Hybrid Interval Type-2 Fuzzy AHP and COPRAS-G-based trusted neighbour node Discovery in Wireless Sensor Networks

[1]E Jyothi Kiranmayi, [2]N V Rao and [3]K S Nayanathara
[1]Department of Computer Science, SVD Government Degree College (W), Andhra Pradesh, India.
[2]Department of CSE, CVR College of Engineering, Hyderabad, Telangana, India.
[3]Department of ECE, CVR College of Engineering, Hyderabad, Telangana, India.
[1]jkiranmayi1@gmail.com, [2]nvyaghresh@gmail.com, [3]ksattirajunayanathara@gmail.com

Correspondence should be addressed to E Joythi Kiranmayi : jkiranmayi1@gmail.com.

Article Info
Journal of Machine and Computing (http://anapub.co.ke/journals/jmc/jmc.html)
Doi: https://doi.org/10.53759/7669/jmc202303023
Received 02 December 2022; Revised from 22 March 2023; Accepted 20 April 2023.
Available online 05 July 2023.

Abstract—In Wireless Sensor Networks (WSNs), reliable and rapid neighbour node discovery is considered as the crucial operation which frequently needs to be executed over the entire lifecycle. Several neighbour node discovery mechanisms are proposed for reducing the latency or extending the sensor nodes' lifetime. But majority of the existing neighbour node discovery mechanisms failed in addressing the critical issues of real WSNs related to energy consumptions, constraints of latency, uncertainty of node behaviors, and communication collisions. In this paper, Hybrid Interval Type-2 Fuzzy Analytical Hierarchical Process (AHP) and Complex Proportional Assessment using Grey Theory (COPRAS-G)-based trusted neighbour node discovery scheme (FAHPCG) is proposed for better data dissemination process. In specific, Interval Type 2 Fuzzy AHP is applied for determining the weight of the evaluation criteria considered for neighbour node discovery, and then Grey COPRAS method is adopted for prioritizing the sensor nodes of the routing path established between the source and destination. It adopted the merits of fuzzy theory for handling the uncertainty and vagueness involved in the change in the behavior of sensor nodes during the process of neighbour discovery. It is proposed with the capability of exploring maximized number of factors that aids in exploring the possible dimensions of sensor nodes packet forwarding potential during the process of neighbour node discovery. The simulation results of the proposed FAHPCG scheme confirmed an improved neighbour node discovery rate of 23.18% and prolonged the sensor nodes lifetime to the maximum of 7.12 times better than the baseline approaches used for investigation.

Keywords—Wireless Sensor Networks (WSNs), Neighbor Node Discovery, Fuzzy Theory, Analytical Hierarchical Process (AHP), Complex Proportional Assessment (COPRAS), Grey Theory.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) comprise of a set of closely placed sensor nodes which are positioned randomly to observe ecological variations. The primary function of the nodes is to detect, sense and forward information about the ecological changes to a Base Station (BS) or sink [1]. The nodes include processing units along with power backup [2]. These networks confront two main challenges based on attaining energy efficiency and selection of neighbours. As nodes are placed in remote and inaccessible regions, charging devices frequently becomes an uphill task. The network has limited resources, preventing nodes from adapting to application demands [3]. The environment in which the nodes are deployed is not predictable, and it is expected that nodes adapt with its neighbours. In case the sink is at a distance from the node that forwards data, it transmits information through existing neighbours. The nodes trust their neighbours to forward information [4]. Nodes which are positioned in the region of an adversary are open to vulnerability. They may be compromised, or bogus information may be injected. The nodes influenced by a threat from outside may not be considered reliable as they do not convey the original sensed information [5].

Neighbour discovery is essential for protocols that are used in wireless networks. Neighbours are adjacent nodes present in the region of coverage of the communicating node. The nodes which are single hop away are immediate neighbours of the forwarding node [6]. The neighbours help the communicating node in discovering the network along the routing paths [7]. External attackers execute actions on neighbours to mislead, falsify and alter information that is transmitted [8]. As WSNs demand multi-hop communication amid the source and the sink, data transmission is open to susceptibility. These wireless networks demand safe routing to stop data from getting retrieved by external nodes. Optimal routing offers improved neighbour selection, easy communication along with reduced routing overhead [9].

Neighbour selection based on trust is used to assess neighbours based on performance which ensures increased reliability as well as privacy during data transmission. Trust gives the reliability level of a node that is based on its actions. For every protocol, the trusted choice of neighbour is vital during neighbour discovery [10]. Safe routing protocols assure security at the network layer except node misbehaviour attack. Cryptography as well as authentication security techniques are unsuitable for dealing with misbehaviour attacks [11]. The progress of trust as well as reputation-dependent security mechanisms is resilient to behavioural attacks. In case of trust-based security managing mechanisms, node actions are anticipated depending on former observations [12]. The trust level is determined over time slots to find node feasibility to take part in routing. Trust-based models provide protected relationships amid nodes by calculating reputation in a particular period. Managing periodic reputation is defaced in huge and thickly inhabited networks owing to repeated transmission of update information. The present protocols emphases on choosing safe neighbours regardless of the resource constraints of nodes [13]. This leads to quick energy drain of favoured nodes. In addition, some protocols transmit huge information sequences to preserve trust updates leading to injection of false information that reduces the node's trust [14]. In a huge network, the transmitting node is not capable of selecting the suitable communication pair depending on trust. In case the neighbour is chosen deprived of any intent, it is hard to ensure trustworthiness of the node. This demands mutual cooperation amid nodes [15]. Owing to the lack of trust amid networks, the network lifespan is dropped which affects the whole process of transmission.

In this paper, Hybrid Interval Type-2 Fuzzy Analytical Hierarchical Process (AHP) and Complex Proportional Assessment using Grey Theory (COPRAS-G)-based trusted neighbour node discovery scheme (FAHPCG) is proposed for better data dissemination process. In specific, Interval Type 2 Fuzzy AHP is applied for determining the weight of the evaluation criteria considered for neighbour node discovery, and then Grey COPRAS method is adopted for prioritizing the sensor nodes of the routing path established between the source and destination. It adopted the merits of fuzzy theory for handling the uncertainty and vagueness involved in the change in the behavior of sensor nodes during the process of neighbour discovery. It is proposed with the capability of exploring maximized number of factors that aids in exploring the possible dimensions of sensor nodes packet forwarding potential during the process of neighbour node discovery. The simulation experiments of the proposed FAHPCG scheme is conducted using PDR, throughput, energy consumptions, neighbour node discovery rate and network lifetime with different number of sensor nodes, malicious or malevolent nodes, and simulation time.

The remaining section of the paper is structured as follows. Section 2 presents the comprehensive review of the existing trusted neighbour node discovery scheme with an extract and literature that formed the motivation of this proposed work. Section 3 provides a detailed view of the proposed FAHPCG with the importance of fuzzy theory, COPRAS-G and AHP during the process of reliable neighbor node discovery. Section 4 demonstrates the simulation results and discussion of the proposed FAHPCG with the baseline mechanisms with different number of sensor nodes, malicious nodes and simulation time.

II. RELATED WORKS

In this section the comprehensive review of the existing reliable neighbor node discovery mechanisms contributed to the literature over the recent years are presented with an extract of the literature.

Ahmed et al. [16] proposed a Trust and Energy aware Secure Routing Protocol (TESRP) which uses a non-centralised trust model for finding and segregating misbehaving nodes during trust assessment stage. TESRP uses a multi-facet routing mechanism based on trust level, remaining energy along with hop-counts. It does not consider the geographic data or tight time synchronization. This guarantees data dissemination through reliable nodes and balances energy consumption amid reliable nodes while moving along shortest paths. The proposed scheme offers improved throughput, network lifespan and energy consumption in contrast to existing algorithms. It is robust to heavy network loads and shows stable enhancement in network performance. Karthik and Ananthanarayana [17] proposed a hybrid approach that assigns a trust score to data and nodes depending on quality of data and communication trust correspondingly. The proposed Hybrid Trust Management Scheme (HTMS) identifies data fault using temporal and spatial associations. It scores the sensed data based on correlation metric along with provenance data. It uses the trust score of data for making decisions. It employs the communication trust along with provenance data for assessing the trust score of intermediary and source nodes. In case the reliability of data item is ensured for making critical decisions, it assigns reward by adding trust score to intermediate and source nodes. Else, it gives punishments by dropping the trust score of nodes. HTMS can identify malevolent, faulty and selfish nodes along with unreliable data. It also offers an acceptable level of attack resistance.

