Yugoslav Journal of Operations Research
35 (2025), Number 2, 417–436
DOI: https://doi.org/10.2298/YJOR240217011C

Research Article

A COMPREHENSIVE DECISION ASSESSMENT FOR TRUST EVALUATION IN WIRELESS SENSOR NETWORKS

Thilagasree CHAKKARAPANI SUMATHI
Department of Mathematics, SRMV College of Arts and Science, Coimbatore, India
csthilagasree95@gmail.com,

Jayakumar THIPPAN
Department of Mathematics, SRMV College of Arts and Science, Coimbatore, India
jayakumar.thippan68@gmail.com, ORCID: 0000-0003-1336-6696

Brainy JOSEPH RAJ VIKILAL JOICE
Department of Mathematics, Bharathiar University, Coimbatore, India
brainy.maths@buc.edu.in,

Pragathi SUBRAMANIAM
Department of Mathematics, Bharathiar University, Coimbatore, India
pragathi.maths@buc.edu.in,

Daekook KANG*
Department of Industrial and Management Engineering, Institute of Digital Anti-aging Health Care, Inje University, 197 Inje-ro, Gimhae-si, Gyeongsangnam-do, Republic of Korea 50834
dkkang@inje.ac.kr, ORCID: 0000-0002-1885-9409

Received: February 2024 / Accepted: April 2024

Abstract: This study endeavors to tackle the pressing issue of network security within Wireless Sensor Networks (WSNs) through the introduction of an innovative integrated Pythagorean fuzzy-based method for evaluating network nodes. The primary aim is to

*Corresponding author

enrich decision making frameworks within WSNs by furnishing a robust methodology for identifying and eradicating malevolent nodes. Investigation employs an integrated Pythagorean fuzzy-based methodology to appraise network nodes by scrutinizing specific trust attributes. Comparative assessment with alternative contemporary Multiple Criteria Decision Making (MCDM) trust models is conducted to gauge the effectiveness of the proposed strategy. The results underscore the efficacy of the integrated Pythagorean fuzzy-based approach in bolstering network security through the precise identification and elimination of malicious nodes. Comparative analysis with other MCDM trust models highlights the superiority of the proposed approach in evaluating network nodes based on trust attributes. In light of the findings, it is advised to integrate fuzzy decision analysis methodologies into decision making systems for WSNs to enhance network security. Additionally, future research endeavors could concentrate on refining and expanding upon the proposed methodology to effectively address emerging security challenges within WSNs.

Keywords: Wireless sensor networks, security, SECA, ARAS, Pythagorean fuzzy sets, trustable neighbour.

MSC: 03B52, 68T27, 68T37, 90B50, 91B06.

1. INTRODUCTION

The Internet of Things (IoT) significantly relies on Wireless Sensor Networks (WSNs) for sensing and actuation. It has been developed to assess, monitor, and record environmental changes. WSNs provide several benefits compared to other network types, such as increased flexibility, cost-effectiveness, and simplified deployment. They are mostly comprised of haphazardly positioned sensor nodes that monitor the region of interest and provide data to the base station [1]. The addition of one or more intermediary nodes along the path to receive and send data packets increases network coverage in comparison to single hop networks and requires less energy for data transmission via the sensor nodes [2]. In complicated multi hop networks, it is possible for numerous channels to become accessible and be used to increase network resilience, jeopardizing network security. Regardless of the massive amount of data being received and sent between the source and sink nodes [3], they are frequently the subject of internal and external assaults as depicted in figure 1.

However, due to the resource-constrained nature of WSNs, they encounter several challenges and concerns that must be resolved to guarantee dependable and secure data transmission [4]. The fundamental attributes of wireless communication, such as transmission through open air and shared access to the medium, create security vulnerabilities that attackers can exploit to execute malicious attacks. Specifically, WSNs are vulnerable to a range of malicious activities, encompassing eavesdropping, jamming, spoofing, and denial of service DoS attacks. which are explained as follows.

- **Tampering:** In this case, the intruder alters or damages the node's services and seizes entire control of the targeted node in order to obtain keys and other encrypted materials involved for data security.

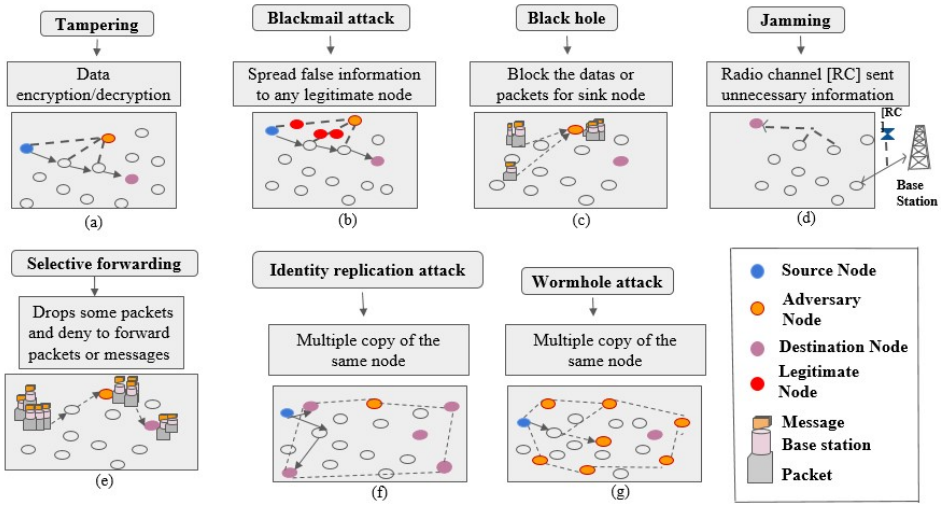

Figure 1: Types of Malicious Attacks

- **Blackmail attack:** A malicious node sends false information about a lawful node to the network. If the hostile node succeeds to take down a significant amount of nodes, network operations will be disrupted.
- **Black hole attack:** In this assault, an attacked node serves as a blackhole, and when packets flow through it, the intruder attracts the packets to himself, preventing them from reaching the destination or sink node.
- **Jamming:** In jamming attacks, hostile nodes disrupt lawful communication by generating purposeful interruption in networks. A typical jamming attack is distinguished by massive energy efficiency, poor detection likelihood, and resilience to jamming.
- **Selective Forwarding:** In this attack, a compromised node takes the role of a router, discarding or deleting some of the specified packet information and refusing to relay these signals.
- **Identity replication:** A legitimate node is duplicated several times and distributed in various regions of the network to gather information. When there are several nodes with the same identity, establishing if the network has been hacked becomes difficult.
- **Wormhole attack:** It is one of the most lethal attacks on the WSNs. In this attack, the intruder carefully deploys unauthorized nodes around the network to build a tunnel via which data packets are delivered to the attacker.

