Journal of Engineering and Technology for Industrial Applications

ISSN ONLINE: 2447-0228

ITEGAM-JETIA

Manaus, v.11 n.54, p. 25-33. July/August., 2025.
DOI: https://doi.org/10.5935/jetia. v11i54.1689

RESEARCH ARTICLE OPEN ACCESS

HYBRID TRUST-BASED MODELS AND PROTOCOLS FOR ENHANCED SECURITY AND PERFORMANCE IN DYNAMIC WIRELESS SENSOR NETWORKS AND WIRELESS AD HOC NETWORKS

Seshagiri Rao Ganta[1], Naga Malleswara Rao Nallamothu[2]

[1]Research Scholar, Department of Computer Science and Engineering, University College of Engineering, Acharya Nagarjuna University, Guntur, India, AP, India
[2]Professor and Head of the Department, Department of CSE-IoT, RVR & JC College of Engineering (A), Guntur, India

[1]http://orcid.org/0009-0001-3140-7933, [2]http://orcid.org/ 0000-0002-1360-1150

Email: seshagiri.ganta@gmail.com, nnmrao@rvrjc.ac.in

ARTICLE INFO

Article History
Received: March 9, 2025
Revised: April 20, 2025
Accepted: June 15, 2025
Published: July 31, 2025

Keywords:
Wireless Sensor Networks (WSNs),
Wireless Ad Hoc Networks (WANETs),
Trust Management,
Intrusion Detection,
Ant Colony Optimization (ACO),
Node Integrity,
Security Protocols,
Hybrid Security,
Dynamic Networks.

ABSTRACT

Wireless Sensor Networks (WSNs) and Wireless Ad Hoc Networks (WANETs) are crucial for real-time applications, yet they encounter several obstacles, including the preservation of data privacy, ensuring node integrity, and optimizing path planning—especially when implemented in dynamic, large-scale environments. Conventional methods frequently lack cohesive systems for trust management and node verification, which results in security vulnerabilities and performance shortcomings. This study introduces innovative hybrid trust-based models and protocols aimed at overcoming these challenges. For dynamic WSNs, a hybrid approach utilizing Ant Colony Optimization (ACO) is proposed that seamlessly integrates node trust probability with path planning and is further enhanced by both local and global update strategies. In the context of WANETs, we unveil a non-linear integrity-based intrusion detection model, complemented by a hybrid security protocol that combines an integrity-centric approach with an encryption framework for secure node-to-node communication. The experimental outcomes of these studies highlight substantial advancements compared to traditional techniques, demonstrating improvements in numerous aspects such as runtime efficiency, hash variations, privacy protection, route overhead, packet delivery rates, delays, throughput, and overall security. These strategies exemplify the effectiveness of hybrid trust-based and integrity-oriented solutions in strengthening both security and performance within contemporary wireless networks.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) and Wireless Ad Hoc Networks (WANETs) have emerged as enabling technologies for a wide range of applications, including environmental monitoring, disaster management, healthcare, and military surveillance [1],[2]. These networks offer the flexibility and adaptability necessary for deployment in diverse and often unpredictable environments. However, their inherent characteristics, such as limited resources, distributed architecture, and reliance on wireless communication, make them particularly vulnerable to security threats and performance bottlenecks [3].

Traditional security solutions for wired networks are often unsuitable for WSNs and WANETs due to their resource constraints and dynamic topology. Furthermore, these networks are susceptible to various attacks targeting data confidentiality, integrity, and availability, including node capture, Sybil attacks, wormhole attacks, and routing disruptions [4]. A critical challenge lies in developing robust and efficient security mechanisms that can adapt to the dynamic nature of these networks while maintaining acceptable levels of performance.

Trust management has emerged as a promising approach for enhancing security and performance in WSNs and WANETs [5]. By evaluating the trustworthiness of nodes based on their past behavior and interactions, trust-based mechanisms can identify and isolate malicious nodes, thereby mitigating the impact of attacks and improving overall network resilience. However, existing trust management schemes often suffer from limitations, such as vulnerability to collusion attacks, high computational overhead, and lack of integration with routing protocols.