Ahmed et al. [18] proposed an Energy-aware Secure Routing with Trust (ESRT) scheme designed for disaster relief processes which sustains a reliable setting by isolating malevolent nodes. ESRT is based on factors which include trust, energy along with hop count for choosing routes. This routing approach aids in balancing the amount of energy consumed amid reliable nodes while forwarding data involving shorter paths, thereby dropping the amount of transmissions along with contention in wireless medium. To circumvent pre-mature energy exhaustion of reliable node, ESRT includes remaining energy dependent threshold scheme in path selection which aids in prolonging network lifespan. ESRT is based on direct, indirect as well as estimated positive probability of nodes. It does not consider geographic information or strict time synchronization. It is resilient to considerable network load and shows stable enhancement in performance. It is efficient in dynamically identifying and segregating misbehaving as well as malfunctioning nodes during trust assessment stage, whereas energy awareness is integrated in path setup stage of the routing protocol that aids in improved load balancing amid reliable nodes. It is found that the proposed scheme offers better throughput and network lifespan, involving reduced end-to-end delay with increased Normalized Routing Load (NRL) in contrast to standard schemes. AlFarraj et al.[19] formulated an Activation Function-based Trusted Neighbour Selection (AF-TNS) for resource-restricted WSNs to improve security. It functions in 2 stages namely, trust assessment with energy constraint and metric-based node assessment to preserve reliability of neighbours. It uses sequential activation function along with arbitrary transigmoid function to simplify the tedious process of decision making by differentiating reliable and un-reliable nodes to maintain performance of the network. It assures consistency of nodes by periodic update as well as cross investigation of trust over transmissions. From the outcomes, it is obvious that the scheme offers improved malevolent detection rate, throughput and network lifetime, involving reduced delay, energy and false detective rate.

Javid [20] proposed a neighbour discovery mechanism that integrated Neighbour Node Approaching Distinct Energy-Efficient Mates (NADEEM), Fallback Approach NADEEM (FA-NADEEM) and Transmission Adjustment-NADEEM (TA-NADEEM). In case of NADEEM, nodes that are immutable are not chosen for forwarding by using different selection factors. It removes void holes by using a fallback recovery scheme that delivers data effectively to the destination. It chooses nodes that are closer in the backward direction and determines the route to the destination. It dynamically changes the range of transmission to support greedy forwarding amid nodes. The non-void nodes can only act as forwarders. It dynamically modifies the range of transmission of the void node to forward packets to the destination effectively. It determines feasible regions based on linear programming for ideal energy dissipation and improvement of throughput. The proposed scheme offers better results in terms of energy, Packet Delivery Ratio (PDR) as well as void nodes. The performance is analysed for diverse transmission ranges along with data rates. Zhao et al. [21] proposed Exponential-based Trust and Reputation Evaluation System (ETRES) for assessing the nodes' trust along with their reputation. It observes nodes' behaviour and applies exponential distribution to distribute the trust of nodes. This enables selection of consistent nodes to take part in data forwarding and removing malevolent node attacks. Entropy theory is used for measuring the improbability of direct trust. Indirect trust strengthens interaction information when improbability of direct trust is more. Exponential distribution is examined to show trust and reputation. Entropy theory aids in accessing the uncertainty level. It reduces the computing power in nodes and also prolongs the network lifespan. Confidence factor related to direct trust is computed depending on the amount of co-operation amid nodes which dynamically regulates the nodes' trust to deteriorate the impact of compromised nodes.

Anwar et al. [22] proposed Belief based Trust Evaluation Mechanism (BTEM) to isolate malevolent from trust-worthy nodes and overcome Bad-mouth, Denial of Service (DoS) as well as On-Off attacks. Bayesian belief-based method is used for finding malevolent nodes and isolating them. Bayesian estimation is used for finding the nodes' direct as well as in-direct trusts. It takes data correlation gathered over time, and then determines the imprecise knowledge for making decisions that support safe data delivery, thus evading malevolent nodes. It offers co-operation and determines trust amid nodes by identifying and segregating malevolent nodes. In contrast to existing methods, the proposed scheme offers better performance in detecting malevolent nodes with reduced delay and improved network throughput and trustworthiness. Gautam and Kumar [23] proposed a dynamic and effective trust model depending on ranking scheme for recommending suitable secure neighbour node. To rank neighbours, voting mechanism along with hybrid Analytical Hierarchy Process (AHP) and Technique for Order Preference by Similarity to the Ideal Solution (TOPSIS) is used. It includes a case study that shows the efficacy of the scheme in offering protection against internal attacks. It quantitatively assesses the trustworthiness of neighbouring nodes in the range 0 and 1. It chooses the best node amid alternatives.

In addition, Das and Dwivedi [24] proposed a Multi Agent Weight based Clustering-Dynamic Trust Estimation (MWC-DTE) scheme for reliable transmission involving reduced energy. Weight Based Clustering Algorithm (WBCA) is employed for efficient Cluster Head (CH). It depends on communication power, ideal node degree, battery power as well as mobility. DTE scheme is used for assessing dynamic trust. The proposed mechanism includes several modules that are based on direct, indirect, integrated and update trust. Direct trust is computed based on factors including data, energy and communication trusts. Indirect trust is computed by Third Party (TP) recommendation. It is assessed by considering both direct and indirect weights. The proposed model offers improved performance based on execution time, energy efficacy, delay and network lifespan.

III. DETAILED VIEW OF THE PROPOSED FAHPCG-BASED NEIGHBOUR NODE DISCOVERY SCHEME

In this section, the detailed view of the proposed Hybrid Interval Type-2 Fuzzy AHP and COPRAS-G-based trusted neighbour node discovery (FAHPCG) Scheme is presented as follows.

This proposed FAHPCG Scheme is implemented over each intermediate sensor nodes which acts as the router in transmitting the data from the source to the destination nodes. The sensor nodes existing in the routing path established between the source and destination is explored for determining the reliable neighbourhood nodes which confirms the delivery of packets in the network. Initially, the primitives of Interval Type-2 Fuzzy Sets (IT1FS) is presented for exploring the uncertain and vagueness behavior of sensor nodes during the process of data dissemination in the network.

Primitives of Interval Type-2 Fuzzy Sets (IT1FS)

Type-1 Fuzzy Set (T1FS) is not capable of handling uncertainties, which is operational on meaningless data which represents uncertainty of these fuzzy sets. In case a value of 0.5 is assigned, it means the element fits 50% to T1FS. The membership degree varies with people. Single membership reveals uncertainty. Nevertheless, T1FS faces challenges like complications in aggregating expert opinions along with presence of noisy data in measurements which lead to imprecision. T2FS. It is an improved version of T1FS. T2FSs are capable of handling uncertainties efficiently when compared to T1FS. Both FSs are linked to values amid [0, 1]. FSs are featured using membership functions. T1FSs have 2-Dimensional (2D) Membership Function (MF), while T2FSs have 3-Dimensional (3D) MF. MF, the Footprint of Uncertainty (FOU) offers added freedom to get more data. Instead, T2FS is hard to comprehend and apply owing to computational problems and increased mathematical formulation. Interval T2FSs (IT2FS) focus on reducing the computational complexity of T1FSs. They are formulated mathematically as shown below.

