Ingénierie des Systèmes d'Information
Vol. 30, No. 1, January, 2025, pp. 83-100
Journal homepage: http://iieta.org/journals/isi

Optimal Wireless Sensor Network Ant-Lifetime Routing Algorithm Using Multi-Phase Pheromone

Sinduja Mysore Siddaramu[1*], Rekha Kanathur Ramaswamy[2]

[1] Department of Electronics and Communication Engineering, Visvesvaraya Technological University, Belagavim 590018, India
[2] Department of Electronics and Communication Engineering, SJB Institute of Technology, Bengaluru 560060, India

Corresponding Author Email: krrekha@sjbit.edu.in

https://doi.org/10.18280/isi.300108

Received: 2 February 2024
Revised: 21 August 2024
Accepted: 8 January 2025
Available online: 25 January 2025

Keywords:
Wireless Sensor Networks (WSN), Ant-Colony Optimization (ACO) algorithm, ant-colony optimisation router chips (ACORC), traditional ant-colony optimisation algorithms (TACOP), trusted secure routing algorithm

ABSTRACT

The research introduces a Pheromone-based Ant Trusted Routing Algorithm (PATRA), aimed at improving routing efficiency and security in Wireless Sensor Networks (WSN). The approach will combine Ant-Colony Optimization (ACO) with reputation-based mechanisms to ensure trusted data delivery through the selection of more trustworthy and energy-efficient nodes. Packet Delivery Ratio (PDR), Energy Consumption, Packet Loss Rate, and the number of received packets are considered for the performance metrics that are observed through extensive simulations with a range of environments, including the possibility of malicious nodes. The results indicate that PATRA consistently outperforms conventional approaches like Quality of Service - Particle Swarm Optimization (QOS-PSO), Ant Colony Optimization Routing Control (ACORC), and Trust-Aware Node Activity Routing Protocol (TANARP) by maintaining a high PDR, reduced energy consumption, and lower packet loss rates with a maximization of received packets. These further demonstrate that PATRA possesses robustness regarding the impact of malicious nodes and network lifetime. The simulation experiments also confirm that the proposed approach outperforms the previous approaches by a large margin in security, efficiency, and reliability, and is thus a promising approach to be employed for secure and energy-efficient WSNs.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) face significant challenges in network routing due to the large number of devices involved, unpredictable and unstable connections, and their deployment in physically unsecured environments. This makes security a key concern. The Pheromone Ant Secure Routing Algorithm addresses these issues by leveraging principles from Ant Colony Optimization (ACO), specifically designed for WSNs with a focus on security. In this approach, "ant" agents (small control packets) are used to discover and select optimal paths throughout the network. Additionally, the Pheromone-Based Lifetime Routing Algorithm (PATRA) is introduced, aiming to enhance energy efficiency through optimized routing, improve network resilience in dynamic conditions, and ensure high data integrity for secure communication [1].

WSNs often struggle with balancing energy consumption, adaptability, and security due to their dynamic and resource-constrained environments. Existing approaches have typically fallen short in addressing these challenges effectively [2]. This gap led to the development of PATRA, which offers a more comprehensive solution by optimizing energy efficiency, adaptability, and security in routing [3].

Ensuring routing security in WSNs is crucial for maintaining the integrity and confidentiality of data, which is vital for their use in various applications such as monitoring of the environment, healthcare, defense, and many more. This study highlights the importance of advancing routing security measures to improve the practicality and reliability of WSNs in real-world deployments [4].

Figure 1 illustrates the basic structure of ant colony routing. However, when applying this approach to WSNs, certain security and efficiency concerns must be addressed:

- **Resource Efficiency**: Nodes within WSNs are often constrained by limited power, memory, and computational capabilities. Therefore, the routing algorithm should be lightweight, reducing the number and size of control packets as well as minimizing the computational load on each node.
- **Dynamic Adaptability**: WSNs are prone to rapid and unpredictable changes due to environmental factors, node mobility, or nodes joining and leaving the network. As a result, the algorithm must be capable of adapting to these changes swiftly to maintain reliable and continuous service.
- **Security Considerations**: Due to the open nature of wireless communication, WSNs are vulnerable to a range of attacks, including eavesdropping, replay attacks, man-in-the-middle attacks, and even physical tampering with the nodes. A secure routing algorithm must take these risks into account by safeguarding the confidentiality and integrity of both the

control packets and pheromone tables. Additionally, it should authenticate node communications, detect, and defend against malicious entities that attempt to misroute data or compromise the network's routing infrastructure [5].

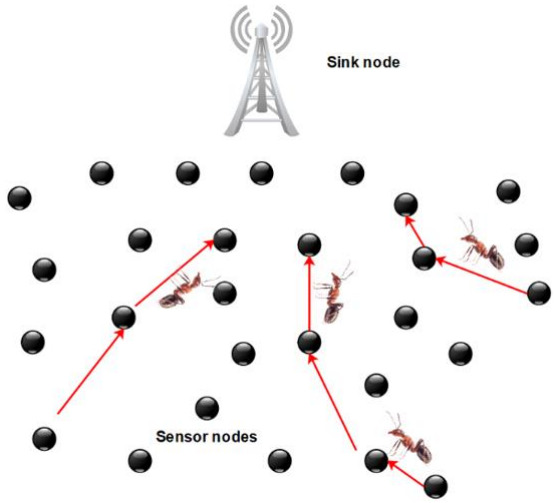

Figure 1. Fundamental structure of ant colony-lifetime routing

1.1 The algorithm for WSN Pheromone Ant Secure Routing

Designing a secure and efficient routing algorithm for WSNs based on ant pheromone trail concepts involves multiple phases [6]. Below is a simplified version of how a Pheromone Ant Secure Routing Algorithm could be structured specifically for WSNs, keeping in mind the unique challenges of network topology, node capacity, and security requirements:

- **Data Encryption**: To ensure the confidentiality of control messages, encrypting the data packets traveling through the network is essential. This ensures that even if packets are intercepted, the information, such as pheromone values or destination addresses, remains secure and inaccessible to unauthorized parties [7].
- **Node Authentication**: Verifying that the participating nodes are legitimate members of the network is crucial. Cryptographic techniques, such as digital signatures or MAC codes, can be employed to authenticate the 'ant' packets and pheromone updates, ensuring they come from trusted sources [8].
- **Resilience to Attacks**: The algorithm should be capable of maintaining its integrity in the face of attacks. It should incorporate mechanisms to detect and counteract false routing information introduced by malicious nodes, preventing the propagation of such data and safeguarding legitimate routing paths [9].
- **Route Diversity**: To mitigate the risk of relying on specific nodes or paths (which could become security vulnerabilities), the algorithm could diversify the routes used for different packets. This strategy would maintain multiple viable routes, ensuring continued operation even if some routes are less efficient or compromised [10].

Developing such a system requires balancing security and efficiency, ensuring that the added computational and communication overhead for security features does not exceed the resource constraints of WSN nodes. Additionally, robust testing and adaptation are essential, as different WSN deployment environments and threat models will demand unique adjustments and optimizations [11].

1.2 Research of the Pheromone Ant Secure Routing Algorithm in WSN

The Pheromone Ant Secure Routing Algorithm, inspired by ant colony behavior and adapted for network routing, particularly in WSNs, represents a unique fusion of biological principles with technological applications. However, as with many innovative methods, there are several research gaps and challenges that need to be addressed. Overcoming these gaps is essential to improve the reliability, efficiency, and security of the algorithm in real-world scenarios. Exploring these areas further can lead to significant advancements in the practical deployment and effectiveness of such algorithms in WSNs and similar networks [12].

1.2.1 Efficiency in large-scale networks

Efficiency in large-scale networks is a significant concern, particularly when using complex algorithms like the Pheromone Ant Secure Routing Algorithm in environments such as WSNs. As network size increases, several challenges and efficiency issues arise that demand innovative research and optimization solutions.

- **Gap**: Ant-based routing generates significant overhead due to the continuous transmission of ant packets for route discovery and maintenance. As the network scale expands, this complexity and resource consumption grow exponentially.
- **Research Opportunity:** Developing methods to enhance the scalability and efficiency of the algorithm in large-scale WSNs while maintaining route optimality and ensuring security features remain intact.

1.2.2 Security against sophisticated attacks

Ant-based routing algorithms, especially within WSNs, encounter significant security challenges. Despite their dynamic and adaptive nature, these algorithms are vulnerable to various advanced attacks. Addressing these security concerns is critical to ensure reliable and secure communication in WSNs [13].

- **Gap**: Although these algorithms implement basic security measures, they remain susceptible to sophisticated attacks, such as advanced man-in-the-middle attacks, Sybil attacks, or coordinated intrusions by malicious nodes.
- **Research Opportunity**: Developing advanced intrusion detection systems specifically designed for ant-based routing protocols, as well as improving the algorithm's resilience against a broader spectrum of security threats [14].

1.2.3 Real-time operation and dynamic adaptation

Real-time operation and dynamic adaptation are crucial in routing protocols, particularly in ant-based routing for WSNs, to ensure efficient and continuous service. These networks experience frequent changes in node availability, topology, and environmental conditions, making it essential for routing protocols to adapt swiftly to maintain optimal performance.

- **Gap**: The highly dynamic nature of WSNs, where nodes can frequently change status or new security threats can arise, presents a challenge for ant-based algorithms, which may not adapt rapidly enough to sustain optimal performance.
- **Research Opportunity**: Exploring real-time adaptation techniques and predictive adjustments that respond to network behavior trends or changing environmental conditions to enhance the algorithm’s responsiveness and effectiveness [15].

1.2.4 Energy efficiency

Energy efficiency is crucial in WSNs due to the constrained power resources of sensor nodes, often deployed in remote locations where battery replacement or recharging is difficult. In ant-based routing, various factors contribute to energy consumption, and optimizing these factors is essential for extending the network's operational lifespan [16].

- **Gap**: WSN nodes typically have limited power supplies, and the frequent transmission and processing of ant packets can deplete these resources rapidly.
- **Research Opportunity**: Improving the energy efficiency of ant routing protocols by introducing adaptive control mechanisms for ant packet transmission rates, potentially based on the nodes' current energy levels or operational priorities, to conserve energy and extend network longevity [17].

1.2.5 Integration with existing technologies

Integrating ant-based routing protocols with existing technologies in WSNs is crucial for their practical applicability and efficiency. This integration poses challenges due to the unique characteristics of WSNs and the existing technological frameworks, yet it presents exciting research opportunities [18].

- **Gap**: Many WSNs operate in environments that involve multiple protocols and technologies, creating uncertainty about how well ant-based routing algorithms can be integrated with these systems.
- **Research Opportunity**: Investigating hybrid approaches that combine ant-based routing with other protocols to harness the strengths of various systems, and analyzing the compatibility issues that emerge during such integrations to enhance overall network performance and adaptability.

1.2.6 Quantitative performance assessment

Quantitative performance assessment is essential for evaluating the effectiveness, efficiency, and practical viability of ant-based routing protocols in WSNs. This involves systematically measuring performance against various quantitative metrics that align with the specific objectives and limitations of WSNs.

- **Gap**: A comprehensive quantitative evaluation comparing ant-based routing protocols with conventional methods across diverse performance metrics and network conditions is often lacking.
- **Research Opportunity**: Conducting extensive simulations and real-world testing to analyze the performance impacts and trade-offs of ant-based routing protocols, offering clearer insights into when and how these algorithms should be optimally utilized in different network scenarios [19].

1.2.7 Robustness in diverse environments

The robustness of ant-based routing protocols in various deployment scenarios of WSNs is vital, given the diversity of environments—from industrial settings and urban areas to remote, harsh conditions. A routing protocol's ability to maintain performance across these varied conditions is a strong indicator of its reliability [20].

- **Gap**: WSNs are deployed in environments with differing characteristics and challenges, such as varying levels of electromagnetic interference, physical obstacles, or extreme weather conditions.
- **Research Opportunity**: Conducting tests and refining ant-based routing algorithms in a wide range of environmental conditions, while developing adaptive mechanisms that automatically adjust algorithm parameters to ensure optimal performance in diverse scenarios.