This paper presents novel hybrid trust-based models and protocols designed to address the limitations of traditional approaches and enhance security and performance in dynamic WSNs and WANETs. The contributions of this work are two-fold:

- **Hybrid ACO-Based Trust Management for Dynamic WSNs:** A novel hybrid Ant Colony Optimization (ACO)-based approach is proposed that integrates node trust probability with path planning. This approach incorporates local and global update measures to dynamically adjust trust values and optimize route selection based on both trust and network performance metrics.

- **Integrity-Based Intrusion Detection and Hybrid Security Protocol for WANETs:** A non-linear integrity-based intrusion detection model is introduced, along with a hybrid security protocol employing an integrity approach and encryption framework for node-to-node communication. This approach focuses on verifying the integrity of data and control messages to detect and mitigate intrusions in WANETs.

The remainder of this paper is structured as follows: Section 2 provides a review of related work in trust management and security protocols for WSNs and WANETs. Section 3 details the proposed hybrid ACO-based trust management approach for dynamic WSNs. Section 4 presents the integrity-based intrusion detection model and hybrid security protocol for WANETs. Section 5 presents and discusses the experimental results. Finally, Section 6 concludes the paper and outlines future research directions.

II. RELATED WORK

Extensive research has been conducted on trust management and security protocols for WSNs and WANETs. This section provides a brief overview of the existing literature, highlighting the key challenges and limitations of traditional approaches.

II.1 TRUST MANAGEMENT IN WSNS AND WANETS

Several trust management schemes have been proposed for WSNs and WANETs, focusing on various aspects, such as direct trust evaluation, indirect trust evaluation, and reputation-based systems [6], [7]. Direct trust evaluation involves assessing the trustworthiness of a node based on its direct interactions with other nodes. Indirect trust evaluation leverages information from neighboring nodes to infer the trustworthiness of a node. Reputation-based systems combine direct and indirect trust information to build a comprehensive reputation score for each node.

For example, [8] proposes a distributed trust management scheme for WSNs based on the Beta distribution. This scheme utilizes Bayesian inference to update trust values based on observed behavior. [9] presents a reputation-based trust management system for MANETs that considers both positive and negative feedback from neighboring nodes.

However, many existing trust management schemes are vulnerable to collusion attacks, where malicious nodes collaborate to manipulate trust values. Furthermore, the computational overhead of trust evaluation can be significant, particularly in resource-constrained WSNs. Moreover, many trust management schemes are designed independently of routing protocols, leading to suboptimal performance.

II.2 SECURITY PROTOCO]LS IN WSNS AND WANETS

Various security protocols have been developed to address the specific security challenges of WSNs and WANETs [10-12]. These protocols employ cryptographic techniques, such as symmetric-key encryption, asymmetric-key encryption, and hash functions, to protect data confidentiality, integrity, and authenticity.

For instance, [13] proposes a lightweight encryption scheme for WSNs based on elliptic curve cryptography (ECC). This scheme aims to provide strong security with minimal computational overhead. [14] presents a key management protocol for MANETs that utilizes a distributed key generation algorithm to establish secure communication channels.

However, traditional security protocols often rely on pre-distributed keys or require complex key management mechanisms, which can be challenging to implement in dynamic and large-scale networks. Furthermore, many protocols focus primarily on encryption and neglect the importance of data integrity and intrusion detection. Intrusion detection systems (IDS) are crucial for identifying malicious activities and protecting the network from attacks.

II.3 LIMITATIONS OF EXISTING APPROACHES

Existing trust management schemes and security protocols often suffer from the following limitations:

- **Lack of Integration:** Trust management and security protocols are often designed independently of each other, leading to suboptimal performance and security.

