Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.031422
Article

Tech Science Press

Fuzzy Reputation Based Trust Mechanism for Mitigating Attacks in MANET

S. Maheswari and R. Vijayabhasker*

Department of Electronics and Communication Engineering, Anna University Regional Campus, Coimbatore, 641046, India
*Corresponding Author: R. Vijayabhasker. Email: vb@aurcc.ac.in
Received: 17 April 2022; Accepted: 29 May 2022

Abstract: Mobile Ad-hoc Networks (MANET) usage across the globe is increasing by the day. Evaluating a node's trust value has significant advantages since such network applications only run efficiently by involving trustable nodes. The trust values are estimated based on the reputation values of each node in the network by using different mechanisms. However, these mechanisms have various challenging issues which degrade the network performance. Hence, a novel Quality of Service (QoS) Trust Estimation with Black/Gray hole Attack Detection approach is proposed in this research work. Initially, the QoS-based trust estimation is proposed by using a Fuzzy logic scheme. The trust value of each node is estimated by using each node's reputation values which are determined based on the fuzzy membership function values and utilizing QoS parameters such as residual energy, bandwidth, node mobility, and reliability. This mechanism prevents only the black hole attack in the network during transmission. But, the gray hole attacks are not identified which in turn increases the packet drop rate significantly. Hence, the gray hole attack is also detected based on the Kullback-Leibler (KL) divergence method used for estimating the statistical measures. Additional QoS metrics are considered to prevent the gray hole attack, such as packet loss, packet delivery ratio, and delay for each node. Thus, the proposed mechanism prevents both black hole and gray hole attacks simultaneously. Finally, the simulation results show that the effectiveness of the proposed mechanism compared with the other trust-aware routing protocols in MANET.

Keywords: Mobile ad-hoc network; trust estimation; blackhole; grayhole attack; fuzzy logic; qos parameters; kullback-leibler divergence

1 Introduction

In modern decades, the most popular and widely used wireless network is Mobile Ad-hoc Network (MANET) which is a self-organizing and decentralized system. MANET is a collection of various wireless mobile nodes which collectively operate together. Nodes may communicate with each other nodes with the direct distributed wireless radio links. Such networks are quite vulnerable to many attacks due to their open and dynamic nature. Information transmission from source to destination is achieved with the help of the other nodes in the routing path. The most challenging task in MANET is the routing scheme since handling a network with a considerable amount of nodes was difficult [1]. Over the past

decades, several routing protocols have been proposed with limited resources. Some of them are energy and bandwidth and consideration of the security in the network.

Trust is defined as the degree of belief among the different entities. The trust for the same entity is varied while different people evaluate it. Trust management is the system that can assure the different features such as security, access control, intrusion detection, malicious nodes mitigation, etc. These are all the critical requirements for effective routing in MANET [2]. The selfish node does not cooperate with the other nodes and drops the packet during transmission since such node accumulates its resources. Therefore, reputation mechanisms are utilized to avoid such malicious behaviors of the nodes in the network.

A reputation is defined as an import of the past behavior of an entity. The reputation system maintains a black list that contains the records of malicious nodes. The malicious nodes may cause several attacks such as a black hole attack and cooperative attack for which a trust-based mechanism is utilized. In trust-based approaches, the trust value associated with each other node is represented with the trustworthiness of each neighboring node [3]. Trust in MANET has various roles, such as authentication, acknowledgment, etc., for successful packet transmission and delivery. The essential factors of trust management are trust establishment, trust update, and trust revocation.

Different trust management systems and reputation mechanisms have been proposed for detecting and isolating the malicious nodes in MANET. A novel QoS trust computation was proposed [4] by using the Fuzzy Petri Nets. In this approach, the trust value of each node was computed based on its QoS parameters. The MANET was represented as Dynamic Adaptive Fuzzy Petri Nets (DAFPN) model with a Concurrent Reasoning Algorithm (CRA). The estimation of the certainty factor using a fuzzy expert system was required for delivering each packet from node to node. The estimated certainty factor was used to evaluate the intermediate nodes' trust values during the routing process. However, several issues are addressed, such as high packet drop rate, high time and space complexities based on the FPN, less efficiency, requires additional statistical measures, less QoS performance, etc.

Hence, this research work enhances the QoS trust estimation approach with the Black/Gray hole Attack Detection approach. The QoS-based trust estimation is initially proposed using a Fuzzy logic scheme. The trust value of each node is estimated using the reputation values of each node determined based on the fuzzy membership function values that utilize QoS parameters such as residual energy, bandwidth, node mobility, and reliability. This mechanism prevents only the black hole attack in the network during transmission. However, the gray hole attacks are not identified. This significantly increases the packet drop rate. Hence, the gray hole attack is also detected based on the Kullback-Leibler (KL) divergence method used for estimating the statistical measures. Additional QoS metrics are considered, such as packet loss, packet delivery ratio, and delay for each node. Thus, the proposed mechanism simultaneously prevents black and gray hole attacks by reducing the complexity and improving QoS performance.

The rest of the paper is organized as follows: Section 2 presents the works related to trust estimation and reputation-based trust management in MANET. Section 3 explains the concept of the proposed trust-based routing protocol. Section 4 describes the performance evaluation of the proposed mechanism. Finally, Section 5 concludes the research work and presents the future scope.

2 Related Works

Reputation-based Internet Protocol security (RIPsec) scheme [5] was proposed in MANET. The main aim of this mechanism was to construct the MANET, which can support higher bandwidth applications secured by both internal and external attacks. This scheme was proposed for solving the security issues in routing protocols for MANET. This scheme consists of behavior grading, link and message encryption, and multipath routing. The encryption links and encryption-wrapped nodes were used for preventing the

network from external attacks, whereas the internal attacks were prevented by behavior grading. Moreover, end-to-end message security was improved by using public and private certificates to prevent attacks. Also, the network availability was improved by behavior grading and the Round-Robin (RR) multipath routing protocol. However, this mechanism does not have a direct defense against bad-mouthing attacks.

Exponential Reliability Coefficient-Based Reputation Mechanism (ERCRM) was proposed [6] for isolating the selfish nodes in MANET. The proposed approach was performed according to the measured energy metric and ERC through the second-hand information obtained from their neighbor nodes. The reliability coefficient was manipulated by exponential failure rate according to the moving average approach. This mechanism was assumed to be more efficient and effective due to the combination of energy efficiency and packet forwarding nature of nodes to mitigate selfishness. In addition, this mechanism was used for isolating type-I and type-II categories of selfish nodes, so the network performance was improved. However, additional statistical coefficients were required for further improvement on network performance.

