Journal of Computer Science

Original Research Paper

Hybrid Optimization to Trust Enhanced Secure Routing Optimization with IABC and CGWAA for MANET

Yuvaraja Panneer Selvam and Suganthi Perumal

Department of Computer Science, Namakkal Kavingnar Ramalingam Government Arts College for Women, Thillaipuram, Namakkal, Tamil Nadu, India

Article history
Received: 07-10-2024
Revised: 30-12-2024
Accepted: 14-02-2025

Corresponding Author:
Yuvaraja Panneer Selvam
Department of Computer Science, Namakkal Kavingnar Ramalingam Government Arts College for Women, Thillaipuram, Namakkal, Tamil Nadu, India
Email: psyuvaraja.p@gmail.com

Abstract: Routing in Mobile Ad Hoc Networks (MANET) presents significant challenges due to the dynamic nature of network topology. Optimal route selection and efficient route discovery are matched by effective routing in MANET. This study proposes a Hybrid Optimization to Trust-Enhanced Secure Routing Optimization (HO-TESRO) designed to address these challenges in IoT environments by integrating metrics such as link stability, bandwidth, energy, and trust. The HO-TESRO model employs the Improved Artificial Bee Colony (IABC) algorithm to select optimal routes and utilizes the Chaotic Grey Wolf Adaptive Algorithm (CGWAA) algorithm in combination with the Advanced Encryption Standard (AES) to ensure secure communication. The trust-based CGWAA algorithm evaluates and selects the most secure and efficient multiple paths, while the AES-CGWAA mechanism validates node keys and shared codes for each data transfer, ensuring a safe connection. The proposed model was evaluated using extensive simulations in MATLAB, and its performance was compared against existing techniques. The findings show major improvements in detection rate, throughput, packet loss ratio, latency, and packet delivery ratio. These findings underscore the efficacy of HO-TESRO in providing a robust, secure, and energy-efficient routing solution for IoT-based MANET, addressing critical issues of resource allocation and secure routing.

Keywords: MANET, Secure Routing, HO-TESRO, IABC, CGWAA, AES

Introduction

In recent years, the rapid growth of Internet of Things (IoT) networks and wireless communication systems has led to an increased demand for secure, efficient, and reliable data transmission. As these networks expand, they face numerous challenges, including security vulnerabilities, dynamic network conditions, and the need for efficient resource allocation (Kaur and Kakkar, 2022). One of the critical issues in these networks is routing optimization, where selecting the best path for data transmission can directly impact network performance, security, and energy efficiency (Srilakshmi *et al*., 2022; Veeraiah *et al*., 2021). Traditional routing protocols often fail to address these challenges adequately, especially in dynamic environments where network conditions frequently change. To address these issues, hybrid optimization techniques have emerged as a promising approach, integrating various optimization algorithms to enhance routing performance while maintaining security and trust (Sun *et al*., 2019). Secure routing is essential for protecting data integrity, confidentiality, and availability in communication networks (Srilakshmi *et al*., 2021).

In the IoT and other wireless networks, secure routing involves not only selecting optimal paths but also ensuring that these paths are trustworthy and resilient against potential threats (Vinitha *et al*., 2021). The incorporation of trust mechanisms into routing protocols helps to mitigate risks such as data tampering, eavesdropping, and denial-of-service attacks (Rodrigues, John, 2020). However, implementing trust-enhanced secure routing poses significant challenges due to the inherent complexity of evaluating trust levels, dynamically adapting to network changes, and optimizing multiple conflicting objectives simultaneously. This necessitates the use of advanced optimization techniques that can handle the multi-dimensional nature of routing problems while ensuring security and trust. Hybrid optimization combines multiple meta-heuristic algorithms, leveraging their individual strengths to achieve superior performance in solving complex optimization problems (Han *et al*., 2022). These

algorithms are designed to overcome the limitations of traditional optimization methods, such as slow convergence rates and susceptibility to local optima. By integrating different optimization strategies, hybrid algorithms provide a more robust and flexible framework for addressing the unique challenges of trust-enhanced secure routing (Kalidoss *et al*., 2020; Hu *et al*., 2022). The hybrid approach allows the system to explore a broader solution space and adapt more effectively to the dynamic conditions of IoT and wireless networks (Nagaraju *et al*., 2020). In trust-enhanced secure routing, the integration of hybrid optimization techniques enables the dynamic evaluation and selection of routes based on multiple criteria, including trust levels, path reliability, energy efficiency, and overall security. Trust metrics can be derived from various sources, such as node behavior, historical data, and real-time network conditions, to assess the credibility of each route (Selvi *et al*., 2019; Mittal *et al*., 2021).

Hybrid optimization helps in balancing these metrics, ensuring that the chosen route not only meets performance requirements but also adheres to security and trust standards. This approach enhances the overall robustness of the network by minimizing the likelihood of selecting compromised or unreliable routes (Ourouss *et al*., 2021). Moreover, hybrid optimization techniques facilitate adaptive routing decisions in real time, which is crucial for maintaining optimal performance in highly dynamic environments. As network conditions change, such as variations in node availability, traffic loads, and potential security threats, the optimization framework continuously updates its routing strategies to reflect the current state of the network. This adaptability is particularly valuable in IoT networks, where nodes often have limited resources, and environmental factors can significantly impact network performance. The proposed approach to trust-enhanced secure routing through hybrid optimization aims to address the complexities of modern communication networks by integrating advanced optimization techniques with security and trust assessment (Zhang *et al*., 2024). By leveraging the strengths of multiple algorithms, this approach seeks to enhance the reliability, security, and efficiency of data transmission, ultimately supporting the growing demands of IoT and other next-generation networks (Shende and Sonavane, 2020). The hybrid optimization framework offers a comprehensive solution to the multifaceted challenges of secure routing, paving the way for more resilient and trustworthy communication systems in the future.

The contributions of this study are manifested below:

- This study introduces the HO-TESRO model, which integrates multiple optimization techniques to enhance secure routing in IoT-based MANET
- This study employs the IABC algorithm to optimize route selection based on key metrics such as link stability, bandwidth, and energy, thereby improving overall route discovery and selection processes in dynamic network environments
- This study develops a trust-based routing mechanism using CGWAA to evaluate and select the most secure and reliable routes, addressing critical security challenges associated with dynamic and decentralized MANET
- This study incorporates AES in combination with CGWAA to ensure secure data transmission, validating node keys and shared codes for each data transfer, which significantly enhances the security of communications in MANET

Novelty: The proposed HO-TESRO model demonstrates scientific novelty by integrating the Improved Artificial Bee Colony (IABC) algorithm with the Chaotic Grey Wolf Adaptive Algorithm (CGWAA) for trust-based, energy-efficient routing in MANETs, a novel combination not explored in prior studies. Unique features include AES-CGWAA for secure key validation and the trust metric's dynamic evaluation for route optimization. This approach enhances routing by simultaneously addressing security, resource allocation, and energy efficiency. Broader implications include its potential application in IoT-enabled smart cities, disaster recovery networks, and military communications, where secure, reliable, and adaptive routing is critical to managing dynamic environments effectively.

