SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V11I1P108

Volume 11 Issue 1, 101-115, January 2024

Original Article

An Adapted Walrus Optimal Routing with Reputation Trust Based Secure Protocol For WSN

R. Kennady[1], K. Thinakaran[2]

[1,2]*Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Tamilnadu, India.*

[1]*Corresponding Author : kennadycmc@gmail.com*

Received: 17 October 2023 Revised: 27 November 2023 Accepted: 18 December 2023 Published: 13 January 2024

Abstract *- Security and energy use are two crucial issues for Wireless Sensor Networks (WSNs) because of their scarce resources and changeable topology. Additionally, many attacks, excessive energy consumption, and transmission bottlenecks between nodes remain; however, trust-based methods are available now to deal with the undesirable behaviour of nodes. The authors of this research suggest a solution to this problem by introducing the Adapted Walrus Optimal Routing with Reputation Trust-based Secure Protocol (AWORTSP) for WSN. The total capacity of the cluster in AWORTSP could be regulated to raise its Energy Efficiency (EE) and prevent overconsumption of energy by employing the totality of adaptive determination Cluster Head (CH-nodes), determination of Residual Energy (RE), and the number of neighbour nodes. In unison, the trust maintenance scheme is integrated into AWORTSP for protection against internal threats and optimal data transmission. Through MATLAB simulations and comparisons by established routing algorithms, we assess the efficacy of the proposed AWORTSP. EE, Packet Loss Rate (PLR), RE, End-to-End (E2E) delay, Packet Delivery Ratio (PDR), Detection Rate (DR), and communication cost are all areas where AWORTSP is seen to excel over competing algorithms. Additionally, outcomes demonstrate that AWORTSP can successfully avoid potentially harmful nodes in the routing procedure. Because of this, AWORTSP will have a longer lifespan on the network than competing protocols. The research could be helpful in intelligent healthcare systems, which would benefit greatly. Delivering services that use less energy and hence keep the network online for longer additionally helps improve communication throughout data exchange.*

Keywords *- WSN, Clustering, Trust management, Network security, Adapted Walrus Optimal Routing, Walrus Optimization, Trust-based Secure Protocol, Network lifetime.*

1. Introduction

WSNs are a subset of ad hoc networks with nodes not perpetually located in one location. Small, self-configuring Sensor Nodes (SNs) are the fundamental elements of a WSN. Randomly disseminated WSN nodes record and observe physical phenomena in inaccessible areas. These SNs rely on limited computational resources, including battery life and storage space, to function effectively. WSNs are a specific type of ad-hoc network characterized by nodes that do not remain stationary in a fixed position indefinitely. The core components of a WSN are miniature SNs that possess the capability to self-configure.

Using randomly distributed WSN nodes captures and monitors physical phenomena occurring in remote and hard-to-reach areas. To activate with optimal efficiency, the routine of these SNs is contingent upon a finite set of computing resources, including factors like battery longevity, storage capacity, and processing capabilities [1]. The typical SN inside a sensor network can execute three primary functions. The network can perceive and analyze its surroundings, transmitting and processing the acquired information.

In certain specific scenarios, SNs are fortified with supplementary infrastructure to enable position recognition and network mobility integration. The characteristics of the sensors are adjusted to fully utilize their resources, such as memory, power, and network connectivity-the energy sources of a sensor drain fast during communication between nodes.

The region subject to surveillance generally lacks human presence, making repairing or rebuilding SNs unfeasible. A topological rearrangement can potentially transpire in the event of a failure of a single network node to execute its designated function. In this scenario, it will be necessary to reconfigure the network topology and initiate retransmission. The longevity of a WSN is expected to be diminished through the inadequate battery capacities of the individual

SNs. Therefore, increasing energy competence and extending network lifespan are the two WSN challenges that must be addressed most urgently.

Researchers are now pursuing an investigation of WSN routing to enhance the technology. Thus far, the implementation of energy-efficient routing has presented a significant challenge. A data-transfer protocol is necessary for the nodes, specifically routers, inside a WSN to effectively cooperate and ascertain the most efficient pathway for transmitting data. Using an energy-efficient data transmission protocol, which can be customized to spread the energy load between all nodes regularly, can potentially decrease the power consumption of a WSN.

Due to the potential occurrences of data packet loss caused by factors such as missing, disruption, or manipulation by attackers [2, 3], only SNs deemed authentic must be allowed to transmit data operation. Hence, it is imperative to implement necessary measures to safeguard data packets against potential risks during their transmission.

Trust-based methodologies have proven to be efficacious in addressing the issue of malicious nodes inside WSN. In cyber security, the concept of trust holds paramount significance. Through the valuation of the protection state of SNs by analyzing their activities and relations and by dynamically distinguishing between normal nodes and hostile nodes, potential security threats like privacy breaches, data alterations, and the potential for orchestrating more advanced attacks [4, 5] are effectively reduced.

In circumstances characterized by high risk and insecurity, developing security measures in WSNs assumes paramount importance. Researchers must prioritize the inclusion of robust security protocols to ensure data protection during transmission since neglecting this aspect is not a viable option. Maintaining data security and secrecy in a WSN creates challenges due to its disseminated nature and the restricted capabilities of each node [6]. The predominant authentication method in most wireless networks is based on encryption and cryptographic keys. The implementation of encryption protocols guarantees the preservation of privacy, verifiability, and integrity, albeit at a considerable expenditure of resources and time.

Intrusion Detection Systems (IDS) and trust-based algorithms have demonstrated higher effectiveness in recognizing malicious nodes. The trust control paradigm offers enhanced adaptability, flexibility, and certainty compared to traditional security approaches. Establishing a reliable network of sensor devices enables the provision of services related to sharing and security. By utilizing node confidence values as a determining factor, the trust model effectively augments the security measures of public networks. Hence, the security predicament in WSNs is effectively mitigated using strategies centered around lightweight trust and reputation mechanisms.

1.1. Problem Statement

Specific inquiries exist that elude a conclusive resolution. These problems may also be denoted as stochastic problems or NP-hard problems. Conventional deterministic techniques have limitations in their ability to address such conditions effectively. In this case, optimization procedures would be employed to ascertain the most optimal options. Routing in WSNs is one of the NP-hard issues, hence requiring optimization techniques. The Objective Function (OF) plays a crucial role in optimization approaches. The OF can potentially encompass a singular target or several objectives, contingent upon the stochastic problem being addressed.

The application of SI-based optimization approaches to the problem of route optimization in WSN over a decade is highly relevant to the present discourse. Swarm behavior refers to the synchronized aggregation or movement of birds and animals of similar dimensions in a unified direction [7]. Swarm-dwelling organisms and bird species adhere to a set of three fundamental principles: firstly, they tend to emulate the behavior of their neighboring individuals; secondly, they strive to keep consistent proximity to their neighboring counterparts; and thirdly, they actively avoid any form of physical contact or collision with their neighboring entities. Swarm intelligence algorithms offer a means to identify the most optimal solutions for real-world issues.

1.2. Research Objectives

The proposed AWORTSP aims to improve network security measures and ensure the long-term sustainability of grids. The cluster size is limited by the remaining energy and the thickness of adjacent nodes, besides the number of nodes at the apex of an evolving decision cluster. Furthermore, it proposes a trust management method that relies on the distribution of AWOR as a pivotal factor for selecting a secure CH. This technique aims to enhance network performance in the presence of attacks.

The subsequent segments of the work are prepared as follows. The subsequent sector of the work encompasses a comprehensive analysis and evaluation of several works closely associated with the topic. Section 3 introduces the AWO routing protocol, which was created on trust management and designed to protect cluster selection and accomplish load balancing among networks. Section 4 of the paper focuses on the analysis, numerical simulation, and the conclusion in Section 5.

2. Related Works

The difficulty with routing in WSN is that it uses up all available resources at each node while communicating. The excessive consumption of resources during the

communication of data in the network has a detrimental impact on the lifetime of WSNs and compromises the overall performance of the network. The literature presents Nature Inspired Optimization (NIO) methods to tackle this difficulty. The employment of WSNs in academic works has demonstrated notable enhancements in productive energy and the system's life expectancy. Nature-inspired path optimization algorithms are of utmost importance in WSNs because they enhance routing efficiency, reduce energy consumption, and extend network lifespan [8].

In [9], a protocol, Low Energy Adaptive Clustering Hierarchy and Trust Management (LEACH-TM), was developed. This protocol incorporated many factors, for example, the count of active decision CH nodes of WSN, the remaining energy level, and the density of adjacent nodes, to effectively regulate the dimensions of the cluster. This approach aimed to enhance EE and prevent nodes from experiencing excessive energy consumption. To mitigate internal attacks, the LEACH-TM protocol has a trust management strategy.

The simulation findings demonstrate that, when associated with the LEACH-SWDN and LEACH protocols, the LEACH-TM protocol exhibited superior performance in extending the network historically and achieving energy consumption balance. It was necessary to balance network durability and data security to mitigate the risks posed by reply attacks, selective forwarding attacks, modification attacks, and information leakages. Additionally, it was essential to consider EE during the routing process. However, it should be noted that the current approach exhibits limitations regarding scalability, and further experimentation was required to address this issue.

