sciendo
ISSN 1335-8871
MEASUREMENT SCIENCE REVIEW
Journal homepage: https://content.sciendo.com

A Novel Scalable Trust-Aware Deep Reinforcement Learning Algorithm for Energy-Efficient and Secure Routing in Software-Defined Wireless Sensor Networks for IoT

Jasmine Alponse[1], Yaashuwanth C[1*], Prathibanandhi K[2]

[1]*Department of Information Technology, Sri Venkateswara College of Engineering, Sriperumbudur, India, jasmine.alponse@gmail.com, yaashuwanth@gmail.com*
[2]*Department of Electrical and Electronics Engineering, Sri Sairam Engineering College, Chennai, India, prathiraj90@gmail.com*

Abstract: Wireless Sensor Networks (WSNs) are the backbone of Internet of Things (IoT) ecosystems, but they remain constrained by limited energy, dynamic topologies, and increasing security threats. Conventional metaheuristic-based routing protocols typically optimize either energy efficiency or security, but rarely achieve both in a scalable manner. To address this research gap, we propose a trust-aware Software Defined Wireless Sensor Network (SDWSN) framework that integrates the Coati Optimization Algorithm (COA) for multi-objective routing with a hyperelliptic curve (HEC)-based blind signcryption scheme for lightweight yet robust data security. The novelty of this work lies in the joint optimization of energy, delay, trust, and hop count while simultaneously ensuring confidentiality, integrity, and anonymity through blind signcryption. Unlike traditional ECC and RSA, the proposed HEC-based scheme reduces computational complexity, making it suitable for resource-constrained IoT devices. The architecture leverages software-defined networking (SDN) programmability and the OpenFlow protocol to dynamically adapt routes based on real-time trust and energy metrics. Simulation results in NS-3 show that the proposed COA-HEC model significantly outperforms existing schemes (SEHR, IBFA, ESMR, GMPSO) by improving throughput (18.8 %–59.4 %), packet delivery ratio (by 4.8 %–12.4 %), and reducing average delay (up to 61 %) and energy consumption. The proposed framework establishes a scalable and secure routing paradigm for real-time IoT applications such as industrial automation, healthcare monitoring, and smart cities, thus advancing the state of the art in trust-aware SDWSNs.

Keywords: Coati Optimization Algorithm, blind signcryption, OpenFlow protocol, trust and energy, delay and hop

1. INTRODUCTION

The exponential growth of the Internet of Things (IoT) has transformed conventional communication paradigms by interconnecting billions of smart devices for real-time monitoring [2], data processing, and control across various domains, such as smart homes, healthcare, and industrial automation. [3]. However, this proliferation introduces significant challenges regarding energy efficiency, trust, and security in Wireless Sensor Networks (WSNs), which form the foundational infrastructure of IoT ecosystems [11]. These challenges are further magnified by limited energy resources, node heterogeneity, and susceptibility to malicious attacks [4]. To address these issues, software-defined networking (SDN) has emerged as a promising paradigm, decoupling the control and data planes to enhance programmability and centralized network management in WSNs, thus forming Software-Defined Wireless Sensor Networks (SDWSNs) [1]. Trust-aware SDWSNs integrate trust evaluation mechanisms into the SDN architecture to ensure that data are transmitted through reliable nodes, thereby mitigating the risks associated with node compromise and untrusted behaviors [17]. Moreover, the OpenFlow protocol has been widely adopted in SDWSNs to dynamically manage routing paths based on real-time network conditions, significantly improving network adaptability and performance. Among various intelligent optimization techniques, the Coati Optimization Algorithm (COA), inspired by the cooperative foraging behavior of coatis, offers a biologically inspired method for achieving energy-aware and trust-based routing decisions. The algorithm efficiently balances exploration and exploitation in selecting optimal routes by minimizing energy consumption, while maximizing trust scores among participating nodes. The COA has shown promise in enhancing reliability, reducing latency, and supporting scalability in dynamic IoT environments. Especially in time-sensitive applications, such as smart cities and industrial control systems, COA can ensure robust performance by dynamically adjusting routes based on changing network and trust metrics. To further strengthen the security of transmitted

DOI: 10.2478/mr-2025-0039

*Corresponding author: yaash_it@rediffmail.com (Yaashuwanth C) data, Blind Signcryption, an amalgamation of digital signature and encryption, is integrated within the SDWSN architecture. This mechanism not only ensures data confidentiality and integrity, but also provides anonymity by concealing the sender's identity, thus meeting the stringent privacy requirements of IoT communication. The use of hyperelliptic curve (HEC) cryptography in blind signcryption improves computational efficiency and strengthens security, especially for resource-constrained IoT devices [6]. Despite advancements in optimization and security protocols for WSNs, three critical gaps remain: 1) Partial optimization – most approaches optimize only energy or delay while neglecting trust and security; 2) Security limitations – cryptographic mechanisms like ECC and RSA introduce high computational overhead unsuitable for IoT; 3) Scalability issues – traditional metaheuristics struggle to adapt in large heterogeneous SDWSNs.

