International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7705
***Article Received:** 12 June 2023 **Revised:** 28 July 2023 **Accepted:** 11 August 2023*

Fuzzy TOPSIS-based Secure Neighbor Discovery Mechanism for Improving Reliable Data Dissemination in Wireless Sensor Networks

E. Jyothi Kiranmayi[1], Dr. N. V. Rao[2], Dr. K. S. Nayanatara[3]
[1]Computer Science Engineering
SVD Goverment Degree College (W)
Nidadavole, INDIA
jkiranmayi1@gmail.com
[2]Computer Science Engineering
CVR College of Engineering
Hyderabad, INDIA
[3]Electronics and Comminication Engineering
CVR College of Engineering
Hyderabad, INDIA

Abstract—Wireless Sensor Networks (WSNs) being an indispensable entity of the Internet of Things (IoT) are found to be more and more widely utilized for the rapid advent of IoT environment. The reliability of data dissemination in the IoT environment completely depends on the secure neighbor discovery mechanism that are utilized for effective and efficient communication among the sensor nodes. Secure neighbor discovery mechanisms that significantly determine trustworthy sensor nodes are essential for maintaining potential connectivity and sustaining reliable data delivery in the energy-constrained self organizing WSN. In this paper, Fuzzy Technique of Order Preference Similarity to the Ideal Solution (TOPSIS)-based Secure Neighbor Discovery Mechanism (FTOPSIS-SNDM) is proposed for estimating the trust of each sensor node in the established routing path for the objective of enhancing reliable data delivery in WSNs. This proposed FTOPSIS-SNDM is proposed as an attempt to integrate the merits of Fuzzy Set Theory (FST) and TOPSIS-based Multi-criteria Decision Making (MCDM) approach, since the discovery of secure neighbors involves the exchange of imprecise data and uncertain behavior of sensor nodes. This secure neighbor is also influenced by the factors of packet forwarding potential, delay, distance from the Base Station (BS) and residual energy, which in turn depends on multiple constraints that could be possibly included into the process of secure neighbor discovery. The simulation investigations of the proposed FTOPSIS-SNDM confirmed its predominance over the benchmarked approaches in terms of throughput, energy consumption, network latency, communication overhead for varying number of genuine and malicious neighboring sensor nodes in network.

Keywords- Wireless Sensor Network (WSN); Secure Neighbor Discovery; Fuzzy Set Theory (FST); Multi criteria Decision Making (MCDM); Technique of Order Preference Similarity to the Ideal Solution (TOPSIS);

I. INTRODUCTION

Wireless Sensor Network (WSN) is a group of closely packed nodes which are positioned arbitrarily to observe ecological variations. The primary purpose of nodes is to examine the ecological changes, observe and transfer them to Base Station (BS) or sink. The nodes are armed with processing units and battery for carrying out these functions [1]. Owing to deficiency of placement areas, the networks face challenges like attaining energy efficiency and choice of neighbor. The nodes are positioned in remote areas which are unreachable, and revitalizing these devices sporadically is unfeasible. The network is resource-restricted, stopping the nodes from adapting based on the application demands [2]. The deployment area is chosen randomly, and it is expected that the nodes acclimate with the neighboring nodes. In case the sink is distant from the transmitter, it transmits information by involving the existing neighbors. The node hopes that its neighbor would forward information; else it has no option. Nodes positioned in the region of an opponent are open to susceptibility like being compromised or injection of bogus information. Nodes which are impacted by an exterior threat cannot be considered as good nodes which offer precise sensed data[3-4]. Discovery of neighbors is essential for routing protocols used, wherein neighbors are instant nodes which are seen in the transmitter's region. The nodes which are a hop away are said to be direct neighbors.

The neighbors help the transmitter in discovering network through several paths [5]. Exterior attackers execute activities on neighboring nodes to mislead, forge as well as alter transmission of information [6]. The transmitted data is open to vulnerability owing to multi-hop distance amid source and sink. A secure

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7705
***Article Received:** 12 June 2023 **Revised:** 28 July 2023 **Accepted:** 11 August 2023*

routing protocol is essential for multi-hop networks to stop data from being retrieved by external nodes. An optimal routing mechanism should enable reasonable choice of neighbors, continuous communication and reduced routing overhead [7]. Neighbor selection based on trust is the currently used method to authenticate neighbors depending on the performance which ensures improved consistency and confidentiality during transmission of data. Trust shows the reliability a node obtains depending on its actions. Reliable neighbor selection is essential for every protocol [8].

Secure protocols designed for routing guarantee security at the network layer for protection from attacks except node misbehavior attacks. Authentication schemes and cryptography are unsuitable for dealing with misbehavior attacks. The development of trust as well as reputation-dependent security mechanisms is resilient to behavioral attacks. In case of trust-based security mechanisms, the node activities are forecast depending on the former observations. The level of trust is calculated for a node over accepted time slots to regulate the possibility of it to partake in routing as well as transmission [9-10]. These models are expected to offer safe associations amid nodes by determining the standing over a specific period of time. Sporadic reputation handling is compromised in highly populated networks owing to recurrent exchanges of information related to updates. Some protocols emphasis on choosing specific safe neighbor regardless of the nodes with resource restrictions. This leads to quick energy depletion of the chosen nodes. Further, alternative category of protocols interchange huge information sequences to maintain trust updates. This causes inclusion of false information by assailants to minimalize the node's trust [11]. In a huge network, the transmitter is not capable of choosing suitable communication pair depending on trust. In case a neighbor is chosen without any intent, the node's reliability may not be guaranteed. This demands nodes' shared collaboration [12-14]. Owing to the lack of trust in a network, the network life span is reduced thus affecting the whole process of transmission. Moreover, diversified number of trust-based neighbour discovery mechanisms was contributed to the literature for thwarting malicious behavior of mobile nodes which aids in achieving reliable data dissemination amid source and sink nodes of network. In specific, MCDM making approaches are considered to be ideal in assessing the trust of sensor nodes during the process of trusted node neighbor discovery initiated along the routing path of the network.

In this paper, Fuzzy Technique of Order Preference Similarity to the Ideal Solution (TOPSIS)-based Secure Neighbor Discovery Mechanism (FTOPSIS-SNDM) is proposed for estimating the trust of each sensor node in the established routing path for the objective of enhancing reliable data delivery in WSNs. This proposed FTOPSIS-SNDM is proposed as an attempt to integrate the merits of Fuzzy Set Theory (FST) and TOPSIS-based Multi-criteria Decision Making (MCDM) approach, since the discovery of secure neighbors involves the exchange of imprecise data and uncertain behavior of sensor nodes. This secure neighbor is also influenced by the factors of packet forwarding potential, delay, distance from the BS and residual energy, which in turn depends on multiple constraints that could be possibly included into the process of secure neighbor discovery. The experiments of proposed FTOPSIS-SNDM show its predominance over the benchmarked approaches in terms of throughput, amount of energy consumed, network latency, communication overhead for varying number of genuine and malicious neighboring nodes in the network.