The research in [10] introduced the development of a protocol called Swarm Intelligence Adaptive Neuro-Fuzzy Inferences System Routing (SI-ANFISR) for clustered WSNs. This method aimed to ascertain the CHs and best pathways for multi-hop communication within the system. The technique used a weighted clustering scheme to select CHs from clusters to achieve this objective. Additionally, the method encompassed the development of the ANFIS approach to facilitate the selection process. This model has three input constraints: RE, node history, and degree. The Squirrel Search Algorithm (SSA) effectively tuned the Membership Function of the ANFIS system. No prior studies have used the combination of ANFIS and SSA for routing till now.

In [11], a SI-Centric Routing Algorithm (SICROA) was developed as a potential solution for WSNs. The primary objective of SICROA was to harness the benefits offered by the ant colony optimization. The routing protocol under consideration aimed to mitigate the issues associated with the AODV procedure while enhancing routing efficiency by implementing collision prevention, link-quality forecasting, and preservation techniques. The suggested solution has been shown to strengthen network routine by substituting the regular "Hello" data with an interpose mechanism, which helps anticipate and identify link interruptions. Hence, the network's total performance can be enhanced by implementing suitable protocols for processing each control message. The objective of this study was to suggest an adaptive trust model by incorporating a filtering method. The primary focus was to achieve high accuracy and trust evaluation speed. A significant amount of communication overhead and a high time complexity can be observed.

The research in [12] introduced a Layered-Based Routing (LBR)-Grey Wolf Optimizer (GWO) routing scheme, which incorporates the technique. LBR-GWO aimed to improve the durability of the system network. The SNs were classified into four distinct network layers in this methodology. In the first tier, the SNs were designated as CHs. If the initial layer has more than two nodes, the collection of CHs was determined through a game theory-based mechanism. Instead, the assortment of CH was conducted based on the remaining energy levels of the SNs. LBR-GWO approach demonstrated suitability for clustered networks compared to other methodologies.

The simulation findings provide evidence that this algorithm effectively balanced the energy value of nodes, hence enhancing the longevity of the WSN network in comparison to the HEED, LEACH, and PSO algorithms. The objective was to improve the network's longevity by incorporating energy-efficient clustering techniques and adopting a hierarchical architecture to provide high scalability. Nevertheless, the absence of a security mechanism to distinguish aberrant nodes from ordinary nodes, the presence of a high time complexity, and the lack of consideration for inter-cluster routing were notable shortcomings in the design.

The study in [13] proposed a trust-aware routing method named AF-TNS in WSNs, which utilized an activation function as its core mechanism. The implementation of this strategy consisted of two sequential processes: firstly, an energy-restricted trust evaluation was conducted, followed by an additive metric-based node evaluation. These steps were designed to safeguard the trustworthiness of surrounding nodes.

The AF-TNS algorithm employed a stochastic Transigmoid function to determine the selection of protected and apprehensive nodes to sustain network constancy. The simulation findings demonstrated that using AF-TNS enhanced both the DR and the network's longevity. The process of selecting reliable neighbors during secure transmission was facilitated by a decision-making system, which contributed to the complete constancy of the network.

The design of a trust system lacks robustness, exhibits limited scalability, and fails to incorporate a clustering process.

The AOSTEB model in [14] provided an additional ACO-based NIO protocol to realize EE and safe data broadcast. The protocol consisted of three stages: cluster building, establishment of various pathways, and data transmission from the basis to the target. Hence, the NIO framework with a Particle Swarm Optimizer (PSO) algorithm-based routing protocol has been developed to tackle the fundamental challenge in WSN effectively.

The protocol LD2FA-PSO, as proposed in [15], employed a network model to generate the segment table and utilized finite automata to construct the path table. The protocol effectively ensured both EE and safety in the context of data transfer inside a WSN. PSO was a technique to efficiently determine the ideal route for data transmission within a WSN. The objective was to identify a practical and secure path from the basis to the destination while minimizing computational complexity. This was achieved by considering a hierarchical topology and prioritizing energy conservation in the clustering process to enhance the overall network lifetime. However, significant delays in the data delivery procedure and the associated high communication costs were notable concerns.

The research in [16] presented a strategy for route design that combined an ACO approach with an Artificial Bee Colony (ABC) approach. The assortment of nodes for the route was determined based on their energy levels and distances from the BS. The outcomes exhibited superior energy conservation about a non-bio-inspired algorithm. It ensured the accessibility of data, achieved high levels of accuracy and detection speed, minimized delays, and reduced communication costs during the routing process. Nevertheless, the omission of energy considerations in the routing procedure, the neglect of EE in the safety mechanism, and the disregard for the clustering device's potential to enhance scalability are noteworthy. The ABC optimization approach improved the selection of optimal CHs, as discussed in [17].

In addition, the study implemented a polling control mechanism that relied on identifying busy and idle nodes during the steady state stage to enhance energy management. The achieved DR and accuracy were found to be high, but the convergence speed was seen to be low. Therefore, there was a need to enhance the data aggregation process. In [18], the CGTABC procedure was implemented to choose CHs during the setup phase of the LEACH protocol.Additionally, they utilized an ACO-based routing procedure to determine the optimal paths among the CHs and the BS. The system exhibits significant scalability concerning EE within the clustering process and a high DR and accuracy. However, it also incurred substantial communication overhead and exhibited high time complexity.

2.1. Review Summary

The present literature on the topic of WSNs primarily concentrates on the advancement of routing protocols. These protocols incorporate many optimization strategies, including trust management, swarm intelligence, and bio-inspired algorithms. The main objective of these techniques is to improve EE, network longevity, and security. Although these protocols effectively tackle various difficulties, such as maintaining energy consumption balance, ensuring network resilience, and implementing trust-aware routing, they have significant drawbacks regarding scalability, security methods, time complexity, and communication overhead. Several protocols do not adequately address both EE and security, and there is a constant requirement for additional research to tackle scale concerns. Furthermore, the existing designs commonly suffer from the lack of solid security methods to differentiate abnormal nodes, significant time complexity, and the failure to consider inter-cluster routing. The research gap indicates the requirement for integrated methodologies that successfully harmonize EE, scalability, and security concerns in WSNs, guaranteeing comprehensive resolutions for the various issues presented by these dynamic and resource-limited networks.

3. Proposed Model

This section presents the implementation of the proposed optimal routing in WSN based on AWORTSP. The network process is depicted in Figure 1. The clustering protocol strategy in WSN is demonstrated through an optimization procedure. In this procedure, the initial step involves the identification of high-energy, balanced, and reliable nodes from a set of randomly generated nodes. The primary process of the proposed scheme is merging nodes into clusters, and selecting the CH depends upon the computation of WSN node attributes. Furthermore, to choose CHs from a pool of candidates, the suggested methodology introduces a WO optimization-driven clustering methodology.

This method consists of SNs with higher remaining power and trust ratings compared to the average trust and energy of all nodes in WSN. The primary objective of AWOR is to minimize the communication overhead through data broadcast between the BS and the CH, regardless of the direction, by choosing the most efficient path. Finally, data transmission from the transmitter to the receiver occurs via the most efficient route.

This section explains the WSN system, the energy consumption, and the attack mechanism. The WSN network model is a conceptual framework used in several fields to represent the interconnections and relationships between different entities or components within a system. The network model of AWORTSP is illustrated in Figure 1.