IT2F AHP

AHP is used in Multiple Criteria Decision Making (MCDM) is a qualitative technique which considers subjective as well as objective preferences of an individual or group. Basically, AHP involves a theoretical hierarchical structure which includes goals or alternatives, main as well as sub-criteria. It focuses on finding comparative priority as well as criteria weight along with alternatives depending on the judgements of decision makers [28]. This structure enables AHP to be more powerful and efficient amid MCDM, capable of handling complex as well as uncertain problems in real-life by involving qualitative and quantitative principles. Several real-world problems are indeterminate and imprecise. Decision makers find it difficult to choose the best decision. The FS theory is extensively used for handling inaccurate, imprecise, and indeterminate data in real-life situations. To aid in taking the best decision, linguistic terms may be used as quantitative data which is then refined by using assessment techniques of FS theory. The AHP technique includes understandings along with judgements made by decision makers that are typically taken under indeterminate and inaccurate assessment of quantitative/qualitative criteria. Hence, conventional AHP might be moderately biased and detrimental due to the uncertainty linked with the unpredictable errors prevalent in the comparison matrices. The experts verbally express their experiences along with judgments in Pairwise Comparisons (PCs). The linguistic representation seems to be more precise than static value judgements. They are several kinds of Fuzzy-AHP (F-AHP) applications that employ diverse linguistic terms. F-AHP improves the confidence level of decision makers by dropping the judgmental subjectivity as well as uncertainty related to PCs. Moreover, Buckley [33] has enhanced F-AHP by applying Geometric Mean (GM) to Triangular Fuzzy Numbers (TFNs). GM aids in computing fuzzy weights for F-AHP along with extent analysis, thus focusing on computational challenges. The upper as well as lower membership functions permit some quantity of freedom to represent vague and imprecision of real-life settings. To remove ambiguity and imprecision, F-AHP is improved as IT2FS AHP. The steps of IT2FS AHP are listed below [25-27].

Step 1:Identify the goal, criterion, and alternatives (mobile nodes) considered during the process of neighbour node discovery

In this step, the merits of T1F AHP is applied for determining the key criteria, sub-criteria, alternative (exploring different sensor nodes under routing process). and objective based on linguistic terms.

Step 2: Construction of Fuzzy PC Matrices

In this step, the construction of PC matrices with respect to each sensor nodes (alternative), criteria and sub-criteria are evaluated using the linguistic terms that are signified by TFNs. The scales of the IT2F [29-32] considered during the construction of PC matrices is presented in **Table 1.**

Table 1. IT2FS of Linguistic Terms Considered for PC Matrix Construction

Linguistic Variables	Trapezoidal IF Scales
Equally important (E)	(1,1,1,1;1,1) (1,1,1,1;1,1)
Weakly Important (WI)	(1,2,4,5;1,1) (1.2,2.2,3.8,4.8;0.8,0.8)
Strongly important (S)	(3,4,6,7;1,1) (3.2,4.2,5.8,6.8;0.8,0.8)
Very Strongly important (VS)	(5,6,8,9;1,1) (5.2,6.2,7.8,8.8; 0.8,0.8)
Absolutely important (AS)	(7,8,9,9;1,1) (7.2,8.2,8.8,9; 0.8,0.8)

In this context, the comparison value ‘$\tilde{\tilde{\mathrm{T}}}_{\imath\jmath}$’ defined as TFNs within IT2FS $\left(\tilde{\tilde{\mathrm{M}}}\right)$ is represented in Equation (1) and (2)

$$\tilde{\tilde{\mathrm{M}}} = \begin{pmatrix} 1 & \tilde{\tilde{\mathrm{T}}}_{12} & \cdots & \tilde{\tilde{\mathrm{T}}}_{1\mathrm{n}} \\ \tilde{\tilde{\mathrm{T}}}_{21} & 1 & \cdots & \tilde{\tilde{\mathrm{T}}}_{2\mathrm{n}} \\ \vdots & \vdots & \vdots & \vdots \\ \tilde{\tilde{\mathrm{T}}}_{\mathrm{n}1} & \tilde{\tilde{\mathrm{T}}}_{\mathrm{n}2} & \cdots & 1 \end{pmatrix} = \begin{pmatrix} 1 & \tilde{\tilde{\mathrm{T}}}_{12} & \cdots & \tilde{\tilde{\mathrm{T}}}_{1\mathrm{n}} \\ \frac{1}{\tilde{\tilde{\mathrm{T}}}_{12}} & 1 & \cdots & \tilde{\tilde{\mathrm{T}}}_{2\mathrm{n}} \\ \vdots & \vdots & \vdots & \vdots \\ \frac{1}{\tilde{\tilde{\mathrm{T}}}_{1\mathrm{n}}} & \frac{1}{\tilde{\tilde{\mathrm{T}}}_{2\mathrm{n}}} & \cdots & 1 \end{pmatrix} \tag{1}$$

where

$$\frac{1}{\tilde{\tilde{\mathrm{T}}}_{\imath\jmath}} = \left(\left(\frac{1}{\mathrm{T}^{\mathrm{U}}_{\mathrm{ij}_4}}, \frac{1}{\mathrm{T}^{\mathrm{U}}_{\mathrm{ij}_3}}, \frac{1}{\mathrm{T}^{\mathrm{U}}_{\mathrm{ij}_2}}, \frac{1}{\mathrm{T}^{\mathrm{U}}_{\mathrm{ij}_1}}; \mathrm{H}_1\left(\tilde{\tilde{\mathrm{T}}}^{\mathrm{U}}_{\imath\jmath}\right), \mathrm{H}_2\left(\tilde{\tilde{\mathrm{T}}}^{\mathrm{U}}_{\imath\jmath}\right)\right), \left(\frac{1}{\mathrm{T}^{\mathrm{L}}_{\mathrm{ij}_4}}, \frac{1}{\mathrm{T}^{\mathrm{L}}_{\mathrm{ij}_3}}, \frac{1}{\mathrm{T}^{\mathrm{L}}_{\mathrm{ij}_2}}, \frac{1}{\mathrm{T}^{\mathrm{L}}_{\mathrm{ij}_1}}; \mathrm{H}_1\left(\tilde{\tilde{\mathrm{T}}}^{\mathrm{L}}_{\imath\jmath}\right), \mathrm{H}_2\left(\tilde{\tilde{\mathrm{T}}}^{\mathrm{L}}_{\imath\jmath}\right)\right)\right) \tag{2}$$

Step 3: Determine the Consistency Ratio (CR) related to each PC Matrix (PCM)
This step aids in the computation of constancy of PCMs resembles conventional AHP. If the outcome of PCM is steady, then IT2 PCM is reliable. If CR≤0.1, then consistency is acceptable. If CR>0.1, the sensor nodes are again estimated using the parameters of assessment.

Step 4: Compute Geometric Mean (GM)
In this step, the GM scheme is employed for aggregating the judgement score or neighbourhood recommendation provided by the sensor nodes. This GM computed for every row is computed using the Equation (3) and (4), with the fuzzy weights determined using normalization.

$$\tilde{\tilde{\mu}}_\imath = \left(\tilde{\tilde{\mathrm{T}}}_{\imath1} \otimes \tilde{\tilde{\mathrm{T}}}_{\imath2} \otimes \ldots \otimes \tilde{\tilde{\mathrm{T}}}_{\imath\mathrm{n}}\right)^{\frac{1}{\mathrm{n}}} \tag{3}$$

Where

$$\sqrt[\mathrm{n}]{\tilde{\tilde{\mathrm{T}}}_{\imath1}} = \begin{pmatrix} \left(\sqrt[\mathrm{n}]{\mathrm{T}^{\mathrm{U}}_{\mathrm{ij}_1}}, \sqrt[\mathrm{n}]{\mathrm{T}^{\mathrm{U}}_{\mathrm{ij}_2}}, \sqrt[\mathrm{n}]{\mathrm{T}^{\mathrm{U}}_{\mathrm{ij}_3}}, \sqrt[\mathrm{n}]{\mathrm{T}^{\mathrm{U}}_{\mathrm{ij}_4}}; \mathrm{H}_1\left(\tilde{\tilde{\mathrm{T}}}^{\mathrm{U}}_{\imath\jmath}\right), \mathrm{H}_2\left(\tilde{\tilde{\mathrm{T}}}^{\mathrm{U}}_{\imath\jmath}\right)\right), \\ \left(\sqrt[\mathrm{n}]{\mathrm{T}^{\mathrm{L}}_{\mathrm{ij}_1}}, \sqrt[\mathrm{n}]{\mathrm{T}^{\mathrm{L}}_{\mathrm{ij}_2}}, \sqrt[\mathrm{n}]{\mathrm{T}^{\mathrm{L}}_{\mathrm{ij}_3}}, \sqrt[\mathrm{n}]{\mathrm{T}^{\mathrm{L}}_{\mathrm{ij}_4}}; \mathrm{H}_1\left(\tilde{\tilde{\mathrm{T}}}^{\mathrm{L}}_{\imath\jmath}\right), \mathrm{H}_2\left(\tilde{\tilde{\mathrm{T}}}^{\mathrm{L}}_{\imath\jmath}\right)\right) \end{pmatrix} \tag{4}$$