Literature Review

To improve safe data routing, (Khot and Naik, 2021) presented the Particle-Water Wave Optimization (P-WWO) method in 2021. This technique combines Particle Swarm Optimization (PSO) with Water Wave Optimization (WWO). The P-WWO method minimizes distance and time while guaranteeing dependable packet transmission through a route maintenance procedure. It chooses cluster heads based on a fitness metric that takes into account energy, delay, trust, consistency, and maintainability. Veeraiah and Krishna (2022) used a new multipath routing protocol in 2022 to address energy optimization and security in MANETs. This technique selects the cluster head and detects intrusions by combining fuzzy clustering with fuzzy Naive Bayes (fuzzy NB). The routing method successfully thwarts assaults like flooding, black holes, and selective packet drops by using the BSWOA to choose routes efficiently based on connection, energy, trust, and throughput.

Wang *et al*. (2020) created a cloud architecture to manage fuzzy metrics by combining Fuzzy Petri Nets (FPN) for node credibility evaluation with a trust reasoning approach. In order to improve Quality of Service (QoS), their trust entropy-based routing algorithm chooses routes by decreasing trust entropy while taking into account both route hops and node trust

values. Tangade *et al*. (2020) suggested a hybrid cryptography (TMHC)-based trust management plan to enhance Vehicular Ad-hoc Network (VANET) security. For strong authentication and trust management, this approach uses symmetric Hash Message Authentication Codes (HMAC) and asymmetric identity-based digital signatures. These are evaluated by an Agent Trusted Authority (ATA) and a trusted Roadside Unit (RSU) using reward points. Awan *et al*. (2022) presented a blockchain-based encryption and trust assessment paradigm that used public and private blockchains to authenticate Aggregator Nodes (AN) and Sensor Nodes (SN). Using the RSA cryptosystem for data security, this model detects and eliminates rogue nodes that take advantage of network resources, achieving secure routing based on residual energy and trust values.

By determining the shortest path with the lowest communication costs, the Enhanced Hybrid Ant Colony Optimization Routing Protocol (EHACORP), introduced by Ramamoorthy and Thangavelu (2022), increased routing efficiency. Vehicle distance calculations and ant colony optimization are the two stages of the protocol's operation. In order to guarantee safe routing and worldwide optimization, Shi *et al*. (2019) created a secure routing protocol in 2019 that integrates residual energy and distance and evaluates each relay node's trust value based on historical packet-forwarding behavior. When compared to the Reputation-Based Mechanism to Stimulate Cooperation (RBMSC), this enhanced Dijkstra algorithm produces routes with better delivery ratios and less packet loss. Deebak and Al-Turjman (2020) presented a secure routing and monitoring system that used an Authentication and Encryption Model (ATE) and the Two-Fish (TF) symmetric key technique. Ad hoc On-Demand Multipath Distance Vector (AOMDV) and Multipath Optimized Link State Routing (OLSR) protocols are used in this technique to improve monitoring and fortify against mobile threats.

The Energy-Aware Trust and Opportunity-depending Routing (ETOR) method was used by Hajiee *et al*. (2021) in 2021. They used a hybrid fitness function to choose opportunistic and secure nodes for routing depending on tolerance. Using variables including energy, trust, QoS, connection, distance, hop count, and network traffic, the algorithm optimizes routes. Lastly, And and Darwish (2021) improved routing security in Wireless Sensor Networks (WSNs) in 2021 by combining deep blockchain with Markov Decision Processes (MDPs). Their method ensures safe message forwarding by using Proof of Authority (PoA) for node authentication and deep learning to make validation group selection easier.

Problem Statement

The increasing complexity and scale of modern networks necessitate advanced optimization techniques to address security and efficiency challenges in routing. Traditional routing algorithms often fail to adapt to dynamic network conditions and trust-related issues, leading to suboptimal performance and increased vulnerability to attacks. Hybrid optimization approaches, which combine multiple heuristic and meta-heuristic algorithms, offer a promising solution by leveraging their complementary strengths to enhance routing security and efficiency. This study aims to develop a hybrid optimization approach to trust-enhanced secure routing optimization, integrating various optimization techniques to improve trust-based decision-making and secure data transmission in complex network environments. The proposed methodology seeks to address critical issues such as trust management, routing security, and optimization of network resources, ultimately contributing to more reliable and secure network operations in the face of evolving threats and dynamic conditions.

Materials and Methods

This section outlines the computational environment, simulation setup, and key parameters used to evaluate the proposed model. The simulation was conducted using MATLAB R2023a, leveraging optimization and deep learning toolboxes for implementation. The experiments were executed on a system with an Intel Core i7-12700K processor, 32GB DDR5 RAM, and Windows 11 64-bit OS. A dynamic network topology with 50 to 100 nodes was simulated, where each node maintained a predefined transmission range and followed mobility patterns reflecting real-world scenarios. The simulation was run for 25 seconds, capturing network performance at regular intervals. Key performance metrics considered for evaluation include:

- Delay: Measures the time taken for data to traverse the network
- Detection Rate: Assesses the accuracy of identifying network anomalies or failures

Proposed Methodology

The proposed HO-TESRO methodology addresses critical routing challenges in MANETs by overcoming inefficiencies and security vulnerabilities found in traditional approaches. Conventional routing algorithms often struggle with dynamic network conditions, leading to suboptimal route selection and frequent breaks. HO-TESRO tackles this by using the Improved Artificial Bee Colony (IABC) algorithm, which optimizes routes based on link stability, bandwidth, and energy, ensuring efficient and stable paths. Additionally, the lack of trust and security in MANET routing is a major concern, as

these networks are prone to malicious attacks. To counter this, HO-TESRO integrates the Chaotic Grey Wolf Adaptive Algorithm (CGWAA) to evaluate the trustworthiness of nodes, select secure routes, and enhance overall network reliability and safety. The overall proposed methodology is shown in Fig. (1).