The remaining sections of the paper is organized as follows. Section 2 shows the complete review of the trust-based neighbour node discovery mechanisms contributed to the literature over the recent years with pros and cons. Section 3 presents the detailed view of the proposed FTOPSIS-SNDM scheme with its indispensable role in neighbour node discovery during the process of routing in the network. Section 4 shows the simulation results and discussion of the proposed FTOPSIS-SNDM scheme with respect to throughput, trusted neighbour node discovery rate, energy consumption and packet delay for varying amount of nodes and malevolent neighbour nodes. Section 5 shows the conclusion with main contributions of proposed work and scope of future improvement.

II. EXISTING WORK

AlFarraj et al. [15] proposed a Trusted Neighbor Selection approach using the merits of Activation Function (TNSAF) for better packet delivery between the source and destination sensor nodes in WSNs. It functions in 2stages, trust assessment with energy restraint and node assessment based on added metric that facilitates maintaining the reliability of neighbors. It identifies the reliable and non-reliable nodes by efficient decision making process, employing sequential activation and arbitrary transigmoid functions that retain network performance. It offers better malevolent detection rate with reduced delay, and increased throughput and network lifespan. Khalid et al. [16] have designed Adaptive Trust-based Routing Protocol (ATRP) which includes direct, indirect along with witness trusts which is based on factors including resources as well as security in the trustworthiness involving pair wise comparison. It employs MCDM, wherein trust metrics are recognized based on varying network performance leading to improved decision as several uncertainty features are taken into consideration. By considering the resources, the necessity for retransmission is highly reduced. Based on the amount of interactions, the impact of flooding on the network is also lessened. The decision offered by the lower layer assessors dropped higher layer assessor's task, thus permitting them to persist for a longer time. Multi-hop

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7705
***Article Received:** 12 June 2023 **Revised:** 28 July 2023 **Accepted:** 11 August 2023*

assessments assist in making improved decisions as the assessor has a larger vision of the network. It performs further assessments on efficient nodes at numerous hops which aids to balancing energy consumption and prolonging network lifespan. It involves assessments at several layers instead of single hop assessments. The factors considered balance load distribution and offers more precise choice of succeeding forwarder. It offers prolonged lifespan, reduced delay, packet loss and energy consumption in contrast to present protocols.

Yang et al. [17] have designed a trusted mechanism for routing by using block chain as well as Reinforcement Learning (RL) that focuses on offering security as well as efficacy. The routing scheme stores the routing information of nodes on Block chain using token transactions that makes routing information observable and difficult to tamper. This distributed information organization platform offers distributed, tamper-resistant and observable features of block chain transactions that improves reliability of routing information. RL is used to study the dynamic, consistent and increased routing information from block chain and dynamically choose trusted as well as effectual links. Even with nearly 50% malevolent nodes, the routing mechanism offers better performance involving reduced delay and energy consumption, and improved throughput. Renjith[18] have proposed ANFIS based Trust Evaluation (ATE) routing protocol by employing ANFIS and NN. It offers improved lifetime and trusted data forwarding. It reduces the computational complexity and offers improved network lifespan. Including trust into ANFIS enhances security and enables choosing effective routing paths for rapid forwarding of data. Trust restricts malevolent nodes from entering into the cluster. From the simulation outcomes, it is evident that Trust-Aware data Aggregation (TAA) Protocol along with ANFIS performs better when compared to the present TRAF and ETARP protocols.

Abd El-Moghithand Darwish [19] have designed a trusted mechanism for routing which includes deep block chain along with Markov Decision Processes (MDPs) to support safe routing. To validate transmission, the proposed scheme uses Proof of Authority (PoA) in blockchain network. Blockchain token represents packet routing, and every transaction is confirmed by validators before being disseminated to blockchain network. The authentication group essential for proofing is chosen using Deep Learning (DL) method which emphases on node properties. MDPs are used in selecting the appropriate next hop node that is proficient in securely transmitting messages. Every transaction tracker becomes observable and tamper-resilient, nodes are capable of monitoring dynamic as well as reliable routing information on a blockchain network. Based on testing data, routing system offers better performance even in the presence of more than half of malevolent nodes in contrast to present routing algorithms. This MDP model ensures quick route discovery and evades links to hostile nodes. It is efficient in eliminating hostile attacks involving reduced latency. Hajiee et al. [20] have proposed an energy and trust-based routing scheme by using learning automata as well as assessment function. Learning automata finds trusted and malevolent nodes by using the conforming assessment function. The assessment function is based on remaining energy, node's reliability and amount of hops to sink factors for assessing the node when compared to threshold. Data reaches the destination safely and reliably. To get the value of trust in the assessment function, direct and indirect trusts of every node are computed. The assessment outcomes of proposed scheme show improved performance based on throughput, lifespan, mean end-to-end delay and standardized routing load in contrast to existing schemes. random to ensure improved performance of the filtering scheme against neighbors. In addition, Sajan et al [22] have proposed Three-Level Weighted Trust evaluation-based Grey Wolf Optimization (3LWT-GWO) scheme for efficient identification of fake nodes and offering ideal paths through reliable nodes for distributing data safely to the destination. It is classified into 3 stages namely, trust-dependent clustering, CH selection and ideal routing. Clustering is performed initially by calculating Overall Trust Score (OTS) for every node depending on parameters including energy, direct, indirect, Long-term neighbor reference, authentication and link quality trusts. It aids in identifying insecure nodes after which clustering is John and Deepa [21] have proposed Recommendation Filtering based Trust Model (RFTM) for safeguarding the path amid source and sink by removing fraudulent malevolent nodes. It removes the dishonest endorsements that are given by malevolent neighbours. It is a challenge owing to attacks including ballot as well as bad mouthing. The issues due to malevolent node while transmitting trust information in prevailing trust models are detailed. It employs an Artificial Intelligence (AI)-based Dempster Shafer theory along with deviation test schemes for avoiding fake recommendations from trust assessment. The proposed scheme offers improved throughput and Packet Delivery Ratio (PDR). Nodes are chosen at done. The node's weight is computed depending on the remaining energy, node distance as well as energy, and one with maximum weight is selected as CH. Ideal routing is done depending on GWO algorithm by determining the energy, distance, trust satisfactory degree as well as delay. Depending on the identified path, packets are delivered to the destination. The proposed scheme involves less energy and delay, offering improved throughput, accuracy, lifespan and detection rate.

