Journal of Population Therapeutics & Clinical Pharmacology

RESEARCH ARTICLE
DOI: 10.47750/jptcp.2023.30.11.010

Weight Red Deer Algorithm Based Clustering Selection And Fuzzy Trust Evaluation For Wireless Sensor Networks

A. Prakash[1]*, M prakash[2]

[1]Professor, Department of computer science, Hindusthan college of arts & science, Coimbatore.

[2]Research scholar, Department of computer science, Hindusthan college of arts & science, Coimbatore.

***Corresponding author:** A. Prakash, Professor, Department of computer science, Hindusthan college of arts & science, Coimbatore, Email:prakashankar75@gmail.com

Submitted: 07 March 2023; Accepted: 17 April 2023; Published: 10 May 2023

ABSTRACT

Wireless Sensor Networks (WSNs) have received the most interest owing to their vast variety of applications.WSNs detect air pollution, humidity, and temperature, and seismic event detections. They are made up of thousands of sensor nodes that interact with one another.The primary issues with the WSN in the current system are security and energy usage. Additionally, they are unable to defend against attacks from compromised or self-centered internal nodes with proper identities.Weight Red Deer Algorithm (WRDA) is suggested in this study as a solution to the aforementioned issue.The system model, fuzzy trust assessment, outlier identification, and CH node selection are the primary stages of this study.Fuzzy trust evaluation is initially used to translate transmission evidences into trust values and minimise trust uncertainty.A K-Means-based outlier identification approach is then presented to analyse a large number of trust values from fuzzy trust assessment or trust recommendation.A meta-heuristic-based secure clustering technique is provided to balance sensor node security and energy savings while selecting CHs.Energy, neighbours, and node base station distance, and security assurance are among the parameters utilized in the WRDA strategy to choose CHs.CHs at the intermediate layer establish the routing backbone to collect, integrate, and transmit data from member nodes. The simulation reveals that the proposed WRDA architecture outperforms existing techniques in throughput, network lifetime, data transfer rate, and energy use.

Keywords: *Wireless Sensor Networks (WSNs), fuzzy trust evaluation, clustering, Cluster Head (CH) selection, security, K-Means Clustering (KMC),Weight Red Deer Algorithm (WRDA)*

INTRODUCTION

WSNs are built on many low-cost, resource-constrained sensor nodes that can perceive, process, and communicate[1]. After being put in the intended area to sense, sensor nodes may build an ad hoc network automatically.Real-time decision making is made possible because to the connection between the physical world and digital computing systems provided by WSNs.As a result of the unpredictable characteristics and ever-changing topology of WSNs, the sensor nodes that make up the network coordinate their efforts to perform sensing activities and transfer data hop by hop across the network in accordance with a set of predetermined routing protocols [2]. WSNs are often installed in hostile environments and operate in an unsupervised manner, making them

susceptible to a variety of assaults, the routing process, in particular. Greyhole, Wormhole, Blackhole, and selective forwarding assaults are examples. Traditional cryptography-based security methods are very sophisticated, incompatible with the unique traits and severe limitations of WSNs, and require extensive resources [3].Additionally, they are unable to defend against attacks from compromised or self-centred internal nodes with proper identities.Trust management strategies are often used to address these issues in order to increase the dependability and quality of WSNs."Confidence in or reliance on some quality or attribute of a person or thing, or the truth in a statement" is the standard definition of trust[4]. The trust management system states that a sensor node in the network may communicate with reliable nearby nodes to alert them to any unclear conduct in their neighbours. The trust management system may be updated or improved with the use of this information.

A reliable technique for detecting illegal nodes and ensuring security in WSNs is trust assessment.An accurate, efficient, and dynamic trust assessment model for WSNs is utilized in [5], which dynamically adjusts update parameters and direct and indirect trust weights.Direct trust is calculated by taking into account the punishment factor, regulating function, communication trust, data trust, and energy trust.The suggestions from a third party that can be trusted are used to conditionally assess indirect trust.The integrated trust metric is weighted dynamically using direct and indirect trust.The flexibility of a sliding window based on an induced ordered weighted averaging operator is improved by an updating method, for adding up.To update the direct trust value, it may dynamically adjust the parameters and the number of interaction history windows.

Attacks, routing, and energy efficiency are the three main problems in WSN [6].All routing protocols take the Quality of Service (QoS) into consideration.End-to-end latency assurance, bandwidth storage, energy efficiency, packet loss, the lifespan of the network, etc. are some of the QoS criteria.There are several methods for locating the routing issue in WSN. However, since energy is important to sensor nodes, most people make an effort to anticipate their power consumption. The concurrent supply of QoS is included in the lower protocols.

Cluster-based techniques effectively arrange WSNs for data aggregation and energy savings by designating select nodes as Cluster Heads (CHs).A CH transmits data to a sink after aggregating and compressing it using information received by cluster nodes [7]. But because the node now has more responsibilities, the network will degrade unevenly due to a higher energy drain. Additionally, in order to simplify data aggregation, it selects a collecting CH to gather sensed data from the CH surrounding the target.As a result, it is possible to aggregate the sensed data close to the data source, which saves long-distance data transfer and lowers the cost of data collection.To balance energy cost, the efficient target monitoring system assigns a lifespan to each CH based on position and remaining energy. Figure 1 depicts WSN architecture.

