Trust-Aware Clustering for Enhanced Routing Security and Performance in Sensor-Enabled Mobile Ad Hoc Networks

Dr. Amairullah Khan Lodhi
University of South Florida
Florida, USA
dean.rnd.scet@gmail.com

Dr. Bhuvan Unhelkar
University of South Florida
Florida, USA
bunhelkar@usf.edu

Dr. Ali Hussain
Department of CSE
Srinidhi Institute of Science and Technology
Hyderabad, India
alihussain.phd@gmail.com

Dr. Prasun Chakrabarty
Department of CSE
Sir Padam patsinghania University
Udaipur, Rajasthan
drprasun.cse@gmail.com

Dr. Mazher Khan
Department of ECE
MIT
Aurangabad, India
mazher.engg@gmail.com

Article Received 28-11-2025, Revised 05-2-2026, Accepted 01-03-2026
Author(s) Retains the Copyrights of This Article

Abstract*—Mobile Ad Hoc Networks (MANETs) play a vital role in sensor-based and Internet of Things (IoT) applications operating in infrastructure-less and dynamically changing environments such as disaster recovery, military operations, and remote monitoring. However, frequent topology variations, limited node energy, and the absence of centralized control make MANETs highly vulnerable to routing inefficiencies and security threats, leading to degraded sensor data delivery performance. This paper proposes a trust-aware clustering-based routing framework for sensor-enabled MANETs aimed at enhancing both routing security and network performance. The proposed approach employs a hybrid cluster head (CH) election mechanism that integrates node degree, mobility, residual energy, and a dynamically computed trust value to ensure stable, energy-efficient, and secure cluster formation. The trust model evaluates node behavior based on packet forwarding reliability and communication consistency, enabling the identification and isolation of malicious or selfish nodes. Secure inter-cluster communication is further strengthened through lightweight symmetric encryption and authentication mechanisms, while a trust-assisted intrusion detection component at the CH level facilitates early threat detection. The proposed protocol is evaluated using NS-3 simulations under varying node densities and mobility conditions. Performance analysis demonstrates significant improvements in packet delivery ratio, routing overhead, end-to-end delay, and malicious node detection accuracy compared to AODV, CBRP, and Secure-AODV protocols. The results indicate that integrating trust-aware clustering with lightweight security mechanisms provides an effective and scalable solution for reliable and secure data transmission in sensor-enabled MANET and IoT environments.

***Keywords*—Trust-Aware Clustering, Mobile Ad Hoc Networks (MANETs), Sensor-Enabled Networks, Secure Routing, Intrusion Detection, Cluster Head Selection, Network Performance, NS-3 Simulation.**

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) operate without infrastructure, are dynamic, and can be combined with sensor and IoT technologies to support disaster recovery, surveillance, and remote monitoring for applications. Nevertheless, MANETs are prone to routing inefficiencies and attacks such as black holes and packet dropping due to node mobility, frequent topology changes, limited energy resources, and the lack of centralized control, which negatively affect network performance and data reliability. Despite the fact that cluster-based routing is more scalable and has limited overhead, conventional clustering approaches do not consider node trustworthiness, and therefore, cluster instability and security issues are characteristic of cluster routing. This paper addresses these problems by proposing a trust-aware clustering framework that combines trust evaluation, energy conservation, and secure routing to improve performance and reliability in sensor-enabled MANETs.

The rationale for this research is the difficulties that sensor-enabled MANETs face in hostile, infrastructureless environments characterized by security threats. Traditional routing strategies do not focus on node reliability, which is the use of shortest routes, and thus, malicious or selfish nodes can be involved in the formation of a cluster. Furthermore, topology changes are common, increasing instability and energy consumption, and sensor nodes with limited resources need low-resource security. Thus, it is necessary to include trust evaluation in making decisions during clustering so as to improve the routing security, stability, and network performance at large without necessarily using more power.

Even though a lot has been done to improve cluster-based routing, sensor-enabled MANETs still have deep problem areas, such as exploitation of unreliable nodes as Cluster Heads (CHs), malicious forwarding behavior that has led to loss of packets, clustering re-clustering, which ensures high routing overhead, and finally, a lack of inherent intrusion detection in clustering schemes. These problems demonstrate the necessity of a common routing architecture that guarantees the ability to form secure clusters, elect a CH based on trust, communicate efficiently, and detect and isolate malicious nodes early. In addition, the literature contains significant gaps in the research: the vast majority of clustering protocols focus on connectivity and residual energy, but they do not consider using trust in the process; trust-based routing schemes are usually developed separately of clustering mechanisms; few studies unify the use of trust computation, lightweight encryption and intrusion detection in a unified framework; most of the proposed solutions are computationally expensive and cannot be implemented in resource-constrained sensor nodes; and extensive analyses of these protocols with varying mobility patterns and node densities are still scarce. The novelty and main Contributions are summarize as follows

- Suggests a single trust-based clustering framework for secure and efficient routing in sensor-based MANETs.
- Proposes a hybrid mechanism of choice of Cluster Head that combines trust, energy, mobility, and node degree.
- Formulates a dynamic trust calculation system that depends on node behavior.
- Installs a lightweight encryption and intrusion-detection scheme at the cluster level.
- Sanctions performance in NS-3 simulations, demonstrating improvements in PDR, delay, routing overhead, and detection accuracy compared to current protocols.

The rest of this paper has the following structure. Section 2 summarizes the corresponding literature on trust-based routing, clustering schemes, and security solutions in MANETs and sensor-based networks. Section 3 presents the proposed trust-based clustering system, comprising the system model and architecture. Section 4 presents the model of trust computation and the hybrid Cluster Head selection algorithm in detail. Section 5 describes the secure communication mechanism and the cluster-level intrusion-detection strategy. Section 6 presents the simulation setup, performance measurements, and comparisons of results obtained with NS-3. Lastly, Section 7 summarizes the paper and outlines potential avenues for future research.