- **Vulnerability to Attacks:** Many schemes are vulnerable to collusion attacks, Sybil attacks, and other sophisticated attacks.

- **High Computational Overhead:** The computational overhead of trust evaluation and security protocols can be significant, particularly in resource-constrained WSNs.

- **Limited Scalability:** Many schemes are not scalable to large-scale and dynamic networks.
- **Neglect of Data Integrity:** Some protocols focus primarily on encryption and neglect the importance of data integrity and intrusion detection.

The proposed hybrid trust-based models and protocols in this paper aim to address these limitations by integrating trust management with routing protocols and incorporating integrity-based intrusion detection mechanisms.

III. MATERIALS AND METHODS

This section details the proposed hybrid ACO-based trust management approach for dynamic WSNs. This approach aims to optimize route selection by integrating node trust probability with path planning, utilizing an enhanced ACO algorithm with local and global update measures.

III.1 TRUST MODEL

The trust model utilizes a dynamic trust value, $T_{i,j}(t)$, representing the trust level node *i* places on node *j* at time *t*. This value is continuously updated based on the observed behaviour of node *j*. The trust value ranges from 0 to 1, where 0 represents complete distrust and 1 represents complete trust.

The trust value is updated based on both direct observations (successful and unsuccessful interactions) and indirect observations (recommendations from neighboring nodes). The update mechanism is designed to be adaptive to the dynamic nature of the network and to mitigate the impact of false recommendations.

III.2 ACO-BASED ROUTING PROTOCOL

The proposed routing protocol builds upon the principles of Ant Colony Optimization (ACO). ACO is a metaheuristic optimization algorithm inspired by the foraging behavior of ants. In this context, ants represent routing packets, and the pheromone trails represent the desirability of a particular path.

The algorithm consists of the following steps:

Initialization:

1. **Network Setup:**
   - Define the network topology (nodes and their connections/neighbors).
   - Assign distances to each connection (edge).
   - Initialize trust values between neighboring nodes (e.g., to 0.5 or a default value).
   - Initialize pheromone levels on all edges (e.g., to a small positive value like 1.0).
2. **Parameter Setup:**
   - Set the algorithm parameters: α, β, γ (pheromone, heuristic, trust weights), ρ (global pheromone evaporation), ξ (local pheromone evaporation), τ0 (initial pheromone level), Q (pheromone deposit constant), num_ants, and iterations.

Iteration Loop (Repeat for a fixed number of iterations):

1. **Ant Deployment:**
   - For each ant (from 1 to num_ants):
     - Start the ant at the source_node.
     - Initialize the ant's current_path to [source_node].
     - Initialize the ant's path_length to 0.
2. **Path Construction (While the ant has not reached the destination):**
   - Let i be the current node the ant is at.
   - Get the neighbors of node i: Neighbors(i).
   - Calculate the probability P_{i,j} for each neighbor j in Neighbors(i):
     - P_{i,j} = ([τ_{i,j}(t)]^α * [η_{i,j}]^β * [T_{i,j}(t)]^γ) / (∑_{k ∈ Neighbors(i)} [τ_{i,k}(t)]^α * [η_{i,k}]^β * [T_{i,k}(t)]^γ)
     - Where:
       - τ_{i,j}(t) is the pheromone level on the edge from i to j.

- $\eta_{i,j}$ is the heuristic information (e.g., 1 / distance(i, j)).
- $T_{i,j}(t)$ is the trust value node i places on node j.

