SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V11I1P107

Volume 11 Issue 1, 86-100, January 2024

Original Article

An Adapted Fire Hawk Cluster-Based Trust Coati Optimal Routing for Effectual Security in 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 *- Wireless Sensor Networks (WSNs) are growing, improving human well-being, and being used for medical and military operations has highlighted the importance of data security. This is essential to avoid data handling, and thus, trust administration is an excellent way to handle these concerns by establishing Sensor Node (SN) trust associations. The Adapted Fire Hawk Cluster-based Novel Trust Coati Optimal Routing (AFHC-NTCOR) technique considers node energy restrictions to improve WSNs network security. The methodology also uses the Fire Hawk Optimizer (FHO) algorithm for clustering that selects Cluster Heads (CHs) from candidate SNs. They are chosen based on their energy reserves and trustworthiness stages, which must be above the network's averages. AFHC-NTCOR uses a trustworthy routing algorithm to determine inter-cluster routing paths. Information is sent from CHs to the Base Station (BS) via these pathways. With the Coati Optimization (CO) algorithm, the suggested route construction strategy considers energy and dependability. The Network Simulator version 2 (NS2) platform compares the AFHC-NTCOR protocol to other safe routing systems in energy consumption, data transfer rate, detection ratio, packet loss frequency, accuracy, and latency. This research shows that AFHC-NTCOR surpasses other methods in usefulness and effectiveness.*

Keywords *- WSN, Clustering, Trust management, Network security, Modified fire hawk, Coati Optimal Routing, Network lifetime.*

1. Introduction

WSNs consist of a multitude of sensors that are distributed over an extensive geographical region. The users assert their responsibility for determining the setting and employ a streamlined, decentralized approach to examine the gathered data [1, 2]. Due to their multifunctionality, these devices possess utility across various domains, including military applications, wherein they can be employed to identify and orchestrate the movements of adversary units. In addition to their application in agriculture monitoring, industrial product control, and the detection of chemical and nuclear radiation and biological risks [3, 4], they are also utilized.

WSNs have proven valuable in various domains, including smart homes, transportation systems, urban environments, and the preservation of historic and commercial landmarks [5, 6]. The nodes inside WSNs are typically equipped with batteries that are not readily replaceable or rechargeable. The nodes necessitate a substantial amount of electricity to effectively carry out their tasks of detecting, processing, and transmitting environmental data.

According to previous research studies [7, 8], the energy consumption associated with data transit is more significant than data processing or sensing. Hence, energy management plays a critical role in WSN. Clustering emerges as a pragmatic and productive approach to attaining this objective.

The utilization of a clustered topology [9] contributes to the enhancement of energy efficiency and the preservation of transmission bandwidth. In this architectural framework, the network is partitioned into many clusters, wherein distinct SNs are assigned responsibilities inside each cluster. Selecting CHs in this scenario presents a challenging undertaking. Hence, exploring alternative approaches, such as meta-heuristic algorithms, is imperative to tackle this difficulty effectively.

Cluster-based routing systems encompass both clusters, such as inter and intra-communication. Enhancing the durability of the network can be attributed to the solutions' scalability and Energy Efficiency (EE). The topic of cluster-based routing in WSNs has garnered significant scholarly interest in recent times.

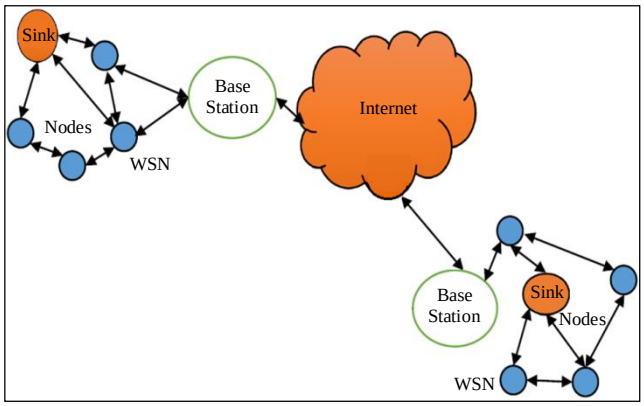

Fig. 1 Flow diagram of proposed model

Nevertheless, further enhancements and modifications are required for these studies to address the unique challenges WSNs pose compared to their wired counterparts. Characteristics commonly associated with WSNs include limited resources, unpredictable connectivity, autonomous operations, and the absence of centralized control [10].

Figure 1 depicts a standard representation of a WSN setting. In this scenario, SNs are distributed around a specific geographical region to gather data on that area. The collected data, comprising various attributes, is received by a central BS or sink node. The transmission adheres to a predetermined trajectory consisting of discrete microsensor nodes. The underlying infrastructure facilitates the transmission process, which includes components like cloud computing.

Hence, establishing secure WSNs poses a significant challenge in environments with elevated risks and a lack of security measures. Therefore, researchers must acknowledge the significance of assuring the data communication security mechanism. A conflict arises when attempting to strike an equilibrium between optimizing safety measures and minimizing energy value. From a particular perspective, the significance of devising secure protocols for SNs is comparable to establishing robust security mechanisms for the secure broadcast of data to the central BS.

Nevertheless, deploying intricate security measures to guarantee secure data transmission is constrained for SNs owing to their restricted access to energy sources. In the context of developing protocols for WSNs, the establishment of a routing mechanism that is both reliable and resource-efficient necessitates the integration of security measures alongside concerns for energy efficiency. Researchers have focused on cluster-based trusted routing systems to enhance security and efficiency. Extensive research has responded to the demand for a safe and productive routing solution in WSNs. Throughout history, many protocols have been devised with the primary objective of safeguarding the confidentiality of data during its acquisition and transmission [11]. Most of these protocols guarantee data security by utilizing established cryptographic techniques.

Nevertheless, it is widely acknowledged that the efficacy of these conventional protocols is limited within the domain of WSNs, primarily due to their inherent characteristics that result in excessive consumption of vital resources of SNs, including memory, processing capabilities, and power supply [12]. Most of these protocols also operate under the statement that all nodes within the network will exhibit honesty and cooperation during data transmission [13]. The requirement for centralized key management poses significant challenges within the domain of WSNs, thereby hindering the effectiveness of conventional protocols in WSNs. Although considerable progress has been made in developing these methods, further improvement is still needed.

1.1. Problem Statement

Contemporary approaches to enhancing the security of data transmission are predicated upon trust-based protocols and reputation-based procedures. Nonetheless, a limitation of these solutions is their reliance on established routing paths for data. The occurrence of a non-functional node inside the network leads to delays, increased retransmissions, and the repetitive modernization of the routing methodology. These consequences have implications for trust and reputation-based techniques.

The circumstance has led to the development an excellent and adaptable routing technique that guarantees the protected dissemination of data packets. Trust- and reputation-based methodologies are utilized to overcome the constraints obligatory by the fixed-path data broadcast procedure. The broadcasting capabilities of WSNs can be enhanced by using the Opportunistic Routing (OR) protocol.

Nevertheless, WSNs encounter a challenge regarding their broadcasting capabilities, which, although beneficial for opportunistic routing, can also lead to interference. This phenomenon occurs due to the potential for a defective or malevolent node inside the network to intercept a data packet that an SN is transmitting. These malignant nodes pose a significant risk to the functioning of the WSN and undermine its objectives. The security of WSNs can be compromised if malignant nodes can intercept data transmission inside the network. Trust-aware protocols have been proposed as a viable way to address this issue [14-16]. The OR routing technique exclusively employs nodes that have been assessed as trustworthy and reliable while excluding nodes that have been identified as faulty or unreliable.

1.2. Research Contribution

This study provides an overview of the current advancements in research and proposes a novel methodology for ensuring secure routing. Incorporating the finite energy

reserves of nodes in WSNs into the approach is anticipated to enhance network security. A novel approach known as AFHC-NTCOR is developed to reach the desired destination. The AFHC-NTCOR protocol employs trust-based methodologies and CO routing techniques to ensure data transfer security between the source and destination nodes. Furthermore, this study introduces a clustering technique that utilizes the Adapted FHO (AFHO) within the AFHC-NTCOR framework.

This approach facilitates the identification of nodes that can assume the role of CHs. A novel cost function is established to assess potential solutions in the clustering process. In summary, the AFHC-NTCOR system employs a reliable routing algorithm to establish inter-cluster routes, hence facilitating the broadcast of data from CHs to the BS. Based on the findings of the performance analysis, it can be concluded that the proposed schemes exhibited significantly superior performance correlated to the standard methodologies.

The content of this manuscript is structured in the given order: The literature review commences in Section 2 and persists throughout the subsequent sections of the study. The details about the proposed approach are expounded upon in Section 3 of the publication, whereas the outcomes of the conducted tests and simulations are presented in Section 4. In Section 5, an analysis of the study's results is presented, along with probable avenues for future research.