Trust management is an important aspect of WSN as it contributes to the development of highly durable, adaptable, and efficient systems. The confidence in neighboring nodes

is the foundation for information exchange and transmission between nodes. With the identification of hostile or unreliable nodes, trust analysis improves network security. In a trust analysis, the trustor does an assessment of the trustee's reliability using either subjective or objective standards. The objective criteria are those that can be measured, such as Quality of Service (QoS), whereas the subjective criteria are those that are based on the qualitative description of the trustor whose values vary depending on each trustor, such as social ties, prior evidence, and Quality of Security (QoSec). These trust parameters support the removal of the flawed node from the mechanism and the identification of the dependable neighbor.

Trust is a hazy and ambiguous term that cannot be defined as a number between zero and one. The uncertainty surrounding the connection between the trustor and trustee may be better handled by fuzzy set theory, which gives approximations between 0 and 1. The number of nodes continuously increases as the network gets more intricate, endangering network security. This necessitates the creation of strong trust frameworks, which will increase the networks' energy effectiveness and resilience. The process of choosing a reliable neighbour demands the simultaneous examination of several trust criteria, which may be successfully handled using MCDM approaches ([5],[6],[7],[8],[9]). Using these methodologies and a variety of criteria, the selection of a trustworthy neighbour node is quantitatively assessed among the many nodes. The use of fuzzy-based MCDM approaches provides a viable alternative to the time-consuming effort of calculating accurate values for all of the criteria.

In an unclear setting, fuzzy sets [10] aid in describing the degree of truthiness of an option with regard to a criterion. The use of extended fuzzy sets, such as intuitionistic fuzzy sets (IFS) [11], however, aids in describing the degree of truthiness and falsity of an option in relation to the criteria. Despite the criterion total of truthiness and falsity should be less than one, the applicability of IFS in extremely complicated scenarios is restricted. To circumvent IFS's limits, Yager [12] developed the concept of Pythagorean fuzzy sets (PFS), in which the total of the squares of the truthiness and falsity of an option in relation to the criteria should be less than one. This has given experts more leeway in articulating their suggestions in Pythagorean linguistic terms. Due to their adaptability, PFS [13] have been used to communicate human cognitive concepts when addressing with issues in engineering [14], management science [15], computer applications [16], pattern recognition [17], cluster analysis [14], and other fields [18, 19]. Further, a fuzzy decision analysis can be a useful tool for detecting defective nodes and therefore improving network security. Therefore, it is imperative to develop a multi-criteria decision-making model to encourage cooperation in WSNs, especially in light of the detrimental impact caused by malicious and selfish nodes on network performance. This research presents an integrated pythagorean fuzzy-based technique for appraising network nodes by investigating certain trust qualities. In addition, the model's efficacy is evaluated by comparing the results to those of other contemporary MCDM trust models. The abbreviations are depicited in table 1.

The paper is structured as follows: Section 2 presents the review of literature, the basic definitions and the algorithm of the developed framework are given in section 3 . In section 5 we discuss about the considered problem and the results and discussion are presented in section 6. Section 7 presents the conclusion and the future implications.

Table 1: Nomenclature

AHP	Analytic Hierarchy Process
ARAS	Additive Ratio Assessment System
CODAS	Combinative Distance-Based Assessment
EDAS	Evaluation Based on Distance from Average Solution
IoT	Internet of Things
MCDM	Multi-Criteria Decision Making
PFS	Pythagorean Fuzzy Sets
QoS	Quality of Service
QoSec	Quality of Security
SECA	Simultaneous Evaluation of Criteria and Alternatives
SWARA	Step-wise Weight Assessment Ratio Analysis
TOPSIS	Technique for Order Preference by Similarity to Ideal Solution
VIKOR	VlseKriterijumska Optimizacija I Kompromisno Resenje
WSN	Wireless Sensor Networks

2. EXISTING INTEGRATED FUZZY DECISION APPROACHES IN WSN

This section reviews different fuzzy logic and neural network-based techniques that researchers have devised for determining a node's trustworthiness in a wireless sensor network (WSN) [20]. A novel approach, referred to as the Pythagorean fuzzy MCDM model, integrates Pythagorean Fuzzy Sets with VlseKriterijumska Optimizacija I Kompromisno Resenje (VIKOR) and technique for order preference by similarity to ideal solution (TOPSIS) methodologies to address resource depletion attacks and enhance QoS within the network. By leveraging the advantages of Pythagorean Fuzzy Sets, this model effectively manages the uncertainty and vagueness present in the information exchanged during the data routing process [21]. The Hybrid Grey PIvot Pairwise RElative Criteria Importance Assessment (PIPRECIA) and Grey Operational Competitiveness RAting (OCRA) Method –based MCDM, aimed to deterring malicious and selfish nodes to enhance cooperation among sensor nodes along routing paths [22]. In particular, potential issues should be seen and addressed in network channels using a few strategies, as discussed in the following table 2.

Pythagorean fuzzy sets offer a valuable framework for visualizing and analyzing malicious attacks of neighboring nodes in WSNs. With Pythagorean fuzzy sets, the degree of membership and non-membership can be represented with greater granularity, enabling a more detailed analysis of the extent to which neighboring nodes are affected by malicious attacks [33]. The visualization of malicious attacks facilitated by Pythagorean fuzzy sets can aid in the development of more effective security measures and protocols to safeguard WSNs against potential threats. This proactive approach helps enhance the overall resilience and robustness of WSNs in the face of evolving security challenges.

The use of subjective or objective approaches for evaluating attribute weights aids specialists in determining which criteria to emphasise. Simultaneous evaluation of alternatives and criteria (SECA), a multi-objective paradigm for assessing alternatives and criteria, was suggested by Keshavarz-Ghorabaee et al. [34]. This method facilitates in the dynamic assigning of weights to criteria based on information obtained from decision matrices. SECA is especially useful when the weights of decision-making components

Table 2: Trust models and their implications

Authors	Methodology	Implications
Gautam et al.[23]	Fuzzy Analytic Hierarchy Process (AHP)-TOPSIS technique	To determine the trustful neighbour for information packet distribution to neighbouring nodes and assess the adjacent nodes using QoS parameters.
Ogundoyin et al. [24]	Triangular Fuzzy Numbers in AHP technique	To assess trust parameters in fog computing services. The characteristics of QoS, QoSec, social relationships, prior reputation, and recommendations are used to evaluate an effective fog computing service.
Ya et al.[25]	Fuzzy-based RTMDC protocol	To improve the effectiveness of data transmission and energy use, they recommended using a dual communication method rather than a single communication mode.
Rizwanullah et al.[26]	Triangular fuzzy based AHP algorithm	To simultaneously evaluate the trust measures such as QoS, QoD, social relationships, prior reputation, and recommendations
Paul et al. [27]	TOPSIS method	To analyse the trust assessment and management (MATEM) for the Delay Tolerant Networks (DTNs) based on security metrics including attack detection, false positive, and false negative rates
Alghofaili et al.[28]	Simple Multi-Attribute Rating Technique (SMART)	For calculating trust values and the long short-term memory (LSTM) algorithm for analyzing behavioral changes based on the trust threshold in IoT devices and services
AlFarraj et al. [29]	The activation function-based trust paradigm	To provide safe routing in WSNs based on criteria such as latency, energy, throughput, network longevity, and false detective rate when delivering information to the neighbor nodes
Gandhi et al.[30]	Fuzzy logic rule prediction technique	To analyse the nodes for trustworthiness and isolated the afflicted nodes, which aids in determining secure paths for efficient packet delivery.
Singh et al. [31]	Advanced Hybrid Intrusion Detection System (AHIDS), MPNN includes BPNN and FFNN based on fuzzy logic	To recognise some of the security issues that sensor nodes encounter, such as Sybil attacks, wormhole attacks, and hello flood attacks
Sinha et al. [32]	Anomaly-based intrusion detection system (AIDS) based on a fuzzy inference method and a neural network (NN)	To identify the malicious assaults such as denial of service that cause network outages.