Trust-based certificate revocation was proposed [7] for improving the routing security in MANET. The major objective of this approach was to reduce the vulnerability issues from nodes and enhance network security based on the certification authority and trust-based threshold revocation approach. Initially, the trust value was computed from the direct and indirect trust values. After that, the certificate authorities were used for distributing the secret key to all the nodes. Finally, the trust-based threshold revocation method was introduced, and the values were in which the misbehaving nodes were removed from the network. However, the packet drop rate was high.

An enhanced machine learning-based reputation algorithm [8] was proposed for MANET. The approach prevented many patterns of attacks. Digital signature-based mechanisms have been introduced that do not need trusted third parties or servers always online. In addition, an algorithm named Fading Memories was also enhanced that allows looking back at longer histories by using a smaller number of features. Then, a novel technique called Dynamic threshold was introduced for improving the accuracy. However, the overhead was not minimized, and reliability was not considered.

A novel reputation computation model was proposed [9] based on the subjective logic for MANET. In this approach, a node that queries another's reputation was accumulated the subjective opinions from their common neighbors. The familiarity values were used to compute the weighting factor that determines how much a node's recommending opinion impacts the reputation computation result. This familiarity facilitates the nodes to obtain opinions with lower uncertainty values, which is useful for the nodes to recognize the selfish nodes and reduce the convergence time for isolating the selfish nodes. However, the complexity of this approach was high.

A reputation-based trust management framework [10] was proposed in MANET to detect and prevent network vulnerabilities based on the piggybacking trust vectors and the routing tables. The approach [10] investigates both malicious and selfish node attacks. The distributed reputation mechanism was proposed. This is useful for the nodes to exclude them from the network while the transient faults are tolerated. This mechanism may have functioned with an on-demand routing protocol where the attacks were identified by collaborative monitoring and exchanging the information among the nodes. Moreover, the load balancing was also achieved based on the selection of nodes from the set of trusted nodes. However, the detection rate is less.

A lightweight trust-based QoS routing protocol [11] was proposed in MANET. This approach's principle of trust and QoS metric estimation was initially presented to establish a trust-based QoS mechanism. Based on this approach, the trust degree was computed between the nodes from the direct trust determination of direct observation. In addition, indirect trust estimation was also achieved based on the neighbor's recommendations for accelerating the trust establishment. Moreover, the link delay was assumed as a

QoS constraint requirement since the NP-completeness of multi-QoS constraints issues. Then, the Trust-based QoS Routing (TQR) was designed based on the tradeoff between the trust degree and link delay. However, the detection ratio was less, and routing overhead was high.

A trust management protocol [12] was proposed to analyze the group communication systems where selfish nodes exist, and system survivability was essential to mission execution. In this approach, the tradeoff between a node's welfare, such as energy conservation for improving the network lifetime, and global welfare, such as achieving the given mission with enough service availability, was considered. Also, the best design condition of this behavior framework was identified for balancing selfish and altruistic behaviors. However, the system reliability and survivability of this model were less.

Trust prediction and trust-based source routing [13] were proposed in MANET. In this approach, a dynamic trust prediction mechanism was proposed to analyze the node's trustworthiness, measured according to the node's historical behaviors and future behaviors by using a fuzzy logic rules prediction approach. The trust management strategies, such as anti-attack, decision-making, etc., were developed based on computed trustworthiness. In addition, this mechanism was combined with the source routing protocol, so the proposed approach was known as Trust-based Source Routing Protocol (TSR). This mechanism was used to improve flexibility and feasibility, which helps select the shortest path with the specific security requirements for data packet transmission. However, the QoS requirement criteria were not considered for improving the network performance.

A dynamic trust-based mechanism [14] was proposed for mitigating the gray hole attack in MANET. In this approach, each node and its neighboring nodes' trust value and association status were computed by monitoring their network behavior. The trust model was combined with the Dynamic Source Routing (DSR) protocol. The path selection procedure follows the RRES-RREP model. Therefore, the gray hole nodes were detected and avoided from the path selection process. However, the routing overhead and packet drop rate were high.

A dynamic reputation management system [15] was proposed for identifying and isolating the misbehaving nodes in MANET. In this approach, the reputation of nodes was measured based on the data-driven weighted average approach, which utilizes the number of successfully transmitted data and control packets that the node carries out for the other nodes in the network as against its transmitted packets. The distinctive direct monitoring mechanism was employed with the highest effectiveness for detecting and mitigating the different misbehaving nodes in MANET. By using this approach, the probability of acquiring the faulty second-hand information was removed, and the routing overhead was reduced by using the directly obtained information. However, the energy consumption of nodes was high during the packet transmission.

Reputation-based clustering algorithms [16] were proposed in MANET. In this approach, an in-depth analysis was presented for trust-based clustering protocols and investigated how reputations were combined with such protocols. The various attacks and clustering mechanisms were studied to identify their limitations, and a novel clustering mechanism was designed against different misbehaving. This approach was useful for detecting and mitigating malicious and misbehaving nodes with low communication and processing overhead. In this approach, the selection of security methods depended upon their overhead and security requirements. However, lack of solutions affected the network performance in both secure and hostile environments.

MANET proposed an openness–based trust and reputation management system [17] to measure and model reputation and trust propagation. In this approach, an individual reputation of nodes was modeled by employing the Dirichlet probability distribution. The trust of each node was also estimated based on the node's normal network performance and the quality of recommendations about the other nodes. The cooperative nodes were rewarded for expanding their energy during the transmission of packets to the

other nodes or for the dissemination of genuine recommendations. The available network resources mitigated the uncooperative nodes.

Furthermore, the Ruffle algorithm was introduced for ensuring the cooperative nodes, which allows the activation of sleep nodes. At the same time, their service was not required for packet transmission to its neighboring trustworthy nodes. However, the effectiveness of this approach was less.

A distributed trust and reputation model [18] was proposed in MANET for malicious nodes detection. In this approach, the malicious nodes were identified based on each node's trust values, which are estimated according to the reputation. Neighbor nodes computed the reputation value of each node according to its packet transmission behavior. The reputation information, computed under different scenarios, was collected, stored, and exchanged between the nodes. The trustworthy nodes were detected by using the highest reputation values, which in turn depends on the predefined threshold value. The nodes with reputation values less than the threshold value were identified as malicious nodes in the network. However, the efficiency of this mechanism was less.