Addressing these research gaps can significantly improve the robustness and reliability of ant-based secure routing systems. WSNs, with their nodes collecting and transmitting environmental data to a sink node or control center, are widely used in fields such as environmental monitoring, healthcare, and military applications. However, due to their particular operating conditions, WSNs are susceptible to attacks like wormhole, Sybil, and selective forwarding [21].

Consequently, the WSN routing algorithm's security and reliability must be rigorously studied. Many existing routing algorithms focus on resource constraints, such as energy efficiency and network lifespan, with less attention paid to security. These algorithms often leave networks vulnerable to attacks by malicious nodes. Mitigating the harmful effects of these malicious nodes and their behavior can strengthen routing security. While encryption, key management, and authentication help, they cannot fully protect against internal malicious nodes [22].

Trust-based security mechanisms, which establish trust or reputation scores among network nodes, can help address these internal threats. Unfortunately, reputation-based routing in WSNs has not been widely studied. Most WSN routing algorithms prioritize data transmission efficiency, energy consumption, transmission delay, and network security within resource constraints. Figure 2 represents the functional flowchart of reputation and trust in WSNs.

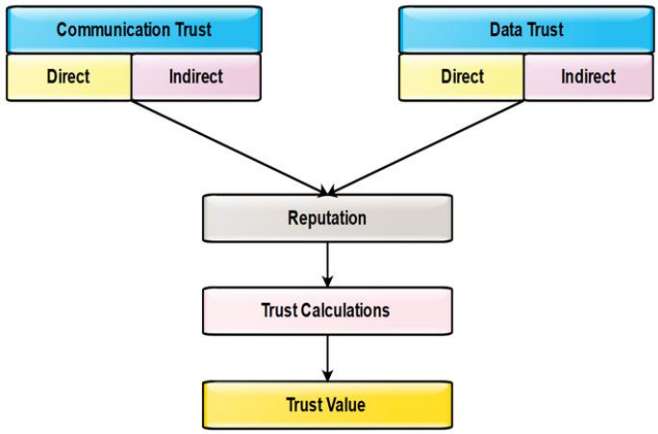

Figure 2. Functional flow chart of reputation and trust in WSNs

Various routing methods, such as data-centric, location-based, and hierarchical routing, have been studied extensively. For example, Abhay et al. [23] improved WSN routing protocols using a combination of ACO and fuzzy inference systems to assess route quality and energy efficiency. The directed diffusion protocol, coupled with fuzzy logic, enhanced energy efficiency. However, ACO offers superior automatic route correction, which is more effective than fuzzy systems that rely on trial-and-error calibration. Zhu et al. [24] developed an energy-efficient WSN routing algorithm using the Harmony Search (HS) meta-heuristic, which excels in global search with minimal parameterization. While HS-based routing addresses energy efficiency, it neglects security. Like other methods, it remains vulnerable to attacks from malicious nodes that can disrupt routing when security is compromised [25, 26].

Mahendra et al. [27] introduced a Distributed Energy-Balanced Uneven Clustering (DEBUC) routing protocol for WSNs, which uses inter-cluster multi-hop routing and uneven clustering to balance energy consumption. By creating clusters of varying sizes, energy usage among cluster heads is optimized by adjusting cluster nodes based on relay load, ensuring that all cluster heads deplete energy evenly. DEBUC employs time-based competitive clustering to divide nodes into smaller clusters at the proximity of the base station, but it does not address event-based networks where environmental factors affect data production. Xu et al. [28] have presented the Trust Energy-Efficient Routing Protocol (TERP), designed to enhance both trustworthiness and energy efficiency in WSNs. Inspired by the Destination-Sequenced Distance-Vector (DSDV) protocol, TERP builds on the Bellman-Ford algorithm by preventing routing loops using sequence numbers. TERP improves network performance by increasing data flow and extending node lifespans, ensuring more secure data transmission between nodes.

Zhu et al. [29] optimized WSN routing through an ant-colony-based approach, focusing on energy constraints and real-time performance. They introduced direction-based pheromones to guide ant colonies toward nodes, addressing network energy limits. However, the study does not prioritize security in routing protocols. Sun et al. [30] developed CRT2FLACO, a protocol on clustering routing which combines ACO with fuzzy logic to balance load and extend network lifespan. By evaluating residual energy, nearby nodes, and base station distance, the protocol efficiently saves transmission energy. While CRT2FLACO enhances energy savings and load balancing, its empirical rules and lack of focus on communication security pose limitations. This research introduces the Multi-Attribute Pheromone Ant Secure Routing Algorithm (MPASR), which addresses security and energy challenges in WSNs by incorporating node reputation values. Combining residual node energy, transmission latency, and reputation scores, this method enhances network security, resilience, and longevity. Reputation values are calculated using direct and indirect credit values, and nodes with high coincidence rates are excluded to minimize computation. This strengthens the network's defense against internal threats while improving communication quality and security. The paper proposes an improved ACO method, integrating node reputation, residual energy, and delay in transmission to balance security and energy consumption, preventing node failure. The article provides an introduction to trustworthy routing algorithms, presents MPASR for secure routing in WSNs, and concludes with the analysis of simulation experiment findings.

2. RELATED WORK

Sharma et al. [31] reviewed various clustering methodologies that have been so far proposed in WSNs, focusing on uneven clustering in order to address the hot-spot problems arising due to non-uniform power consumption by the nodes. In this work, different clustering algorithms have been studied for energy efficiency, load balancing among cluster heads, and prolonging network lifetime. It deals with the novelty of rigorous analysis of uneven clustering properties and algorithms that achieve significant improvement in the reliability and communication range. The negative aspect is that the methods used in uneven clustering can result in complexities within cluster formation and its maintenance, which might increase the computational overhead. Dubey et al. [32] presented a hybrid algorithm, PPO-ACO, which selects the optimal path in IoT-based WSNs integrated with 5G technology. The innovation of PPO and ACO combines reinforcement learning with swarm intelligence in order to improve energy efficiency, security, and address the stochastic nature of the network. In this way, the proposed approach provides better performance on node activeness and energy consumption compared to other techniques. The major drawback of this integration includes computational complexity that might influence the performance in real-time when PPO integrates ACO for large-scale networks. Kumar and Thomas [33] proposed an efficient MASP data gathering scheme that helps in enhancing the energy efficiency of network lifetime by utilizing a mobile sink(s) in WSN. It contributes to novelty by using an improved ACO and integer linear programming on data collection path incorporation with residual energy, channel noise, and delay. On the improvement of this technique, more energy will be saved and the higher throughput is achieved that also gets affirmed from NS2 simulations. However, its sink node mobility is bounded and hence less scalable or adaptive upon handling dynamic network scenarios. Alqarni et al. [34] proposed a routing strategy using discrete differential evolution and ant colony optimization in order to address energy consumption and routing delay issues in WSNs. In this, the authors made a worthy contribution to a formal model for optimizing cluster head selection and proposed a mobile sink-based routing algorithm to balance the load in order to extend the lifetime of the network. The experimental results reflect that the considerable network lifetime of 54%, reduction of transmission delay of 63%, and energy consumption of 47% have a trade-off in implementation complexity with discrete differential evolution coupled with ACO and, therefore, more computational overhead. Kumar et al. [35] proposed the hybrid Whale-Ant Optimization Algorithm, WAOA, for achieving energy-efficient routing in WSNs. The novelty is the selection of the cluster head by Whale Optimization Algorithm and the usage of Ant Colony Optimization for finding the optimal routing. This algorithm demonstrates very good performance when compared with the state-of-the-art methods and outperforms them, improving both network lifetime and energy efficiency. A drawback is that the hybrid approach may increase algorithmic complexity, making it challenging to implement in resource-constrained environments.

El Khediri et al. [36] propose a hybrid ABC and ACO-based clustering and routing approach for improving the energy efficiency in WSNs. The novelty of the idea is considering residual energy, distance, and node centrality for CH election and path optimization through ACO. This technique has proved to have a highly increased network lifetime and energy consumption compared to the conventional clustering protocols. However, it requires many optimization parameters, which can be difficult to tune and implement. In this paper, Sachithanandam et al. [37] present a Deep Reinforcement Learning-Enhanced Hybrid African Vulture and Aquila Optimizer for dynamic clustering and energy management in WSNs. This paper provides two novelties, where firstly, it couples global and local search capabilities of the African Vulture and Aquila Optimizers, respectively. Next, real-time adaptation uses deep reinforcement learning. Results will be an energy-efficient one for about 20% higher without complex integration of these sorts of advanced optimization techniques.

Deploying these will also be a complex task in real and practical terms. Wang et al. [38] proposed an improved ACO algorithm for node energy consumption optimization in WSNs. They have introduced a pseudo-random proportional rule with the purpose of enhancing state transitions in order to avoid algorithm stagnation. Much improvement was realized in choosing optimal paths with shorter length and high energy, hence resulting in a 52% increment of the search speed. However, a drawback is the potential trade-off between achieving energy efficiency and handling dynamic topology changes effectively. Ketshabetswe et al. [39] proposed the BACREED algorithm, a hybrid of ACO and CS, for energy-efficient routing in WSNs. The novelty is the integration of FELACS with CS for data compression and optimization of routing. Simulation results prove its superiority in energy efficiency and reduction of path length compared to existing methods. One disadvantage of this could be the sensitivity to parameter tuning that this algorithm might have in its adaptability on various configurations of the network.

3. ANT COLONY OPTIMISATION (ACO)

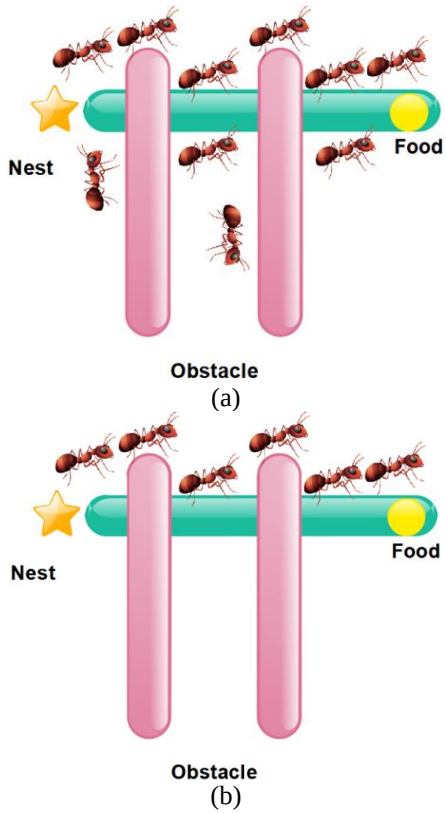

Figure 3. (a) Path selection initialization; (b) The ants finding the shortest path

Ant Colony Optimization (ACO) leverages the foraging behavior of ants as a metaheuristic to solve combinatorial optimization problems. In ACO, algorithms mimic the behavior of real ants. As illustrated in Figure 3, ants deposit pheromone trails while searching for food, which other ants can detect and follow back to their colony. These pheromones guide the ants to the most efficient route between the nest and the food source. Over time, the ants collectively discover the shortest path [40]. Figure 3(a) shows the initial state where ants are randomly exploring different paths. Figure 3(b) depicts the final state, where the ants have established and are following the optimal, shortest path based on the pheromone trails. This process illustrates how ACO algorithms evolve and optimize solutions by using pheromone-based feedback, just as ants refine their foraging paths.

ACO was initially applied to solve the Travelling Salesman Problem (TSP). In the TSP, the objective is to find the shortest possible route that visits each city exactly once and returns to the starting city. The ACO approach for solving the TSP uses multiple ants to explore potential routes among N cities. The next city that each ant visits is determined by a combination of the distance between cities and the intensity of the pheromone trail [41].

