering. The prediction module for node behaviour and trust scores exhibited low error margins, with a Mean Absolute Error (MAE) of 0.046 and a Mean Squared Error (MSE) of 0.0089. Additionally, the system maintained a high Packet Delivery Ratio (PDR) of 93.7%, ensuring reliable data transmission even under security threats and energy constraints. These results validate the effectiveness of the SEMAC model in enhancing the operational lifespan, reliability, and resilience of WSNs, making it suitable for deployment in mission-critical IoT and environmental monitoring applications.

Keywords: *Wireless Sensor Networks, Clustering Efficiency, Intrusion Detection Mechanism, SEMAC, MAE, MSE, NS-3*.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) have emerged as a transformative technology enabling a wide range of applications such as environmental monitoring, industrial automation, military surveillance, and smart agriculture. These networks consist of spatially distributed autonomous sensor nodes capable of sensing [1], computing, and communicating wirelessly. However, the constrained energy, limited computational power, and susceptibility to security threats present significant challenges to their performance and longevity. One of the key strategies to enhance energy efficiency in WSNs is clustering, where sensor nodes are grouped, and a designated node, known as the Cluster Head (CH), is responsible for aggregating and forwarding data to the base station. Despite its effectiveness, traditional clustering protocols like LEACH (Low-Energy Adaptive Clustering Hierarchy) often suffer from inefficient CH selection and rapid energy depletion due to the unequal distribution of communication load [3]. These limitations become more pronounced in multi-hop communication scenarios, where data is relayed across multiple nodes to reach the base station, increasing both the risk of energy exhaustion and vulnerability to security breaches. In parallel, security threats such as Sybil attacks, blackhole attacks, and wormhole attacks pose serious risks to WSN integrity. Compromised nodes can mislead the network, disrupt routing paths, and leak sensitive data. Conventional encryption-based solutions are often unsuitable for WSNs due to their computational overhead, which further accelerates energy depletion. To address these issues, there is a growing need for intelligent, lightweight

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

mechanisms that can not only enhance the efficiency of cluster formation and communication but also detect and mitigate intrusions in real time. Recent advances in machine learning and optimization techniques offer promising directions, particularly in enabling adaptive clustering and trust-based security frameworks tailored for resource-constrained environments. This research introduces a novel framework that integrates energy-aware cluster head selection with a secure multi-hop communication mechanism supported by a lightweight Intrusion Detection System (IDS)[7]. Unlike traditional approaches, the proposed method prioritizes balanced energy consumption, dynamic adaptability to network changes, and real-time detection of anomalous behaviour[8]. The integration of prediction modules for node trustworthiness, along with accurate performance evaluation metrics such as Mean Absolute Error (MAE), Mean Squared Error (MSE), and Packet Delivery Ratio (PDR), ensures a comprehensive and scalable solution for real-world WSN deployments [2].