2. Related Works

This segment focuses on the discussion of cluster-based trust optimum routing-based techniques. In [17], a TBSIOP called Trust-Based Secure Intelligent OR Protocol was proposed. The protocol under consideration utilized three separate features of WSNs to compute the probability of a node being malevolent. The criteria used for trust computation include seriousness in legitimacy in acknowledgment, advancing data packets, and energy depletion. According to the trust factor computation, the relay selection method of the anticipated protocol effectively mitigates the assortment of malevolent nodes as relay nodes. The protocol under consideration was implemented on the list of forwarder nodes generated by the effective OR mechanism, which was under consideration subjected to simulation and compared with the trust-based routing techniques previously documented in the literature. The TBSIOP exhibited superior performance but was accompanied by a relatively high processing time [18].

The research paper [19] introduced a secure routing system for WSNs known as "Realisable Secure Aware Routing" (RSAR). The main emphasis of this strategy lies in enhancing EE by utilizing data aggregation. This study aimed to assess the reliability of individual SNs inside the network. Subsequently, an optimization methodology was employed for the restricted struggle scenario, which was then succeeded by introducing an optimal trust extrapolation model. The data flow optimization was achieved by minimizing its volume and eliminating extraneous data from the system. Once all the relevant data was gathered, it was transmitted to the recipient.

The method proposed in [20] utilized game theory and clustering techniques to observe behavior and analyze trust in relationships. The method of determining the trust factor of a node, commonly referred to as the evidence congregation structure, encompasses the integration of the concept of clustering.

In [21], a trust-based adaptive routing approach for WSNs was introduced. This study considered three trust values: indirect, observer, and direct. The trust factors that have been determined were then subjected to comparison using the matching method. The cross-layer strategy discussed in [22] examines the routing principle employed in environmentally friendly IoT networks that rely on WSNs. This work presented a mathematical model that aims to facilitate data transfer in IoT applications by computing the QoS (Quality of Service) characteristics. The diagnostic and perilous path-loss models determined the confidence level accompanying the often utilized nodes.

In [23], a trust-aware routing system was shown, incorporating numerous features. This protocol considered several factors, such as data transport, data, power, and recommendation. This study utilized a sliding time window to detect anomalous user behavior.

The authors in [24] recommended a secure routing algorithm for WSNs that used the whale optimization clustering technique. This study aimed to ascertain the most reliable node to function as the CH. Various criteria like energy, density, delay, distance to the cluster, and transmission rate were considered in the selection process.

In [25], the Swarm-Intelligence-Centric Routing Algorithm (SICROA) was developed as a potential solution for WSNs seeking to exploit the benefits of the ant colony optimization procedure. The routing protocol aimed to mitigate the issues encountered in the AODV protocol and enhance routing efficiency by implementing collision circumvention, maintenance techniques, and link-quality prediction. The suggested solution demonstrated an enhancement in network performance by the substitution of the regular "Hello" data with an intersect mechanism that aids in the anticipation and identification of link interruptions. As a result, the network's overall performance could be enhanced by implementing suitable protocols for processing each control message. Hence, it can be deduced that this approach based on Swarm Intelligence (SI) offered an appropriate resolution to challenges encountered within an

intricate setting while functioning in a decentralized manner and sticking to straightforward behavioral principles. The work in [26] introduced a Multi-Objective Function (MOF) algorithm for WSNs that draws inspiration from nature, like the Shuffled Frog-Leaping procedure and Firefly. The MOF employed by MOSFA incorporates many factors to select suitable CHs in each cycle.

2.1. Review Summary

The survey presented above illustrated the diverse contributions made by researchers in security, dependability, scalability, and energy efficiency to improve the longevity of WSNs. Despite the existence of several approaches for problem-solving, it is apparent that the efficiency of data transfer for long-distance communication through a single hop remains a limitation. Therefore, multi-hop-based communication was favored. In addition, many earlier secure protocols based on clustering exhibit notable computational and communicational burdens, posing a substantial restriction in improving and optimizing the longevity of nodes in WSNs.

3. Proposed Model

This section discusses the proposed optimal routing in WSN using the AFHC-NTCOR model. The clustering protocol strategy in WSN is presented through an optimization procedure. This procedure selects high-energy, balanced, and trusted nodes from randomly generated nodes at the outset. The merging of nodes into clusters and the collection of CHs are determined based on evaluating node properties in a WSN.

In addition, the AFHC-NTCOR approach introduces an AFHO-based clustering methodology to select CHs from a pool of candidate SNs. These nodes are nominated based on their remaining energy value and trust levels, which must exceed the trust values of every network node. CO is expected to reduce communication overhead during data transmission between the BS and CH, or vice versa, by choosing the most optimum path. The representation of the entire network process is demonstrated in Figure 2.

The proposed system elucidates the propagation model in reference [21]. The nodes detect the data transmitted to the BS through direct or hop-by-hop messages. Using natural communication methods in long-distance scenarios results in higher energy consumption. Therefore, the multi-hop message mechanism is preferred to decrease energy usage.

During the process of transcribing data, energy is expended by SNs. Measuring the distance between nodes and the BS was crucial in estimating energy consumption. The system under consideration utilizes Euclidean interval measurements to determine the gap among two nodes in WSN, denoted as A and B, within the network. This is achieved by employing Equation (1).

$$d(A,B) = \sqrt{(B_x - A_x)^2 + \left(B_y - A_y\right)^2} \qquad (1)$$

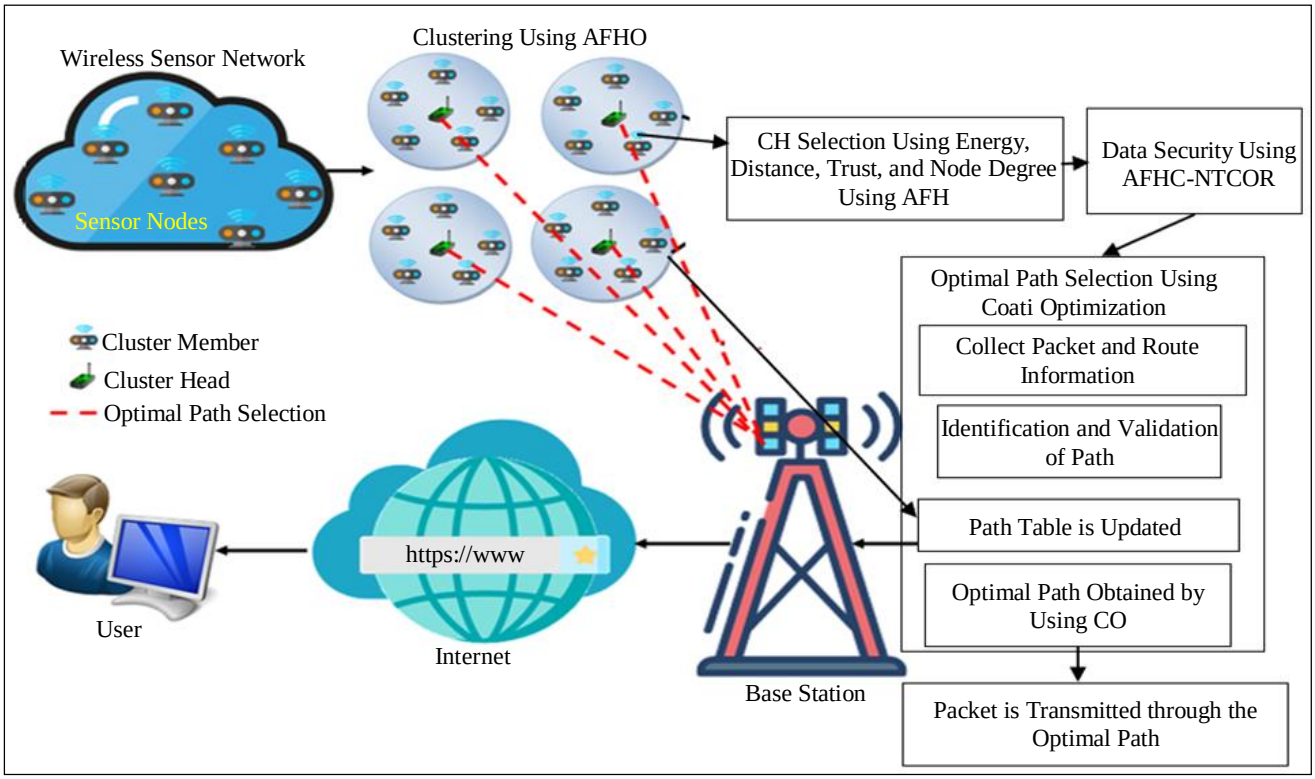

Fig. 2 Overall process of AFHC-NTCOR protocol

To transmit a message consisting of n bits from a transmit node, the energy required, denoted as E_t, could be computed utilizing (2). In this, E_e Indicates the energy needed to operate the node for transmitting and receiving the n-bit message. The Euclidean distance, dt, is considered, with d_0 representing the threshold value TH. The term fs means free space, E_i represents the initial energy of the nodes, and mp refers to multipath.