Step 5: Determine Fuzzy Weights of every Criterion
In this step, the fuzzy weights associated with each criterion used for assessing the trust of neighbouring sensor nodes during the routing process is specified in Equation (5)

$$\tilde{\tilde{\mathrm{W}}}_\imath = \tilde{\tilde{\mu}}_\imath \otimes \left(\tilde{\tilde{\mu}}_1 \oplus \tilde{\tilde{\mu}}_2 \oplus \ldots \oplus \tilde{\tilde{\mu}}_\mathrm{n}\right)^{-1} \tag{5}$$

Step 6: De-Fuzzify IT2FS to Compute the Criteria Weights
In this step, a Trapezoidal T2FS is transformed into the value of Best Non-fuzzy Performance (BNP) for de-fuzzifying and ranking IT2FS (Kahraman et al. [35]) as specified in Equation (6)

$$\mathrm{De-fuzzified}\left(\tilde{\tilde{\mathrm{W}}}_\imath\right) = \frac{\left[\frac{(\mathrm{u_U}-\mathrm{l_U})+\left(\varphi_\mathrm{U}*m^1_U-\mathrm{l_U}\right)+\left(\vartheta_\mathrm{U}*m^2_U-\mathrm{l_U}\right)}{4}\right]+\mathrm{l_U}+\left[\frac{(\mathrm{u_L}-\mathrm{l_L})+\left(\varphi_\mathrm{L}*m^1_L-\mathrm{l_L}\right)+\left(\vartheta_\mathrm{L}*m^2_L-\mathrm{l_L}\right)}{4}+\mathrm{l_L}\right]}{2} \tag{6}$$

Step 7: Standardise Crisp Weights of every Criteria
In this step, the crisp weights associated for each criteria used for estimating the trust of sensor nodes are standardized using Equation (7)

$$\mathrm{W_i} = \frac{\mathrm{De-fuzzified}\left(\tilde{\tilde{\mathrm{W}}}_\imath\right)}{\sum_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{De-fuzzified}\left(\tilde{\tilde{\mathrm{W}}}_\imath\right)}, \quad \mathrm{i} = 1, \ldots, \mathrm{n} \tag{7}$$

COPRAS -G Method
MCDM is based on a situation wherein a decision maker has his choice amid alternatives by taking into consideration a specific set of conditions. In case of real-world applications, the values of the criteria may not be represented by precise numbers. Hence, multi-attributed DM problems should be operated with fuzzy or interval-based values. Zavadskas et.al

[36] have proposed Complex Proportional Assessment method with Grey interval numbers (COPRAS-G). This scheme with interval-based values of attribute depends on real conditions of DM and Grey systems theory applications. It uses a ranking method of substitutes based on their importance as well as utility degrees. The steps are listed below.

Step 1: Selection of criteria for evaluating the sensor nodes (alternatives)
In this step, the factors considered for evaluating the potential of the sensor nodes during the process of neighbour node discovery is determined. In this proposed scheme, the factors such as packet forwarding potential, energy possessed by each sensor node, distance between the sensor nodes, node degree and node centrality is considered as the criteria for evaluating the trust of sensor nodes.

Step 2: Constructing the Grey Decision Making (GDM) matrix '$\otimes\boldsymbol{G}$*'*
In this step, the Grey Decision Making (GDM) matrix '⊗G' is constructed using the number of sensor nodes under evaluation (represented in the rows), and the number of factors considered for evaluation (represented in the columns)

$$\otimes G = \begin{bmatrix} \otimes g_{11} & \cdots\cdots & \otimes g_{1m} \\ \otimes g_{21} & \cdots\cdots & \otimes g_{2m} \\ \vdots & \vdots \ \ddots & \vdots \\ \otimes g_{n1} & \cdots\cdots & \otimes g_{nm} \end{bmatrix} = \begin{bmatrix} \underline{g_{11}}; \overline{g_{11}} & \dots\dots & \underline{g_{1m}}; \overline{g_{1m}} \\ \underline{g_{21}}; \overline{g_{21}} & \cdots\cdots & \underline{g_{2m}}; \overline{g_{2m}} \\ \vdots & \vdots \ \ddots & \vdots \\ \underline{g_{n1}}; \overline{g_{n1}} & \cdots\cdots & \underline{g_{nm}}; \overline{g_{nm}} \end{bmatrix}; j = 1,2,\dots,n \ , \ i = 1,2,\dots,m \tag{8}$$

Where, m – number of criteria used for assessing the trust of sensor nodes, n – The number of sensor nodes under evaluation, $\otimes g_{ji}$ is found by $\underline{x_{ji}}$ (lower limit), $\overline{g_{ji}}$ (upper limit) - Score of alternate 'j' in terms of criterion (i)

In this step, the linguistic terms with the related grey numbers [33] for evaluating the sensor nodes as presented in **Table 2.**

Table 2. Grey Numbers Associated with The Linguistic Terms

Linguistic Variables	**Grey Numbers**
Very Good (VG)	[9, 10]
Good (G)	[6, 9]
Moderate Good (MG)	[5, 6]
Fair (F)	[4, 5]
Moderate Poor (MP)	[3, 4]
Poor (P)	[1, 3]
Very Poor (VP)	[0, 1]

Step 3: Normalization of GDM matrix$(\otimes\widetilde{\boldsymbol{G}})$.
In this step, the constructed normalized GDM matrix is constructed based on Equation (9)

$$\underline{\widetilde{g_{ji}}} = \frac{\underline{g_{ji}}}{\frac{1}{2}\left(\sum_{j=1}^{n}\underline{g_{ji}} + \sum_{j=1}^{n}\overline{g_{ji}}\right)}, \overline{\widetilde{g_{ji}}} = \frac{\overline{g_{ji}}}{\frac{1}{2}\left(\sum_{j=1}^{n}\underline{g_{ji}} + \sum_{j=1}^{n}\overline{g_{ji}}\right)} \tag{9}$$

The modified standardized GDM matrix is given by Equation (10)

$$\otimes\tilde{G} = \begin{bmatrix} \underline{\widetilde{g_{11}}}; \overline{\widetilde{g_{11}}} & \underline{\widetilde{g_{12}}}; \overline{\widetilde{g_{12}}} & \dots & \underline{\widetilde{g_{1m}}}; \overline{\widetilde{g_{1m}}} \\ \underline{\widetilde{g_{21}}}; \overline{\widetilde{g_{21}}} & \underline{\widetilde{g_{22}}}; \overline{\widetilde{g_{22}}} & \cdots & \underline{\widetilde{g_{2m}}}; \overline{\widetilde{g_{2m}}} \\ \vdots & \vdots & \ddots & \vdots \\ \underline{\widetilde{g_{n1}}}; \overline{\widetilde{g_{n1}}} & \underline{\widetilde{g_{n2}}}; \overline{\widetilde{g_{n2}}} & \cdots & \underline{\widetilde{g_{nm}}}; \overline{\widetilde{g_{nm}}} \end{bmatrix} \tag{10}$$

Step 4: Finding the Criteria Weights$(\boldsymbol{W_i})$
In this step, the comparative significance weight of every criterion used for estimating the trust of sensor nodes is computed using IT2F AHP.

Step 5: Determining the Weighted Standardized GDM Matrix$(\otimes \boldsymbol{\widehat{G}})$.