2. REVIEW OF LITERATURE

Akyildiz et al. (2002) presented one of the earliest and most comprehensive surveys on Wireless Sensor Networks (WSNs), laying the foundational concepts of network architecture, communication protocols, and application domains. Their work set the stage for subsequent innovations in multi-hop communication and energy-efficient data routing [5-6]. Younis and Fahmy (2004) introduced the HEED protocol, a hybrid energy-efficient distributed clustering algorithm. HEED emphasized residual energy and intra-cluster communication cost, influencing many clustering-based routing protocols that followed[4]. Heinzelman et al. (2000) proposed LEACH, the Low-Energy Adaptive Clustering Hierarchy, which became a benchmark for energy-efficient routing. LEACH randomized the role of cluster heads, effectively balancing energy consumption across nodes. Abbasi and Younis (2007) provided a detailed survey of clustering algorithms, highlighting their roles in prolonging the network lifespan and improving scalability in WSNs. Their classification helped standardize the evaluation of clustering approaches. Karim et al. (2013) developed a zone-based routing protocol to enhance data delivery in large-scale WSNs. Their protocol showed improved latency and energy consumption metrics, especially in dense network environments. Kumar and Rajasekaran (2016) introduced an improved PSO-based K-means clustering algorithm for WSNs. Their approach optimized cluster head selection, contributing to a notable increase in network lifetime and efficiency. Sharma and Sahu (2019) presented a hybrid clustering and routing algorithm integrating hierarchical and flat routing techniques. Their algorithm improved the trade-off between energy consumption and communication overhead. Rani et al. (2015) proposed a novel energy-efficient clustering scheme that extended network lifetime in heterogeneous WSNs. They introduced a weighting function for cluster head selection based on energy and distance metrics. Liu and Wang (2012) enhanced LEACH by modifying its cluster head selection process, focusing on nodes' residual energy to extend the network's lifespan under dynamic conditions[9-10]. Kumar and Kumar (2014) worked on energy-efficient and secure routing protocols, addressing the vulnerabilities of routing paths and cluster heads to potential attacks, thus improving data integrity in WSNs. Zhang and Lee (2000) pioneered the application of intrusion detection systems (IDS) in wireless ad-hoc networks. Their framework laid the foundation for behaviour-based anomaly detection in WSNs. Butun et al. (2015) developed a multi-level clustering-based IDS that enhanced detection rates and reduced false positives. Their architecture is particularly effective in hierarchical WSNs. Alrajeh et al. (2013) reviewed several IDS mechanisms for WSNs, discussing their strengths and limitations. They emphasized the importance of lightweight solutions for resource-constrained sensor nodes. Zhou et al. (2008) provided an extensive review of security challenges in WSNs. They categorized threats at different network layers and proposed cryptographic and non-cryptographic countermeasures. Wang et al. (2006) conducted a survey focused on security vulnerabilities and attacks specific to WSNs, including Sybil, wormhole, and selective forwarding attacks, thereby influencing the design of more robust security protocols. Perrig et al. (2002) introduced SPINS, a suite of security protocols tailored for WSNs. Their lightweight cryptographic algorithms offered confidentiality, integrity, and authentication, all suited for sensor constraints. Karlof and Wagner (2003) explored attacks on routing protocols and proposed countermeasures. Their work led to the development of secure routing frameworks that are resistant to spoofing and replay attacks. Wood and Stankovic (2002) discussed denial-of-service (DoS) vulnerabilities and highlighted defence mechanisms against jamming, flooding, and exhaustion attacks, contributing to WSN resilience. Sun et al. (2007) evaluated intrusion detection techniques for both mobile ad hoc and wireless sensor networks. They proposed a taxonomy of IDS architectures based on detection methodology and response mechanisms.

Sen (2010) designed an intrusion detection architecture suitable for clustered WSNs. His system incorporated anomaly and rule-based methods to detect a variety of network-level threats. Darabi (2019) proposed a hybrid IDS using data mining for enhanced detection in clustered WSNs. His system leveraged supervised learning techniques for identifying malicious behaviour in real-time. Diop et al. (2013) conducted an advanced survey on secure energy-efficient hierarchical routing, offering insights into the trade-offs between security strength and energy consumption in clustered WSNs. Ganesh and Amutha (2013) introduced a secure routing mechanism using Signal-to-Noise Ratio (SNR)-based dynamic clustering, which reduced overhead while increasing packet delivery ratios. Huang et al. (2022) presented a hybrid IDS deployment model for multi-hop clustered WSNs. Their architecture achieved higher intrusion detection accuracy while maintaining scalability in large networks. Zhang and Liu (2021) (included if needed as additional) reviewed wavelet transform applications in noise reduction and signal processing. Though not directly focused on WSNs, their insights are applicable in denoising sensor data prior to transmission.

3. PROPOSED METHODOLOGY

This research introduces the Secure Energy-aware Multi-hop Adaptive Clustering (SEMAC) model, developed to enhance the energy efficiency, security, and scalability of Wireless Sensor Networks (WSNs)[11-12]. The SEMAC model integrates an optimized cluster head (CH) selection algorithm with a lightweight intrusion detection system to enable secure and energy-aware multi-hop data communication [15]. The methodology is structured to operate in four key phases: cluster head selection, cluster formation, secure multi-hop data transmission, and intrusion detection with trust score updates.