In addition, Table 1 which presents the consolidated summary of the existing works contributed to the literature with the pros and cons.The mentioned limitations in Table 1 motivated the option of formulating, implementing and evaluating the potentiality of the proposed Fuzzy Technique of

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7705
***Article Received:** 12 June 2023 **Revised:** 28 July 2023 **Accepted:** 11 August 2023*

Order Preference Similarity to the Ideal Solution (TOPSIS)-based Secure Neighbor Discovery Mechanism (FTOPSIS-SNDM).

III. PROPOSED METHOD

The proposed FTOPSIS-SNDM scheme is presented with its merits and role in the determination of neighbourhood node discovery during process of routing between the source and the sink nodes.

TABLE I. CONSOLIDATED SUMMARY OF THE REVIEWED EXISTING WORKS CONTRIBUTED TO THE LITERATURE

Author	***Mechanism Utilized***	***Pros***	***Cons***
AlFarraj et al. [15]	Trusted Neighbor Selection approach using the merits of Activation Function (TNSAF)	It identifies the reliable and non-reliable nodes by efficient decision making process, employing sequential activation and arbitrary transigmoid functions that retain network performance.	The accuracy in trusted neighbour node detection still needs significant improvement
Khalid et al. [16]	Adaptive Trust-based Routing Protocol (ATRP)	It employs MCDM, wherein trust metrics are recognized based on varying network performance leading to improved decision as several uncertainty features are taken into consideration	It handled the issue of uncertainty to some level, but it is still cannot handle more dynamic routing environment
Yang et al. [17]	Blockchain and Reinforcement Learning (RL)-based Trusted Routing Mechanism	It routing strategy stored the routing information of nodes on Blockchain using token transactions that makes routing information observable and difficult to tamper.	The pattern learning of behaviors need to includemore impactful factors of routing in order to model possible actions of nodes under routing
Renjith [18]	ANFIS based Trust Evaluation (ATE) routing protocol	It reduces the computational complexity and offers improved network lifespan. Including trust into ANFIS enhances security and enables choosing effective routing paths for rapid forwarding of data.	The degree of uncertainty handled by this ATE needs improvement with minimized false positive rate
Abd El-Moghith and Darwish [19]	Deep blockchain along with Markov Decision Processes (MDPs)-based trustedrouting mechanism	It identified the authentication group essential for proofing by using Deep Learning (DL) method which emphases on node properties. MDPs are used in selecting the appropriate next hop node that is proficient in securely transmitting messages	This MDP approach ignored some potential behavior of sensor nodes under routing, and thus the adopted model is not comprehensive
Hajiee et al. [20]	Energy and trust-based routing scheme using learning automata and assessment function.	.It employed Learning Automata and assessment function for determining trusted and malevolent nodes and assessing the node when compared to threshold	The assessment function need to be formulated using weighted coefficient for determining the impact of each factors during the process of routing
John and Deepa [21]	Recommendation Filtering based Trust Model (RFTM)	It employed an Artificial Intelligence (AI)-based Dempster Shafer theory along with deviation test schemes for avoiding fake recommendations, such that it improves throughput and Packet Delivery Ratio (PDR).	The bias adopted duting the process of filtering is skewed and failed in exploring possible dimensions that could be considered for evaluation.
Sajan et al [22]	Three-Level Weighted Trust evaluation-based Grey Wolf Optimization (3LWT-GWO) scheme	It adopted GWOA for clustering and identifying insecure nodes based on the node's weight computed depending on the remaining energy, node distance as well as energy	It need to balance the proper deviation between the local search and global search during the process of clustering.

A. Primitives of Fuzzy-TOPSIS (F-TOPSIS) Method

TOPSIS is the potential MCDM designed by Hwang & Yoon using the concept of 'Comparative nearness to an Optimal Solution [24]. The central aim is to determine an ideal solution from numerous substitutes which should be nearer to Positive Ideal Solution (PIS) and away from Negative Ideal Solution (NIS) [25]. In this method, once the weights of every determined criteria are defined, scores are computed, standardized and the geometric distance of every alternate to PIS as well as NIS is determined [26]. The finest alternate is chosen based on the co-

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7705
***Article Received:** 12 June 2023 **Revised:** 28 July 2023 **Accepted:** 11 August 2023*

efficient representing closeness that is taken as the complex classification index representing the choice with increased similarity to optimal solution. In case of traditional TOPSIS scheme, the input which includes the decision matrix should be numeric as well as clear. In spite of offering an easy understanding, the application demonstrates to be ineffective in handling problems related to neighborhood node selection with trustworthiness as it is not capable of handling uncertainty. However, TOPSIS can be modified to handle the imprecision of evaluation information by integrating with fuzzy logic. Fuzzy-based TOPSIS (F-TOPSIS), a MCDM tool associates conventional TOPSIS with FST, in which the weights are identified as linguistic terms and modified to fuzzy numbers as depicted in Figure 1.

Figure 1. Coprehensive view of the proposed FTOPSIS-SNDM scheme.

Once weights are assigned to criteria by involving linguistic variables, followed by production of decision matrices made up of fuzzy numbers in the range (0,1), F-TOPSIS is framed using the ensuing steps:

Step 1: Build Normalized Fuzzy Decision Matrix (NFDM)
Consider 'S' as NFDM.

$$S = [s_{ij}]_{p\times q'}, i = 1,2,\dots.p, j = 1,2,\dots q \quad (1)$$

The standardised values for both benefit as well as cost criteria are given below:

$$s_{ij} = \left(\frac{x_{ij}}{z_j^+}, \frac{y_{ij}}{z_j^+}, \frac{z_{ij}}{z_j^+}\right) \quad (2)$$

$$s_{ij} = \left(\frac{x_j^-}{z_{ij}}, \frac{x_j^-}{y_{ij}}, \frac{x_j^-}{x_{ij}}\right) \quad (3)$$

where,

Benefit criteria: $z_j^+ = \max\{z_{ij}\}$

Cost criteria: $x_j^- = \min\{x_{ij}\}$

The benefit criteria issued when candidate's interest is to assume that the maximum score is the finest option. Likewise, cost criteria is used when interest is to consider the minimum score as the motivating solution. It is notable that the range of standardized Triangular Fuzzy Numbers (TFNs) fit into (0; 1).