are unknown. This approach has been employed in the secure distribution of feeder identification [35], AHP and SECA methods in resource allocation in hybrid fog computing issues [36], energy storage system selection [37], and assessment of sustainable manufacturing strategies [38], and so on. The additive ratio assessment (ARAS) approach, created by Zavadskas et al. [39], is an MCDM tool for prioritising alternatives. The utility function valuation is used to rate the alternatives. It adheres to a certain normalisation for the qualitative and quantitative criteria. The approach is preferred in the decision process due to its low operative time and flexibility to the regarded problem in getting accurate findings. Hu et al. [40] used a q-rung orthopair fuzzy hybrid Step-wise Weight Assessment Ratio Analysis (SWARA)-ARAS approach to analyse the risk associated with IoT supply chain management. Mohammadian et al. [41] established an interval valued triangular fuzzy based SWARA-ARAS decision support system to help policymakers find IoT applications for future investment in the agriculture sector. The technique has been used to help in the resolution of various MCDM challenges such as IT people selection [42], site selection [43], appraisal of oil gas well drilling projects [44], digital supply chain management [45], and environmental concerns [46, 47].

According to the reviewed literature, the utilisation of the SECA-ARAS approach for trustful neighbour selection in WSN has not been investigated previously. Triangular fuzzy number is used to express the acceptability of alternatives in regard to each criterion, and it provides only membership grades (i.e., trustworthiness) while ignoring non-membership grades (i.e., untrustworthiness). It is hard to tell whether a node is totally trustworthy since there is always a reluctance to define such things. Providing ratings for both membership (i.e., trustworthiness) and non-membership (i.e., untrustworthiness) may help to better comprehend the node's position. In this study, we employed pythagorean fuzzy numbers to indicate the node's attitude towards each considered criterion. In this study, the trustable neighbour for the considered network is identified using the Pythagorean fuzzy based SECA approach in conjunction with the ARAS method.

2.1. Contributions of the Study

The following outlines the essential points aimed to elicit the significance of the proposed study.

- Exploration and Utilization of IoT Innovations in WSN: This research makes a significant contribution by delving into and harnessing IoT advancements within WSN, thereby bolstering their adaptability for a wide range of applications and settings.
- Utilization of Pythagorean Fuzzy Sets for Malicious Attack Analysis: Through the integration of Pythagorean fuzzy sets, this study presents a fresh method for scrutinizing malicious attacks in WSN, delivering more resilient and nuanced insights into security threats and vulnerabilities.
- Introduction of the Integrated SECA-ARAS Approach for Threat Anticipation: This research pioneers and assesses the Integrated SECA-ARAS approach, which offers a structured methodology for forecasting optimal threatening regions within WSN. This enhances proactive measures for threat mitigation and resource allocation strategies.

3. THEORETICAL FRAMEWORK

Definition 3.1. *[14]*

Let $\mathfrak{U}$ be the universe of discourse. A set, F expressed as $F = \{\langle \rho(t), \varsigma(t)\rangle | t \in \mathfrak{U}\}$, where ρ, ς represent the membership and nonmembership grades satisfying $0 \leq (\rho(t))^2 + (\varsigma(t))^2 \leq 1$ is called the pythagorean fuzzy set. Further, $H_F(t) = 1 - \sqrt{(\rho(t))^2 + (\varsigma(t))^2}$ represent the hesitancy degree of $t \in \mathfrak{U}$. The pair $N = \langle \rho, \varsigma \rangle$ denote the Pythagorean fuzzy number(PFN).

Definition 3.2. *[14]*

The score γ of a PFN, $N = \langle \rho, \varsigma \rangle$ is defined as

$$\gamma(N) = (\rho(t))^2 - (\varsigma(t))^2 \tag{1}$$

Figure 2 presents the methodological framework of the proposed model. Here, the SECA method is used for determining the influential parameters and the ARAS method is used for prioritizing the options. The considered methods are enhanced using the PF logic. Algorithm 1 and 2 presents the working procedure of the developed model.

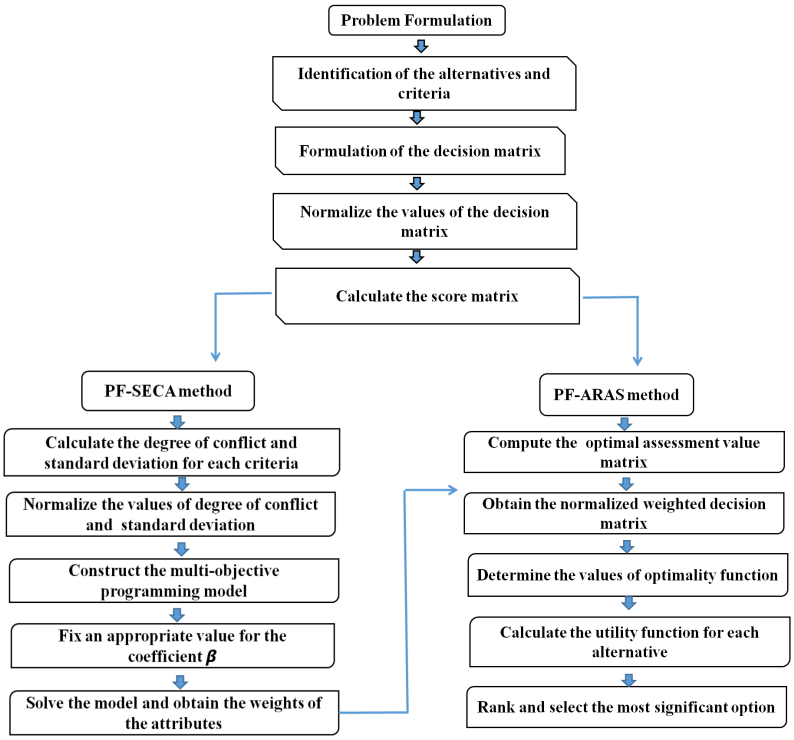

Figure 2: Framework of the proposed model

4. PROBLEM DESCRIPTION

In a WSN, the situation involves a source node (referred to as node A) aiming to send a data packet to another node (referred to as node R) located several hops away within the network. To establish this communication, node A must identify an appropriate neighboring node to relay or forward the data packet toward the target node, node R.