A trust-based routing mechanism [19] was proposed for MANET. Initially, the challenging issues in MANET routing security were investigated. Then, a trust-based scheme named Fr AODV was proposed for securing AODV routing protocol in MANET based on the utilization of the friendship mechanism. A detailed analysis on QoS parameters [20–33] has been carried out and recent works [34–44] have been studied. The nodes estimated the routing paths based on the selected features such as node reputation and identity information before transmitting the data through the estimated paths. However, in this mechanism, the packet delivery ratio was less.

3 Proposed Methodology

This section briefly discusses the proposed QoS-based trust estimation using Fuzzy logic and attack detection approaches. Initially, trust estimation is performed based on each node's reputation values, which are estimated using a fuzzy logic system with QoS parameters as input. In addition, the black hole and gray hole attacks detection approach is proposed for isolating the malicious nodes in the network by including additional metrics and statistical measures.

3.1 Fuzzy Logic Based Trust and Reputation Estimation

The base station is required for transmitting the signal from source to destination through the other nodes with a given transmit power in the network establishment phase. Each mobile node measures the approximate distance to the base station according to the intensity of the received signal. In addition, distance measurement is used for selecting the appropriate transmit power for reducing the energy consumption of the nodes. Due to the limited energy, some nodes are selfish or malicious in saving their energy. Therefore the most important is to consider the reputation paradigm for network nodes. The lower the reputation value indicates that the nodes are more selfish. Hence, the node's reputation value is one of the most crucial factors that require consideration in the measurement of trust value. Node reputation value is computed by the similarity of collected data and the historical interaction experience between the nodes. For each transmission, the reputation value of one node may charge a certain reputation value from the other nodes as compensation for energy consumption and measured by using fuzzy logic. The evaluation of the reputation process is shown in Fig. 1. The estimation of reputation follows two aspects: direct reputation value and indirect reputation value. Direct reputation refers that the reputation value of node y is calculated based on the direct historical interaction between nodes x and y. In contrast, the indirect reputation value of y is estimated from the recommended value according to the other node's reputation to y.

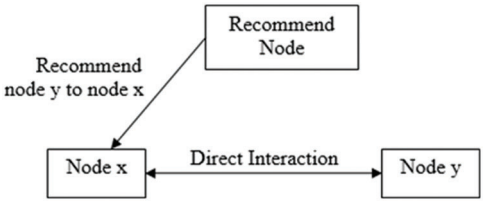

Figure 1: Reputation evaluation process

A fuzzy logic controller is a rule-based system in which a fuzzy rule represents the control mechanism. The fuzzy logic controller consists of a fuzzifier, rule-base, fuzzy inference, and fuzzified. A fuzzifier operator has the effect of converting the crisp values to the fuzzy sets, and it is denoted as i=fuzzifier (i_0), where i_0 refers to the crisp input value, i refers to the fuzzy set, and fuzzifier is a fuzzification operator. Rule-base contains IF-THEN rules measured through fuzzy logic such as low, medium, and high. Fuzzy inference converts input values into output values using fuzzy logic. It is essential for decision-making. It includes the membership functions and logic operators. Then, the defuzzifier is denoted as y_op=defuzzifier(y), where y refers to the fuzzy controller action, y_op is the crisp value of control action, and defuzzifier is the fuzzified operator. Defuzzification is defined as the process of converting fuzzy terms to crisp values.

3.2 Estimation of Direct Reputation Value

Direct reputation value is obtained by monitoring two nodes' direct interaction and utilizing the historical interaction experience between the nodes. The more successful interactions of node x to node y are represented as higher reliability of node x to node y. In a period, if the number of interactions from node x to node y is N and the number of successful interactions is K then the direct interaction of node x to node y is measured as follows:

$$\varphi_{xy} = \begin{cases} 0.5 + \dfrac{K - (N-K)}{2N_0}, & N < N_0 \\ \dfrac{K}{N}, & N \geq N_0 \end{cases} \tag{1}$$

In Eq. (1), N_0 refers to the threshold of interaction frequency. The most significant factor to the reliability of the evaluation and reputation value is interaction time. Hence, the interaction time of node x to node y is split into S segments. For the collected information in data s of node x, the time attenuation factor ρ_s and the importance factor V_s are applied for measuring the direct reputation value. The fuzzy membership function of Direct Reputation Value (DRV) of node x is estimated as follows:

$$DRV_x = \frac{\sum_{y=1}^{M} \sum_{s=1}^{S} \varphi_{xy} \rho_s V_s}{S} \tag{2}$$

In Eq. (2), M refers to the number of neighbor nodes of node x. Based on the direct interaction, the fuzzy membership function of DRV is rewritten as:

$$DRV_x = \begin{cases} \dfrac{\sum_{y=1}^{M} \sum_{s=1}^{S} 0.5 + K - (N-K)\rho_s V_s}{2N_0 S}, & N < N_0 \\ \dfrac{\sum_{y=1}^{M} \sum_{s=1}^{S} K \rho_s V_s}{NS}, & N \geq N_0 \end{cases} \tag{3}$$

3.3 Estimation of Relative Reputation Value

Consider the feature vector of data collected by the node x in a period is expressed as Fx=(t, e, a, v), where t is the type of object, e is the event type, a is the attribute of the observation region, and v is the value of perceptual information. The similarity of data feature vectors computes the relative reputation between the nodes. There are two adjacent nodes x and y. Their data feature vectors are represented as DFx=(t_x, e_x, a_x, v_x) and DFy=(t_y, e_y, a_y, v_y). The similarity of data feature vectors of node x and node y in a period is given as follows:

$$Sim(DF_x,\ DF_y) = cos(\overrightarrow{DF_x},\ \overrightarrow{DF_y}) = \frac{\overrightarrow{DF_x} \cdot \overrightarrow{DF_y}}{|\overrightarrow{DF_x}||\overrightarrow{DF_y}|} \tag{4}$$