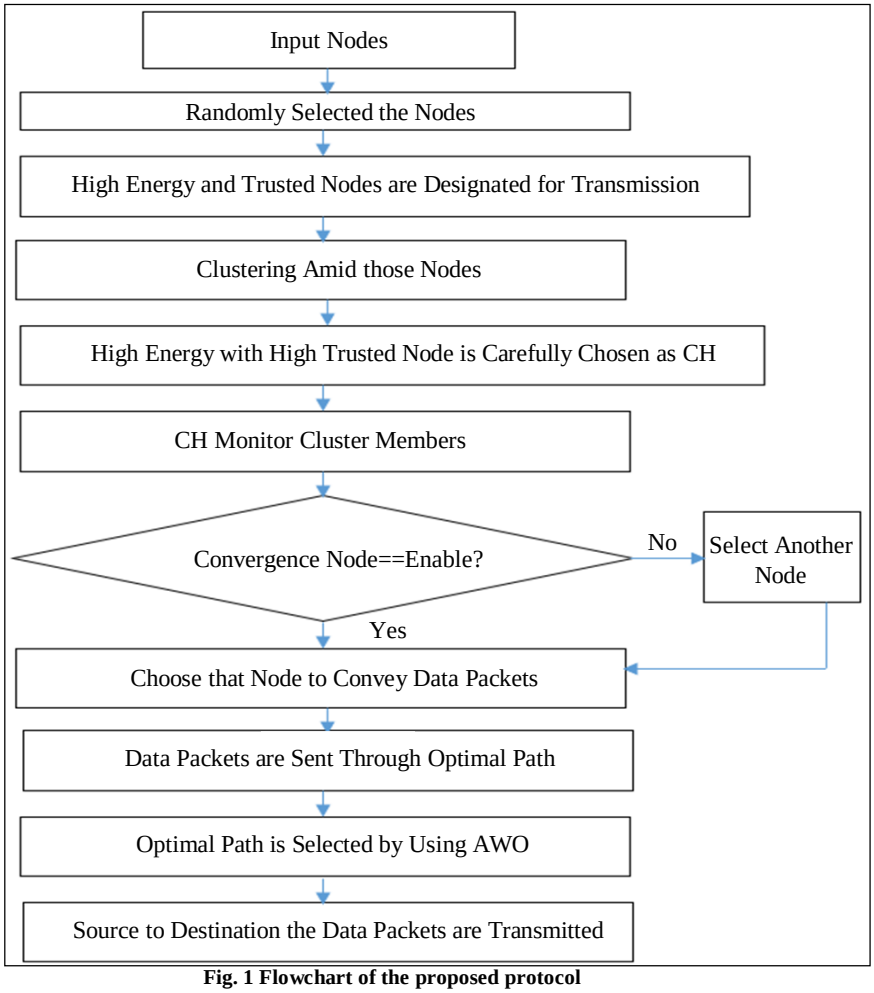

Fig. 1 Flowchart of the proposed protocol

During the initiation of the network, it is possible for all nodes, denoted as $srn_1, srn_2, \ldots, srn_i, \ldots, srn_N$, to function as CH. Within this network, the CHs see the surrounding environment and transmit the gathered data to their CHs. Later, the designated CH does the data aggregation task and sends the accumulated message to the BS over a predetermined route. Upon receiving the accumulated message, BS assesses the information and issues appropriate commands to the prevailing network conditions. The underlying six presumptions of the network are briefly outlined as follows:

- The BS remains stationary, and its placement is fixed within the network.
- The BS possesses an inexhaustible energy supply and exhibits a significant level of computational capability.
- The position of the BS on the WSN is communicated to all nodes.
- Each node inside the system is homogeneous and may be uniquely identified by a distinct ID, IDsni.
- The nodes within the network are stationary and distributed randomly.
- A positioning mechanism is implemented on each node to ascertain its precise location.

The energy consumption model: One of the primary concerns in WSNs pertains to optimizing energy value in nodes. This is because these WSN nodes are provided by a limited energy capacity, which is not readily replaceable or rechargeable. The node carries out a range of functions, including sensing, processing, sending/receiving messages, and data storage in the server.

The process of communication in SNs is an operation that requires an essential amount of energy. The energy consumption for exchanging each k-bit frame among receptors (srn_i) and srn_j (sender) is determined based on the energy model. It should be noted that the distance between srn_i and $srn_j$is represented by the variable dt. The energy utilized by $srn_i$is derived from the equation.

$$E_{TrX}(k,d) = \begin{cases} E_{el} \times k + E_{fs} \times k + dt^2, & dt < dt_0 \\ E_{el} \times k + E_{mp} \times k + dt^4, & dt < d_0 \end{cases} \quad (1)$$

In addition, the energy utilized by srn_j is represented in equation (2). In this section, we will discuss the second point.

$$E_{ReX}(k,d) = E_{el} \times k \quad (2)$$

The energies utilized in the amp in the unrestricted space, power, and Multi-Path (mp) model are denoted as E_{el}, E_{fs}, and E_{mp}, respectively. Additionally, the distance threshold, denoted as dt_0, can be determined by the equation $\sqrt{E_{fs}/E_{mp}}$.

The concept of an attack model: Due to the distinctive characteristics exhibited by WSNs, such as dynamic topology, deployment in challenging and inaccessible environments, and the absence of a central controller, continuous monitoring of these networks is exceedingly tricky [19, 20]. Furthermore, malicious individuals can gain unauthorized access to, manipulate, or alter the data transmitted between SNs due to the wireless link between these nodes. Therefore, it can be inferred that these networks are susceptible to cybersecurity breaches [21]. The AWORTSP routing technique is a routing scheme utilized in network communication systems.

The calculation of trust value: To identify nodes not behaving correctly, each node observes and monitors one or more behavioral features shown by its neighboring nodes. The mapping of each behavioral aspect establishes a trust metric, which is then aggregated to form a composite measure known as the trust value. Direct trust is the value solely derived from an individual node's self-observations. Nodes can assess the trustworthiness of other nodes by utilizing suggestions from neighboring nodes. This process, known as indirect trust, allows nodes to create an opinion on the reliability of other nodes. Subsequently, direct and indirect trust values are summated to derive the overall trust value.

The trust design is performed within discrete time intervals referred to as rounds. Node Nd will compute the overall trust of node tN according to the provided equation. Node Nd evaluates the direct trust of node tN at time t, provided that these nodes are one-hop neighbors. The suggested cluster approach involves node Nd utilizing the immediate comment of node tN during the periodic trust evaluation cycle.

Node Nd has implemented a particular detection technique to gather direct observations to evaluate node tN. It is important to note that nodes Nd and tN are adjacent to one other, with a one-hop distance, at time t. A node's trustworthiness can be assessed through a comprehensive investigation of qualitative and quantitative factors that influence values of direct trust. In the projected approach, the sender was acknowledged (Agd) for the packet transmission.

The parameters encompass the following: if node Nd monitors node tN, the proportion of obtained packets corresponds to the assured number of Agd transmitted by node tN. The proportion would not exceed the ratio of node tN. Based on the observed difference in the proportion, node P could determine if node tN exhibits response foraging activity. According to reference [16], if there is an insignificant and consistent change in the ratio of acknowledged packets during the successive time interval (t_i, t_{i-1}), it can be inferred that node j is functioning well. Equation (1) computes the ratio of the received packet rate.

$$Rp_{Nd,tN}(t) = \frac{Rp_{Nd,tN}(t) - Rp_{Nd,tN}(t-1)}{Rp_{Nd,tN}(t) + Rp_{Nd,tN}(t-1)} \quad (3)$$

One protective measure against replay Agd attacks involves monitoring receiving nodes and their acknowledgment of predefined time intervals. The direct trust $(Dt_{Nd},(t))$ of node Nd for node tN is determined by combining various trust variables, as described in Equation (4).

$$\mathrm{D}t_{Nd,tN}(t) = w_1 * \left(1 - \left|\mathrm{R}p_{Nd,tN}(t)\right|\right) + w_2 * \left|Sp_{Nd,tN}(t)\right| + w_3\left(1 - \left|DF_{Nd,tN,}(t)\right|\right) + w_4 * \left|FA_{Nd,tN}(t)\right| \quad (4)$$

Reputation Trust Calculation: When determining trust with reputation RV values, it is necessary to consider communicating trust with information trust. The reputation of SN i to SN j is represented by the beta distribution β, which can be stated as,

$$RV_{ij} = \beta(\mathfrak{a} + 1, \mathfrak{b} + 1) \quad (5)$$

Here, $\mathfrak{a}$ and $\mathfrak{b}$ are parameters that determine the shape of the distribution. The concept of DT analysis pertains (rewritten in Equation (4)) to the probabilistic P anticipation of the reputation functionality, as represented by the equation:

$$Dt_{Nd,tN}(t) = P\left(RV_{ij}\right) = \frac{\mathfrak{a}+1}{\mathfrak{a}+\mathfrak{b}+2} \quad (6)$$

Equation (6) demonstrates that, during the analysis of a node, only the values of a and b are retained. Following the trust computation, node Nd classified node tN's behavior based on the trust rate. Calculation (7) categorizes a node's Behavior Level (Bl) into two distinct classifications: standard and malevolent. If the behavior of a node is equivalent to or exceeds 0.8, it is classified as malevolent and excluded from the CH selection process.

$$Bl_Q = \frac{1}{Dt_{Nd,tN}(t)} \quad (7)$$

A node can be considered normal if the value of Bl_Q is within the range of 0 to 0.7, inclusive. A node can be

classified as malicious if its Bl_Q Value falls within the range of 0.8 to 1. Once the energy calculation and trust node detection processes are completed, the nodes are clustered to facilitate efficient and optimal routing. Each cluster consists of four types of SNs, including a backup node, Cluster Member (CM), CH, and cluster gateway. The preliminary construction of the CH is performed by the Weighted Clustering (WC) approach in the anticipated approach, while the projected procedures will handle the cluster preservation.

During the cluster establishment phase, the node with the lowermost united weight will be chosen as the CH. In contrast, the node with the second lowermost collective weight will be designated as the backup node for the cluster. In the AWORTSP system, the CH is responsible for allocating resources to all members within a cluster.