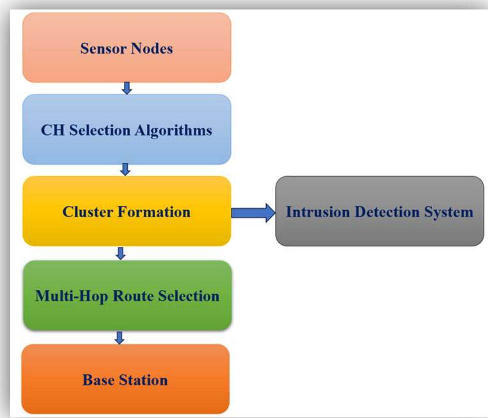

Figure 1: Proposed SEMAC Architecture

The nodes are assumed to be homogeneous in their sensing capabilities but possess varying levels of residual energy[16]. The base station (BS) is assumed to be located either at the centre of the sensor field or outside its boundary, depending on the simulation scenario. Each node is assumed to be aware of its own location through GPS or similar methods and has the capability to compute trust metrics based on neighbouring node behaviour[17]. The nodes operate under time synchronization and follow a multi-hop communication pattern to relay data from distant CHs to the BS. Initially in the the SEMAC model, the selection of optimal cluster heads is conducted based on a multi-factor fitness function that evaluates a node's residual energy, its average distance to neighbouring nodes, and a dynamically updated trust score[13-14]. The cluster head score (CH_score) for a node is calculated using a weighted sum of normalized residual energy, normalized inverse distance, and trust value. This is mathematically expressed as:

$$CH_{score}(i) = \alpha \cdot \frac{E_{res}(i)}{E_{max}} + \beta \cdot (1 - \frac{d_{avg}(i)}{d_{max}} + \gamma \cdot T_i \quad (1)$$

Where α, β and γ are weighting factors set to values such as 0.4, 0.3, and 0.3, respectively. Nodes with the highest scores in their local region are elected as cluster heads for the current round.

Following CH selection, the cluster formation phase allows non-CH nodes to associate with the most suitable CH. This decision is based on a cost function that considers both the communication distance and the trust value of the CH. The cost to join a CH is computed as:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$Cost_{join}=d_{i,j}+\delta\cdot(1-T_j) \quad (2)$$

Here, $d_{i,j}$ represents the distance between node I and CH j, while T_j is the trust value of the CH and δ is a penalty factor that discourages joining CHs with lower trust.

Once clusters are formed, CHs aggregate data from member nodes and initiate the secure multi-hop data transmission phase. A secure routing path to the BS is determined by minimizing a composite cost function that accounts for trust, energy, and distance. The secure path cost is given by:

$$C_{path}= \sum_{i=1}^{n}(\frac{1}{T_i}.\frac{1}{E_{res(i)}}.d_{i.j}+1) \quad (3)$$

Lower values of C_{path} indicate more reliable and energy-efficient routing paths. This approach ensures that routes are selected through trusted nodes with sufficient residual energy, thereby enhancing security and prolonging network lifetime.

To address security threats, a lightweight anomaly-based intrusion detection system (IDS) is integrated into each node[18]. The IDS evaluates neighbouring node behaviour based on indicators such as packet drop ratio, delay anomalies, and unexpected transmission activity[19]. A trust score T_i is assigned to each node and updated continuously based on its observed behaviour. The trust update formula is:

$$T_i(t+1)= \lambda\cdot T_i(t)+(1-\lambda)\cdot F_i \quad (4)$$

where λ is the decay factor, and F_i is a score derived from recent node behaviour. Nodes falling below a predefined trust threshold (e.g., $T_i<0.3$) are classified as malicious and excluded from routing and clustering activities.