The fuzzy membership function of Relative Reputation Value (RRV) of node x in this period is given as,

$$RRV_x = \frac{\sum_{y=1}^{M} \lambda(1 + Sim(DF_x,\ DF_y))}{M} \tag{5}$$

In Eq. (5), M refers to the number of nodes adjacent to the node $\boldsymbol{x}$ and $\lambda > 0$ denotes the similar parameters for estimating the relative reputation value. By using Eq. (3), the fuzzy membership function of RRV is rewritten as follows:

$$RRV_x = \begin{cases} \dfrac{\sum_{y=1}^{M} \lambda\left(1 + \dfrac{\overrightarrow{DF_x} \cdot \overrightarrow{DF_y}}{|\overrightarrow{DF_x}||\overrightarrow{DF_y}|}\right)}{M}, & \lambda > 0 \\ 0, & \lambda \leq 0 \end{cases} \tag{6}$$

3.4 Estimation of Reputation Value Using Fuzzy Logic

The reputation value of node x consists of Direct Reputation Value (DRV), Relative Reputation Value (RRV), and Income and Expenses Value (IEV). The fuzzy membership function for overall reputation is denoted as follows:

$$RV_x = \omega_1 DRV_x + \omega_2 RRV_x + \omega_3 IEV_x, \quad \omega_1 + \omega_2 + \omega_3 = 1 \tag{7}$$

By using Eq. (7), the fuzzy rules are given below for measuring the overall reputation value of node $\boldsymbol{x}$.

- IF $\omega_1 > (\omega_2 + \omega_3)$ THEN the reputation value of node x is measured using DRV.
- IF $\omega_2 > (\omega_1 + \omega_3)$ THEN the reputation value of node x is measured using RRV.
- IF $\omega_3 > (\omega_1 + \omega_2)$ THEN the reputation value of node $\boldsymbol{x}$ is measured using IEV.

If $IEV_x \geq 0$ then, the node $\boldsymbol{x}$ will have a high reputation value. On the other hand, if $\boldsymbol{IEV_x} < 0$ then, the node $\boldsymbol{x}$ is normal, and it has the lowest reputation value. Based on this, the trust value of each node is measured by using the following rules:

- IF reputation value is high, THEN the trust value of node $\boldsymbol{x}$ is high.
- IF reputation value is low, THEN the trust value of node $\boldsymbol{x}$ is low.

Thus, the nodes with the highest trust value are selected as the routing path members during the data transmission.

3.5 Trust and Reputation Estimation Based on Fuzzy Logic Using QoS Parameters

In this approach, the reputation is measured based on the QoS parameters such as node energy, bandwidth, node mobility, and node reliability. These parameters are given as input to the fuzzy system to generate the rules required for measuring the reputation values. The calculation of QoS parameters are following:

- Node Energy: A node has to receive and transmit the packets to the next-hop node in data packet transmission. The energy for each node is calculated based on the following equation:

$$E_{total} = 2E_{act}k + E_{amp}r^2k \tag{8}$$

where $\boldsymbol{E_{act}}$ refers to the transmitter or receiver activation energy. An amplifier requires $\boldsymbol{E_{amp}r^2}$ amount of energy for transmitting K-bit data over the distance $\boldsymbol{r}$.

- Bandwidth: Bandwidth is the number of data sent from one node to the other node within a given time duration. It is also referred to as the capacity of the communication channel.

$$BW = \frac{Transmitted\ Data\ Rate\ (bits)}{Time\ taken\ (\text{sec})} \tag{9}$$

• Node mobility: Mobility is defined as the movement of the mobile nodes and how their location, velocity, and acceleration change over the time duration. It measures how two nodes are dependent on their motion and how current velocity is related to the previous velocity. The distance between the nodes is calculated as follows:

$$Mobility = d = \sqrt[4]{k \cdot \frac{P_t}{P_r}} \tag{10}$$

In Eq. (10), $\boldsymbol{k}$ refers to the constant value, $\boldsymbol{P_t}$ refers the power required for transmission, and $\boldsymbol{P_r}$ refers to the power required for reception.

- Node reliability: A node can assess the neighbor node reliability according to the number of packets it received and transmitted accurately. Node reliability $(\boldsymbol{r})$ is estimated as a random variable by using Bayesian inference theory, and the value lies between $[\boldsymbol{0}, \boldsymbol{1}]$. Consider the node has transmitted a number of packets accurately among the $\boldsymbol{b}$ number of received packets then the expectation of reliability is as follows:

$$E[r] = \frac{\alpha_n}{\alpha_n + \beta_n} \tag{11}$$

where

$$\alpha_n = \alpha_{n-1} + a_{n-1}$$

and

$$\beta_n = \beta_{n-1} + b_{n-1} - a_{n-1}$$

and

$$\alpha_0 = \beta_0 = 0$$

The fuzzy logic system uses these QoS metrics as fuzzy input variables in evaluating the reputation of each node based on the threshold value. In MANET, the attenuation rate of a node's QoS parameters is linear in data transmission; hence, the triangular membership function measures the fuzzy input and

output variables. A fuzzy system has two processes such as fuzzification and defuzzification. In the fuzzification process, all QoS parameters are aggregated. In the defuzzification process, the threshold value is calculated. Both processes are performed based on the fuzzy rule base, which is given in Tab. 1. The threshold value (τ) is considered as the function of QoS resources attenuation rate. If the nodes have a high attenuation rate of their QoS resources, then their transmission will have a higher threshold value and vice versa.

$$Th = f(\Delta E,\ \Delta BW,\ \Delta M,\ \Delta R) \tag{12}$$

Table 1: Fuzzy rule base

Energy	Bandwidth	Mobility	Reliability	Threshold value
High	High	High	High	High
High	Medium	High	High	High
Low	Low	Low	Low	Low
Very Low	Very Low	Medium	Medium	Very Low

In Eq. (12) Δ refers to the attenuation rate of QoS parameters. The value of the threshold is varied based on the QoS parameters.

Then, the reputation and trust value for each node is measured based on the computed threshold value as follows:

- IF threshold value is high, THEN the reputation and trust values of node x are high.
- IF threshold value is low, THEN the reputation and trust values of node x are low.
- IF threshold value is very low, THEN the reputation and trust values of node x are very low (i.e., negligible).

Thus, the nodes are selected based on the highest reputation and trust values for creating a membership for path creation, where the path data transmission is carried out. Then, the average trust value of routing paths is calculated for each transmission, and the computed average trust value of all routes is compared with the route having the highest trust value. At some instant, the source does not receive any acknowledgment since the route has a black hole node, and the packets are dropped. Due to the black hole node, the average trust value of the route will become zero, and the path is avoided from the network for data transmission. Thus, the black hole attack is detected and prevented.