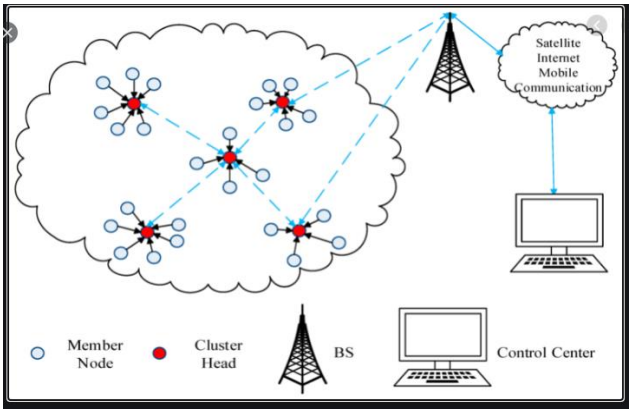

FIG 1: Architecture of WSN

J Popul Ther Clin Pharmacol Vol 30(11):e81–e94; 10 May 2023.

The aim of this work is to ensure the CH node selection in WSN using sensor nodes. There is several research and methodologies introduced but the security is not achieved significantly. The current methods are limited in their ability to identify attacks in WSN and use less energy. In order to address the aforementioned problems, WRDA and fuzzy trust assessment are presented in this study to enhance the overall performance of WSN systems.This research's main contributions are the system model, fuzzy trust evaluation, outlier detection, and CH node selection.Efficient WSN technologies extend network lifetime and minimise energy usage in the recommended strategy.

The essay continues as follows: In Section 2, there is a short overview of the literature on WSN security measures, attack detection, and CH selection.Section 3 provides further information on the suggested process for choosing CH nodes and evaluating fuzzy trust.Section 4 provides the performance analysis discussion and simulation findings. Finally, Section 5 summarizes the findings.

LITERATURE SURVEY

In [8],Pavani et al (2019) utilized a wireless sensor network's Secure Cluster-Based Routing Protocol (SCBRP), which transmits data using optimized Firefly algorithms and adaptive Particle Swarm Optimisation (PSO).This research aims to minimize node energy use to extend the network a long life.The SCBRP was developed using secure routing, energy-efficient clustering, and security verification. Based on hexagonal sensor network design.Using NS-3, the performance of the used SCBRP is assessed, and it is gauged using a variety of metrics including energy consumption, packet loss rate, encryption time, and decryption time.When compared to earlier methods, the simulation results show improved performance.

In [9], Wang et al (2018) To combat malevolent forwarding risks including new-flow attacks and selective forwarding assaults, SDWSNs were given the benefit of the energy-efficient Trust Management and Routing Mechanism (ETMRM).To provide a simple trust monitoring and evaluation system at the node level, we first improve the Sensor Flow tables in the ETMRM.Based on sensor node trust data, we next use a controller-level trust management system to identify and isolate bad nodes.We also provide a method for finding aggregation locations that is energy-efficient, ensuring control traffic delivery, and aggregating report messages.Thirdly, to ensure the transmission of data traffic, we create a trust routing system that takes the node's energy and trust level into account.Experiments show that the architecture recognises and blocks internal network assaults, such as Greyhole, Blackhole, and new-flow attacks.Compared to the related study SDN-WISE, ETMRM increases network longevity and reduces control overhead. Additionally, the ratio of delivered packets increases.

In [10], Nguyen et al (2020) RDAC-BC, a revolutionary technique to clustering based data transmission in ubiquitous wireless networks, combines the Red Deer Algorithm (RDA) with blockchaintechnology to provide secure data transfer.The clustering process is carried out through the RDAC-BC approach, which goes through node initialization.Through the use of the clustering technique, clusters are constructed and CHs are chosen. Following CH selection, Cluster Members (CMs) and CHs securely transmit data using blockchain technology.In order to accomplish energy efficiency and security, RDAC and blockchain technologies are used. The RDAC-BC technique's experimental validation is evaluated from several angles, and the findings are contrasted with those obtained from other techniques.The collected data showed that the RDAC-BC strategy had better outcomes in terms of energy use, network longevity, Packet Delivery Ratio (PDR), and throughput.

In [11], Saidi et al (2020) a misbehaviour detection method and a secure CH election process. In addition to other measures, the trust level of the sensor node served as the election's primary statistic.Another issue addressed was how to choose the most reliable node to serve as CH.A monitoring technique employing several trust kinds was also created to assess how sensor nodes behave.Keeping only reliable nodes in the network while removing rogue ones was the objective.The compromised CH scenario was considered to isolate the malicious CH without

affecting network performance.Then, local clustering and a cluster member trust assessment mechanism were used.According to simulations, the method prevents hostile nodes from becoming CHs and shields the network from compromised CH after the election.The technique successfully detected malicious nodes with a high rate and few false positive and false negative alerts in terms of misbehaviour detection.

In [12], Yang et al (2018) WSNs often use the recommended trust-based secure technique. The question of how to get behavioural data for trust evaluation, however, has not received much attention to date.Here, we offer a method for collecting evidence in WSNs that is based on dynamic behavior monitoring and game theory.Network security and energy saving are trade-offs that may be made. The cluster-based routing protocol is further combined with a trust evaluation mechanism that is based on this behavior monitoring system.

In [13], Yang et al (2021) introduced a safe clustering approach for WSNs that is based on evolutionary games and includes fuzzy trust assessment.To decrease trust uncertainty and turn transmission evidences into trust values, a fuzzy trust assessment approach is first given.Fuzzy trust evaluation or trust suggestion generates many trust values are then further examined using a K-Means based outlier identification technique.It may increase the precision of outlier identification and reveal the similarities and differences across sensor nodes.We present an evolutionary game-based safe clustering approach to balance security and energy savings for sensor nodes while selecting cluster heads.By isolating the questionable nodes, a sensor node that was unsuccessful in serving as the cluster head may safely choose its own head.The results of the simulations demonstrate that the secure clustering protocol is capable of successfully protecting the network against intrusions by selfish or compromised internal nodes. Consequently, a significant improvement in the timely data transfer rate can be made.

PROPOSED METHODOLOGY

This study suggests using the WRDA algorithm and fuzzy trust assessment to increase WSN security while reducing energy usage.The system model, fuzzy trust assessment, outlier identification, and this research focuses on CH node selection. Fig. 2 displays the proposed work's general block diagram.