The cluster gateway node is accountable for facilitating messages between different clusters. If the definite CH is absent, the backup node can assume the role of CH to prevent clustering complexity and reduce message broadcast within the cluster. A clustering technique will identify the novel selected as CH with the highest weight in the subsequent analysis. The operational mechanisms of the forthcoming procedure are delineated as follows:

- If two CHs exhibit similarity, the deviations in CHs will be distorted until the delay time. If the CH variations are within the same bandwidth, they will be overdue up to a specific limit.
- The significance of the old CH, backup node, and innovative CH lies in their design principles, which are based on the degree of the node and the battery life.
- Based on the principle of priority, if the precedence of a new CH is higher than that of an existing CH, the new CH will retain its role as the CH. In contrast, the priority of the older CH will be assigned to the backup node's priority. If the priority of a previous CH is more advanced than a backup node, the previous CH will be designated as the backup node and will function as a cluster member. Otherwise, the last CH will serve as a CM, and the backup SN will maintain its current rank.
- The primary characteristic of a backup node, CH, is determined by the combined metrics of node degree and lasting battery capacity of the recently arriving CH.
- The maximum border is determined by separating the transmission series by the speed multiplied by two.

Suppose the precedence of a novel CH is lower than that of an earlier CH, and the precedence of the novel CH is higher than that of a backup node. In that case, the novel CH will function as a backup node and perform as a CM, while the earlier CH will continue to function as the CH for the cluster. Otherwise, if the novel CH does not meet these conditions, it will function as a CM within the cluster. To examine the malicious node and minimize the transmission duration, the optimal path has been chosen based on the AWOR.

3.1. Adaptive WO for Optimal Routing

The WO method is a metaheuristic approach that operates on a population-based framework. In this algorithm, the individuals inside the population, referred to as SNs, are modeled as walruses. Within the context of the optimization issue, each walrus in the WO algorithm represents a possible solution. These walruses are responsible for selecting the ideal nodes as part of the optimization process.

Therefore, the spatial arrangement of each walrus, referred to as a node, within the search space establishes the potential standards for the variables associated with the problem. Hence, it can be inferred that individual walruses can be represented as vectors, and the dynamics of the walrus population can be mathematically described by employing a population matrix. During the earliest stages of WO deployment, the populations of walruses are initialized randomly. The population matrix of the WO is obtained using Equation (8).

$$X = \begin{bmatrix} WX_1 \\ \vdots \\ WX_i \\ \vdots \\ WX_N \end{bmatrix}_{N\times M} = \begin{bmatrix} wx_{1,1} & \cdots & wx_{1,j} & \cdots & wx_{1,m} \\ \vdots & \ddots & \vdots & \iddots & \vdots \\ wx_{i,1} & \cdots & wx_{i,j} & \cdots & wx_{i,m} \\ \vdots & \ddots & \vdots & \iddots & \vdots \\ wx_{N,1} & \cdots & wx_{N,1} & \cdots & wx_{N,1} \end{bmatrix}_N \quad (8)$$

Let WX represent the population of walruses, WX_i denote the ith walrus's optimal solution, $wx_{i,j}$ signify the rate of the jth result inconstant proposed through the ith walrus, N denotes the total quantity of walruses, and M represents the choice variable quantity. For example, as previously stated, apiece walrus aids as a potential result to the delinquent at hand. By considering the proposed values for the decision variables associated with each walrus, the OF of the problem may be assessed. The expected standards for the OF derived from walruses are indicated in Equation (9).

$$FV = \begin{bmatrix} FV_1 \\ \vdots \\ FV_i \\ \vdots \\ FV_N \end{bmatrix} \quad (9)$$

The OF vector, denoted as FV represents the set of OFs. Each element of the vector, FV_i, corresponds to the value of the OF assessed for the ith walrus. The values of the OF serve as the most influential metric for evaluating the quality of potential solutions. The optimal result that yields the highest value for the OF is sometimes called the best contender. Conversely, the candidate result that causes the most unfavorable cost for the goal occupation is referred to

as the worst member. Based on the iterative updates of the OF values, the finest and worst individuals are also subject to modification. Modifying the location of walruses within the WO is conceptualized into three distinct phases, which are determined by the inherent behavioral patterns exhibited by this species.

The initial stage involves implementing a feeding plan focused explicitly on exploration. Walruses exhibit dietary diversity by consuming an extensive range of marine creatures, including over sixty species, for instance, sea cucumbers, tube worms, tunicates, soft corals, shrimp, and numerous mollusks [22]. The walrus uses its vigorous flipper movements and sensitive vibrissae to locate and acquire food [23]. The mathematical modeling of walrus movement updates their position by incorporating the feeding mechanism, with the most crucial member of the group providing guidance. This process is represented by Equations (10) and (11). During this procedure, a novel location (referred to as a "new node")for the walrus is initially created according to Equation (12). The new location, denoted as Ts, is considered a replacement for the prior position if it leads to an improvement in the value of the OF. This concept is mathematically represented in Equation (13).

$$wx_{i,j}^{P_1} = wx_{i,j} + rand_{i,j}.\left(SW_j - Is_{i,j}.wx_{i,j}\right) \quad (10)$$

$$WX_i = \begin{cases} WX_i^{P_1} & F_i^{P_1} < F_i, \\ WX_i & else, \end{cases} \quad (11)$$

The position of the ith walrus in the first phase is denoted as wx_i^{P1}, where i represents the walrus index. The jth dimension of this position is represented as $wx_{i,j}^{P1}$. The OF value of the ith walrus in the first phase is denoted as F_i^{P1}. The random numbers $rand_{i,j}$ are generated from the recess (0, 1). The finest candidate result, measured as the robust walrus, is denoted as SW.

The integers $Is_{i,j}$ are randomly selected from the set {1, 2}. The use of the parameter $Is_{i,j}$ enhances the exploration capability of the algorithm. Specifically, setting it to 2 leads to more substantial and extensive changes in the walruses' positions, in contrast to the default value of 1, which represents the usual displacement state. These criteria enhance the algorithm's global search capabilities by enabling it to escape from local bests and identify the original optimal region inside the problem-solving domain.

The second step involves the process of migration. The migration procedure, known as Ts, is utilized in the field of WO to facilitate the navigation of walruses within the search space, enabling them to identify and explore suitable habitats. The mathematical modeling of this behavioral mechanism is represented by Equations (12) and (13). The underlying assumption of this model is that each walrus undergoes migration to a different walrus, selected randomly, inside a distinct region of the search space. Consequently, the novel location is initially derived by Equation (12). According to reference [13], if the unknown location enhances the amount of the function goal, it supersedes the previous location of the walrus.

$$wx_{i,j}^{P_2} = \begin{cases} wx_{i,j} + rand_{i,j}.(wx_{k,j} - Is_{i,j}.wx_{i,j}, & FV_k < FV_i; \\ wx_{i,j} + rand_{i,j}.\left(wx_{i,j} - wx_{k,j}\right), & else \end{cases} \quad (12)$$

$$WX_i = \begin{cases} WX_i^{P_2} & FV_i^{P_2} < FV_i, \\ WX_i & else, \end{cases} \quad (13)$$

The variable $WX_i^{P_2}$represents the newly produced position for the ith walrus in the second phase. Similarly, $WX_{i,j}^{P_2}$ denotes the OF value of the ith walrus in the jth dimension. The position of the designated walrus to travel the ith walrus near it is represented by WX_k, where k is an element of the set $\{1,2,\ldots,N\}$ and k is not equal to i. Additionally, $wx_{k,j}$ represents the jth dimension of the selected walrus and FV_k represents it's OF rate.

Exploitation: Walruses are consistently predicated through the assassin whale and the polar bear. Implementing evasion and combat tactics against these assassins resulted in relocating the walruses from their initial position within the surrounding area. The simulation of the natural performance of walruses enhances the exploitation capability of the WO algorithm in the local search within the problem-solving space surrounding potential results. The WO design assumes that the range of walrus location shift happens in a neighborhood centered around each walrus, with a specific radius.

Given the initial repetitions of the algorithm, it is observed that emphasis is placed on a global search to identify the most optimal region within the search space. To facilitate this, the neighborhood radius was treated as the variable, initially set to its maximum values, and subsequently reduced during each iteration of the algorithm. Considering this rationale, the current phase of the WO model has incorporated the utilization of local lower and upper boundaries to establish a changeable radius via multiple iterations of the algorithm.

WO assumes a neighborhood surrounding each walrus to simulate this behavior in the context of walruses. Within this neighborhood, a new position is created for each walrus by employing the randomization techniques described in Equations (12) and (13). If there is an improvement in the value of the OF, the new location will replace the prior position following Equation (14).

$$wx_{i,j}^{P_2} = wx_{i,j} + \left(ub_{local,j}^{t,} + \left(ub_{local,j}^{t} - rand.lb_{local,j}^{t}\right)\right) \quad (14)$$

$$Local\ bounds: \begin{cases} lb_{local,j}^{t} = \frac{c}{t}, \\ ub_{local,j}^{t,} = \frac{ub_j}{t}, \end{cases} \quad (15)$$

$$WX_i = \begin{cases} wX_i^{P_3} & FV_i^{P_3} < FV_i, \\ WX_i & else, \end{cases} \quad (16)$$

The position of the ith walrus, denoted as $WX_i^{P_3}$, is determined based on the 3rd phase. $WX_{i,j}^{P_3}$ represents the jth dimension of this position. $FV_i^{P_3}$ represents the OF value of the ith walrus. The variable t represents the iteration contour. ub_j, lb_j are the upper and lower bounds, respectively, for the jth variable. $lb_{local,j}^{t}$ and $ub_{local,j}^{t,}$, which are used to pretend local exploration near the applicant results. The repetition progression is a method that involves the repeated performance or occurrence of a particular action, event, or sequence of events.