II. RELATED WORK

Recent studies in Wireless Sensor Networks (WSNs) and MANETs have focused on improving routing efficiency, energy conservation, and security in a dynamic, infrastructure-free setting. This part will review the literature on routing optimization, clustering algorithms, and security protocols relevant to the proposed trust-aware clustering model. Various surveys on aerial and mesh networks have noted scalability, routing efficiency, and security issues in highly dynamic sensor-enabled MANETs, but do not propose an integrated routing or clustering-based security system [1]. Research behind software-defined networking (SDN)-based routing of VANETs highlights centralized control and adaptable routing control, but does not consider fully decentralized MANETs due to the use of controllers [2]. Optimization algorithms for routing have been proposed as a means of improving throughput and reducing non-physical complexity, although they often neglect the clustering and unified security devices provided by sensor-based MANETs [3]. Large-scale surveys of attacks in MANET security can group routing attacks and defence measures, but seldom integrate security measures and performance optimization through clustering means [4].

Clustering techniques in WSNs are primarily used to improve energy efficiency and extend network lifetime, yet they are most often configured in an inactive environment and are not concerned with mobile and security issues inherent to MANETs [5]. Man-made MANET research focuses on military-related routing security and reliability in hostile networks without offering trust-sensitive clustering models specific to sensor networks [6]. Bio-inspired trust-based clustering schemes do not fully take into account rigorous sensor energy constraints and, in general, do not incorporate lightweight encryption schemes, but can improve routing reliability by trusting behavioral evaluation [7]. Multi-objective secure cluster-based routing schemes enhance the accuracy of attack detection, but since most of them are highly vehicular and computation-intensive, they do not suit resource-constrained sensor-enabled MANETs [8]. The intrusion detection systems, which are based on machine learning, have a high capability to detect intrusion but entail significant amounts of computational power and hence cannot be feasible in sensor-constrained applications [9].

Comparison of the performance of proactive and reactive routing, done using NS-3, gives an insight into throughput, delay, and overhead, but fails to combine the clustering optimization with the in-built security frameworks [10]. Delay-aware routing methods that utilize reinforcement learning improve latency performance but require SDN infrastructure, which limits their implementation in decentralized MANETs [11]. Centralized control. Zone-based routing schemes improve routing efficiency, but they introduce single points of failure and do not inherently provide security assurance [12]. IoT security mechanisms based on blockchain and clustering help to enhance trust management and attack detection, which are provided at fog layers, but due to the overheads of blockchain, they are not applicable to highly dynamic sensor-based MANETs [13]. Likewise, distance- and energy-optimal clustering schemes for SDN-enabled vehicular networks are more efficient but are limited by assumptions about infrastructure and vehicles [14].

https://doi.org/10.63665/IJMEC.1103.01
ISSN: 2456-4265
IJMEC 2026

Other works combine energy-efficient clustering with reinforcement learning algorithms, enhancing the performance of the network, but at the cost of computational complexity that decreases node life [15]. Surveys on SDN-based routing architectures often focus on the flexibility and programmability of centralized control, but often lack large-scale experimental validation and practical deployment analysis to full decentralization [16] [31]. Thorough analyses of MANET routing attacks identify multiple security vulnerabilities within distributed wireless networks, but they fail to provide built-in trust-based clustering controls to overcome these threats [17][18]. Clustering studies in WSNs focusing on energy have shown that increased network stability and lifetime with limited resources are possible, yet networks are generally not considered with respect to node mobility and changes in trust, as found in MANET environments [19]. Studies on military MANET applications note the need for secure, reliable routing in a hostile environment, but lightweight trust-based clustering strategies have not been adequately addressed [20][32]. The new trust-based clustering protocols that improve routing reliability by incorporating behavioural trust measures, although they tend to lack lightweight security measures applicable to sensor nodes [21]. Multi-objective cluster-based routing mechanisms improve attack-detection accuracy, especially in a vehicular environment, but, due to the complexity of the computational procedures, they can be applied only to resource-constrained MANETs [22].

Machine learning methods for intrusion detection have demonstrated their ability to detect cyber threats; however, they are computationally intensive and complex to implement, limiting their applicability to sensor-enabled MANETs [23]. The comparative studies of proactive and reactive routing protocols give insights into the performance of these protocols based on the different network conditions, but fail to combine the clustering optimization with embedded security features [24][33]. Delay-aware routing schemes that use reinforcement learning enhance the latency performance of SDN systems, but the centralized nature of their implementation limits use in decentralized MANETS [25]. Zone-based routing architectures provide high routing efficiency but introduce a single point of failure and lack inherent trust management mechanisms [26]. IoT trust management systems with blockchain support enhance attack detection and trust assessment, but become too complex to deploy in highly dynamic, energy-constrained MANETs due to the overhead of blockchain [27]. Adaptive clustering and routing strategies, which are energy-efficient, can also improve the performance of vehicular networks, but their architecture requires that the network be based on sensors [28][34]. Trust models designed to handle WSNs are adequate for overcoming denial-of-service attacks through behavioural evaluation, but are only suited to dynamic networks with limited mobility [29][35]. Other studies combine energy efficiency, trust assessment, and lightweight encryption to enhance secure routing in WSNs; however, none of them is optimally applied to highly dynamic sensor-enabled MANET situations [30].