3.1 Dynamic path selection

Dynamic path selection introduces a probabilistic approach driven by historical and dynamic factors, ensuring a more adaptive decision-making process [42]. The probability of ant k choosing path $i \to j$ is redefined as given in Eq. (1).

$$S_{ij}^{k}(\tau) = \frac{\sigma_{ij}(\tau) \cdot \xi_{ij}}{\sum_{p \in \text{nodes}_k} \sigma_{ip}(\tau) \cdot \xi_{ip}} \tag{1}$$

where, $S_{ij}^{k}(\tau)$: Selection probability for node j from node i by ant k at time τ, $\sigma_{ij}(\tau)$: Adaptation factor, representing the cumulative influence of historical pheromones and dynamic weights, ξ_{ij}: Priority score based on node-specific metrics (e.g., energy, distance, or reliability) and nodes_k: The set of all nodes accessible from i for ant k.

3.2 Reinforcement and decay

Reinforcement and Decay Allows for the gradual forgetting of outdated paths while reinforcing effective ones [43]. The dynamic update rule for the adaptation factor $\sigma_{ij}(\tau)$ is expressed as Eq. (2).

$$\sigma_{ij}(\tau + 1) = \sigma_{ij}(\tau) \cdot e^{-\alpha} + \omega \cdot \Psi_{ij}^{k}(\tau) \tag{2}$$

where, $e^{-\alpha}$Exponential decay to reduce the weight of older information, ω Reinforcement constant, determining the impact of new updates and $\Psi_{ij}^{k}(\tau)$: Success score contributed by ant k for path $i \to j$, based on factors such as energy efficiency and reliability.

3.3 Success score

Success score combines energy, distance, and reliability to provide a holistic evaluation of paths [44]. The success score $\Psi_{ij}^{k}(\tau)$ for a path $i \to j$ is computed as Eq. (3).

$$\Psi_{ij}^{k}(\tau) = \frac{1}{1 + \frac{\text{Dist}_{ij}}{\text{Energy}_j \cdot \text{Reliability}_j}} \tag{3}$$

where, Dist_{ij} Distance between nodes i and j, Energy_jResidual energy of node j and Reliability_j Historical reliability of node j, representing its consistency in forwarding data.

3.4 Pheromone reinforcement

Pheromone reinforcement $\Delta\psi_{ij}(t)$ represents the amount of pheromone deposited on the edge connecting nodes i and j [45]. This value is calculated using Eq. (4).

$$\Delta\psi_{ij}(t) = \frac{1}{1 + W_{ij} \cdot P_j} \tag{4}$$

where, W_{ij} denotes the traffic weight on the edge, and P_j is the priority index of node j. The equation ensures that paths with lower congestion and higher priority receive stronger reinforcement, supporting efficient routing decisions.

3.5 Pheromone update

Pheromone update $\psi_{ij}(t+1)$ determines how pheromone levels on an edge evolve over time [46]. The Eq. (5) is expressed as:

$$\psi_{ij}(t+1) = \psi_{ij}(t) \cdot (1 - \lambda) + \Delta\psi_{ij}(t) \tag{5}$$

where, λ represents the evaporation rate, reducing the influence of outdated pheromone trails. $\Delta\psi_{ij}(t)$ adds the newly deposited pheromone, ensuring that recent successful paths are reinforced. This dynamic update balances exploration and exploitation in the system.

4. REPUTATION-BASED MECHANISMS AND ACO IN WSNS

Figure 4 shows the integrated approach of reputation-based mechanisms with ACO concepts, which play a crucial role in enhancing the efficiency and reliability of the WSN. The sensing field has sensor nodes cooperating in order to sense the environment. Reputation-based mechanisms assign trust scores to sensor nodes in the network based on their previous record of reliability, energy efficiency, and accuracy of data. High-rated reputation nodes are prioritized as routers because of the integrity and high transmission of data while lowering malicious or faulty ones. Reputation-based evaluation is dynamic with the status in view, reinforcing the establishment of trust in reliable nodes to be isolated from those of little dependability [47].

From sensor nodes to the sink node via the data transmission cloud, routing decisions will be made by ACO principles. By drawing inspiration from the method through which ants find the best path, ACO will consider the number of pheromones on different transmission paths according to the energy consumed, distance, and reputation of each node. The paths with higher pheromone levels, which represent efficient and reliable communication, are reinforced, while the others gradually fade away because of evaporation. It ensures that the most optimal and trustworthy routes are continually used for data transmission [48].

The aggregated data in the sink node is sent to the internet management system for processing and storage. ACO-guided routing and reputation scores ensure that only the best-quality data reaches this stage, reducing overhead and increasing the performance of the system. This processed information is accessed by the end-user using internet-enabled devices, based on a secure, efficient, and reliable WSN infrastructure [49].

This work will highlight how the integration of reputation-based mechanisms and ACO works out the optimal solution to build a reliable, secure, and energy-efficient network in application areas like environmental monitoring, industrial automation, and smart city solutions.

4.1 Evaluation of node reputation

Figure 5 depicts a hierarchical architecture for the reputation-based node evaluation and ACO routing of WSN. There exist five layers that can perform the tasks in the light of their specification and will jointly ensure data communication takes place well and with dependability. The top layer consists of the reputation layer which updates the nodal trustworthiness w.r.t performance evaluation about energy efficiency, transmission accuracy, etc., in the earlier rounds. This layer assigns a reputation score to every node, which forms the basis for routing decisions [50].

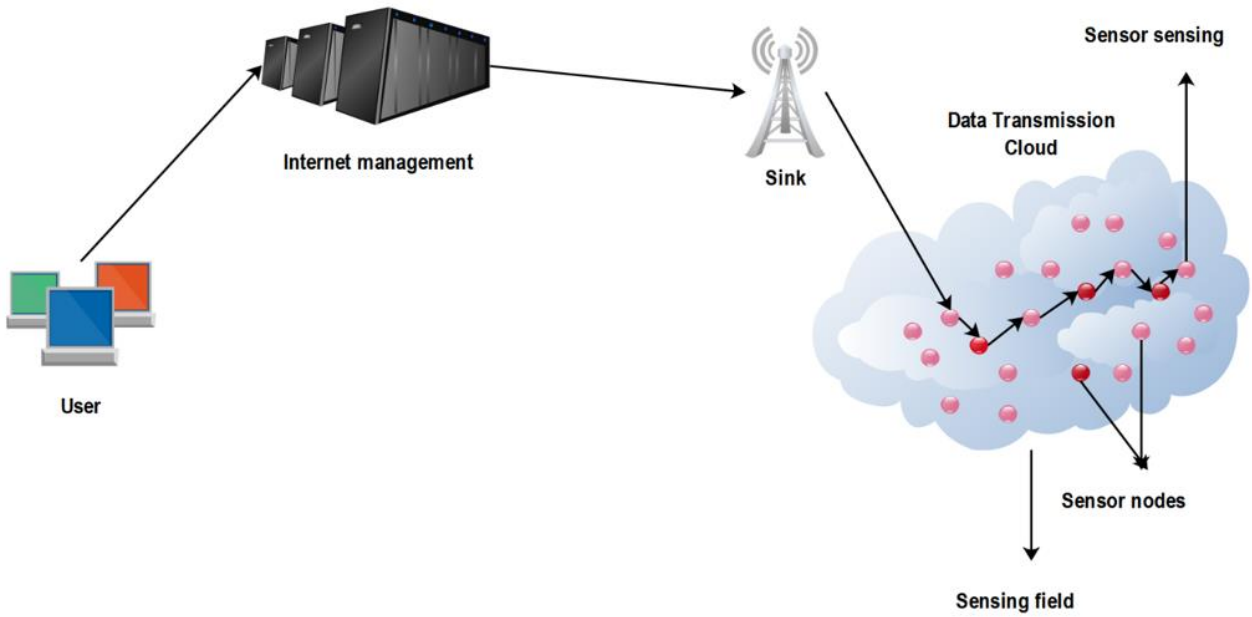

Figure 4. Reputation-based mechanisms and ACO for WSN architecture

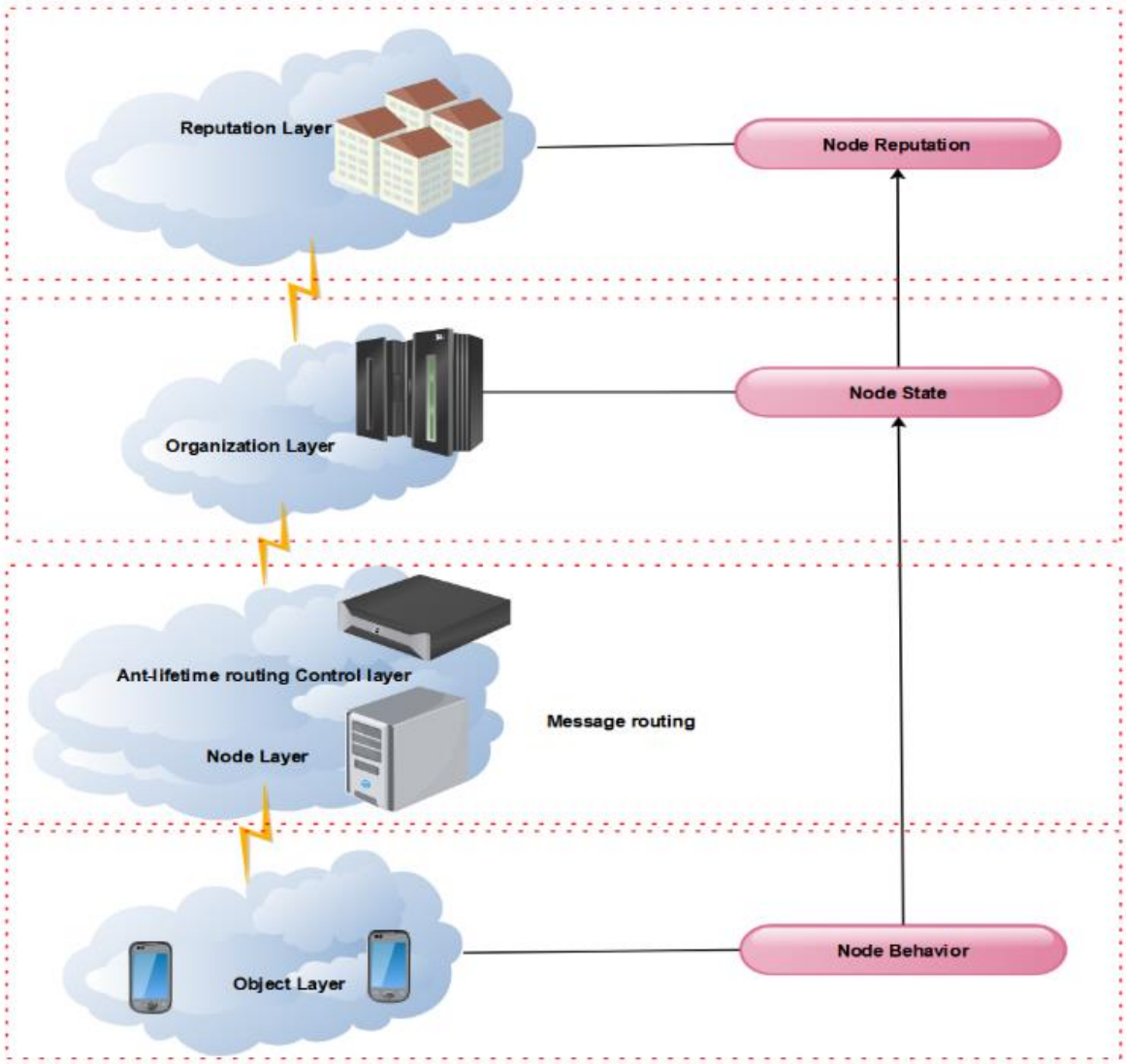

Figure 5. Hierarchical architecture for reputation-based node evaluation and ACO routing

Organization Layer: Essentially monitors the state of the nodes by examining various parameters like the availability of resources, the degree of activities, etc. This is, in fact, a coordination layer for integrating the information of the reputation layer for an informed routing strategy. ACO operates in the ant lifetime routing control layer, performing message routing. It dynamically computes the paths by combining pheromone levels with the reputation score of the nodes, always reinforcing the best routes at the expense of less useful paths that get dropped gradually [51].