$$E_t = \begin{cases} E_e * nm + nm * e_{fs} * dt^2 dt < d_0 \\ E_e * nm + nm * e_{mp} * dt^4 dt = d_0 \end{cases} \quad (2)$$

The nm bit message is received by employing the Equation. The entire energy E_r usage of a node, denoted as E_{us}. The location of the residual energy E_{rs} of the WSN node is unknown. The computation is performed by utilizing Equations (3-5).

$$E_r = E_e * nm \quad (3)$$

$$E_{us} = E_t * E_r \quad (4)$$

$$E_{rs} = E_i * E_{us} \quad (5)$$

In each iteration, the assortment of CH is determined by comparing the TH(n) with the RE of the nodes. The TH(n) is calculated using Equation (6).

$$TH(n) = \begin{cases} \frac{P}{1-P*\left(rmod\frac{1}{P}\right)} * \frac{E_{rs}}{E_i} \; if \; nm > S \\ 0 \quad otherwise \end{cases} \quad (6)$$

In the context of the CH selection issue, the variable P represents the total quantity of possible solutions. Following the CH procedure selection, clusters amid the nodes are established using the MFHO swarm intelligence method.

3.1. Clustering Mechanism Using MFHO Algorithm

The obligation for designing and implementing the FHO-based clustering technique lies with BS. In this method, it is postulated that the BS is accountable for monitoring the network nodes like sn_i, where i = 1, 2, ..., N and possesses knowledge of their respective statuses, encompassing trust levels, positions, and energy levels. The clustering method operates on the suggestion that the sum of clusters is encoded, denoted as k clusters, resulting in the display of clusters as $C_1, C_2, \ldots, C_k$. Additionally, the CH assumes a rotational function among the nodes to mitigate node discharge and maintain energy balance within the network. Therefore, all nodes can function as CHs. During each period, the BS employs the FHO technique to determine the optimal CHs within the system. The algorithmic representation of FHO can be found in Algorithm 1. The clustering mechanism comprises several distinct steps, which are outlined below:

3.1.1. The Initialization Process of a Population

During this stage, the Biogeography-based optimization procedure evaluates Candidate Solutions (CS_i) that represent FHs and prey. In the CH collection problem context, each FH is assumed to be an array of *k* items, where *k* denotes CH numbers.

Within this array, every individual component contains the unique Identifier (ID) of a SN, denoted as sn_j. The Traffic Class (TC) Identifier (ID) is chosen arbitrarily from a candidate channel CH set called CaCH. The set is formally defined in Equation (7).

$$CaCH = \left\{ sn_j | E^{t,}_{rs,j} \geq \frac{\left(\sum_{i=1}^{\mathcal{N}} E^t{}_{rs,i}\right)}{\mathcal{N}}, Tr_j^t \geq \frac{\left(\sum_{i=1}^{\mathcal{N}} Tr_i^t\right)}{\mathcal{N}} \right\} \quad (7)$$

It should be noted that the CaCH set comprises the identification of SNs with RE ($E^{t,}_{rs,j}$) and trust level (Tr_i^t) exceed every network node's Average Remaining Energy (ARE) and ATV. Trust Tr_i^t is determined by either previous communication or previous comments.

The current level of observed misbehavior, cumulative misbehavior, and the preceding trust level determine the present trust value calculation in a prior interaction-based trust prediction approach. The present perception of misbehavior pertains to the conduct of a node at the current point in time. In contrast, the cumulative misbehavior and preceding trust value indicate the extent to which a node has engaged in misconduct in past times. The present occurrence O of node A's deviant behavior at time t, enacted by node B, is quantified in the subsequent manner:

$$O(Tr_i^t) = \begin{cases} 1-\alpha \leq Tr_i^t \leq 1 & trusted\ highly \\ 1-\beta \leq Tr_i^t \leq 1-\alpha & trusted \\ 1-\gamma \leq Tr_i^t \leq 1-\beta & untrusted \\ 0 \leq Tr_i^t < 1-\gamma & untrusted\ highly \end{cases} \quad (8)$$

The variables α, β, and γ are subject to the condition that α is less than β, β is less than γ, and γ is less than 1. These variables might be adjusted based on the setup and security demands to establish the node's state. The determination of these values remains contingent upon the prevailing technological and safety conditions.

For example, the ability of the network to tolerate a drop in effectiveness is one factor determining whether a node's trust value needs to be recognized as belonging to the untrusted sector. Furthermore, the adaptability or persistence of these characteristics is contingent upon the prevailing security issues. Consequently, nodes with low energy levels and inadequate security measures are ineligible for selection as CH. The process of Tc can be described by Equation (9).

$$CS = SF.\begin{bmatrix} CS_1 \\ CS_2 \\ \vdots \\ CS_i \\ \vdots \\ CS_P \end{bmatrix} = \begin{bmatrix} cs_1^1, cs_1^2, \dots, cs_1^j cs_1^k \\ cs_2^1, cs_2^2, \dots, cs_2^j cs_2^k \\ \vdots \\ cs_i^1, cs_i^2, \dots, cs_i^j cs_i^k \\ \vdots \\ cs_P^1, cs_P^2, \dots, cs_P^j cs_P^k \end{bmatrix}, \{ i = 1,2, \dots, P \; j = 1,2, \dots, k \quad (9)$$

In this context, CS_i denotes the ith candidate result within the search area. SF represents a scaling factor, whereas k represents the number of CHs. Furthermore, the notation cs_i^j denotes the identifier of sn_j, which is selected randomly from the CaCH collection and subsequently incorporated into the candidate solution.

3.1.2. Evaluation Process

Each candidate's result is evaluated based on the cost function outlined in Equation (10) during this stage.

$$f_{ct} = \sum_{i=1}^{4} \omega_i f_i \quad (10)$$

The weight coefficients ω_i are constrained to the range (0,1). The sum of the products is denoted by $\sum_{i=1}^{4} \omega_i f_i$. Considering that f_{ct} is a cost function, it follows that an optimal result is attained by minimizing f_{ct}. In Equation (10), the variable f_{ct} is expressed as a linear combination of f_{c1}, f_{c2}, f_{c3}, and f_{c4}. Based on the Equation (10) presented by f_1, it is observed that the BS prefers selecting nodes as CH that meet two specific characteristics. The SNs in the network are located near the cluster center, resulting in a minimal distance between the Cluster Member (CM) nodes ($CM_r \in Cl_j$) and their associated CH (CH_j). The distance between CHs should be sufficiently large to ensure a well-distributed presence of CHs overall network sections.

$$f_{c1} = \frac{\sum_{j=1}^{k} \left(\frac{\sum_{\forall CM_r \in Cl_j} d(CM_r, CH_j)}{|cl_j|} \right)}{\min_{\forall CH_j \neq CH_g} \{ d(CH_j, CH_g) \}} \quad (11)$$

Here, Cl_j represents the size of the cluster Cl_j, and $dt(CM_r, CH_j) = \sqrt{(x_r - x_j)^2 + (y_r - y_j)^2}$ is the Euclidean distance between the centroid CM_r and the centroid CH_j, with the spatial coordinates (x_r, y_r) and the spatial coordinates $x_j y_j$ of CH_j. Additionally, the term $dt(CH_j, CH_g)$ represents the distance measurement between CH_j and CH_g. In contrast, according to the Equation (12) and the variable f_{c2}, it can be observed that the BS prefers selecting CHs from nodes with high energy levels. The present preference arises since f_{c2} is calculated as the summation of the ratio between the ARE of CMs and the energy of CHs. To reduce the value of f_{c2}, it is necessary for the ARE of CMs to be lower than the RE of CHs.

$$f_{c2} = \sum_{j=1}^{k} \left(\frac{\frac{\sum_{\forall CM_r \in Cl_j} E_{rs,r}^t}{|cl_j|}}{E_{rs,r}^t} \right) \quad (12)$$

The Equation (12) represents the ratio of the RE of $M_r$and CH_j, signified as $E_{rs,r}^t$ and $E_{rs,j}^t$, correspondingly, divided by the absolute value of the clustering coefficient of CH_j, denoted as (Cl_j). Furthermore, as stated by f_{c3} via Equation (13), BS exhibits a preference for selecting CHs from nodes that are near the BS. The reduction in energy consumption and delay during the information transfer procedure amid CHs and the BS is realized.

$$f_{c3} = \max_{j-1,2,\dots,k} \{ dt(CH_j, BS) \} \quad (13)$$

Based on the Equation (13) proposed by f_{c4}, it can be inferred that the preference of BS lies in maintaining a nearly identical size for all clusters. Hence, the utilization of standard deviation enables the comparison of cluster magnitudes. When the value of this metric approaches 0, it indicates that the sizes of the clusters are nearly equal.

$$f_{c4} = \max_{j-1,2,\dots,k} \left\{ \frac{\sqrt{\sum_{j=1}^{k} \left(|lc_j| - \left(\frac{\sum_{j=1}^{k} |cl_j|}{k} \right) \right)}}{\left(\frac{\sum_{j=1}^{k} |cl_j|}{k} \right)} \right\} \quad (14)$$

After carefully evaluating the available alternatives, it has been determined that the most optimal solution is identified as the primary option with no cost (gigabytes). The ten remaining candidate solutions will be classified into two categories based on cost value.