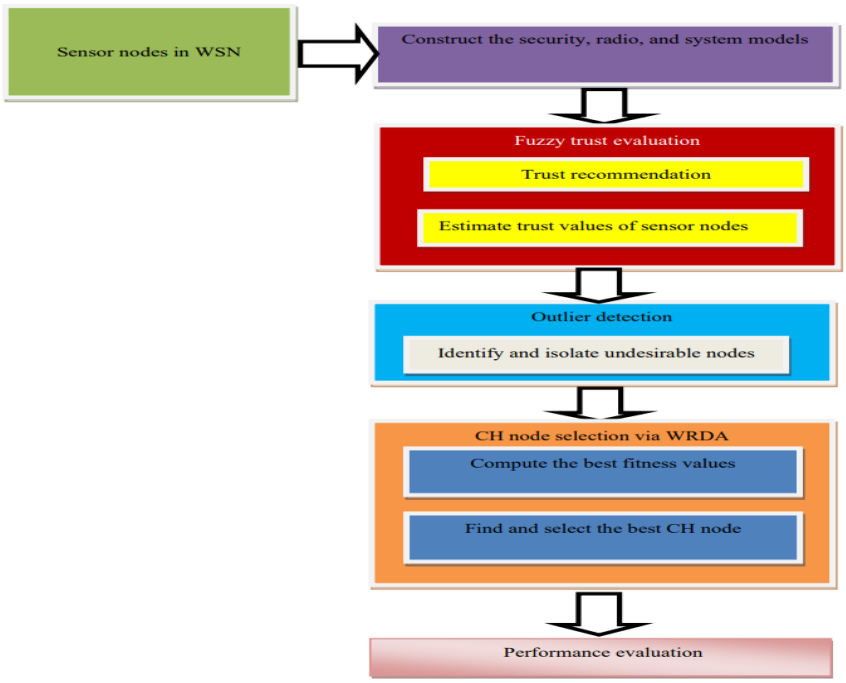

FIG 2: Block diagram of the planned project overall

J Popul Ther Clin Pharmacol Vol 30(11):e81–e94; 10 May 2023.

System Model

Since it is more adaptable and effective for WSNs, the hierarchical network model is taken into consideration in this paper. Clusters are groupings of sensor nodes that make up the network.A cluster head, a few member nodes, and them make up each one. Data sensing for interest is a task carried out by every node in the bottom layer. Cluster heads gather, combine, and transmit data from member nodes in the intermediate layer while also constructing the routing backbone.The top-layer base station relays cluster head data to the server.

Radio model

Open wireless channel quality is unstable and may sometimes be either excellent or terrible due to interferences.A Markov chain with two states is then created S = {s0, s1} in this research serves as the time-varying wireless medium [14]; an example of this is presented in Fig. 3.

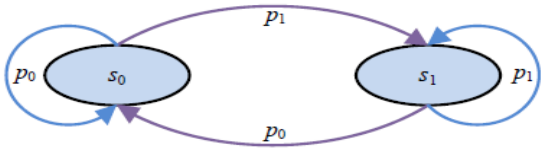

FIG 3: Model for channel quality based on Markov chains

The low and excellent states of the channel quality are represented here by s0 and s1, respectively. Exponential distribution random variable, the time period t during which the channel quality changes between each stage is

$$p(t) = \begin{cases} \alpha_i e^{-\alpha_i t} & t \geq 0 \\ 0 & t < 0 \end{cases} \quad (1)$$

where $\alpha_i, i \in \{0,1\}$positive-negative ratios. The channel's chance state will change from poor to excellent is then determined by$p_0 = \alpha_0/(\alpha_0 + \alpha_1)$ and $p_1 = \alpha_1/(\alpha_0 + \alpha_1)$ respectively

A free-space propagation model or a two-ray ground reflection model may explain wireless transmission loss based on the transmitter-receiver distance d[15].If d goes below a threshold, d_0, the first model better represents transmission loss. The second model fits all other scenarios. Calculating the threshold d_0

$$d_0 = \sqrt{\varepsilon_{fs}/\varepsilon_{amp}} \quad (2)$$

where $\varepsilon_{fs}$and $\varepsilon_{amp}$are the transmission loss models' enhanced characteristic constants

To transfer a k-bit data packet over distance d, a node needs energy [15].

$$E_{Tx}(k,d) = \begin{cases} kE_{elec} + k\varepsilon_{fs}d^2, & d < d_0 \\ kE_{elec} + k\varepsilon_{amp}d^4, & d \geq d_0 \end{cases} \quad (3)$$

where $E_{elec}$is the power used by the electronics of the transmitter or receiver

For a k-bit data packet, the energy used by the receiver may be calculated by

$$E_{Rx}(k) = kE_{elec} + kE_{DA} \quad (4)$$

where E_{DA}stands for the amount of energy that is used up by the receiver in the process of aggregating a one-bit packet

Security model

In order to prevent attacks in resource-constrained WSNs, this article offers a trust-based security architecture that includes trust evidence gathering, fuzzy trust assessment, trust recommendation, trust grouping, and outlier detection (see Fig. 4).To construct a trust-based secure system, each sensor node listens to communications to accumulate trust evidence from other nodes.After updating the evidence, an IT2 fuzzy logic system (FLS) is used to fuzzy infer trust levels. This is done so that the uncertainty caused by the trust evidences can be effectively reduced.When combined with a

method for trust recommendations, each node has the ability to amass a large number of trust values, which are then subjected to additional analysis through trust grouping.Next, the group means identify anomalous nodes, while simultaneously determining whether or not a given node is malevolent.