3.6 Trust Estimation for Detection of Hybrid Black Hole/Gray Hole Attack

The trust estimation using the QoS parameter is used for detecting only the black hole attacks in the network. Using this mechanism, both black and gray hole attacks are detected. In addition to that, the QoS metrics such as packet loss rate, packet delivery rate, delay, and statistical measures for each node like mean, deviation, kurtosis, and skew are estimated. KL divergence method is also used to estimate the same QoS factors. The considered additional QoS parameters are described below:

- Packet Loss Rate (PLR) is defined as the fraction of packets lost with respect to the packets transmitted from source to destination via neighboring nodes in the network.

$$PLR = \frac{Number\ of\ Packets\ Lost}{Number\ of\ Packets\ Transmitted} \tag{13}$$

- Packet Delivery Ratio (PDR) is defined as the fraction between the number of received packets by the destination and the number of packets generated by the source.

$$PDR = \frac{Number\ of\ Packets\ Received\ by\ Destination}{Number\ of\ Packets\ Generated\ by\ Source} \tag{14}$$

- Delay is defined as the amount of time taken for a bit of data to be transmitted across the network from one node to another node.

In addition, the statistical measures such as mean, deviation, kurtosis, and skew for each node are calculated, and its divergence values are calculated based on the KL divergence. For each QoS parameter, the mean (15) and standard deviation (16) values of each node are calculated as follows:

$$Mean_Q,\ (\mu_Q) = \frac{Q_1 + Q_2 + Q_3 + \ldots + Q_n}{n} \tag{15}$$

where $\boldsymbol{n}$ refers to the number of iterations, the standard deviation is measured as follows:

$$SD_Q,\ (\sigma_Q) = \sqrt{\frac{(Q_1 - \mu_Q)^2 + (Q_2 - \mu_Q)^2 + \ldots + (Q_n - \mu_Q)^2}{n}} \tag{16}$$

In addition, kurtosis and skew are calculated for each node's QoS parameter values based on the following equations:

$$Kurtosis,\quad (k_Q) = \frac{1}{n \cdot \sigma^4} \sum_{l=i}^{n} (Q_l - \mu_Q)^4 \tag{17}$$

$$Skew,\quad (s_Q) = \frac{1}{n \cdot \sigma^3} \sum_{l=i}^{n} (Q_l - \mu_Q)^3 \tag{18}$$

After calculating the statistical measures, the divergence between node $\boldsymbol{x}$ and $\boldsymbol{y}$ is measured based on the KL divergence. Initially, the matrix is constructed based on the elements such as the values of the QoS parameter of each node. This matrix is used to monitor behavior variations such as node activities. Using this matrix, the variation of behavior is calculated between different time durations based on the divergence. The node with the abnormal divergence is identified as the malicious node in the network. The divergence is determined by using KL divergence, which measures the similarity between two probability distributions.

$$KL[x(q)||y(q)] = \int^{p} (x) log \frac{p(x)}{p(y)} dq \tag{19}$$

In Eq. (18), $x(q)$ refers to the statistical measures of node x, $y(q)$ refers to the statistical measures of node y, $p(x)$ and $p(y)$ are probability distributions of statistical measures of node x and y respectively. Thus, the divergence between two nodes is measured according to their statistical measure values. The variations in the values are indicated that the node's behavior changes. Therefore, the gray hole attack nodes in the network are detected effectively and removed from the routing path.

Hence, both black and gray hole attacks are detected based on trust estimation and statistical measures during packet transmission. The performance effectiveness of the proposed mechanism is evaluated in the section below.

4 Experimental Results

The simulation is conducted in Network Simulator (NS-2) for the metrics packet delivery ratio, packet delay, throughput, and false positives. The comparisons are made between Fuzzy Reputation-based Trust estimation (FRT), QoS-aware Fuzzy Reputation-based Trust estimation (QFRT), and QFRT with Mitigation of the Black hole and Gray hole Attacks (QFRT-MBGA) approaches. The simulation parameters are shown in Tab. 2.

Table 2: Simulation parameters

Simulation parameters	Values
Simulation tool	NS2.35
Simulation area	1400 × 1400
Number of nodes	50
Node velocity	10–60 m/s
Simulation time	600 s
Transmission range	250 m
Packet size	512 bytes

4.1 Packet Delay

Packet delay is the fraction of the total time taken by all the packets to reach the destination to the number of packets. It is computed as follows:

$$Packet\ Delay = \frac{Total\ time\ taken\ by\ all\ the\ packets}{Number\ of\ packets} \tag{20}$$

In Fig. 2, the comparison of packet delay (sec) for FRT, QFRT, and QFRT-MBGA is shown. In this graph, the number of nodes is taken in x-axis and the packet delay (sec) is taken in y-axis. It is observed that the QFRT-MBGA mechanism has reduced packet delay compared with the other two mechanisms while network size is increased.

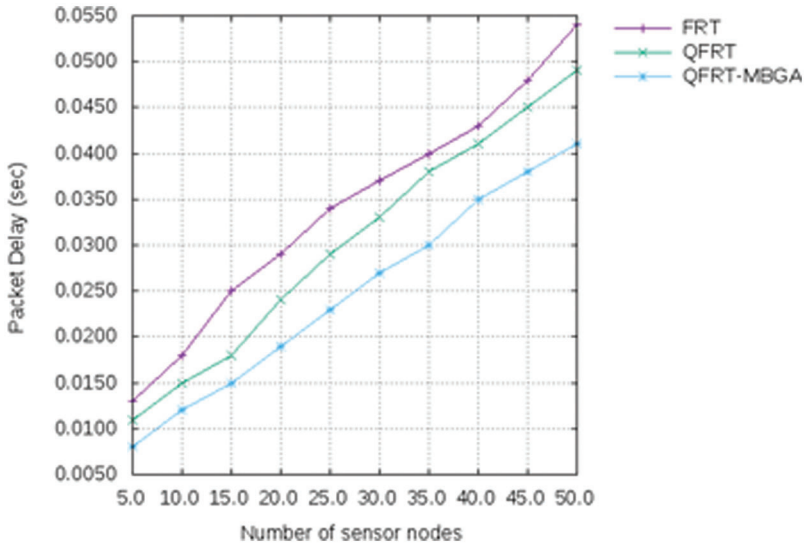

Figure 2: Number of nodes *vs.* packet delay

4.2 Throughput

Throughput is defined as the total amount of data packets correctly received by the destination node per unit time. It gives information on whether the data packets are correctly delivered to the destinations or not. Usually, it is measured in Kilobits per second (Kbps).

$$Throughput = \frac{Number\ \ of\ \ transmitted\ \ packets}{Time\ \ taken} \tag{21}$$

In Fig. 3, the comparison of throughput (Kbps) for FRT, QFRT, and QFRT-MBGA is shown. In this graph, the number of nodes is taken in x-axis and throughput (Kbps) is taken in y-axis. It is observed that the throughput decreases when the number of nodes increases. If the number of nodes is increased, a node bandwidth is shared with the neighbor nodes therefore the node bandwidth is decreased. Hence, the throughput is also decreased. The bandwidth is considered as the QoS parameter in the proposed approach; hence it includes the intermediate nodes with the threshold level of bandwidth. Thus, the QFRT-MBGA mechanism has better throughput compared with the other two mechanisms.