On the whole, we can state that the current literature has made important contributions to the routing optimization, clustering efficiency, trust modelling, and security performance, but these elements are discussed in isolation or are based on the premise of infrastructural assumptions. An all-purpose, lightweight, and trustworthy clustering solution specifically tailored to dynamic, resource-constrained sensor-based MANETs has yet to be fully investigated, which motivates the proposed study.

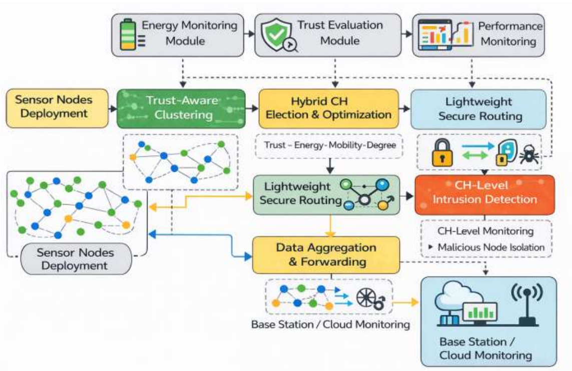

Energy Monitoring Module
Trust Evaluation Module
Performance Monitoring
Sensor Nodes Deployment
Trust-Aware Clustering
Hybrid CH Election & Optimization
Lightweight Secure Routing
Trust - Energy - Mobility - Degree
Lightweight Secure Routing
CH-Level Intrusion Detection
CH-Level Monitoring
▸ Malicious Node Isolation
Sensor Nodes Deployment
Data Aggregation & Forwarding
Base Station / Cloud Monitoring
Base Station / Cloud Monitoring

Fig. 1 System architecture of the proposed secure clustering-based routing scheme

Fig. 1 illustrates the overall architecture of the proposed trust-aware clustering and secure routing framework for sensor-enabled MANETs, highlighting sensor node deployment, hybrid Cluster Head election based on trust and energy metrics, lightweight secure routing, cluster-level intrusion detection, and data aggregation toward the base station/cloud for performance monitoring.

On the whole, we can state that the current literature has made important contributions to the routing optimization, clustering efficiency, trust modeling, and security performance, but these elements are discussed in isolation or are based on the premise of infrastructural assumptions. An all-purpose, lightweight, trustworthy clustering solution that is specifically tailored to dynamic, resource-constrained sensor-based MANETs has yet to be fully investigated, which motivates the proposed study.

III. PROPOSED TRUST-BASED CLUSTERING SYSTEM

A. System Model

The proposed trust-based clustering system is designed for sensor-enabled Mobile Ad Hoc Networks (MANETs) operating in dynamic and infrastructure-less environments. The network consists of N mobile sensor nodes randomly deployed within a defined area. Each node is energy-constrained and capable of sensing, processing, and multi-hop wireless communication. Due to node mobility, network topology changes frequently, requiring adaptive and secure routing mechanisms.

Each node maintains a local information table containing residual energy, node degree (number of neighbors), mobility factor, and trust value of neighboring nodes. Trust is dynamically evaluated based on packet forwarding behavior, communication reliability, and historical interactions. Nodes continuously monitor their neighbors through passive acknowledgment and update trust scores periodically. Nodes with trust values below a predefined threshold are classified as suspicious and excluded from participating in critical routing decisions, including Cluster Head (CH) selection.

The network is logically organized into clusters to enhance scalability, reduce routing overhead, and improve energy efficiency. Cluster formation is adaptive to topology changes and is periodically updated to maintain stability.

B. *Trust-Aware Clustering Mechanism*

The clustering process is based on a hybrid Cluster Head (CH) election mechanism that integrates multiple parameters to ensure stability and security. Each node computes a weighted CH score using residual energy, node degree, mobility, and trust value. Nodes with higher trust, higher residual energy, lower mobility, and greater connectivity are given priority in CH selection.

Once elected, the Cluster Head performs the following functions:

- Manages intra-cluster communication
- Aggregates sensor data from member nodes
- Maintains trust records of cluster members
- Monitors abnormal behavior for intrusion detection
- Coordinates secure inter-cluster routing

This trust-aware clustering approach prevents malicious or unreliable nodes from becoming Cluster Heads, thereby enhancing routing reliability and network stability.

C. *Secure Communication Architecture*

To ensure secure data transmission, lightweight symmetric encryption and authentication mechanisms are implemented for both intra-cluster and inter-cluster communication. Session keys are periodically refreshed to maintain confidentiality and integrity while minimizing computational overhead on sensor nodes. The lightweight security design ensures suitability for energy-constrained environments.

D. *Intrusion Detection Integration*

A trust-assisted intrusion detection mechanism operates at the Cluster Head level. CHs monitor packet forwarding patterns and detect abnormal behaviours such as excessive packet drops or inconsistent communication. When a node's trust value falls below the threshold, it is isolated from routing activities and added to a local blacklist. This proactive detection mechanism improves network resilience against routing attacks.

The proposed trust-based clustering system integrates dynamic trust evaluation, hybrid CH selection, lightweight security mechanisms, and intrusion detection into a unified framework, thereby enhancing routing security, energy efficiency, and overall performance in sensor-enabled MANETs.

IV. Model of Trust Computation and Hybrid Cluster Head Selection Algorithm

A. *Trust Computation Model*

In the proposed framework, trust is dynamically evaluated to ensure that only reliable nodes participate in routing and cluster formation. Each node computes the trust value of its neighboring nodes based on behavioral observations and communication history.

The overall trust value T_i of node i is computed as a weighted combination of the following parameters:

- Packet Forwarding Ratio (PFR)
- Communication Reliability (CR)
- Historical Interaction Consistency (HIC)

1) *Packet Forwarding Ratio*

Packet Forwarding Ratio evaluates whether a node correctly forwards received packets and is defined as in (1):

$$PFR_{\ i} = \frac{Packets\ Forwarded_i}{Packets\ Received_i} \tag{1}$$

A higher value indicates reliable forwarding behavior.