Solutions with lower cost functions, as defined by Equation (15), will be referred to as FHs. On the other hand, solutions with higher cost functions will be regarded as prey, as per Equation (16).

$$FiH = \begin{bmatrix} FiH_1 \\ FiH_2 \\ \vdots \\ FiH_l \\ \vdots \\ FiH_f \end{bmatrix}, l = 1,2, \dots, f \quad (15)$$

$$Py = \begin{bmatrix} Py \\ Py \\ \vdots \\ Py \\ \vdots \\ Py \end{bmatrix}, q \quad (16)$$

The variable FH_l represents the n-th instance of an FH, while the variable f denotes the total number of FHs. The symbol Py_q represents the q-th prey within the search field of FHO, while the symbol m denotes the total of prey numbers.

3.1.3. Establishing the Geographic Range of FHs

Each FH shows its territory by identifying and selecting nearby prey during this stage. To ascertain the territorial boundaries of each FH, calculate the total Euclidean distance among the chosen CHs in the Py_q network model and the chosen CHs in the FiH_l Network model, using Equation (17).

$$D_q^l = \sum_{l=1}^{f} \sum_{q=1}^{m} \sqrt{\sum_{j=1}^{k} \left(cs_l^j - cs_q^j\right)^2} \tag{17}$$

In Equation (17), the objective is to calculate the sum of the square roots of the squared alterations between the elements of two sets, denoted as cs_l^j and cs_q^j.

3.1.4. The Process of Apprising FHs

During this stage, each FH obtains combustible materials from the ground and ignites them within their designated area to induce prey to evacuate under duress. This behavior is employed to update the location of the FiH. The user's text can be rewritten as follows: The vector $\left[cs_l^{\sim 1}, cs_l^{\sim 2}, \ldots, cs_l^{\sim k}\right]$ should be arranged by Equation (18).

$$cs_l^{\sim i} = \begin{cases} cs_l^j, & rd_1 = 0 \; and \; rd_2 = 0 \\ cs_{nr-to-GB,}^i & rd_1 \neq 0 \; and rd_2 < 0.5, \quad \begin{cases} j = 1,2,\ldots,k \\ l = 1,2,\ldots,f \end{cases} \\ cs_{nr-to-brFiH,}^j & Otherwise \end{cases} \tag{18}$$

In this context, the notation $cs_{nr-to-GB}^i$ denotes selecting a node from the CaCH set closer to the equivalent CH in GB. Additionally, the term $s_{nr-to-brFiH}^j$ denotes selecting a node from the CaCH series near the equivalent CH in the FH while having a lower cost function than the present FH. The variables rd_1 and rd_2 represent random numbers that are uniformly distributed between 0 and 1.

Prey Adaptation

The FH strategically sets fire into its designated territory during this stage. As a result, the prey inside this area must consciously decide to modify its movement patterns to navigate the altered environment effectively. The decision of Tc is utilized to determine the updated position of the prey, denoted as $Py_q^{new} = (\left[cs_q^{\sim 1}, cs_q^{\sim 2}, \ldots, cs_q^{\sim k}\right]$. Every component of the PRnew q is derived using Equation (19).

$$cs_q^{\sim i} = \begin{cases} cs_l^j, & rd_3 = 0 \; and \; rd_4 = 0 \\ cs_{nr-to-FiH,}^i & rd_3 \neq 0 \; and \; rd_4 < 0.5, \\ cs_{rd,}^j & Otherwise \end{cases} \tag{19}$$

The term $cs_{nr-to-FiH}^i$ denotes the process of selecting a node from the CaCH set based on its proximity to the spot of the relevant CH in the FH relative to the prey. The term cs_{rd}^j denotes the process of selecting a node at random from the CaCH collection. The variables rd_3 and rd_4 represent two randomly generated numbers within the range of 0 to 1. Next, Py_q^{new} is computed by utilizing the cost purpose defined in Equation (19). The calculation of Py_q^{new} is recomputed utilizing Equation (20) due to the possibility of the prey relocating towards the domain of additional FHs.

$$cs_q^{\sim i} = \begin{cases} cs_l^j, & rd_5 = 0 \; and \; rd_6 = 0 \\ cs_{nr-to-arFiH,}^i & rd_3 \neq 0 \; and rd_4 < 0.5, \\ cs_{rd,}^j & Otherwise \end{cases} \tag{20}$$

In this context, the abbreviation "$cs_{nr-to-arFiH}^i$"is presented. The process involves selecting a node from the CaCH set adjacent to the location of the equivalent CH in a free hawk. Let rd_5 and rd_6 represent two randomly generated numbers inside the interval (0, 1). The convergence condition refers to the criteria to be met for a mathematical or computational process to converge or approach stability and accuracy. The Termination Criterion (Tc) represents the last state of the FHO algorithm.

Upon the fulfillment of the end state, the FHO will reach its completion, resulting in the return of GB as the ultimate solution. The clustering methodology defines the termination criterion as the number of iterations such that the lambda value is not greater than zero.

Once the algorithm has been performed, BS transmits a message known as state determination to the nodes in WSN. Once clusters have been formed, the data transmission stage commences, during which CMs transmit their data directly to the CH at a predetermined time.

Upon receiving the CMs' data, the CHs collect the acknowledged message and transmit the merged message to the BS via the most efficient channels available. During this phase, the optimizer aims to prioritize the exploration of the feature space's vicinity that contains solutions of higher quality. The phenomenon enhances the search process inside a specific geographical area instead of encompassing broader portions of the overall landscape. An optimally structured optimizer should possess the ability to strike a judicious equilibrium between the inclinations for exploration and exploitation effectively.

Alternatively, the likelihood of encountering Local Optima (LO) and experiencing limitations in convergence maturity is heightened. An adaptive scaling factor, referred to as the AFHO algorithm, is implemented to enhance the efficacy of the FHO process. Following the construction of clusters and the selection of CHs, the ideal path is determined by utilizing the CO approach. The proposed protocol demonstrates enhanced performance.

Algorithm 1: Cluster formation among nodes using FHO
Input: Candidate CH set, Sensor nodes: $sn_1, sn_2, \ldots . sn_{\mathcal{N}}$, clusters: $Cl_1, Cl_2, \ldots \ldots, Cl_k$, T_s: simulation time, T_g: the guide message periodic time, T_{CH}: CH assortment process time
Output: CH selection CH_1, CH_2, CH_k
Begin
$t = 0$
Repeat
If t mod $T_g = 0$ then
For $i = 1$ to $\mathcal{N}$ do
Send a guide data from $\mathrm{sn_i}$ to BS;
BS: Store the trust value, location, and energy of sn_i in the memory;
End for
End if
If t mod $T_{CH} = 0$ then
Consider each $S_i = \left[s_1^1, s_1^2, \ldots ., s_1^j, \ldots ., s_1^k\right]$ as an array with k elements;
Select the initial value of the CS_i from CCH randomly;
Determine the initial population as CS based on Equation 8;
Evaluate the cost value of each solution based on Equation 9;
Sort the solutions based on their cost value;
Obtain the GB (Global Best) solution as the main fire;
If iteration $\leq \lambda$, then
Choose a random integer (f) as the number of FHs;
Divide the distance among FHs and preys (Py) based on Equation 15;
Calculate the distance among FHs and preys according to Equation 16;
Regulate the land of each FH;
Update the spot of FHs based on Equation 17;
Update the spot of PRs based on Equation 18;
Evaluate the cost value of PRs based on Equation 19;
If the cost value of PRs is not improved, then
Update the position of PRs based on Equation 19;
End if
Obtain the GB solution as the main fire;
end if
$Iteration = Iteration + 1$;
Return GB;
Send an SD message to all nodes;
End if
$t = t + 1$;
Until $t \leq T_{simulation}$
End

3.2. Mathematical Model of CO Algorithm

The CO approach relies on modeling two natural actions of coatis to update the position of candidate solutions. The behaviors under consideration encompass the strategic approach employed by coatis, namely when engaging in attacks on iguanas, as well as their method for evading predators. Consequently, the population of CO undergoes updates in two distinct phases.