2. RELATED WORKS

Recent research on WSN optimization has highlighted various meta-heuristic approaches to improve energy efficiency and security. Amir et al. [5] introduced Ex-GWO and I-GWO protocols that prioritize energy conservation by considering residual energy, distance, and traffic load in route selection. Similarly, Singh et al. [8] developed a fuzzy Gray Wolf Optimizer (GWO) with opportunistic routing to minimize power expenditure, and GirijaVani et al. [7] proposed the SEAMHR protocol, which enhances security through meta-heuristic analysis and counter mode cryptography. Mauro Conti et al. [13] further contributed with SARP, a scalable and secure IoT routing protocol that prevents insider attacks while maintaining energy efficiency. Khalid Haseeb et al. [9] designed the Secure and Energy-Aware Heuristic-Based Routing (SEHR) protocol to optimize energy and resource routing decisions while protecting against unauthorized malicious attacks. In another study, Haseeb et al. [10] presented an energy-efficient and secure multi-hop routing protocol (ESMR). Majid Alotaibi [12] implemented the Improved Blowfish Algorithm (IBFA) in conjunction with the Crossover Mutated Marriage in Honey Bee (CM-MH) model for encryption, decryption, optimal route determination, and encoding processes.

Table 1. Summary of key related works and their limitations.

Method / Protocol	Optimization technique	Security mechanism	Parameters considered	Limitations
Ex-GWO, I-GWO [5]	GWO variants	None	Energy, distance, traffic load	Poor adaptability in dynamic networks, high complexity
Fuzzy-GWO [8]	Hybrid fuzzy + GWO	None	Energy efficiency	Performance degradation in heterogeneous networks
SEAMHR [7]	Metaheuristic analysis	Counter-mode cryptography	Delay, energy, security	Security issues due to CTR reuse, high overhead
SEHR [9]	Heuristic-based routing	Lightweight cryptography	Energy-aware routing	Integrity flaws, limited energy optimization
ESMR [10]	Secret sharing	Key sharing + multi-hop	Energy, security	No mobility support, ignores QoS metrics
IBFA [12]	Blowfish with CM-MH	Symmetric encryption	Energy, security	No authentication, high complexity, vulnerable patterns
GMPSO [16]	Genetic mutation PSO	None	Energy efficiency, throughput	High controller overhead, ignores trust, longer flow times
BOA-ACO [15]	BOA + ACO	None	Cluster-head routing, energy	No built-in security, limited scalability
IEE-LEACH [20]	Improved LEACH hybrid routing	None	Energy	Focuses only on lifespan, no security
HPSO-ILEACH [18]	PSO + Improved LEACH	None	Energy aggregation	Lacks robust trust/security
PSOGA [14]	PSO + GA hybrid	None	Energy, packet transmission	Limited scalability, no lightweight security

Yao et al. [19] proposed an adaptive particle swarm optimization ensemble and genetic mutation-based routing for selecting control nodes in IoT-enabled software-defined WSNs. Prachi et al. [15] developed the Butterfly Optimization Algorithm (BOA) to select optimal cluster heads from sets of nodes. Yang Liu et al. [20] presented IEE-LEACH to address the energy consumption challenges of the LEACH protocol in WSNs. Sharmin et al. [18] introduced an approach to enhance energy efficiency and network longevity in WSNs by developing a solution using HPSO and ILEACH for Cluster Head selection during data aggregation. Mukesh Mishra et al. [14] proposed a multi-objective optimization method to ensure efficient packet transmission from source to sink or base station. This approach [21] uses a novel hybrid algorithm, PSOGA, which combines particle swarm optimization and genetic algorithms to determine optimal data transmission paths. Esau Taiwo et al. [6] proposed a new Wireless Sensor Network model using multicore WS clustering to reduce power consumption. Table 1 compares existing approaches with the proposed COA-HEC framework. In contrast, the proposed COA-HEC framework integrates the exploration–exploitation efficiency of COA, a Bayesian trust model for node reliability, and HEC-based blind signcryption [22] for lightweight secure communication [23]. This unique integration ensures not only efficient and adaptive routing, but also robust confidentiality, integrity, and anonymity, making it particularly suitable for large-scale, dynamic IoT environments [24] and smart city infrastructures.

The methodological innovations of this work are based on the integration of three key components:

- A COA-based multi-objective routing mechanism,
- A Bayesian trust model that combines interaction and efficiency trust, and
- A HEC-based blind signcryption scheme for lightweight, secure communication.

The motivation for these choices arises from the limitations identified in existing approaches, where optimization is often only partial (energy- or delay-centric), cryptographic techniques such as ECC and RSA result in high computational costs, and scalability in large, heterogeneous SDWSNs remains a persistent challenge.

3. PROPOSED FRAMEWORK

The framework establishes a separation between control management logic and data, comprising three layers: application, control, and information. The application layer contains definitions, objectives, services, and network operations, while the control layer handles administration, configuration, and forwarding node selection. Fig. 1 shows the system architecture of the proposed model, with nodes featuring three modules and a controller with three primary modules.