In this step, the weighted standardized GDM values are computed by multiplying the standardized DM with the weight vector of every criterion as specified in Equation (11)

$$\otimes \widehat{g_{ji}} = \otimes \widetilde{g_{ji}}.W_i;\text{ or }\underline{\widehat{g_{ji}}} = \underline{\widetilde{g_{ji}}}.W_i\text{ and }\overline{\widehat{g_{ji}}} = \overline{\widetilde{g_{ji}}}.W_i \tag{11}$$

At this juncture, the resultant weighted normalized GD matrix is constructed using Equation (12)

.

$$\otimes \widehat{G} = \begin{bmatrix} \otimes \widehat{g_{11}} & \otimes \widehat{g_{12}} & \cdots & \otimes \widehat{x_{1m}} \\ \otimes \widehat{g_{21}} & \otimes \widehat{g_{22}} & \cdots & \otimes \widehat{g_{2m}} \\ \vdots & \vdots & \ddots & \vdots \\ \otimes \widehat{g_{n1}} & \otimes \widehat{g_{n2}} & \cdots & \otimes \widehat{g_{nm}} \end{bmatrix} = \begin{bmatrix} \underline{\widehat{g_{11}}};\overline{\widehat{g_{11}}} & \underline{\widehat{g_{12}}};\overline{\widehat{g_{12}}} & \ldots & \underline{\widehat{g_{1m}}};\overline{\widehat{g_{1m}}} \\ \underline{\widehat{g_{21}}};\overline{\widehat{g_{21}}} & \underline{\widehat{g_{22}}};\overline{\widehat{g_{22}}} & \cdots & \underline{\widehat{g_{2m}}};\overline{\widehat{g_{2m}}} \\ \vdots & \vdots & \ddots & \vdots \\ \underline{\widehat{g_{n1}}};\overline{\widehat{g_{n1}}} & \underline{\widehat{g_{n2}}};\overline{\widehat{g_{n2}}} & \cdots & \underline{\widehat{g_{nm}}};\overline{\widehat{g_{nm}}} \end{bmatrix} \tag{12}$$

Step 6: Determination of comparative significance related to each sensor nodes

In this step, determine the comparative significance of each sensor nodes by estimating the total value of 'P_j' (greater values) and R_j (lesser values) for every criterion values.

$$P_j = \tfrac{1}{2}\textstyle\sum_{i=1}^{k}\left(\underline{\widehat{g_{ji}}} + \overline{\widehat{g_{ji}}}\right) \quad j = 1,2,\ldots,n; \quad i = 1,2,\ldots,q \tag{13}$$

$$R_j = \tfrac{1}{2}\textstyle\sum_{i=k+1}^{m}\left(\underline{\widehat{g_{ji}}} + \overline{\widehat{g_{ji}}}\right) \quad j = 1,2,\ldots,n; \quad i = q+1,q+2,\ldots,m \tag{14}$$

Step 7: Identification of lower value of '$\boldsymbol{R_j}$*'.*

In this step, the lowest value for 'R_j' is identified for confirming the reliability attributed by each sensor nodes during the routing process as specified in Equation (15)

$$R_j = \min_j R_j \tag{15}$$

Step 8: Determine the relative significance of each sensor node

In this step, the . relative significance of each sensor node [34] with respect to other nodes under evaluation is achieved based on Equation (16)

$$Q_j = P_j + \frac{\sum_{j=1}^{n} R_j}{R_j \sum_{j=1}^{n} \frac{1}{R_j}} \tag{16}$$

Step 9: Estimation of utility degree

In this step, the utility degree related to each sensor node (N_j) is estimated for finding the trusted alternative (K) [37-38] using Equation (17)

$$K = \max_j Q_j \tag{17}$$

This utility degree of each sensor nodes permits the comparison with idyllic alternates. It ranges from 0% (worst alternate) to 100% (best alternate) as specified in Equation (18)

$$N_j = \frac{Q_j}{Q_{max}} x100\% \tag{18}$$

IV. SIMULATION RESULTS AND DISCUSSION

The performance of the propounded FAHPCG is compared with the standard AF-TNS, NADEEM and ESRT schemes based on the simulation performed using ns-2.34 simulator[37][38].

Comparative Investigation of the proposed FAHPCG using different neighboring sensor nodes

In this initial part of comparative investigation, the performance of the proposed FAHPCG and the baseline AF-TNS, NADEEM and ESRT schemes are compared based on neighbour discovery rate, packet delivery rate, end-to-end delay, and energy consumption under different neighbouring sensor nodes. **Fig 1** and **2** presents the plots of neighbour discovery rate and packet delivery rate achieved by the proposed FAHPCG scheme and the baseline AF-TNS, NADEEM and ESRT schemes under different neighbouring sensor nodes. The neighbour discovery rate of the proposed FAHPCG scheme is identified to be improved over the benchmarked schemes, since it adopted the benefits of fuzzy theory for handling uncertainty in node behaviour and COPRAS-G for estimating the trust of sensor nodes. It also adopted the merits of AHP for exploring the possible dimensions of factors which attributes towards trusted neighbour sensor node discovery. At the same time, packet delivery rate achieved by the proposed FAHPCG scheme is determined to be comparatively better than the baseline AF-TNS, NADEEM and ESRT schemes under different neighbouring sensor nodes, since it normalized the score of trust with respect to possible criteria using the merits of grey theory. Thus, the proposed FAHPCG scheme under different neighbouring sensor nodes improved the rate of neighbour node discovery by 16.21%, 19.32%, 22.39%, and 24.68%, better than the benchmarked AF-TNS, NADEEM and ESRT approaches. Moreover, PDR attained by the proposed FAHPCG scheme under different neighbouring sensor nodes is improved by 17.82%, 20.64%, 22.83%, and 25.12%, better than the benchmarked AF-TNS, NADEEM and ESRT approaches.

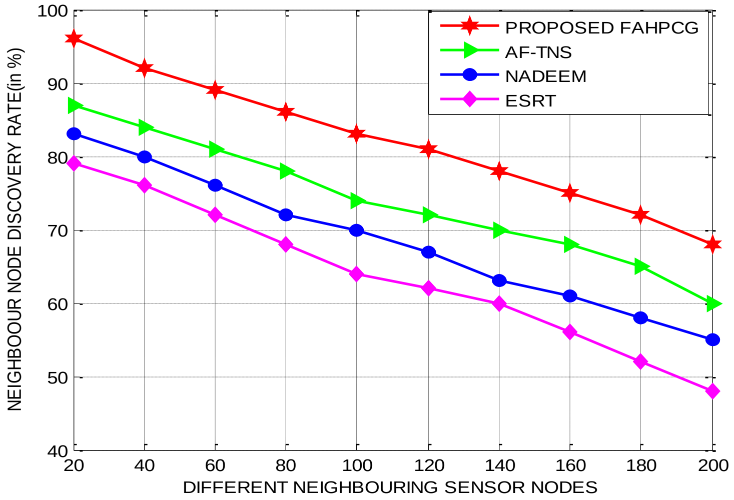

Fig 1. Proposed FAHPCG-Neighbour Node Discovery Under Different Neighbouring Sensor Nodes

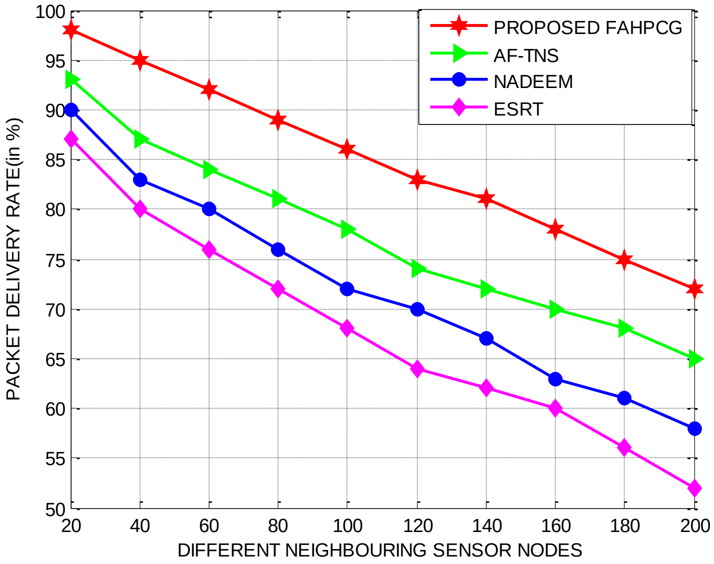

Fig 2. Proposed FAHPCG-PDR Under Different Neighbouring Sensor Nodes

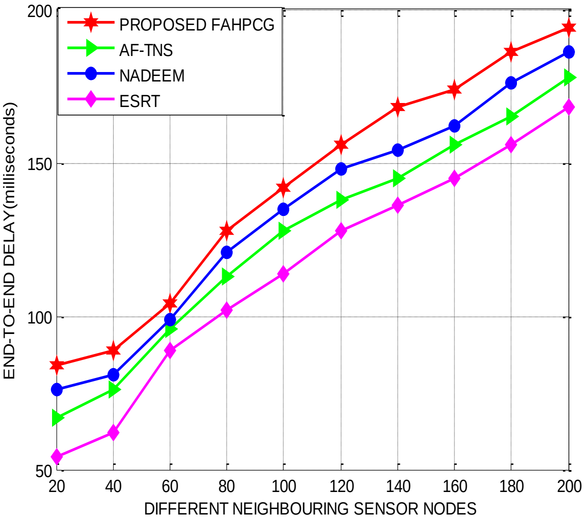

Fig 3. Proposed FAHPCG-End-To-End Delay Under Different Neighbouring Sensor Nodes