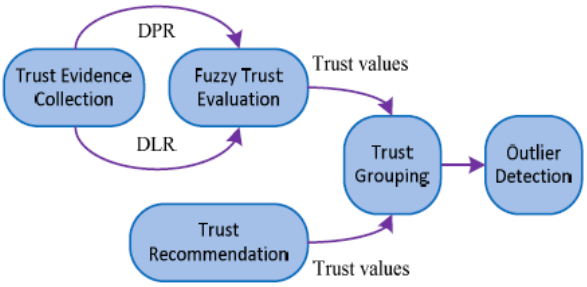

FIG 4: Outlier detection

Trust evidences such the packet dropping rate (DPR) and packet delaying rate (DLR) have been collected to verify packet transmission safety. These rates may show the changes that occur with respect to packets when assaults take place throughout the routing process.Malicious nodes may often launch three different types of assaults on data packets: altering, dropping, and delaying. Data packets must be verified by the destination node to verify integrity in order to avoid tampering attacks.From the viewpoint of sender nodes, the tampering attack may be seen as a dropping attack since any packet that is determined to have been altered should be deleted owing to authentication failure [16]. As a result, all types of assaults on data packets may be somewhat indicated by the two trust evidence, DPR and DLR.

Fuzzy Trust Evaluation

It has been shown that IT2 FLS has a smoother control surface and a superior capacity to cope with uncertainty than its type-1 (T1) equivalent [17]. The most important distinction is that the rule base has at least one IT2 fuzzy set among its collection of fuzzy sets. To begin, the fuzzier module transforms crisp inputs into fuzzy sets using a normalization process.After that, the inference engine analyses the input fuzzy sets and the rule base to deduce a solution. The rule base includes IF THEN clauses to specify the connections between the inputs and the results.Thirdly, while a T1 fuzzy set is being collected, the type reducer performs type reduction. Finally, using denormalization, the defuzzifier produces clear output.

TABLE 1: Fuzzy Rules of Trust Evaluation

No.	DLR	DPR	Trust output
1	*Low*	*Low*	*Complete Trust*
2	*Medium*	*Low*	*Trust*
3	*High*	*Low*	*Medium Trust*
4	*Low*	*Medium*	*Medium Trust*
5	*Medium*	*Medium*	*Medium Distrust*
6	*High*	*Medium*	*Distrust*
7	*Low*	*High*	*Distrust*
8	*Medium*	*High*	*Intense Distrust*
9	*High*	*High*	*Complete Distrust*

The FLS receives the collected trust evidences from the DPR and DLR as inputs to assess the trust of sensor nodes.To characterize the membership grade of DPR, three fuzzy sets are used that correlate to the language variables low, medium, and high. The membership grade of the output's trust is determined using seven IT2 fuzzy sets with the variables total mistrust, strong mistrust, total mistrust, medium mistrust, medium trust, and full trust. Nine fuzzy rules are shown in Table 1 that use IF THEN clauses to convert fuzzy sets between trust evidence and trust output. Consider the first guideline: The trust output is full trust if both DLR and DPR are low.

Assume that the FLS's input vector is x = (x1, x2). Here, the input variables for DPR and DLR are represented by x1 and x2, respectively. There are seven actions that must be taken in order to get the output trust value.

Using the matching fuzzy set of the kth kth(k = 1, 2, ..., 9)rule, determine the membership grade for the variable xi (i= 1, 2), represented as G (xi k).

F in view of the (k = 1, 2, ..., 9) rule for x, determine the firing grade G (x k) using the product t-norm.

Determine the output trust intervals $[T_l(x^k), [T_r(x^k)$of the kth rule for kth (k =1, 2, ..., 9). The left and right trust values in this example are Tl and Tr, respectively. Particularly, the kth (k =2, 3, ..., 8) rule's trust fuzzy set is vertically symmetrical, resulting in left and right output trust intervals. Since the intervals have the same firing grade, they should be halved.

Reconstructing the trust set requires converting the value pairs of trust interval against grade to trust value versus grade interval {<Ta(xt), [Gl(xt), Gu(xt)]>, t = 1,2, ...,16}. It is trust The average of the left and right values is Ta. Trust fuzzy sets are determined by, Ta lower and higher membership grades are Gl and Gu, respectively.

Sort all trust values and normalize all lower and higher membership grades individually in the trust set.

Defuzzification may be used to get the final output trust value T(x) given the input x.

$$T(x) = \frac{T_L(x)+T_R(x)}{2} \qquad (5)$$

Outlier detection

In this part, an independent outlier identification method based on K-Means is developed to identify harmful outliers.The introduction of the trust suggestion mechanism updates the trust values effectively to speed up convergence.Clustered WSNs only communicate with the cluster leader and member nodes. If a sensor node joins a trusted cluster, it can request the head's trust recommendation.

In the event that a sensor node i receives the cluster head k advised trust value T (k, j) for node j, it modifies node j trust value as follows:

$$T(i,j) = \begin{cases} \frac{T(i,j)+T(i,k)T(k,j)}{1+T(i,k)} & if\ T(i,j) > 0 \\ T(i,k)T(k,j), & otherwise \end{cases} \qquad (6)$$

where T (i, k) is node i's modified trust value. T (k, j) is node k trust in node j.

The method for detecting outliers relies on rounds. Through fuzzy inference or trust recommendations, a sensor node first modifies the trust values of other nodes in each round.Furthermore, the K-Means algorithm is used to analyse these updated trust values. Using the results, isolate the cluster heads from the malicious nodes. As there is no contact between nodes, each node must record the trust value for other nodes as 0.Node outlier identification begins after two interactions.The outlier identification procedure only proceeds in rounds when a node operates as a cluster member node and may update trust values.