3.2.1. Phase 1: Exploration of Hunting and Attacking Strategies on Iguanas

The initial stage of enhancing the population of coatis (specifically, CMs) within the search space is formulated by imitating their approach in attacking iguanas (i.e., nodes exhibiting malevolent behavior). Within this method, a collective of coatis ascends the arboreal structure to access an iguana and induce a state of fear within it. A group of coatis congregates beneath a tree, patiently awaiting the descent of the iguana.

Following the descent of the iguana to the ground, the coatis engage in an act of predation by attacking and pursuing it without displaying any hostile intent. This method facilitates the displacement of coatis to various locations across the search space, a phenomenon commonly referred to as clustering. This behavior serves as evidence of the exploration capability of the CO in conducting a global search inside the problem-solving domain. The schematic representation of this method is depicted in Figure 3. In the context of CO design, it is postulated that an optimal location within the population is equated with an iguana's location. It is additionally postulated that around fifty percent of the coatis engage in arboreal locomotion. In comparison, the remaining fifty percent adopt a passive stance, awaiting the descent of the iguana to the terrestrial surface. Hence, the mathematical simulation of the coatis' ascent from the tree is achieved using Equation (21).

$$ClX_i^{P1}: clx_{i,j}^{P1} = clx_{i,j} + rl \cdot \left(Ia_j - In \cdot clx_{i,j} \right), \text{for } i = 1, 2, \ldots, \left\lceil \frac{\mathcal{N}}{2} \right\rceil \text{ and } j = 1, 2, \ldots, m \quad (21)$$

Once the iguana descends to the ground, it is positioned randomized inside the search space. Coatis on the ground exhibit movement within a simulated search space, as determined by Equations (22) and (23).

$$Ia^G: Ia_j^G = lb_j + r \cdot \left(ub_j - lb_j\right), j = 1, 2, \ldots, m, \quad (22)$$

$$CLX_i^{p1}: CLX_{i,j}^{p1} = \begin{cases} clx_{i,j} + r \cdot \left(Ia_j^G - I \cdot clx_{i,j}\right), & F_{Ia^G} < F_i, \\ clx_{i,j} + r \cdot \left(clx_{i,j} - Ia_j^G\right), & else, \end{cases} \quad (23)$$

$$\text{for } i = \left\lceil \frac{\mathcal{N}}{2} \right\rceil + 1, \left\lceil \frac{\mathcal{N}}{2} \right\rceil + 2, \ldots, \mathcal{N} \text{ and } j = 1, 2, \ldots, m.$$

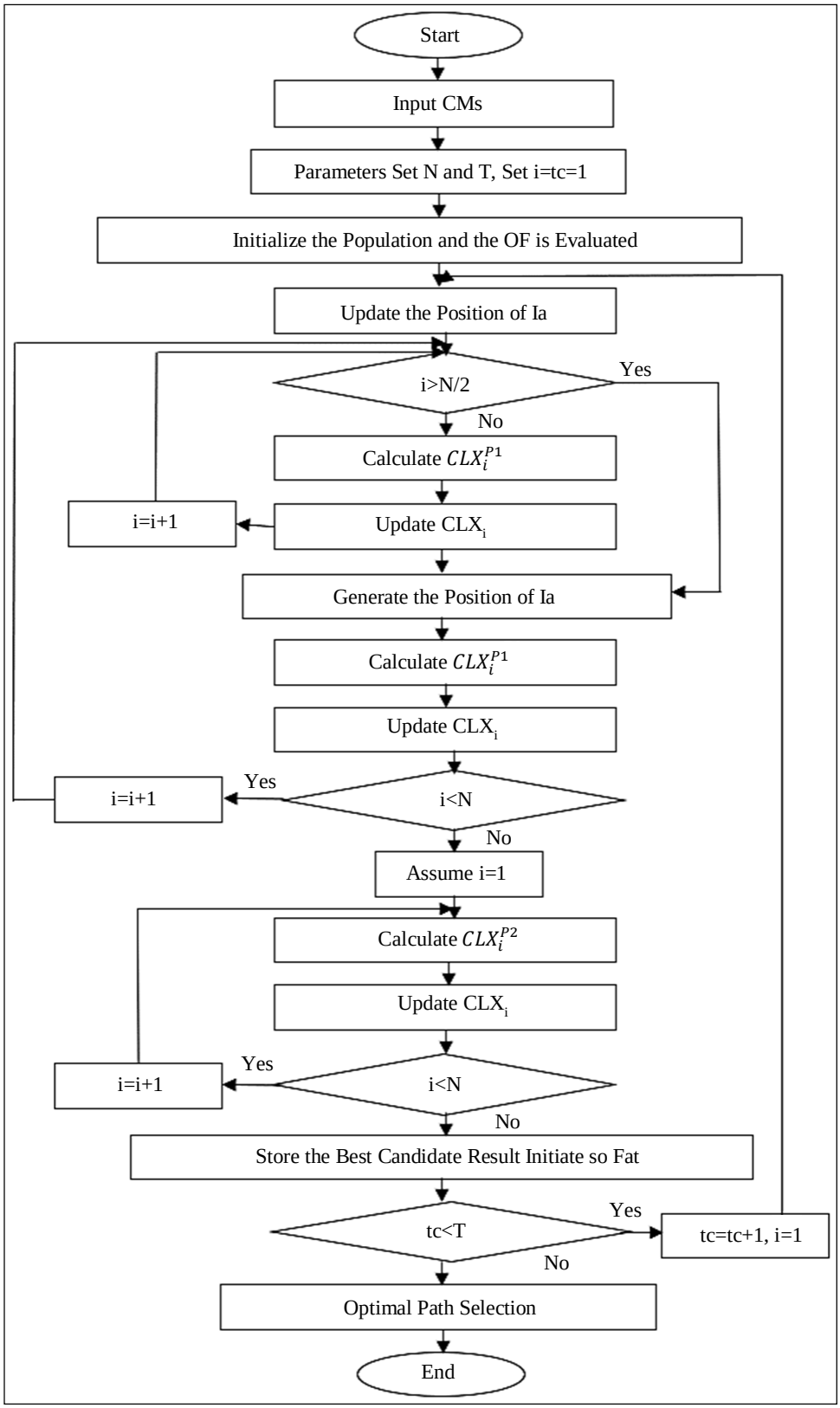

Fig. 3 Flowchart depicting the process of selecting the ideal path based on CO

Suppose the new position, referred to as the new CM node, calculated for each coati, specifically the CH, results in an improvement in the value of the OF. In that case, it is deemed acceptable for the update process. However, if the new position does not improve the OF (Objective Function), the coati will remain in its old position. The update condition is applied to the values of i ranging from 1 to N, as simulated using Equation (24).

$$CLXi = \begin{cases} CLX_i^{P1} & F_i^{P1} < OF_i, \\ CLX_i, & else. \end{cases} \quad (24)$$

Here, CLX_i^{P1} represents the newly determined location for the ith coati, $CLX_{i,j}^{P1}$ refers to its jth dimension, and OF_i^{P1} represents a certain value. P1 denotes the value of the OF, rl is a randomly generated real number within the range of (0, 1). Ia symbolizes the location of the iguana inside the search space, specifically referring to the position of the best member. Ia_j signifies the jth dimension of the iguana's position.

Let In be an integer randomly chosen from the set {1, 2}. Ia_j^G represents the position of the iguana on the minced, which is generated randomly. Ia^G denotes the jth dimension of the iguana's position. The value of the OF for Ia^G is denoted as OF_{Ia^G}. The base function, the most significant integer function, is represented by $\lfloor \cdot \rfloor$.