Define Network Parameters

To effectively implement HO-TESRO in MANET, defining the network parameters, along with the initialization steps for setting up the network topology and node parameters:

- Link stability measures the likelihood of maintaining a connection between two nodes over time, which is crucial in MANETs due to the dynamic nature of the topology. The formula is represented as per Eq. (1):

$$ls_{ij} = \frac{t_{up}}{t_{up}+t_{down}} \quad (1)$$

where, ls_{ij} is the link stability between nodes i and j, t_{up} is the Total time the link between nodes i and j is up, and t_{down} represents the total time the link is down:

- Bandwidth refers to the available data transmission capacity on a route, which impacts the route's ability to handle traffic. The formula is represented as per Eq. (2):

$$bw_{ij} = \min(bw_i, bw_j) \quad (2)$$

where, bw_{ij} is the bandwidth available between nodes i and j, $and\ bw_i$ and bw_j are the Bandwidth capacities of nodes i and j:

- Energy refers to the remaining battery power of nodes, which is critical for maintaining communication without interruptions. The formula is represented as per Eq. (3):

$$e_{res} = e_{init} - e_{cons} \quad (3)$$

where, e_{res} is the residual energy of a node, e_{init} is the initial energy of the node, and e_{cons} is the energy consumed during communication and computation:

- Trust evaluates the reliability and security of nodes based on past interactions and behaviors. The formula is represented as per Eq. (4):

$$t_{ij} = \alpha \times t_{dir} + (1-\alpha) \times t_{indir} \quad (4)$$

- Initialization: Define the number of nodes N and their positions within a simulation area of size $X \times Y$. Nodes are typically placed randomly, and their movement can be modeled using mobility models like the Random Waypoint Model
- Position vector: Initialize node positions as (x_i, y_i) where $i = 1,2, \ldots N$ and represented using Eq. (5):

$$(x_i, y_i) = Random(0, X), Random(0, Y) \quad (5)$$

- Velocity vector: Define the speed and direction of each node, v_i and represented using Eq. (6):

$$v_i = v_x, v_y \quad (6)$$

- Transmission Range: Define the maximum distance within which nodes can communicate and represented using Eq. (7):

$$d_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \quad (7)$$

- Node State Variables: Initialize each node with parameters such as initial energy, available bandwidth, and trust values. Figure (1) depicts the overall proposed architecture.

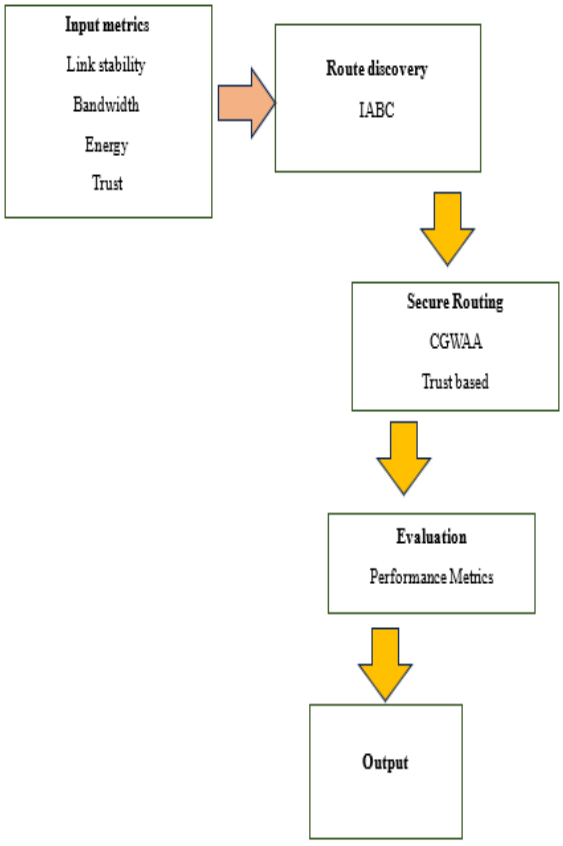


Fig. 1: Overall proposed architecture flow

Route Discovery-IABC

ABC algorithm is a metaheuristic optimization inspired by honey bees' foraging behavior. It consists of employed, onlookers, and scout bees. Employed bees scout food sources and share data with onlooker bees, who probabilistically select sources based on quality. Meanwhile, scout bees emerge from employed bees, exploring new regions when abandoning their current sources, adding an exploration element to prevent local optima entrapment. The ABC algorithm efficiently emulates social cooperation and intelligent foraging to iteratively refine solutions in the search space for optimal or near-optimal outcomes, making it applicable to diverse optimization challenges.

In the ABC algorithm, the swarm consists of employed and onlooker bees, each comprising half of the total swarm size, which equals the number of solutions. It starts with a randomly distributed population of ss solutions (food sources), where ss is the swarm size. Each solution, $A_i = \{a_{i,1}, a_{i,2}, \ldots, a_{i,ds}\}$, with ds as the dimension size, generates candidate solutions C_i in its neighborhood to optimize as per Eq. (8):

$$c_{i,j} = a_{i,j} + \emptyset_{i,j} \cdot (a_{i,j} - a_{k,j}) \quad (8)$$

The algorithm randomly selects a candidate solution A_k (where $I \neq k$) and a dimension index j from $\{1, 2, \ldots, ds\}$, then determines random number $\emptyset_{i,j}$ within [-1, 1]. Using these, a new candidate solution C_i, is generated. If C_i fitness surpasses A_i, $A_i$is will be updated; otherwise, it will remain unchanged. Employed bees share their food source info through dances with onlooker bees. Onlookers evaluate this information and choose a food source probabilistically based on nectar amount, akin to roulette wheel selection as Eq. (9) suggests:

$$r_i = \frac{fit_i}{\sum_{j=1}^{ss} fit_j} \oplus Levy(\beta) \quad (9)$$

In the ABC algorithm, incorporating Lévy flight enhances resource search efficiency by enabling a random walk during the employed bee phase. This novel mechanism generates new solutions around the best food source, improving search direction and algorithm performance. The selection probability of the ith food source is determined by its fitness value, denoted as fit_i. A higher fitness value indicates a higher probability of selecting the $right$ food source. If a position cannot be enhanced within a predefined number of cycles (referred to as the limit), the food source is abandoned. In such cases, denoted by A_i, the scout bee identifies a new food source to replace it, as per Eq. (10):

$$A_{i,j} = lob_j + ra(0,1) \cdot (upb_j - lob_j) \quad (10)$$

Within the range [0, 1], a normal distribution is used to create the random number $ra(0,1)$. The lower and upper bounds of the jth dimension are denoted by the symbols lob and up, respectively.