Step 2: Build Weighted NDM (WNDM) matrix

$$T = [t_{ij}]_{p\times q'}, i = 1,2,\dots.p, j = 1,2,\dots q \quad (4)$$

Where, $t_{ij} = s_{ij} \times w_j$

w_j-'j^{th}' attribute's weight

Step 3: Define Fuzzy PIS (FPIS, F^+) and Fuzzy NIS (FNIS, F^-):

$$F^+ = (t_1^+, t_2^+, \dots t_n^+) \quad (5)$$

$$F^- = (t_1^-, t_2^-, \dots t_n^-) \quad (6)$$

where, $t_j^+ = (1;1;1)$ and $t_j^- = (0;0;0)$

Step 4: Find the distance of every substitute from '$F^+(D_i^+)$' as well as '$F^-(D_i^-)$'correspondingly

$$D_i^+ = \sum_{j=1}^{n} D(t_{ij}, t_j^+) \quad (7)$$

$$D_i^- = \sum_{j=1}^{n} D(t_{ij}, t_j^-) \quad (8)$$

Where,
D(A,B) -Distance amid 2 FTNs,
X = (x_1, y_1,z_1) and Y = (x_2, y_2,z_2), and is calculated as:

$$D(X,Y) = \sqrt{\frac{1}{3}((x_1-x_2)^2 + (y_1-y_2)^2 + (z_1-z_2)^2)} \quad (9)$$

Step 5: Determine the Closeness Co-efficient (CC_i) of every alternate (sensor neighbourhood node)

$$CC_i = \frac{d_i^-}{d_i^+ + d_i^-} \quad (10)$$

Step 6: Rank the alternates (sensor neighbourhood node during routing process)
The alternates are arranged based on diminishing order of'CC_i'. The finest substitute is nearer to 'F^+' as 'CC_i' moves towards 1.

Linguistic Variables

F-TOPSIS demands linguistic terms for evaluating the significance level of criteria, thus permitting the assessment of suppliers' performance [27]. A5-point scale to be implemented during experts' decision from Very Low (VL) that shows

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7705
***Article Received:** 12 June 2023 **Revised:** 28 July 2023 **Accepted:** 11 August 2023*

reduced quality and supplier's capability for achieving a service to Very High (VH) that would be qualified to best promising performance in the assessed problem.

Linguistic terms listed in Table 1 are suggested to be used in F-TOPSIS models implemented for selection of supplier, where in 'x', 'y' and 'z' illustrate crisp numbers of assessment scale.

TABLE II. LINGUISTIC TERMS IN F-TOPSIS

Linguistic Term	***VL***	***L***	***M***	***H***	***VH***
Valor fuzzy	(x_{VL} , y_{VL} , z_{VL})	(x_L , y_L , z_L)	(x_M , y_M , z_M)	(x_H , y_H, z_H)	(x_{VH} , y_{VH} , z_{VH})

Linguistic variables are defined, followed by attribution of fuzzy values to appropriate term scale. The terms are to be modelled using TFs, as these functions are appropriate for this problem as specified in Table 3.

TABLE III. FN SCALE FOR SIGNIFICANCE(WEIGHT) LEVEL OF DECISION CRITERIA AND CRITERIA'S PERFORMANCE ASSESSMENT

Linguistic Term	**VL**	**L**	**M**	**H**	**VH**
Criteria Weight	(0.0, 0.0, 0.25)	(0.0, 0.25, 0.50)	(0.25, 0.50, 0.75)	(0.50, 0.75, 1.0)	(0.75, 1.0, 1.0)
Performance Evaluation	(0.0, 0.0, 2.5)	(0.0, 2.5, 5.0)	(2.5, 5.0, 7.5)	(5.0, 7.5, 10)	(7.5, 10, 10)

Definition of packet forwarding potential, delay, distance from the base station and residual energy-based criteria for trust evaluation

This proposed scheme considered the decision criteria associated with the process of trusted neighbor node discovery by considering the factors that impacts the performance and behavior of sensor nodes [28]. It specifically considered TOPSIS, since the perception of the sensor nodes' behavior together with its performance in the past is utilized for evaluation without considering any additional data [29]. Further, the use of Fuzzy TOPSIS facilitated the option of adopting the relation between the pre-determined linguistic terms with quantitative and qualitative scale to assess the influence of each criteria during the process of trusted-neighbor discovery. The set of trust impacting considered during evaluating the behavior of neighboring sensor nodes during routing process of presented as follows.

Criterion (C1): Packet Forwarding Potential

It is the factor which depicts the forwarding potential of each sensor nodes. It is the rate at which the packet received by sensor nodes is forwarded to its neighbouring node with any packet drop. When the amount of packets dropped by node is higher, then the trust possessed by that node is considered to be low during the process of routing. The scale of reference with respect to this criterion 'Packet forwarding potential' is presented in Table 3.

TABLE IV. SCALE OF REFERENCE WITH RESPECT TO CRITERION (C1-PACKET FORWARDING RATE)

Linguistic Term	**VL**	**L**	**M**	**H**	**VH**
Rating Scale	0	0.2	0.5	0.8	1

C2: Delay

It is the factor which aids in determining the trustworthiness of each sensor nodes. If the packets at a particular node reaches after a huge delay, then the forwarder neighbour sensor node is identified as malicious nodes in the routing path. Otherwise, it is considered to a cooperating and genuine neighbourhood sensor node which can be considered for routing. The scale of reference with respect to this criterion termed 'delay' is presented in Table 5.

TABLE V. SCALE OF REFERENCE WITH RESPECT TO CRITERION (C2-DELAY)

Linguistic	**VL**	**L**	**M**	**H**	**VH**
Rating Scale	1	0.8	0.5	0.2	0

C3: Distance from the sink

This factor termed distance of the sensor nodes from the sink plays an anchor role in exploring the trust worthiness of sensor nodes during the routing process. When the distance between each sensor node and the sink is high, then it has the maximized probability of packet dropping in the network. Thus the scale of reference with respect to distance from the sink is shown in Table 6.

TABLE VI. SCALE OF REFERENCE WITH RESPECT TO CRITERION (C3-DISTANCE FROM SINK)

Linguistic	**VL**	**L**	**M**	**H**	**VH**
Rating Scale	1	0.8	0.5	0.2	0

C4: Residual Energy

It is the factor which aids in determining the trustworthiness of each sensor nodes in the network with respect to energy possessed by them after the routing process. When the energy possessed by a sensor node is high, then it possesses high trust as the probability of packet dropping due to selfishness is

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7705
***Article Received:** 12 June 2023 **Revised:** 28 July 2023 **Accepted:** 11 August 2023*

highly reduced. Thus the scale of reference with respect to residual energy is presented in Table 7.