3.2.2. The Predation Evasion Process (Exploitation Phase)

The mathematical modeling of the second phase of apprising the position of coatis in the search space is derived from observing their natural behavior when confronting and evading predators. Coatis, non-malicious nodes with shorter transmission times, are the basis for this modeling process. When a predator initiates an attack on a coati, the animal promptly evades and disengages from its current location. The strategic movements of the coati result in its establishment in secure proximity to its present location, thereby demonstrating the coati's proficiency in exploiting local search opportunities. The present study examines the pattern diagram of coatis' approach to evading predators. To replicate this behavior, a random position is created near the current location of each coati, utilizing equations (25) and (26).

$$lb_j^{lo} = \frac{lb_j}{tc}, ub_j^{lo} = \frac{ub_j}{tc}, where\ tc = 1, 2, \ldots, T \quad (25)$$

$$CLX_i^{P2}: clx_{i,j}^{P2} = clx_{i,j} + (1 - 2rd) \cdot \left(lb_j^{lo} + rd \cdot \left(ub_j^{lo} - lb_j^{lo}\right)\right), \quad i = 1, 2, \ldots, \mathcal{N}, j = 1, 2, \ldots, m \quad (26)$$

The acceptability of the newly calculated location is contingent upon its ability to enhance the value of the goal function, as determined by the condition modeled by Equation (27).

$$\mathrm{CL}X_i = \begin{cases} CLX_i^{P2} & OF_i^{P2} < OF_i, \\ CLX_{ij} & else \end{cases} \quad (27)$$

The new location is denoted as CLX_i^{P2}, is determined for the ith coati during the second phase of CO. CLX_{ij} represents the jth dimension of this position, while OF refers to the OF. The variable rd represents an arbitrary number within the range of (0, 1). The variable tc represents the iteration counter. lb_j^{lo} and ub_j^{lo} Correspondingly, it signifies the j[th] decision variable's local lower and upper bounds.

Algorithm 2: Optimal path selection using CMs of nodes
Input: CMs as Coatis' population
Output: optimal path selection
Input the optimization delinquent data.
Established the total iterations T and the coatis $\mathcal{N}$.
Initialization of the position of all coatis and assessment of the OF for this initial population.
For $t = 1{:}T$
Update the location of the iguana followed by the best member location of the population.
//Exploration Phase
For $i = 1{:}[\mathcal{N}/2]$
Calculate the new position for the ith coati using (20).
Update the position of the ith coati using (23).
End for
For $i = 1{:}\left[\frac{\mathcal{N}}{2}\right]{:}\mathcal{N}$
Calculate the random position for the ith coati using (21).
Calculate the new position for the ith coati using (22).
Update the position of the ith coati using (23).
End for
// Exploitation Phase
Calculate the local bounds for variables using (24).
For $i = 1{:}\mathcal{N}$
Calculate the new position for the ith coati using (25).
Update the position of the ith coati using (26).
End for
Except for the best candidate result found so far,
End for
Output of the obtained solution by CA for a given optimal path selection problem.
End COA

Acknowledging the growing importance of data security in WSNs, AFHC-NTCOR introduced a cluster-based trust mechanism utilizing the FHO algorithm. This approach strategically selected trustworthy CHs based on energy reserves and trustworthiness levels, ensuring they surpass network averages. The technique employed a reliable routing algorithm for inter-cluster communication, optimizing data

pathways. The CO algorithm enhanced optimal route selection by considering EE and dependability.

3.3. Cache-Based Side-Channels

Attacks present the categorization of cache-based SC attacks in the following paragraphs. Understanding the sort of information that is released is crucial for differentiating and categorizing the attack appropriately. Separates time-driven attacks from trace-driven attacks. Active and passive time-driven attacks are the two subtypes created to organize time-dependent attacks further.

4. Results and Discussion

This segment will analyze the performance parameters of the anticipated AFHC-NTCOR routing scheme and compare it to existing trust-based routing schemes, namely Hybrid MFO-FA (Moth Flame Optimizer and Firefly Algorithm) [25], RDSAOA-EECP (energy and distance-based multi-objective red fox optimization) [26], and Hybrid CL-ALO (Cross-Layer with Harris-Hawk Optimization) [27]. The performance of the proposed secure routing strategy is estimated in comparison to other existing methods in terms of energy consumption, data throughput, packet loss rate, latency, and detection ratio, as well as PLR and PDR.

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. This review demonstrates the superior and successful performance of AFHC-NTCOR compared to alternative approaches. Table 1 presents a comprehensive overview of the critical parameters employed in the simulation procedure.

Table 1. Simulation parameters

Area	**100*100**
Nodes Number	100
BS Location	(50,50)
Initial Energy	0.5J
E	50nJ/bit
Packet Size	4000bits
ε_{fs}	10pJ/bit/m^2
ε_{mp}	0.0013pJ/bit
CH_timer	2s
In_timer	1s
Join_timer	2s
δ_s	2s
δ_m	2s
δ_i	1s

4.1. Residual Energy

Figure 4 presents an analysis of the RE across several methods. It should be noted that the energy disbursed in each node is equivalent to the total energy essential to carry out data broadcast operations, such as transmitting or receiving data. According to the depicted data, it can be observed that AFHC-NTCOR exhibits the highest RE level among the evaluated algorithms, with improvements of 12%, 27%, and 37% in comparison to Hybrid MFO-FA, RDSAOA-EECP, and CL-ALO, respectively. According to the findings presented in Figure 4, the trust value plays a vital part in mitigating the detrimental impact of intimidating nodes on the efficient energy value of nodes in WSN, hence enhancing energy consumption in the AFHC-NTCOR system.

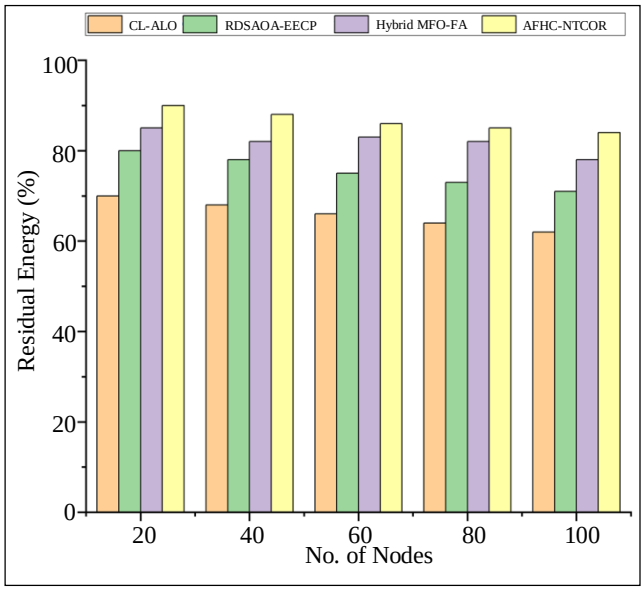

Fig. 4 Comparison of the AFHC-NTCOR model's residual energy

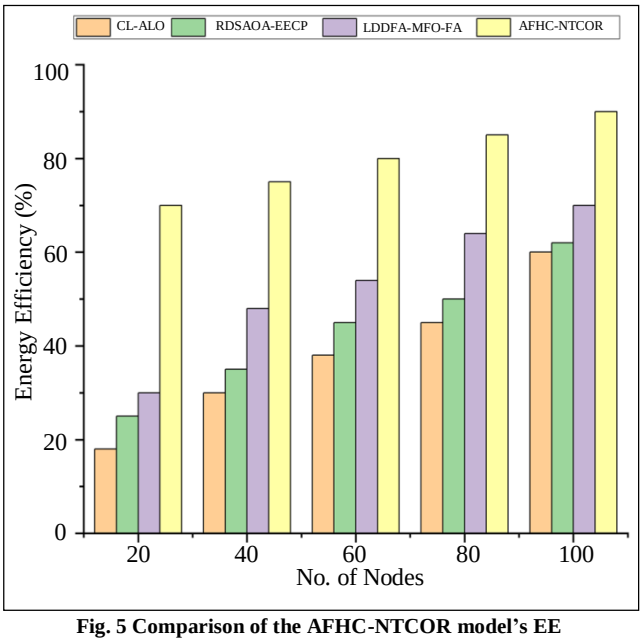

Fig. 5 Comparison of the AFHC-NTCOR model's EE

4.2. Energy Efficiency

Figure 5 illustrates the graphical depiction of the comparison of EE. Based on the data presented in the figure, it can be observed that AFHC-NTCOR exhibits superior EE, with an increase of 57.71%, 86.45%, and twice as much as Hybrid MFO-FA, RDSAOA-EECP, and CL-ALO, respectively. This finding provides evidence that the use of AFHC-NTCOR can potentially prolong a network's operational lifespan. According to the findings presented in Figure 5, there is a positive correlation between the rise in the quantity of WSNs and the rise in EE.

4.3. Throughput

The term "throughput" denotes the quantity of data effectively sent from one position to another within a specified timeframe. Figure 6 presents a comparison of throughput across several systems. Throughput refers to the quantity of packets successfully transmitted to the intended destination within a specified time frame. The AFHC-NTCOR methodology exhibits the maximum efficiency of 190kbps compared to alternative methods such as Hybrid MFO-FA, RDSAOA-EECP, and CL-ALO. Path quality is critical in AFHC-NTCOR's determination of the optimal route to the destination. Therefore, the implementation of AFHC-NTCOR is probable to enhance the data delivery rate, thereby positively impacting the overall throughput.