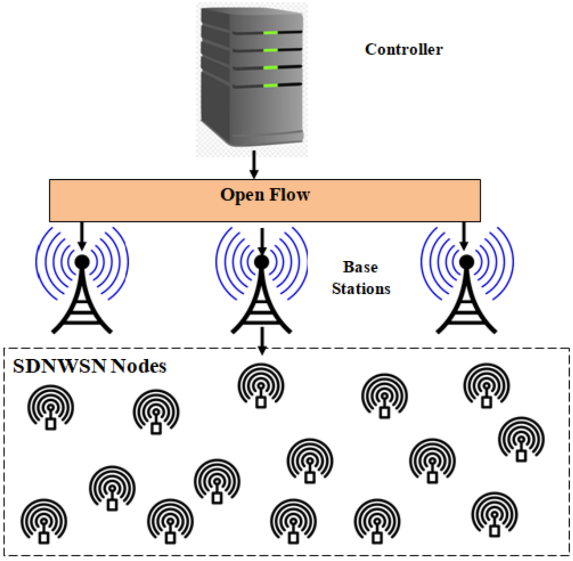

Fig. 1. Proposed system model overview.

The proposed algorithm, shown in Fig. 2, defines an objective function to enable diverse, trust-based routing. The proposed system includes three node modules and three principal controller modules. The data plane incorporates discovery modules for the BS, adjacent nodes, and the controller, while the controller contains modules for topology discovery, link discovery, and virtual routing.

A. Discovery modules in data plane

The proposed methodology combines neighbor discovery, base station (BS) identification, and controller recognition into a unified module using a singular broadcast message disseminated by the controller. This broadcast communication includes the sender's identification, remaining energy levels, and hop count to the base station. Neighboring nodes use this information to populate their respective tables and build a three-dimensional array (TDA[n][n][2]) that records the proximity, energy metrics, and hop counts of neighbors. This strategy effectively reduces communication overhead and energy consumption compared to traditional multi-message approaches.

B. Link discovery module

This module efficiently identifies and monitors node interconnections. Instead of transmitting comprehensive neighbor lists, nodes share information only about neighbors with lower identification numbers. This data, stored in the same TDA array, avoids redundancy and allows the controller to determine the existence of links. The architecture supports bidirectional link configuration.

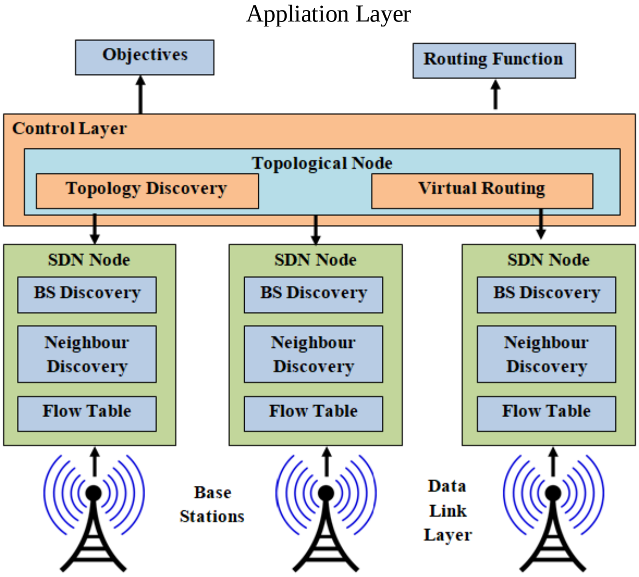

Fig. 2. Proposed system architecture for SDWSN.

C. Topology discovery module

Leveraging the global perspective gained from the preceding modules, the controller systematically constructs and maintains the network topology by clustering nodes and identifying common nodes within clusters. Since the nodes are static, the topology remains stable until the energy of the nodes is depleted.

D. Routing module

This module determines optimal routing pathways based on application-specific quality of service (QoS) requirements. The controller selects the next hop by evaluating node trust, proximity to the base station, and residual energy levels to ensure efficient and reliable data transmission.

E. Trust calculation

Trust estimation is essential for maintaining secure and reliable communication in SDWSN. The proposed trust model evaluates node behavior using two key components: interaction trust and efficiency trust, each tailored for both control and data traffic. By employing a lightweight Bayesian approach, the model accurately quantifies trust, enabling the identification and exclusion of malicious nodes and thereby enhancing network security. This is modeled by the expectation of the beta distribution:

$$T_{ij}^{\mathrm{int}} = \frac{s_{ij} + 1}{s_{ij} + f_{ij} + 2} \tag{1}$$

where T_{ij}^{int} is the interaction trust value, ranging from 0 to 1. If n_{ij}^{forw} denotes the number of packets correctly forwarded by neighbor j, and n_{ij}^{recv} is the total number of packets sent to j, efficiency trust is calculated as:

$$T_{ij}^{\mathrm{eff}} = \frac{n_{ij}^{\mathrm{forw}}}{n_{ij}^{\mathrm{recv}}} \tag{2}$$