TABLE VII. SCALE OF REFERENCE WITH RESPECT TO CRITERION (C4-RESIDUAL ENERGY)

Linguistic	**VL**	**L**	**M**	**H**	**VH**
Rating Scale	0	0.2	0.5	0.8	1

The aforementioned four criterion are considered during the process of trusted neighbour sensor node discovery during the process of data dissemination between the source and sink in WSNs. In specific, the term "Closeness Co-efficient" defined using Equation (10) aids in ranking the sensor nodes in the routing path, such that the nodes with good rank and threshold value of detection greater than 0.4(determined through simulation with different values, and it is the point at which maximum malicious neighbours are identified to attain maximized packet forwarding capability) is considered for the routing process, and the remaining untrustworthiness nodes are isolated from the routing path.

IV. RESULTS AND DISCUSSION

Simulation experiments of proposed FTOPSIS-SNDM and the baseline RFTM, TNSAF and RAFTSPR approaches are performed using ns-2.34 simulator. The methods of RFTM, TNSAF, RAFTSPR are chosen for comparison with the proposed FTOPSIS-SNDM scheme, since the benchmarked approaches more or less adopted a comprehensive method of trust evaluation through the extraction of impact factors that helps in determining the neighbour node is trustworthy or not to attribute towards potential reliable data dissemination in WSNs.

This implementation is conducted with 500 mobile nodes arbitrarily distributed in terrain area of 1500 x 1500 square meters. The simulation time considered for implementing the proposed FTOPSIS-SNDM and the baseline approaches is 9.52 minutes [30]. The complete set of mobile nodes possesses a transmission range of 250 meters with the traffic types of Constant Bit Rate (CBR) to facilitate constant rate of packet transmission amid source and destination in network for restricting the traffic rate. Moreover, Ad hoc On-demand Distance Vector (AODV) is adopted for facilitating a routing path with free interference. In addition, Table 7 shows the simulation setup considered during implementation of proposed FTOPSIS-SNDM and the baseline approaches.

TABLE VIII. SIMULATION SETUP USED FOR IMPLEMENTING THE PROPOSED FTOPSIS-SNDM SCHEME

Simulation Parameter	**Value used**
Number of mobile nodes	500
Network terrain area	1500 x 1500 square meters
Transmission range	250 meters
Simulation time	9.52 minutes
Traffic source	CBR
Base protocol	AODV
Traffic rate	20 packets per second
Mobility model	Random Way Point
MAC type	802.11g
Size of the packet	512 Bytes
Initial energy of mobile nodes	25 J
Threshold trust estimation and node replacement	0.4
Trust Update Interval	0.02-1.0

The simulation experiments of the proposed FTOPSIS-SNDM and the baseline RFTM, TNSAF and RAFTSPR approaches are performed in three folds. In the initial portion of analysis, the performance of proposed FTOPSIS-SNDM and the baseline mechanisms are compared using Throughput, Trusted neighbour node discovery rate, energy consumption and packet delay with different amount of nodes. In the next portion of analysis, proposed FTOPSIS-SNDM and the baseline schemes are evaluated based on Packet delivery rate, energy consumption, Detection rate and packet drop rate with different amount of malicious nodes. In the lat portion of analysis, the potentiality of the proposed FTOPSIS-SNDM and standard schemes are evaluated using Throughput, Network lifetime, False positive rate, packet delay with different trust update interval.

A. Performance Assessment of Proposed

In this experimental investigation, the performance of proposed FTOPSIS-SNDM ans the baseline schemes are compared using Throughput, Trusted neighbour node discovery rate, energy consumption and packet delay with varying amount of sensor nodes. Figure 2 and 3 presents the plots of throughput and trusted neighbour node discovery rate achieved by proposed FTOPSIS-SNDM scheme and the baseline RFTM, TNSAF and RAFTSPR approaches with different number of sensor nodes. The proposed FTOPSIS-SNDM mechanism explored feasible number of parameters during node behavior process, and handled the issue of impreciseness that are more commonly visualized with the change in the behavior of sensor nodes in the network. This predominance in handling the degree of information uncertainty aided the proposed FTOPSIS-SNDM mechanism in improving the throughput of the network to an anticipated level. Therefore, proposed FTOPSIS-SNDM with different sensor nodes improved the throughput by a predominant margin of 21.32%, 14.28%, and 17.64%, superior than the baseline schemes used for investigation. Moreover, the Trusted neighbour node discovery rate achieved by the proposed FTOPSIS-SNDM with different sensor nodes is enhanced by 16.98%, 19.14% and 21.36% in contrast to baseline schemes used for investigation.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7705
***Article Received:** 12 June 2023 **Revised:** 28 July 2023 **Accepted:** 11 August 2023*

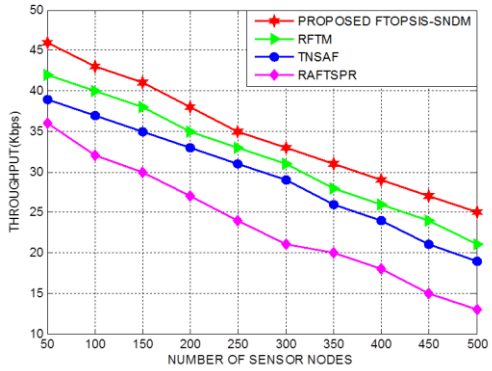

Figure. 2 Throughput for varying number of sensor nodes

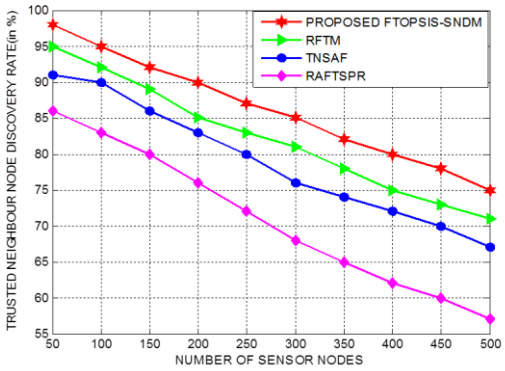

Figure. 3 Trusted neighbour node discovery rate for varying number of sensor nodes