4.4. Packet Delivery Ratio

The measure under consideration is to assess the efficacy of routing protocols in WSNs. Figure 7 illustrates the performance comparison of the projected AFHC-NTCOR method with known approaches, namely Hybrid MFO-FA, RDSAOA-EECP, and CL-ALO. 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 AFHO has resulted in an enhanced PDR in the context of optimal routing. As the quantity of nodes rises, the PDR for all routing methods also increases.

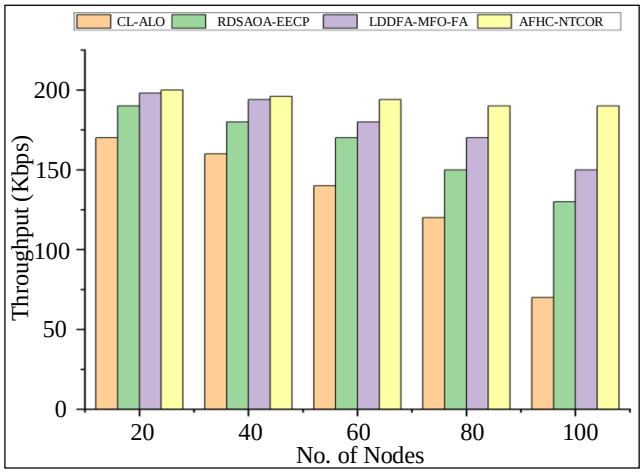

Fig. 6 Comparison of the AFHC-NTCOR model's throughput

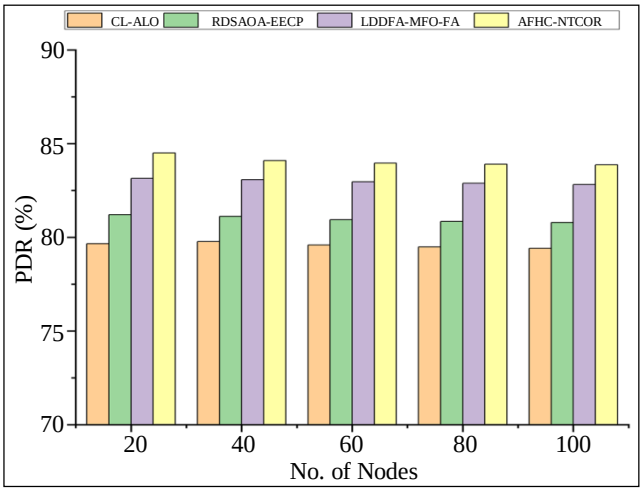

Fig. 7 Comparison of the AFHC-NTCOR model's PDR

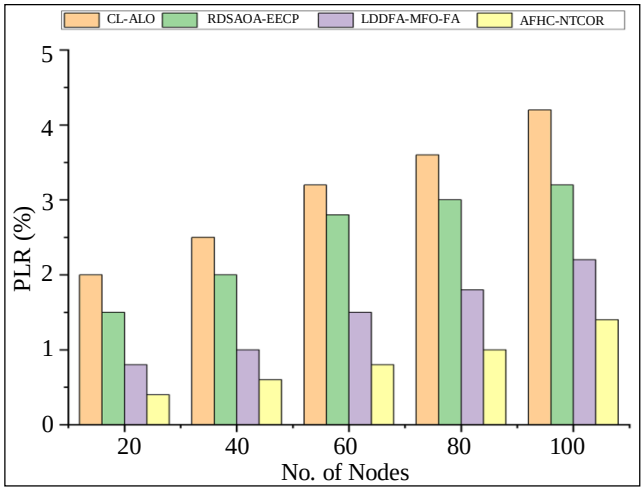

Fig. 8 Comparison of the AFHC-NTCOR model's PLR

4.5. Packet Loss Rate

This section conducts a comparative analysis of the PLR, as depicted in Figure 8. The suggested AFHC-NTCOR exhibits a lower PLR compared to existing protocols such as Hybrid MFO-FA, RDSAOA-EECP, and CL-ALO, which result in reductions of 47.22%, 60.80%, and 75.32%, respectively. As the quantity of nodes rises, packet loss decreases across all routing techniques. Cumulating the rate of WSN nodes in a system will enhance the likelihood of locating a suitable node for packet forwarding.

4.6. End-to-End Delay

Figure 9 presents a comparison of the delay seen in various ways. The proposed AFHC-NTCOR algorithm reduces latency by 32.20%, 42.83%, and 58.17% compared to the Hybrid MFO-FA, RDSAOA-EECP, and CL-ALO algorithms, respectively. The primary rationale behind this is that AFHC-NTCOR prioritizes selecting pathways that exhibit high energy levels, superior quality, and dependable performance for data transfer. Consequently, this leads to a

decrease in route disappointment and subsequently minimizes the necessity for the route discovery procedure, which is known for its time-consuming nature. In the clustering progression, assigning nodes with trust levels below the mean trust level of all WSN nodes as the CH is not feasible.

Accordingly, clusters are accomplished by secure CHs. Additionally, it is crucial to acknowledge that hostile nodes cannot operate as intermediary nodes inside a designated route. The reason for this is that the path selection mechanism considered the dependability of the path. Therefore, data transmission processes exclude routes that involve hostile nodes. The elements have played a significant role in the commendable performance of AFHC-NTCOR in effectively reducing network latency when faced with negative nodes.

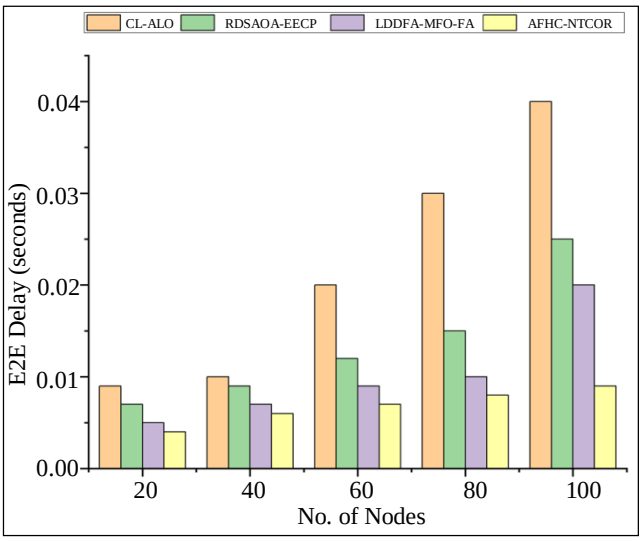

Fig. 9 Comparison of the AFHC-NTCOR model's delay

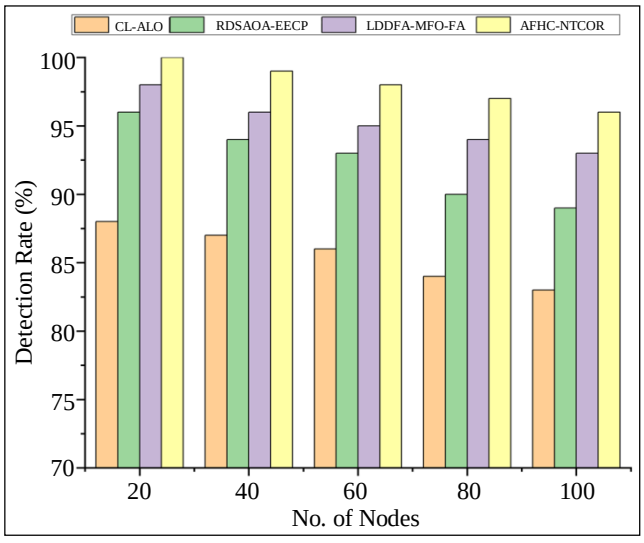

Fig. 10 Comparison of the AFHC-NTCOR model's detection rate

4.7. Detection Rate

Figure 10 presents a comparison of the detection rates across several techniques. The detection rate measures the effectiveness of trust systems implemented in different schemes for accurately identifying rogue nodes inside a network. The value is equivalent to the proportion of discovered malevolent nodes to the entire malevolent nodes inside the WSN. The AFHC-NTCOR algorithm demonstrates an enhanced detection rate of 3.07%, 6.58%, and 9.26% compared to the Hybrid MFO-FA, RDSAOA-EECP, and CL-ALO algorithms.

4.8. Communications Cost

Figure 11 illustrates a comparative analysis of communications costs across several models. This statistic quantifies the frequency of official data transmitted through a node to transmit a packet to the intended destination node successfully and assesses the trustworthiness of the participating nodes.

The AFHC-NTCOR approach reduces 26.39%, 36.36%, and 44.07% compared to the Hybrid MFO-FA, RDSAOA-EECP, and CL-ALO methods in communication cost, respectively. This demonstrates that the research model exhibits a commendable performance concerning overheads.