Trust Evaluation-CGWAA

The Chaotic Grey Wolf Adaptive Algorithm (CGWAA) is an advanced optimization technique that combines the Grey Wolf Optimizer (GWO) with chaotic maps to enhance search efficiency and avoid local optima. In CGWAA, grey wolves simulate leadership and social hierarchy to explore and exploit the solution space, while chaotic sequences introduce randomness, improving convergence speed and precision. This adaptive mechanism helps balance exploration and exploitation, making CGWAA effective in complex optimization problems, including secure routing and resource management in dynamic network environments. The GWO algorithm is inspired by the social structure and hunting strategies of grey wolves, modeling the top three wolves α, β and δ as leaders guiding the pack (ω wolves) towards optimal solutions. The algorithm mimics the wolves' hunting process through three main phases: Encircling the prey, collaboratively hunting, and attacking to capture the prey. These steps drive the pack towards the global optimum, balancing exploration and exploitation to solve complex optimization problems efficiently.

- In the GWO algorithm, the encircling behavior of grey wolves is mathematically modeled using equations that update the positions of wolves relative to the prey. Eq. (11) calculates the distance between a wolf and prey, while Eq. (12) updates the wolf's position, simulating encircling to move closer to the target.

Distance calculation:

$$dis = c \times x_p(t) - x(t) \quad (11)$$

Position update:

$$x(t+1) = x_p(t) - a \times dis \quad (12)$$

Here, x_p represents the position of the prey, and X denotes the position vector of a grey wolf. t is the current iteration, while c and a are coefficient vectors that guide the wolves' movement, calculated using Eq. (13):

$$a = 2ara_1 - A(t) \quad (13)$$

Incorporating the logistic chaotic map into the Grey Wolf Optimizer (GWO) enhances the encircling behavior by introducing chaotic dynamics, thereby improving population diversity and avoiding premature convergence. The logistic map is defined by proposed Eqs. (14-15):

$$c = 2ra_2 \times m_{t+1} \quad (14)$$

$$m_{t+1} = \delta \times m_t \times (1 - m_t) \quad (15)$$

where, t represents time, m is the number of critical points within the interval [0, 1], and δ is the control parameter, adding nonlinearity to the search process. When δ is set between 3.5 and 4, the map exhibits chaotic behavior, which can be used to update the positions of wolves in GWO's encircling phase. In the encircling behavior, the chaotic map introduces random perturbations in wolf positions, enhancing exploration by dynamically adjusting the distance dis and position vectors. This chaotic influence helps in maintaining a balance between exploration and exploitation by preventing wolves from settling prematurely into suboptimal areas, thus improving the overall performance of the GWO algorithm; ra_1 and ra_2 are random vectors within the range; the elements of vector A decrease linearly from 2-0 over the iterations, as shown by Eq. (16):

$$A(t) = 2 - \frac{2t}{T} \quad (16)$$

Here, t is the current iteration, and T is the maximum number of iterations:

- In the GWO algorithm, the hunting behavior is modeled by assuming that the α, β, and δ wolves possess the best knowledge of the prey's location. These top three wolves guide the search process, and their positions represent the best solutions for the current situation. The remaining ω wolves update their positions based on the guidance of these leader wolves, gradually converging toward the prey (optimal solution). Eqs. (17-19) mathematically describe this behavior, calculating the new positions of ω wolves by averaging the influence of α, β and δ wolves, thereby refining the search and ensuring a coordinated approach toward finding the global optimum:

$$di_\alpha = |c_1 \times x_\alpha - x(t)| \quad (17)$$

$$dis_\beta = \left|c_2 \times x_\beta - x(t)\right| \quad (18)$$

$$dis_\gamma = \left|c_3 \times x_\gamma - x(t)\right| \quad (19)$$

Where c_1, c_2, and c_3 are calculated using Eq. (14):

$$x_{i1}(t) = x_\alpha(t) - a_{i1} \times dis_\alpha(t) \quad (20)$$

$$x_{i2}(t) = x_\beta(t) - a_{i2} \times dis_\beta(t) \quad (21)$$

$$x_{i3}(t) = x_\gamma(t) - a_{i3} \times dis_\gamma(t) \quad (22)$$

From Eqs. (20–22), x_α, x_β and x_γ are the top three solutions, with a_1 , a_2 , a_3 , dis_α , dis_β , and dis_γ calculated accordingly using Eq. (24):

$$x(t+1) = \frac{x_{i1}(t) + x_{i2}(t) + x_{i3}(t)}{3} \quad (24)$$

- In GWO, the attacking phase starts when wolves converge on the prey, marking the hunt's end. This phase is governed by the parameter a, which decreases linearly from 2-0 over iterations, balancing exploration and exploitation. During the first half of the iterations, the focus is on exploration and diversifying the search, while the second half emphasizes exploitation and honing in on optimal areas. Wolves adjust their positions randomly between their current location and the prey's position, refining their approach to achieve the global optimum

In order to attain the maximum iterations (maxiter), GWO iteratively encircles, hunts, and attacks. The search is guided by the optimal wolves (α, β, and δ), who are constantly updating their positions during this procedure. Even though GWO works well, it frequently encounters problems like low population diversity and an unbalanced exploration-exploitation ratio. These issues can cause premature convergence and make it difficult to find the global optimum, particularly in complex problems where preserving diversity and striking a balance between search tactics are essential for best results.

Secure Communication-AES

In 2001, the U.S. National Institute of Standards and Technology (NIST) created the Advanced Encryption Standard (AES) for electronic data encryption. Its greater security over its predecessor, the Data Encryption Standard (DES), and its variations, such as Triple DES (3DES), is why it is so popular today. AES encrypts data in fixed-size blocks and functions as a block cipher. The key sizes that it takes are 128, 192, or 256 bits. There are several rounds to the encryption process, and each round consists of four primary steps:

- SubBytes: Each byte in the block is substituted with another byte using a predefined substitution table (S-box)
- ShiftRows: The rows of the block are shifted cyclically to the left
- MixColumns: Each column of the block is transformed using a matrix multiplication operation
- AddRoundKey: Each byte of the block is combined with a byte of the round key using bitwise XOR

The key size determines how many rounds are completed: A 128-bit key is subjected to 10 rounds, a 192-bit key to 12 rounds, and a 256-bit key to 14 rounds. AES encryption ensures data confidentiality and security, making it suitable for various applications such as wireless security, database encryption, secure communications, and file encryption. Its robustness against cryptographic attacks and its widespread adoption in both hardware and software implementations make it a cornerstone of modern cryptographic systems.

Algorithm 1 outlines the HO-TESRO methodology, integrating IABC for efficient route discovery, CGWAA for trust evaluation, and AES for secure communication.