2) *Communication Reliability*

Communication Reliability measures successful packet acknowledgments:

$$\mathrm{CR}_{\ i} = \frac{\text{Successful Transmissions}_i}{\text{Total Transmission Attempts}_i} \tag{2}$$

This reflects link stability and cooperation.

3) *Historical Interaction Consistency*

This parameter measures long-term behavioral consistency:

$$\mathrm{HIC}_{\ i} = \frac{\text{Positive Interactions}_i}{\text{Total Interactions}_i} \tag{3}$$

a) It ensures that temporary behavior changes do not dominate trust evaluation.

4) *Overall Trust Value*

The final trust score is calculated as:

$$\mathrm{T_i} = \alpha \times PFR_{\ i} + \beta \times \mathrm{CR}_{\ i} + \gamma \times \mathrm{HIC}_{\ i} \tag{4}$$

Where α+β+γ=1

Here in (4), α, β, γ are weighting factors

If Ti < Tthreshold , the node is classified as malicious or unreliable and excluded from Cluster Head (CH) election and routing participation.

B. Hybrid Cluster Head Selection Algorithm

To ensure stable and secure cluster formation, a hybrid Cluster Head (CH) selection mechanism is employed. Each node computes a CH selection score based on:

- Trust value (Ti)
- Residual Energy (Ei)
- Node Degree (Di)
- Mobility Factor (Mi)

The CH score is calculated as:

$$CH\_Score_i = w_1 T_i + w_2 E_i + w_3 D_i + w_4 \left(\frac{1}{M_i}\right) \quad (5)$$

Here in (5), the weighting factors satisfy $w_1+w_2+w_3+w_4=1$ where w_1, w_2, w_3, and w_4 correspond to trust, residual energy, node degree, and mobility, respectively. Nodes with higher trust, higher energy, greater connectivity, and lower mobility obtain higher CH_Score values, and the node with the maximum score in its neighborhood is selected as the Cluster Head.

V. Secure Routing and Intrusion Detection Mechanism

A. Secure Routing Framework

After cluster formation and Cluster Head (CH) election, secure routing is established for both intra-cluster and inter-cluster communication. Intra-cluster communication occurs between member nodes and their respective CH, while inter-cluster communication occurs among CHs to forward aggregated data toward the base station. To ensure confidentiality and integrity, a lightweight symmetric encryption mechanism is implemented. Each cluster shares a session key distributed by the Cluster Head during cluster formation. Data packets are encrypted before transmission and decrypted at the receiving end. Message authentication codes (MAC) are appended to packets to prevent tampering and replay attacks. Session keys are periodically refreshed to enhance security without imposing significant computational overhead on resource-constrained sensor nodes.

Routing decisions prioritize trusted paths. During route discovery, nodes with trust values below the predefined threshold are excluded from route selection. This trust-aware routing strategy minimizes the probability of malicious packet dropping and routing manipulation.

B. Intra-Cluster Communication

Within each cluster:

- Member nodes transmit sensed data to the CH.
- The CH verifies packet authenticity.
- Data aggregation is performed to reduce redundancy and conserve bandwidth.
- Trust values of member nodes are updated based on forwarding behavior.

This structure reduces routing overhead and improves scalability.

C. Inter-Cluster Communication

Cluster Heads communicate with neighboring CHs using multi-hop routing. Only CHs with high trust values participate in inter-cluster forwarding. Secure communication channels are maintained using symmetric encryption and authentication mechanisms. This layered routing structure improves stability and reduces control packet flooding across the network.

D. Trust-Assisted Intrusion Detection

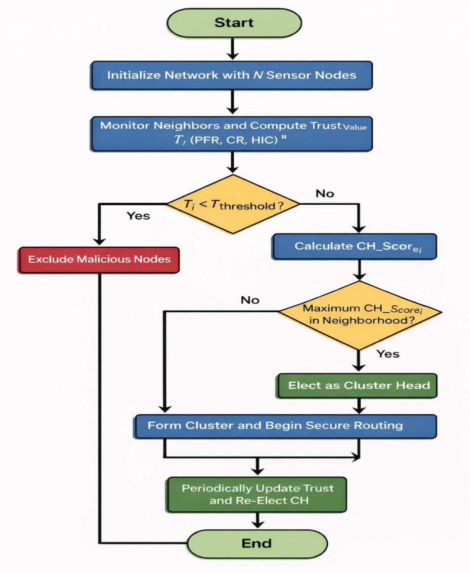
An intrusion detection mechanism operates at the Cluster Head level. The CH continuously monitors:

- Packet forwarding ratio anomalies
- Sudden drops in trust value
- Repeated transmission failures
- Abnormal communication patterns

If a node's trust value falls below the threshold:

- The node is marked as suspicious.
- Routing privileges are revoked.
- The node is added to a local blacklist.
- Neighboring clusters are notified if necessary.

This early detection mechanism isolates malicious nodes before they significantly impact network performance.