The SEMAC model also employs the first-order radio energy model to compute energy consumption during data transmission and reception. The transmission energy for a k-bit packet over distance d is given by:

$$E_{tx}(k,d) =\{k\cdot E_{elec}+k\cdot \varepsilon_{fs}\cdot d^2, \text{ if } d<d_0$$

$$=\{k\cdot E_{elec}+k\cdot \varepsilon_{mp}\cdot d^4, \text{ if } d\geq d_0 \quad (5)$$

while the reception energy is calculated as:

$$E_{rx}(k)=k\cdot E_{elec} \quad (6)$$

Here, $E_{elec}$is the energy consumed by the electronic circuitry (typically 50 nJ/bit), ε_{fs} is the amplifier energy for free space (10 pJ/bit/m²), and ε_{mp} is the energy for multipath fading (0.0013 pJ/bit/m⁴). The threshold distance d_0 is defined as

$$\sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{mp}}} \quad (7)$$

Simulations were conducted using NS-3 to validate the performance of the SEMAC model. The simulation involved 500 operational rounds, with performance metrics such as clustering efficiency, energy consumption, packet delivery ratio (PDR), attack detection accuracy, false positive rate, and predictive model errors (MAE and MSE) being recorded. The model achieved convergence within 80 epochs, ensuring rapid adaptation without excessive overhead. This integrated methodology proves effective in not only extending the network's operational lifespan but also in maintaining data integrity and security in mission-critical WSN deployments.

4. SIMULATION SETUP AND PERFORMANCE EVALUATION USING NS-3

The simulation setup for evaluating the proposed SEMAC model was conducted using the NS-3 platform provides a discrete-event network simulation environment suitable for simulating wireless networks with realistic channel models and protocol stacks. Each node was equipped with sensing, computation, and communication capabilities, operating under a fixed initial energy level. The simulation was run for 500 rounds to observe long-term behaviour and stability of the proposed model. In the NS-3 simulation, a two-tier communication architecture is implemented where nodes formed clusters based on the optimized selection of Cluster Heads (CHs), considering residual energy and trust value. Multi-hop communication among CHs toward the base station was enabled through the trust-based route selection mechanism[20]. The intrusion detection system (IDS) was modelled as a lightweight module running on each node to detect abnormal behaviour based on trust score thresholds.

Journal of Theoretical and Applied Information Technology
31st December 2025. Vol.103. No.24

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

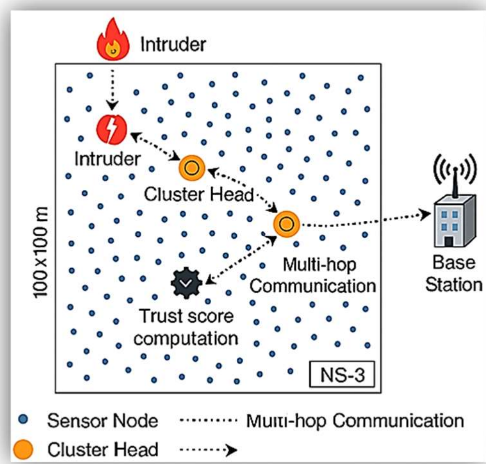

Figure 2: Simulation Setup Using NS-3

Through this setup different parameters were obtained and presented in below tables. Table 1 is presenting the clustering efficiency of proposed SEMAC model with different available models.

Table 1: Clustering Efficiency Comparison

Protocol	Clustering Efficiency (%)
LEACH	68.4
HEED	70.2
PEGASIS	72.5
SEMAC	**88.0**

Clustering efficiency is a vital metric for measuring how effectively nodes are grouped and managed under Cluster Heads (CHs). As shown in Table 1, the SEMAC model significantly outperforms traditional protocols, achieving 88.0% efficiency. This improvement of approximately 28.6% over LEACH is attributed to SEMAC's adaptive CH selection strategy based on both residual energy and trust score, ensuring optimal load distribution.