The AFHC-NTCOR model exhibits competitive performance across various metrics compared to existing models, including CL-ALO, RDSAOA-EECP, and LDDFA-MFO-FA. Regarding residual energy, the AFHC-NTCOR model consistently outperforms CL-ALO and RDSAOA-EECP, showcasing higher residual energy levels at different node counts. The EE, Throughput, PDR, and Detection Rate also demonstrate favorable results for AFHC-NTCOR, indicating its effectiveness in optimizing energy consumption while maintaining robust communication.

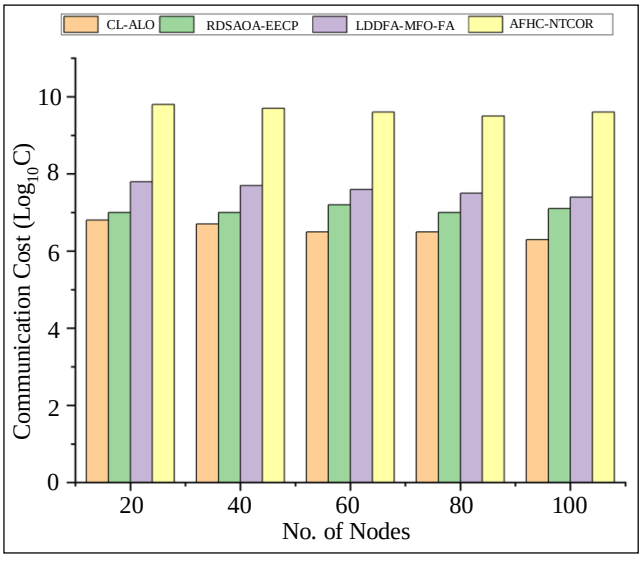

Fig. 11 Comparison of the AFHC-NTCOR model's communication cost

However, the model tends to have higher communication cost values, suggesting a potential trade-off between communication efficiency and other performance metrics. AFHC-NTCOR presents a promising approach, particularly in scenarios prioritizing EE and network robustness.

5. Conclusion

This study suggests a novel technique called AFHC-NTCOR for efficient energy use and routing in WSN. The AFHC-NTCOR protocol ensures secure data transfer between the source and destination nodes by employing trust-based techniques and coati optimum routing. Furthermore, the AFHC-NTCOR algorithm introduces a clustering technique that relies on the AFHO.

The method is accountable for the selection of CH nodes. A novel cost function is introduced during the clustering phase to determine and evaluate responses. The present study focuses on utilizing coati optimization to enhance the routing performance in WSNs, resulting in the collection of an optimal path. The AFHC-NTCOR protocol establishes inter-cluster pathways by employing a trusted routing algorithm. These paths are utilized for transmitting data from CHs to the BS.

The performance findings indicate that the AFHC-NTCOR approach achieved superior performance in various metrics, including throughput, energy consumption, latency, packet loss rate, detection ratio, and PDR, when compared to existing systems such as Hybrid MFO-FA, RDSAOA-EECP, and CL-ALO. In the future, there will be an emphasis on enhancing trust-based clustering in WSN by utilizing various optimization techniques.

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] Efat Yousefpoor, Hamid Barati, and Ali Barati, "A Hierarchical Secure Data Aggregation Method Using the Dragonfly Algorithm in Wireless Sensor Networks," *Peer-to-Peer Networking and Applications*, vol. 14, pp. 1917-1942, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] Mohammad Sadegh Yousefpoor, and Hamid Barati, "DSKMS: A Dynamic Smart Key Management System Based on Fuzzy Logic in Wireless Sensor Networks," *Wireless Networks*, vol. 26, pp. 2515-2535, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] Mohammad Sadegh Yousefpoor, and Hamid Barati, "Dynamic Keys Management Algorithms in Wireless Sensor Networks: A Survey," *Computers Communications*, vol. 134, pp. 52-69, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[4] Amir Masoud Rahmani et al., "An Energy-Aware and Q-Learning-Based Area Coverage for Oil Pipeline Monitoring Systems Using Sensors and Internet of Things," *Scientific Reports*, vol. 12, pp. 1-17, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Hojjatollah Esmaeili, Behrouz Minaei Bidgoli, and Vesal Hakami, "CMML: Combined Metaheuristic-Machine Learning for Adaptable Routing in Clustered Wireless Sensor Networks," *Applied Soft Computing*, vol. 118, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Natalie Temene et al., "A Survey on Mobility in Wireless Sensor Networks," *Ad Hoc Networks*, vol. 125, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Amir Masoud Rahmani et al., "An Area Coverage Scheme Based on Fuzzy Logic and Shuffled Frog-Leaping Algorithm (SFLA) in Heterogeneous Wireless Sensor Networks," *Mathematics*, vol. 9, no. 18, pp. 1-41, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] Mohammad Sadegh Yousefpoor et al., "Secure Data Aggregation Methods and Countermeasures against Various Attacks in Wireless Sensor Networks: A Comprehensive Review," *Journal of Network and Computer Applications*, vol. 190, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] Asha Jerlin Manuel et al., "Optimizations of Routing-Based Clustering Approach in Wireless Sensor Network: Review and Open Research Issues," *Electronics*, vol. 9, no. 10, pp. 1-29, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[10] Chao Chen, Li-Chun Wang, and Chih-Min Yu, "D2CRP: A Novel Distributed 2-Hop Cluster Routing Protocol for Wireless Sensor Networks," *IEEE Internet of Things Journal*, vol. 9, no. 20, pp. 19575-19588, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Salim El Khediri, "Wireless Sensor Networks: A Survey, Categorization, Main Issues, and Future Orientations for Clustering Protocols," *Computing*, vol. 104, pp. 1775-1837, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] Adnan Ahmed et al., "A Secure Routing Protocol with Trust and Energy Awareness for Wireless Sensor Network," *Mobile Networks and Applications*, vol. 21, pp. 272-285, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[13] Mahmood Salehi et al., "Towards a Novel Trust-Based Opportunistic Routing Protocol for Wireless Networks," *Wireless Networks*, vol. 22, pp. 927-943, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[14] Abdulhamid Zahedi, and Faryad Parma, "An Energy-Aware Trust-Based Routing Algorithm Using Gravitational Search Approach in Wireless Sensor Networks," *Peer-to-Peer Networking and Applications*, vol. 12, pp. 167-176, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[15] Deep Kumar Bangotra et al., "An Intelligent Opportunistic Routing Algorithm for Wireless Sensor Networks and Its Application towards e-Healthcare," *Sensors*, vol. 20, no. 14, pp. 1-21, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[16] Thangaramya Kalidoss et al., "QoS Aware Trust Based Routing Algorithm for Wireless Sensor Networks," *Wireless Personal Communications*, vol. 110, pp. 1637-1658, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[17] Deep Kumar Bangotra et al., "A Trust Based Secure Intelligent Opportunistic Routing Protocol for Wireless Sensor Networks," *Wireless Personal Communications*, vol. 127, pp. 1045-1066, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[18] Adam Raja Basha, "Energy Efficient Aggregation Technique-Based Realizable Secure Aware Routing Protocol for Wireless Sensor Network," *IET Wireless Sensor Systems*, vol. 10, no. 4, pp. 166-174, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[19] Liu Yang et al., "A Dynamic Behavior Monitoring Game-Based Trust Evaluation Scheme for Clustering in Wireless Sensor Networks," *IEEE Access*, vol. 6, pp. 71404-71412, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[20] Nor Azimah Khalid, Quan Bai, and Adnan Al-Anbuky, "Adaptive Trust-Based Routing Protocol for Large Scale WSNs," *IEEE Access*, vol. 7, pp. 143539-143549, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[21] Mohammed Zaki Hasan, Fadi Al-Turjman, and Hussain Al-Rizzo, "Analysis of Cross-Layer Design of Quality-of-Service Forward Geographic Wireless Sensor Network Routing Strategies in Green Internet of Things," *IEEE Access*, vol. 6, pp. 20371-20389, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[22] Boyuan Sun, and Donghui Li, "A Comprehensive Trust-Aware Routing Protocol with Multi-Attributes for WSNs," *IEEE Access*, vol. 6, pp. 4725-4741, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[23] Richa Sharma, Vasudha Vashisht, and Umang Singh, "WOATCA: A Secure and Energy Aware Scheme Based on Whale Optimization in Clustered Wireless Sensor Networks," *IET Communication*, vol. 14, no. 8, pp. 1199-1208, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[24] 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]

[25] Amirhossein Barzin et al., "A Hybrid Swarm Intelligence Algorithm for Clustering-Based Routing in Wireless Sensor Networks," *Journal of Circuits, Systems and Computers*, vol. 29, no. 10, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[26] 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]

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