The following is a representation of pseudocode for the algorithm known as WO. Upon incorporating the advancements made during the initial, second, and third phases, the positional data of the walruses has been updated. Consequently, the first iteration of the WO algorithm has been successfully executed, resulting in the derivation of fresh positional values for the walruses and OFs. Updating and improving candidate solutions is iteratively performed per the workflow processes outlined by the equations. The last repetition is reached at (10) to (16).

After the algorithm has finished executing, WO presents the most optimal candidate solution discovered throughout the execution as the solution to the specified problem. Continue to iterate through the processes until all final requirements have been met. However, the computational complexity of this optimization is considerable. To mitigate this issue, the WO optimal parameter is selected using an enhanced version of the GWO algorithm called Improved GWO (IGWO), referred to as AWO. In the typical GWO algorithm, selecting β, α, and δ wolves from the wolf pack is based on the fitness of everyone. Subsequently, the positions of the individuals chosen are updated using the following formulas:

$$\overrightarrow{WX}_{k,i}^{t+1} = \frac{\overrightarrow{WV_{\alpha,i}^{t}} + \overrightarrow{WV_{\beta,i}^{t}} + \overrightarrow{WV_{\delta,i}^{t}}}{3} \quad (17)$$

$$\overrightarrow{WV_{k,i}^{t}} = \overrightarrow{wx_k^t} - A.|C.\overrightarrow{wx_k^t} - \overrightarrow{wx_i^t}| \quad (18)$$

The variables $\overrightarrow{wx_i^t}$ and $\overrightarrow{WX}_{k,i}^{t+1}$ represent the i-th location and separate in the t-th and (t+1)-th iterations, respectively.

The variable $\overrightarrow{wx_k^t}$ signifies the position of the k-th distinct, where k can signify the location of α, β, and δ. The variables A and C have the same meaning as the formulation in WOA.

The concept of AWOR refers to a modified approach to routing work orders. An adaptive scaling factor is a variable that dynamically adjusts or modifies a specific parameter or value based on changing conditions or inputs. In both the WO and GWO algorithms, the scaling factor exhibits a linear reduction to regulate the transition from global optimization to local optimization. Nevertheless, this methodology is inadequate in addressing the pragmatic circumstances, given that most optimization problems entail intricate non-linear procedures. Therefore, a formula for an adaptive scaling factor is presented in the following manner:

$$ad = 2 - \min\left\{2, \frac{Of_*^{t-1}}{Of_*^{t}}(1 - \cos\frac{t\pi}{T}\right\} \quad (19)$$

Here, Of_*^t andOf_*^{t-1} Correspondingly, they represent the optimal fitness values in the recent and previous iteration. In the given equation, the scaling factor is influenced by the ratio of $\frac{Of_*^{t-1}}{Of_*^{t}}$, which results in an increased search range if $\frac{Of_*^{t-1}}{Of_*^{t}}$ or vice versa $\frac{Of_*^{t-1}}{Of_*^{t}} \geq 1$ is greater than or equal to 1. The cosine function presents a non-linear element in the scaling factor. Moreover, utilizing the minimal value function guarantees that the scaling factor equals or exceeds zero.

3.2. Enhancing the Model Using GWO

Within the framework of the WO, it is observed that an individual's ideal position is crucial in controlling the position update for other individuals. This approach has the potential to expedite convergence, but its robustness is limited, as it may become trapped in the vicinity of a suboptimal solution.

To improve the capacity to search for global solutions and expedite the convergence of local optimization, the position update formula of the GWO is implemented as a replacement for the initial optimal position update method. In addition, we introduce the historical optimal location of each individual, denoted as $\overrightarrow{WX_l^t}$, to calculate WV_l^t. The updated formula for determining position is as follows:

$$\overrightarrow{WX_i}^{t+1} = wg_\alpha^t\,\overrightarrow{WV_\alpha^t} + wg_\beta^t\,\overrightarrow{WV_\beta^t} + wg_\delta^t\,\overrightarrow{WV_\delta^t} \quad (20)$$

The variables wg_α, wg_β, wg_δ, and w_l represent the weights assigned to α, β, δ, and the ideal local location. Similarly, $\overrightarrow{WV_\alpha^t}$, $\overrightarrow{WV_\beta^t}$, and $\overrightarrow{WV_l^t}$ denote the instruction vectors associated with α, β, δ, and the historical optimal position of each person. The weights w_α^t, w_β^t, w_δ^t, and w_l^t are

contingent upon the suitability of their corresponding places. In the context of minimal optimization, it is observed that the location is assigned a higher weight when the fitness value is smaller. Subsequently, these weights are normalized to fall within the range of (0, 1). The weight may be determined through the utilization of the following calculation:

$$wg_k^t = \frac{1}{of_k^t \cdot \left(\sum \frac{1}{of_j^t}\right)} \quad (21)$$

The symbol Of_k^t represents the fitness at location k,j in $\sum \frac{1}{Of_j}$, which can indicate the fitness of α, β, δ, or the historical ideal position l for each person. In the GWO algorithm, the influence of the optimal position is controlled by a randomly generated number, denoted as C_i, which lies within the range of (0, 2). Nevertheless, this approach is characterized by a lack of control regarding the precise balance between global and local optimization.

To address this problem, the variables |1 - ad| and 1 - |1 - ad| are incorporated as enhancements to the original $\overrightarrow{WV}_{k,i}^t$. The variable |1 - ad| is used to regulate the impact of α, β, and δ, while 1 - |1 - ad| is employed to control the inspiration of the historical ideal location, l. As the value of "a" drops from 2 to 0, the absolute value of "1 - ad" initially declines from 1 to 0, then increases from 0 to 1.

This approach effectively exploits the α, β, and δ positions, promoting convergence in the initial and concluding stages. During the intermediate stage, when the absolute value of the difference between 1 and ad is near zero, and the absolute worth of the difference between 1 and ad is close to 1, the primary influence on the position update is determined by the variable l and random fluctuations. As a result, the population exhibits enhanced global optimization capabilities. The expression for V^t can be stated as follows:

$$\overrightarrow{WV}_{k,i}^t = |1 - ad|\overrightarrow{WX}_k^t - A * ||1 - ad|\overrightarrow{WX}_k^t - \overrightarrow{WX}_i^t| \quad (22)$$

$$\overrightarrow{WV}_{l,i}^t = \left(1 - |1 - ad|\overrightarrow{WX}_l^t - A * (1 - |1 - ad|)\overrightarrow{WX}_l^t - \overrightarrow{WX}_i^t\right) \quad (23)$$

The variable k in the vector $\overrightarrow{WX}_k^t$ can be denoted by the symbols α, β, and δ. In the optimization procedure, the warmup technique is employed. Specifically, during the initial N_{warmup} iterations (e.g., 2), a significantly reduced scaling factor (e.g., 0.1) is utilized. Subsequently, after the warmup rounds, the scaling factor returns to its regular behavior. This approach facilitates the identification of an optimal direction for the entire community, enabling individuals to discern the most effective means of improving their physical fitness.

3.2.1. The Integration of an Enhanced Hunting Strategy from the GWO into the WO

Within the study, two methods, spiral hunting, and the usual optimal position update method, are employed in the WO algorithm. Each of these methods has an equal probability of 50% of being implemented. A novel possibility, denoted as p, is offered due to the broader search scope of the spiral hunting method and the more local scope of the optimal position update approach. The variable p represents the probability associated with the spiral hunting technique, and it diminishes gradually toward zero as the process unfolds. This approach of branch control effectively maintains a population density that is neither excessively dense nor excessively sparse.

$$p = \theta^t . \frac{ad}{2} \quad (24)$$

$$\theta^t = \frac{N.Of_*^{t-1}}{\sum_{i=1}^{N} Of_{1\,i}^t} \quad (25)$$

The expression $\sum_{i=1}^{N} Of_{1\,i}^t$ denotes the summation of the fitness values of all people in the population. The variable N represents the total number of personalities in the population. Lastly, Of_*^{t-1} represents the best fitness value among the individuals in the current population. One of the key challenges in SI is the significant increase in the concentration ratio θ inside the population. As the value of θ increases, it leads to a reduction in the diversity of the population, hence posing challenges to the pursuit of global optimization. Consequently, the concentration ratio of the population is computed and utilized to regulate the ratio θ. The pseudocode for implementing the AWO algorithm is outlined in the following pseudocode.

Start AWO
  Input nodes (population)
  Set the N and the T as iteration number
  walruses' locations Initialization process
  For $t = 1{:}T$
    Update the strongest walrus (i.e., node)
    For $i = 1{:}N$
Stage 1: Alimentation strategy of exploration
  Compute the new location of the jth walrus using (8).
  Apprise the ith walrus location via (9).
Stage 2: Migration
  Select an immigration terminus for the ith walrus.
  Compute the novel location of the jth walrus via (7).
  Apprise the ith walrus position via (8).
Stage 3: Absconding and aggressive against hunters (exploitation)
  Compute a new location in the locality of the walrus via (10)
  Apprise the $i$thwalrus location using (11).
  // The optimal parameter selection is done by using IGWO//

Observed signals were monitored and then centered and blanched.