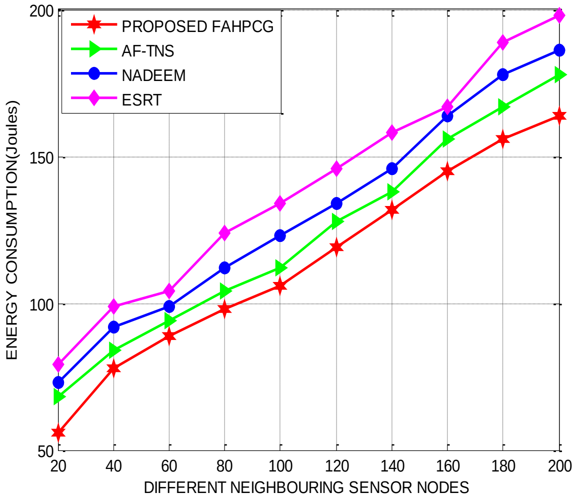

Fig 4. Proposed FAHPCG-Energy Consumption Under Different Neighbouring Sensor Nodes

Fig 3 and **Fig 4** demonstrates the plots of end-to-end delay, and energy consumption incurred by the proposed FAHPCG scheme and the baseline AF-TNS, NADEEM and ESRT schemes under different neighbouring sensor nodes. The proposed FAHPCG scheme minimizes the end-to-end delay comparatively better than the benchmarked schemes, since it hybridized grey theory and COPRAS for handling the uncertainty of information exchanged between the sensor nodes, and multi-attribute exploration adopted during the process of trust estimation. Likewise, the proposed FAHPCG scheme reduced the energy utilization on par with the baseline approaches as it prevented maximized probability of packet retransmission during the process of data dissemination through the inclusion of COPRAS-G. It also adopted the merits of interval-based values related to the attribute depending on real conditions of DM and Grey systems theory applications. It also used a ranking method of sensor nodes based on their importance as well as utility degrees. Thus, the proposed FAHPCG scheme under different neighbouring sensor nodes minimized the end-to-end delay incurred by 15.64%, 18.52%, 20.96%, and 22.19%, better than the benchmarked AF-TNS, NADEEM and ESRT approaches. Moreover, energy utilized by the proposed FAHPCG scheme under different neighbouring sensor nodes is reduced by 14.52%, 16.98%, 19.41%, and 22.91%, better than the benchmarked AF-TNS, NADEEM and ESRT approaches.

Comparative Investigation of the proposed FAHPCG using different neighboring malicious nodes

In this second part of comparative investigation, the performance of the proposed FAHPCG and the baseline AF-TNS, NADEEM and ESRT schemes are compared based on throughput, detection rate, neighbour node discovery rate, and packet latency under different neighbouring malicious nodes. **Fig 5** and **Fig 6** presents the plots of throughput and detection rate achieved by the proposed FAHPCG scheme and the baseline AF-TNS, NADEEM and ESRT schemes under different neighbouring malicious nodes. Thus, the proposed FAHPCG scheme under different neighbouring malicious nodes improved the throughput by 15.42%, 17.69%, 19.56%, and 22.38%, better than the benchmarked AF-TNS, NADEEM and ESRT approaches. Moreover, detection rate achieved by the proposed FAHPCG scheme under different neighbouring malicious nodes is improved by 16.34%, 18.92%, 20.98%, and 22.61%, better than the benchmarked AF-TNS, NADEEM and ESRT approaches.

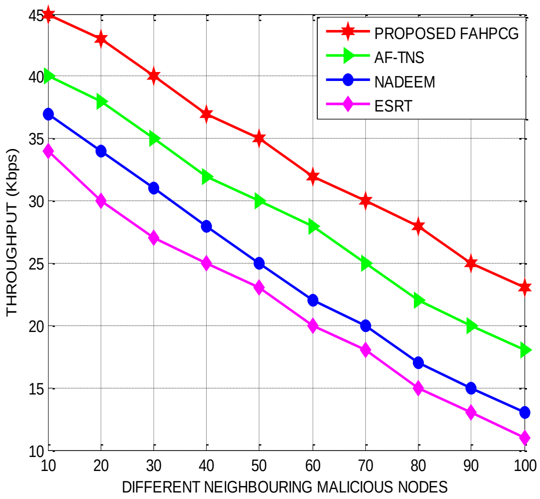

Fig 5. Proposed FAHPCG-Throughput Under Different Neighbouring Malicious Sensor Nodes

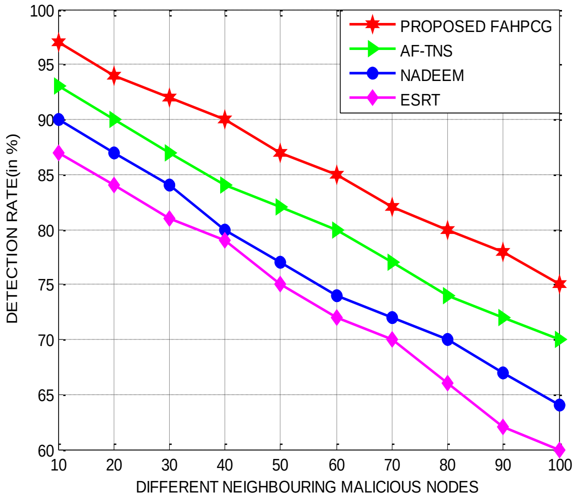

Fig 6. Proposed FAHPCG-Detection Rate Under Different Neighbouring Malicious Sensor Nodes

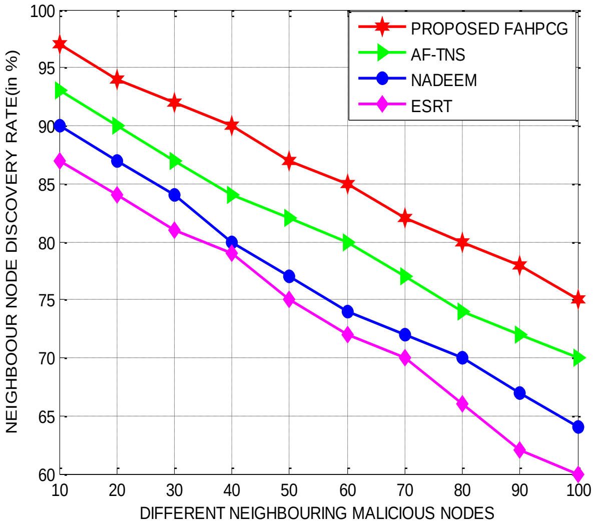

Fig 7. Proposed FAHPCG- Neighbour Node Discovery Rate Under Different Neighbouring Malicious Sensor Nodes

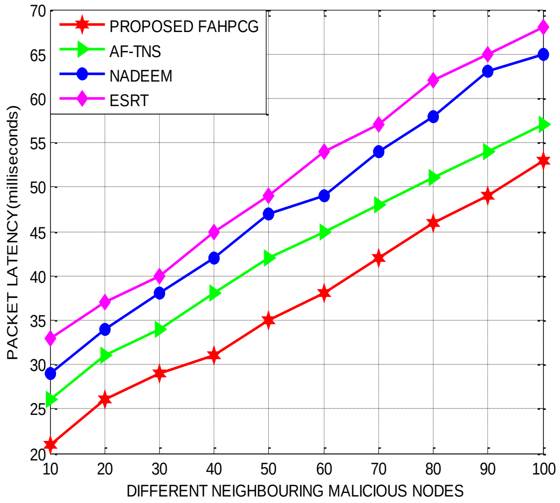

Fig 8. Proposed FAHPCG- Packet Latency Under Different Neighbouring Malicious Sensor Nodes

Fig 7 and **Fig 8** presents the plots of neighbour node discovery rate and packet latency achieved by the proposed FAHPCG scheme and the baseline AF-TNS, NADEEM and ESRT schemes under different neighbouring malicious sensor nodes. Thus, the proposed FAHPCG scheme under different neighbouring sensor nodes improved the rate of neighbour node discovery by 17.42%, 19.98%, 21.54%, and 23.88%, better than the benchmarked AF-TNS, NADEEM and ESRT approaches. Moreover, packet latency incurred by the proposed FAHPCG scheme under different neighbouring malicious sensor nodes is improved by 14.38%, 17.83%, 19.62%, and 22.86%, better than the benchmarked AF-TNS, NADEEM and ESRT approaches.