The Node Layer provides the actual routing of packets according to optimized routes given by the control layer. This maintains flawless communications among the nodes according to reputation-based routing policies. Finally, the object layer checks the behavior of each node regarding specified mechanisms for routing and reputation, respectively. It is further utilized to allow end-to-end users' interaction with the network. All these layers together provide the basis for efficient, secure, and reliable communication in WSN.

4.2 Node reputation evaluation

Node reputation, R_i can be defined as the level of dependability of node i during transmissions that are successful with priority weight assignment within a certain timeframe derived using Eq. (6).

$$R_i = \frac{\sum_{t=1}^{T} (S_i \cdot P_i)}{T} \tag{6}$$

Here, R_i is the reputation score of nodes i, which gives an idea about the reliability of the node in the network. S_i is the number of successful data transmissions carried out by node i. P_i is the priority weight of node i, which depends on factors like energy and trustworthiness. T is the total time considered for reputation calculation to capture the comprehensive performance of the node [52].

4.3 Node state monitoring

Node state S_i decides the working condition of a node based on analyzing its energy level and congestion factor. The value of it is calculated by the use of Eq. (7).

$$S_i = E_i \cdot \frac{1}{C_i} \tag{7}$$

where, S_i is the state value of node i, reflecting its capability for routing. Further, E_i is the residual energy at node i and C_i is the congestion level at node i, representing its current load.

This will ensure that nodes with more energy and lower congestion have higher probabilities of getting selected for routing, again improving network efficiency [53].

4.4 Message routing optimization

The decision model determines the probability P_{ij} for the choice of node j as a subsequent hop from node i as the combined result of pheromone levels, heuristic factors, and node reputation. Its value is obtained from Eq. (8).

$$P_{ij} = \frac{(\tau_{ij})^{\alpha} \cdot (\eta_{ij})^{\beta} \cdot R_j}{\sum_{k \in \text{neighbors}} (\tau_{ik})^{\alpha} \cdot (\eta_{ik})^{\beta} \cdot R_k} \tag{8}$$

Here, P_{ij} represents the probability of selecting node j as a successor node from node i. τ_{ij} is pheromone level on the route between nodes i and j, η_{ij} may be the heuristic value, most of the time the inverse value of the distance between nodes i and j, and also R_j, which represents node j's reputation score, reflecting its reliability. In addition, α and β are the weighted parameters of the relative importance of the pheromone level and heuristic values, respectively [54].

4.5 Node reputation assessment

It emphasizes the relationship between a node's performance-that is, successful transmissions, its priority weight, and time of observation. It ensures nodes with higher performance and trustworthiness are given better reputations for routing decisions [55]. Each node's reputation R_i can be calculated using the given in Eq. (9).

$$R_i = \frac{S_i \cdot P_i}{T} \tag{9}$$

where, R_i is defined as the Reputation score of nodes i, which signifies its reliability, S_i is given as the number of successful data transmissions by node i, P_i is defined as Priority weight assigned to node i, based on factors such as energy and trustworthiness and T total time duration over which the reputation is evaluated.

The beta distribution is a continuous probability distribution that is defined on the interval [0, 1]. It is a general tool that has been widely used to model random variables representing probabilities, proportions, or uncertainties in Bayesian statistics and other applications [56]. The Beta distribution is parameterized by two shape parameters, α, and β, which determine its shape. The probability density function of the Beta distribution is given by Eq. (10).

$$f(x; \alpha, \beta) = \frac{x^{\alpha-1}(1-x)^{\beta-1}}{B(\alpha, \beta)}, \; 0 < x < 1 \tag{10}$$

where, $\alpha > 0$ is represented as the Shape parameter controlling the behavior near 0, $\beta > 0$ is depicted as Shape parameter controlling the behavior near 1 and $B(\alpha, \beta)$ is identified as the beta function, defined as Eq. (11).

$$B(\alpha, \beta) = \int_0^1 t^{\alpha-1}(1-t)^{\beta-1}\, dt = \frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha+\beta)} \tag{11}$$

where, Γ is the Gamma function.

Figure 6 demonstrates a framework integrating feedback mechanisms and the PATRA (Pheromone-based Ant Trusted Routing Algorithm) reputation model for evaluating node performance in a Wireless Sensor Network (WSN). Nodes, represented as $Node\_1, Node\_2, \ldots, Node\_N$, are connected through servers ($Server\_1$ and $Server\_2$) to facilitate secure communication. Feedback data from these nodes is collected and processed using the feedback collector. This feedback captures communication performance metrics such as successful transmissions, energy utilization, and congestion levels [57].

This feedback captures communication performance metrics such as successful transmissions, energy utilization, and congestion levels. The PATRA model then analyzes this information to assign a reputation score to each node. The assigned reputation score reflects the node's reliability and trustworthiness, which guides routing decisions. This iterative feedback mechanism ensures the dynamic update of local parameters, reinforcing trust in nodes with high performance while penalizing unreliable nodes. By continuously refining node reputation and optimizing routing, this architecture improves WSN security, data integrity, and energy efficiency [58].

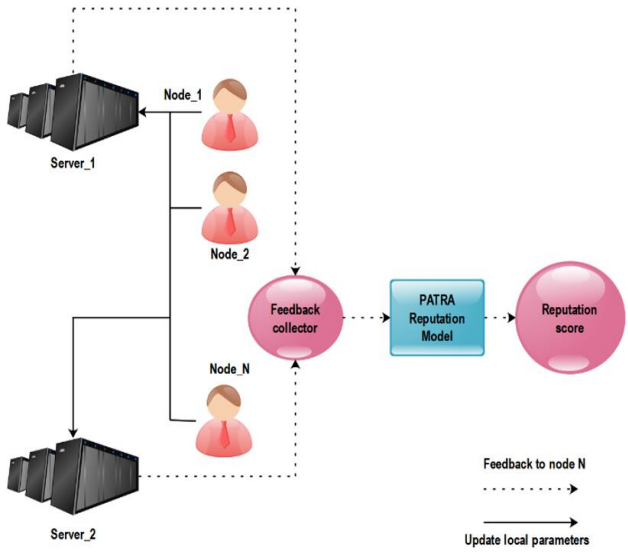

Figure 6. Node reputation assessment framework using PATRA

4.5.1 Indirect value of reputation

In many WSNs, the variable node distributions often generate significant overlaps of sensing ranges among different nodes. Figure 7(a) describes how the entire area of interest is completely enclosed by the three nodes. A fourth node completely overlapping the sensing range in Figure 7(b) would fall into the category of Figure.

Thus, its removal will save the network much energy with little loss of either overall trust or performance. A high number of unnecessary nodes could be removed by ensuring no overlapped coverage for these nodes, saving energy for extending the lifetime of a resource-constrained WSN without losing efficiency. The aim here is to ensure that only those nodes absolutely necessary remain operational for optimized energy and network security [59].

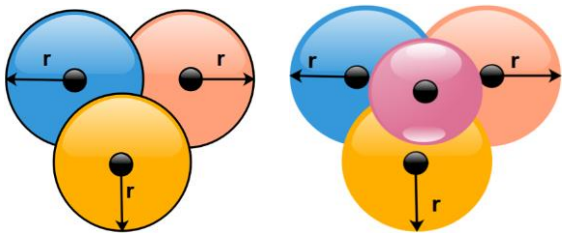

Figure 7. Node overlap coverage analysis (a) Three nodes cover everything; (b) Four nodes cover everything [59]

The node reputation assessment framework discussed here assesses the trustworthiness of nodes in a WSN by feedback mechanisms and the PATRA reputation model. This framework will integrate direct and indirect feedback from nodes to dynamically compute their reputation scores, which are crucial for secure and efficient routing [60]. The reputation score Ri of node i is a weighted combination of its direct feedback (F_i^{direct}) and indirect feedback F_i^{indirect} and it is expressed by the Eq. (12).

$$R_i = \omega_d \cdot F_i^{\text{direct}} + \omega_i \cdot F_i^{\text{indirect}} \tag{12}$$

where, ω_d and ω_i are weight factors for direct and indirect feedback, respectively, such that $\omega_d + \omega_i = 1$. This combination ensures both observed interactions and recommendations from trusted neighbors contribute to the reputation assessment [61, 62].

4.5.2 Direct feedback calculation

Direct feedback evaluates the node's performance based on its immediate interactions. It is defined as given in Eq. (13).

$$F_i^{\text{direct}} = \frac{\alpha_i}{\alpha_i + \beta_i} \tag{13}$$

where, α_i is defined as: the number of successful interactions observed for node i and, β_i described as number of unsuccessful interactions observed for node i. Basically, the ratio that reflects a node's reliability about its share of successful interactions against its total number of interactions. Individuals with a higher number of successes (α_i) are then rewarded with higher direct feedback scores [63].

4.5.3 Indirect feedback calculation

Indirect feedback aggregates opinions from neighboring nodes about the target node i. It is computed as given Eq. (14).

$$F_i^{\text{indirect}} = \frac{\sum_{j \in N_i} w_j \cdot R_j}{\sum_{j \in N_i} w_j} \tag{14}$$

where, N_i is set of neighbouring nodes which give feedback about node i, w_j is a description of the weight assigned to feedback given by node j - normally it will be proportional to $j's$ reputation - and R_j is described by the following. Reputation score of nodes j, in the opinion of its neighbours. In this way, indirect feedback takes care that opinions from more reputable nodes (w_j) will have greater weights and this reduces the impact of untrustworthy nodes [64].

4.5.4 Dynamic updates and adaptation

To make the reputation scores reflect the most recent behavior, the feedback parameters αi and βi are periodically updated by using a weakening factor h and it is determined by the Eq. (15).

$$\alpha_i = h \cdot \alpha_i \text{ and } \beta_i = h \cdot \beta_i \tag{15}$$

where, $0 < h \leq 1$. This decay mechanism weakens the influence of older interactions and emphasizes more recent observations in the reputation assessment process [65].

4.5.5 Joint information entropy

The joint entropy $H(X,Y)$ defines the total uncertainty or information content of the combined random variables X and Y. It determines the weighted sum of the logarithms of the joint probabilities $P(x,y)$ of the outcomes of X and Y. It defined as given in Eq. (16).

$$H(X,Y) = -\sum_{x \in X} \sum_{y \in Y} P(x,y) \cdot \log_2 P(x,y) \tag{16}$$

where, $H(X,Y)$ is the Joint entropy of random variables X and Y, $P(x,y)$ is described the joint probability of outcomes x and y and X,Y is represented the random variables with respective sets of possible outcomes [66].

4.5.6 Node information entropy

The information entropy H (X) gives the uncertainty (information) that is concentrated within a single node: H is computed by the sum over all states X that can take the given node, weighted by the corresponding probability P, and further, by the logarithm of such probability. This provides a measure, among other things, of the amount of randomness or variety within the node's individual sets of observed behavior-simply expressed by Eq. (17).

$$H(X) = -\sum_{x \in X} P(x) \cdot \log_2 P(x) \tag{17}$$

H(X) is considered to be the information entropy of node X, which for a random variable having X representing possible states of the node shows P(x) to be its probability.

4.5.7 Dynamic trust calculation with adaptive uncertainty adjustment

The dynamic trust value of node i for node j, which fuses successful and failed interactions with an uncertainty adjustment factor. The equation innovatively incorporates a scaling coefficient (κ) to adapt the influence of uncertainty based on interaction density, enhancing the reliability and

robustness of trust evaluations in dynamic network environments by using the given Eq. (18).

$$T_{ij} = \frac{\alpha_{ij} + \kappa \cdot \gamma}{\alpha_{ij} + \beta_{ij} + \kappa \cdot (\gamma + 1)} \quad (18)$$

where, T_{ij} is represented as the trust value of node i for node j; it denotes the degree to which j is regarded by i as reliable. Furthermore, α_{ij} denotes the total number of successful interactions that have taken place between node i and node j; β_{ij} is defined as the total number of failures associated with the interactions between node i and node j; γ refers to a baseline uncertainty factor that considers incomplete evidence of interactions; κ, on the other hand, is a dynamic scaling coefficient which defines how much importance needs to be given to uncertainty as characterized by γ with regard to density of interaction or network condition [67].