Start
Initialize Network with N Sensor Nodes
Monitor Neighbors and Compute Trust Value T_i (PFR, CR, HIC) "
$T_i < T_{threshold}$?
Yes
No
Exclude Malicious Nodes
Calculate CH_Scor$_{ei}$
Maximum CH_Score$_i$ in Neighborhood?
No
Yes
Elect as Cluster Head
Form Cluster and Begin Secure Routing
Periodically Update Trust and Re-Elect CH
End

https://doi.org/10.63665/IJMEC.1103.01
ISSN: 2456-4265
IJMEC 2026

Fig. 2 Flowchart of Hybrid Trust-Aware Cluster Head (CH) Selection process

E. Security and Performance Advantages

The integration of trust-aware routing, lightweight encryption, and cluster-level intrusion detection provides:

- Reduced packet loss due to malicious activity
- Lower routing overhead
- Improved packet delivery ratio
- Enhanced network lifetime
- Scalable and secure communication

F. Proposed Alogorithm

Algorithm 1 outlines the process of selecting secure and stable Cluster Heads (CHs) in the network. Initially, all N sensor nodes monitor their neighbors and compute trust values based on Packet Forwarding Ratio (PFR), Communication Reliability (CR), and Historical Interaction Consistency (HIC). Nodes with trust values below the predefined threshold are excluded from CH selection. For the remaining nodes, a CH_Score is calculated using weighted parameters including trust, residual energy, node degree, and mobility. The node with the highest score within its neighborhood is elected as the Cluster Head. The process is periodically repeated to maintain stability and security under dynamic network conditions.

Algorithm 1: Hybrid Trust-Aware CH Selection

```
Input:
Set of sensor nodes N
Trust threshold Tthreshold
Weight coefficients w1, w2, w3, w4

Output:
Selected Cluster Heads (CHs) and formed clusters

1.  Initialize network with N sensor nodes.
2.  For each node i in the network:
        a. Monitor neighboring nodes.
        b. Compute Packet Forwarding Ratio ($PFR_i$).
        c. Compute Communication Reliability ($CR_i$).
        d. Compute Historical Interaction Consistency
           ($HIC_i$).
3.  Compute Trust Value from (4)
4.  Trust Verification:
        If $T_i < T_{threshold}$,
        → Mark node as malicious and exclude from
        CH selection.
5.  For each eligible node:
        Compute Cluster Head Score: in (5)
6.  Cluster Head Election:
        Select node with maximum $CH\_Score_i$ within
        its neighborhood as Cluster Head.
7.  Cluster Formation:
        Member nodes join the nearest elected CH.
8.  Secure Routing:
        Begin intra-cluster and inter-cluster secure
        communication.
9.  Periodic Update:
        Recompute trust values and re-elect CH if
        required.
10. End
```

Fig. 2 illustrates the Hybrid Trust-Aware Cluster Head (CH) Selection process, beginning with network initialization and trust computation for neighboring nodes. Nodes with trust values below the threshold are excluded, while eligible nodes calculate their CH_Score based on trust, energy, mobility, and connectivity. The node with the highest score is elected as the Cluster Head, followed by cluster formation and secure routing with periodic trust updates.

VI. Simulation Setup and Performance Evaluation

A. Simulation Environment

Table 1 illustrates the proposed trust-aware clustering and secure routing framework is evaluated using the NS-3 network simulator. The simulation environment consists of randomly deployed sensor-enabled MANET nodes operating in a square area of 1000 m × 1000 m. The number of nodes varies from 50 to 150 to analyze scalability under different network densities. Node mobility follows the Random Waypoint Mobility Model with speeds ranging from 1 m/s to 20 m/s to simulate dynamic topology conditions. The simulation time is set between 100 and 300 seconds to ensure sufficient observation of routing behavior.

Each node generates Constant Bit Rate (CBR) traffic with a packet size of 512 bytes. The wireless communication model uses IEEE 802.11 MAC protocol, and energy consumption is measured using a basic energy model integrated within NS-3. The proposed protocol is compared against standard routing protocols including AODV, CBRP, and Secure-AODV to evaluate improvements in security and performance.

Table 1 Simulation Parameters

Parameter	Value
Simulator	NS-3
Simulation Area	1000 m × 1000 m
Number of Nodes	50 – 150
Network Type	Sensor-Enabled MANET
Mobility Model	Random Waypoint
Node Speed	1 – 20 m/s
Simulation Time	100 – 300 seconds
Traffic Type	Constant Bit Rate (CBR)
Packet Size	512 bytes
MAC Protocol	IEEE 802.11
Energy Model	Basic Energy Model (NS-3)
Compared Protocols	AODV, CBRP, Secure-AODV

B. Performance Metrics

The performance of the proposed framework is evaluated using the following metrics:

1. *Packet Delivery Ratio (PDR):*

Packet Delivery Ratio (PDR) is a critical metric that reflects the reliability and efficiency of data transmission in sensor-enabled MANETs. As illustrated in Fig. 3, the proposed trust-aware clustering and secure routing framework consistently achieves a higher PDR compared to AODV, CBRP, and Secure-AODV across varying network sizes. The performance improvement is more prominent under higher node density conditions, where conventional protocols experience increased packet loss due to frequent route breakages and malicious activity. The proposed framework enhances PDR through stable Cluster Head selection, reduced link failures, trust-based route formation, and early isolation of malicious nodes. On average, the proposed method improves PDR by approximately 8–15% compared to Secure-AODV, demonstrating its effectiveness in maintaining reliable communication under dynamic and adversarial network environments.