Performance Evaluation of the proposed FAHPCG based on neighbouring selfish sensor node

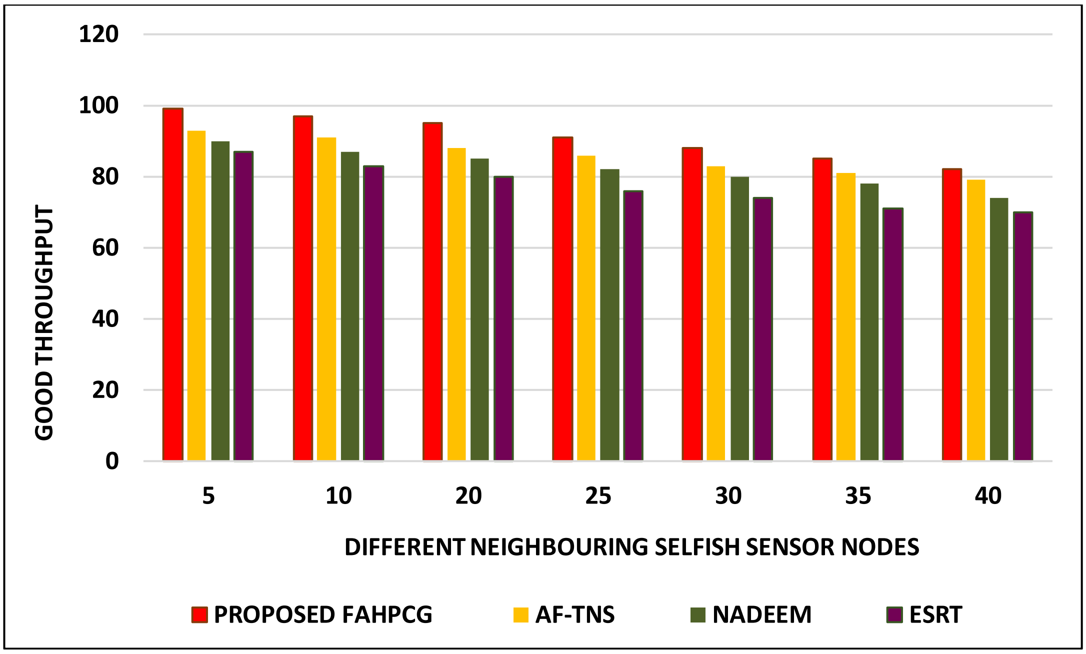

Fig 9. Proposed FAHPCG- Packet Latency Under Different Neighbouring Selfish Sensor Nodes

In this final part of comparative investigation, the performance of the proposed FAHPCG and the baseline AF-TNS, NADEEM and ESRT schemes are compared based on good throughput and neighbour node discovery rate under different neighbouring selfish nodes. **Fig 9** presents the good throughput achieved by the proposed FAHPCG scheme and the baseline AF-TNS, NADEEM and ESRT schemes under different neighbouring selfish sensor nodes. Thus, the proposed FAHPCG scheme under different neighbouring selfish sensor nodes improved the good throughput by 17.42%, 19.98%, 21.54%, and 23.88%, better than the benchmarked AF-TNS, NADEEM and ESRT approaches.

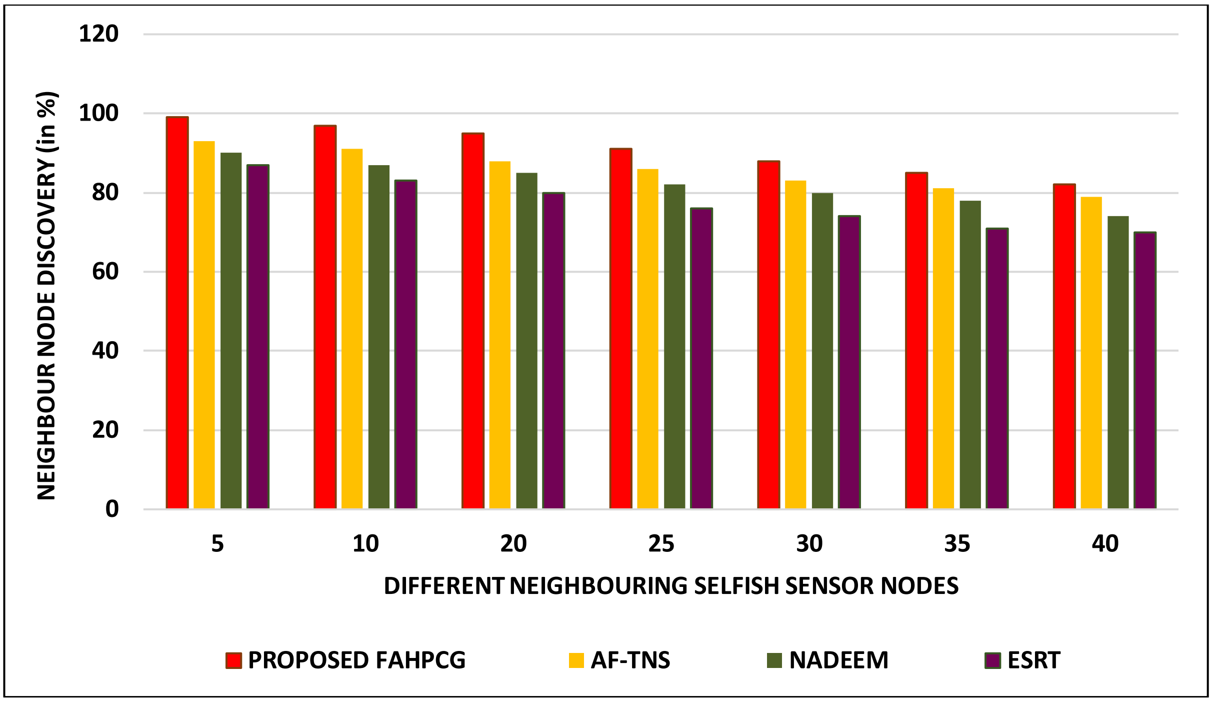

Fig 10. Proposed FAHPCG- Neighbouring Node Discovery Rate Under Different Neighbouring Selfish Sensor Nodes

In addition, **Fig 10** presents the neighbouring node discovery rate achieved by the proposed FAHPCG scheme and the baseline AF-TNS, NADEEM and ESRT schemes under different neighbouring selfish sensor nodes. Moreover, the neighbouring node discovery rate attained by the proposed FAHPCG scheme under different neighbouring selfish sensor nodes is improved by 14.38%, 17.83%, 19.62%, and 22.86%, better than the benchmarked AF-TNS, NADEEM and ESRT approaches.

V. CONCLUSION

The proposed FAHPCG scheme achieved reliable dissemination using trusted neighbouring node discovery using the advantages of Interval Type 2 Fuzzy AHP and Grey COPRAS method. It determined the weight of the evaluation criteria during neighbour node discovery based on Interval Type 2 Fuzzy AHP. At the same time, it achieved the prioritization of the sensor nodes of the routing path established between the source and destination using COPRAS-G. It adopted fuzzy theory for handling the uncertainty and vagueness involved in the change in the behavior of sensor nodes during the process of neighbour discovery**.** It explored maximized number of factors that aids in exploring the possible dimensions of sensor nodes packet forwarding potential during the process of neighbour node discovery. The simulation results of the proposed FAHPCG scheme confirmed an improved neighbour node discovery rate of 23.18% and prolonged the sensor nodes lifetime to the maximum of 7.12 times better than the baseline approaches used for investigation. As the part of future scope, it is planned to formulate and implement a Hybrid TOPSIS and COPRAS-based neighbour node discovery scheme and compare it with the proposed FAHPCG scheme.