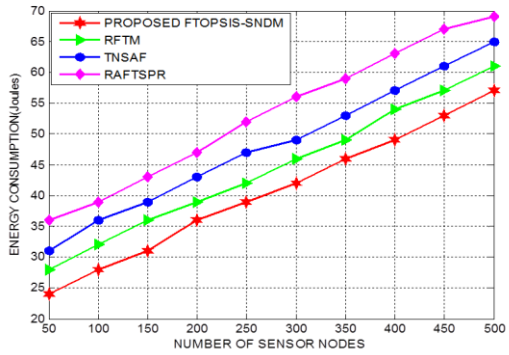

Figure. 4 Energy consumption for varying number of sensor nodes

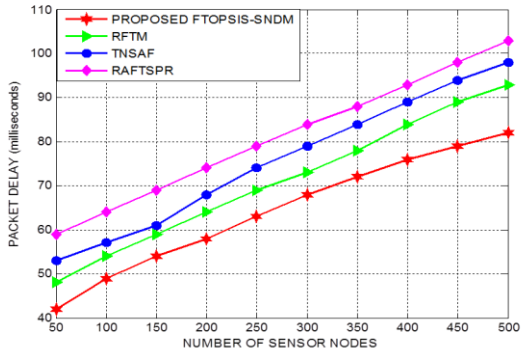

Figure. 5 Packet delay for varying number of sensor nodes

Moreover, Figure 4 and 5 demonstrates the energy consumption and packet delay incurred by the FTOPSIS-SNDM and standard mechanisms for varying amount of nodes. The proposed FTOPSIS-SNDM mechanism facilitated rapid rate of detection, which helped in isolating the malicious sensor nodes from the routing path, which thereby reduces the unnecessary energy drain in the network with any specific reason. This detection rate of the proposed approach also reduced the time incurred by the packets travelling from one sensor node to the another, such that it reaches the essential nodes for attaining reactive decision making process. It also reduces the feasible number of packet retransmissions to an expected level which adds extra benefits in terms of communication overhead. Thus the proposed FTOPSIS-SNDM confirmed reduced consumption of 19.26%, 21.58% and 24.19% when compared to the baseline schemes used for examination. Furthermore, the packet delay experienced by the proposed FTOPSIS-SNDM is reduced by 14.38%, 16.84% and 18.62% in contrast to the standard mechanisms taken for examination.

Packet delivery rate as well as detection rate achieved by the proposed FTOPSIS-SNDM and the baseline schemes for varying amount of malicious nodes. The proposed FTOPSIS-SNDM scheme explored different dimensions of trust evaluating parameters associated with sensor nodes, and paved a reliable route between the source and the sink. It adopted multiple number of criteria during neighbouring node discovery, such that malicious node are never included as the neighbouring nodes during the process of routing. It incorporated multiple levels of trust computation phenomenon(trust computation determined based on first hand and second hand information determined from the neighbours with respect to individual node level and comprehensive network level) with different combinations of criteria, which aided in better detection rate of malicious neighbourhood node during the routing process. The packet delivery rate achieved by the proposed FTOPSIS-SNDM for varying number of malicious sensor nodes is improved by 18.94%, 21.82% and 24.84% when compared to the baseline schemes used for investigation. Moreover, the detection rate attained by the proposed FTOPSIS-SNDM with different malicious sensor nodes is enhanced by a significant level of 17.64%, 19.21% and 22.39% in contrast to baseline schemes used for investigation.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7705
***Article Received:** 12 June 2023 **Revised:** 28 July 2023 **Accepted:** 11 August 2023*

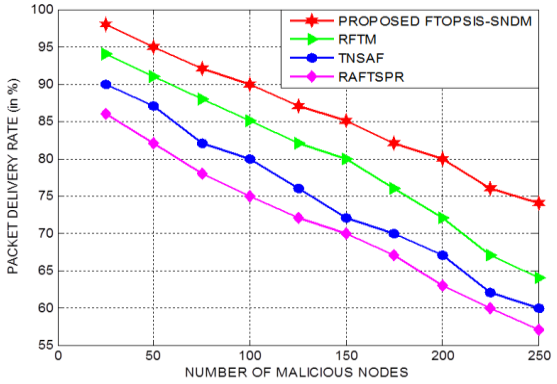

Figure. 6 Packet delivery rate for varying number of malicious nodes

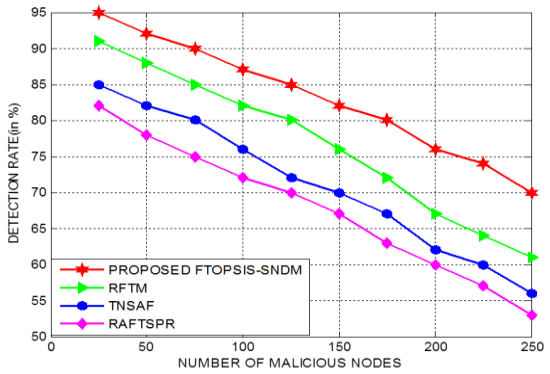

Figure. 7 Detection Rate for Varying Number of Malicious Nodes

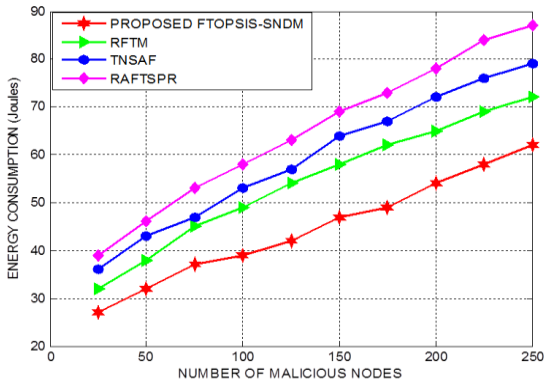

Figure. 8 Energy consumption for varying number of malicious nodes

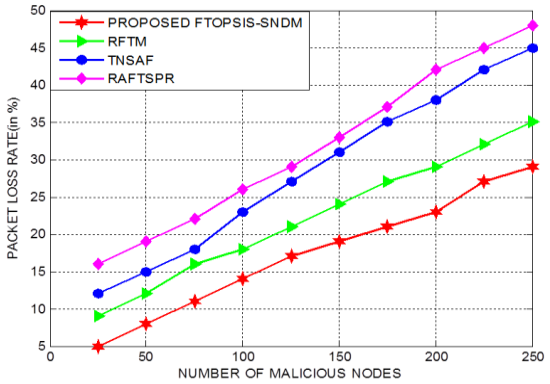

Figure. 9 Packet loss rate for varying number of malicious nodes

In addition, Figure 8 and 9 depict the plots of energy consumption and packet drop rate incurred by the proposed FTOPSIS-SNDM and the baseline schemes for varying number of malicious sensor nodes. The proposed FTOPSIS-SNDM handles the degree of uncertainty and vagueness included into the information shared between the sensor nodes of the network. It facilitated dynamic strategy to exploit different factors which impacts the cooperation of the sensor nodes for guaranteeing reliable data deliver between the source and destination, This adopted of multiple criteria and dynamic strategy paved the way for identifying trustworthy neighbourhood sensor nodes during the process of routing. This neighbourhood discovery strategy minimized energy consumption and packet drop to the desirable level without hurdling the network lifespan. Thus the proposed FTOPSIS-SNDM for varying number of malicious sensor nodes confirmed better energy consumption of 17.21%, 19.84% and 22.86%in contrast to the baseline schemes used for investigation. Moreover, the packet loss rate with different malicious sensor nodes is significantly reduced by the proposed FTOPSIS-SNDM to a considerable margin of 16.84%, 18.62% and 21.32% when compared to the baseline schemes used for investigation.