Cluster Head (CH) node selection using Weight Red Deer Algorithm (WRDA)

The CH node selection in this part is carried out using WRDA. Clustering is one of the effective process which are applied in the WSN to preserve the precious battery power of sensor nodes. It produces a certain number of clusters from data and tries to minimize distances. The following describes the objective of the function:

$$J = \sum_{j=1}^{k} \sum_{i=1}^{x} ||x_i^{(j)} - c_j||^2 \qquad (7)$$

where $||x_i^{(j)} - c_j||^2$is a selected metric used to calculate how far a data point $x_i^{(j)}$ is from the cluster center. The indicator c_j measures the separation between each cluster center and the n data points.It is predicated on the idea that sensor nodes may inform the sink of their locations and are randomly dispersed.The number of clusters that must be created depending on the number of network nodes may be determined after the sink has all of the nodes' positions. Then, all network sensors receive a broadcast of the CHs list [19]. Afterward, the sensor nodes that have been designated as CHs start to function as CHs and announce their presence on the network.So, to select best CH node WRDA is proposed in this work.

Using a Red deer group's behavior as a paradigm, RDA is an evolutionary algorithm. Red deer are either male or female, with the former being known as a stag.A harem is a collection of hinds and a few stags. A stag will be gathered to serve as the harem's leader.To draw the attention of the hinds, stags scream loudly, and the one who does so most often become the commander.The commander is tasked with mating with and caring for the hinds in the harem. Red deer are generated in greater numbers with higher fitness levels thanks to intergenerational mating between stags and hinds and competition among stags to become the commander [20]. When it increases the fitness of commander it will produce more number of best CH nodes. The WRDA comprises the following steps:

Initialization of the red deer

Deriving the overall or nearly optimum solutions to a particular issue is the aim of this approach. Any solution in a solution space (P) is denoted by the symbol red deer (RD).

$$RD = [L_1, L_2, \dots L_D] \quad (8)$$

D stands for the solution's dimension in this case. By using the clearly stated fitness functions, a solution's efficacy is assessed, and it is provided as

$$f(RD) = f[L_1, L_2, \dots L_D] \quad (9)$$

The population is produced by NP-hard red deer problems. Two kinds of red deer are distinguished, and the elitist trait is used to choose them.Male red deer with the best match are identified as N_{ma} and marked with a marking. Hinds (N_{hd}) are the rest of the red deer. The set of men is constructed from the total population as

$$N_{ma} = round\{\beta_1 NP\} \quad (10)$$

where, $\beta_1$is a constant value chosen at random, and $\beta_1 \in [0.2, 0.5]$. N_{hd} is the notation for the number of hinds$N_{hd} = NP - N_{ma}$.

Roar male Red Deers

This level uses neighbourhood node solutions to enhance male RD placements.Three randomly generated constant variables were utilized in the algorithm's original form, but in this improved version, just one of those kinds of variables is used.By keeping the randomness for updating the male RDs' locations and the original algorithm's natural observation, the improved version was able to maintain both. Male RD position updates are calculated as follows:

$$male_{new} = \begin{cases} male_{old} - (1-\gamma) * (ub - lb) * \frac{n}{i^{2+n}}, & \gamma < 0.5 \\ male_{old} + \gamma * (ub - lb) * \frac{n}{i^{2+n}} & \gamma \geq 0.5 \end{cases} \quad (11)$$

where, γ is an actual number produced at random (γ ∈ [0, 1]), The present generation is denoted by the letters i, n represents the number of generations. ub and lb denote the search space's upper and lower boundaries.

Selection of male commanders

Commanders and stags are separated from other male RDs. Commanders (N_{cm}) make up 20% to 50% of men.

$$N_{cm} = round\{\beta_2 . N_{ma}\}, \beta_2 \in [0.2, 0.5] \quad (12)$$

β2 is random. The remaining males are stags (N_{st}).

$$N_{st} = N_{ma} - N_{cm} \quad (13)$$

Male commanders and stags fight

The commanders and stags are utilized to engage in combat according to the original RD method, and this process is heavily dependent on randomness.In this situation, it is believed that

two random constant variables are crucial. The updated RD method employs a single random constant variable rather than two constant random variables.This phase also places a great deal of emphasis on the current iteration (i) and the overall number of iterations (n).Because of the mathematical depiction of the battling process, more dominant characteristics and less recessive ones are retained. Commanders (cm) and stags (st) dispute generates two new solutions using the following formula.

$$NM_1 = \lambda_1 * cm + (1 - \lambda_1) * st - \lambda_1 * (ub - lb) * \frac{n - i/n}{i^2 * n}, \lambda_1 > 0.5 \quad (14)$$

$$NM_2 = (1 - \lambda_1) * cm + \lambda_1 * st + (1 - \lambda_1) * (ub - lb) * \frac{n - i/n}{i^2 * n}, \lambda_1 \leq 0.5 \quad (15)$$

where NM_1 and NM_2 are the names of two new solutions. $\lambda_1$is a constant at random where $\lambda_1 \in$ {0, 1}. Fitting values for each of the four solutions are calculated using the fitness function, i. e. cm, st, NM_1 and NM_2. The commander is the best answer, while the stag is the second-best(best CH node).

Form harems

A harem composed of a number of hinds under the authority of a male commander is found in the original RDA [21].Harem size is solely determined by commander strength. Based on the intrinsic, domain-specific behavior of stags and commanders and their objective fitness in diminishing order of magnitude, the original RDA's harem formation approach emphasizes the female hinds that are accessible.The updated RDA imagines hinds with an unlimited supply of commanders and a randomizing border, Y. By choosing a commander's hinds, the harem (Z) is formed.

X = Number of unassigned commanders / total number of hinds

Y = Integer at random between 1 and X

Z = (Y * Number of hinds that are unassigned)/X

The first commander receives the N number of hinds, and then the second commander will get the N number of hinds, and so on.