The specific investigation at hand revolves around identifying four nearby nodes (referred to as nodes B, C, D, and E) situated in close proximity to node A. These neighboring nodes are potential candidates for relaying the data packet toward the destination node, node R.

The selection of the suitable neighboring node among B, C, D, and E holds significant importance as it can influence various factors such as data transmission efficiency, network congestion, energy consumption, and overall network performance. Consequently,

Table 3: Algorithm 1

Algorithm 1: Criteria Weight evaluation using Pythagorean fuzzy SECA Method
Input : $\{\rho(t),\varsigma(t)\}_{p\times q}, 1 \le p \le r, 1 \le q \le s$=PFDM
Output : Weight of each attributes η_s , 1≤q≤s
Initialize s ← number of criteria
r ← number of neighbour nodes
%% Calculate the correlation between each pair of vectors of criteria
for q=1 to r
π_q=$\sum_{k=1}^{s}(1-d_{qk})$
end
%% Define the normalized values of σ_q and π_q
for q=1 to s
σ_q^N=$\frac{\sigma_q}{\sum_{k=1}^{s}\sigma_k}$,
π_q^N=$\frac{\pi_q}{\sum_{k=1}^{s}\pi_k}$.
end
%% Formulation of multi-objective non-linear programming model
for p=1 to r
max S_p=$\sum_{q=1}^{s} h_q d_{pq}^N$,
end
for q=1 to s
if $h_q \le 1$ and $h_q \ge \varepsilon$
min λ_b=$\sum_{q=1}^{s}(h_q-\sigma_q^N)^2$,
min λ_c=$\sum_{q=1}^{s}(h_q-\pi_q^N)^2$, such that $\sum h_q = 1$
end
end
%% Transform the multi-objective non-linear programming model to the optimization Model
if $\lambda_a \le S_p$
max F=λ_a-$\beta(\lambda_b+\lambda_c)$,
for p=1 to r
for p=1 to r
max S_p=$\sum_{q=1}^{s} h_q d_{pq}^N$,
end
for q=1 to s
if $h_q \le 1$ and $h_q \ge \varepsilon$
min λ_b=$\sum_{q=1}^{s}(h_q-\sigma_q^N)^2$,
min λ_c=$\sum_{q=1}^{s}(h_q-\pi_q^N)^2$, such that $\sum h_q = 1$
end
end
end
end

Table 4: Algorithm 2

Algorithm 2: Prioritization of each alternatives using Pythagorean fuzzy ARAS technique
Input :
1. $\{\rho(t),\varsigma(t)\}_{p\times q}, 1 \le p \le r, 1 \le q \le s$=Normalized PFDM ;
2. Weight of each attributes η_s , 1≤q≤s
Output : Weight of each attributes ζ_r , 1≤p≤r
Initialize s ← number of criteria
r ← number of neighbour nodes
for p=1 to r
for q=1 to s
$\tilde{d}_{pq}$=$\bar{d}_{pq}h_q$
end
end
%% To determine the values of optimality function
for p=1 to r
R_p=$\sum_{q=1}^{s}\tilde{d}_{pq}$
end
%% Calculate the utility degree M_p of an alternative ζ_p
for p=1 to r
M_p=$\frac{R_p}{R_0}$
end

the investigation likely entails evaluating diverse parameters or metrics such as signal strength, link quality, available bandwidth, and the energy levels of neighboring nodes to make well-informed decisions regarding which node(s) to choose for data transmission.

Moreover, depending on the specific requirements and constraints of the WSN application, the selection process may also consider additional factors such as node mobility, data aggregation capabilities, and network topology. Additionally, routing protocols and algorithms may be utilized to optimize data transmission routes and ensure dependable communication between nodes within the network., is in figure 3.

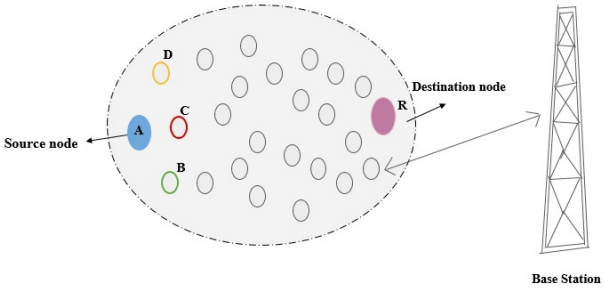

Figure 3: Structure of the WSN Model

5. ADAPTATION TO THE PROBLEM

A trust based integrated fuzzy MCDM paradigm ([48], [49], [50], [51]) is employed in the proposed WSN framework to determine the best choice among all possible alternatives [52]. The trustor and trustee relationship among the source node and the neighbouring nodes are evaluated based on the trust attributes whose values are expressed in the form of pythagorean fuzzy number. All trust factors are divided into four groups. The factors that have a favourable influence on circulation are classified as benefit criteria, whereas those that have a negative impact are classified as cost criteria. Bandwidth, heterogeneity, confidentiality, data reputation, authentication, integrity, lightweight, geographic distribution, friendliness, cooperativeness, reputation, lifetime, and applicability in terms of trust are among the benefit criteria, while delay and cost are among the cost criteria and those descriptions are listed as follows.

Bandwidth (ζ_{11})**:**

- Bandwidth refers to the maximum rate of data transfer across a network. It determines how much data can be transmitted in a given amount of time.
- High bandwidth facilitates faster data transfer, enabling smoother communication and quicker access to resources.

Delay (ζ_{12})**:**

- Delay, also known as latency, is the time taken for data to travel from the source to the destination.

- High delay can degrade user experience and affect the performance of interactive applications, leading to delays in responses and increased frustration.

Heterogeneity (ζ_{13})**:**

- In computing systems, heterogeneity refers to the presence of diverse elements such as different hardware architectures, operating systems, or programming languages within a single system or network.
- Heterogeneity poses both challenges and opportunities in distributed computing. On one hand, it can lead to complexities in interoperability and communication among diverse components.

Throughput (ζ_{14})**:**

- Throughput is a measure of the rate at which a system can process tasks or data within a given period of time.
- It's a critical metric in evaluating the performance of systems, especially in high-demand environments.

Confidentiality (ζ_{21})**:**

- Confidentiality ensures that sensitive information is accessible only to authorized parties and is protected from unauthorized access or disclosure.
- Confidentiality is critical for protecting personal data, financial information, trade secrets, and classified government information from malicious actors and unauthorized users.

Data Replication (ζ_{22})**:**

- Data replication involves creating and maintaining multiple copies of data across different locations or nodes in a network.
- It is commonly used in distributed systems, content delivery networks (CDNs), and cloud computing environments to enhance reliability and performance.

Authentication (ζ_{23})**:**

- Authentication verifies the identity of users or entities attempting to access a system or resource.
- It ensures that only authorized users can access sensitive data or perform specific actions.