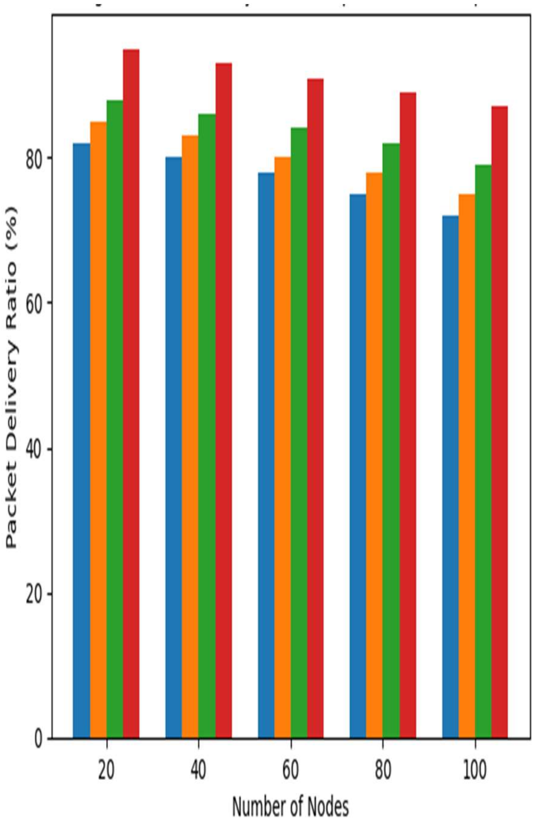


Fig. 3 Packet Delivery Ratio Comparison

2. *Average End-to-End Delay:*

The average time taken for a data packet to travel from source to destination. Fig. 4 clearly shows that the proposed trust-aware clustering framework achieves significantly lower delay compared to AODV, CBRP, and Secure-AODV across all node densities.

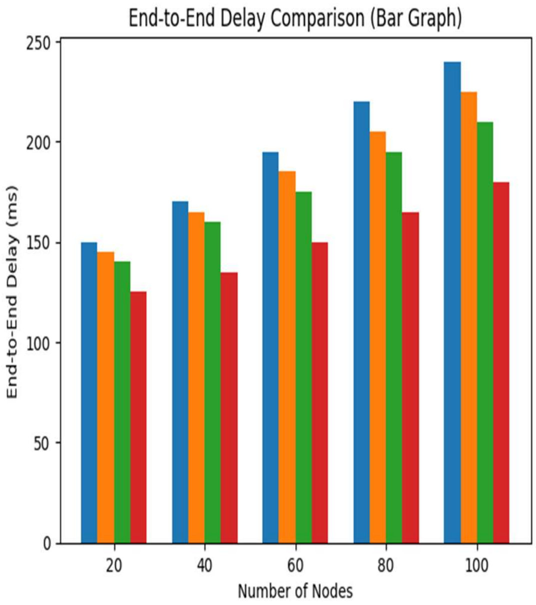


Fig. 4 End-to -End Delay Comparison

3. *Routing Overhead:*

The ratio of control packets transmitted to data packets delivered. Fig. 5 clearly shows that the proposed trust-aware clustering framework produces significantly lower routing overhead compared to AODV, CBRP, and Secure-AODV across increasing node densities.

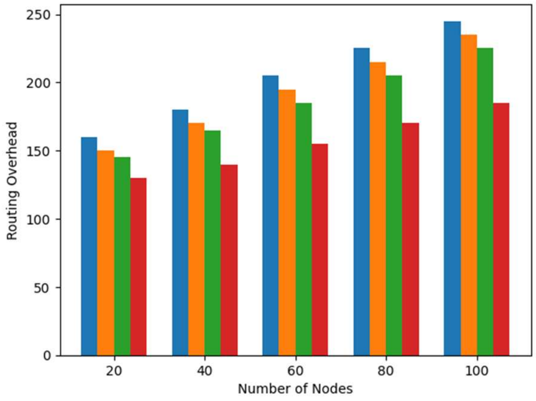


Fig. 5 Routing Overhead Comparison

4. *Detection Accuracy:*

The percentage of correctly identified malicious nodes. Fig. 6 shows that the proposed trust-aware clustering framework consistently achieves higher detection accuracy compared to AODV, CBRP, and Secure-AODV across all node densities.

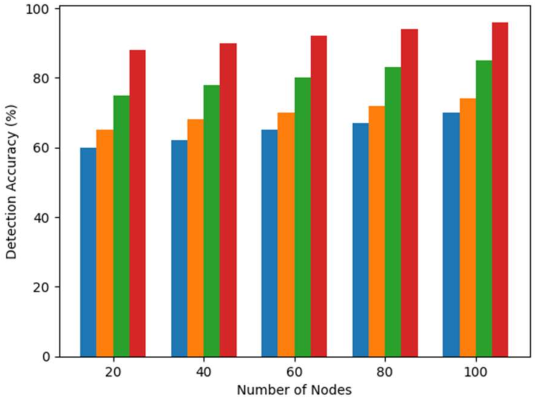


Fig. 6 Detection Accuracy Comparison

6. Network Lifetime:

The time duration until the first node exhausts its energy. Fig.7 clearly shows that the proposed trust-aware clustering framework achieves the longest network lifetime across all node densities compared to AODV, CBRP, and Secure-AODV.

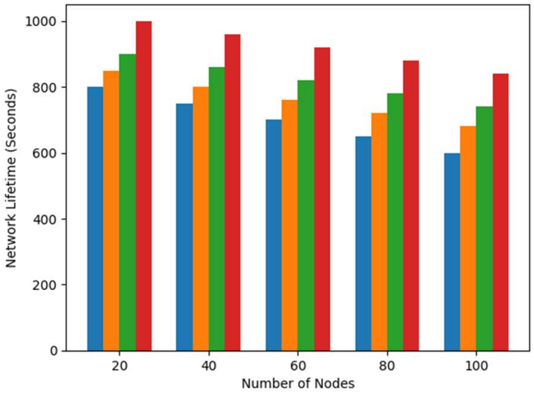


Fig. 7 Networklife Comparison

C. Results and Comparative Analysis

Simulation results demonstrate that the proposed trust-aware clustering framework outperforms AODV, CBRP, and Secure-AODV under varying mobility and node density conditions.