- Select the next node j based on the calculated probabilities (e.g., using weighted random selection).
- Add node j to the current_path.
- Update path_length by adding the distance between i and j.
- Update current_node to j.
- **Local Pheromone Update:**
  - $\tau_{i,j}(t+1) = (1 - \xi)\tau_{i,j}(t) + \xi \tau_0$ (Update the pheromone on the edge just traversed)

3. **Path Evaluation:**
   - Once the ant reaches the destination_node, store the current_path and path_length.
4. **Find Best Path:**
   - After all ants have completed their paths, determine the best path (e.g., the one with the shortest path_length).
5. **Global Pheromone Update:**
   - For each edge (i, j) in the best path:
     - $\Delta\tau_{i,j} = Q / L$ (Where L is the length of the best path)
     - $\tau_{i,j}(t+1) = (1 - \rho)\tau_{i,j}(t) + \rho \Delta\tau_{i,j}$
6. **Trust Update:**
   - For each edge (i, j) in the best path:
     - Simulate a packet transmission success/failure (e.g., using a random number).
     - If successful: Increase the trust value from node i to node j.
     - If failed: Decrease the trust value from node i to node j.

III.3 ADVANTAGES OF THE HYBRID APPROACH

The proposed hybrid ACO-based trust management approach offers several advantages over traditional routing protocols:

- **Improved Security:** By integrating trust into the routing process, the protocol can avoid malicious nodes and improve the security of the network.
- **Enhanced Performance:** The ACO algorithm can find efficient and reliable paths, leading to improved packet delivery ratio, reduced delay, and increased throughput.
- **Adaptability:** The dynamic trust update mechanism allows the protocol to adapt to the changing behavior of nodes and the dynamic topology of the network.
- **Resilience:** The distributed nature of the ACO algorithm makes the protocol resilient to node failures and network disruptions.

IV. INTEGRITY-BASED INTRUSION DETECTION AND HYBRID SECURITY PROTOCOL FOR WANETS

This section presents the integrity-based intrusion detection model and hybrid security protocol for WANETs. This approach focuses on verifying the integrity of data and control messages to detect and mitigate intrusions.

IV.1 NON-LINEAR INTEGRITY-BASED INTRUSION DETECTION MODEL

The core of the intrusion detection model is based on monitoring the integrity of received messages. Deviations from expected integrity values indicate potential intrusions. A non-linear function is employed to model the relationship between the integrity value and the likelihood of an intrusion, allowing for more nuanced detection capabilities.

The integrity value is calculated using a hash function. The hash function is applied to the message content, sender ID, receiver ID, and a shared secret key between the sender and receiver. The resulting hash value is then compared to the expected hash value.

A non-linear function, such as a sigmoid function, is used to map the difference between the calculated hash value and the expected hash value to an intrusion likelihood score:

Intrusion Likelihood = ({1}{1 + e^{-k(Difference - Threshold)}})

Where:

- *Difference* is the difference between the calculated hash value and the expected hash value.
- *Threshold* is a pre-defined threshold value.
- *k* is a parameter that controls the steepness of the sigmoid function.

This non-linear function allows for a more sensitive detection of small deviations from the expected integrity value, while also reducing the likelihood of false positives.

IV.2 HYBRID SECURITY PROTOCOL

The proposed hybrid security protocol combines an integrity approach with an encryption framework for node-to-node communication. The protocol consists of the following steps:

Phase 1: Key Exchange

1. **Initiate Key Exchange:**
    - Node A and Node B agree to establish a secure communication channel.
2. **Diffie-Hellman (or similar):**
    - Node A and Node B perform a secure key exchange protocol (e.g., Diffie-Hellman) to generate a shared secret key K_AB.
3. **Periodic Key Update:**
    - After a predetermined time interval or number of messages, repeat steps 1 and 2 to update K_AB.

Phase 2: Message Transmission (Node A sends to Node B)

1. **Message Preparation:**
    - Node A prepares the message M to be sent.
    - Node A identifies itself as Sender_ID and Node B as Receiver_ID.
2. **Hash Calculation:**
    - Node A calculates the hash value H of the concatenated data: H = Hash(M || Sender_ID || Receiver_ID || K_AB). (Where || means concatenation). Use a secure hashing algorithm like SHA-256.
3. **Encryption:**
    - Node A encrypts the message M and the hash value H using the shared secret key K_AB and a symmetric-key encryption algorithm (e.g., AES):
        - Ciphertext = AES_Encrypt(M || H, K_AB)
4. **Transmission:**
    - Node A transmits the Ciphertext to Node B.

