

Topology-Aware Grey Wolf Optimization for Energy-Efficient and Stable Routing in 6G Cyber Defense Networks

¹J. Shanbagam, ²D. Maheswari

¹Department of Computer Science, RVS College of Arts and Science(Autonomous), Coimbatore, India

²School of Computer Studies-PG, RVS College of Arts and Science(Autonomous), Coimbatore, India

Abstract:- 6G cyber defense networks have many challenges that make it difficult to ensure safe and efficient routing. These challenges come from the topology that changes constantly, the very dense connectivity that exists, the strict requirements for latency, the limited resources for energy, and the continuous exposure to various cyber threats which include jamming, spoofing, malicious relays, and denial-of-service attacks. Traditional routing protocols such as AODV, DSR, OLSR, and DYMO can be used to establish communication routes, but they are often not very effective in environments that are highly dynamic and dangerous. This study examines the integration of conventional routing protocols with metaheuristic optimization techniques. The project's goal is to improve communication routing more dependable, robust, and energy-efficient. Simulations are done in OMNeT++ platform to record different transmission times and scenarios impacted by security issues in 6G networks. The proposed TA-GWO framework reaches a packet delivery ratio of 98.7%, a delay of 84 milliseconds, and a throughput of 589 kbps when OLSR is used during long transmission intervals. The results from the experiments show that this model provides optimal routing performance. Additionally, the suggested method reduces network lifetime to 472 seconds, normalized routing load to 0.34, routing overhead to 0.22, and energy consumption to 38.9 J. These results suggest that the TA-GWO-based 6G cybersecurity routing architecture provides significant improvements in energy efficiency, routing stability, and communication that can withstand threats when compared to existing metaheuristic techniques.

Keywords: 6G Cyber Defense Networks, Metaheuristic Optimization, TA-GWO Optimization, Routing Efficiency, OMNeT++ simulation.

1. Introduction

It is a common belief that 6G communication technologies will enable smart services to function in networks that are highly reliable and have low latency while continuously improving. 6G networks facilitate communication among distributed defense nodes, autonomous platforms, mobile command units, surveillance devices, and Internet of Things sensing systems in the context of cyber defense. Even when faced with challenges such as hostile interference, high mobility, changing topologies, and limited energy resources, routing must ensure the delivery of packets in a manner that is safe, flexible, and energy-efficient. Mobile wireless networks generally utilize conventional routing techniques which include Ad hoc On-Demand Distance Vector, Dynamic Source Routing, Optimized Link State Routing, and Dynamic MANET On-Demand. However, when dealing with potential cyber threats, routing decisions in 6G cyber defense and networks that involve the Internet of Things must consider additional elements such as changes in topology, reliability of connections, trustworthiness of nodes, and stability, which leads to a reduction in performance.

To solve these problems, researchers have looked into metaheuristic optimization methods for adaptive routing. These algorithms can search a lot of places at once and improve route selection by changing a number of network settings at once. Most of the research that has been done so far, on the other hand, focuses on traditional wireless networks instead of the specific needs of 6G cyber security environments. This study aims to address the highlighted gap by introducing a methodology called Topology-Aware Grey Wolf Optimization (TA-GWO), designed to improve reliable and energy-efficient routing in 6G cyber security networks. The approach finds routes in real time by looking at the network's features and how quickly the topology changes. The results from OMNeT++ simulations indicate that TA-GWO improves packet delivery ratio, throughput, delay, routing overhead, and reliability of the network. Consequently, TA-GWO is suggested as a feasible approach for ensuring secure and reliable routing in the future 6G cyber defence networks and infrastructures related to the Internet of Things.

1.1 Key Contributions

1. A comprehensive 6G cyber defense network simulation framework is developed in OMNeT++ to evaluate AODV, DSR, OLSR, and DYMO under varying topology and traffic conditions.
2. Multiple metaheuristic optimization methods, including ACO, WOA, GWO, and QPSO, are integrated with routing protocols to improve energy efficiency, route stability, and resilient communication.
3. A TA-GWO approach is proposed to dynamically adapt routing decisions based on topology variation and cyber defense communication requirements.
4. The proposed approach incorporates security-oriented route stability awareness, enabling routing paths to remain efficient under dynamic and potentially hostile 6G network environments

1.2 Rest of Section of the Study

- Section 2: Related Works – Overview of existing Routing algorithms in 6G WSNs and their gaps.
- Section 3: Methodology – Proposed SNN-based proactive intrusion prevention and routing framework.
- Section 4: Results and Analysis – Comparative evaluation showing enhanced security and efficiency.
- Section 5: Conclusion and Future Works – Summary of contributions with future directions for scalability and adaptability.

2. Literature Survey

Metaheuristic clustering integrated with routing optimization has consistently demonstrated measurable gains over classical hierarchical protocols. **Rodriguez et al. (2020)** proposed a Yellow Saddle Goatfish Algorithm (YSGA)-based clustering and routing protocol and reported improvements in network lifetime and reduced energy consumption compared to LEACH and PEGASIS under simulated WSN scenarios [1]. Comparing HEED and LEACH variations in different environments, **Mohan et al. (2022)** developed the IMCMR-UWSN for underwater WSN demonstrated superior packet delivery ratios and reduced energy consumption [2]. **Lakshmana et al. (2022)** developed a hybrid metaheuristic clustering scheme supported by the IoT, enhancing the stability of residual energy and the overall network lifetime in comparison to TEEN and HEED [3].

Hybrid optimization methods started improving performance by 2023. **S.K. Sharma et al. (2023)** demonstrated that a hybrid nature-inspired clustering-routing system led to reduced latency and increased throughput when compared to LEACH and PEGASIS [4]. **El Khediri et al. (2024)** showed that when comparing SEP and TEEN with similar node deployments, there were clear reductions in average energy consumption and extended lifetimes [5]. **Wang et al. (2024)** implemented fuzzy clustering along with a quantum-inspired routing algorithm in industrial wireless sensor network applications [6]. They reported lower routing costs and better reliability metrics compared to the LEACH and HEED benchmarks, along with noticeable improvements in residual energy retention during simulated rounds. By the year 2025, a more advanced hybridization trend was observed. **Dinesh (2025)** found that combining Chaotic PSO for cluster head selection with an Attention-based RNN routing module resulted in better route stability and longer endurance when compared to routing methods based solely on CPSO and LEACH [7]. Numerical simulation graphs indicated longer periods of stability and fewer packet retransmissions under similar node density conditions. This was noted as one of the rare integrations of ML routing optimization in studies related to WSN clustering.

Xiao et al. (2026) developed HCR-QCICA which is intended for industrial WSN [8]. Their findings indicated that this system was more reliable and consumed less energy in scenarios where there was a significant amount of industrial traffic present. Across all studies, performance improvements are reflected in metrics such as increased First Node Death (FND), extended Last Node Death (LND), higher packet delivery ratio (PDR), reduced delay, and lower average energy consumption. This means that there is still need for intelligent clustering frameworks that are based on datasets and use machine learning [9-12]. Machine learning-based optimization techniques have been widely adopted for routing in wireless 6G networks [13-16].

Table.1. Comparative Study of Metaheuristic-Based CH Selection Approaches in WSN

Author	CH Optimization Algorithm	Routing Protocol	Research Gap
Rodríguez et al. (2020) [1]	YSGA	YSGA-based multi-hop routing	Simulation-only, scalar fitness, no ML
Mohan et al. (2022) [2]	Improved Metaheuristic Clustering	IMCMR	Domain-specific model without Pareto optimization
Lakshmanan et al. (2022) [3]	Hybrid Metaheuristic (energy-aware clustering)	Energy-aware multi-hop routing	Weighted scalar fitness approach without predictive modeling.
S.K. Sharma et al. (2023) [4]	Hybrid Nature-inspired Metaheuristic	Hybrid data routing optimization	Centralized Model Not Applied.
El Khediri et al. (2024) [5]	Hybrid Metaheuristic CH selection	Cluster-based multi-hop routing	No adaptive weights.
Wang et al. (2024) [6]	Fuzzy-based clustering + Quantum-inspired optimization	Energy-efficient routing via quantum annealing strategy	Complex implementation, simulation-only
Dinesh (2025) [7]	CPSO	Attention-based RNN routing	ML is partially applied to support the routing process.
Xiao et al. (2026) [8]	Hybrid Metaheuristic Clustering	HCR-QCICA routing optimization	Computational complexity.