Mating Procedure and Mating Algorithm

According to the original RDA, many hinds mated with the harem leader [12]. Each commander mates with every hind (hn) under his care under the modified RDA. The mating procedure is carried out as follows.

$$N_{of1} = \lambda_2 * cm + (1 - \lambda_2) * hn - \lambda_2 * (ub - lb) * \frac{n - i/n}{i^2 * n}, \lambda_2 > 0.5 \quad (16)$$

$$N_{of2} = (1 - \lambda_2) * cm + \lambda_2 * hn + (1 - \lambda_1) * (ub - lb) * \frac{n - i/n}{i^2 * n}, \lambda_2 \leq 0.5 \quad (17)$$

where, λ_2 is a random constant value ($\lambda 2 \in$ {0, 1}). Stags can mate with any harem's hinds, but they can only mate one hind every generation.

Population for next generation

In this step, the next generation is created. Fitness function evaluation of offspring RDs is essential. RDs from the preceding generation and the current offspring have different fitness values, the better RDs are divided up for the next generation.This selection procedure uses the roulette wheel selection approach [15]. The optimal answer may not change for a very long time if these procedures are followed through with a given number of iterations.

To extend the life of the WSN, only those nodes with excellent residual energy and favourable channel conditions will be taken into account.After establishing the clusters and finalizing the CHs, the system computes the route after establishing the CHs' placements. The base station processes data collected.In order to save battery life, it will spend less time and travel a shorter distance while visiting each cluster to gather data from CHs. The distance between the clusters and speed are two other factors that must be considered.

Input: no. of sensor nodes

Output: best CH node selection (energy efficiency and security assurance)

1. Start
2. Initialize red deers (sensor nodes) using (8)
3. Define the objective function via (9)
4. Roar red male deers
5. Update the position of sensor nodes (11)
6. Select the possible CH nodes

7. Select γ percent of best male red deer as male commander
8. Fight between male commander and stages (to obtain better solutions)
9. Update new CH nodes using (14) and (15)
10. Form harems (avoid least percent sensor nodes)
11. Mate male commander of harem
12. Select the best CH nods
13. Return the commander
14. Update new optimal CH nodes using (16) and (17)
15. Ensure energy efficiency and security
16. Select the next generation
17. Stop the conditions
18. Obtain the optimal CH nodes
19. End

Simulation result

The Taylor Kernel Fuzzy C-means Clustering (TKFCC) [23] and Evolutionary Game based Secure Clustering protocol with Fuzzy trust assessment and Outlier detection [22] techniques are compared to the proposed WRDA method in this part.Table 2 lists the simulation settings, and NS-2 is utilized to repeat this work. Throughput, energy use, data transmission rate, and network longevity are compared between the current and suggested techniques.

TABLE 2: Simulated variables

Parameter	values
No. of Nodes	100
Area Size	1100 * 1100(Meter)
Mac	802.11
Total energy	150 Joule
Initial value of energy	1.5 Joule
Radio Range	250m
Simulation Time	60 sec
Packet Size	bytes

Throughput

The throughput of a network or communication channel is the pace at which data packets are successfully carried through it.

$$Throughput = total\ number\ of\ packets\ sent\ /time \quad (18)$$

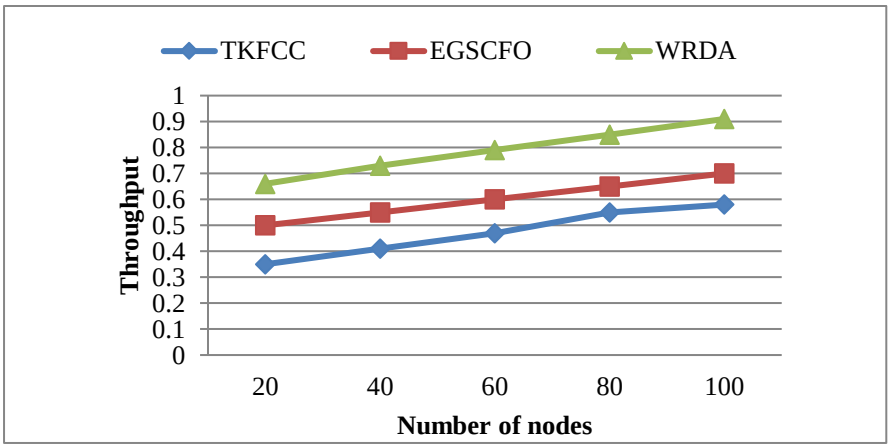

FIG 5: Throughput comparison

J Popul Ther Clin Pharmacol Vol 30(11):e81–e94; 10 May 2023.

Fig. 5 compares TKFCC, EGSCFO, and WRDA throughput metrics. The number of nodes and throughput metric are monitored on the x- and y-axes, respectively. In order to identify and determine the CH nodes in WSN efficiently, the suggested WRDA approach is applied.With no information being lost, this makes it easier to precisely collect and send secure data across nodes. It demonstrates that although the new WRDA technique offers greater throughput, the current TKFCC and EGSCFO methods provide lesser throughput.

Energy consumption

The term "energy consumption" describes the typical energy required over time for a packet's transmission, reception, or forwarding activities to a network node.

$$Energy\ (e) = [(2 * pi - 1)(e_t + e_r)d \quad (19)$$

pi is the data packet, e_t is the energy used to transmit packet i, and e_r is the energy used to receive packet i, where d is the distance between the transmission node and the destination node.