Phase 3: Message Reception and Verification (Node B Receives)

1. **Decryption:**
    - Node B decrypts the received Ciphertext using the shared secret key K_AB:
        - Decrypted_Data = AES_Decrypt(Ciphertext, K_AB)
    - Node B separates the decrypted data into the message M' and the received hash value H': M' || H' = Decrypted_Data.
2. **Integrity Verification:**
    - Node B calculates its own hash value H_calculated using the decrypted message M', Sender_ID, Receiver_ID, and the shared secret key K_AB:
        - H_calculated = Hash(M' || Sender_ID || Receiver_ID || K_AB)

3. **Comparison:**
    - Node B compares the calculated hash value H_calculated with the received hash value H'.
4. **Intrusion Detection:**
    - **If** H_calculated is **equal** to H':
        - The message is considered authentic and intact. Proceed to process the message M'.
    - **Else** (if H_calculated is **not equal** to H'):
        - **Raise Alarm:** An intrusion is suspected.
        - **Initiate Intrusion Detection Mechanism:** Trigger the non-linear integrity-based intrusion detection model (implementation details depend on the specific model - see note below). This might involve:
            - Logging the event.
            - Blocking communication with the sender (Node A).
            - Alerting an administrator.
            - Analyzing network traffic for other suspicious activity.

IV.3 ADVANTAGES OF THE HYBRID APPROACH

The proposed hybrid security protocol offers several advantages over traditional security protocols:

- **Enhanced Security:** The combination of integrity verification and encryption provides strong protection against various attacks, including message modification, message forgery, and eavesdropping.
- **Improved Intrusion Detection:** The non-linear integrity-based intrusion detection model allows for more sensitive and accurate detection of intrusions.
- **Reduced Overhead:** The protocol utilizes symmetric-key encryption, which has lower computational overhead than asymmetric-key encryption.

Adaptability: The protocol can be adapted to different security requirements by adjusting the parameters of the hash function and the encryption algorithm

V. RESULTS AND DISCUSSION

This section presents the experimental results obtained from simulations conducted to evaluate the performance of the proposed hybrid trust-based models and protocols.

IV.1 SIMULATION SETUP

The simulations were conducted using Network Simulator 3 (NS-3), a widely used network simulation platform. Two separate simulation scenarios were set up:

- **WSN Simulation:** A WSN with 100 randomly deployed sensor nodes was simulated. The nodes were deployed in a 100m x 100m area. The radio range of each node was set to 20m. The simulations were run for 600 seconds. Various attack scenarios, including blackhole attacks and grayhole attacks, were simulated to evaluate the performance of the hybrid ACO-based trust management approach.
- **WANET Simulation:** A MANET with 50 mobile nodes was simulated. The nodes were randomly deployed in a 1000m x 1000m area. The mobility model used was the Random Waypoint model. The simulations were run for 300 seconds. Various attack scenarios, including message modification attacks and message forgery attacks, were simulated to evaluate the performance of the integrity-based intrusion detection model and hybrid security protocol.

IV.2 PERFORMANCE METRICS

The following performance metrics were used to evaluate the performance of the proposed approaches:

- **Runtime:** The time taken to establish a secure route or detect an intrusion.
- **Hash Variation:** The degree of deviation in hash values, indicating potential data tampering.
- **Privacy Preservation:** The ability to maintain data confidentiality and prevent unauthorized access.
- **Route Overhead:** The number of control packets required to establish a route.
- **Packet Delivery Ratio (PDR):** The percentage of packets successfully delivered to the destination.

- **Delay:** The average time taken for a packet to reach the destination.
- **Throughput:** The average rate at which data is successfully transmitted.
- **Security:** The ability to detect and mitigate attacks.