4.5.8 Updating of communication behaviour

Dynamic updating of communication behavior adaptively updates the trust values of the nodes in a network based on their recent interactions. This ensures that the assessment of trust captures the most recent behavior while it gradually discounts outdated interactions. The updated trust value is computed as given in Eq. (19).

$$T_{ij}^{(t+1)} = \lambda \cdot T_{ij}^{(t)} + (1 - \lambda) \cdot \text{NewInteraction}_{ij} \quad (19)$$

where, $T_{ij}^{(t+1)}$ is the updated trust value of node i for node j at time $t + 1$, $T_{ij}^{(t)}$ is the previous trust value of node i for node j at time t, λ is given by the forgetting factor $(0 < \lambda \leq 1)$, which determines the weight of the past trust when updating. $\text{NewInteraction}_{ij}$is defined by the trust score derived from the newest interaction between nodes i and j, depending on whether it resulted in success or failure [68].

4.5.9 Holistic evaluation of reputation value

A holistic approach in reputation value integrates the following factors: Direct and indirect feedback, uncertainty for calculating the overall reputation score of a node. This would render the assessment balanced and robust to the reliability of a node in the network and it's determined by the Eq. (20).

$$R_i = \omega_d \cdot F_i^{\text{direct}} + \omega_i \cdot F_i^{\text{indirect}} + \omega_u \cdot U_i \quad (20)$$

Ri is the overall description of the holistic reputation score of node i about overall reliability, F_i^{direct} is the representation for the direct feedback score with respect to node i for its interaction, F_i^{indirect} is the description of an indirect feedback score for node i based on recommendations by the neighboring nodes. Ui-described uncertainty factor for node i to model incomplete or insufficient evidence on interaction evidence. $\omega_d, \omega_i, \omega_u$ represented weight coefficients controlling direct feedback, indirect feedback, and uncertainty respectively such that $(\omega_d + \omega_i + \omega_u = 1)$.

4.6 Residual energy

Residual energy is the energy left in a node after its operational and communication activities in a network. It is one of the critical parameters in energy-constrained networks, such as WSNs, where efficient usage of energy is very important for a longer lifetime and reliability of the network, and it is represented by Eq. (21).

$$E_{\text{residual}} = E_{\text{initial}} - \left(E_{\text{transmit}} + E_{\text{receive}} + E_{\text{idle}} + E_{\text{processing}}\right) \quad (21)$$

This, E_{residual}, represents the residual energy of the node. On the other hand, E_{initial} is defined as the energy a node possesses at the time it is deployed; E_{transmit} - energy during transmission of data; E_{receive} - meaning thereby the amount of energy wasted by this particular node due to reception of that packet, while E_{idle} represents energy utilized in idle mode during conditions that have a node neither in transmit nor receive state, $E_{\text{processing}}$ defines energy consumption for data processing or computational work [69].

4.7 Latency in communication

Communication delay is a factor that greatly affects the wireless sensor network routing protocol. Higher delays will have a great impact on network communication. In this study, node distance and communication latency τ_{ij} will be examined. Node communication latency may be represented by physical distance. Although nodes are close, node voltages may be close to the minimum of the sensor. This may greatly minimize node communication. The two nodes are far apart. Thus, here a distance concept is suggested towards a better representation of communications latency given in Eq. (22).

$$\tau_{ij} = \left[\left[\frac{1}{V_0 - V_{min}} * (\omega_{ij})^2\right]^{-1}\right] \quad (22)$$

V_0 is 3 V and matches the wireless sensor network node voltage during system operation. The critical voltage Vmin is commonly 2.7 V. Also, Eq. (23) defines ω_{ij} as the Manhattan metric distance between nodes i and j. The equation above accounts for energy-distance correlation and voltage volatility. The formula quickly adjusts the effective distance between nodes as voltage drops, which is useful. For distance between two objects with P number properties, let i = $(u_{i1}, u_{i2},..., u_{ip})$ and j = $(u_{j1}, u_{j2},..., u_{jp})$. Manhattan, L1, or taxicab distance measures i-j. The total of their absolute coordinate disparities [70-73].

$$\omega(i,j) = \left|u_{i1} - u_{j1}\right| + \cdots \ldots \ldots \ldots \ldots \ldots + |u_{ip} - x_{jp}| \quad (23)$$

4.8 ACO reputation

ACO reputation mechanism integrates the behavioral principles of ants, such as pheromone trails and path optimization, with reputation-based assessments to enhance routing efficiency and reliability in WSNs. The concept leverages the dynamic adjustment of pheromone levels influenced by node reputation, residual energy, and transmission delay, ensuring secure and energy-efficient data transmission [74-76].

4.8.1 Reputation-based pheromone update

The pheromone concentration (ρ_{ij}) of a path between nodes i and j is updated concerning node reputation (μ_{ij}), residual energy (ξ_{ij}), and communication delay τ_{ij} given in Eq. (24).

$$\rho_{ij} = \theta_1 \cdot \mu_{ij} + \theta_2 \cdot \xi_{ij} - \theta_3 \cdot \tau_{ij} \quad (24)$$

where, ρ_{ij} is the concentration of pheromones for determining the attractiveness of the route, μ_{ij} describes a reputation value at node's reliability based on the historic records analyzed previously; ξ_{ij} defines the amount of residual energy at the current instant for enforcing energy-efficient routing, and τ_{ij} denotes communication delay that has to be minimized so as not to allow high-latency paths in the network, and lastly, $\theta_1, \theta_2, \theta_3$ are weight coefficients needed for giving relevance to the corresponding parameters to balance their effects [77-80].

4.9 The specific process of a proposed Pheromone-Based Lifetime Routing Algorithm (PATRA)

To have the optimization of ant colonies and determination of node reputation values, multiple ants must be dispatched along each path to record the information of the node attribute. These pheromone values play an important role in identifying the optimal path. A flowchart showing how this is done is represented in Figure 8, showing the dispatch of the ants to the collection of data regarding the nodes and pheromone update for recording to the determination of the best path.

4.9.1 Algorithm: ACO for reputation-based routing

This Algorithm 1 describes the ACO process for finding the optimal path based on node reputation in a Wireless Sensor Network (WSN).

Step 1: Initialize parameters

- Set the total number of ants (m), maximum iterations ($T_{\max}$), and initialize pheromone levels (ρ_{ij}) for all paths.
- Define weight coefficients ($\theta_1, \theta_2, \theta_3$) for reputation, residual energy, and delay.
- Initialize the ant counter $A = 0$.

Step 2: Increment the ant counter

- Increment A by 1: $A = A + 1$.

Step 3: Check If All Ants Are Processed

- If $A > m$, proceed to Step 8. Otherwise, continue.

Step 4: Choose the next node

- For the current node, evaluate the probability of choosing the next node j using the ACO probabilistic formula as shown in the equation

$$P_{ij} = \frac{(\rho_{ij})^{\alpha} \cdot (\eta_{ij})^{\beta}}{\sum_{k \in \text{neighbors}} (\rho_{ik})^{\alpha} \cdot (\eta_{ik})^{\beta}},$$

where, ρ_{ij}: Pheromone level on the path $i \to j$, η_{ij}: Heuristic value based on node reputation, residual energy, and delay, α, β : Weight parameters for pheromone and heuristic influence.

Step 5: Check target node

- If the selected node is the target, go to Step 6.
- Otherwise, repeat Step 4 for the next node.

Step 6: Modify pheromone levels

- Update pheromone levels on the path using the reputation-based pheromone update formula as shown in the equation

$$\rho_{ij} = (1 - \theta) \cdot \rho_{ij} + \theta \cdot (\theta_1 \cdot \mu_{ij} + \theta_2 \cdot \xi_{ij} - \theta_3 \cdot \tau_{ij}),$$

where, μ_{ij} is the reputation of node j, ξ_{ij} is represented by the residual energy of node j , τ_{ij} is described as the Communication delay to node j and θ is identified as evaporation coefficient.

Step 7: Update Iteration Counter

- Increment the iteration counter: $t = t + 1$.
- If $t > T_{\max}$, proceed to Step 8.
- Otherwise, return to Step 2.

Step 8: Compare and Output Results

- Compare the paths traversed by all ants.
- Select the path with the highest cumulative pheromone level and reputation score as the optimal path.
- Output the results.

End

The algorithm terminates after identifying the optimal path.

Figure 8. The proposed optimal wireless sensor network ant-lifetime routing algorithm using multi-phase pheromone

5. RESULTS AND DISCUSSION

Table 1 lists the key simulation parameters used for evaluating the ACO-based routing framework in WSNs. It includes values such as network size, area dimensions, energy metrics, and protocol configurations necessary for modeling and analyzing the system's performance.

Figure 9 provides a glimpse of nodes scattered around a rectangular area of 100m × 100m, thus showing the randomly deployed pattern of sensor nodes. Each dot represents a sensor node, placed to depict the way nodes are dispersed over the sensing field of interest.

This deployment is to check the network performance on coverage, connectivity, and reliability issues under different configurations. It will help analyze how node placement affects data transmission efficiency and energy utilization key considerations in the design of effective WSNs. The x- and y-axes are set to represent the coordinates within the simulation area; thus, through the coordinate positions of every node, one can further analyze various network behaviors.

Table 1. Simulation parameters for ACO in WSNs

SI. No	Parameter	Value
1	Number of Nodes	100
2	Simulation Area	100m x 100m
3	Transmission Range	100m
4	Initial Energy	1J
5	Packet Size	1024 bytes
6	Data Rate	250 kbps
7	Simulation Time	500 seconds
8	Node Mobility	Random Waypoint
9	Energy Consumption per Transmission	0.01J
10	Routing Protocol	AODV

Table 2. The various redundant nodes with respect to different configuration

Node Coincidence Threshold	5m	10m	20m
1.2	0	0	0
1.57	2.2	2.2	2.2
1.757	2.2	5.3	0
2.5	2.2	14	0
2.75	2.2	18.5	0

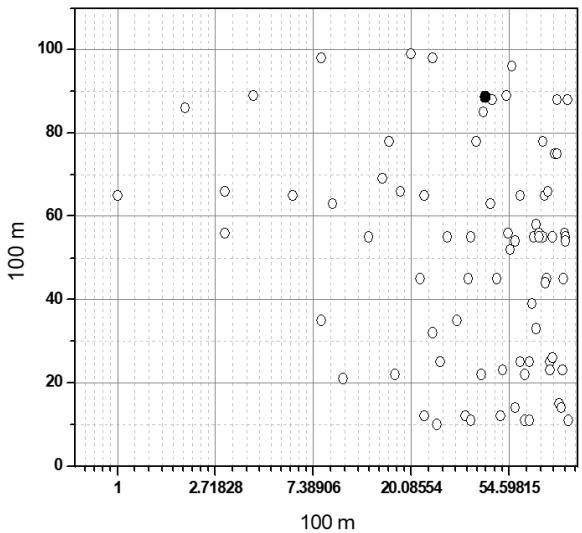

Figure 9. Simulation experiments Wireless Sensor Network node deployment diagram

Table 2 presents the number of redundant nodes under various node coincidence thresholds (5m, 10m, and 20m). It demonstrates how increasing the threshold impacts redundancy, providing insights into optimizing node usage, reducing energy consumption, and improving efficiency in WSNs.

5.1 Performance comparison of proposed and conventional methods for Packet Delivery Ratio

Figure 10 represents the performance analysis of the proposed PATRA in comparison with other conventional techniques, such as QOS-PSO, ACORC, and TANARP, based on the PDR with respect to malicious nodes. The X-axis represents the number of malicious nodes in the network, y-axis shows PDR in percentage, which essentially shows the ratio of delivered packets to the total transmitted ones. The graph shows that PATRA maintains a higher PDR in compared to conventional techniques throughout and even with increased malicious node numbers.