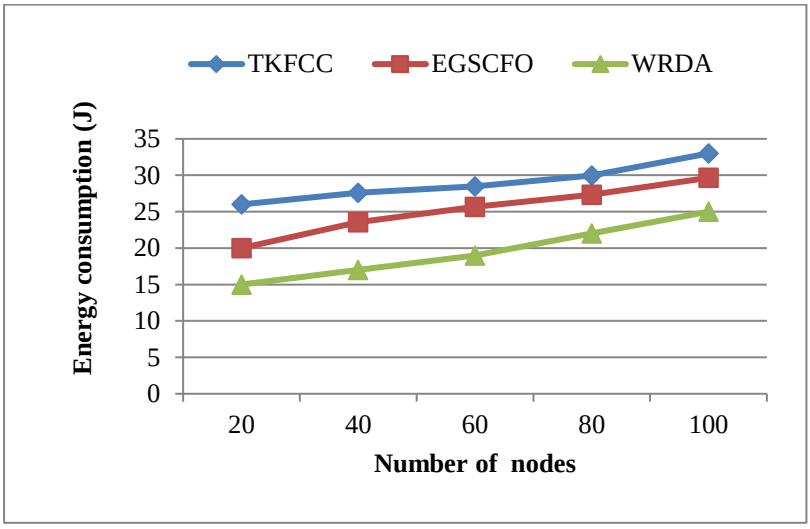

FIG 6: Comparing energy consumption

As shown in Fig. 6, the new WRDA algorithm and current TKFCC, EGSCFO, and methods are used to compare energy usage. The y-axis measures energy usage, while the x-axis measures the number of nodes.During the data packet transmission, consumption of energy is significantly minimized with the help of proposed WRDA algorithm over the WSN.This is so that non-CH nodes in WRDA have the lowest likelihood of wasting energy since their data packets are almost certainly relayed to the base station in a timely manner.It demonstrates that the suggested WRDA algorithm uses less energy than the current approaches, which use more energy.

Network lifetime

When the suggested strategy results in longer network lifetimes, the system is deemed superior.

$$Lifetime\ \mathbb{E}[L] = \frac{\varepsilon_0 - \mathbb{E}[E_w]}{P + \lambda \mathbb{E}[E_r]} \qquad (20)$$

where P represents the network's total constant, continuous power usage, $\varepsilon_0$is the whole starting energy that cannot be recharged, $\lambda$is the typical amount of data collected by each sensor per second, $\mathbb{E}[E_w]$ when the network is unsuccessful, how much energy will be anticipated to be lost or left unused$\mathbb{E}[E_r]$how much energy each sensor is estimated to need for reporting

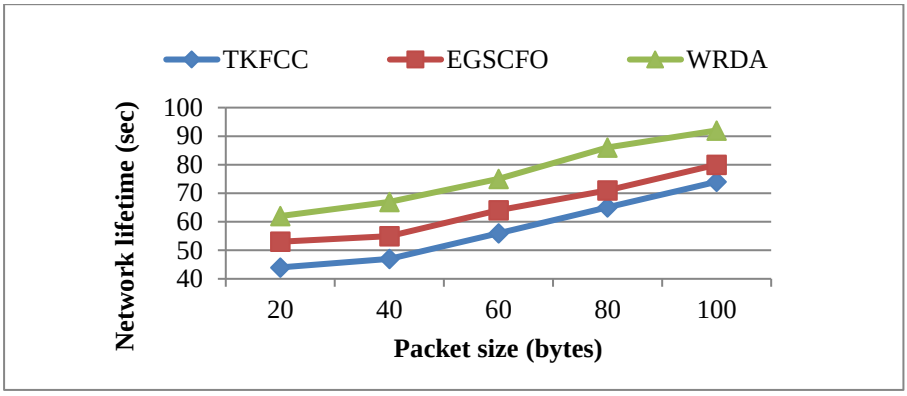

FIG 7: Network lifetime

For the specified packet size, Fig. 7 shows the network lifetime. Number of nodes is shown on the x-axis, while network lifespan is plotted on the y-axis.During transmission of data packets, the lifetime of sensor node is significantly improved using proposed WRDA. This is because of performing CH based data transmission using WRDA algorithm. Fuzzy trust assessment and outlier identification prevent rogue nodes, increasing packet transmission.As packet size increases, the proposed system extends network lifetime. It shows that the planned WRDA outlasts the TKFCC and EGSFO techniques.

Data Transfer Rate

The quantity of data transmitted from one location to another in a certain length of time is called the data transmission rate.Data transmission rate is the pace at which a specific amount of data transfers between locations. The bandwidth of a route generally enhances data transmission rate.

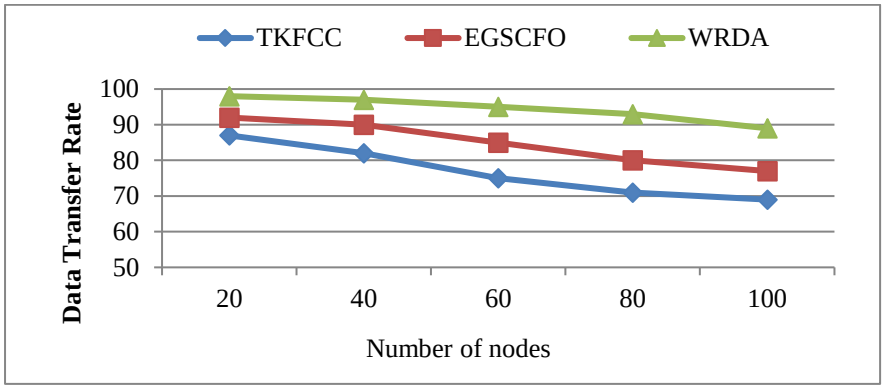

FIG 8: Data transfer rate

In Fig 8, the data transmission rates of TKFCC, EGSFO, and WRDA are compared. The x and y axes show nodes and data transmission rate.TKFCC and EGSFO technologies reduce data transmission rates. The suggested WRDA increases data transmission rate greatly in proposed system.Thus, TKFCC, EGSFO methods enable efficient and secure WSN data transmission.