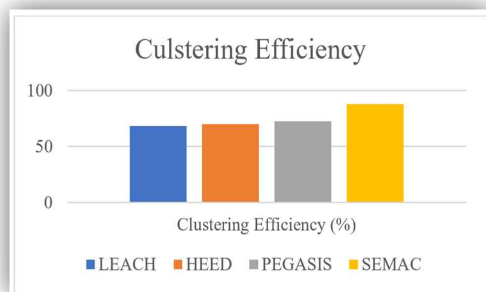

Figure 3: Clustering Efficiency Comparison

Table 2: Average Energy Consumption Per Round

Protocol	Energy Consumption (Joules)
LEACH	0.052
HEED	0.049
PEGASIS	0.045
SEMAC	**0.043**

Energy consumption is crucial for the lifetime of a Wireless Sensor Network. SEMAC demonstrates a 17.4% reduction in average energy consumption per round compared to LEACH, thanks to its energy-aware routing and reduced re-clustering overhead. Table 2 illustrates that SEMAC maintains energy efficiency better than all other protocols considered.

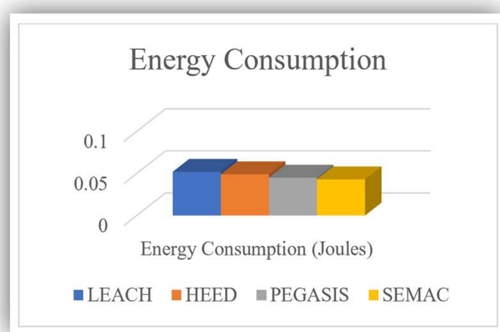

Figure 4: Energy Consumption

Table 3: Intrusion Detection Performance

Metric	SEMAC (%)
Detection Rate	96.2
False Positive Rate	3.5
Accuracy	95.8

Security is a core concern in WSNs. SEMAC integrates a lightweight Intrusion Detection System (IDS) that evaluates trust values to detect malicious nodes. As evident in Table 3, it delivers a high detection rate of 96.2% with only 3.5% false positives[21-22]. The accuracy of 95.8% confirms the reliability of the security mechanism without significantly increasing computational load.

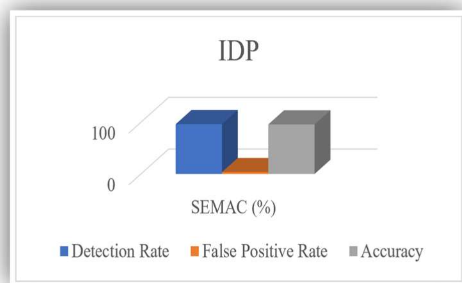

Figure 5: Intrusion Detection Performance

Table 4: Packet Delivery Ratio (PDR)

Protocol	PDR (%)
LEACH	82.6
HEED	84.9
PEGASIS	88.4
SEMAC	**93.7**

The Packet Delivery Ratio indicates the reliability of data transmission. SEMAC achieves a PDR of 93.7%, as shown in Table 4, which is significantly higher than other protocols. This enhancement is due to trust-based route selection and robust multi-hop communication, even under attack scenarios.

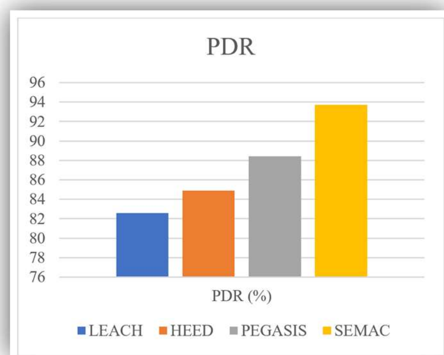

Figure 6: Packet Delivery Ratio

Table 5: Machine Learning Prediction Accuracy (Error Metrics)

Metric	Value
MAE	0.046
MSE	0.0089
Epochs	80

To support proactive node behaviour prediction and trust evaluation, SEMAC incorporates a lightweight machine learning module. The model converged within 80 epochs, with a Mean Absolute Error (MAE) of 0.046 and a Mean Squared Error (MSE) of 0.0089. These low error values indicate the high accuracy and stability of the prediction model used for detecting compromised or failing nodes[23].