Lightweight (ζ_{24})**:**

- Lightweight refers to the design philosophy aimed at minimizing resource consumption, such as memory, processing power, and energy, while maintaining essential functionality and performance.

- Lightweight solutions are particularly desirable in environments with limited resources, such as embedded systems, mobile devices, and Internet of Things (IoT) devices.

Geographical Distribution (ζ_{31})**:**

- Geographical distribution refers to the spread of resources, users, or infrastructure across different geographic locations.
- It enables redundancy, fault tolerance, and scalability by distributing resources closer to users and reducing latency.

Friendliness (ζ_{32})**:**

- Friendliness in the context of WSNs refers to the ability of sensor nodes to interact and cooperate with each other in a cooperative manner.
- Cooperative behaviors among sensor nodes contribute to the overall efficiency, reliability, and resilience of the WSN by promoting information sharing, load balancing, and fault tolerance.

Cooperativeness (ζ_{33})**:**

- Cooperativeness in WSNs refers to the ability of sensor nodes to collaborate and work together towards common goals, such as data collection, processing, and routing.
- By fostering cooperation among sensor nodes, WSNs can achieve better coverage, reduced energy consumption, improved data accuracy, and enhanced network scalability.

Reputation (ζ_{41})**:**

- Reputation plays a crucial role in various domains, including e-commerce, social networks, and online communities.
- It represents the perceived trustworthiness, reliability, and credibility of individuals, organizations, or entities within a community or ecosystem.

Lifetime (ζ_{42})**:**

- The lifetime of a WSN refers to the duration for which the network can operate without requiring maintenance or replacement of sensor nodes.
- Maximizing the lifetime of a WSN is crucial, especially in applications where sensor nodes are deployed in remote or inaccessible locations.

Cost (ζ_{43})**:**

- Cost considerations play a significant role in the design, deployment, and maintenance of WSNs, particularly in large-scale deployments or resource-constrained environments.

- Optimizing costs in WSNs involves selecting cost-effective hardware components, deploying energy-efficient protocols, minimizing deployment and maintenance overheads, and maximizing the longevity of sensor nodes to achieve desired performance within budget constraints.

Applicability (ζ_{43})**:**

- Applicability refers to the suitability or relevance of a particular solution, algorithm, or technique to the requirements and constraints of the network and its intended application scenarios.

Further, the Pythagorean fuzzy based SECA approach helps in acquiring weight values for the trust parameters. In addition, the acquired weights are compiled in order to rank the alternatives using the utility function-based ARAS technique. Following that, the inherent steps taken to determine the absolute trust value of observed nodes in WSN are detailed further.

Table 5: Linguistic scale for rating alternatives

Linguistic Terms	Rating value
Extremely Trustworthy(ET)	0.9
Highly Trustworthy (HT)	0.8
Moderately Trustworthy (MT)	0.7
Trustworthy (T)	0.6
Equally Trustworthy (ET)	0.5
Untrustworthy (U)	0.4
Moderately Untrustworthy (MU)	0.3
Highly Untrustworthy (VU)	0.2
Extremely Untrustworthy (EU)	0.1

A decision matrix is constructed with p rows $(1 \leq r \leq p)$ representing the neighboring nodes and$q$ columns$(1 \leq s \leq q)$ corresponding to the trust attributes. The linguistic terms presented in Table 5 is incorporated for developing the matrix. The developed matrix with each elementis expressed in the form of pythagorean fuzzy number. The basic steps of any method consist of the following:

1. Construct the decision matrix $D = [D_{rs}]_{p\times q}$ as in eqn (2)

$$\begin{array}{cccc} & \eta_1 & \eta_2 & \cdots & \eta_n \\ \zeta_1 & (\rho_{11},\varsigma_{11}) & (\rho_{12},\varsigma_{12}) & \cdots & \left(\mu_{1q},\varsigma_{1n}\right) \\ \zeta_2 & (\rho_{21},\varsigma_{21}) & (\rho_{22},\varsigma_{22}) & \cdots & \left(\rho_{2q},\varsigma_{2q}\right) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \zeta_p & (\rho_{p1},\varsigma_{p1}) & (\rho_{p2},\varsigma_{p2}) & \cdots & (\rho_{pq},\varsigma_{pq}) \end{array} \tag{2}$$

2. Normalize the matrix based on eqn (3).

$$x_{ij}^N = \begin{cases} \frac{x_{ij}}{\max_k x_{kj}} & \text{if } j \in BC \\ \frac{\min_k x_{kj}}{x_{ij}} & \text{if } j \in NC \end{cases} \tag{3}$$

3. Develop the score matrix $\tilde{D} = [\tilde{D}_{rs}]_{p\times q}$ as in eqn (4) following definition 3.2.

$$\tilde{D}_{rs} = \begin{pmatrix} \tilde{d}_{11} & \tilde{d}_{12} & \dots & \tilde{d}_{1q} \\ \tilde{d}_{21} & \tilde{d}_{22} & \dots & \tilde{d}_{2q} \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{d}_{p1} & \tilde{d}_{p2} & \dots & \tilde{d}_{pq} \end{pmatrix} \tag{4}$$

The algorithm 1 of the pythagorean fuzzy SECA method is employed for estimating the criteria weights h_s corresponding to each criteria η_s. The weight vectors h_s are obtained as which satisfy $\sum_{s=1}^{q} h_s = 1$.

Furthermore, the algorithm 2 of the ARAS methods which ranks the alternatives based on the utility values provides the trustable neighbour. The weight vectors calculated using SECA method is fused with the ARAS method for prioritizing the alternatives.

Table 6: Score matrix for evaluation

	η_{11}	η_{12}	η_{13}	η_{14}	η_{21}	η_{22}	η_{23}	η_{24}	η_{31}	η_{32}	η_{33}	η_{41}	η_{42}	η_{43}	η_{44}
B	0.1	0.4	0.5	0.6	0.2	0.4	0.7	0.5	0.3	0.4	0.8	0.5	0.2	0.7	0.5
C	0.1	0.5	0.3	0.4	0.5	0.2	0.4	0.6	0.4	0.2	0.6	0.1	0.3	0.5	0.4
D	0.5	0.6	0.4	0.3	0.5	0.1	0.1	0.4	0.2	0.7	0.5	0.6	0.5	0.5	0.4
E	0.2	0.3	0.3	0.5	0.5	0.4	0.1	0.5	0.7	0.5	0.2	0.8	0.6	0.5	0.1

6. RESULTS AND DISCUSSION

This study aims to examine and rank the key components in determining WSN trustworthiness.

- We prioritised 15 sub-criteria using an integrated fuzzy method. Then, four neighbouring nodes that we identified were investigated to see if they were more secure and appropriate for data forwarding using our preferred method. The proposed integrated decision procedure is executed using LINGO and MATLAB. Following steps (1) to (3), the score matrix obtained is presented in Table 6. The figure 4 below demonstrates how the SECA technique allocates weights based on each attribute and according to the ARAS method's ranking results in figure 5, node E is the most trustable followed by the nodes B, D, and C.