Data Availability

No data was used to support this study.

Conflicts of Interests

The author(s) declare(s) that they have no conflicts of interest.

Funding

No funding was received to assist with the preparation of this manuscript.

Ethics Approval and Consent to Participate

The research has consent for Ethical Approval and Consent to participate.

Competing Interests

There are no competing interests.

References

[1]. Zhang, P., Wang, S., Guo, K., & Wang, J. (2018). A secure data collection scheme based on compressive sensing in wireless sensor networks. Ad Hoc Networks, 70, 73-84.

[2]. Merad Boudia, O. R., Senouci, S. M., & Feham, M. (2018). Secure and efficient verification for data aggregation in wireless sensor networks. *International Journal of Network Management*, *28*(1), e2000.

[3]. Wang, J., & Chen, Y. (2018). Research and improvement of wireless sensor network secure data aggregation protocol based on SMART. *International Journal of Wireless Information Networks*, *25*(3), 232-240.

[4]. Janakiraman, S., & Jayasingh, B. B. (2019). A hyper-exponential factor-based Semi-Markov prediction mechanism for selfish rendezvous nodes in MANETs. Wireless Personal Communications, 108(3), 1493-1511.

[5]. Tolba, A. (2017). Organizing multipath routing in cloud computing environments. *International Journal of Advanced Computer Science and Applications*, *8*(1).

[6]. Stoleru, R., Wu, H., & Chenji, H. (2012). Secure neighbor discovery and wormhole localization in sensor ad hoc networks. *Ad Hoc Networks*, *10*(7), 1179-1190.

[7]. Janakiraman, S., Priya, M. D., & Jebamalar, A. C. (2021). Integrated context-based mitigation framework for enforcing security against rendezvous point attack in MANETs. Wireless Personal Communications, 119(3), 2147-2163.

[8]. Kumar, G., Rai, M. K., & Saha, R. (2017). Securing range free localization against wormhole attack using distance estimation and maximum likelihood estimation in wireless sensor networks. *Journal of Network and Computer Applications*, *99*, 10-16.

[9]. Malik, S. K., Dave, M., Dhurandher, S. K., Woungang, I., & Barolli, L. (2017). An ant-based QoS-aware routing protocol for heterogeneous wireless sensor networks. *Soft computing*, *21*(21), 6225-6236.

[10]. Sengathir, J., & Manoharan, R. (2016). Exponential reliability factor based mitigation mechanism for selfish nodes in MANETs. Journal of Engineering Research, 4, 1-22.

[11]. Ahmed, A. M., Kong, X., Liu, L., Xia, F., Abolfazli, S., Sanaei, Z., & Tolba, A. (2017). BoDMaS: bio-inspired selfishness detection and mitigation in data management for ad-hoc social networks. *Ad Hoc Networks*, *55*, 119-131.

[12]. Usman, A. B., & Gutierrez, J. (2018). Trust-based analytical models for secure wireless sensor networks. In *Security and Privacy Management, Techniques, and Protocols* (pp. 47-65). IGI Global.

[13]. Janakiraman, S., & Priya, M. D. (2022). Selfish node detection scheme based on bates distribution inspired trust factor for MANETs. EAI Endorsed Transactions on Energy Web, 9(6), e1-e1.

[14]. Xia, F., Liaqat, H. B., Ahmed, A. M., Liu, L., Ma, J., Huang, R., & Tolba, A. (2016). User popularity-based packet scheduling for congestion control in ad-hoc social networks. *Journal of Computer and System Sciences*, *82*(1), 93-112.

[15]. Sengathir, J., & Manoharan, R. (2017). Co-operation enforcing reputation-based detection techniques and frameworks for handling selfish node behaviour in MANETs: A review. Wireless Personal Communications, 97, 3427-3447.

[16]. Ahmed, A., Bakar, K. A., Channa, M. I., & Khan, A. W. (2016). A secure routing protocol with trust and energy awareness for wireless sensor network. Sensor Networks and Applications, 21(2), 272-285

[17]. Karthik, N., & Ananthanarayana, V. S. (2017). A hybrid trust management scheme for wireless sensor networks. Wireless Personal Communications, 97(4), 5137-5170.

[18]. Ahmed, A., Bakar, K. A., Channa, M. I., Khan, A. W., & Haseeb, K. (2017). Energy-aware and secure routing with trust for disaster response wireless sensor network. Peer-to-Peer Networking and Applications, 10(1), 216-237.

[19]. AlFarraj, O., AlZubi, A., & Tolba, A. (2018). Trust-based neighbor selection using activation function for secure routing in wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 1-11.

[20]. Javaid, N. (2019). NADEEM: Neighbor node approaching distinct energy-efficient mates for reliable data delivery in underwater WSNs. Transactions on Emerging Telecommunications Technologies, e3805.

[21]. Zhao, J., Huang, J., & Xiong, N. (2019). An effective exponential-based trust and reputation evaluation system in wireless sensor networks. IEEE Access, 7, 33859-33869.

[22]. Anwar, R. W., Zainal, A., Outay, F., Yasar, A., & Iqbal, S. (2019). BTEM: Belief based trust evaluation mechanism for wireless sensor networks. Future generation computer systems, 96, 605-616.

[23]. Gautam, A. K., & Kumar, R. (2021). 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), 14(4), 1336-135

[24]. Das, R., & Dwivedi, M. (2022). Multi agent dynamic weight based cluster trust estimation for hierarchical wireless sensor networks. Peer-to-Peer Networking and Applications, 15(3), 1505-1520.

[25]. Mendel, J. M., John, R. I., & Liu, F. (2006). Interval type-2 fuzzy logic systems made simple. *IEEE transactions on fuzzy systems*, *14*(6), 808-821.

[26]. Zadeh, L. A. (1975). The concept of a linguistic variable and its application to approximate reasoning—I. *Information sciences*, *8*(3), 199-249.

[27]. Liang, Q., & Mendel, J. M. (2000). Interval type-2 fuzzy logic systems: theory and design. *IEEE Transactions on Fuzzy systems*, *8*(5), 535-550.

[28]. Saaty, T. L. (1977). A scaling method for priorities in hierarchical structures. Journal of mathematical psychology, 15(3), 234-281.

[29]. Bevilacqua, M., Ciarapica, F. E., & Giacchetta, G. (2006). A fuzzy-QFD approach to supplier selection. Journal of Purchasing and Supply Management, 12(1), 14-27.

[30]. Zadeh LA (1965) Fuzzy sets. Information and control 8(3): 338-353.

[31]. Wang TC, Chen YH (2008) Applying fuzzy linguistic preference relations to the improvement of consistency of fuzzy AHP. Information sciences 178(19): 3755-3765.

[32]. Van Laarhoven, P. J., & Pedrycz, W. (1983). A fuzzy extension of Saaty's priority theory. *Fuzzy sets and Systems*, *11*(1-3), 229-241.

[33]. Buckley JJ (1985) Fuzzy hierarchical analysis. Fuzzy sets and systems 17(3): 233-247.

[34]. Chang, D. Y. (1996). Applications of the extent analysis method on fuzzy AHP. *European journal of operational research*, *95*(3), 649-655.

[35]. Kahraman, C., Öztayşi, B., Sarı, İ. U., & Turanoğlu, E. (2014). Fuzzy analytic hierarchy process with interval type-2 fuzzy sets. *Knowledge-Based Systems*, *59*, 48-57.

[36]. Zavadskas, E. K., Kaklauskas, A., Turskis, Z., & Tamošaitienė, J. (2009). Multi-attribute decision-making model by applying grey numbers. *Informatica*, *20*(2), 305-320.

[37]. Tavana, M., Momeni, E., Rezaeiniya, N., Mirhedayatian, S. M., & Rezaeiniya, H. (2013). A novel hybrid social media platform selection model using fuzzy ANP and COPRAS-G. *Expert Systems with Applications*, *40*(14), 5694-5702.

[38]. Li, G. D., Yamaguchi, D., & Nagai, M. (2007). A grey-based decision-making approach to the supplier selection problem. *Mathematical and computer modelling*, *46*(3-4), 573-581.