Algorithm 1: HO-TESRO
1. Initialize network parameters: number of nodes, position, velocity, energy, bandwidth, and trust values. 2. For each node in the network: a. Calculate link stability between nodes using Eq. (1). b. Calculate available bandwidth between nodes using Eq. (2). c. Calculate residual energy using Eq. (3). d. Evaluate the trustworthiness of the node using Eq. (4). 3. Use Improved Artificial Bee Colony (IABC) algorithm for route discovery: a. Randomly initialize ss solutions (routes). b. Generate candidate solutions (routes) using Eq. (8). c. Select the best route based on fitness and Lévy flight enhancement (Eq. (9)). d. If there is no improvement after limit cycles, the scout bee searches for new routes. 4. Use Chaotic Grey Wolf Adaptive Algorithm (CGWAA) for trust evaluation: a. Initialize wolf positions based on the trust values of nodes. b. Update wolf positions Eq. (12) to refine node trustworthiness. c. Introduce chaos using the logistic map to enhance exploration Eqs. (14-15). 5. For selected routes, ensure secure communication using AES encryption Encrypt data packets using AES with a 128-bit key. b. Perform SubBytes, ShiftRows, MixColumns, and AddRoundKey steps. 6. Transmit data through the selected and secure route. 7. Repeat until all data is transmitted or max iterations are reached.

Results and Discussion

Experimental Setup

Using MATLAB, the experiment assessed the Proposed model against Artificial Bee Colony (ABC), Grey Wolf Optimization (GWO), and Chaotic Grey Wolf Adaptive Algorithm (CGWAA). The Proposed model showed clear advantages in all key performance areas. It achieved lower delays, higher detection rates, and better energy efficiency compared to the other models. Additionally, it demonstrated reduced data loss, a longer network lifetime, improved routing accuracy, and higher throughput. These improvements are attributed to the advanced routing and security optimizations integrated into the Proposed model, which collectively enhanced its overall performance and effectiveness.

Overall Performance Evaluation

Tables (1-6) present the performance metrics of various existing optimization algorithms and a proposed model across six key performance indicators. The delay represents the time taken by each algorithm to complete a task. The Proposed model excels with the lowest delays, starting at three units at a time of 5 sec and increasing to 4.562 units at a time of 25 sec. In comparison, GWO shows delays ranging from 17-33.630 units. The Proposed model's efficiency in reducing delay is evident across all time intervals. The detection Rate metric measures the accuracy of detection by the models. The Proposed model achieves the highest detection rates, peaking at 95% at time 5 sec and remaining high at 90.992% at time 25 sec. GWO's detection rate declines significantly from 88-63.964%. The Proposed model's consistently high detection rate indicates superior accuracy and reliability. Energy consumption reflects the efficiency of the algorithms' energy use. The Proposed model demonstrates superior energy efficiency, with values of 92 at time 5 sec and 87.992 at time 25 sec. GWO's energy consumption, in contrast, decreases from 84-48.234, highlighting the Proposed model's effectiveness in managing energy resources more efficiently.

Table 1: Delay

Time (sec)	5	10	15	20	25
GWO	17	20.9432	23.76612	24.03634	33.63082
ABC	15	15.39516	15.41151	15.44701	15.59676
CGWAA	12	14.08176	14.42496	16.52814	17.04283
Proposed	3	3.712693	3.741145	4.00811	4.562057

Table 2: Detection rate

Time (sec)	5	10	15	20	25
GWO	88	71	67.0568	64.23388	63.96366
ABC	90	75	74.60484	74.58849	74.55299
CGWAA	92	80	77.91824	77.57504	75.47186
Proposed	95	92	91.28731	91.25885	90.99189

Table 3: Energy

Time (sec)	5	10	15	20	25
GWO	84	72	55	51.0568	48.23388
ABC	86	71	70.60484	70.58849	70.55299
CGWAA	89	77	74.91824	74.57504	72.47186
Proposed	92	89	88.28731	88.25885	87.99189

Table 4: Loss

Time (sec)	5	10	15	20	25
GWO	0.05	0.182797	0.188522	0.21426	0.237023
ABC	0.01	0.118762	0.129523	0.175376	0.191603
CGWAA	0.02	0.138122	0.155276	0.183937	0.198367
Proposed	0.003889	0.109634	0.139853	0.162453	0.174563

Table 5: Network lifetime

Time (sec)	5	10	15	20	25
GWO	12	29	32.9432	35.76612	36.03634
ABC	20	35	35.39516	35.41151	35.44701
CGWAA	38	50	52.08176	52.42496	54.52814
Proposed	55	58	58.71269	58.74115	59.00811

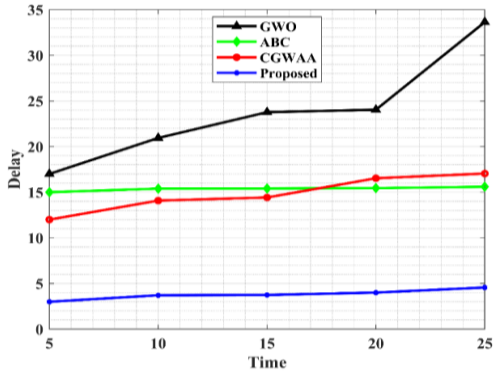
Table 6: Throughput

Time (sec)	5	10	15	20	25
GWO	659	579	509	439	369
ABC	774	694	624	554	484
CGWAA	836	756	686	616	546
Proposed	995	915	845	775	705

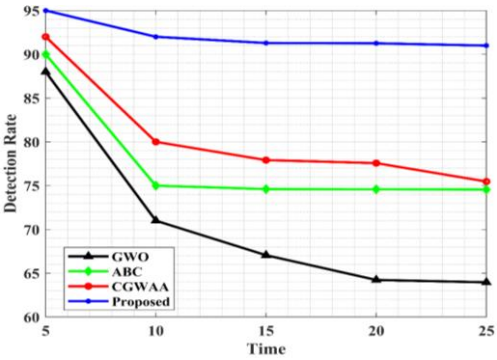
Loss indicates the error or inefficiency in the model's output. The Proposed model has the lowest loss values, with a minimum of 0.003889 at time 5 sec and a maximum of 0.174563 at time 25 sec. GWO's loss values are higher, ranging from 0.05-0.237023. Lower loss values in the Proposed model reflect its higher accuracy and efficiency. Network lifetime measures the operational duration before system failure. The Proposed model leads with an increased network lifetime, from 55 at time 5 sec to 59.008 at time 25 sec. GWO's network lifetime is notably shorter, ranging from 12-36.036. This extended network lifetime signifies the robustness and durability of the Proposed model. Throughput gauges the rate of successful data transmission. The Proposed model achieves the highest throughput, with values like 995 at time 5 sec and 705 at time 25 sec. GWO's throughput ranges from 659-369, indicating that the Proposed model is more effective at handling high data rates.