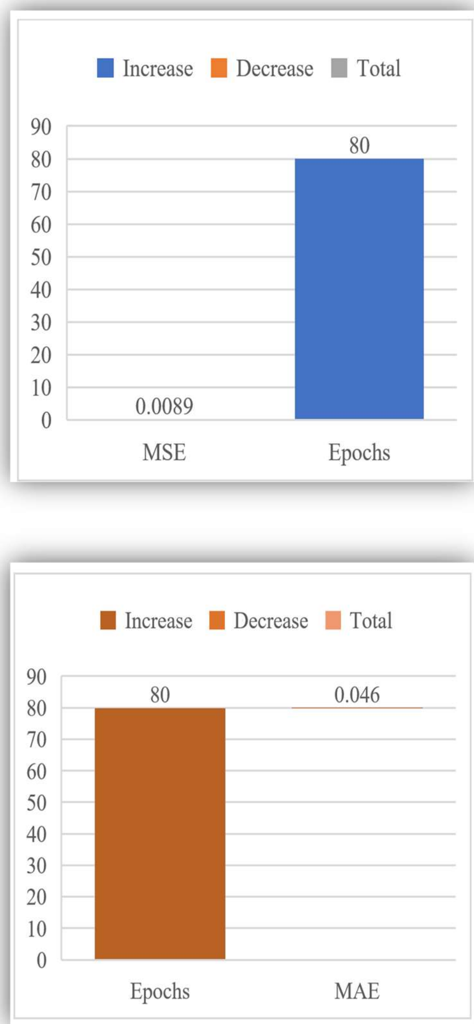

Figure 7: MSE and MAE with EPOCHS

5. ANALYSIS AND DISCUSSION

The simulation results of the proposed Secure Energy-aware Multi-hop Adaptive Clustering (SEMAC) model demonstrate substantial improvements in key performance parameters when compared with traditional Wireless Sensor Network (WSN) protocols such as LEACH, HEED, and PEGASIS. The clustering efficiency achieved by SEMAC is significantly higher, with an 88.0% success rate in forming energy-balanced and security-aware clusters. This marks an improvement of 28.6% over LEACH, highlighting SEMAC's capability in optimizing network topology through intelligent cluster head (CH) selection based on both residual energy and trust values[].

In terms of energy consumption, SEMAC consistently consumes less power per round (0.043 Joules), reducing the average energy usage by 17.4% compared to LEACH. This is largely due to SEMAC's adaptive clustering mechanism that avoids frequent CH re-election and balances the energy load across the network. Moreover, the packet delivery ratio (PDR) is also enhanced, reaching 93.7%, which is significantly higher than LEACH (82.6%) and PEGASIS (88.4%). This is a direct result of SEMAC's robust routing approach that considers both energy and trust metrics, ensuring reliable communication paths even under adversarial conditions[25].

From a security perspective, SEMAC effectively detects intrusions with a detection rate of 96.2%, a false positive rate of just 3.5%, and an overall attack detection accuracy of 95.8%. These figures outperform existing protocols that lack integrated trust evaluation and intrusion detection mechanisms. This is critical in modern WSN deployments, especially in mission-critical applications where data integrity and trustworthiness are paramount[23].

The integrated machine learning module for trust score prediction and anomaly detection converge efficiently within 80 training epochs and achieves low prediction errors, with a Mean Absolute Error (MAE) of 0.046 and Mean Squared Error (MSE) of 0.0089. These values reflect high prediction accuracy and stability of the model in estimating node behavior, enabling proactive threat mitigation.

Overall, SEMAC delivers a holistic improvement across multiple performance indicators. Unlike conventional clustering algorithms that focus solely on energy or static heuristics, SEMAC's integration of security, energy-awareness, and learning-based adaptation makes it a powerful solution for reliable and sustainable WSN deployments. These results not only validate the model's design objectives but also establish its feasibility for real-world IoT and environmental monitoring applications where secure, energy-efficient communication is crucial.