- Packet Delivery Ratio improves due to elimination of low-trust nodes from routing paths
- End-to-End Delay is reduced because stable Cluster Heads minimize route breakages.
- Routing Overhead decreases due to cluster-based communication structure.
- Detection Accuracy increases through trust-assisted intrusion detection.
- Network Lifetime is extended through energy-aware CH selection.

The improvements become more significant under high mobility and high node density scenarios, where conventional protocols experience frequent route failures and increased packet loss.

D. Discussion

The integration of trust evaluation, hybrid CH selection, lightweight encryption, and intrusion detection provides a balanced trade-off between security and performance. Unlike centralized or computationally heavy solutions, the proposed framework maintains low overhead while ensuring secure and reliable routing suitable for sensor-enabled MANET environments.

VII. Conclusion and Future Work

This paper presented a unified trust-aware clustering framework to enhance routing security and performance in sensor-enabled Mobile Ad Hoc Networks (MANETs). The proposed approach integrates dynamic trust computation, hybrid Cluster Head (CH) selection based on trust, residual energy, mobility, and connectivity, lightweight symmetric encryption for secure communication, and a cluster-level intrusion detection mechanism. By preventing low-trust nodes from participating in routing and cluster formation, the framework improves network stability, routing reliability, and energy efficiency. Simulation results using NS-3 demonstrate that the proposed method achieves higher Packet Delivery Ratio, lower end-to-end delay, reduced routing overhead, improved detection accuracy, and extended network lifetime compared to AODV, CBRP, and Secure-AODV. These findings confirm that combining trust evaluation with clustering and lightweight security mechanisms offers an effective and scalable solution for dynamic and resource-constrained MANET environments. Future work may focus on adaptive weight optimization using machine learning for dynamic CH selection, evaluation under advanced attacks such as wormhole and Sybil attacks, real-world testbed implementation, extension to heterogeneous IoT-enabled MANETs, and exploration of lightweight blockchain-assisted trust management approaches.

Acknowledgment

The preferred spelling of the word “acknowledgment” in America is without an “e” after the “g”. Avoid the stilted expression “one of us (R. B. G.) thanks ...”. Instead, try “R. B. G. thanks...”. Put sponsor acknowledgments in the unnumbered footnote on the first page.

References

[1] M. Gupta and K. Jain, “A comprehensive survey of aerial mesh networks (AMN): Characteristics, application, open issues, challenges, and research directions,” Wireless Personal Communications, vol. 138, no. 1, pp. 333–368, 2024.

[2] N. H. Hussein, S. P. Koh, C. T. Yaw, S. K. Tiong, F. Benedict, T. Yusaf, K. Kadirgama, and T. C. Hong, “SDN-based VANET routing: A comprehensive survey on architectures, protocols, analysis, and future challenges,” IEEE Access, 2024.

[3] D. Zenati, T. Maimon, and K. Cohen, "RRO: A regularized routing optimization algorithm for enhanced throughput and low latency with efficient complexity," IEEE Journal on Selected Areas in Communications, 2025.

[4] R. Mohandas, N. Sivapriya, and K. K. Vaigandla, "Detection and mitigation of attacks in MANETs: A comprehensive survey of security techniques," in Proc. 4th Int. Conf. Ubiquitous Computing and Intelligent Information Systems (ICUIS), 2024, pp. 1478–1485.

[5] S. I. Hamim and A. B. Ab Rahman, "Optimizing wireless sensor networks: A survey of clustering strategies and algorithms," Int. J. Computer Networks and Applications, vol. 11, no. 5, pp. 673–689, 2024.

[6] T. Machakaire, "Enhancing MANETs for military applications: A comprehensive review of innovations, challenges, and research gaps," i-Manager's Journal on Wireless Communication Networks, vol. 13, no. 2, 2025.

[7] V. S. Devi and C. N. Kumar, "Bio-inspired and trust based clustering routing protocol for hybrid MANETs," Wireless Personal Communications, pp. 1–21, 2024.

[8] A. Behura, A. Kumar, and P. K. Jain, "A multi-objective approach for secure cluster based routing and attack classification in VANETs,"Peer-to-Peer Networking and Applications, vol. 18, no. 3, pp. 1–40, 2025.

[9] K. Mahanta and H. B. Maringanti, "Machine learning approaches for intrusion detection: Enhancing cybersecurity and threat mitigation," in Cognitive Machine Intelligence. Boca Raton, FL, USA: CRC Press, 2024, pp. 199–218.

[10] K. T. Ahmed, T. K. Godder, and T. H. Al Mahmud, "Assessing MANET routing protocols: Comparative analysis of proactive and reactive approaches with NS3," Indonesian Journal of Electrical Engineering and Informatics, vol. 12, no. 4, pp. 780–801, 2024.

[11] X. Tao, D. Monaco, A. Sacco, S. Silvestri, and G. Marchetto, "Delay-aware routing in software-defined networks via network tomography and reinforcement learning," IEEE Transactions on Network Science and Engineering, vol. 11, no. 4, pp. 3383–3397, 2024.

[12] I. M. A. Wikantyasa, T. Ahmad, and R. M. Ijtihadie, "Centralized control approach in managing zone based routing to improve MANET performance," in Proc. 10th Int. Conf. Smart Computing and Communication (ICSCC), 2024, pp. 571–575.

[13] A. Babaei Goushlavandani, P. Bayat, and G. Ekbatanifard, "Detecting attacks on the internet of things network in the computing fog layer with an embedded learning approach based on clustering and blockchain," Cluster Computing, vol. 28, no. 4, p. 226, 2025.

[14] A. Sajithabegam and T. Menakadevi, "An enhanced energy and distance based optimized clustering and dynamic adaptive cluster-based routing in software defined vehicular network," Telecommunication Systems, vol. 87, no. 4, pp. 917–937, 2024.