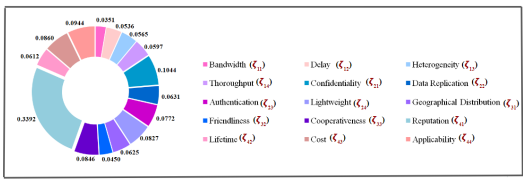

Figure 4: Attribute Weights by SECA Approach

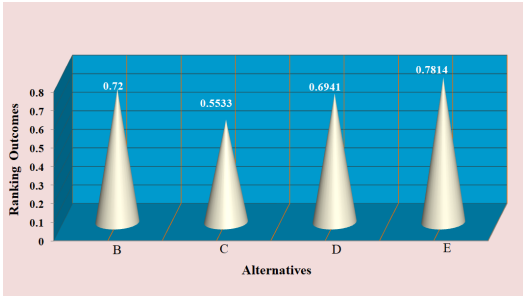

Figure 5: Ranking Results of each Alternatives based on ARAS Approach

- In light of this, the resulting node could be trusted to embark on WSN communication. The outcome is then compared to existing MCDM techniques [53], with the Evaluation Based on Distance from Average Solution (EDAS) [54] and TOPSIS [21] algorithms being assessed using the suggested weight methodology. Utilization of a pairwise comparison-based AHP technique [23], a similarity measurement-based TOPSIS approach, and a distance-based EDAS approach yield diverse ranking values, as shown in the figure 6. In essence, the AHP method based on pairwise comparisons is depicted in Figure 6, while its application in illustrating the superiority of the proposed methods through ranking and weighting techniques is visualized in Figure 4a.

- Moreover, in order to assess the significance of weighting, various ranking methodologies are also incorporated into weighing techniques. In this regard, VIKOR [21] and Combinative Distance-Based Assessment (CODAS) [55] methods are employed as alternatives to TOPSIS, being enhanced distance-based techniques. The visual representation in Figure 4a illustrates the integration of decision-making approaches. Here, the proposed weighting values, along with the score matrix, are applied to VIKOR, AHP, and CODAS methods to ascertain rankings. Additionally, AHP and RS [56] methods are utilized to derive weighting outcomes, which are subsequently incorporated into the proposed ARAS method.

- The superiority of the suggested approach is ultimately evaluated using Spearman's rank correlation coefficient, as illustrated in Figure 4b. While the identification of reliable neighbors holds significant importance, our approach provides a more secure option among the considered methodologies.

- Further, a sensible approach is employed to showcase the consistency of outcomes in prioritization. To achieve this, weighting values have been interchanged in three different ways, each resulting in distinct ranking outcomes, is tabulated in table 4. Notably, ranking result 3, based on experts' subjective weights, aligns closely with the proposed ranking result. Consequently, the proposed method exhibits appropriate ranking precedence for the given problem.

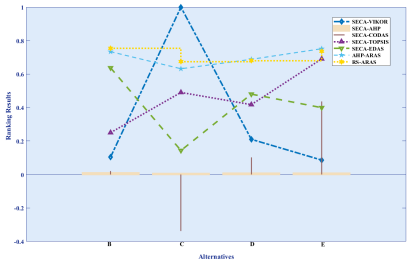

Figure 6: Comparison of each Approaches Ranking Results

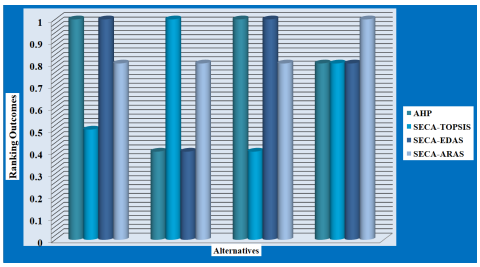

Figure 7: Outcomes by the Spearman's rank correlation coefficient

Table 7: Ranking Results by Sensitive Analysis

Alternatives	B	C	D	E
Ranking Result 1	0.7776	0.6572	0.7135	0.6365
Ranking Result 2	0.6242	0.5229	0.7239	0.6762
Ranking Result 3	0.7222	0.5579	0.6745	0.7554

7. CONCLUSION

Privacy in WSNs has emerged as a critical consideration across various expedition scenarios, where different nodes rely on their neighbors for transmitting sensed data securely to a sink node. Recognizing the importance of trust in decision-making processes, this study advocated for the implementation of a trust information system to effectively identify nodes capable of facilitating secure communication.

Drawing upon research findings, this study extensively examined various parameters and delineated a suitable framework for assessing trustworthiness. By conducting a comprehensive review of sophisticated trust measures in WSNs, further addressed diverse concerns associated with ensuring secure communication.

To ascertain the most suitable neighbor node for secure communication, the study introduced a novel ranking algorithm, integrating the SECA and ARAS approaches. This algorithm considered multiple factors including QoS, QoSec, social relationships, and past reputation to evaluate the reliability of surrounding nodes, quantified on a scale from 0 to 1. Notably, reliability took precedence over delay and cost in the selection process.

Furthermore, the study underscored the dynamic nature of node rankings, as values

of QoS, QoSec, social relationships, and past reputations may influence node rankings over time. A case study involving four alternatives and parameters is presented to illustrate the efficacy of the proposed algorithm in determining the optimal node for secure communication.

Quantitative analysis demonstrated the adaptability and effectiveness of the proposed strategy. However, decision-making methodologies must consider ethical implications and consequences. However, ethical dilemmas or conflicting ethical principles can complicate the decision-making process and pose challenges for decision-makers. To overcome from these issue in future research endeavors, the study aims to enhance decision-making processes by integrating advanced MCDM techniques, leveraging fuzzy systems and other elements to further optimize node selection processes in WSNs.

Funding: This work was funded by National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT) (No. 2022R1C1C1006671).

REFERENCES

[1] H. Wang, X. Huang, and Y. Wu, "Gd3n: Adaptive clustering-based detection of selective forwarding attacks in wsns under variable harsh environments," *Information Sciences*, vol. 665, p. 120375, 2024.

[2] P. Ashok Babu, L. Kavisankar, J. Xavier, V. Senthilkumar, G. Kumar, T. Kavitha, A. Rajendran, G. Harikrishnan, A. Rajaram, A. G. Adigo *et al.*, "Selfish node detection for effective data transmission using modified incentive sorted pathway selection in wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, p. 9359135, 2022.

[3] N. Tabassum, G. D. Devanagavi, R. C. Biradar, and C. Ravindra, "Survey on data aggregation based security attacks in wireless sensor network," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 3, pp. 3131–3139, 2023.

[4] B. A and S. Ravindran, "Intelligent fuzzy logic based intrusion detection system for effective detection of black hole attack in wsn," *Peer-to-Peer Networking and Applications*, vol. 17, no. 4, pp. 1813–1829, 2024.

[5] S. Narayanamoorthy, T. N. Parthasarathy, S. Pragathi, P. Shanmugam, D. Baleanu, A. Ahmadian, and D. Kang, "The novel augmented fermatean mcdm perspectives for identifying the optimal renewable energy power plant location," *Sustainable Energy Technologies and Assessments*, vol. 53, p. 102488, 2022.