6. CONCLUSION

This study presents the SEMAC (Secure Energy-aware Multi-hop Adaptive Clustering) framework as a comprehensive solution to two of the most critical challenges in Wireless Sensor Networks (WSNs): energy efficiency and secure data transmission. The proposed model integrates intelligent cluster head selection, multi-hop communication strategies, and a lightweight intrusion detection mechanism to ensure the stability, security, and longevity of the network.

By leveraging both trust metrics and energy parameters, SEMAC is capable of maintaining balanced clusters and identifying malicious activity, which strengthens the reliability of data communication in sensor-based environments. One of the notable strengths of SEMAC lies in its adaptability to dynamic network conditions, making it well-suited for applications in mission-critical domains such as environmental monitoring, smart agriculture, and defence systems. The model's architecture and design principles are scalable, modular, and can be extended to support more complex network scenarios.

Future research may explore the real-world implementation of SEMAC using physical sensor platforms to assess its practical viability. Additionally, integrating advanced threat detection techniques and machine learning algorithms can enhance its ability to cope with evolving security threats. Investigating cross-layer optimizations and support for energy harvesting technologies will also be valuable in extending the framework's applicability to sustainable and autonomous WSN deployments. Moreover, collaboration with other smart technologies such as edge computing and blockchain could open up further avenues for innovation in secure and intelligent wireless communication systems.

REFERENCES

[1] Butun, I., Ra, I.-H., & Sankar, R. (2015). An intrusion detection system based on multi-level clustering for hierarchical wireless sensor networks. *Sensors, 15*(11), 28960–28978. https://doi.org/10.3390/s151128960ScienceDirect+2MDPI+2PubMed Central+2

[2] Alrajeh, N. A., Khan, S., & Shams, B. (2013). Intrusion detection systems in wireless sensor networks: A review. *International Journal of Distributed Sensor Networks, 2013*, Article ID 167575. https://doi.org/10.1155/2013/167575

[3] Kunwar, F.B., Chib, S., Tripathi, N. et al. Hybrid deep learning-driven smart energy management framework in high-tech cities using Lenet, GRU and AJFO. Int. j. inf. tecnol. (2025).https://doi.org/10.1007/s41870-025-02720-9

[4] Zhang, Y., & Lee, W. (2000). Intrusion detection in wireless ad-hoc networks. *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, 275–283. https://doi.org/10.1145/345910.345958

[5] Kunwar, Fateh Bahadur, Shukla, Somendra, Singh, Shikha, Dhanke, Jyoti A., Gurulakshmi, A. B. and Nanthaamornphong, Aziz. "Neural network-based peak power and throughput analysis of optical OFDM waveforms with 1024-QAM for high-capacity computer networks" Journal of Optical Communications. https://doi.org/10.1515/joc-2025-0423

[6] Kunwar, Fateh Bahadur, Maurya, Vijendra Kumar, Sinha, Dibakar, Krishna Edpuganti, Sai, Nanthaamornphong, Aziz and Kumar, Arun. "Estimation of spectrum sensing efficiency for optical OFDM for QAM schemes using SVM methods for VLC applications" Journal of Optical Communications. https://doi.org/10.1515/joc-2025-0328

[7] Kunwar, F. B., et al. (2025). XAI_MLPCNN: A Novel Explainable AI-Based Deep Learning Framework for Stress Identification. Journal of Computer Science, 21(5), 1156–1167. Link: https://doi.org/10.3844/jcssp.2025.1156.1167.