In summary, recent studies (2020-2026) unequivocally illustrate that metaheuristic-based clustering, when combined with routing optimization, consistently surpasses conventional protocols such as LEACH, TEEN, HEED, and PEGASIS regarding network longevity, residual energy retention, packet delivery ratio, and latency reduction. Basic ML-based routing integrations, like RNN-assisted schemes, makes route more reliable over time. On the other hand, hybrid and domain-aware solutions make routes more stable and better at balancing the load. Even though all the studies show that numbers are getting better, they all have the same problems: they are only validated through simulations, they mostly use scalar weighted fitness functions, and they don't have standardized datasets or studies of real-world deployment. Due to a lack of adaptive multi-objective modelling and intelligent predictive CH selection, WSN research needs more accurate, learning-assisted, and dataset-driven metaheuristic clustering frameworks.

3. Methodology

The proposed approach uses both metaheuristic optimization and traditional routing protocols to measure how well routing works in a 6G cyber security network. OMNeT++ simulates the network, and there are a lot of 6G-capable defense nodes set up in a changing topology. AODV, DSR, OLSR, and DYMO are examples of protocols that were first used to set up basic communication channels. To make defense-aware route optimization, information about node connectivity, hop count, delay, residual energy, topology variation, and route stability are gathered.

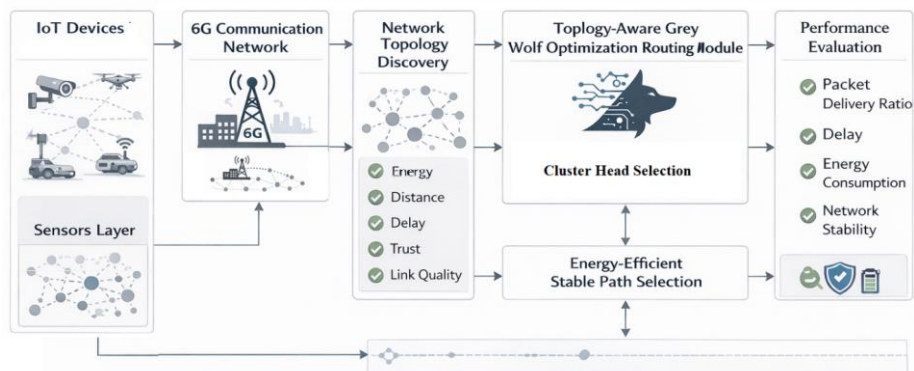


Figure 1. Optimization Framework for Energy-Efficient 6G cyber defense network

Figure 1 presents the proposed routing structure based on TA-GWO for a 6G cyber security network which is intended to be stable and energy efficient. The framework initiates at the layer of IoT devices where various sensors and devices that are spread out generate traffic for the network. The 6G communication layer gives information about the network's topology, including node connectivity, residual energy, link quality, communication delay, and trust metrics. The TA-GWO routing module finds the best communication routes based on network stability, energy efficiency, and routing security. A cyber defense module makes networks safer and finds bad nodes. Ultimately, performance metrics which consist of the packet delivery ratio, delay, energy consumption, and network durability are utilized to evaluate the enhanced routing paths. The proposed design aims to enhance communication in the next-generation 6G IoT-enabled cyber defense networks to be more reliable, secure, and energy efficient.

a. Dataset Description

The study's dataset was generated artificially from OMNeT++ simulation traces depicting a 6G cyber defence communication environment. In the simulation environment, N mobile nodes are randomly distributed across a two-dimensional area $A = L \times W$. The Random Waypoint Mobility Model dictates that each node selects a random destination and velocity $v \in [v_{min}, v_{max}]$, stops for T_p , and then repeats the process. Simulating communication between nodes employs wireless ad hoc communication assumptions relevant to tactical 6G settings. CBR generates traffic over UDP, and network activity is monitored in a variety of load, density, and mobility scenarios. The node position over time is defined as:

$$(\mathbf{x}_i(\mathbf{t}), \mathbf{y}_i(\mathbf{t})) = (\mathbf{x}_i(\mathbf{0}), \mathbf{y}_i(\mathbf{0})) + \mathbf{v}_i \mathbf{t} \quad (1)$$

Where v_i is the velocity vector of node i . IEEE 802.11 MAC is used to describe communication between nodes with a transmission range of R . A bidirectional link exists between nodes i and j when: $d_{ij} \leq R$, where

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

Constant Bit Rate (CBR) over UDP generates traffic with S bytes packet size and λ packets/sec rate T_{sim} represents the simulation time.

Table.2. Simulation Parameters

Parameter	Value
Number of Nodes	25–100
Area Size	1000 × 1000 m
Mobility Model	Random Waypoint
Speed	1–20 m/s
Pause Time	0–20 s
Transmission Range	250 m
MAC Protocol	IEEE 802.11
Traffic Type	CBR over UDP
Packet Size	512 bytes
Simulation Time	200–500 s

This table shows the predefined network and protocol configurations that are utilized uniformly across all simulation scenarios to maintain experimental consistency. These include the mobility model, MAC layer configuration, transmission range, traffic type, packet size, and other baseline values. Keeping these parameters constant ensures that performance differences are only due to the targeted experimental factors.

Table 3. Simulation Scenario Configuration for Routing Protocol

Scenario ID	Nodes (N)	Area (m × m)	Speed (m/s)	Pause Time (s)	Traffic Flows	Packet Rate (pkt/s)	Simulation Time (s)	Purpose
S1	25	1000 × 1000	1–5	20	5	4	300	Low density, low mobility
S2	50	1000 × 1000	1–10	10	10	4	300	Medium density
S3	75	1000 × 1000	1–15	5	15	4	300	High density
S4	50	1000 × 1000	10–20	0	10	4	300	High mobility stress
S5	50	1000 × 1000	1–10	10	20	8	300	High traffic load

Table 3 describes the experimental scenarios used to assess the performance of AODV, DSR, OLSR, and DYMO under different network conditions. For controlled performance comparison, each scenario systematically increases a single stress factor such as node density, mobility speed, or traffic load while keeping other parameters constant. The scalability, resilience, and congestion handling behavior are examined for the network size, mobility parameters, traffic characteristics, and simulation time of the configuration. Figure 2 demonstrates the Node Distribution before and during data transmission in the protocol proposed.

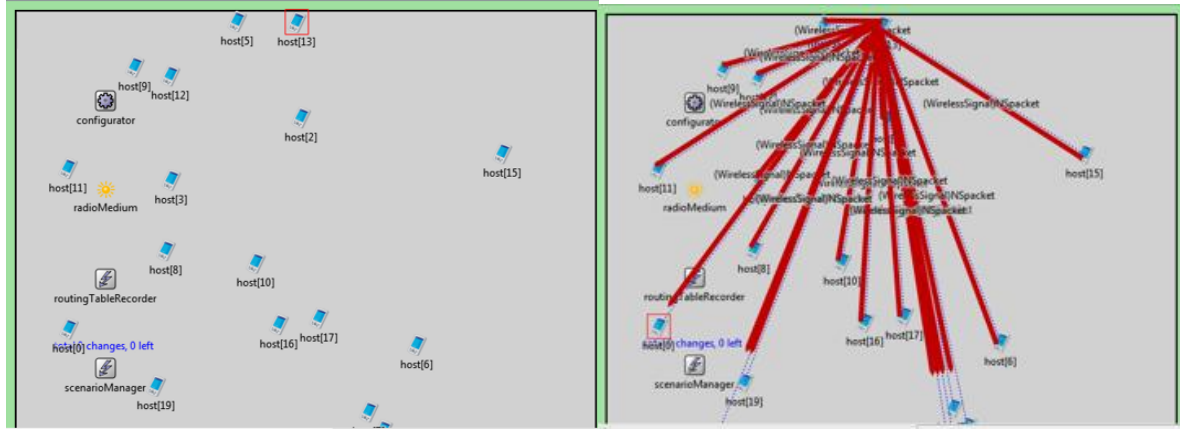


Figure 2. Node Distribution Before and During Data Transmission in the Proposed Protocol

b. Preprocessing

Before the performance evaluation, the raw simulation traces generated by OMNeT++ are treated to remove transitory effects and obtain reliable routing information. Initially, a warm-up phase T_{warm} is eliminated to eliminate startup bias induced by routing table convergence and early packet instability. Metric computation takes into account only data during the interval $t \in [T_{warm}, T_{sim}]$. Validation of node mobility traces ensures node coordinates remain inside the defined simulation area $A=L \times W$. The link connection between nodes i and j is confirmed using the condition:

$$d_{ij}(t) = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \leq R \quad (3)$$