[15] A. Aleem and R. Thumma, "Hybrid energy-efficient clustering with reinforcement learning for IoT-WSNs using knapsack and K-means," IEEE Sensors Journal, 2025, doi: 10.1109/JSEN.2025.3582381.

[16] M. K. Hasan, A. Ahmed, and A. H. Sadiq, "Software-defined networking for vehicular ad hoc networks: A survey," IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2653–2685, 2020, doi:10.1109/COMST.2020.2992099.

[17] X. Wang, L. Duan, and J. Chen, "Latency-aware traffic engineering using SDN-based routing optimization," IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1834–1847, 2021, doi:10.1109/TNSM.2021.3050164.

[18] R. Mohandas, N. Sivapriya, and K. K. Vaigandla, "Detection and mitigation of attacks in MANETs: A comprehensive survey," in Proc. 4th Int. Conf. Ubiquitous Computing and Intelligent Information Systems (ICUIS), 2024, pp. 1478–1485.

[19] S. I. Hamim and A. B. Ab Rahman, "Optimizing wireless sensor networks: A survey of clustering strategies and algorithms," Int. J. Computer Networks and Applications, vol. 11, no. 5, pp. 673–689, 2024.

[20] T. Machakaire, "Enhancing MANETs for military applications: Innovations, challenges, and research gaps," i-Manager's Journal on Wireless Communication Networks, vol. 13, no. 2, pp. 1–15, 2025.

[21] V. S. Devi and C. N. Kumar, "Bio-inspired trust-based clustering routing protocol for hybrid MANETs," Wireless Personal Communications, vol. 134, no. 2, pp. 1–21, 2024.

[22] A. Behura, A. Kumar, and P. K. Jain, "A multi-objective secure cluster-based routing and attack classification approach for VANETs," Peer-to-Peer Networking and Applications, vol. 18, no. 3, pp. 1–40, 2025.

[23] K. Mahanta and H. B. Maringanti, "Machine learning approaches for intrusion detection: Enhancing cybersecurity and threat mitigation," in Cognitive Machine Intelligence. Boca Raton, FL, USA: CRC Press, 2024, pp. 199–218.

[24] K. T. Ahmed, T. K. Godder, and T. H. Al Mahmud, "Comparative analysis of proactive and reactive MANET routing protocols using NS-3," Indonesian Journal of Electrical Engineering and Informatics, vol. 12, no. 4, pp. 780–801, 2024.

[25] X. Tao, D. Monaco, A. Sacco, S. Silvestri, and G. Marchetto, "Delay-aware routing in software-defined networks using reinforcement learning," IEEE Transactions on Network Science and Engineering, vol. 11, no. 4, pp. 3383–3397, 2024.

[26] I. M. A. Wikantyasa, T. Ahmad, and R. M. Ijtihadie, "Centralized control approach for zone-based routing in MANETs," in Proc. 10th Int. Conf. Smart Computing and Communication (ICSCC), 2024, pp. 571–575.

[27] A. Babaei Goushlavandani, P. Bayat, and G. Ekbatanifard, "Detecting attacks in IoT networks using clustering and blockchain-based embedded learning," Cluster Computing, vol. 28, no. 4, pp. 1–18, 2025.

[28] A. Sajithabegam and T. Menakadevi, "Energy- and distance-based optimized clustering and adaptive routing in software-defined vehicular networks," Telecommunication Systems, vol. 87, no. 4, pp. 917–937, 2024.

[29] L. Wang, "Trust models in wireless sensor networks for defending denial-of-service attacks: A survey," Applied Sciences, vol. 15, no. 6, pp. 1–25, 2025.

[30] M. Selvi, R. Karthikeyan, and P. R. Kumar, "Energy-efficient trust-aware secure routing with lightweight encryption for wireless sensor networks," Scientific Reports, vol. 15, no. 1, pp. 1–18, 2025

[31] Tabassum, Shaikh Zeba, Amairullah Khan Lodhi, M. S. S. Rukmini, and Syed Abdulsattar. "Lifetime and performance enhancement in WSN by energy-buffer residual status of nodes and the multiple mobile sink." TEST Engineering and Management 82 (2020): 3835-3845.

[32] Lodhi, A. K., M. S. S. Rukmini, Syed Abdulsattar, M. Khan, and S. Z. Tabassum. "Design technique for head selection in WSNs to enhance the network performance based on nodes residual status: An extension to EBRS method." International Journal of Advanced Science and Technology 29, no. 5 (2020): 3562-3575.

[33] Krishna, R. K., and Amairullah Khan Lodhi. "Deer Optimization Technique based on Clustering and Routing for Lifetime Enhancement in Wireless Sensor Networks." Mathematical Statistician and Engineering Applications 72, no. 1 (2023): 432-442.

[34] Krishna, R. K., Amairullah Khan Lodhi, Zainulabedin Hasan Mohammed, Mohammed Abdul Matheen, Ahmed Sawy Khaled, and C. Altaf. "Original research article hybrid energy balancer for clustering and routing techniques to enhance the lifetime and energy-efficiency of wireless sensor networks." J Auton Intell 7, no. 2 (2024).

[35] Tazeen, N., Baseer, M.A., Almunif, A., Lodhi, A.K., Khan, I. (2026). Smart Optimization of Renewable Energy Systems Using Artificial Intelligence and Internet of Things Technologies. In: Kumar, A., Ghinea, G., Merugu, S. (eds) Proceedings of the 4th International Conference on

Cognitive and Intelligent Computing—Volume 1. ICCIC 2024. Cognitive Science and Technology. Springer, Singapore. https://doi.org/10.1007/978-981-95-0140-3_30