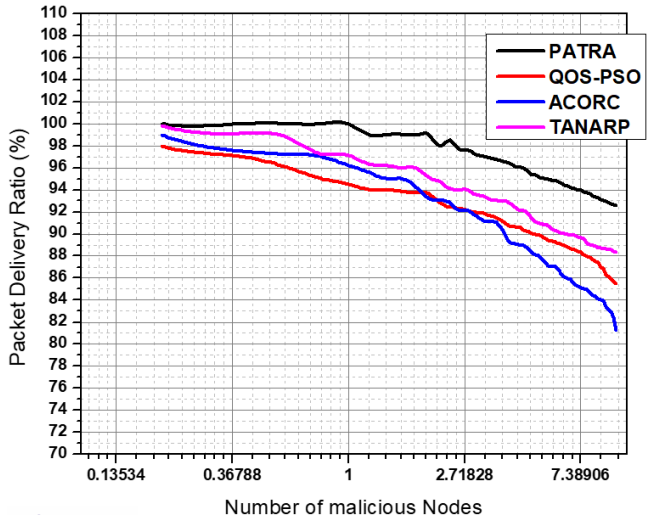

Figure 10. Performance analysis of Packet Delivery Ratio with malicious nodes [59]

This better performance is due to PATRA's dynamic reputation-based routing mechanism and adaptive pheromone updates that prioritize the use of reliable nodes and thus limit malicious activities. However, on the other side, there is a more pronounced effect on the decline of the PDR value, especially in the case of classic methods, since those algorithms are more susceptible to disrupting malicious nodes because either their routing method is stationary or less adaptable. Thus, the figure proves how robust and effective PATRA is in providing guaranteed, reliable data transmission over these adverse network conditions.

5.2 Energy efficiency comparison of proposed and conventional methods

Figure 11 shows that PATRA has always had low energy consumption, in contrast to traditional approaches, thus proving its energy efficiency. With the increase in malicious nodes, conventional approaches, such as ACORC and TANARP, present a steep energy consumption rate due to their inability to handle malicious activities which are subjected to high retransmissions and redundant communication. In contrast, PATRA tries to keep energy

consumption at a minimum by utilizing its reputation-based routing mechanism, which gives the highest priority to the nodes that have higher reliability and residual energy levels, thus preventing unnecessary transmissions and prolonging network lifetime.

This efficient exploitation of energy assures the continuity in network performance, while it solves one of the greatest challenges in WSNs: The energy exhaustion challenge. The figure illustrates how PATRA can come out best in optimizing the utilization of energy in handling malicious activities.

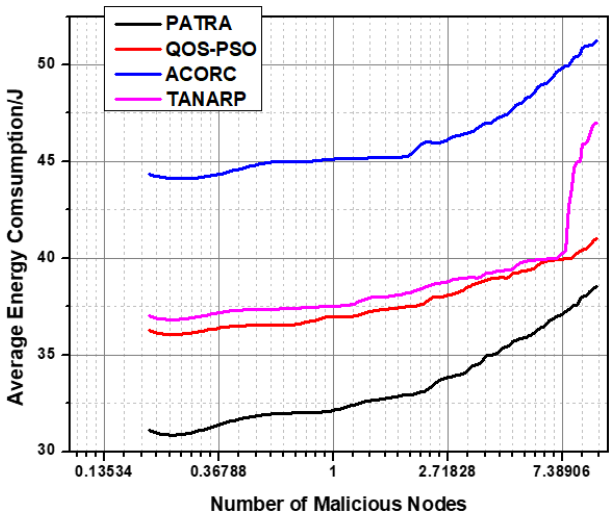

Figure 11. The performance analysis between the proposed method and with conventional with respect to average energy consumption [59]

5.3 Packet loss rate analysis of proposed and conventional methods

Figure 12 compares the performance of the proposed PATRA, Pheromone-based Ant Trusted Routing Algorithm, with conventional methods like QOS-PSO, ACORC, and TANARP for packet loss rate versus time. In this plot, the x-axis represents the time in simulation, and the y-axis represents the packet loss rate in percentage.

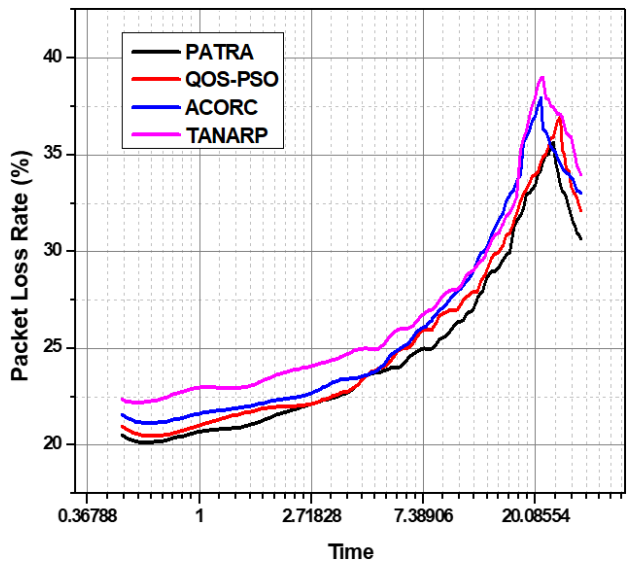

Figure 12. The performance analysis between the proposed method with conventional methods with respect to the packet loss rate (%)

It can be seen from this simulation that the proposed method of PATRA keeps its packet loss rate lower, while the conventional methods start significantly increasing towards the end of this simulation under conditions involving high network traffic and potentially malicious activities. The increased packet loss of methods like TANARP and ACORC is due to the less adaptability of these methods: They have static routing mechanisms which cannot give priority to reliable and trustworthy nodes, effectively.

In contrast, PATRA demonstrates a more stable packet loss rate due to its adaptive routing strategy, which incorporates node reputation, energy levels, and pheromone updates. By favouring reliable nodes and dynamically adjusting routing paths, PATRA minimizes packet loss even under challenging network conditions, ensuring higher reliability in data transmission. The figure highlights the effectiveness of PATRA in reducing packet loss, contributing to overall network efficiency and performance.

5.4 Packet loss rate comparison for varying node counts

Figure 13 shows the packet loss rate comparison of the proposed PATRA with other traditional methods, such as QOS-PSO, ACORC, and TANARP, for different numbers of nodes. The x-axis shows the number of nodes in the network, and the y-axis represents the packet loss rate in percentage.

It is observed from the bar graph that, out of all methods, the proposed PATRA method gives the minimum packet loss rate for all node counts. With an increase in nodes, the packet loss rate for all approaches goes up due to increased traffic and congestion within the network. However, conventional methods give very high packet loss rates, especially those related to TANARP and ACORC due to their inefficient handling of congestion and dynamic routing challenges.

In turn, the performance of PATRA outperforms PATRA based on a reputation-based routing mechanism and adaptive pheromone updates, giving the former first priority over the latter. It gives high preference to nodes that are reliable and efficient, hence making it transmit packets through optimum paths in an attempt to minimize packet loss. This is further affirmed that PATRA will be well scalable with robustness by minimizing the packet loss even in big-scale and complex networks.

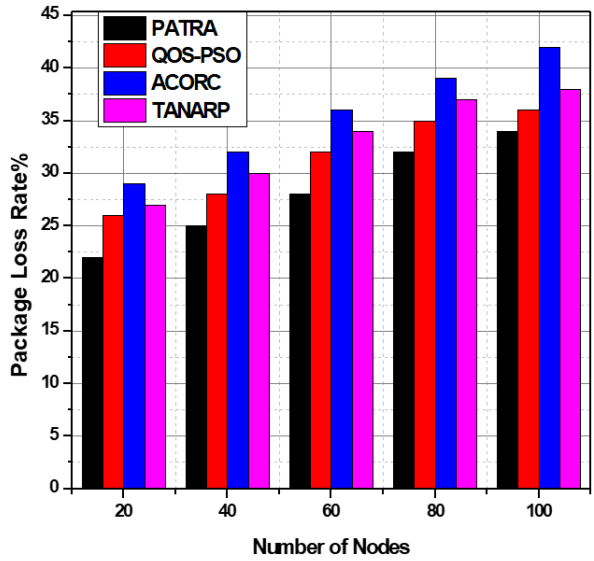

Figure 13. Packet loss rate comparison analysis

5.5 Comparison of the number of received packets across methods

Figure 14 illustrates the performance comparison of the proposed PATRA with that of other conventional methods like QOS-PSO, ACORC, and TANARP using the number of packets received during the simulation. The x-axis represents the instances of the simulation, while the y-axis shows the number of packets received.

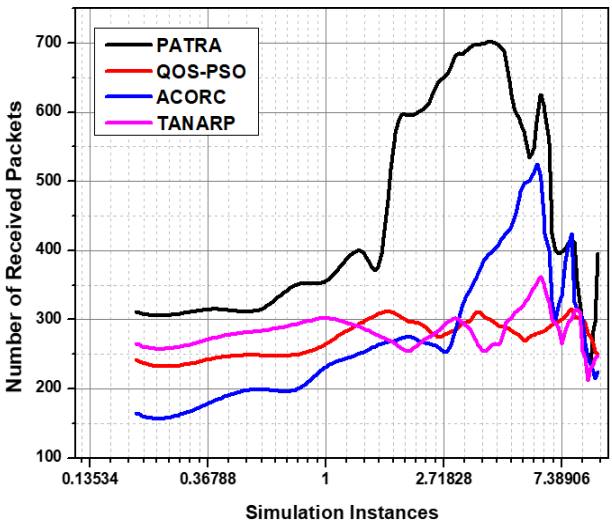

Figure 14. Performance analysis of the number of received packets

In the proposed PATRA method, the number of received packets is considerably higher throughout the simulation compared to conventional methods. This may be because PATRA can select reliable nodes by using a reputation-based routing mechanism and adaptive pheromone update for efficient and secure data transmission. In contrast, all the conventional methods, namely TANARP and ACORC, show a gradual increase in packet reception at the beginning but fail to maintain stability under higher simulation instances due to their low adaptability to network dynamics and malicious node activities.

6. CONCLUSION

The research work has been conducted on the life-time enhancement of nodes in WSN using the proposed algorithm. It has improved data transmission security, energy consumption, local convergence, flexibility, accuracy, and dependability of nodes by using the proposed PATRA method. Adopting the ant colony method to find a quick and effective multipath to deliver the packet from source to destination will help you achieve this. Due to this process, the coincidence rates and data updates at nodes have improved. The proposed model is used to compute and formulate the residual node energy and the transmission delay. Based on the simulation results, the proposed algorithm works better than other methods when looking at packet delivery rates of 0.45% for QOS-PSO, 0.25 for ACORC, and 0.86% for TACOP to compare. Apart from this, average energy consumption is reduced in the proposed method as compared to conventional methods of 0.52%, 0.56%, and 0.45% of QOS-PSO, ACORC, and TACOP, respectively. In this paper, a simulation analysis has been carried out by considering the packet loss rate. The proposed method has better performance in comparisons to conventional methods, such as 0.12 for QOS-PSO. 0.65% for ACORC and 0.45% for TACOP to be compared.

ACKNOWLEDGMENT

The authors express their gratitude to SJB Institute of Technology, Bengaluru and Visvesvaraya Technological University (VTU), Belagavi for all the support and encouragement provided to take up this research work and publish this paper.