Here R is the transmission range. Incomplete packet transmissions or corrupted event log entries are filtered to prevent distortion in Packet Delivery Ratio (PDR) and delay measurements. Control and data packets are isolated from trace logs to generate routing-specific analytics. Remove duplicate packet IDs for proper counting of P_{sent} and $P_{received}$. Time stamps are synced to compute the end-to-end delay:

$$D_{avg} = \frac{1}{P_{received}} \sum (t_{receive} - t_{send}) \quad (4)$$

Additionally, routing overhead is evaluated by separating control messages (RREQ, RREP, RERR, HELLO, and TC) from total transmissions. The final processed dataset comprises of structured performance metrics per scenario and per procedure, allowing fair comparison evaluation.

c. Routing Protocols

Routing protocols in 6G cyber defense networks allow for dynamic path building among distributed mobile defense nodes without relying on fixed infrastructure. Because these settings have frequent topology changes, mission-critical traffic, limited node energy, and are vulnerable to cyber disturbances, routing protocols must offer quick recovery, low overhead, steady forwarding, and resilient communication behavior. This paper evaluates the routing performance of AODV, DSR, OLSR, and DYMO as baseline mechanisms before augmentation using topology-aware metaheuristic optimization.

3.3.1 Ad hoc On-Demand Distance Vector (AODV)

AODV is a reactive distance-vector routing protocol in which routes are created only when a source node requires communication with a destination. Each node maintains a routing entry (Destination, NextHop, HopCount, DestSeqNum, Lifetime), where the destination sequence number ensures route freshness and loop freedom. A route r_1 is preferred over r_2 if $Seq_D^{r_1} > Seq_D^{r_2}$, or if equal, when $HopCount^{r_1} < HopCount^{r_2}$. When no valid route exists, the source broadcasts a Route Request $RREQ = \{S, D, Seq_S, Seq_D^{req}, ID, HopCount\}$. Intermediate nodes increment $HopCount \leftarrow HopCount + 1$ and establish reverse paths. A Route Reply (RREP) is generated by the destination or an intermediate node with $Seq_D \geq Seq_D^{req}$, ensuring freshness while minimizing hop-based path cost defined as

$$C_{path} = \sum_{i=1}^n \mathbf{1} = n \quad (5)$$

Where n is the total number of hops. Route maintenance is triggered by link failure detection using HELLO messages or link-layer feedback. Upon detecting a break, a node invalidates the route, increments the sequence number $Seq_D \leftarrow Seq_D + 1$, and propagates a Route Error (RERR) upstream. Valid routes satisfy the loop-free invariant: along a path toward D , sequence numbers are non-decreasing and hop counts strictly decrease, i.e. $Seq_D(n_k) \leq Seq_D(n_{k+1})$ and $HopCount(n_k) > HopCount(n_{k+1})$. Route lifetime follows a soft-state model.

$$T_{exp} = t_{current} + \text{ActiveRouteTimeout} \quad (6)$$

This automatically removes stale entries. Although AODV reduces unnecessary periodic control traffic, its route discovery overhead grows approximately as $O(N)$ due to network-wide flooding, making performance sensitive to node density and mobility rate.

▪ Dynamic Source Routing (DSR)

DSR is a reactive source-routing protocol in which the complete path from source to destination is embedded within the packet header, eliminating the need for intermediate nodes to maintain up-to-date routing tables. When a source S requires a route to destination D , it broadcasts a Route Request $RREQ = \{S, D, ID, RouteRecord\}$, where *RouteRecord* accumulates node addresses as the packet propagates. Each intermediate node appends its address, i.e., $RouteRecord \leftarrow RouteRecord + n_i$. When the request reaches D or a node with a cached route, a **Route Reply** (RREP) containing the complete ordered path

$$P = \{n_0 = S, n_1, \dots, n_k = D\} \quad (7)$$

is returned. The routing cost is hop-based and expressed as $C_{\{path\}} = |P| - 1$, indicating the number of links traversed. Because the complete route is explicit, forwarding at node n_i simply follows the next hop described in P , avoiding routing table lookups. In DSR, route n_i intenance is based on acknowledgments and input from the connection layer. If a link breaks between n_i and n_{i+1} , a Route Error (RERR) is returned to the source, and the broken link is removed from the route cache. Nodes maintain a route cache storing multiple paths $\{P_1, P_2, \dots, P_m\}$ for the same destination, allowing rapid switching without new flooding. The probability of successful packet delivery can be approximated as

$$P_{\{success\}} = \prod_{i=1}^k (1 - p_i) \quad (8)$$

Where p_i is the link failure probability of hop i . While eliminating periodic control messages reduces overhead during stable conditions, header overhead grows linearly with path length, $H_{overhead} \propto |P|$, making DSR less scalable in large or high-mobility networks.

▪ Optimized Link State Routing (OLSR)

OLSR is a proactive link-state routing protocol designed for mobile ad hoc networks, where each node maintains up-to-date topological information through periodic message exchange. Unlike classical flooding, OLSR minimizes broadcast redundancy using Multi-Point Relays (MPRs). For a node n , the MPR set $M(n) \subseteq N_1(n)$ (where $N_1(n)$ denotes one-hop neighbours) is selected such that all two-hop neighbours $N_2(n)$ are covered, satisfying $\bigcup_{m \in M(n)} N_1(m) \supseteq N_2(n)$. Only nodes in $M(n)$ forward Topology Control (TC) messages, reducing control overhead compared to full flooding. Route computation is based on shortest-path calculation using Dijkstra's algorithm, where the path cost is typically hop based.

$$C_{path} = \sum_{i=1}^k w_i \quad (9)$$

With default weight $w_i = 1$. Each node periodically transmits HELLO messages to discover neighbours and compute MPRs, and TC messages to disseminate link-state information network-wide. The routing table is continuously updated, and routes are immediately available without discovery delay. The control overhead can be approximated as $O(M)$, where M is the number of selected MPR nodes, significantly smaller than total nodes N in dense networks. Route optimality follows the shortest-path constraint $d(S, D) = \min C_{path}$. While OLSR eliminates route discovery latency and performs well in dense or moderately mobile environments, its periodic control messaging introduces steady overhead even when no data transmission occurs, making it less efficient in sparse or low-traffic scenarios.

4. Dynamic MANET On-demand (DYMO)

DYMO is a reactive distance-vector routing protocol developed as a successor to AODV, designed to simplify route discovery and maintenance while retaining loop-free guarantees. When a source node S requires a path to destination D , it broadcasts a Route Request $RREQ = \{S, D, Seq_S, Seq_D^{req}, HopCount\}$. Each intermediate node increments $HopCount \leftarrow HopCount + 1$ and records a reverse route toward SS . Unlike DSR, DYMO does not use source routing, instead, it maintains routing table entries $(Destination, NextHop, HopCount, SeqNum, Lifetime)$ similar to AODV. A Route Reply (RREP) is generated by D or an intermediate node with a fresh route satisfying $Seq_D \geq Seq_D^{req}$. Route selection follows freshness-first logic, i.e., route r_1 is preferred over r_2 if $Seq_D^{r_1} \geq Seq_D^{r_2}$, or if equal, when $HopCount^{r_1} < HopCount^{r_2}$. The path cost remains hop-based.

$$C_{path} = \sum_{i=1}^n 1 = n \quad (10)$$

Route maintenance is triggered upon link failure detection, where the detecting node increments the sequence number $Seq_D \leftarrow Seq_{D+1}$ and broadcasts a Route Error (RERR) message to invalidate dependent routes. DYMO accumulates routing information during both RREQ and RREP propagation, enabling intermediate nodes to learn routes to multiple nodes without additional control packets. Loop freedom is preserved through the invariant that along any valid path toward D , sequence numbers are non-decreasing and hop counts strictly decrease. Although DYMO removes some complexity found in AODV (e.g., optional HELLO mechanisms), route discovery still requires network-wide flooding with overhead approximately $O(N)$, making scalability sensitive to node density and mobility rate.