CONCLUSION

In this work, proposed WRDA method is used for optimizing the CH node selection and fuzzy trust evaluation for attack detection over WSN.First, a fuzzy trust assessment approach converts transmission evidences into trust values and reduces trust uncertainty.A K-Means-based outlier identification approach is then presented to analyse a large number of trust values from

fuzzy trust assessment or trust recommendation.In this paper, the WRDA method is suggested as a way to choose the optimal CH node. Through the best fitness values, the best CH node is chosen.When choosing a CH node, the best result is obtained by using the fitness function to take into account the remaining energy, distance, neighbors, and secured data.As a consequence, it was determined that the suggested WRDA technique outperforms the alternatives already in use in terms of throughput, network longevity, data transfer rate, and energy usage. Future work may heavily emphasize the development of innovative routing protocols for shortest route routing.

REFERENCES

1. Yang, Liu, et al. "An unequal cluster-based routing scheme for multi-level heterogeneous wireless sensor networks." Telecommunication Systems 68 (2018): 11-26.
2. Yang, Guisong, et al. "Global and local reliability-based routing protocol for wireless sensor networks." IEEE Internet of Things Journal 6.2 (2018): 3620-3632.
3. Jadidoleslamy, Hossein, Mohammad Reza Aref, and Hossein Bahramgiri. "A fuzzy fully distributed trust management system in wireless sensor networks." AEU-International Journal of Electronics and Communications 70.1 (2016): 40-49.
4. Shaikh, Riaz Ahmed, and Ahmed Saeed Alzahrani. "Trust management method for vehicular ad hoc networks." Quality, Reliability, Security and Robustness in Heterogeneous Networks: 9th International Conference, QShine 2013, Greader Noida, India, January 11-12, 2013, Revised Selected Papers 9. Springer Berlin Heidelberg, 2013.
5. Ye, Zhengwang, et al. "An efficient dynamic trust evaluation model for wireless sensor networks." Journal of Sensors 2017 (2017).
6. Elsmany, EymanFathelrhman Ahmed, et al. "EESRA: Energy efficient scalable routing algorithm for wireless sensor networks." IEEE Access 7 (2019): 96974-96983
7. Thakkar, Ankit, and KetanKotecha. "Cluster head election for energy and delay constraint applications of wireless sensor network." IEEE sensors Journal 14.8 (2014): 2658-2664
8. Pavani, Movva, and PolipalliTrinatha Rao. "Adaptive PSO with optimised firefly algorithms for secure cluster-based routing in wireless sensor networks." IET Wireless Sensor Systems 9.5 (2019): 274-283.
9. Wang, Rui, et al. "ETMRM: An energy-efficient trust management and routing mechanism for SDWSNs." Computer Networks 139 (2018): 119-135.
10. Nguyen, GiaNhu, et al. "Blockchain enabled energy efficient red deer algorithm based clustering protocol for pervasive wireless sensor networks." Sustainable Computing: Informatics and Systems 28 (2020): 100464.
11. Saidi, Ahmed, KhelifaBenahmed, and NouredineSeddiki. "Secure cluster head election algorithm and misbehavior detection approach based on trust management technique for clustered wireless sensor networks." Ad Hoc Networks 106 (2020): 102215.
12. Yang, Liu, et al. "A dynamic behavior monitoring game-based trust evaluation scheme for clustering in wireless sensor networks." IEEE Access 6 (2018): 71404-71412.
13. Yang, Liu, et al. "An evolutionary game-based secure clustering protocol with fuzzy trust evaluation and outlier detection for wireless sensor networks." IEEE Sensors Journal 21.12 (2021): 13935-13947.
14. Chan, Wai Hong Ronald, et al. "Adaptive duty cycling in sensor networks with energy harvesting using continuous-time Markov chain and fluid models." IEEE Journal on Selected Areas in Communications 33.12 (2015): 2687-2700.
15. Yang, Liu, et al. "A hybrid, game theory based, and distributed clustering protocol for wireless sensor networks." Wireless Networks 22 (2016): 1007-1021.
16. Tan, Shuaishuai, Xiaoping Li, and Qingkuan Dong. "A trust management system for securing data plane of ad-hoc networks." IEEE Transactions on Vehicular Technology 65.9 (2015): 7579-7592.
17. Peng, Wei, et al. "Interval type-2 fuzzy logic based transmission power allocation strategy for lifetime maximization of WSNs." Engineering Applications of Artificial Intelligence 87 (2020): 103269.
18. Sreejith, S., H. Khanna Nehemiah, and A. Kannan. "A clinical decision support system for polycystic ovarian syndrome using red deer algorithm and random forest classifier." Healthcare Analytics 2 (2022): 100102.
19. Haider, Syed Kamran, et al. "Energy Efficient UAV Flight Path Model for Cluster Head Selection in Next-Generation Wireless Sensor Networks." Sensors 21.24 (2021): 8445

20. Sreejith, S., H. Khanna Nehemiah, and A. Kannan. "A clinical decision support system for polycystic ovarian syndrome using red deer algorithm and random forest classifier." Healthcare Analytics 2 (2022): 100102.
21. Zitar, Raed Abu, and LaithAbualigah. "Application of red deer algorithm in optimizing complex functions." 2021 14th International congress on image and signal processing, biomedical engineering and informatics (CISP-BMEI). IEEE, 2021.
22. Yang, Liu, et al. "An evolutionary game-based secure clustering protocol with fuzzy trust evaluation and outlier detection for wireless sensor networks." IEEE Sensors Journal 21.12 (2021): 13935-13947.
23. Augustine, Susan, and John Patrick Ananth. "Taylor kernel fuzzy C-means clustering algorithm for trust and energy-aware cluster head selection in wireless sensor networks." Wireless Networks 26 (2020): 5113-5132.