To capture both behavioral aspects, the combined regional trust T_{ij} for routing purposes is given by a weighted sum:

$$T_{ij} = \alpha T_{ij}^{\mathrm{int}} + (1 - \alpha)\, T_{ij}^{\mathrm{eff}} \tag{3}$$

where $0 \le \alpha \le 1$ balances the importance of interaction and efficiency trust. The energy consumed in transmitting J bits over a distance d follows the LEACH model:

$$E_{tx} = \begin{cases} J \cdot E_{\mathrm{elec}} + J \cdot \epsilon_{fs} \cdot d^2, & \text{if } d < d_0 \\ J \cdot E_{\mathrm{elec}} + J \cdot \epsilon_{mp} \cdot d^4, & \text{if } d \ge d_0 \end{cases} \tag{4}$$

where E_{elec}, ϵ_{fs}, and ϵ_{mp} are hardware parameters, and d_0 is the threshold between channels. Additionally, the end-to-end delay for a path from source c to sink s is evaluated as the sum of per-hop latencies:

$$D_{c \to s} = \sum_{k=1}^{N} d_k \tag{5}$$

F. Proposed Coati Optimization Algorithm

This proposed algorithm can applied in smart home environments, including applications such as home sensors. It represents the weight of the j^{th} node in routing as the next node of the i^{th} node. The objective function (4), which considers delay, energy, trust, and distance, is provided as input to the COA, which selects the optimal forwarding node based on the decisions made by the COA algorithm.

$$OB_j = \frac{\delta_1 \cdot LT_{ij} + \delta_2 \cdot Dist_j + \delta_3 \cdot D_{c \to s}}{\delta_4 * ER_j} \tag{6}$$

where $\delta_1, \delta_2, \delta_3,\ and\ \delta_4$ are relative coefficients with $\delta_1 + \delta_2 + \delta_3 + \delta_4 = 1$. $Dist_j$ represents the distance between the BS and the neighbor node j. The COA is an optimization technique that uses a population of coatis to search for a solution to a given problem. Each coati has a location in the search space (SS), corresponding to a set of values for the decision variables. This position serves as a potential solution to the problem. The starting point of the COA is determined using (6) through random initialization of the positions of the coatis.

$$X_i : x_{i,j} = lb_j + r \cdot \left(ub_j - lb_j\right), \quad i = 1,2, \ldots N, j = 1,2, \ldots m \tag{7}$$

The coatis population in COA is mathematically represented using the matrix “X" called the population matrix.

$$X = \begin{bmatrix} x_{1,1} & \cdots & x_{1,m} \\ \vdots & \ddots & \vdots \\ x_{N,1} & \cdots & x_{N,m} \end{bmatrix}_{N*M} \tag{8}$$

Candidate solutions (CSs) are positioned in the decision variables, leading to the assessment of different values for the problem’s objective function, as shown in (9).

$$F = \begin{bmatrix} F_1 \\ \vdots \\ F_i \\ \vdots \\ F_N \end{bmatrix}_{N*1} = \begin{bmatrix} F(X_1) \\ \vdots \\ F(X_i) \\ \vdots \\ F(X_N) \end{bmatrix}_{N*1} \tag{9}$$

In the proposed meta-heuristic algorithm, the quality of the CS determines the outcome of the objective function, with the optimal member selected accordingly. The mathematical foundation of COA lies in population-based optimization inspired by natural cooperative behaviors. This approach accounts for topological and energy constraints to achieve optimal routing.

Phase 1: Hunting as well as attacking strategy on iguana (exploration)

The initial stage of population updating in SS is modeled by simulating the coatis’ attacking approach on iguanas. A group of coatis climbs a tree to capture an iguana and frighten it. This causes the coatis to move to various locations in SS, demonstrating exploration capability in the global search. In the COA design, the location of the best member is identified as the iguana’s location. The positions of the coatis climbing the tree are given by (10), representing the diversification of node selection.

$$X_i^{p1} : x_{i,j}^{p1} = x_{i,j} + r \cdot \left(Ig_j - I \cdot x_{i,j}\right), \quad i = 1,2, \ldots \left\lfloor \frac{N}{2} \right\rfloor, j = 1,2..m \tag{10}$$

Once an iguana falls to the ground, it relocates to a random position in SS. Depending on these random locations, the coatis found on the ground move within SS as described below. They move based on random positions, ensuring broader exploration of the SS as in (11) and (12)

$$Ig^G: Ig_j^G = lb_j + r \cdot \left(ub_j - lb_j\right), j = 1,2, \dots m \tag{11}$$

$$X_i^{P1}: x_{i,j}^{P1} = \begin{cases} x_{i,j} + r \cdot \left(Ig_j^G - I \cdot x_{i,j}\right), F_{Ig^G} < F_i \\ x_{i,j} + r \cdot \left(x_{i,j} - Ig_j^G\right), \quad \text{else} \end{cases} \tag{12}$$

A new position determined for each coati is accepted for updating if it improves the value of the objective function (better path). Otherwise, the coati remains in its previous location. The update condition is determined using (13) for $i = 1, 2, \dots, N$.

$$X_i = \begin{cases} X_i^{P1}, F_i^{P1} < F_i \\ X_i \quad \text{else} \end{cases} \tag{13}$$

Phase 2: Escaping from predators (exploitation)

The next stage involves updating the location of coatis in SS, which is mathematically modeled based on the natural behavior of coatis when facing and escaping predators. To simulate this behavior, an arbitrary location is generated near the current location of each coati using (14) and (15).

$$lb_j^{\text{local}} = \frac{lb_j}{t}, ub_j^{\text{local}} = \frac{ub_j}{t} \tag{14}$$

$$x_{i,j}^{P2} = x_{i,j} + (1 - 2r) \cdot \left(lb_j^{\text{local}} + r \cdot \left(ub_j^{\text{local}} - lb_j^{\text{local}}\right)\right), \quad i = 1,2,..N, j = 1,2,..m \tag{15}$$

The newly considered location is accepted if it increases the objective function value (16),

$$X_i = \begin{cases} X_i^{P2}, \quad F_i^{P2} < F_i \\ X_i, \quad \text{else} \end{cases} \tag{16}$$

A HEC-based blind signcryption scheme is proposed (illustrated in Fig. 3) to ensure secure data routing between sensor nodes and the BS in WSNs. The scheme guarantees sender anonymity, reduces computational and communication costs, and involves three participants: the controller, the sender node, and the BS, across four stages: setup, key generation, blind signcryption, and unsigncryption.