Initialize parameters of ad, $\overrightarrow{Wx_l^t}$, $\overrightarrow{WV_{k,i}^t}$, α, β, and δ, and p , and then generate a certain number of separation matrixes as grey wolf individuals initialize the position and decision radius of these grey wolves and then compute each grey wolf's initial fitness rate.

Compute the optimal position and the optimal fitness of these particles.

Update individual position according to (18), authorize the set of neighbors using (19), and compute the probability of movement via Equation (20).

Estimate each grey wolf's next position and decision radius, and further recommence the next step size.

Estimate the optimal fitness rate of all grey wolves.

If optimal fitness value > fitness, new locations will be updated.

Regulate whether to gratify the end condition.

If satisfied, jump out of the loop; else, go to Step 4.

end

Save the best candidate solution as the optimal node selection result so far.

end

Return the output to the best optimal node

End AWO

4. Results and Discussion

This segment will analyze the performance parameters of the proposed AWORTSP and compare them with existing trust-based routing schemes such as Adapted Fire Hawk Cluster-based Trusted Coati Optimal Routing (AFHC-NTCOR), Hybrid Moth Flame Optimizer and Firefly Algorithm (MFO-FA) and RDSAOA-EECP (energy and distance based multi-objective red fox optimization) [25].

Experiments were performed using MATLAB 2020A, and simulations were executed on a system with an Intel i7 64-bit CPU, 12GB of RAM, and storage comprising a 500GB SSD and a 1TB HDD. The system's performances were compared to alternative secure routing methodologies regarding energy consumption, latency, data transfer rate, PLR, DR, and accuracy. The performance review provides evidence of the superior and positive performance of AWORTSP compared to alternative approaches.

4.1. Residual Energy

Figure 2 examines the RE across various methods. In each node, the energy consumption is equivalent to the total energy necessary for executing data transmission operations, such as transmitting or receiving data. According to the data presented in the figure, it can be observed that AWORTSP exhibits the highest RE level. Compared to AFHC-NTCOR, Hybrid MFO-FA, and RDSAOA-EECP, AWORTSP demonstrates an improvement in this metric by 2%, 17%, and 27%. According to the findings presented in Figure 2, the trust value plays a crucial role in mitigating the detrimental impact of hostile SNs on their energy, hence enhancing energy consumption in the AWORTSP protocol. In contrast, the suggested technique emphasizes the energy levels of the identified paths in the routing mechanism. The factors mentioned above have a favorable impact on the functioning of AWORTSP.

Furthermore, a negative correlation exists between the measure of remaining energy and assailants. If numerous attackers infiltrate the WSN network, it can be observed that the energy level across all protocols will diminish. Conversely, it can be inferred that the occurrence of malevolent nodes has the contrary consequence of augmenting the energy consumption of target nodes during the transmission of a substantial quantity of RREQs throughout the network.

Figure 3 displays the graphical depiction of the comparison of EE. Based on the data presented in the figure, it can be observed that AWORTSP exhibits the highest EE, with improvements of 57.71% 86.45%, and a twofold increase in comparison AFHC-NTCOR, Hybrid MFO-FA and RDSAOA-EECP, respectively. This finding demonstrates that using AWORTSP can significantly prolong a network's lifespan.

A positive correlation exists between the amount of WSN nodes and energy efficiency, indicating that energy efficiency also increases as the number of SNs increases. This implies that a direct correlation exists between these two parameters. The underlying cause of this matter is readily apparent. In scenarios where the network exhibits high density, the inter-node distance is reduced, enabling SNs to establish more optimal and reliable paths. Consequently, this leads to enhanced EE within the network.

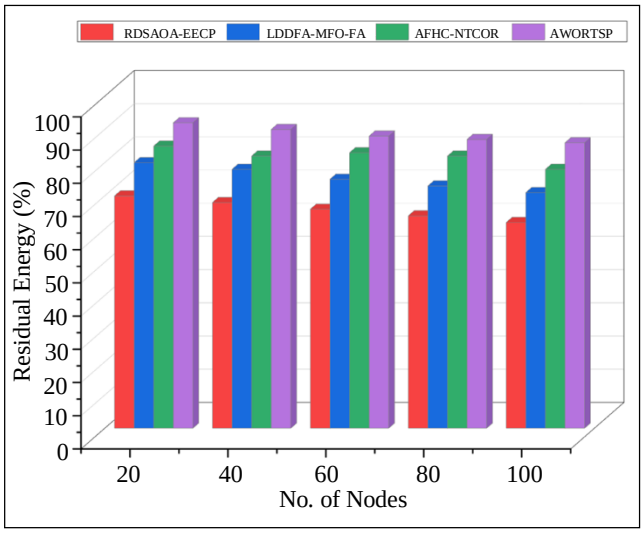

Fig. 2 RE comparison among proposed and existing protocols

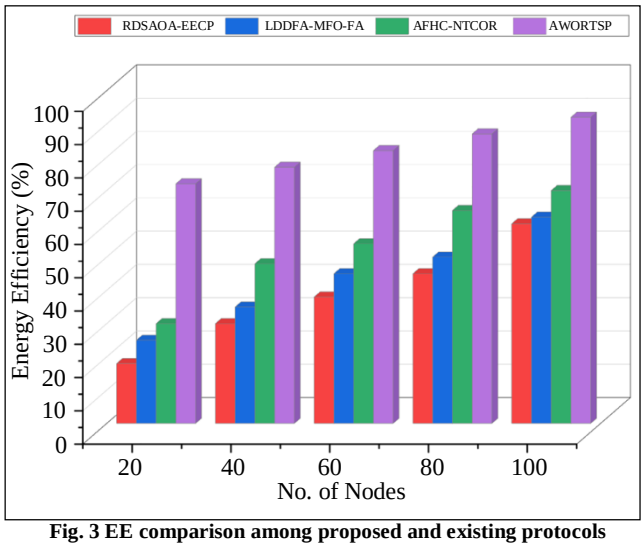

Fig. 3 EE comparison among proposed and existing protocols

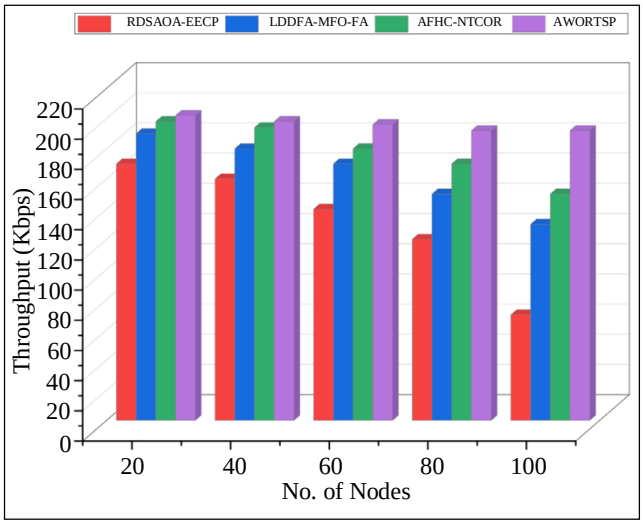

Fig. 4 Throughput comparison among protocols

4.2. Throughput

Figure 4 presents a comparison of throughput across several systems. Throughput refers to the quantity of packets effectively communicated to the intended destination within a specified time. The AWORTSP methodology exhibits the maximum efficiency of 190kbps compared to alternative methods such as AFHC-NTCOR, Hybrid MFO-FA, and RDSAOA-EECP. AWORTSP's consideration of the quality of the identified paths.

Accordingly, using AWORTSP can potentially enhance the rate at which data is delivered, thereby positively impacting the overall throughput. Moreover, CHs are selected from a pool of reliable nodes to mitigate the potential adverse impact of malevolent nodes on both communications. Based on the findings in Figure 4, a negative correlation is observed between the number of attackers and the throughput. In Figure 4, the AWORTSP algorithm demonstrates a reduced susceptibility to hostile nodes due to the effective security mechanism incorporated within its architecture, enabling the detection and isolation of such nodes. Therefore, it is unlikely that they would exert a detrimental impact on the overall performance of this plan.

4.3. Packet Delivery Ratio

Figure 5 depicts a performance comparison of the proposed AWORTSP algorithm with known methods such as AFHC-NTCOR, Hybrid MFO-FA, and RDSAOA-EECP. The suggested scheme achieved a higher PDR than existing schemes due to the effective trust evaluation and cluster formation. The selection of optimal parameters in the IGWO has increased the PDR within the context of AWO optimal routing. As the number of nodes expands, the PLR increases across all routing algorithms.