a. Metaheuristic Optimization

4.1.1 Proposed: Topology-Adaptive Grey Wolf Optimization (TA-GWO)

The proposed Topology-Aware Grey Wolf Optimization (TA-GWO) builds on traditional GWO by including safe relay selection and stable route optimization into a unified routing framework for 6G cyber security networks. Instead of depending just on flat route creation, the network first chooses appropriate defence relay nodes that can provide robust and energy-efficient communication. Each node n_i is evaluated for **CH candidacy** using a **topology-aware fitness function**:

$$F_{CH}(i) = w_1 \frac{E_{res}(i)}{E_{max}} + w_2 \frac{Deg(i)}{Deg_{max}} - w_3 M(i) - w_4 C(i) + w_5 \left(1 - \frac{Deg(i)}{Deg_{max}}\right) \quad (11)$$

Here, $E_{res}(i)$ is residual energy, $Deg(i)$ is node degree (connectivity), $M(i)$ represents mobility factor and $C(i)$ denotes communication cost. TA-GWO treats candidate CH sets like wolves, iteratively selecting the best CH configuration based on cluster stability and energy balance. Topology adaptation involves updating weights based on the network mobility rate ΔT . High mobility prevents highly mobile nodes from becoming CHs, resulting in less frequent re-clustering. After clustering, TA-GWO optimizes inter-cluster routing. Each candidate route between CHs is called a wolf. Path fitness is defined as:

$$F_{Route}(P) = \alpha \frac{1}{H(P)} + \beta S(P) + \gamma \frac{E_{avg}(P)}{E_{max}} - \delta D(P) \quad (12)$$

Here, $H(P)$ is hop count, $S(P)$ is link stability (e.g., $\prod e^{-\mu_{ij}^t}$), $E_{avg}(P)$ is average residual energy, and $D(P)$ is end-to-end delay. The traditional GWO update rule: $X(t+1) = X_p(t) + A|CX_p(t) - X(t)|$ is maintained, but the exploration-exploitation balance is dynamically changed based on the topology change rate. When mobility grows, exploration prevails to avoid unstable CHs and routes. When the network stabilizes, exploitation refines the shortest stable paths. Figure 3 depicts the workflow of TA-GWO Model

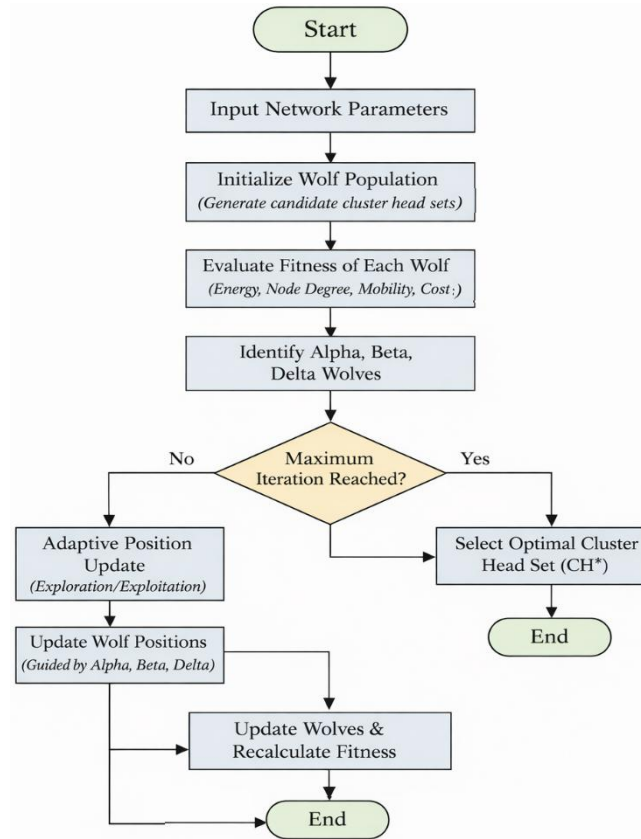


Figure 3. Workflow of TA-GWO Model

Pseudo-code:

Input: **Set of nodes N , Node parameters:** $[E_{res}, Deg, M, C]$, **Mobility rate ΔT , Max iterations T_{max}**

Output: **Optimal Cluster Head set CH^* and optimal inter – cluster route P^***

Phase 1: Cluster Head SelectionInitialize wolf population $W = \{W_1, W_2, \dots, W_k\}$

Each wolf encodes a candidate set of cluster head

for each wolf W_i :

$$F_{CH}(W_i) = w_1 \frac{E_{res}(i)}{E_{max}} + w_2 \frac{Deg(i)}{Deg_{max}} - w_3 M(i) - w_4 C(i)$$

Identify alpha (α), beta (β), and delta (δ) wolves based on highest F_{CH} **while** termination condition not met:Adapt A based on ΔT :**if** ΔT is high:

Increase exploration factor

Increase weight on mobility penalty

else:

Increase exploitation

Increase weight on energy and degree

for each wolf W_i :

Compute distance vectors:

$$D\alpha = |C1 * X\alpha - X_i|$$

$$D\beta = |C2 * X\beta - X_i|$$

$$D\delta = |C3 * X\delta - X_i|$$

Update position:

$$X_{i_{new}} = (X_i - A_1 * D\alpha + X\beta - A_2 * D\beta + X\delta - A_3 * D\delta) / 3$$

Recalculate F_{CH} for updated wolvesUpdate α, β, δ **end for**Select optimal cluster head set: $CH^* = \alpha$

Here, $E_{res}(i)$ is the residual energy of node i , E_{max} is the maximum possible node energy (normalization), $Deg(i)$ is the number of neighbours (connectivity strength), $M(i)$ is the mobility factor (average speed or link variation rate), $C(i)$ is the communication cost (distance or transmission power), w_1, w_2, w_3, w_4 are weight coefficients, and A, C are coefficient vectors controlling exploration/exploitation. Parameter A lowers as iterations progress from exploration to exploitation. D represents the distance between the current solution and the leader. Higher residual energy and node connectedness make a node more suitable for becoming a Cluster Head (CH), however high mobility and communication costs limit its selection likelihood. During the optimization process, each wolf represents a potential CH set, and the fitness function assesses cluster stability and energy balance. The Grey Wolf Optimization process modifies potential CH configurations using alpha, beta, and delta leadership. When topology variance (ΔT) is significant, exploration rises to avoid unstable CH selection. When the network becomes stable,

exploitation intensifies to refine energy-efficient CH placement. The best wolf (α) indicates the final CH arrangement, which allows for balanced and stable cluster development.

Phase 2: Inter-Cluster Routing Optimization

for each source-destination pair:

for each route P_j :

$$F_{\text{Route}(P_j)} = \alpha_1 * \left(\frac{1}{H(P_j)} \right) + \alpha_2 * \text{Stability}(P_j) + \alpha_3 * \left(\frac{E_{\text{avg}}(P_j)}{E_{\text{max}}} \right) - \alpha_4 * \text{Delay}(P_j)$$

 Identify $\alpha_{\text{route}}, \beta_{\text{route}}, \delta_{\text{route}}$

 While termination condition not met:

 Adapt parameter A using ΔT .

for each route wolf:

$$D\alpha = |C1 * X\alpha - Xi|$$

$$D\beta = |C2 * X\beta - Xi|$$

$$D\delta = |C3 * X\delta - Xi|$$

 Update position using GWO rule

end for

 Recompute route fitness

 Update α_{route}

 Select optimal route: $P^* = \alpha_{\text{route}}$

end for

Forward data packets through P^*

Here, $H(P)$ is the hop count of route, $S(P)$ denotes path stability, $E_{\text{avg}}(P)$ is the average residual energy along route, $D(P)$ represents the end-to-end delay and α_i is Route weighting coefficients. The top three routes with the highest fitness are identified as $\alpha_{\text{route}}, \beta_{\text{route}}, \delta_{\text{route}}$. During the optimization process, the exploration parameter A is adapted based on the topology variation rate ΔT . Each candidate route updates its position using the standard GWO mechanism by computing the distance from the leading routes and adjusting its position accordingly. The route fitness values are recalculated iteratively until the termination condition is satisfied. Finally, the best route $P^* = \alpha_{\text{route}}$ is selected as the optimal inter-cluster path, and data packets are forwarded through this route to ensure stable and energy-efficient communication.