Setup stage:

The controller selects a finite field $\mathbb{F}\_q$ and a divisor D of the HEC, chooses $n \in \mathbb{Z}_q *$, and computes the public–private key pair:

$$P_{\text{pub}} = nD$$

$$P_{\text{priv}} = n$$

Key generation:

The controller sends $(P_{\text{pub}}, P_{\text{priv}})$ to the requesting sensor node via a secure channel.

Blind signcryption:

The sender selects two random values $r_1, r_2 \in \mathbb{Z}_q *$ and computes:

$$K = r_1 P_{\text{pub}},$$

$$C = M \oplus H_1(K),$$

$$s = r_2 + H_2(C) \cdot P_{\text{priv}} (\text{mod } q)$$

The blind message (C, s) is sent to the controller for signing without revealing M. The controller signs blindly:

$$\sigma = s \cdot P_{\text{pub}}$$

The sender unblinds and forwards (C, σ) to BS.

Unsigncryption:

BS verifies validity by checking:

$$H_2(C) = H_2(M \oplus H_1(K)),$$

If valid, the message is accepted; otherwise, it is rejected. The HEC-based approach offers higher security with smaller key sizes compared to traditional ECC, making it well-suited for resource-constrained WSN environments. The proposed framework incorporates COA, HEC-based signcryption, and trust-aware routing to optimize secure and energy-efficient data transmission within WSNs. Dynamic selection of the cluster head is enabled by the global search efficiency of COA and low overhead. This approach combines the advantages of each approach to provide a comprehensive solution. Simulation results verify our approach's performance advantage across various metricscompared to existing configurations. HEC-based blind signcryption is preferred over traditional lightweight cryptographic algorithms such as ECC, RSA, or AES due to its efficient computational balance.

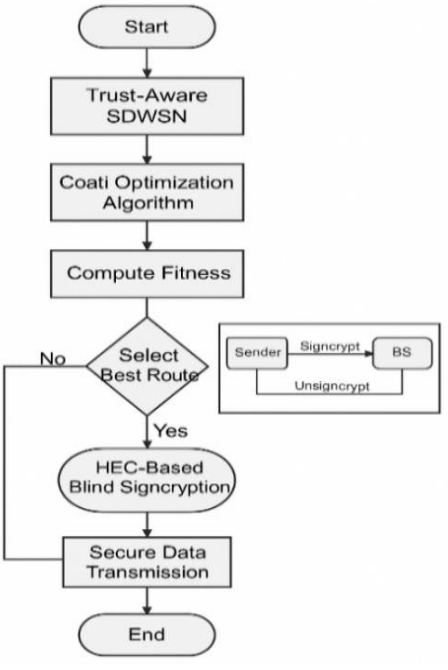

Fig. 3. COA–HEC secure routing flowchart.

4. Results and discussion

The proposed model was analyzed using the NS3 simulator. Various metrics were evaluated to compare the COAHBS scheme with the SEHR and IBFA models: including computational cost, packet delivery ratio, average delay, average throughput, network lifetime, packet loss, communication overhead, and energy consumption. The simulation parameters used in this research are summarized in Table 2. The analysis indicates that COAHBS achieves optimal performance in terms of energy efficiency, packet delivery ratio, minimized packet loss, and reduced computational costs.

Table 2. Details of simulation parameters setup.

Parameter	Values
Simulator model	NS-3.26
Sensor nodes count	50, 100, 150, 200, 250
Simulation area	500×500 m
Optimal path finding protocol	COA
SDN controller count	1
Base station	3
Size of packet	512 bytes
Initial energy	50 J
Simulation time	300 sec
Transmission range	250 m

As shown in Fig. 4 and Table 3, COAHBS consistently outperformed other protocols, achieving an average throughput of 75.6 %, surpassing SEHR, IBFA, ESMR, and GMPSO by 18.8 % - 59.4 %. This improvement is attributed to multi-objective path selection that optimizes trust, delay, hop count, and energy.

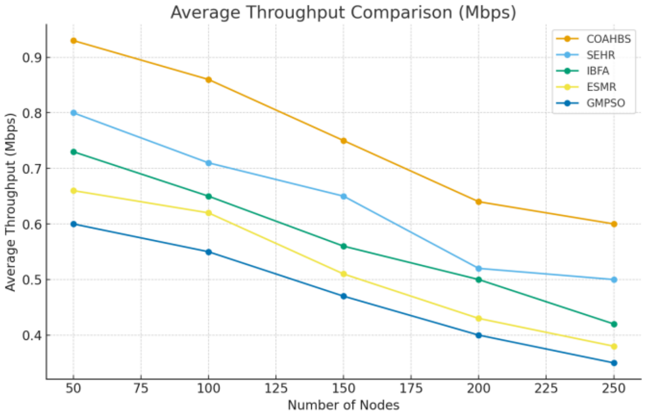

Fig. 4. Average throughput analysis.