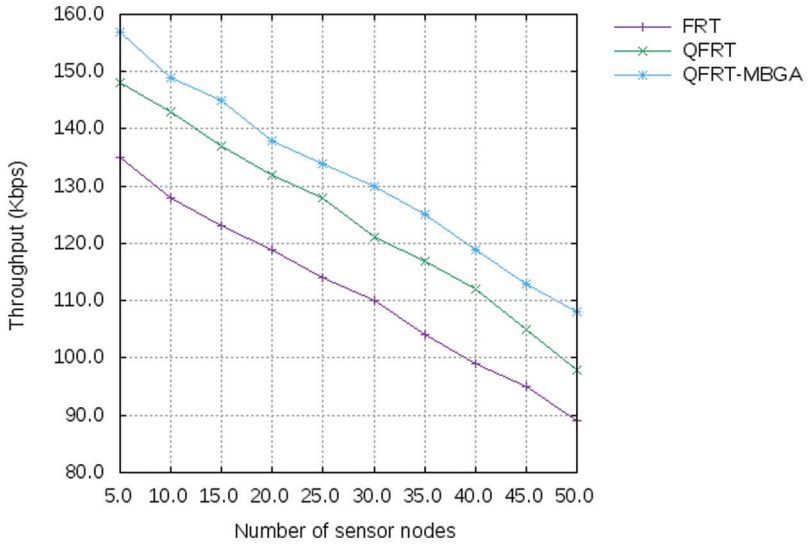

Figure 3: Number of nodes *vs.* throughput

4.3 Packet Delivery Ratio

Packet delivery ratio is the fraction of the total number of data packets received at the destination to the total number of data packets generated at the source node. This is a measure of successful delivery of packets at destination. It is calculated as follows:

$$Packet\ \ delivery\ \ ratio = \frac{Number\ \ of\ \ packets\ \ received}{Number\ \ of\ \ packets\ \ transmitted} \times 100 \tag{22}$$

In Fig. 4, the comparison of the packet delivery ratio for FRT, QFRT, and QFRT-MBGA with node velocity is shown. In this graph, the node velocity (m/sec) is taken on the x-axis and the packet delivery ratio is taken on the y-axis. It is observed that the packet delivery ratio at the destination node is decreased at higher node velocities. Node Velocity is considered as it represents the rate at which the nodes move. If the intermediate nodes do not have adequate energy and bandwidth, then the packet delivery ratio decreases. The black/gray hole attack nodes provide unwanted packet losses, affecting the packet delivery ratio. The proposed QFRT-MBGA mechanism evaluates the node trust in terms of energy,

bandwidth, mobility, and reliability. Thus, QFRT-MBGA has a better packet delivery ratio compared with the other two mechanisms.

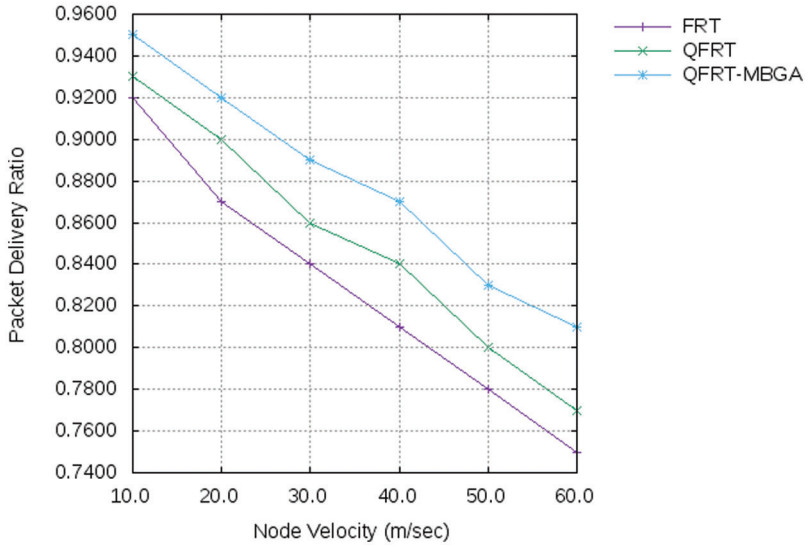

Figure 4: Node velocity *vs.* packet delivery ratio

4.4 False Positives

The false positive is defined as the detection probability of misbehaving nodes against the total number of nodes. It is always desirable to have very less number of false positives.

In Fig. 5, the comparison of false positives for FRT, QFRT, and QFRT-MBGA is shown. In this graph, the number of simulations is taken in x-axis and the number of false positives is taken in y-axis. It is observed that the QFRT-MBGA mechanism has reduced the number of false positives concerning the increased number of simulations.