Topology Adaptation Mechanism

Compute topology variation rate: $\Delta T = \frac{(\text{Number of link changes in interval})}{(\text{Total links})}$

If $\Delta T > \text{threshold}$:

 Increase exploration parameter A

 Increase stability weight

Else:

 Reduce exploration

 Increase hop-count emphasis

The topology adaptation mechanism changes the optimization method depending on how often network connections change. ΔT shows mobile network. A network is very dynamic when ΔT is higher than a certain level. The algorithm then changes the exploration parameter A and focuses on link stability to stay away from paths that are not stable. On the other hand, if ΔT is below the threshold, the network is mostly stable. In this case, the algorithm focuses on hop count and reduces exploration to favor shorter routes. This lets the routing mechanism respond well to changes in the topological conditions. In cyber defense situations, this adaptation mechanism also helps choose the best routes by making it less likely to use unstable or unreliable forwarding nodes and by giving priority to routes that have better communication continuity and stability that is aware of trust.

5. Results and Discussion

This section presents how the routing protocols perform when different metaheuristic optimization methods are used over many transmission times. The tests examines the important network performance factors which include packet delivery ratio, average end-to-end delay, throughput, routing overhead, normalized routing load, energy consumption, and how long the network lasts. The aim is to understand how different optimization methods influence routing efficiency, reliability, and energy use within the network. The results from the simulation scenarios are analyzed using comparative tables and graphical charts which display the differences in performance among the protocols and algorithms. The effectiveness of the proposed TA-GWO optimization method in improving network performance is emphasized when compared to earlier metaheuristic methods.

Table.4 Performance Metrics

Metric	Formula	Description
Packet Delivery Ratio (PDR) (%)	$PDR = \frac{P_{received}}{P_{sent}} \times 100$	Ratio of successfully received data packets to total transmitted packets, indicating reliability of the routing protocol.
Average End-to-End Delay (ms)	$D_{\{avg\}} = \frac{1}{P_{received}} \sum_{k=1}^{P_{received}} (t_{receive}^k - t_{send}^k)$	Average time taken for a data packet to travel from source to destination.
Throughput (kbps)	$Throughput = \frac{\sum_{k=1}^{P_{received}} PacketSize_k}{T_{sim}}$	Total amount of data successfully delivered per unit simulation time.
Routing Overhead	$RO = \frac{ControlPackets}{DataPackets}$	Ratio of routing control packets to transmitted data packets, reflecting protocol efficiency.
Normalized Routing Load (NRL)	$NRL = \frac{Total\ Routing\ Packets}{Total\ Data\ Packets\ Received}$	Measures the routing burden required to successfully deliver data packets.
Energy Consumption	$E_{consumed} = \sum_{i \in N} (E_{initial}(i) - E_{res}(i))$	Total energy consumed by nodes during the simulation.
Network Lifetime	$T_{life} = \min_{i \in N} (t_{death,i})$	Time until the first node in the network exhausts its energy.

Table 4 contains the mathematical equations required to calculate each metric for network reliability, delay characteristics, routing efficiency, and energy use. The proposed Topology-Adaptive Grey Wolf Optimization (TA-GWO) clustering and routing approach is assessed using standard performance criteria.

Table.5 Performance of Routing Protocols using ACO Optimization

Transmission Duration	Metric	DSR	DYMO	AODV	OLSR
1000	PDR	86.3	88.1	90.4	92.2
	Delay	178	162	145	131

	Throughput	428	447	469	488
2000	PDR	87.5	89.4	91.7	93.5
	Delay	172	158	139	126
	Throughput	436	455	478	497
3000	PDR	88.2	90.1	92.4	94.3
	Delay	168	152	135	121
	Throughput	441	462	483	504
4000	PDR	88.9	90.8	93.1	95.1
	Delay	163	147	130	116
	Throughput	447	468	491	512
5000	PDR	89.6	91.4	93.8	95.8
	Delay	158	142	126	111
	Throughput	452	474	498	519

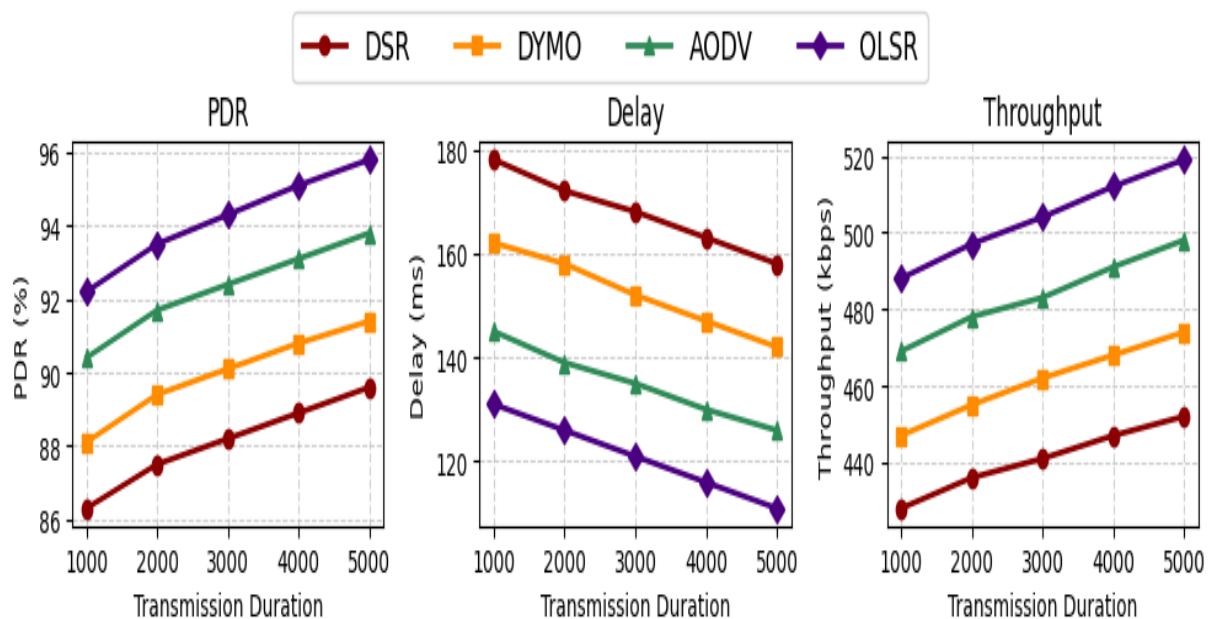


Figure 4. Performance comparison of Routing Protocols using ACO Optimization

Figure 4 represents the performance comparison of routing protocols using ACO Optimization method. Table 5 above shows how well ACO-optimized routing protocols work. PDR gets better as the transmission time goes up. OLSR gets the best value of **95.8%** at **5000** duration, and DSR gets **89.6%**. As the transmission time goes up, the average delay goes down across all protocols. OLSR has the shortest delay at **111 ms**, while DSR has the longest delay at **158 ms**. Throughput slowly goes up, and at the longest length, it reaches **519 kbps** for OLSR and **452 kbps** for DSR. Over all time periods, DYMO and AODV show moderate improvements in performance. Overall, the results show that ACO consistently performs worse than the other metaheuristic approaches when it comes to optimization.