Table 3. Average throughput comparison [Mbps].

Nodes	COAHBS	SEHR	IBFA	ESMR	GMPSO
50	0.93	0.80	0.73	0.66	0.60
100	0.86	0.71	0.65	0.62	0.55
150	0.75	0.65	0.56	0.51	0.47
200	0.64	0.52	0.50	0.43	0.40
250	0.60	0.50	0.42	0.38	0.35

Fig. 5 and Table 4 show that COAHBS maintained the highest packet delivery ratio (PDR) across various node densities, averaging 88.8 %, compared to SEHR 84 %, IBFA 81.4 %, ESMR 77.8 %, and GMPSO 76.4 %. This improvement results from reduced route failures and improved route reliability.

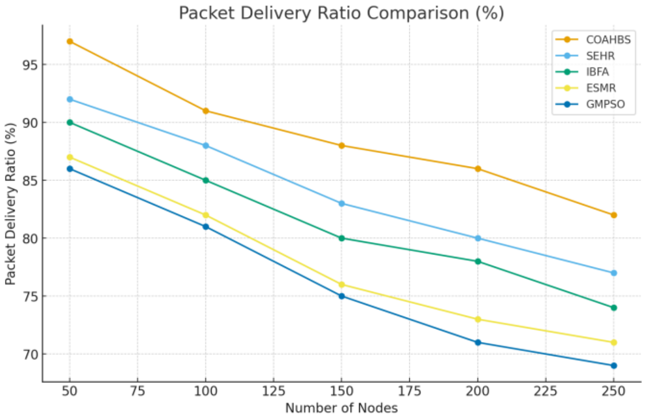

Fig. 5. Analysis of PDR.

Table 4. PDR comparison [%].

Nodes	COAHBS	SEHR	IBFA	ESMR	GMPSO
50	97	92	90	87	86
100	91	88	85	82	81
150	88	83	80	76	75
200	86	80	78	73	71
250	82	77	74	71	69

COAHBS exhibited the lowest delay among all approaches (average 4.83 ms) across all node counts (Fig. 6, Table 5). It achieved a delay reduction of up to 61 % compared to GMPSO, enabling faster data transmission through optimal route selection based on trust and hop-count criteria.

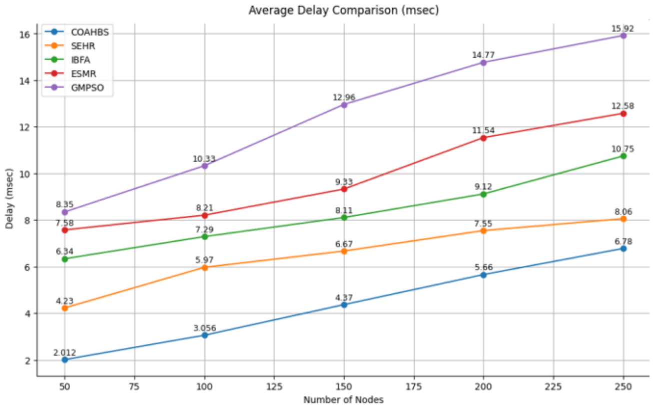

Fig. 6. Average delay analysis.

Table 5. Evaluation of average delay comparison [msec].

Nodes	COAHBS	SEHR	IBFA	ESMR	GMPSO
50	2.012	4.23	6.34	7.58	8.35
100	3.056	5.97	7.29	8.21	10.33
150	4.37	6.67	8.11	9.33	12.96
200	5.66	7.55	9.12	11.54	14.77
250	6.78	8.06	10.75	12.58	15.92

Fig. 7 and Table 6 show that COAHBS was the most energy-efficient protocol, with energy consumption rising from 0.23 J to 0.63 J as the node count increased from 50 to 250, which is significantly lower than that of alternative protocols. This represents a 173.91 % increase, which is considerably more efficient than GMPSO's maximum increase of 160.53 %.

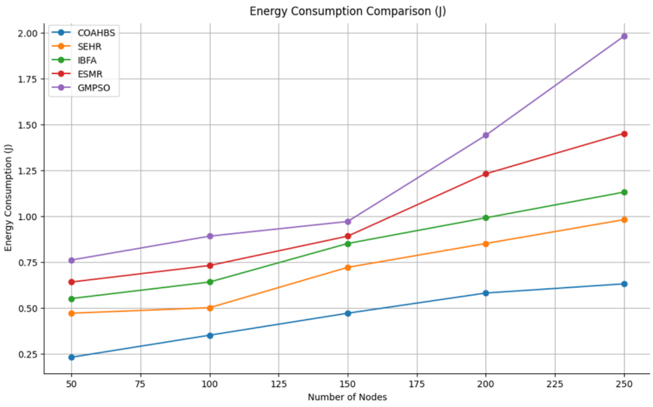

Fig. 7. Energy consumption analysis.

Table 6. Energy consumption comparison [J].