REFERENCES

[1] Eiza, M.H., Owens, T., Ni, Q. (2015). Secure and robust multi-constrained QoS aware routing algorithm for VANETs. IEEE Transactions on Dependable and Secure Computing, 13(1): 32-45. https://doi.org/10.1109/TDSC.2014.2382602

[2] Dhas, C.S.G., Belinda, J.C.M., Manoja, J.D., Ramar, K. (2007). Secure routing using ant colony method and RPS algorithm. International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007), Sivakasi, India, pp. 37-43. https://doi.org/10.1109/ICCIMA.2007.68

[3] Hu, G., Zhang, P., Zhang, W. (2009). The optimal design of tree structure based on ant colony of wireless sensor networks routing. In 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, Chengdu, China, pp. 772-776. https://doi.org/10.1109/DASC.2009.23

[4] Saleem, K., Fisal, N., Al-Muhtadi, J. (2014). Empirical studies of bio-inspired self-organized secure autonomous routing protocol. IEEE Sensors Journal, 14(7): 2232-2239. https://doi.org/10.1109/JSEN.2014.2308725

[5] Sharmin, A., Anwar, F., Motakabber, S.M.A., Hashim, A.H.A. (2021). Secure ACO-Based wireless sensor network routing algorithm for IoT. In 2021 8th International Conference on Computer and Communication Engineering (ICCCE), Kuala Lumpur, Malaysia, pp. 190-195. https://doi.org/10.1109/ICCCE50029.2021.9467223

[6] Junnarkar, A.A., Singh, Y.P., Deshpande, V.S. (2018). SQMAA: Security, QoS and mobility aware ACO based opportunistic routing protocol for MANET. In 2018 4th International Conference for Convergence in Technology (I2CT), Mangalore, India, pp. 1-6. https://doi.org/10.1109/I2CT42659.2018.9058022

[7] Saleem, K., Fisal, N. (2013). Energy efficient information assured routing based on hybrid optimization algorithm for WSNs. In 2013 10th International Conference on Information Technology: New Generations, Las Vegas, USA, pp. 518-524. https://doi.org/10.1109/ITNG.2013.86

[8] Rathee, M., Kumar, S., Gandomi, A.H., Dilip, K., Balusamy, B., Patan, R. (2019). Ant colony optimization based quality of service aware energy balancing secure routing algorithm for wireless sensor networks. IEEE Transactions on Engineering Management, 68(1): 170-182. https://doi.org/10.1109/TEM.2019.2953889

[9] Sahoo, S.K., Nayak, C.K., Pattnaik, S.K., Samal, S., Bandopadhaya, S., Das, J.K. (2021). Automatic QoS

based multicast communication system in MANET. 2021 IEEE International Conference on Signal Processing, Information, Communication & Systems (SPICSCON), Dhaka, Bangladesh, pp. 96-100. https://doi.org/10.1109/SPICSCON54707.2021.9885474

[10] Iwendi, C., Ansere, J.A., Nkurunziza, P., Anajemba, J.H., Yixuan, Z. (2018). An ACO-KMT energy efficient routing scheme for sensed-IoT network. IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society, Washington, USA, pp. 3841-3846. https://doi.org/10.1109/IECON.2018.8591489

[11] Wang, Z.Y., Du, J., Xia, Z.Y., Jiang, C.X., Fang, Z.R., Ren, Y. (2022). Secure routing in underwater acoustic sensor networks based on AFSA-ACOA fusion algorithm. In ICC 2022-IEEE International Conference on Communications, Seoul, Korea, pp. 1409-1414. https://doi.org/10.1109/ICC45855.2022.9838802

[12] Safavat, S., Rawat, D.B. (2020). On the elliptic curve cryptography for privacy-aware secure ACO-AODV routing in intent-based internet of vehicles for smart cities. IEEE Transactions on Intelligent Transportation Systems, 22(8): 5050-5059. https://doi.org/10.1109/TITS.2020.3008361

[13] Pathak, A., Al-Anbagi, I., Hamilton, H.J. (2022). An adaptive QoS and trust-based lightweight secure routing algorithm for WSNs. IEEE Internet of Things Journal, 9(23): 23826-23840. https://doi.org/10.1109/JIOT.2022.3189832

[14] Sur, C., Sharma, S., Shukla, A. (2012). Analysis & modeling multi-breeded Mean-Minded ant colony optimization of agent based Road Vehicle Routing Management. In 2012 International Conference for Internet Technology and Secured Transactions, London, UK, pp. 634-641.

[15] Saleem, K., Fisal, N., Abdullah, M.S., Zulkarmwan, A.B., Hafizah, S., Kamilah, S. (2009). Proposed nature inspired self-organized secure autonomous mechanism for WSNs. 2009 First Asian Conference on Intelligent Information and Database Systems, Dong hoi, Vietnam, pp. 277-282. https://doi.org/10.1109/ACIIDS.2009.75

[16] Wang, S. (2022). Intelligent algorithm in computer network security. 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), Chickballapur, India, pp. 1-4. https://doi.org/10.1109/ICKECS56523.2022.10059831

[17] Muraleedharan, R., Osadciw, L.A. (2008). Secure health monitoring network against denial-of-service attacks using cognitive intelligence. In 6th Annual Communication Networks and Services Research Conference (CNSR 2008), Halifax, Canada, pp. 165-170. https://doi.org/10.1109/CNSR.2008.85

[18] Malathy, S., Geetha, J., Suresh, A., Priya, S. (2018). Implementing elliptic curve cryptography with ACO based algorithm in clustered WSN for border surveillance. 2018 Fourth International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Chennai, India, pp. 1-5. https://doi.org/10.1109/AEEICB.2018.8480856

[19] Sharma, D., Kulkarni, S. (2018). Hybrid technique for improving the network lifetime of wireless sensor networks. In 2018 International Conference on Emerging Trends and Innovations in Engineering and Technological Research (ICETIETR), Ernakulam, India, pp. 1-7. https://doi.org/10.1109/ICETIETR.2018.8529134

[20] Lu, Y.F., Lin, K., Li, K.Q. (2012). Trust evaluation model against insider attack in wireless sensor networks. 2012 Second International Conference on Cloud and Green Computing, Xiangtan, China, pp. 319-326. https://doi.org/10.1109/CGC.2012.35

[21] Subathra, P., Sivagurunathan, S., Selvan, G.E. (2006). Securing mobile ad hoc networks through AntTree clustering and threshold cryptography. In 2006 International Symposium on Ad Hoc and Ubiquitous Computing, Mangalore, India, pp. 48-51. https://doi.org/10.1109/ISAHUC.2006.4290646

[22] Kubalik, J., Mordinyi, R. (2007). Optimizing events traffic in event-based systems by means of evolutionary algorithms. In the Second International Conference on Availability, Reliability and Security (ARES'07), Vienna, Austria, pp. 1101-1107. https://doi.org/10.1109/ARES.2007.113

[23] Abhay, D.A., Akash, S., Ashwin, K., Shenoy, A.G., Auradkar, P.K. (2023). Smart policing: using geospatial crime data to plan patrol routes. In 2023 4th International Conference for Emerging Technology (INCET), Belgaum, India, pp. 1-7. https://doi.org/10.1109/INCET57972.2023.10170289

[24] Zhu, P.F., Cui, J.B., Ji, Y.F. (2021). Universal hash based built-in secure transport in FlexE over WDM networks. Journal of Lightwave Technology, 39(18): 5680-5690. https://doi.org/10.1109/JLT.2021.3094265

[25] Thazeen, S., Mallikarjunaswamy, S., Saqhib, M.N., Sharmila, N. (2022). DOA method with reduced bias and side lobe suppression. In 2022 International Conference on Communication, Computing and Internet of Things (IC3IoT), Chennai, India, pp. 1-6. https://doi.org/10.1109/IC3IOT53935.2022.9767996

[26] Dayananda, P., Srikantaswamy, M., Nagaraju, S., Velluri, R., Kumar, D.M. (2022). Efficient detection of faults and false data injection attacks in smart grid using a reconfigurable Kalman filter. International Journal of Power Electronics and Drive Systems (IJPEDS), 13(4): 2086-2097. https://doi.org/10.11591/ijpeds.v13.i4.pp2086-2097

[27] Mahendra, H.N., Mallikarjunaswamy, S., Subramoniam, S.R. (2023). An assessment of vegetation cover of Mysuru City, Karnataka State, India, using deep convolutional neural networks. Environmental Monitoring and Assessment, 195(4): 526. https://doi.org/10.1007/s10661-023-11140-w

[28] Xu, L., Huang, K., Liu, J.P., Li, D.S., Chen, Y.F. (2022). Intelligent planning of fire evacuation routes using an improved ant colony optimization algorithm. Journal of Building Engineering, 61: 105208. https://doi.org/10.1016/j.jobe.2022.105208

[29] Zhu, R., Boukerche, A., Huang, X., Yang, Q. (2023). DESLR: Energy-efficient and secure layered routing based on channel-aware trust model for UASNs. Computer Networks, 234: 109939. https://doi.org/10.1016/j.comnet.2023.109939

[30] Sun, Z., Wei, M., Zhang, Z., Qu, G. (2019). Secure routing protocol based on multi-objective ant-colony-optimization for wireless sensor networks. Applied Soft Computing, 77: 366-375. https://doi.org/10.1016/j.asoc.2019.01.034

[31] Sharma, Y.K., Ahmed, G., Saini, D.K. (2024). Uneven clustering in wireless sensor networks: A comprehensive review. Computers and Electrical Engineering, 120: 109844. https://doi.org/10.1016/j.compeleceng.2024.109844
[32] Dubey, G.P., Stalin, S., Alqahtani, O., Alasiry, A., Sharma, M., Aleryani, A., Shukla, P.K., Alouane, M.T.H. (2023). Optimal path selection using reinforcement learning based ant colony optimization algorithm in IoT-Based wireless sensor networks with 5G technology. Computer Communications, 212: 377-389. https://doi.org/10.1016/j.comcom.2023.09.015
[33] Kumar, A., Thomas, A. (2012). Energy efficiency and network lifetime maximization in wireless sensor networks using improved ant colony optimization. Procedia engineering, 38: 3797-3805. https://doi.org/10.1016/j.proeng.2012.06.435
[34] Alqarni, M.A., Mousa, M.H., Hussein, M.K., Mead, M.A. (2023). Improved wireless sensor network data collection using discrete differential evolution and ant colony optimization. Journal of King Saud University-Computer and Information Sciences, 35(8): 101725. https://doi.org/10.1016/j.jksuci.2023.101725
[35] Kumar, N., Singh, K., Lloret, J. (2024). WAOA: A hybrid whale-ant optimization algorithm for energy-efficient routing in wireless sensor networks. Computer Networks, 254: 110845. https://doi.org/10.1016/j.comnet.2024.110845
[36] El Khediri, S., Selmi, A., Khan, R.U., Moulahi, T., Lorenz, P. (2024). Energy efficient cluster routing protocol for wireless sensor networks using hybrid metaheuristic approache's. Ad Hoc Networks, 158: 103473. https://doi.org/10.1016/j.adhoc.2024.103473
[37] Sachithanandam, V., Jessintha, D., Balaji, V.S., Manoharan, M. (2025). Deep reinforcement learning and enhanced optimization for real-time energy management in wireless sensor networks. Sustainable Computing: Informatics and Systems, 45: 101071. https://doi.org/10.1016/j.suscom.2024.101071
[38] Wang, L., Luo, Y., Yan, H. (2024). Optimization analysis of node energy consumption in wireless sensor networks based on improved ant colony algorithm. Sustainable Energy Technologies and Assessments, 64: 103680. https://doi.org/10.1016/j.seta.2024.103680
[39] Ketshabetswe, L.K., Zungeru, A.M., Lebekwe, C.K., Mtengi, B. (2024). A compression-based routing strategy for energy saving in wireless sensor networks. Results in Engineering, 23: 102616. https://doi.org/10.1016/j.rineng.2024.102616
[40] Stodola, P., Kutěj, L. (2024). Multi-depot vehicle routing problem with drones: Mathematical formulation, solution algorithm and experiments. Expert Systems with Applications, 241: 122483. https://doi.org/10.1016/j.eswa.2023.122483
[41] Mallikarjunaswamy, S., Nataraj, K.R., Rekha, K.R. (2014). Design of high-speed reconfigurable coprocessor for next-generation communication platform. Emerging Research in Electronics, Computer Science and Technology: Proceedings of International Conference, ICERECT 2012, New Delhi, pp. 57-67. https://doi.org/10.1007/978-81-322-1157-0_7
[42] Kumari, P., Sahana, S.K. (2022). Heuristic initialization based modified ACO (HIMACO) mimicking ant safety features for Multicast Routing and its parameter tuning. Microprocessors and Microsystems, 93: 104574. https://doi.org/10.1016/j.micpro.2022.104574
[43] Bayram, O.B., Ozcan, A. (2023). Determining optimal paths of virtual links in Avionics Full-Duplex Switched Ethernet networks using modified ant colony optimization algorithm. Expert Systems with Applications, 229: 120433. https://doi.org/10.1016/j.eswa.2023.120433
[44] Dhand, G., Sheoran, K. (2020). Protocols SMEER (Secure Multitier Energy Efficient Routing Protocol) and SCOR (Secure Elliptic curve based Chaotic key Galois Cryptography on Opportunistic Routing). Materials Today, 37: 1324-1327. https://doi.org/10.1016/j.matpr.2020.06.503
[45] Suresh, B., Prasad, G.S.C. (2023). An Energy efficient secure routing scheme using LEACH protocol in WSN for IoT networks. Measurement: Sensors, 30: 100883. https://doi.org/10.1016/j.measen.2023.100883
[46] Gurram, G.V., Shariff, N.C., Biradar, R.L. (2022). A secure energy aware meta-heuristic routing protocol (SEAMHR) for sustainable IoT-wireless sensor network (WSN). Theoretical Computer Science, 930: 63-76. https://doi.org/10.1016/j.tcs.2022.07.011
[47] Pavithra, G.S., Pooja, S., Rekha, V., Mahendra, H.N., Sharmila, N., Mallikarjunaswamy, S. (2023). Comprehensive analysis on vehicle-to-vehicle communication using intelligent transportation system. International Conference on Soft Computing for Security Applications, TamilNadu, India, pp. 893-906. https://doi.org/10.1007/978-981-99-3608-3_62
[48] Mahendra, H.N., Mallikarjunaswamy, S., Kumar, D.M., Kumari, S., Kashyap, S., Fulwani, S., Chatterjee, A. (2023). Assessment and prediction of air quality level using ARIMA model: A case study of Surat City, Gujarat State, India. Nature Environment & Pollution Technology, 22(1): 199-210. https://doi.org/10.46488/NEPT.2023.v22i01.018
[49] Umashankar, M.L., Mallikarjunaswamy, S., Sharmila, N., Kumar, D.M., Nataraj, K.R. (2023). A survey on IoT protocol in real-time applications and its architectures. ICDSMLA 2021: Proceedings of the 3rd International Conference on Data Science, Machine Learning and Applications, SingaporeM, pp. 119-130. https://doi.org/10.1007/978-981-19-5936-3_12
[50] Mahendra, H.N., Mallikarjunaswamy, S., Subramoniam, S.R. (2023). An assessment of built-up cover using geospatial techniques—A case study on Mysuru District, Karnataka State, India. International Journal of Environmental Technology and Management, 26(3-5): 173-188. https://doi.org/10.1504/IJETM.2023.130787
[51] Pooja, S., Mallikarjunaswamy, S., Sharmila, N. (2023). Image region driven prior selection for image deblurring. Multimedia Tools and Applications, 82(16): 24181-24202. https://doi.org/10.1007/s11042-023-14335-y
[52] Rathod, S., Ramaswamy, N.K., Srikantaswamy, M., Ramaswamy, R.K. (2022). An efficient reconfigurable peak cancellation model for peak to average power ratio reduction in orthogonal frequency division multiplexing communication system. International Journal of Electrical and Computer Engineering, 12(6): 6239-6247. https://doi.org/10.11591/ijece.v12i6.pp6239-6247
[53] Mallikarjunaswamy, S., Basavaraju, N.M., Sharmila, N., Mahendra, H.N., Pooja, S., Deepak, B.L. (2022). An efficient big data gathering in wireless sensor network