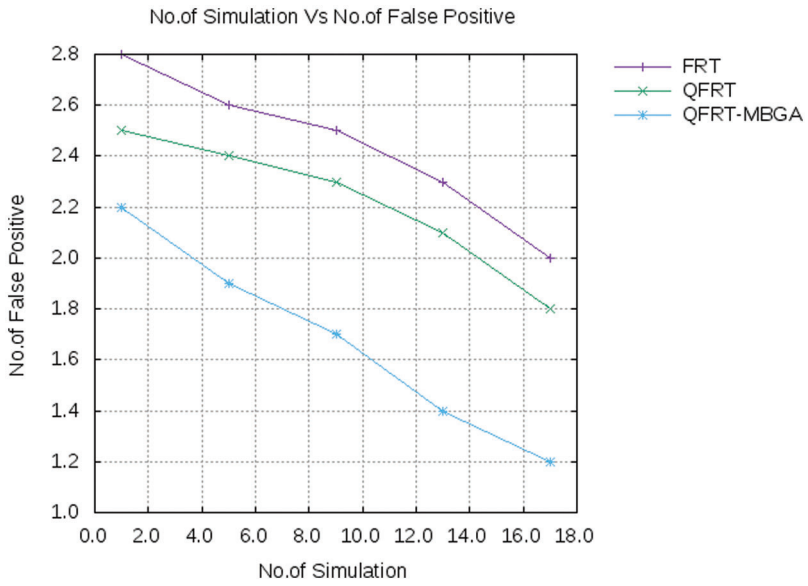

Figure 5: Number of simulation *vs.* number of false positives

5 Conclusion

In this research work, enhanced trust estimation is proposed with black/gray hole attack detection mechanism. In this mechanism, trust estimation is initially proposed for estimating each node's trust value during transmission. The trust estimation is done according to each node's reputation value, which is computed based on the fuzzy logic method. Moreover, QoS parameters such as node's energy, bandwidth, mobility and reliability are calculated and utilized for estimating the reputation and trust values. Then, the trust values' variations are measured to detect the black hole attacks presented in the routing path. Furthermore, the gray hole attacks are also detected and removed by considering the additional QoS metrics such as packet loss rate, packet delivery ratio, and delay with statistical measures of each node like mean, deviation, kurtosis, and skew. Then, the divergence between these statistical measures is estimated by using the KL divergence method. The estimated divergence values indicate that the behavioral changes of the node in the network. Based on these behavior changes, the gray hole nodes are detected. Thus the proposed mechanism prevents both black hole and gray hole attacks in the network during packet transmission. Finally, the simulation results prove that the proposed approach improves the packet delivery ratio and reduces the packet loss rate, delay effectively. Also this work is highly scalable to accommodate more nodes in the network. Future work will be directed towards scaling this work for different networks and with greater number of nodes without compromising on quality.

Acknowledgement: The authors wish to express their thanks to one and all who supported them during this work.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] R. Sharma and A. Panjeta, "A survey on trust-based mobile ad-hoc networks," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 6, no. 6, pp. 64–67, 2016.

[2] R. Vijayan and N. Jeyanthi, "A survey of trust management in mobile ad hoc networks," *International Journal of Applied Engineering Research*, vol. 11, no. 4, pp. 2833–2838, 2016.

[3] J. H. Cho, A. Swami and R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, pp. 562–583, 2011.

[4] N. R. Sirisala and C. S. Bindu, "A novel QoS trust computation in MANETs using fuzzy petri nets," *International Journal of Intelligent Engineering & Systems*, vol. 10, no. 2, pp. 116–125, 2016.

[5] T. H. Lacey, R. F. Mills, B. E. Mullins, R. A. Raines, M. E. Oxley *et al.,* "RIPsec–using reputation-based multilayer security to protect MANETs," *Computers & Security*, vol. 31, no. 1, pp. 122–136, 2012.

[6] J. Sengathir and R. Manoharan, "Exponential reliability coefficient based reputation mechanism for isolating selfish nodes in MANETs," *Egyptian Informatics Journal*, vol. 16, no. 2, pp. 231–241, 2015.

[7] P. Arunachalam, N. Janakiraman, J. Rashid, J. Kim, S. Samanta *et al.,* "Effective classification of synovial sarcoma cancer using structure features and support vectors," *Computers, Materials & Continua*, vol. 72, no. 2, pp. 2521–2543, 2022.

[8] B. Rajkumar and G. Narsimha, "Trust based certificate revocation for secure routing in MANET," *Procedia Computer Science*, vol. 92, no. 7, pp. 431–441, 2016.

[9] A. Shashank, R. Vincent, A. K. Sivaraman, A. Balasundaram, M. Rajesh *et al.,* "Power analysis of household appliances using IoT," in *Int. Conf. on System, Computation, Automation and Networking (ICSCAN)*, Puducherry, India: IEEE Xplore, pp. 1–5, 2021.

[10] R. Akbani, T. Korkmaz and G. V. Raju, "EMLTrust: An enhanced machine learning based reputation system for MANETs," *Ad Hoc Networks*, vol. 10, no. 3, pp. 435–457, 2012.

[11] Y. Liu, K. Li, Y. Jin, Y. Zhang and W. Qu, "A novel reputation computation model based on subjective logic for mobile ad hoc networks," *Future Generation Computer Systems*, vol. 27, no. 5, pp. 547–554, 2011.

[12] M. Ganga, N. Janakiraman, A. K. Sivaraman, A. Balasundaram, R. Vincent *et al.,* "Survey of texture based image processing and analysis with differential fractional calculus methods," in *Int. Conf. on System, Computation, Automation and Networking (ICSCAN)*, Puducherry, India: IEEE Xplore, pp. 1–6, 2021.

[13] A. Banerjee, S. Neogy and C. Chowdhury, "Reputation based trust management system for MANET," in *Emerging Applications of Information Technology (EAIT)*, India: IEEE, pp. 376–381, 2012.

[14] D. Kothandaraman, A. Balasundaram, R. Dhanalakshmi, A. K. Sivaraman, S. Ashokkumar *et al.,* "Energy and bandwidth based link stability routing algorithm for IoT," *Computers, Materials & Continua*, vol. 70, no. 2, pp. 3875–3890, 2021.

[15] B. Wang, X. Chen and W. Chang, "A lightweight trust-based QoS routing algorithm for ad hoc networks," *Pervasive and Mobile Computing*, vol. 13, no. 2, pp. 164–180, 2014.

[16] J. H. Cho and R. Chen, "On the tradeoff between altruism and selfishness in MANET trust management," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2217–2234, 2013.

[17] H. Xia, Z. Jia, X. Li, L. Ju and E. H. M. Sha, "Trust prediction and trust-based source routing in mobile ad hoc networks," *Ad Hoc Networks*, vol. 11, no. 7, pp. 2096–2114, 2013.

[18] N. Bhalaji and A. Shanmugam, "Dynamic trust based method to mitigate greyhole attack in mobile ad-hoc networks," *Procedia Engineering*, vol. 30, no. 6, pp. 881–888, 2012.

[19] P. Arunachalam, N. Janakiraman, A. K. Sivaraman, A. Balasundaram, R. Vincent *et al.,* "Synovial sarcoma classification technique using support vector machine and structure features," *Intelligent Automation & Soft Computing*, vol. 32, no. 2, pp. 1241–1259, 2021.