[6] D. Kang, A. Anuja, S. Narayanamoorthy, M. Gangemi, and A. Ahmadian, "A dual hesitant q-rung orthopair enhanced marcos methodology under uncertainty to determine a used ppe kit disposal," *Environmental Science and Pollution Research*, vol. 29, no. 59, pp. 89 625–89 642, 2022.

[7] S. Narayanamoorthy, A. Anuja, S. Pragathi, M. Sandra, M. Ferrara, A. Ahmadian, and D. Kang, "Assessment of inorganic solid waste management techniques using full consistency and extended mabac method," *Environmental Science and Pollution Research*, vol. 31, no. 7, pp. 9981–9991, 2023.

[8] T. N. Parthasarathy, S. Narayanamoorthy, R. Sulaiman, A. M. Elamir, A. Ahmadian, and D. Kang, "An end-to-end categorizing strategy for green energy sources: Picture q-rung orthopair fuzzy exprom-ii: Mada approach," *Sustainable Energy Technologies and Assessments*, vol. 63, p. 103658, 2024.

[9] J. R. V. J. Brainy, S. Narayanamoorthy, M. Sandra, D. Pamucar, and D. Kang, "An unified fuzzy decision strategy for analysing green fuel alternatives: A road to long-term development," *Engineering Applications of Artificial Intelligence*, vol. 130, p. 107733, 2024.
[10] L. A. Zadeh, "Fuzzy sets," *Information and control*, vol. 8, no. 3, pp. 338–353, 1965.
[11] K. T. Atanassov, *On intuitionistic fuzzy sets theory*. Springer, 2012, vol. 283.
[12] R. R. Yager, "Pythagorean membership grades in multicriteria decision making," *IEEE Transactions on fuzzy systems*, vol. 22, no. 4, pp. 958–965, 2013.
[13] S. Jana and S. Islam, "A pythagorean hesitant fuzzy programming approach and its application to multi objective reliability optimization problem," *Yugoslav Journal of Operations Research*, vol. 34, no. 2, pp. 201–227, 2023.
[14] H. Liao, Y. Chang, D. Wu, and X. Gou, "Improved approach to quality function deployment based on pythagorean fuzzy sets and application to assembly robot design evaluation," *Frontiers of Engineering Management*, vol. 7, no. 2, pp. 196–203, 2020.
[15] H. Yazbek, F. Surriya, S. U. Khan, N. Jan, and D. Marinkovic, "A novel approach to model the economic characteristics of an organization by interval-valued complex pythagorean fuzzy information," *Journal of Computational and Cognitive Engineering*, vol. 2, no. 1, pp. 75–87, 2023.
[16] Z. Yu, S. A. R. Khan, M. Mathew, M. Umar, M. Hassan, and M. J. Sajid, "Identifying and analyzing the barriers of internet-of-things in sustainable supply chain through newly proposed spherical fuzzy geometric mean," *Computers & Industrial Engineering*, vol. 169, p. 108227, 2022.
[17] K. Ullah, T. Mahmood, Z. Ali, and N. Jan, "On some distance measures of complex pythagorean fuzzy sets and their applications in pattern recognition," *Complex & Intelligent Systems*, vol. 6, pp. 15–27, 2020.
[18] F. Xiao and W. Ding, "Divergence measure of pythagorean fuzzy sets and its application in medical diagnosis," *Applied Soft Computing*, vol. 79, pp. 254–267, 2019.
[19] A. Karasan, E. Ilbahar, S. Cebi, and C. Kahraman, "A new risk assessment approach: Safety and critical effect analysis (scea) and its extension with pythagorean fuzzy sets," *Safety science*, vol. 108, pp. 173–187, 2018.
[20] P. Maratha and K. Gupta, "Linear optimization and fuzzy-based clustering for wsns assisted internet of things," *Multimedia Tools and Applications*, vol. 82, no. 4, pp. 5161–5185, 2023.
[21] S. Madhavi, N. Santhosh, S. Rajkumar, and R. Praveen, "Pythagorean fuzzy sets-based vikor and topsis-based multi-criteria decision-making model for mitigating resource deletion attacks in wsns," *Journal of Intelligent & Fuzzy Systems*, vol. 44, no. 6, pp. 9441–9459, 2023.
[22] S. Madhavi, R. Praveen, N. Jagadish Kumar, and S. UdhayaSankar, "Hybrid grey piprecia and grey ocra method-based dynamic multi-criteria decision-making model for mitigating non-cooperating node attacks in wsns," *Peer-to-Peer Networking and Applications*, vol. 16, no. 5, pp. 2607–2629, 2023.
[23] A. K. Gautam and R. Kumar, "A trust based neighbor identification using mcdm model in wireless sensor networks," *Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science)*, vol. 14, no. 4, pp. 1336–1351, 2021.
[24] S. O. Ogundoyin and I. Kamil, "A fuzzy-ahp based prioritization of trust criteria in fog computing services," *Applied Soft Computing*, vol. 97, p. 106789, 2020.
[25] W. Ya, Z. Meng-Ran, N. Lei, and Z. Jia, "Trust analysis of wsn nodes based on fuzzy theory," *International Journal of Computers and Applications*, vol. 42, no. 1, pp. 52–56, 2020.
[26] M. Rizwanullah, S. Singh, R. Kumar, F. S. Alrayes, A. Alharbi, M. M. Alnfiai, P. K. Chaurasia, and A. Agrawal, "Development of a model for trust management in the social internet of things," *Electronics*, vol. 12, no. 1, p. 41, 2022.
[27] A. B. Paul, S. Biswas, S. Nandi, and S. Chakraborty, "Matem: A unified framework based on

trust and mcdm for assuring security, reliability and qos in dtn routing," *Journal of Network and Computer Applications*, vol. 104, pp. 1–20, 2018.

[28] Y. Alghofaili and M. A. Rassam, "A trust management model for iot devices and services based on the multi-criteria decision-making approach and deep long short-term memory technique," *Sensors*, vol. 22, no. 2, p. 634, 2022.

[29] O. AlFarraj, A. AlZubi, and A. Tolba, "Trust-based neighbor selection using activation function for secure routing in wireless sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–11, 2018.

[30] J. R. Gandhi and R. H. Jhaveri, "Packet forwarding misbehaviour isolation using fuzzy trust-based secure routing in manet," *International Journal of Computer Applications*, vol. 122, no. 3, 2015.

[31] R. Singh, J. Singh, R. Singh *et al.*, "Fuzzy based advanced hybrid intrusion detection system to detect malicious nodes in wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 2017, no. 1, p. 3548607, 2017.

[32] S. Sinha and A. Paul, "Neuro-fuzzy based intrusion detection system for wireless sensor network," *Wireless personal communications*, vol. 114, no. 1, pp. 835–851, 2020.