Nodes	COAHBS	SEHR	IBFA	ESMR	GMPSO
50	0.23	0.47	0.55	0.64	0.76
100	0.35	0.50	0.64	0.73	0.89
150	0.47	0.72	0.85	0.89	0.97
200	0.58	0.85	0.99	1.23	1.44
250	0.63	0.98	1.13	1.45	1.98

The COA-HEC framework demonstrates significant scientific contributions by efficiently integrating multi-objective optimization with lightweight cryptography, achieving comprehensive performance improvements in SDWSNs. It ensures energy efficiency [25], trust, reduced delay, and minimal packet loss while maintaining scalability [26] for dense IoT networks. Outperforming existing algorithms, it provides secure, reliable, and practical communication for industrial automation, healthcare monitoring, and smart city infrastructures. While the manuscript presents promising theoretical results, some proofs remain concise. Expanding these proofs with additional intermediate steps and mathematical justifications would enhance the rigor of the work, thereby strengthening the credibility and validity of the proposed framework.

The presented examples effectively validate the applicability of the theoretical results. However, incorporating more varied and complex case studies would better demonstrate the breadth and versatility of the proposed methods, further reinforcing their potential for diverse IoT deployment scenarios.

5. Conclusion

This work presents a significant advancement in SDWSN-based IoT routing through the COA-HEC framework, which integrates multi-objective optimization, trust management, and lightweight cryptography to address critical gaps in existing research, including the simultaneous optimization of energy, trust, delay, and hops, the lack of efficient security, and the limited scalability of traditional metaheuristics. The COA ensures optimal exploration–exploitation for dynamic path selection, while the trust model enhances resilience against malicious nodes. The HEC-based blind signcryption provides confidentiality, integrity, and anonymity with minimal computational and communication overhead, making it suitable for constrained IoT nodes. Extensive NS-3 simulations demonstrate superior performance over SEHR, IBFA, ESMR, and GMPSO, improving throughput by 59.4 %, PDR by 12.4 %, and reducing delay by 61 %. The framework scales efficiently to dense networks and is directly applicable to industrial IoT, healthcare monitoring, and smart city infrastructures. By combining holistic optimization, lightweight security, and real-world applicability, COA-HEC establishes a scalable, secure, and energy-efficient paradigm for next-generation IoT routing, with future work focusing on hardware validation, mobility-aware trust models, and AI-driven predictive optimization. In addition to the theoretical contributions, a more detailed discussion of practical applications such as deployment in large-scale industrial IoT systems, healthcare monitoring platforms, and smart city infrastructures, would be beneficial. Although the manuscript briefly addresses open questions and possible extensions, expanding this discussion would provide a clearer roadmap for future research.

References

[1] Narwaria, A., Mazumdar, A. P. (2023). Software-defined wireless sensor network: A comprehensive survey. *Journal of Network and Computer Applications*, 215, 103755. https://doi.org/10.1016/j.jnca.2023.103636

[2] Muthu, T., Kalimuthu, V. K. (2023). Seagull optimization-based feature selection with optimal extreme learning machine for intrusion detection in fog assisted WSN. *Technical Gazette*, 30 (5), 1547-1553. https://doi.org/10.17559/TV-20230130000295

[3] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17 (4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095

[4] Ammar, M., Russello, G., Crispo, B. (2018). Internet of things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, 38, 8-27. https://doi.org/10.1016/j.jisa.2017.11.002

[5] Seyyedabbasi, A., Kiani, F., Allahviranloo, T., Fernandez-Gamiz, U., Noeiaghdam, S. (2023). Optimal data transmission and pathfinding for WSN and decentralized IoT systems using I-GWO and Ex-GWO algorithms. *Alexandria Engineering Journal*, 63, 339-357. https://doi.org/10.1016/j.aej.2022.08.009

[6] Oladipupo, E. T., Abikoye, O. C., Imoize, A. L., Awotunde, J. B., Chang, T.-Y., Lee, C.-C., Do, D.-T. (2023). An efficient authenticated elliptic curve cryptography scheme for multicore wireless sensor networks. *IEEE Access*, 11, 1306-1323. https://doi.org/10.1109/ACCESS.2022.3233632

[7] Ramachandran, S., Prabakaran, D. (2024). A novel deep reinforcement learning (DRL) method for detecting evasion attack in IoT environment. In *2024 International Conference on Integrated Circuits and Communication Systems (ICICACS)*. IEEE. https://doi.org/10.1109/ICICACS60521.2024.10498632

[8] Singh, J., Deepika, J., Zaheeruddin, Bhat, J. S., Kumararaja, V., Vikram, R., Amalraj, J. J., Saravanan, V., Sakthivel, S. (2022). Energy-efficient clustering and routing algorithm using hybrid fuzzy with grey wolf optimization in wireless sensor networks. *Security and Communication Networks.* https://doi.org/10.1155/2022/9846601

[9] Haseeb, K., Almustafa, K. M., Jan, Z., Saba, T., Tariq, U. (2020). Secure and energy-aware heuristic routing protocol for WSN. *IEEE Access*, 8, 163962-163974. https://doi.org/10.1109/ACCESS.2020.3022285