[20] E. Chiejina, H. Xiao and B. Christianson, "A dynamic reputation management system for mobile ad hoc networks," *Computers*, vol. 4, no. 2, pp. 87–112, 2015.

[21] S. Karthik, R. S. Bhadoria, J. G. Lee, A. K. Sivaraman, S. Samanta *et al.,* "Prognostic kalman filter based Bayesian learning model for data accuracy prediction," *Computers, Materials & Continua*, vol. 72, no. 1, pp. 243–259, 2022.

[22] M. Bidaki and M. Masdari, "Reputation-based clustering algorithms in mobile ad hoc networks," *International Journal of Advanced Science and Technology*, vol. 54, no. 2, pp. 1–12, 2013.

[23] E. Chiejina, H. Xiao and B. Christianson, "A Candour-based trust and reputation management system for mobile ad hoc networks," in *Proc. of the 6th York Doctoral Symp. on Computer Science & Electronics*, USA, pp. 283–298, 2013.

[24] A. Balasundaram, G. Dilip, M. Manickam, A. K. Sivaraman, K. Gurunathan *et al.,* "Abnormality identification in video surveillance system using DCT," *Intelligent Automation & Soft Computing*, vol. 32, no. 2, pp. 693–704, 2021.

[25] J. Sen, "A distributed trust and reputation framework for mobile ad hoc networks," *Recent Trends in Network Security and Applications*, vol. 23, no. 9, pp. 538–547, 2010.

[26] T. Eissa, S. A. Razak, R. H. Khokhar and N. Samian, "Trust-based routing mechanism in MANET: Design and implementation," *Mobile Networks and Applications*, vol. 18, no. 5, pp. 666–677, 2013.

[27] A. Balasundaram, M. Naveen Kumar, A. K. Sivaraman, R. Vincent and M. Rajesh, "Mask detection in crowded environment using machine learning," in *Int. Conf. on Smart Electronics and Communication (ICOSEC)*, Trichy, India*:* IEEE Xplore, pp. 1202–1206, 2021.

[28] M. Zhang, R. Zheng, Y. Li, Q. Wu and L. Song, "R-bUCRP: A novel reputation-based uneven clustering routing protocol for cognitive wireless sensor networks," *Journal of Sensors*, vol. 12, no. 8, pp. 332–345, 2016.

[29] V. Ulagamuthalvi, G. Kulanthaivel, A. Balasundaram and A. K. Sivaraman, "Breast mammogram analysis and classification using deep convolution neural network," *Computer Systems Science and Engineering*, vol. 43, no. 1, pp. 275–289, 2022.

[30] J. Luo, X. Liu, Y. Zhang, D. Ye and Z. Xu, "Fuzzy trust recommendation based on collaborative filtering for mobile ad-hoc networks," *LCN*, vol. 38, no. 12, pp. 305–311, 2008.

[31] D. Kothandaraman, M. Manickam, A. Balasundaram, D. Pradeep, A. Arulmurugan *et al.,* "Decentralized link failure prevention routing (DLFPR) algorithm for efficient internet of things," *Intelligent Automation & Soft Computing*, vol. 34, no. 1, pp. 655–666, 2022.

[32] S. V. Mallapur and S. R. Patil, "Fuzzy logic based trusted candidate selection for stable multipath routing," *International Journal of Information Technology and Computer Science (IJITCS)*, vol. 7, no. 6, no. 12, pp. 837–843, 2015.

[33] P. Sathya and C. Suguna, "Divergence based selfish nodes detection approach in MANET," *International Journal of Future Innovative Science and Engineering Research*, vol. 2, no. 2, pp. 81–88, 2016.

[34] X. R. Zhang, X. Chen, W. Sun and X. Z. He, "Vehicle re-identification model based on optimized densenet121 with joint loss," *Computers, Materials & Continua*, vol. 67, no. 3, pp. 3933–3948, 2021.

[35] X. R. Zhang, W. F. Zhang, W. Sun, X. M. Sun and S. K. Jha, "A robust 3-D medical watermarking based on wavelet transform for data protection," *Computer Systems Science & Engineering*, vol. 41, no. 3, pp. 1043–1056, 2022.

[36] B. Yin, S. W. Zhou, S. W. Zhang, K. Gu and F. Yu, "On efficient processing of continuous reverse skyline queries in wireless sensor networks," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 4, pp. 1931–1953, 2017.

[37] J. M. Zhang, K. Yang, L. Y. Xiang, Y. S. Luo, B. Xiong *et al.,* "A self-adaptive regression-based multivariate data compression scheme with error bound in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 9, no. 3, pp. 913497, 2013.

[38] J. Wang, C. Ju, Y. Gao, A. K. Sangaiah and G. J. Kim, "A PSO based energy efficient coverage control algorithm for wireless sensor networks," *Computers Materials & Continua*, vol. 56, no. 3, pp. 433–446, 2018.

[39] J. Wang, X. J. Gu, W. Liu, A. K. Sangaiah and H. J. Kim, "An empower hamilton loop based data collection algorithm with mobile agent for WSNs," *Human-centric Computing and Information Sciences*, vol. 9, no. 1, pp. 1–14, 2019.

[40] J. Wang, Y. Gao, C. Zhou, S. Sherratt and L. Wang, "Optimal coverage multi-path scheduling scheme with multiple mobile sinks for WSNs," *Computers, Materials & Continua*, vol. 62, no. 2, pp. 695–711, 2020.

[41] J. Wang, Y. Gao, W. Liu, W. Wu and S. J. Lim, "An asynchronous clustering and mobile data gathering schema based on timer mechanism in wireless sensor networks," *Computers Materials & Continua*, vol. 58, no. 3, pp. 711–725, 2019.

[42] J. Wang, Y. Gao, X. Yin, F. Li and H. J. Kim, "An enhanced PEGASIS algorithm with mobile sink support for wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 31, no. 7, pp. 239–252, 2018.

[43] Q. Tang, K. Yang, P. Li, J. M. Zhang, Y. S. Luo *et al.,* "An energy efficient MCDS construction algorithm for wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 12, no. 5, pp. 132–147, 2012.

[44] Z. Liao, J. Wang, S. Zhang, J. Cao and G. Min, "Minimizing movement for target coverage and network connectivity in mobile sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 7, pp. 1971–1983, 2014.