Table.6 Performance of Routing Protocols using WOA Optimization

Transmission Duration	Metric	DSR	DYMO	AODV	OLSR
1000	PDR	88.1	89.7	91.9	93.6
	Delay	168	153	137	123
	Throughput	444	462	486	505
2000	PDR	89.3	90.8	93.0	94.7
	Delay	162	147	132	118
	Throughput	452	470	494	514
3000	PDR	90.0	91.6	93.8	95.5
	Delay	157	142	128	113
	Throughput	458	477	501	522
4000	PDR	90.7	92.3	94.5	96.2
	Delay	152	137	123	108
	Throughput	465	484	509	530
5000	PDR	91.4	92.9	95.1	96.8
	Delay	147	132	118	104
	Throughput	471	491	516	537

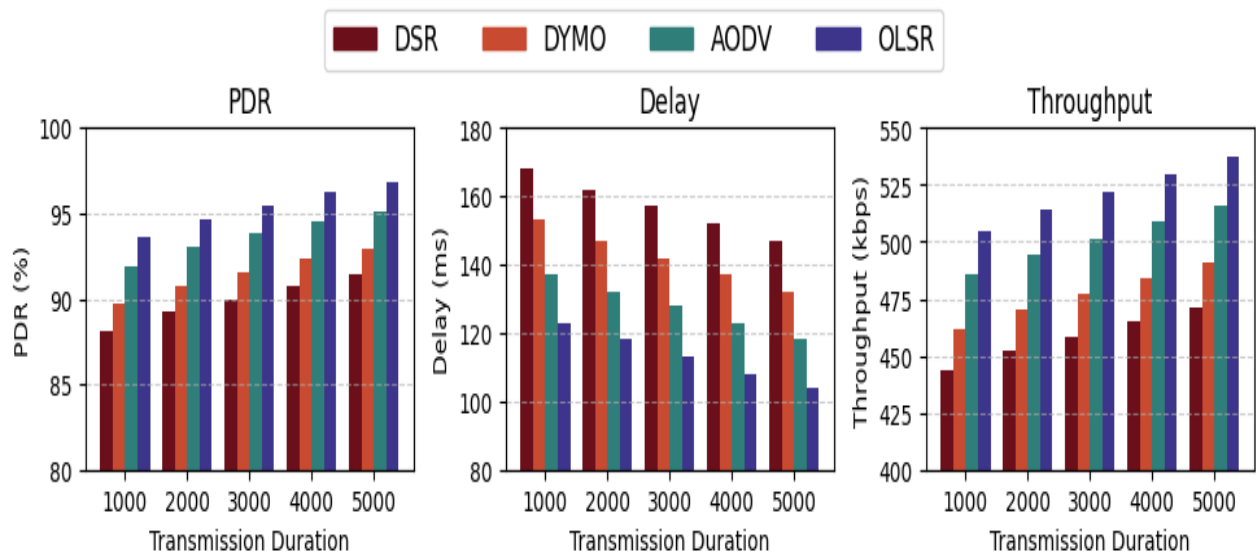


Figure 5. Performance comparison of Routing Protocols using WOA Optimization

Figure 5 represents the performance comparison of routing protocols using WOA Optimization. Table 6 presents the routing performance following the optimization using WOA. The PDR values increase from 88.1 % to 96.8 % as the transmission duration increases, and OLSR consistently performs better than other protocols. When compared to ACO, OLSR has the shortest delay measured at 104 milliseconds during the longest duration. Throughput also goes up, reaching 537 kbps for OLSR and 471 kbps for DSR at the duration of 5000. AODV shows a balanced performance with a PDR of 95.1 % and a latency of 118 milliseconds. DYMO demonstrates moderate improvements in delivery ratio and throughput. These findings indicate that WOA enhances routing efficiency compared to ACO while also keeping network performance stable.

Table.7 Performance of Routing Protocols using GWO Optimization

Transmission Duration	Metric	DSR	DYMO	AODV	OLSR
1000	PDR	89.6	91.1	93.0	94.7
	Delay	158	144	128	115
	Throughput	462	481	505	524
2000	PDR	90.8	92.2	94.1	95.7
	Delay	152	138	123	110
	Throughput	470	489	513	533
3000	PDR	91.5	93.0	94.8	96.4
	Delay	147	133	118	105
	Throughput	476	496	520	540
4000	PDR	92.2	93.7	95.4	97.0
	Delay	142	128	114	101
	Throughput	483	503	528	548
5000	PDR	92.9	94.3	96.0	97.6
	Delay	137	124	110	96
	Throughput	489	509	534	555

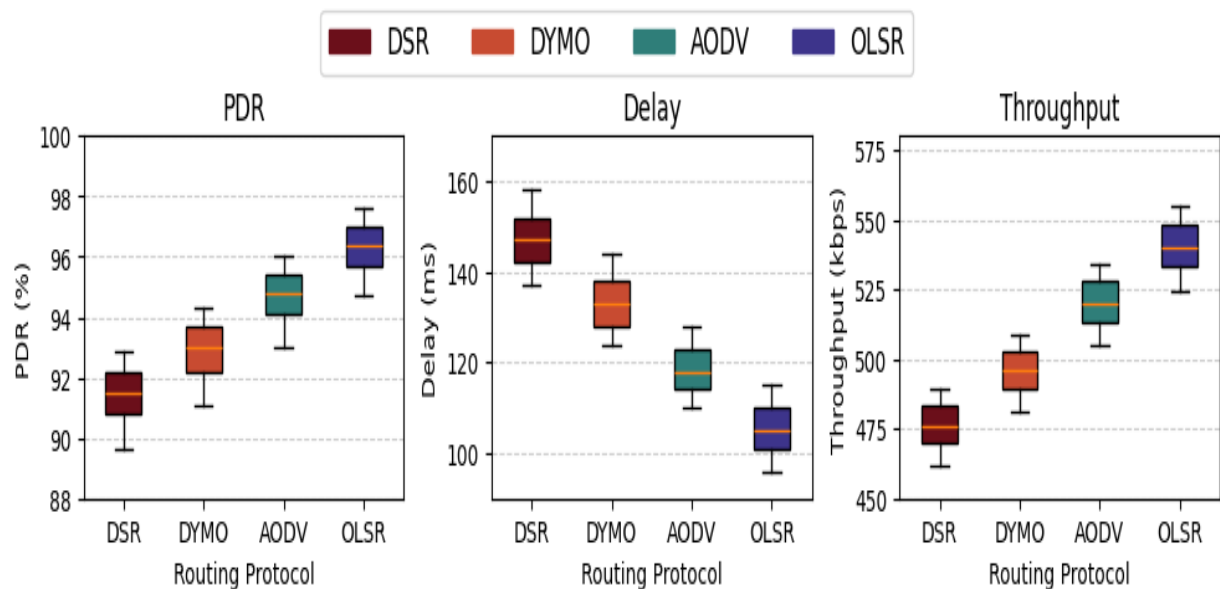


Figure 6. Performance comparison of Routing Protocols using GWO Optimization

Figure 6 shows the performance comparison of Routing Protocols using GWO Optimization. Table 7 presents the routing performance when optimized using WOA. The PDR values increase from 88.1% to 96.8% as transmission duration increases, with OLSR consistently outperforming other protocols. The delay is reduced compared to ACO, where the lowest delay of 104 ms is observed for OLSR at the highest duration. Throughput also improves, reaching 537 kbps for OLSR and 471 kbps for DSR at duration 5000. AODV shows balanced performance with 95.1% PDR and 118 ms delay. DYMO demonstrates moderate improvements in both delivery ratio and throughput. These results indicate that WOA enhances routing efficiency compared to ACO while maintaining consistent network performance.

Table.8 Performance of Routing Protocols using QPSO Optimization

Transmission Duration	Metric	DSR	DYMO	AODV	OLSR
1000	PDR	90.8	92.1	93.9	95.4
	Delay	150	136	121	108
	Throughput	478	497	520	540
2000	PDR	91.9	93.2	94.9	96.3
	Delay	144	131	116	103
	Throughput	486	505	528	548
3000	PDR	92.6	93.9	95.6	97.0
	Delay	139	126	112	98
	Throughput	492	512	535	555
4000	PDR	93.2	94.6	96.2	97.6
	Delay	134	121	108	94
	Throughput	499	519	542	563
5000	PDR	93.8	95.1	96.7	98.1
	Delay	129	116	104	90
	Throughput	505	525	548	570