using reconfigurable node distribution algorithm. In 2022 Fourth International Conference on Cognitive Computing and Information Processing (CCIP), Bengaluru, India, pp. 1-6. https://doi.org/10.1109/CCIP57447.2022.10058620

[54] Mahendra, H.N., & Mallikarjunaswamy, S. (2022). An efficient classification of hyperspectral remotely sensed data using support vector machine. International Journal of Electronics and Telecommunications, 68(3): 609-617. http://doi.org/10.24425/ijet.2022.141280

[55] Shivaji, R., Nataraj, K.R., Mallikarjunaswamy, S., Rekha, K.R. (2022). Implementation of an effective hybrid partial transmit sequence model for peak to average power ratio in MIMO OFDM system. In ICDSMLA 2020: Proceedings of the 2nd International Conference on Data Science, Machine Learning and Applications, Singapore, pp. 1343-1353. https://doi.org/10.1007/978-981-16-3690-5_129

[56] Savitha, A.C., Jayaram, M.N. (2022). Development of energy efficient and secure routing protocol for M2M communication. International Journal of Performability Engineering, 18(6): 426. https://doi.org/10.23940/ijpe.22.06.p5.426-433

[57] Venkatesh, D.Y., Mallikarjunaiah, K., Srikantaswamy, M. (2022). A comprehensive review of low density parity check encoder techniques. Ingénierie des Systèmes d'Information, 27(1): 11-20. https://doi.org/10.18280/isi.270102

[58] Thazeen, S., Mallikarjunaswamy, S., Saqhib, M.N. (2022). Septennial adaptive beamforming algorithm. In 2022 International Conference on Smart Information Systems and Technologies (SIST), Nur-Sultan, Kazakhstan, pp. 1-4. https://doi.org/10.1109/SIST54437.2022.9945753

[59] Zhang, L., Yin, N., Fu, X., Lin, Q.M., Wang, R.C. (2017). A multi-attribute pheromone ant secure routing algorithm based on reputation value for sensor networks. Sensors, 17(3): 541. https://doi.org/10.3390/s17030541

[60] Mahendra, H.N., Mallikarjunaswamy, S., Nooli, C.B., Hrishikesh, M., Kruthik, N., Vakkalanka, H.M. (2022). Cloud based centralized smart cart and contactless billing system. In 2022 7th international conference on communication and electronics systems (ICCES), Coimbatore, India, pp. 820-826. https://doi.org/10.1109/ICCES54183.2022.9835856

[61] Mallikarjunaswamy, S., Sharmila, N., Siddesh, G.K., Nataraj, K.R., Komala, M. (2022). A novel architecture for cluster based false data injection attack detection and location identification in smart grid. Advances in Thermofluids and Renewable Energy: Select Proceedings of TFRE 2020, Singapore, pp. 599-611. https://doi.org/10.1007/978-981-16-3497-0_48

[62] Thazeen, S., Mallikarjunaswamy, S., Siddesh, G.K., Sharmila, N. (2021). Conventional and subspace algorithms for mobile source detection and radiation formation. Traitement du Signal, 38(1): 135-145. https://doi.org/10.18280/ts.380114

[63] Satish, P., Srikantaswamy, M., Ramaswamy, N.K. (2020). A comprehensive review of blind deconvolution techniques for image deblurring. Traitement du Signal, 37(3): 527-539. https://doi.org/10.18280/ts.370321

[64] Umashankar, M.L., Ramakrishna, M.V., Mallikarjunaswamy, S. (2019). Design of high speed reconfigurable deployment intelligent genetic algorithm in maximum coverage wireless sensor network. In 2019 International conference on data science and communication (IconDSC), Bangalore, India, pp. 1-6. https://doi.org/10.1109/IconDSC.2019.8816930

[65] Mahendra, H.N., Mallikarjunaswamy, S., Rekha, V., Puspalatha, V., Sharmila, N. (2019). Performance analysis of different classifier for remote sensing application. International Journal of Engineering and Advanced Technology, 9(1): 7153-7158. http://www.doi.org/10.35940/ijeat.A1879.109119

[66] Thazeen, S., Mallikarjunaswamy, S. (2023). The effectiveness of 6t beamformer algorithm in smart antenna systems for convergence analysis. IIUM Engineering Journal, 24(2): 100-116. https://doi.org/10.31436/iiumej.v24i2.2730

[67] Sithik, M.M., Kumar, B.M. (2022). Intelligent agent based virtual clustering and multi-context aware routing for congestion mitigation in secure RPL-IoT environment. Ad Hoc Networks, 137: 102972. https://doi.org/10.1016/j.adhoc.2022.102972

[68] Mythili, V., Suresh, A., Devasagayam, M.M., Dhanasekaran, R. (2019). SEAT-DSR: Spatial and energy aware trusted dynamic distance source routing algorithm for secure data communications in wireless sensor networks. Cognitive Systems Research, 58: 143-155. https://doi.org/10.1016/j.cogsys.2019.02.005

[69] Mahendra, H.N., Mallikarjunaswamy, S., Basavaraju, N.M., Poojary, P.M., Gowda, P.S., Mukunda, M., Navya, B., Pushpalatha, V. (2022). Deep learning models for inventory of agriculture crops and yield production using satellite images. 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), Mysuru, India, pp. 1-7. https://doi.org/10.1109/MysuruCon55714.2022.9972523

[70] Lakshmanaprabu, S.K., Shankar, K., Rani, S.S., Abdulhay, E., Arunkumar, N., Ramirez, G., Uthayakumar, J. (2019). An effect of big data technology with ant colony optimization based routing in vehicular ad hoc networks: Towards smart cities. Journal of Cleaner Production, 217: 584-593. https://doi.org/10.1016/j.jclepro.2019.01.115

[71] Zandieh, F., Ghannadpour, S.F., Mazdeh, M.M. (2024). New integrated routing and surveillance model with drones and charging station considerations. European Journal of Operational Research, 313(2): 527-547. https://doi.org/10.1016/j.ejor.2023.08.035

[72] Ha, J., Roh, M.I., Kim, K.S., Kim, J.H. (2023). Method for pipe routing using the expert system and the heuristic pathfinding algorithm in shipbuilding. International Journal of Naval Architecture and Ocean Engineering, 15: 100533. https://doi.org/10.1016/j.ijnaoe.2023.100533

[73] Vinitha, A., Rukmini, M.S.S. (2022). Secure and energy aware multi-hop routing protocol in WSN using Taylor-based hybrid optimization algorithm. Journal of King Saud University-Computer and Information Sciences, 34(5): 1857-1868. https://doi.org/10.1016/j.jksuci.2019.11.009

[74] Ye, Z., Mohamadian, H. (2014). Adaptive clustering based dynamic routing of wireless sensor networks via generalized ant colony optimization. Ieri Procedia, 10: 2-10. https://doi.org/10.1016/j.ieri.2014.09.063

[75] Taherian, M., Karimi, H., Kashkooli, A.M., Esfahanimehr, A., Jafta, T., Jafarabad, M. (2015). The

design of an optimal and secure routing model in wireless sensor networks by using PSO algorithm. Procedia Computer Science, 73: 468-473. https://doi.org/10.1016/j.procs.2015.12.028

[76] Jose, M.R., Vigila, S.M.C. (2023). F-CAPSO: Fuzzy chaos adaptive particle swarm optimization for energy-efficient and secure data transmission in MANET. Expert Systems with Applications, 234: 120944. https://doi.org/10.1016/j.eswa.2023.120944

[77] Venkatesh, D.Y., Mallikarjunaiah, K., Srikantaswamy, M. (2023). An efficient reconfigurable code rate cooperative low-density parity check codes for gigabits wide code encoder/decoder operations. International Journal of Electrical & Computer Engineering, 13(6): 6369-6377. https://doi.org/10.11591/ijece.v13i6.pp6369-6377

[78] Pandith, M.M., Ramaswamy, N.K., Srikantaswamy, M., Ramaswamy, R.K. (2023). An efficient reconfigurable geographic routing congestion control algorithm for wireless sensor networks. International Journal of Electrical & Computer Engineering, 13(6): 6388-6398. https://doi.org/10.11591/ijece.v13i6.pp6388-6398

[79] Thazeen, S., Srikantaswamy, M. (2023). An efficient reconfigurable optimal source detection and beam allocation algorithm for signal subspace factorization. International Journal of Electrical and Computer Engineering (IJECE), 13(6): 6452-6465. https://doi.org/10.11591/ijece.v13i6.pp6452-6465

[80] Chikkasiddaiah, C., Govindaswamy, P., Srikantaswamy, M. (2023). An efficient hydro-crop growth prediction system for nutrient analysis using machine learning algorithm. International Journal of Electrical and Computer Engineering (IJECE), 13(6): 6681-6690. https://doi.org/10.11591/ijece.v13i6.pp6681-6690