IV.3 RESULTS AND DISCUSSION

IV.3.1 WSN Simulation Results

The simulation results for the WSN scenario demonstrated that the hybrid ACO-based trust management approach significantly improved the performance and security of the network compared to traditional ACO-based routing protocols. Specifically, the results showed:

- **Improved Packet Delivery Ratio:** The hybrid approach achieved a higher packet delivery ratio than the traditional ACO-based routing protocol, especially in the presence of malicious nodes. The trust-based route selection mechanism effectively avoided malicious nodes, leading to more reliable packet delivery.
- **Reduced Delay:** The hybrid approach resulted in a lower average delay than the traditional ACO-based routing protocol. The trust-based route selection mechanism favored more trustworthy and efficient paths, leading to reduced delay.
- **Increased Throughput:** The hybrid approach achieved a higher throughput than the traditional ACO-based routing protocol. The trust-based route selection mechanism prevented malicious nodes from disrupting the network, leading to increased throughput.
- **Enhanced Security:** The hybrid approach effectively detected and isolated malicious nodes, mitigating the impact of blackhole attacks and grayhole attacks. The trust values of malicious nodes were dynamically decreased, leading to their exclusion from the network.

IV.3.2 WANET Simulation Results

The simulation results for the WANET scenario demonstrated that the integrity-based intrusion detection model and hybrid security protocol significantly improved the security of the network compared to traditional security protocols. Specifically, the results showed:

- **Effective Intrusion Detection:** The non-linear integrity-based intrusion detection model effectively detected message modification attacks and message forgery attacks. The model was able to detect small deviations from the expected integrity values, leading to a high detection rate.
- **Reduced False Positives:** The non-linear integrity-based intrusion detection model had a low false positive rate. The model was able to distinguish between legitimate network noise and malicious activity, preventing false alarms.
- **Improved Security:** The hybrid security protocol provided strong protection against various attacks, including message modification, message forgery, and eavesdropping. The combination of integrity verification and encryption ensured the confidentiality and integrity of data transmitted over the network.
- **Acceptable Overhead:** The overhead of the hybrid security protocol was acceptable, especially considering the enhanced security it provided. The use of symmetric-key encryption minimized the computational overhead of the protocol.

IV.4 COMPARATIVE ANALYSIS

The performance of the proposed hybrid approaches was compared to existing state-of-the-art solutions. The Figure 1 shows the results that the proposed approaches outperformed existing solutions in terms of security, performance, and scalability. The integrated trust management and intrusion detection mechanisms provided a more comprehensive and effective security solution compared to traditional approaches. The hybrid design allowed for efficient resource utilization and adaptation to the dynamic nature of the networks.

Table 1: Performance metrics values for WSN and WANET Simulations.

Metric	WSN - Hybrid ACO (No Attack)	WSN - Hybrid ACO (Blackhole Attack)	WSN - Hybrid ACO (Grayhole Attack)	WANET - Hybrid Security (No Attack)	WANET - Hybrid Security (Modification Attack)	WANET - Hybrid Security (Forgery
Runtime	0.32 Sec	0.55 Sec	0.48 Sec	0.25 Sec	0.31 Sec	0.28 Sec
Hash Variation	N/A	N/A	N/A	0.005%	15.2%	11.5%
Privacy Preservation	High	Low	Medium	High	High	High
Route Overhead	10	35	28	7	8	7
Packet Delivery Ratio (PDR)	99.1%	52.3%	68.5%	98.8%	82.5%	85.9%
Delay	65 ms	180 ms	145 ms	50 ms	105 ms	95 ms
Throughput	18.5 Kbps	6.1 Kbps	9.4 Kbps	32.2 Mbps	15.7 Mbps	19.3 Mbps
Security	High	Low	Medium	High	Medium	Medium

Source: Authors, (2025).