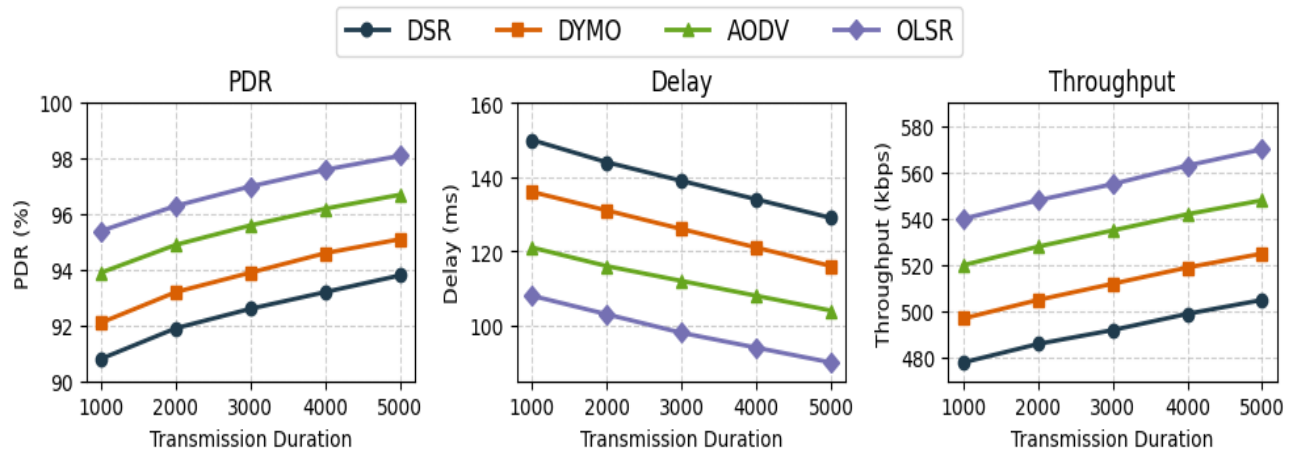


Figure 7. Performance comparison of Routing Protocols using QPSO Optimization

Figure 7 depicts the performance comparison of Routing Protocols using QPSO Optimization. Table 8 presents the routing performance using QPSO optimization. The Packet Delivery Ratio, or PDR, shows a continuous increase, reaching a value of 98.1% for OLSR and 93.8% for DSR when the transmission duration is at its maximum. The average delay recorded is lower than what is seen with GWO, as OLSR achieves an average delay of 90 ms while DSR has an average delay of 129 ms. When the duration is at 5000, the throughput for OLSR rises to 570 kbps and DSR reaches 505 kbps. AODV shows good performance as well, with a PDR of 96.7% and a latency of 104 ms. DYMO shows some modest improvements in both delivery ratio and throughput. These results indicate that QPSO offers better optimization performance and greater routing stability.

Table.9 Performance of Routing Protocols using TA-GWO Optimization

Transmission Duration	Metric	DSR	DYMO	AODV	OLSR
1000	PDR	92.1	93.4	95.0	96.4
	Delay	142	128	114	101
	Throughput	495	514	538	558
2000	PDR	93.0	94.3	95.9	97.1
	Delay	136	123	109	96
	Throughput	503	522	546	566
3000	PDR	93.7	94.9	96.5	97.7
	Delay	131	118	105	92
	Throughput	509	529	553	574
4000	PDR	94.3	95.6	97.0	98.2
	Delay	126	113	100	88
	Throughput	516	536	560	582
5000	PDR	94.9	96.1	97.5	98.7
	Delay	121	108	96	84
	Throughput	522	542	566	589

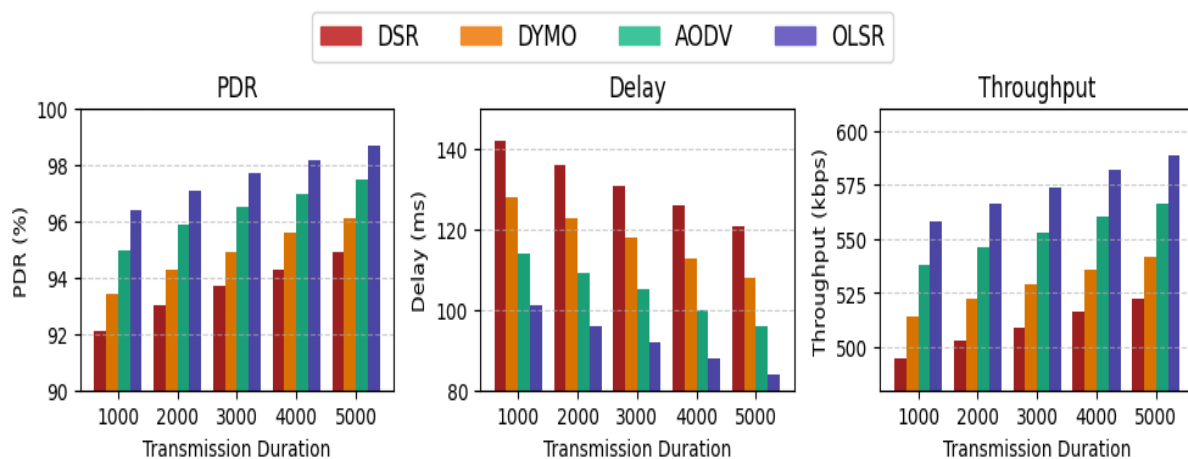


Figure 8. Performance comparison of Routing Protocols using TA-GWO Optimization

Figure 8 shows the performance comparison of Routing Protocols using TA-GWO Optimization algorithm. Table 9 presents the routing performance using the proposed TA-GWO optimization method. The PDR values reach the highest levels among all algorithms, achieving 98.7% for OLSR and 94.9% for DSR at duration 5000. The delay is significantly reduced, with the lowest delay of 84 ms recorded for OLSR, while DSR shows 121 ms. Throughput also achieves the highest values, reaching 589 kbps for OLSR and 522 kbps for DSR. AODV demonstrates strong performance with 97.5% PDR and 96 ms delay, while DYMO records 96.1% PDR and 542 kbps throughput. The results clearly demonstrate that TA-GWO provides superior routing optimization compared to other metaheuristic approaches.

Table 10. Computation of Routing Overhead and NRL

Algorithm	Routing Overhead				NRL			
	DSR	DYMO	AODV	OLSR	DSR	DYMO	AODV	OLSR
ACO	0.42	0.39	0.35	0.31	0.56	0.52	0.48	0.44
WOA	0.40	0.37	0.33	0.29	0.53	0.50	0.45	0.41
GWO	0.38	0.35	0.31	0.27	0.51	0.47	0.43	0.39
QPSO	0.36	0.33	0.29	0.25	0.49	0.45	0.41	0.37
TA-GWO	0.33	0.30	0.26	0.22	0.46	0.42	0.38	0.34

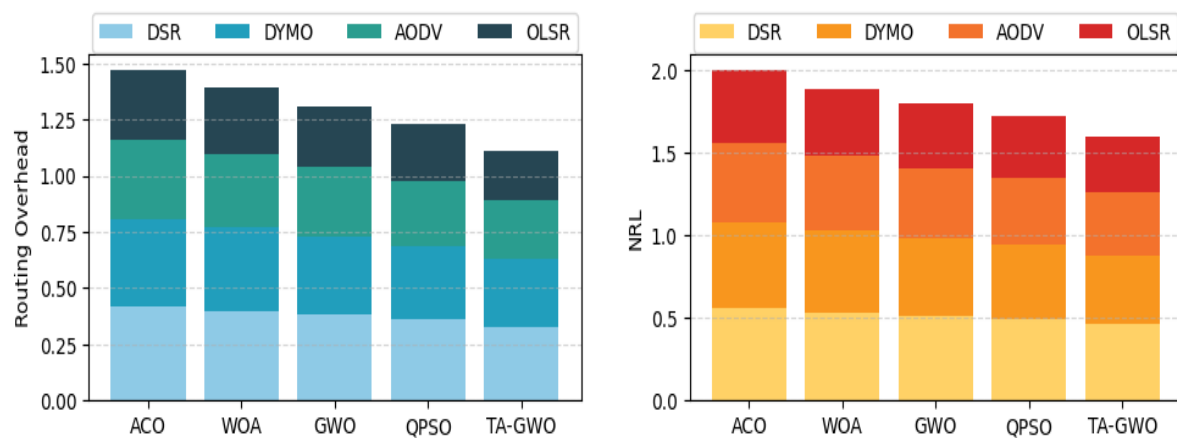


Figure 9. Comparison of Routing Overhead and NRL

Table 10 and Figure 9 above show a comparison of routing overhead and NRL for different routing protocols that use various metaheuristic optimization strategies. Routing overhead refers to the ratio of control packets that are generated during the processes of route discovery and maintenance to the data packets. The number of routing packets sent for each data packet that is successfully delivered is called NRL. Lower routing overhead and NRL values mean that routing is more efficient and that there is less network control traffic. The results show that the suggested optimization strategy cuts down on unnecessary routing transmissions and makes the network as a whole more efficient when compared to older metaheuristic methods.