B. Performance Assessment of Proposed FTOPSIS-SNDM for Varying Trust Update Intervals

In this part of analysis, the potentiality of the proposed FTOPSIS-SNDM and the baseline schemes are evaluated using Throughput, Network lifetime, False positive rate, packet delay with different trust update interval. In particular, Figure 10 and 11 depicts the throughput and network lifetime attained by the proposed FTOPSIS-SNDM scheme and standard RFTM, TNSAF and RAFTSPR approaches with different trust update intervals. The throughput with increasing trust update interval generally gets increase, but the existence of malicious neighbourhood nodes pose challenges during the process of data routing amid the source and the sink node. But the proposed FTOPSIS-SNDM scheme adopted an adaptive mechanism (mechanism that works with possible number of influential parameters that could be possibly derived from the sensor nodes, but these parameters constantly changes depending on the context of monitroitng). This contextual derivation of impactful parametshelped in detecting malicious node at a faster rate and isolating them from the routing path. This isolation process of malevolent nodes prevented unnecessary death of sensor nodes in the network with sustained energy conservation. Thus it attributed towards sustained network lifetime in the network with maximized alive nodes in the network. Thus the FTOPSIS-SNDM scheme with different trust update interval improved the throughput by 10.32%, 14.58% and 16.18%, better than the benchmarked RFTM,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7705
***Article Received:** 12 June 2023 **Revised:** 28 July 2023 **Accepted:** 11 August 2023*

TNSAF and RAFTSPR approaches. Moreover, the network lifetime sustained by the proposed FTOPSIS-SNDM scheme with different trust update interval is maximized by 11.28%, 14.52%, and 17.86%, superior than the baseline schemes used for investigation.

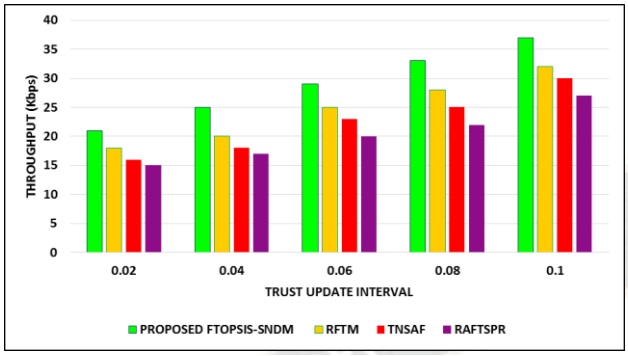

Figure. 10 Throughput for varying trust update intervals

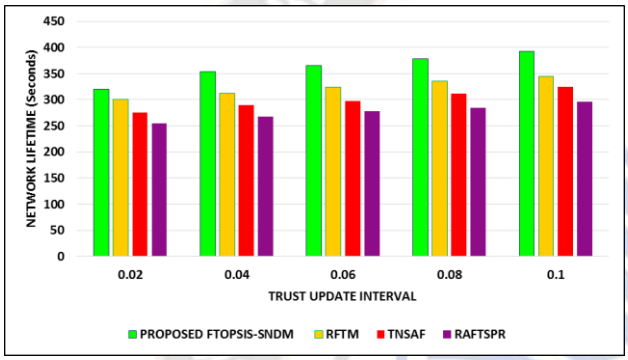

Figure. 11 Network lifespan for varying trust update intervals

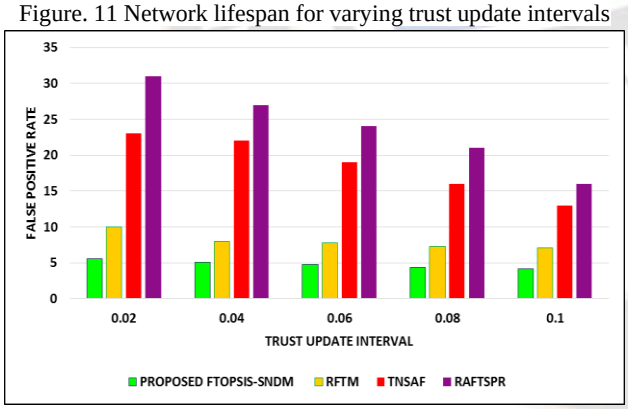

Figure. 12 False positive rate for varying trust update intervals

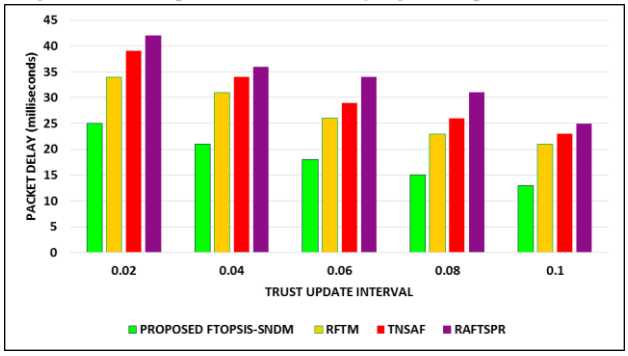

Figure. 13 Packet delay for varying trust update intervals

In specific, Figure 12 and 13 portrays the false positive rate and packet delay realized in network during implementation of proposed FTOPSIS-SNDM scheme and standard RFTM, TNSAF and RAFTSPR approaches with different trust update intervals. The results proved that the false positive rate identified during detection of malevolent neighbourhood sensor nodes is significantly minimized by the proposed FTOPSIS-SNDM scheme, since it included the impactful factors of packet forwarding potential, delay, distance from the base station and residual energy to prevent malicious nodes from acting as the forwarder node. The packet delay is considerably minimized by the proposed FTOPSIS-SNDM scheme as rapid detection rate is achieved with isolation of them during the routing process such that unnecessary time waste is prevented during the process of data transmission. Thus the FTOPSIS-SNDM scheme with different trust update interval reduced the false positive rate by 9.12%, 11.38% and 14.98%, better than the benchmarked RFTM, TNSAF and RAFTSPR approaches. Moreover, the packet delay of the proposed FTOPSIS-SNDM scheme with different trust update interval is minimized by 10.42%, 12.86%, and 15.12%, superior than the baseline schemes used for investigation.