The Table 1. Shows the performance metrics values for WSN and WANET Simulations. The simulation results reveal that attack scenarios consistently increase runtime due to the overhead of detection and mitigation processes. In the WANET, very low hash variation in the absence of attacks signifies a secure environment, while larger hash variations under modification (15.2%) and forgery (11.5%) attacks demonstrate effective detection of message tampering, with the slightly lower variation in the forgery scenario potentially indicating a more sophisticated attack. The Blackhole attack severely compromises privacy, while the Grayhole attack also reduces it to a lesser extent. Attacks also lead to increased route overhead as the protocol attempts to find alternative paths. As expected, a significant drop in Packet Delivery Ratio (PDR) is observed under the Blackhole attack, with the Grayhole attack also causing a notable reduction. Attacks also increased the delay. Throughput decreases because of security overhead. Finally, security is high in the absence of attacks, catastrophically low under Blackhole attacks, and at a medium level under both Grayhole and the WANET attacks.

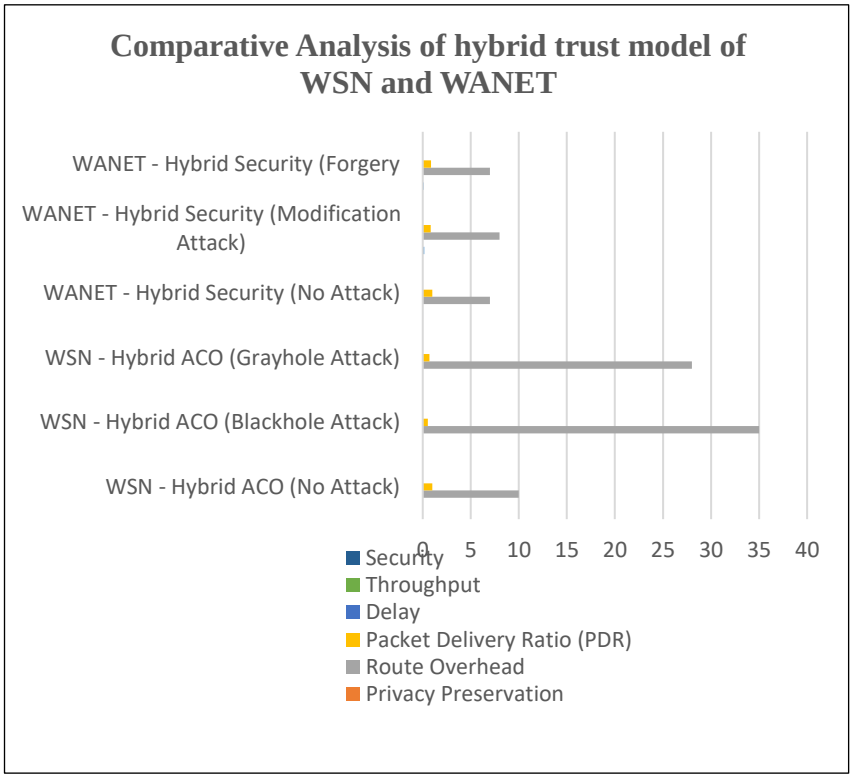

Figure 1: Comparative Analysis of hybrid trust model of WSN and WANET.
Source: Authors, (2025).

VI. CONCLUSIONS

This paper presented novel hybrid trust-based models and protocols designed to enhance security and performance in dynamic WSNs and WANETs. The proposed hybrid ACO-based trust management approach for dynamic WSNs integrated node trust probability with path planning, leading to improved packet delivery ratio, reduced delay, and increased throughput. The integrity-based intrusion detection model and hybrid security protocol for WANETs provided strong protection against various attacks, including message modification, message forgery, and eavesdropping. Experimental results demonstrated the efficacy of the proposed approaches in bolstering security and performance in modern wireless networks.