Table 11. Energy and Network Lifetime Comparison across Metaheuristic Algorithms

Algorithm	Energy Consumption (J) ↓	Network Lifetime (s) ↑
ACO	46.8	402
WOA	44.5	417
GWO	42.3	435
QPSO	40.6	451
TA-GWO	38.9	472

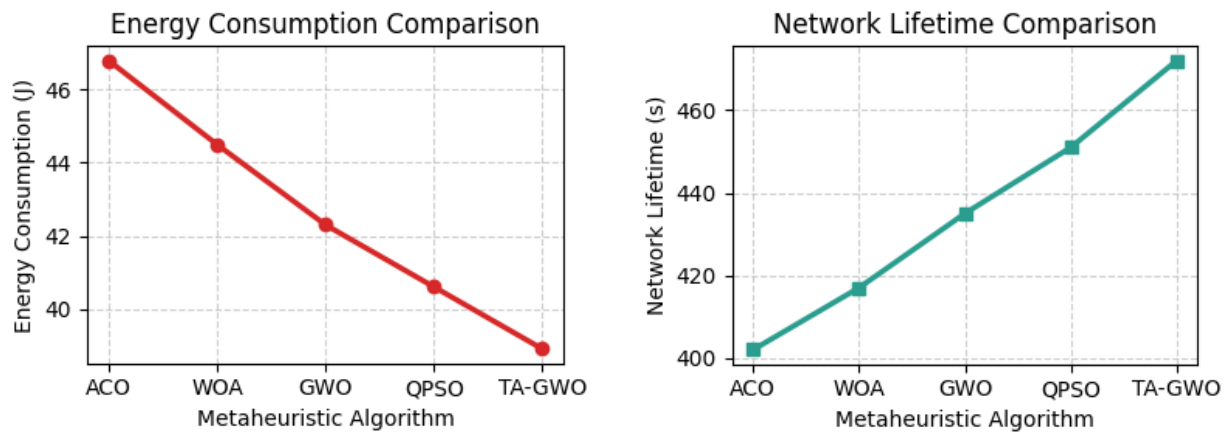


Figure 10. Energy Consumption and Network Lifetime Comparison

Table 11 and Figure 10 shows comparison of energy efficiency among different metaheuristic algorithms, with a focus on overall energy usage and the duration of network lifetime. Energy consumption is the total energy that nodes use during the simulation period, and network lifetime is defined as the time until the first node runs out of energy. A decrease in energy consumption along with an increase in network lifetime indicates better routing and cluster management. The results show that the proposed TA-GWO method achieves the longest network lifetime of **472 seconds** and the lowest energy usage of **38.9 J**, which indicates improved energy efficiency when compared to other optimization methods.

6. Conclusion

This study investigates the effectiveness of various routing algorithms using metaheuristic optimization techniques in the 6G cybersecurity networks, which aim to provide communication that is both robust and energy-efficient. The study investigates ACO, WOA, GWO, QPSO, and a novel methodology known as Topology-Aware Grey Wolf Optimization (TA-GWO), alongside routing protocols such as AODV, DSR, OLSR, and DYMO. To evaluate critical performance metrics such as packet delivery ratio, end-to-end delay, throughput, routing overhead, normalized routing load, energy consumption, and network lifetime, multiple simulations are conducted under varying transmission lengths and network conditions. The result shows the important of optimized routing to make communication systems for 6G cyber better defense work. These systems must be robust, responsive, and energy-efficient. The proposed TA-GWO framework consistently outperforms all other methods in the study. It reduces latency, routing overhead, and routing strain. This increases the speed of packet delivery and throughput. The proposed method conserves energy and extends the lifespan of the network, indicating that its stability and durability under changing conditions. The findings indicate that TA-GWO-routing framework is a viable choice for managing traffic in future 6G cyber defense networks, where security, energy efficiency, and defense are significant factors.

Conflict of interest: The authors declare no conflicts of interest(s).

Data Availability Statement: The Datasets used and /or analysed during the current study available from the corresponding author on reasonable request.

Funding: No fundings.

Consent to Publish: All authors gave permission to consent to publish.

References

- [1] Rodríguez, A. Del-Valle-Soto, C. Velázquez, R. Energy-Efficient Clustering Routing Protocol for Wireless Sensor Networks Based on Yellow Saddle Goatfish Algorithm. *Mathematics* 2020, 8, 1515. <https://doi.org/10.3390/math8091515>.
- [2] Mohan, P. Subramani, N. Alotaibi, Y. Alghamdi, S.; Khalaf, O.I. Ulaganathan, S. Improved Metaheuristics-Based Clustering with Multihop Routing Protocol for Underwater Wireless Sensor Networks. *Sensors* 2022, 22, 1618. <https://doi.org/10.3390/s22041618>.
- [3] Lakshmana, K. Subramani, N. Alotaibi, Y. Alghamdi, S.; Khalafand, O.I. Nanda, A.K. Improved

Metaheuristic-Driven Energy-Aware Cluster-Based Routing Scheme for IoT-Assisted Wireless Sensor Networks. Sustainability 2022, 14, 7712. <https://doi.org/10.3390/su14137712>.

[4] S. K. Sharma, et al., “A Metaheuristic Approach for Hybrid Data Routing in Wireless Sensor Networks,” Wireless Personal Communications, 2023. <https://doi.org/10.1007/s11277-023-10814->

[5] S. El Khediri, et al., “Energy Efficient Cluster Routing Protocol for Wireless Sensor Networks Using Hybrid Meta-Heuristic Approaches,” Ad Hoc Networks, 2024. <https://doi.org/10.1016/j.adhoc.2024.103473>

[6] Wang, H. Liu, K. Wang, C. Hu, H. Energy-Efficient, Cluster-Based Routing Protocol for Wireless Sensor Networks Using Fuzzy Logic and Quantum Annealing Algorithm. Sensors 2024, 24, 4105. <https://doi.org/10.3390/s24134105>.

[7] Dinesh, R., Venkata Srihari Babu, D., Antony, V.A. et al. Efficient cluster head selection and routing in wireless sensor networks using CPSO and Attention-based RNN. Peer-to-Peer Netw. Appl. 18, 281 (2025). <https://doi.org/10.1007/s12083-025-02102-9>.

[8] J. Xiao, et al., “HCR-QCICA: High-Performance Clustering and Routing for Industrial Wireless Sensor Networks,” Expert Systems with Applications, 2026. <https://doi.org/10.1016/j.eswa.2026.131408>

[9] Preethi R, et al. (2023). Metaheuristics Techniques for Cluster Head Selection in WSN: A Survey. International Journal on Recent and Innovation Trends in Computing and Communication, 11(10), 1197–1216. <https://doi.org/10.17762/ijritcc.v11i10.8661>

[10] P. Raj and R. Yadav, “An Improved Cluster Head Selection Algorithm for Wireless Sensor Networks Using Enhanced Particle Swarm Optimization,” Procedia Computer Science, vol. 185, pp. 230–237, 2021.

[11] S. Chaurasia, A. Kumar, and R. Kumar, “MOCRAW: A Meta-heuristic Optimized Cluster head selection based Routing Algorithm for WSNs,” Ad Hoc Networks, vol. 141, Art. no. 103079, 2023.

[12] S. Sharma and M. Chawla, “Cluster Based Metaheuristic Algorithm for Energy-Efficient Wireless Sensor Networks,” Wireless Personal Communications, 2024. (Originally published as ResearchSquare preprint, 2023.)

[13] Raghupathy, M., & Rajasekhar, C. (2025). Deriving a Multi-Objective Function Using Hybrid Meta-Heuristic Approach for Optimal CH Selection and Optimal Routing in WSN. Cybernetics and Systems, 56(7), 1085–1126. <https://doi.org/10.1080/01969722.2025.2468191> .

[14] Maddikera Krishna Reddy, Anusha Sowbarnika Veluswamy, S. Selvanayaki, C. Harini, Pavan Kumar, and Syed Shameem. 2025. Modeling of metaheuristic-based dual cluster head selection with routing protocol for energy-efficient wireless sensor networks. Soft Comput. 29, 6 (Mar 2025), 2999–3020. <https://doi.org/10.1007/s00500-025-10563-6>

[15] O. Gökalp, D. Aydın, and A. Uğur, “An Energy Efficient Cluster Head Selection in Priority Region Aware Wireless Sensor Networks Using Metaheuristic Algorithms,” Journal of Scientific Reports-A, no. 62, pp. 71–89, 2025.

[16] M. Mageshwaran, “Energy-Efficient Cluster Head Selection Using Hybrid Meta-heuristic Algorithms in WSNs,” International Journal of Advanced Science, Innovation and Sustainability (IJASIS), 2026.