[10] Haseeb, K., Islam, N., Almogren, A., Ud Din, I., Almajed, H. N., Guizani, N. (2019). Secret sharing-based energy-aware and multi-hop routing protocol for IoT based WSNs. *IEEE Access*, 7, 79980-79988. https://doi.org/10.1109/ACCESS.2019.2922971

[11] Navaneethan, S., Arun, A. (2025). A comprehensive integrated security model with advanced access control for enhancing WSN computing in IoT frameworks. *Technical Gazette*, 32 (3), 1040-1046. https://doi.org/10.17559/TV-20240822001935

[12] Alotibi, M. (2021). Improved blowfish algorithm-based secure routing technique in IoT-based WSN. *IEEE Access*, 9, 159187-159197. https://doi.org/10.1109/ACCESS.2021.3130005

[13] Conti, M., Kaliyar, P., Rabbani, M. M., Ranise, S. (2020). Attestation-enabled secure and scalable routing protocol for IoT networks. *Ad Hoc Networks*, 98, 102054. https://doi.org/10.1016/j.adhoc.2019.102054

[14] Mishra, M., Sen Gupta, G., Gui, X. (2021). Network lifetime improvement through energy-efficient hybrid routing protocol for IoT applications. *Sensors*, 21 (22), 7439. https://doi.org/10.3390/s21227439

[15] Maheshwari, P., Sharma, A. K., Verma, K. (2021). Energy efficient cluster based routing protocol for WSN using butterfly optimization algorithm and ant colony optimization. *Ad Hoc Networks*, 110, 102317. https://doi.org/10.1016/j.adhoc.2020.102317

[16] Ramteke, R., Singh, S., Malik, A. (2022). Optimized routing technique for IoT enabled software-defined heterogeneous WSNs using genetic mutation based PSO. *Computer Standards & Interfaces*, 79, 103548. https://doi.org/10.1016/j.csi.2021.103548

[17] Balakrishnan, S., Vinoth Kumar, K. (2023). Hybrid sine-cosine Black Widow Spider optimization based route selection protocol for multihop communication in IoT assisted WSN. *Technical Gazette*, 30 (4), 1159-1165. https://doi.org/10.17559/TV-20230201000306

[18] Sharmin, S., Ahmedy, I., Noor, R. M. (2023). An energy-efficient data aggregation clustering algorithm for wireless sensor networks using hybrid PSO. *Energies*, 16 (5), 2487. https://doi.org/10.3390/en16052487

[19] Pandian, I., Thirugnasambantham, S., Balasubramaniam, K., Ravichandran, K. (2025). Improving IoT network longevity with attack repellent energy (SARE) algorithm for energy-efficient and secure routing. *Technical Gazette*, 32 (3), 876-882. https://doi.org/10.17559/TV-20240823001937

[20] Liu, Y., Wu, Q., Zhao, T., Tie, Y., Bai, F., Jin, M. (2019). An improved energy-efficient routing protocol for wireless sensor networks. *Sensors*, 19 (20), 4579. https://doi.org/10.3390/s19204579

[21] Al-Shareeda, M. A., Gaber, T., Alqarni, M. A., Alkinani, M. H., Almazroey, A. A., Almazroi, A. A. (2025). Chebyshev polynomial-based emergency conditions with authentication scheme for 5G-assisted vehicular fog computing. *IEEE Transactions on Dependable and Secure Computing*, 22 (5), 4795-4812. https://doi.org/10.1109/TDSC.2025.3553868

[22] Al-Shareeda, M. A., Anbar, M., Manickam, S., Khalil, A., Hasbullah, I. H. (2021). Security and privacy schemes in vehicular ad-hoc network with identity-based cryptography approach: A survey. *IEEE Access*, 9, 121522-121531. https://doi.org/10.1109/ACCESS.2021.3109264

[23] Shareeda, M. A., Anbar, M., Alazzawi, M. A., Manickam, S., Hasbullah, I. H. (2021). Security schemes based on conditional privacy-preserving vehicular ad hoc networks. *Indonesian Journal of Electrical Engineering and Computer Science*, 21 (1), 479-488. https://doi.org/10.11591/ijeecs.v21.i1.pp479-488

[24] Almazroi, A. A., Aldhahri, E. A., Al-Shareeda, M. A., Manickam, S. (2023). ECA-VFog: An efficient certificateless authentication scheme for 5G-assisted vehicular fog computing. *PLOS One*, 18 (6), e0287291. https://doi.org/10.1371/journal.pone.0287291

[25] Al-Shareeda, M. A., Manickam, S., Mohammed, B. A., Al-Mekhlafi, Z. G., Qtaish, A., Alzahrani, A. J., Alshammari, G., Sallam, A. A., Almekhlafi, K. (2022). CM-CPPA: Chaotic map-based conditional privacy-preserving authentication scheme in 5G-enabled vehicular networks. *Sensors*, 22 (13), 5026. https://doi.org/10.3390/s22135026

[26] Abbood, A. A., Al-Shammri, F. K., Alzamili, Z. M., Al-Shareeda, M. A., Almaiah, M. A., AlAli, R. (2025). Investigating quantum-resilient security mechanisms for flying ad-hoc networks (FANETs). *Journal of Robotics and Control*, 6 (1), 456-469. https://doi.org/10.18196/jrc.v6i1.20559

Received September 21, 2024
Accepted October 13, 2025