V. CONCLUSION

The proposed FTOPSIS-SNDM achieved reliable estimation of trust related to each sensor node during the process of routing path establishment with reliable neighbourhood node discovery. This proposed FTOPSIS-SNDM aided in attaining the objective of enhancing reliable data delivery in WSNs. It combined the merits of FST and TOPSIS-based MCDM for efficient and trustworthy discovery of secure neighbors under the exchange of imprecise data and uncertain behavior of sensor nodes. It adopted a dynamic strategy which identified secure neighbor sensor nodes using the impactful factors of packet forwarding potential, delay, distance from the BS and residual energy into account. The outcomes also confirmed that proposed FTOPSIS-SNDM scheme with different trust update interval reduced the false positive rate and packet delay, on an average by 12.84% and 11.86%, better than the benchmarked RFTM, TNSAF and RAFTSPR approaches. As the part of future scope, a neighbourhood node discovery mechanism using Fuzzy TOPSIS and Fuzzy COPRAS can be formulated, implemented, and compared with the proposed FTOPSIS-SNDM scheme with homogeneous and heterogeneous network conditions.

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] Ambigavathi, M., & Sridharan, D. (2018). Energy-aware data aggregation techniques in wireless sensor network. Advances in power systems and energy management, 165-173.

[5] Tolba, A. (2017) .Organizing multipath routing in cloud computing environments. Int J Adv Comput Sci Appl, 8(1), 455-462.

[6] A. Salem, D. ., & Hashim, E. M. . (2023). Impact of Data Pre-Processing on Covid-19 Diagnosis Using Machine Learning Algorithms. International Journal of Intelligent Systems and Applications in Engineering, 11(1s), 164–171. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2489

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

[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. J Netw Comput Appl, 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 Comput, 21(21), 6225-6236.

[10] Mr. Vaishali Sarangpure. (2014). CUP and DISC OPTIC Segmentation Using Optimized Superpixel Classification for Glaucoma Screening. International Journal of New Practices in Management and Engineering, 3(03), 07 - 11. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/30

[11] Ahmed, A., Bakar, K.A., Channa, M.I., & Khan, A.W. (2016a). A secure routing protocol with trust and energy awareness for wireless sensor network. Mob Netw Appl, 21(2), 272-285.

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

[13] Zhang, B., Huang, Z., & Xiang, Y. (2014). A novel multiple-level trust management framework for wireless sensor networks. Comput Netw, 72, 45-61.

[14] Xia, F., Liaqat, H.B., Ahmed, A.M., Liu, L., Ma, J., Huang, R., Tolba, A. (2016a). User popularity-based packet scheduling for congestion control in ad-hoc social networks. J Comput Syst Sci, 82(1), 93-112.

[15] Esposito, M., Kowalska, A., Hansen, A., Rodríguez, M., & Santos, M. Optimizing Resource Allocation in Engineering Management with Machine Learning. Kuwait Journal of Machine Learning, 1(2). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/115

[16] Xia, H., Yu, J., Pan, Z.K., Cheng, X.G., & Sha E.H.M. (2016b). Applying trust enhancements to reactive routing protocols in mobile ad hoc networks. Wirel Netw, 22(7), 2239-2257.

[17] Xia, H., Yu, J., Pan, Z.K., Cheng, X.G., & Sha E.H.M. (2016b). Applying trust enhancements to reactive routing protocols in mobile ad hoc networks. Wirel Netw, 22(7), 2239-2257.

[18] 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.

[19] Khalid, N. A., Bai, Q., & Al-Anbuky, A. (2019). Adaptive trust-based routing protocol for large scale WSNs. IEEE Access, 7, 143539-143549.

[20] Yang, J., He, S., Xu, Y., Chen, L., & Ren, J. (2019). A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks. Sensors, 19(4), 970.

[21] Renjith, P. N. (2020). Towards secure data forwarding with anfis and trust evaluation in wireless sensor networks. Wireless Personal Communications, 114(1), 765-781.

[22] Abd El-Moghith, I. A., & Darwish, S. M. (2021). Towards designing a trusted routing scheme in wireless sensor networks: A new deep blockchain approach. IEEE Access, 9, 103822-103834.

[23] Hajiee, M., Fartash, M., & Eraghi, N. O. (2021). Trust-based Routing Optimization using Learning Automata in Wireless Sensor Network. Majlesi Journal of Electrical Engineering, 15(4), 87-98.

[24] John, R., & Deepa, J. (2022, April). Trust Model for Secure Routing in Wireless Sensor Network using AI Technique. In 2022 8th International Conference on Smart Structures and Systems (ICSSS) (pp. 1-5). IEEE.

[25] Goar, D. V. . (2021). Biometric Image Analysis in Enhancing Security Based on Cloud IOT Module in Classification Using Deep Learning- Techniques. Research Journal of Computer Systems and Engineering, 2(1), 01:05. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/9

[26] Sajan, R. I., Christopher, V. B., Kavitha, M. J., & Akhila, T. S. (2022). An energy aware secure three-level weighted trust evaluation and grey wolf optimization based routing in wireless ad hoc sensor network. Wireless Networks, 28(4), 1439-1455.

[27] Rahamat Basha, S., Sharma, C., Sayeed, F., Arularasan, A. N., Pramila, P. V., Shinde, S. K., Pant, B., Rajaram, A., &Yeshitla, A. (2022). Implementation of reliability antecedent forwarding technique using straddling path recovery in Manet. Wireless Communications and Mobile Computing, 2022(4), 1-9.

[28] Hwang, C., & Yoon, K. (1981). Methods for multiple attribute decision making. Multiple Attribute Decision Making, 3(4), 58-191.

[29] Shamsuzzoha, A., Piya, S., &Shamsuzzaman, M. (2021). Application of fuzzy TOPSIS framework for selecting complex project in a case company. Journal of Global Operations and Strategic Sourcing, 14(3), 528-566.

[30] Gui, X., Wang, J., Wang, G., Park, J., & Sandhu, R. (2019). Dynamic trust evaluation model based on bidding and multi-attributes for social networks. International Journal of High Performance Computing and Networking, 13(4), 436.

[31] Chen, Q., Liu, L., Yang, Z., & Guo, K. (2016). Prediction approach of critical node based on multiple attribute decision

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7705
Article Received: 12 June 2023 *Revised:* 28 July 2023 *Accepted:* 11 August 2023

making for opportunistic sensor networks. Journal of Sensors, 2016(4), 1-8.

[32] Jagatheswari, S., Ramalingam, P., & Chandra Priya, J. (2022). Improved grey relational analysis-based TOPSIS method for cooperation enforcing scheme to guarantee quality of service in MANETs. International Journal of Information Technology, 14(2), 887-897.

[33] Katsikas, S., &Gkioulos, V. (2020). Security, privacy, and trustworthiness of sensor networks and Internet of things. *Sensors*, *20*(14), 3846.

[34] Wang, Z., Xu, G., Zhang, N., Qi, Z., Wei, F., & He, L. (2021). Ferry node identification model for the security of mobile ad hoc network. Security and Communication Networks, 2021(4), 1-13.