[33] M. Akram, G. Muhammad, and D. Ahmad, "Analytical solution of the atangana–baleanu–caputo fractional differential equations using pythagorean fuzzy sets," *Granular Computing*, vol. 8, no. 4, pp. 667–687, 2023.

[34] M. Keshavarz-Ghorabaee, M. Amiri, E. Zavadskas, Z. Turskis, and J. Antucheviciene, "Simultaneous evaluation of criteria and alternatives (seca) for multi-criteria decision-making," *Informatica*, vol. 29, no. 2, pp. 265–280, 2018.

[35] S. Bahrami and M. Rastegar, "Security-based critical power distribution feeder identification: Application of fuzzy bwm-vikor and seca," *International Journal of Electrical Power & Energy Systems*, vol. 134, p. 107395, 2022.

[36] S. Mishra, M. N. Sahoo, S. Bakshi, and J. J. Rodrigues, "Dynamic resource allocation in fog-cloud hybrid systems using multicriteria ahp techniques," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8993–9000, 2020.

[37] S. Narayanamoorthy, J. Brainy, R. A. Shalwala, T. R. Alsenani, A. Ahmadian, and D. Kang, "An enhanced fuzzy decision making approach for the assessment of sustainable energy storage systems," *Sustainable Energy, Grids and Networks*, vol. 33, p. 100962, 2023.

[38] M. Keshavarz-Ghorabaee, K. Govindan, M. Amiri, E. Zavadskas, and J. Antucheviciene, "An integrated type-2 fuzzy decision model based on waspas and seca for evaluation of sustainable manufacturing strategies," *Journal of Environmental Engineering and Landscape Management*, vol. 27, no. 4, pp. 187–200, 2019.

[39] E. Zavadskas and Z. Turskis, "A new additive ratio assessment (aras) method in multicriteria decision-making," *Technological and economic development of economy*, vol. 16, no. 2, pp. 159–172, 2010.

[40] Y. Hu, A. Al-Barakati, and P. Rani, "Investigating the internet-of-things (iot) risks for supply chain management using q-rung orthopair fuzzy-swara-aras framework," *Technological and Economic Development of Economy*, vol. 30, no. 2, pp. 376–401, 2022.

[41] A. Mohammadian, J. HeidaryDahooie, A. R. Qorbani, E. Zavadskas, and Z. Turskis, "A new multi-attribute decision-making framework for policy-makers by using interval-valued triangular fuzzy numbers," *Informatica*, vol. 32, no. 3, pp. 583–618, 2021.

[42] A. Raj Mishra, G. Sisodia, K. Raj Pardasani, and K. Sharma, "Multi-criteria it personnel selection on intuitionistic fuzzy information measures and aras methodology," *Iranian Journal of Fuzzy Systems*, vol. 17, no. 4, pp. 55–68, 2020.

[43] V. Sihombing, Z. Nasution, M. A. Al Ihsan, M. Siregar, I. Munthe, V. M. Siregar, I. Fatmawati, and D. A. Asfar, "Additive ratio assessment (aras) method for selecting english course branch

locations," in *Journal of Physics: Conference Series*, vol. 1933, no. 1. IOP Publishing, 2021, p. 012070.

[44] J. HeidaryDahooie, E. KazimierasZavadskas, M. Abolhasani, A. Vanaki, and Z. Turskis, "A novel approach for evaluation of projects using an interval–valued fuzzy additive ratio assessment (aras) method: a case study of oil and gas well drilling projects," *Symmetry*, vol. 10, no. 2, p. 45, 2018.

[45] G. Büyüközkan and F. Göçer, "An extension of aras methodology under interval valued intuitionistic fuzzy environment for digital supply chain," *Applied Soft Computing*, vol. 69, pp. 634–654, 2018.

[46] L. Balezentiene and A. Kusta, "Reducing greenhouse gas emissions in grassland ecosystems of the central lithuania: multi-criteria evaluation on a basis of the aras method," *The Scientific World Journal*, vol. 2012, p. 908384, 2012.

[47] C. Ghenai, M. Albawab, and M. Bettayeb, "Sustainability indicators for renewable energy systems using multi-criteria decision-making model and extended swara/aras hybrid method," *Renewable Energy*, vol. 146, pp. 580–597, 2020.

[48] D. Kang, M. Sandra, S. Narayanamoorthy, K. Suvitha, D. Pamucar, and V. Simic, "An enhanced decision making model for industrial robotic selection using three factors: Positive, abstained, and negative grades of membership," *Applied Soft Computing*, p. 111447, 2024.

[49] M. Kamran, S. Ashraf, S. K. Khan, A. H. Khan, H. Zardi, and S. Mehmood, "Integrated decision-making framework for hospital development: A single-valued neutrosophic probabilistic hesitant fuzzy approach with innovative aggregation operators," *Yugoslav Journal of Operations Research*, vol. 34, no. 3, pp. 515–550, 2024.

[50] S. Narayanamoorthy, S. Pragathi, M. Shutaywi, A. Ahmadian, and D. Kang, "Analysis of vaccine efficacy during the covid-19 pandemic period using csf-electre-i approach," *Operations Research Perspectives*, vol. 9, p. 100251, 2022.

[51] S. Narayanamoorthy, L. Ramya, A. Gunasekaran, S. Kalaiselvan, and D. Kang, "Selection of suitable biomass conservation process techniques: a versatile approach to normal wiggly interval-valued hesitant fuzzy set using multi-criteria decision making," *Complex & Intelligent Systems*, vol. 9, no. 6, pp. 6681–6695, 2023.

[52] Suman, R. Kumar, and N. Gandotra, "Novel pythagorean fuzzy based information measure using topsis technique for application in multi-criteria decision making," in *2023 10th International Conference on Computing for Sustainable Global Development (INDIACom)*, 2023, pp. 1271–1276.

[53] D. Kang, K. Suvitha, S. Narayanamoorthy, M. Sandra, and D. Pamucar, "Evaluation of wave energy converters based on integrated electre approach," *Expert Systems with Applications*, vol. 242, p. 122793, 2024.

[54] S. Narayanamoorthy, S. Pragathi, T. N. Parthasarathy, S. Kalaiselvan, J. V. Kureethara, R. Saraswathy, P. Nithya, and D. Kang, "The covid-19 vaccine preference for youngsters using promethee-ii in the ifss environment," *Symmetry*, vol. 13, no. 6, p. 1030, 2021.

[55] A. Mohammadifar, H. Gholami, and S. Golzari, "Novel integrated modelling based on multiplicative long short-term memory (mlstm) deep learning model and ensemble multi-criteria decision making (mcdm) models for mapping flood risk," *Journal of Environmental Management*, vol. 345, p. 118838, 2023.

[56] S. Narayanamoorthy, A. Anuja, D. Kang, J. V. Kureethara, S. Kalaiselvan, and T. Manirathinam, "A distinctive symmetric analyzation of improving air quality using multi-criteria decision making method under uncertainty conditions," *Symmetry*, vol. 12, no. 11, p. 1858, 2020.