The Proposed model, which integrates IABC and AES-CGWAA, consistently outperforms the other algorithms across all performance metrics. Its notable achievements include lower delays, higher detection rates, better energy efficiency, minimal loss, extended network lifetime, and superior throughput. These improvements highlight the effectiveness of the advanced optimization strategies embedded in the Proposed model, making it a significant advancement over GWO, ABC, and CGWAA.

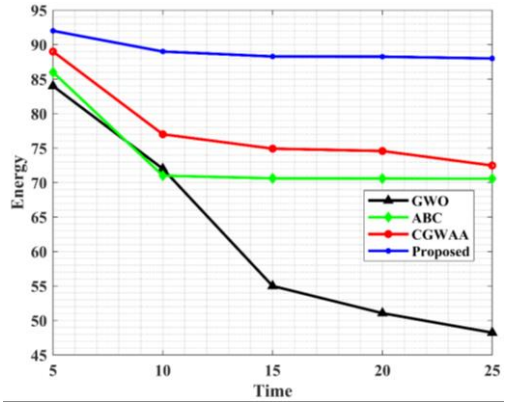
The performance of the proposed model is graphically compared to that of the current models (GWO, ABC, and CGWAA) in Fig (2). It brings attention to important data, including throughput, energy consumption, loss, detection rate, latency, and network lifetime. The Proposed model consistently shows superior performance with lower delays, higher detection rates, and better energy efficiency. The graphical representation clearly illustrates the advantages of the Proposed model over the existing models, emphasizing its enhanced efficiency and effectiveness.



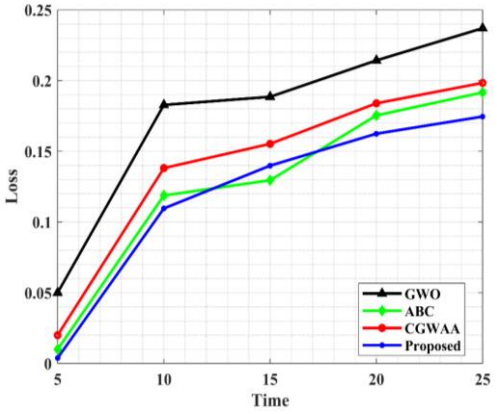
(a)



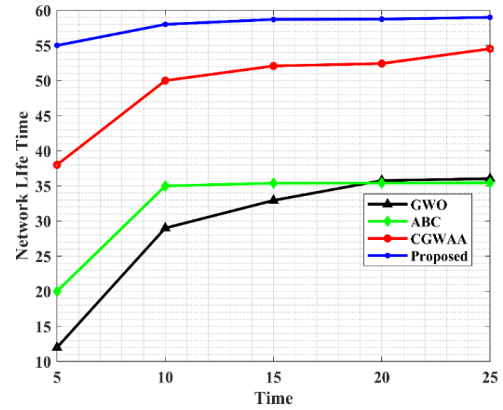
(b)



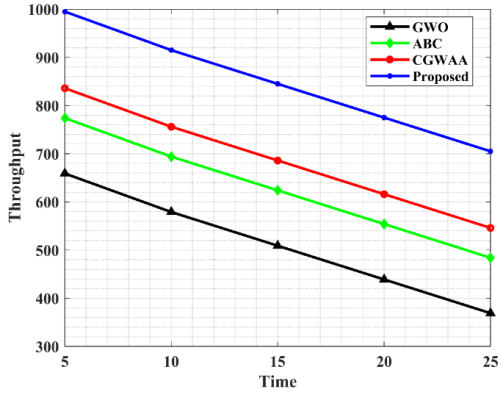
(c)



(d)



(e)



(f)

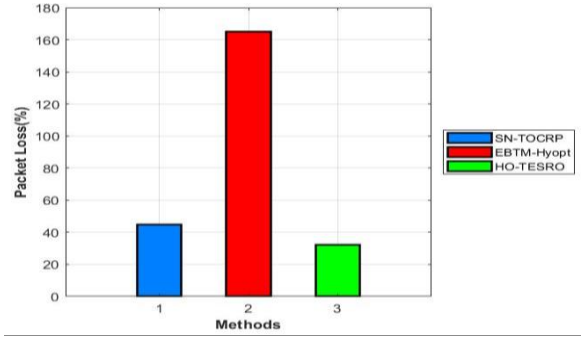
Fig. 2: Proposed and existing model graphical representation

Table (7) provides a comparative analysis of different methods, evaluating them based on key performance metrics such as packet loss, energy consumption, packet delivery ratio, throughput, and delay. The SN-TOCRP (Nirmaladevi and Prabha, 2023) method exhibits minimal packet loss (0.045 kbps) and a high packet delivery ratio (96%). However, it suffers from significantly high energy consumption (88%) and offers a moderate throughput (76 kbps). On the other hand, the EBTM-Hyopt (Narayana *et al.*, 2023) approach demonstrates a higher packet loss (165.6 kbps) and a considerably lower packet delivery ratio (46.34%). Despite these shortcomings, it achieves better throughput (297.99 kbps) and low energy consumption (13%), though it incurs a significant delay (67.49%). Finally, the HO-TESRO model outperforms both with a low packet loss (32 kbps), low energy consumption (10%), and a high packet delivery ratio (97%) while also delivering excellent throughput (320 kbps) and maintaining a moderate delay (35%). Overall, the proposed HO-TESRO model provides a balanced and efficient performance, optimizing energy and network efficiency while minimizing packet loss and delay.

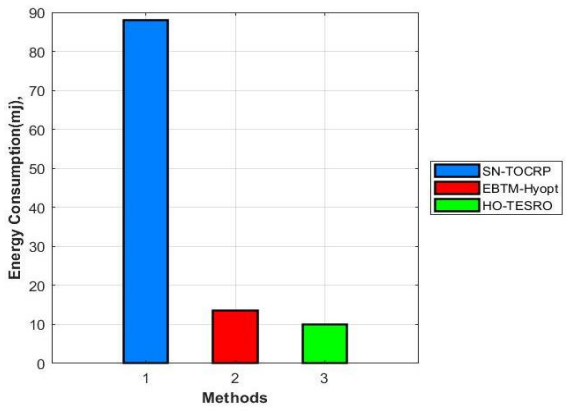
Figure (3) illustrates the comparison between the base paper methods and the proposed model, showcasing their performance across key metrics. The proposed model significantly outperforms the existing methods, particularly in packet delivery ratio, throughput, and energy efficiency, demonstrating improved overall system performance.