4.4. PLR

In this section, a comparison between the PLR and the number of nodes in WSN is visually represented in Figure 6. The suggested AWORTSP exhibits a lower PLR compared to existing protocol schemes such as AFHC-NTCOR, Hybrid MFO-FA, and RDSAOA-EECP, which result in reductions of 47.22%, 60.80%, and 75.32%, respectively. As the nodes rise, there is a corresponding drop in packet loss for all routing techniques. Increasing nodes in a network will enhance the potential for discovering a suitable node to facilitate the forwarding of packets.

Consequently, the AWO system efficiently and promptly detects and isolates adversarial nodes within the network. Because of this phenomenon, nodes that exhibit hostile behavior are effectively barred from engaging in the routing process. Path eminence refers to assessing the amount at which packets are delivered to intermediate nodes along a given path. As a result, if a pathway exhibits substandard characteristics, it is not chosen to transmit data.

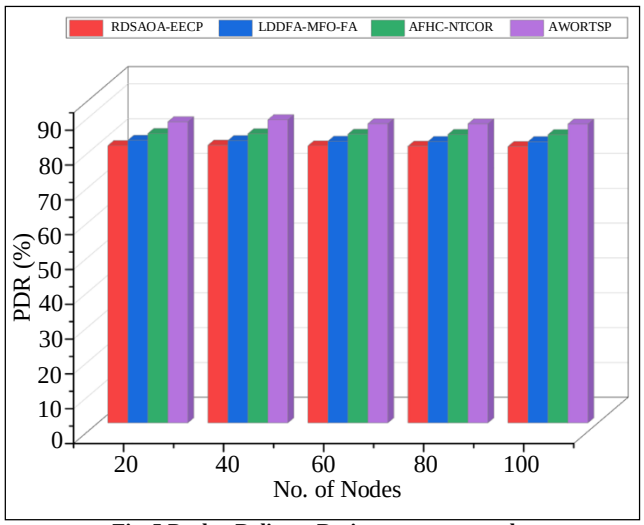

Fig. 5 Packet Delivery Ratio among protocols

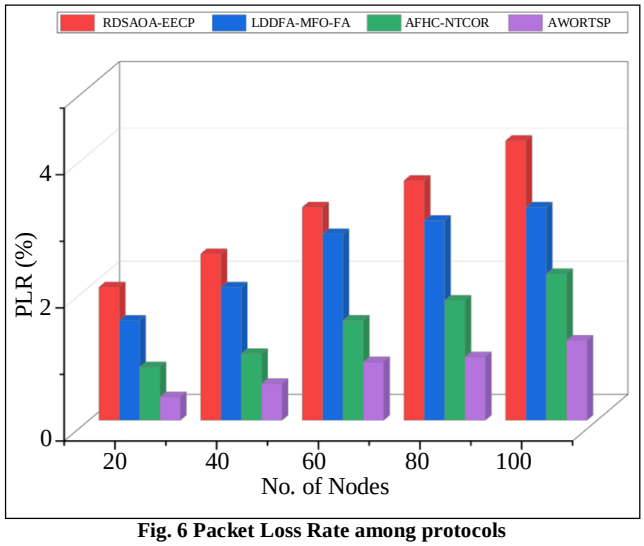

Fig. 6 Packet Loss Rate among protocols

The factors mentioned above contribute to a decrease in the PLR within the context of the analyzed work AWORTSP. Conversely, as indicated by Figure 6, an improvement in total nodes inside the network corresponds to a corresponding increase in the PLR. This can be attributed to the heightened congestion within the network, resulting in collisions and subsequent loss of packets.

4.5. End-to-End Delay

Figure 7 presents a comparison of the delay seen in various ways. The term "delay" refers to the average time it takes for a data packet to be transmitted from its source to its destination. The proposed AWORTSP significantly reduces delay compared to AFHC-NTCOR, Hybrid MFO-FA, and RDSAOA-EECP. Specifically, AWORTSP achieves a delay reduction of 32.20%, 42.83%, and 58.17% compared to the algorithms. The primary rationale behind this phenomenon is that AWORTSP prioritizes selecting pathways that exhibit high energy, superior quality, and dependable performance to facilitate data transfer. Consequently, this leads to a decrease in route failure, thereby reducing the necessity for the route detection process. Specifically, the resulting network delay is elevated when many attackers infiltrate the network. The trust mechanism in AWORTSP can promptly and effectively detect and isolate hostile nodes. By swiftly reducing the trust levels of hostile nodes in response to their hostile behavior, AWORTSP ensures efficient identification and separation.

4.6. Detection Rate

Figure 8 presents a comparison of the DRs across several techniques. The DR measures the efficacy of trust systems implemented in different schemes to identify rogue nodes inside a network. The quantity is equivalent to the proportion of discovered harmful nodes to the total number of malicious nodes inside the network. The proposed AWORTSP demonstrates an improvement in the discovery rate of 3.34%, 6.98%, and 9.34% compared to the AFHC-NTCOR, Hybrid MFO-FA and RDSAOA-EECP algorithms, respectively. The primary factor contributing to the effective detection capability of the Proposed AWORTSP is the consistent monitoring of SN behavior and evaluation of their trust parameters using a weighted trust mechanism. When the frequency of changes in the PDR of an SN is high, the Wireless Trust Management (WTM) system exponentially reduces its trust level and recognizes this node as a black hole attacker. As a result, the incorporation of weight coefficients has enhanced the efficacy of the WTM system in identifying and detecting aggressive actions perpetrated by potential attackers. According to the findings depicted in Figure 8, an inverse relationship exists between the discovery rate and the number of attackers.

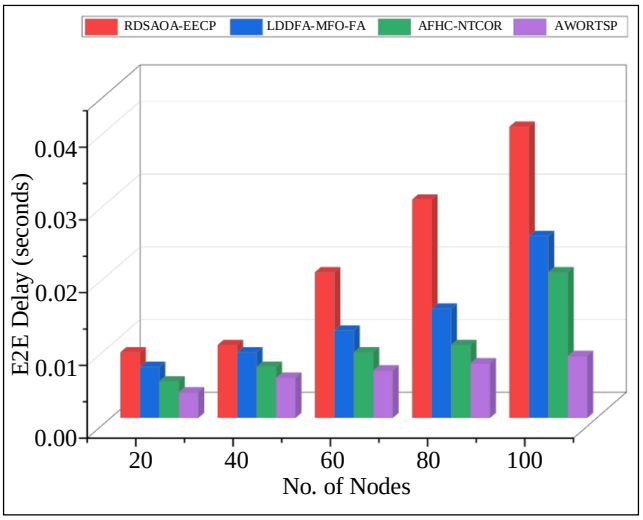

Fig. 7 Delay performance comparison among protocols

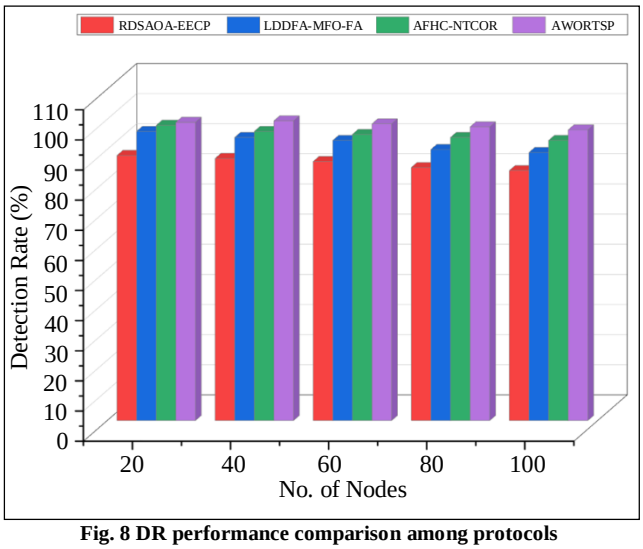

Fig. 8 DR performance comparison among protocols

In instances when a network accommodates a substantial number of attackers, the task of detecting them becomes increasingly challenging for security systems. This difficulty

arises due to the potential collusion and concealment capabilities exhibited by these nodes within the network.

4.7. Communication Cost

Figure 9 illustrates a comparative analysis of communication costs across several schemes. This measure quantifies the frequency of control data transmitted through a node to successfully transmit a packet to the intended destination node and assesses the nodes' trustworthiness. The proposed AWORTSP reduces communication costs compared to the AFHC-NTCOR, Hybrid MFO-FA, and RDSAOA-EECP algorithms. This finding indicates that the AWORTSP exhibits a commendable performance concerning overhead. This phenomenon exerts a beneficial impact on the duration of network operation. The primary cause of this problem stems from the routing process, wherein the proposed AWORTSP algorithm evaluates the reliability, energy, and quality of each discovered route amid source-destination sets. Subsequently, it chooses the route with the highest score to transmit the message. These characteristics assist in the selection of stable routes inside the network. Consequently, there is a decrease in route failures, leading to a corresponding reduction in the necessity to reconstruct failed routes. This phenomenon yields a favorable impact on the reduction of communication expenses.