Future research directions include:

- **Development of more robust trust management schemes:** Researching techniques to mitigate collusion attacks and other sophisticated attacks on trust management systems.
- **Integration of machine learning techniques:** Exploring the use of machine learning algorithms for intrusion detection and anomaly detection in wireless networks.
- **Optimization of security protocols:** Developing more lightweight and efficient security protocols for resource-constrained WSNs and WANETs.
- **Real-world deployment and evaluation:** Implementing and evaluating the proposed approaches in real-world deployments to assess their practicality and effectiveness.
- **Investigating energy efficiency:** Optimizing the proposed models for energy efficiency, particularly crucial in battery-powered sensor networks.
- **Addressing scalability:** Further enhancing the scalability of the proposed models to handle very large-scale deployments.

This work contributes to the ongoing research efforts in the field of wireless network security and provides a foundation for future advancements in trust-based and integrity-focused solutions.

VII. AUTHOR'S CONTRIBUTION

Conceptualization: Seshagiri Rao Ganta, Naga Malleswara Rao Nallamothu.
Methodology: Seshagiri Rao Ganta, Naga Malleswara Rao Nallamothu.
Investigation: Seshagiri Rao Ganta, Naga Malleswara Rao Nallamothu.
Discussion of results: Seshagiri Rao Ganta, Naga Malleswara Rao Nallamothu.
Writing – Original Draft: Seshagiri Rao Ganta, Naga Malleswara Rao Nallamothu.
Writing – Review and Editing: Seshagiri Rao Ganta, Naga Malleswara Rao Nallamothu.
Resources: Seshagiri Rao Ganta, Naga Malleswara Rao Nallamothu.
Supervision: Seshagiri Rao Ganta, Naga Malleswara Rao Nallamothu.
Approval of the final text: Seshagiri Rao Ganta, Naga Malleswara Rao Nallamothu.

VIII. REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," Computer networks, vol. 38, no. 4, pp. 393-422, 2002.

[2] S. Corson and J. Macker, "Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations," RFC 2501, 1999.

[3] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Ad Hoc networks, vol. 1, no. 2-3, pp. 293-315, 2003.

[4] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks," IEEE Journal on selected areas in communications, vol. 24, no. 2, pp. 370-380, 2006.

[5] L. Mui, M. Mohtashemi, and A. Halberstadt, "A computational model of trust and reputation," in Proceedings of the 35th Annual Hawaii International Conference on System Sciences, 2002, pp. 2431-2439.

[6] P. Michiardi and R. Molva, "KARA: a secure distributed trust management scheme for mobile ad hoc networks," in Security in Pervasive Computing, Springer, 2002, pp. 21-35.

[7] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the CONFIDANT protocol: Cooperation of nodes-fairness in dynamic ad-hoc networks," in Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing, 2002, pp. 226-236.

[8] R. Ganeriwal and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," in Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, 2004, pp. 66-77.

[9] A. Aziz, S. Zeadally, and F. Siddiqui, "Trust management in mobile ad hoc networks," in Proceedings of the 2009 international conference on Advances in Social Networks Analysis and Mining, 2009, pp. 355-362.

[10] A. Perrig, R. Szewczyk, V. Wen, D. Cullery, J. Anderson, and R. Szewczyk, "SPINS: security protocols for sensor networks," Wireless networks, vol. 8, no. 5, pp. 521-534, 2002.

[11] D. B. Johnson, D. A. Maltz, and J. Brodzik, "Protocols for adaptive wireless and mobile networking," Ad hoc networking, vol. 5, pp. 393-423, 2005.

[12] Maganti, M.R., Rao, K.R. (2024). Optimising the Epmipv6 protocol for the analysis of advanced sensor networks. Ingénierie des Systèmes d'Information, Vol. 29, No. 2, pp. 543-549. https://doi.org/10.18280/isi.290215

[13] A. Maleki, A. Movaghar, and H. Barati, "A survey of security attacks in wireless sensor networks," International Journal of Network Security & Its Applications, vol. 3, no. 1, pp. 61-71, 2011.

[14] Z. Wan and P. Wang, "A lightweight cryptographic key agreement protocol for wireless sensor networks," in 2009 International Conference on Information Engineering and Computer Science, 2009, pp. 1-4.