Table 7: Base paper comparison with the proposed model

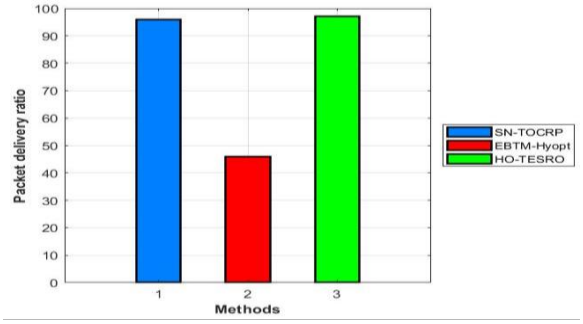
Methods	Pkt Loss (kbps)	Energy consumption (%)	Pkt delivery ratio (%)	Throughput (kbps)	Delay (%)
SN-TOCRP (Nirmaladevi and Prabha, 2023)	0.045	88	96	76	0.425
EBTM-Hyopt (Narayana *et al.*, 2023)	165.6	13	46.34	297.99	67.49
HO-TESRO	32	10	97	320	35



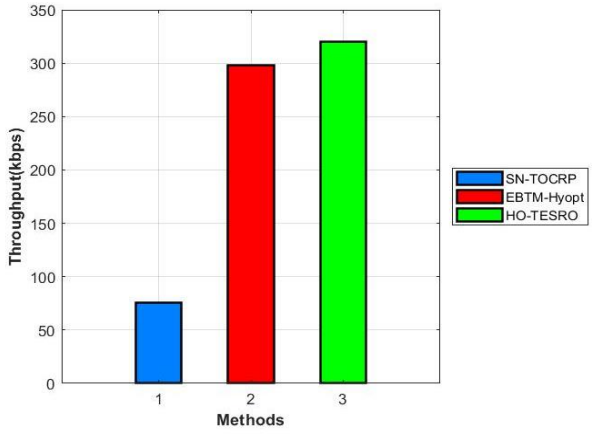
(a)



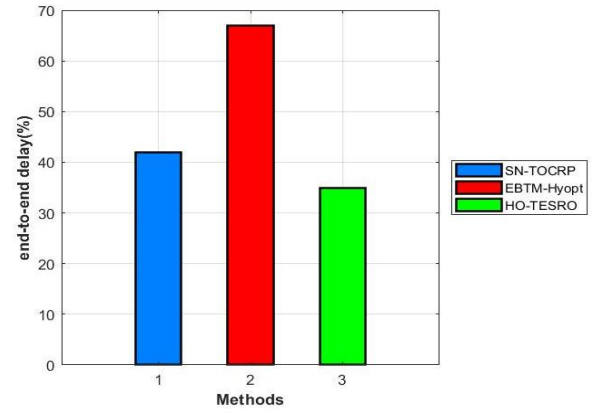
(b)



(c)



(d)



(e)

Fig. 3: Base paper comparison with the proposed model

Conclusion

In order to solve these issues in IoT environments, this article suggested HO-TESRO that integrates metrics including network stability, bandwidth, energy, and trust. The HO-TESRO model used the CGWA) in conjunction with the AES to provide secure communication. The IABC method was implemented to choose the best paths. The AES-CGWAA mechanism verified node keys and shared codes for every data transfer, guaranteeing a secure connection, while the trust-based CGWAA algorithm assessed and chose the most efficient and safe multiple pathways. Comprehensive MATLAB simulations were used to assess the suggested model, and its results were contrasted with those of other methods. Detection rate, packet loss ratio, packet delivery ratio, throughput, and latency all demonstrated significant improvements. These results demonstrated HO-TESRO's effectiveness in tackling the crucial problems of resource allocation and secure routing while offering an IoT-based MANET, a reliable, secure, and energy-efficient routing solution.

Acknowledgment

Generalizability

The evaluation of HO-TESRO can be extended to multiple use cases, including diverse IoT-enabled MANET scenarios like vehicular networks and healthcare systems, to demonstrate adaptability across varied conditions. This will showcase the model's robustness under dynamic network topologies and traffic patterns.

Acknowledgment of Limitations

We acknowledge that the current study is limited to simulation-based analysis and lacks real-world deployment testing. Future work will address scalability and adaptability to highly dynamic IoT environments.

Real-World Impact

The findings are applicable to real-world scenarios, such as smart city infrastructure and IoT healthcare systems, where secure and efficient routing is critical. This underscores the relevance of HO-TESRO in addressing practical challenges like secure data transmission and energy management.

Funding Information

On behalf of all authors, the corresponding author states that they did not receive any funds for this project.

Author's Contributions

Yuvaraja Panneer Selvam: Contributed in software, writing review and editing.

Suganthi Perumal: Involved in conceptualization, formal analysis and writing original draft.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and that no ethical issues are involved.

Conflicts of Interest

The authors declare that we have no conflict of interest.

Data Availability

All the data is collected from the simulation reports of the software and tools used by the authors. Authors are working on implementing the same using real-world data with appropriate permissions.

References

And, I. A. A. E.-M., & Darwish, S. M. (2021). Towards Designing a Trusted Routing Scheme in Wireless Sensor Networks: A New Deep Blockchain Approach. *IEEE Access*, *9*, 103822–103834. https://doi.org/10.1109/access.2021.3098933

Awan, S., Javaid, N., Ullah, S., Khan, A. U., Qamar, A. M., & Choi, J.-G. (2022). Blockchain Based Secure Routing and Trust Management in Wireless Sensor Networks. *Sensors*, *22*(2), 411. https://doi.org/10.3390/s22020411

Deebak, B. D., & Al-Turjman, F. (2020). A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks. Ad Hoc Networks, 97, 102022. https://doi.org/10.1016/j.adhoc.2019.102022

Hajiee, M., Fartash, M., & Osati Eraghi, N. (2021). An Energy-Aware Trust and Opportunity Based Routing Algorithm in Wireless Sensor Networks Using Multipath Routes Technique. *Neural Processing Letters*, *53*(4), 2829–2852. https://doi.org/10.1007/s11063-021-10525-7

Han, Y., Hu, H., & Guo, Y. (2022). Energy-Aware and Trust-Based Secure Routing Protocol for Wireless Sensor Networks Using Adaptive Genetic Algorithm. *IEEE Access*, *10*, 11538–11550. https://doi.org/10.1109/access.2022.3144015