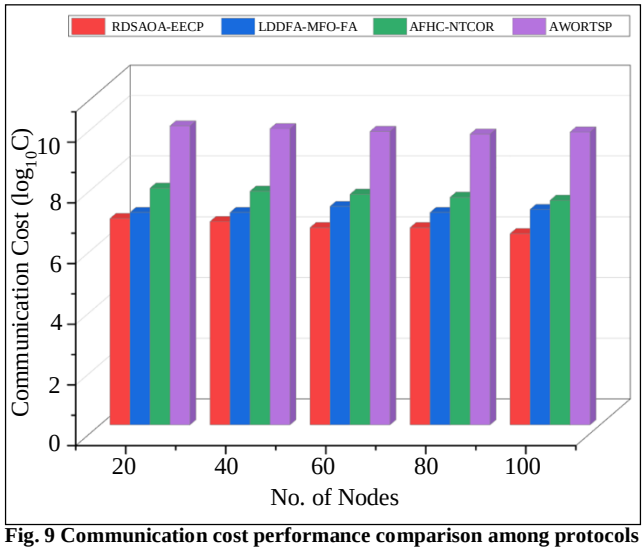

Fig. 9 Communication cost performance comparison among protocols

The AWORTSP model demonstrates promising performance across various metrics compared to other models, including RDSAOA-EECP, LDDFA-MFO-FA, and AFHC-NTCOR. The AWORTSP model excels in balancing EE, data throughput, and reliability. Its consistent outperformance across different metrics positions it as a promising solution for WSNs, especially when energy preservation and reliable data transmission are crucial.

5. Conclusion

This research introduces a novel routing protocol named AWORTSP with three key elements: selecting energy-efficient nodes, utilizing fire hawk-based clustering, and implementing a trusted optimum routing strategy. In this procedure, the initial step involves the identification of high-energy, balanced, and reliable nodes from a set of randomly generated nodes. The merging of nodes into clusters and the CH selections are determined according to the calculation of node properties in a WSN. Furthermore, the proposed methodology introduces a WO methodology to choose CHs from a pool of candidates. This pool consists of SNs with higher ARE and trust levels compared to the Average Remaining Energy (ARE) and ATV of all nodes within the network. The primary objective of AWOR is to minimize the communication overhead during data transfer between the BS and the CH, or vice versa, by determining the most optimum path. Ultimately, the routing process chooses pathways that exhibit superior quality, dependability, and EE. The assessments conducted in this study demonstrate that AWORTSP has outstanding performance concerning PLR, DR, RE, throughput, PDR, and delay. The RE level is enhanced while the throughput experiences improvements. Additionally, the delay is reduced, the DR is increased, and accuracy also increases when compared to the AFHC-NTCOR, Hybrid MFO-FA, and RDSAOA-EECP methods, respectively.

In the future, efforts are directed towards enhancing the precision of the security mechanism devised in AWORTSP by incorporating novel methodologies such as neural networks and swarm-based Reinforcement Learning (RL). The trust device in question possesses considerable efficacy and precision, although it lacks the capacity for self-organization and self-adaptation.

ANNs other learning techniques, like Q-learning, offer valuable solutions for addressing this challenge. Furthermore, the clustering method will be formulated by including several optimization algorithms, and subsequently, an assessment will be conducted to determine their impact on network performance.

Acknowledgments

The authors thank the Saveetha School of Engineering and Saveetha Institute of Medical and Technical Sciences, Chennai, Tamilnadu, India, for their support and motivation throughout this research.

References

[1] Loren P. Clare, Gregory J. Pottie, and Jonathan R. Agre, "Self-Organizing Distributed Sensor Networks," *Unattended Ground Sensor Technologies and Applications*, vol. 3713, pp. 1-9, 1999. [CrossRef] [Google Scholar] [Publisher Link]

[2] Muhammad Ali Jamshed et al., "Challenges, Applications, and Future of Wireless Sensors in Internet of Things: A Review," *IEEE Sensors Journal*, vol. 22, no. 6, pp. 5482-5494, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] Xinying Yu et al., "Trust-Based Secure Directed Diffusion Routing Protocol in WSNs," *Journal of Ambient Intelligences and Humanized Computing*, vol. 13, pp. 1405-1417, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] Zaher Al Aghbari et al., "Routing in Wireless Sensor Networks Using Optimization Techniques: A Survey," *Wireless Personal Communications*, vol. 111, pp. 2407-2434, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[5] Aravinthkumar Selvaraj et al., "Optimal Virtual Machine Selection for Anomaly Detection Using a Swarm Intelligence Approach," *Applied Soft Computing*, vol. 84, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[6] Nithya Rekha Sivakumar et al., "Enhancing Network Lifespan in Wireless Sensor Networks Using Deep Learning-Based Graph Neural Network," *Physical Communication*, vol. 59, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] R. Eberhart, and J. Kennedy, "A New Optimizer Using Particle Swarm Theory," *MHS'95. Proceedings of the Sixth International Symposium on Micro Machine and Human Science*, Nagoya, Japan, pp. 39-43, 1995. [CrossRef] [Google Scholar] [Publisher Link]

[8] Isabel Dietrich, and Falko Dressler, "On the Lifetime of Wireless Sensor Networks," *ACM Transactions on Sensor Networks*, vol. 5, no. 1, pp. 1-39, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[9] Weidong Fang et al., "Trust Management-Based and Energy Efficient Hierarchical Routing Protocol in Wireless Sensor Networks," *Digital Communications and Networks*, vol. 7, no. 4, pp. 470-478, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] Feras Mohammed A-Matarneh et al., "Swarm Intelligence with Adaptive Neuro-Fuzzy Inference System-Based Routing Protocol for Clustered Wireless Sensor Networks," *Computational Intelligence and Neuroscience*, vol. 2022, pp. 1-12, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Changsun Shin, and Meonghun Lee, "Swarm-Intelligence-Centric Routing Algorithm for Wireless Sensor Networks," *Sensors*, vol. 20, no. 18, pp. 1-13, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] Bhanu Dwivedi et al., "LBR-GWO: Layered Based Routing Approach Using Grey Wolf Optimization Algorithm in Wireless Sensor Networks," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 4, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Osama AlFarraj, Ahmad AlZubi, and Amr Tolba, "Trust-Based Neighbor Selection Using Activation Function for Secure Routing in Wireless Sensor Networks," *Journal of Ambient Intelligence and Humanized Computing*, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[14] Vishal Kumar Arora, Vishal Sharma, and Monika Sachdeva, "ACO Optimized Self-Organized Tree-Based Energy Balanced Algorithm for Wireless Sensor Network," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, pp. 4963-4975, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[15] S. Prithi, and S. Sumathi, "LD^{2}FA-PSO: A Novel Learning Dynamic Deterministic Finite Automata with PSO Algorithm for Secured Energy Efficient Routing in Wireless Sensor Network," *Ad Hoc Networks*, vol. 97, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[16] J.C. Blandón, J.A. López, and L.E. Tobón, "Routing in Wireless Sensor Networks Using Bio-Inspired Algorithms," *Between Science and Engineering*, vol. 12, no. 24, pp. 130-137, 2018. [Google Scholar] [Publisher Link]

[17] Fan Chengli et al., "Hybrid Artificial Bee Colony Algorithm with Variable Neighborhood Search and Memory Mechanism," *Journal of Systems Engineering and Electronics*, vol. 29, no. 2, pp. 405-414, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[18] Zongshan Wang et al., "An Energy Efficient Routing Protocol Based on Improved Artificial Bee Colony Algorithm for Wireless Sensor Networks," *IEEE Access*, vol. 8, pp. 133577-133596, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[19] Biswa Mohan Sahoo, Hari Mohan Pandey, and Tarachand Amgoth, "GAPSO-H: A Hybrid Approach towards Optimizing the Cluster-Based Routing in Wireless Sensor Network," *Swarm and Evolutionary Computation*, vol. 60, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[20] Abhilash Singh, Sandeep Sharma, and Jitendra Singh, "Nature-Inspired Algorithms for Wireless Sensor Networks: A Comprehensive Survey," *Computer Science Review*, vol. 39, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[21] Djallel Eddine Boubiche et al., "Cybersecurity Issues in Wireless Sensor Networks: Current Challenges and Solutions," *Wireless Personal Communications*, vol. 117, pp. 177-213, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[22] Nette Levermann et al., "Feeding Behaviour of Free-Ranging Walruses with Notes on Apparent Dextrality of Flipper Use," *BMC Ecology*, vol. 3, pp. 1-13, 2003. [CrossRef] [Google Scholar] [Publisher Link]

[23] Gay Sheffield et al., "Laboratory Digestion of Prey and Interpretation of Walrus Stomach Contents," *Marine Mammal Science*, vol. 17, no. 2, pp. 310-330, 2001. [CrossRef] [Google Scholar] [Publisher Link]

[24] Rajathi Natarajan et al., "Energy and Distance Based Multi-Objective Red Fox Optimization Algorithm in Wireless Sensor Network," *Sensors*, vol. 22, no. 10, pp. 1-19, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[25] Xingsi Xue et al., "A Hybrid Cross Layer with Harris-Hawks Optimization-Based Efficient Routing for Wireless Sensor Networks," *Symmetry*, vol. 15, no. 2, pp. 1-25, 2023. [CrossRef] [Google Scholar] [Publisher Link]