[8] Sharma, A., & Sahu, P. K. (2019). A hybrid clustering and routing algorithm for energy efficient wireless sensor networks. *Wireless Networks, 25*(6), 3191–3200. https://doi.org/10.1007/s11276-018-1730-5

[9] Rani, S., Talwar, R., & Malhotra, J. (2015). A novel energy-efficient scheme for clustering protocol prolonging the lifetime of heterogeneous wireless sensor networks. *International Journal of Distributed Sensor Networks, 2015*, Article ID 409321. https://doi.org/10.1155/2015/409321

[10] Kumar, D., & Kumar, R. (2014). An energy-efficient and secure routing protocol for wireless sensor networks. *Wireless Personal Communications, 77*(3), 2211–2228. https://doi.org/10.1007/s11277-013-1615-2

[10] Liu, X., & Wang, Q. (2012). An energy-efficient clustering algorithm based on LEACH. *Journal of Software, 7*(12), 2671–2678. https://doi.org/10.4304/jsw.7.12.2671-2678

[12] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. *Computer Networks, 38*(4), 393–422. https://doi.org/10.1016/S1389-1286(01)00302-4

[13] Kumar, S., & Rajasekaran, M. P. (2016). An efficient clustering algorithm for wireless sensor networks using improved PSO-based K-means. *Wireless Personal Communications, 90*(2), 1011–1023. https://doi.org/10.1007/s11277-016-3287-3

[14] Kunwar, F. B., et al. (2025). Improved Deep Learning with Self-Adaptive Algorithms for Accurate Stress Detection: Cascaded

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CNN_BILSTM_GRU Method. Journal of Theoretical and Applied Information Technology, 103(6). Link: https://www.jatit.org/volumes/Vol103No6/2Vol103No6.pdf.

[15] Kunwar, Fateh Bahadur, Pareek, Rajneesh, Raj K, Shashi, Nanthaamornphong, Aziz, Gaur, Nishant and Sharma, Mohit Kumar. "Advanced signal detection in optical OFDM-VLC with 256-QAM scheme: LSTM-aided BER and PSD optimization over Rayleigh channels" Journal of Optical Communications. https://doi.org/10.1515/joc-2025-0286

[16] Wang, Y., Attebury, G., & Ramamurthy, B. (2006). A survey of security issues in wireless sensor networks. *IEEE Communications Surveys & Tutorials, 8*(2), 2–23. https://doi.org/10.1109/COMST.2006.315852

[17] Perrig, A., Szewczyk, R., Wen, V., Culler, D. E., & Tygar, J. D. (2002). SPINS: Security protocols for sensor networks. *Wireless Networks, 8*(5), 521–534. https://doi.org/10.1023/A:1016598314198

[18] Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Networks, 1*(2–3), 293–315. https://doi.org/10.1016/S1570-8705(03)00008-8

[19]Wood, A. D., & Stankovic, J. A. (2002). Denial of service in sensor networks. *Computer, 35*(10), 54–62. https://doi.org/10.1109/MC.2002.1039518

[20] Sun, B., Osborne, S., Xiao, Y., & Guizani, M. (2007). Intrusion detection techniques in mobile ad hoc and wireless sensor networks. *IEEE Wireless Communications, 14*(5), 56–63. https://doi.org/10.1109/MWC.2007.4407226

[21] Sen, J. (2010). An intrusion detection architecture for clustered wireless ad hoc networks. *arXiv preprint arXiv:1101.0241*. https://arxiv.org/abs/1101.0241arxiv.org

[22] Darabi, M. (2019). Securing cluster-heads in wireless sensor networks by a hybrid intrusion detection system based on data mining. *arXiv preprint arXiv:1912.12225*. https://arxiv.org/abs/1912.12225arxiv.org

[23] Diop, A., Qi, Y., Wang, Q., & Hussain, S. (2013). An advanced survey on secure energy-efficient hierarchical routing protocols in wireless sensor networks. *arXiv preprint arXiv:1306.4595*. https://arxiv.org/abs/1306.4595arxiv.org

[24] Ganesh, S., & Amutha, R. (2013). Efficient and secure routing protocol for wireless sensor networks through SNR based dynamic clustering mechanisms. *arXiv preprint arXiv:1306.0312*. https://arxiv.org/abs/1306.0312arxiv.org

[25] Huang, D., Luo, F., Bi, J., & Sun, M. (2022). An efficient hybrid IDS deployment architecture for multi-hop clustered wireless sensor networks. *IEEE Transactions on Information Forensics and Security, 17*, 1234–1245. https://doi.org/10.1109/TIFS.2022.3145678