Hu, H., Han, Y., Yao, M., & Song, X. (2022). Trust Based Secure and Energy Efficient Routing Protocol for Wireless Sensor Networks. *IEEE Access*, *10*, 10585–10596. https://doi.org/10.1109/access.2021.3075959

Kalidoss, T., Rajasekaran, L., Kanagasabai, K., Sannasi, G., & Kannan, A. (2020). QoS Aware Trust Based Routing Algorithm for Wireless Sensor Networks. *Wireless Personal Communications*, *110*(4), 1637–1658. https://doi.org/10.1007/s11277-019-06788-y

Kaur, G., & Kakkar, D. (2022). Hybrid optimization enabled trust-based secure routing with deep learning-based attack detection in VANET. *Ad Hoc Networks*, *136*, 102961. https://doi.org/10.1016/j.adhoc.2022.102961

Khot, P. S., & Naik, U. (2021). Particle-Water Wave Optimization for Secure Routing in Wireless Sensor Network Using Cluster Head Selection. *Wireless Personal Communications*, *119*(3), 2405–2429. https://doi.org/10.1007/s11277-021-08335-0

Mittal, N., Singh, S., Singh, U., & Salgotra, R. (2021). Trust-aware energy-efficient stable clustering approach using fuzzy type-2 Cuckoo search optimization algorithm for wireless sensor networks. *Wireless Networks*, *27*(1), 151–174. https://doi.org/10.1007/s11276-020-02438-5

Nagaraju, R., C, V., J, K., G, M., Goyal, S. B., Verma, C., Safirescu, C. O., & Mihaltan, T. C. (2022). Secure Routing-Based Energy Optimization for IoT Application with Heterogeneous Wireless Sensor Networks. *Energies*, *15*(13), 4777. https://doi.org/10.3390/en15134777

Narayana, M. V., Pradeep Kumar, V., Kumar Nanda, A., Rao Jalla, H., & Reddy Chavva, S. (2023). Enhanced Energy Efficient with a Trust Aware in MANET for Real-Time Applications. *Computers, Materials & Continua*, *75*(1), 587–607. https://doi.org/10.32604/cmc.2023.034773

Nirmaladevi, K., & Prabha, K. (2023). A selfish node trust aware with Optimized Clustering for reliable routing protocol in Manet. *Measurement: Sensors*, *26*, 100680. https://doi.org/10.1016/j.measen.2023.100680

Ourouss, K., Naja, N., & Jamali, A. (2021). Defending Against Smart Grayhole Attack within MANETs: A Reputation-Based Ant Colony Optimization Approach for Secure Route Discovery in DSR Protocol. *Wireless Personal Communications*, *116*(1), 207–226. https://doi.org/10.1007/s11277-020-07711-6

Ramamoorthy, R., & Thangavelu, M. (2022). An enhanced hybrid ant colony optimization routing protocol for vehicular ad-hoc networks. *Journal of Ambient Intelligence and Humanized Computing*, *13*(8), 3837–3868. https://doi.org/10.1007/s12652-021-03176-y

Rodrigues, P., & John, J. (2020). Joint trust: an approach for trust-aware routing in WSN. *Wireless Networks*, *26*(5), 3553–3568. https://doi.org/10.1007/s11276-020-02271-w

Selvi, M., Thangaramya, K., Ganapathy, S., Kulothungan, K., Khannah Nehemiah, H., & Kannan, A. (2019). An Energy Aware Trust Based Secure Routing Algorithm for Effective Communication in Wireless Sensor Networks. *Wireless Personal Communications*, *105*(4), 1475–1490. https://doi.org/10.1007/s11277-019-06155-x

Shende, D. K., & Sonavane, S. S. (2020). CrowWhale-ETR: CrowWhale optimization algorithm for energy and trust aware multicast routing in WSN for IoT applications. *Wireless Networks*, *26*(6), 4011–4029. https://doi.org/10.1007/s11276-020-02299-y

Shi, Q., Qin, L., Ding, Y., Xie, B., Zheng, J., & Song, L. (2019). Information-Aware Secure Routing in Wireless Sensor Networks. *Sensors*, *20*(1), 165. https://doi.org/10.3390/s20010165

Srilakshmi, U., Alghamdi, S. A., Vuyyuru, V. A., Veeraiah, N., & Alotaibi, Y. (2022). A Secure Optimization Routing Algorithm for Mobile Ad Hoc Networks. *IEEE Access*, *10*, 14260–14269. https://doi.org/10.1109/access.2022.3144679

Srilakshmi, U., Veeraiah, N., Alotaibi, Y., Alghamdi, S. A., Khalaf, O. I., & Subbayamma, B. V. (2021). An Improved Hybrid Secure Multipath Routing Protocol for MANET. *IEEE Access*, *9*, 163043–163053. https://doi.org/10.1109/access.2021.3133882

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

Tangade, S., Manvi, S. S., & Lorenz, P. (2020). Trust Management Scheme Based on Hybrid Cryptography for Secure Communications in VANETs. *IEEE Transactions on Vehicular Technology*, *69*(5), 5232–5243. https://doi.org/10.1109/tvt.2020.2981127

Veeraiah, N., & Krishna, B. T. (2022). An approach for optimal-secure multipath routing and intrusion detection in MANET. *Evolutionary Intelligence*, *15*(2), 1313–1327. https://doi.org/10.1007/s12065-020-00388-7

Veeraiah, N., Ibrahim Khalaf, O., Prasad, C. V. P. R., Alotaibi, Y., Alsufyani, A., Alghamdi, S. A., & Alsufyani, N. (2021). Trust Aware Secure Energy Efficient Hybrid Protocol for MANET. *IEEE Access*, *9*, 120996–121005. https://doi.org/10.1109/access.2021.3108807

Vinitha, A., Rukmini, M. S. S., & Dhirajsunehra. (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

Wang, X., Zhang, P., Du, Y., & Qi, M. (2020). Trust Routing Protocol Based on Cloud-Based Fuzzy Petri Net and Trust Entropy for Mobile Ad hoc Network. *IEEE Access*, *8*, 47675–47693. https://doi.org/10.1109/access.2020.2978143

Zhang, X., Deng, H., Xiong, Z., Liu, Y., Rao, Y., Lyu, Y., Li, Y., Hou, D., & Li, Y. (2024). Secure Routing Strategy Based on Attribute-Based Trust Access Control in Social-Aware Networks. *Journal of Signal Processing Systems*, *96*(2), 153–168. https://doi.org/10.1007/s11265-023-01908-1