Received: May 21, 2021. Revised: June 24, 2021.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Gaussian Trust Factor-based Grey Decision Making Technique (GTF-GDMT) for Node Cooperation Enforcement in MANETs

Srinivasulu Sirisala[1]* **S. Rama Krishna[1]**

[1]*Department of Computer Science, SVU College of CM&CS, Tirupathi, India*
* Corresponding author's Email: vasusirisala@gmail.com

Abstract: The successful routing in Mobile Ad hoc Networks (MANETs) completely depends on the cooperation established between the mobile nodes during data dissemination. The resource constraint feature of mobile nodes is the main reason behind its non-cooperativeness attributed towards other interacting nodes of the network. This degree of non-cooperation rendered by the mobile node disturbs the routing and degrades the network performance. Thus, a node cooperation enforcing approach that distinguishes genuine node from malicious node is essential for sustaining the network performance. In this paper, Gaussian Trust Factor-based Grey Decision-Making Technique (GTF-GDMT) is proposed for maintaining the network performance independent to the influence of non-cooperative malicious nodes. This proposed GTF-GDMT identified the malicious nodes based on the trust factor that integrates the parameters of link stability and node reputation determined through direct and indirect monitoring process. This computation of trust is achieved using the Gaussian probabilistic distribution model that utilizes multi-perspective parameters that forms the input to the decision-making process. It is proposed for attaining the trade-off between energy consumption, transmission performance and security. The simulation experiments of the proposed GTF-GDMT conducted using ns-2 portrayed its excellence over the baseline schemes in terms of throughput, packet delivery rate, packet delay, energy consumptions and packet drop independent to the number of mobile nodes and malicious nodes in the network.

Keywords: Mobile ad hoc networks (MANETs), Gaussian trust factor, Grey decision making, Malicious nodes, Node cooperation.

1. Introduction

These Mobile ad hoc Networks comprise of multiple cooperating nodes that possesses self-organizing potential and restricted energy. This MANETs are commonly used in the applications of remote area exploration, rescue and disaster relief and military communications, and so on [1]. They possess the significance of mobility, safety and flexibility during the process of communication [2]. Further, MANETs necessitates a collection of cooperating nodes that self organizes them into the network with the view to interact with one another for achieving the common goal of guaranteeing operable and reliable communication [3]. In this context, the packet forwarding process widens the range of data transmission above the one-hop networks among all the cooperative behaviors of mobile nodes [4]. However, the mobile nodes generally possess restricted resources and, in some circumstance, may exhibit selfish behaviors. From the recent past, secured routing is determined to be one of the major challenges in MANETs [5]. The malicious nodes' behavior in the network elevates the risks of threats that induce the possibility of uncertain operations in MANETs [6]. This selfish behavior of mobile nodes is a special case in which a rational node may resist the process of packet forwarding for attaining its own benefit. This irrational behavior of mobile nodes greatly damages the performance of the network communication [7]. At this juncture, the adoption of a potential packet forwarding strategy among the mobile nodes is considered to be highly crucial. Moreover, adoption of significant packet forwarding strategy has the

possibility of enhancing the probability of successful transmissions under unreliable channels [8]. It also has the feasibility of minimizing the energy consumptions of the mobile nodes in order to extend the lifetime of the network.

At this juncture, the packet forwarding strategies need to monitor the behavior of mobile nodes based on direct and indirect interactions for the purpose of determining the selfish and malicious characteristics of mobile nodes cooperating in the routing path. The direct interaction refers to the process of interacting with the mobile node in order to determine its behavior from itself for a period of time [9]. On the other hand, indirect interaction represents the method of determining the behavior of mobile nodes through their neighbours which are cooperating with them for a specific amount of time. Thus, the cooperation degree among the mobile nodes needs to be sustained through potential mitigation of malicious and selfish mobile nodes in the network with maximized optimality [10]. From the recent decades, a diversified number of cooperation enforcing approaches based on acknowledgement, probabilistic distribution-based trust and reputation, watchdog and game theory were contributed in the literature for potential mitigation of malicious nodes. Among them, probabilistic distribution-based trust and reputation approaches were identified to have an upper edge compared to the other malicious node mitigation approaches of the literature [11]. This probability distribution-based trust and reputation approaches is also confirmed to be highly significant for sustaining cooperation among the mobile nodes for the objective of preventing network degradation. Moreover, the Grey decision theory is one of the predominant decision making strategy that helps in not only analyzing the current behaviour of mobile nodes, but also aids in predicting the future behaviour of mobile nodes to a maximized level. In addition, it is also confirmed that the estimation of trust factor through Gaussian distribution enhances the prediction accuracy of the Grey decision process to the utmost level.

In this paper, Gaussian Trust Factor-based Grey Decision-Making Technique (GTF-GDMT) is proposed for enforcing cooperation among the mobile nodes with the objective of sustaining network lifetime and performance. The simulation experiments of the proposed GTF-GDMT and the benchmarked approaches are conducted using ns-2 in order to determine their excellence in terms of throughput, packet delivery rate, packet delay, energy consumptions and packet drop independent to the number of mobile nodes and malicious nodes in the network.

The major contributions of the proposed GTF-GDMT are listed as follows.

i. It utilizes the past, present and future exploration behaviour of each mobile node into account and models them into the trust factor through the merits of Gaussian distribution.
ii. It is proposed for mitigating malicious nodes based on the computation of Gaussian distribution-based trust factor through the combination of link stability and node reputation factors attained through direct and indirect monitoring process.
iii. It facilitates the option of trust computation using the Gaussian probability distribution model that utilizes multi-perspective parameters that forms the input to the decision-making process for the purpose of achieving the trade-off between energy consumption, transmission performance and security.

The remaining section of the paper is organized as follows. Section 2 presents the literature review of the recently proposed node cooperation enforcement schemes with their merits and limitations. Section 3 depicts the complete view of the proposed GTF-GDMT with its significance in improving network performance and lifetime. Section 4 demonstrates the simulation results and investigation of the proposed GTF-GDMT and the competitive approaches with the reasons behind their predominant performance. Section 5 concludes the paper by highlighting the major contributions of the proposed scheme and feasible scope of improvement that can help to extend its dimensions of exploration.

2. Related work

An improved trust-based cooperation enforcing scheme was proposed Manoranjini et al. [12] for enhancing the probability of detecting and preventing malicious nodes in the network. This cooperation enforcing approach included different trust metrics for estimating the behavior of each mobile node completely depending on the association determined between the mobile nodes. It included the merits of QoS metric trusts, service attribute trusts and social attribute trusts for deciding about the genuineness of mobile nodes rendered during their interaction process. It also provided and retained data privacy during its performance testing attained in different scenarios with respect to with and without trusts evaluated in diversified dimensions. The results of this trust-based cooperation enforcing scheme exhibited better performance in terms of missed detection rate, false

acceptance rate, trust level, energy consumption, packet loss and overall throughput. The level of cooperation rendered by this approach was only up to a marginal level. The control and total overhead of this trust scheme was comparatively higher than the competitive approaches. Then, a Reputation Management Scheme using Hierarchical account was proposed with incentive strategy by Shen and Li. [13] for achieving a better network lifetime and a success rate of data transfer. This reputation approach constructed a distributed hash table with locality awareness for ensuring the integrated and potential operation of price sand reputation and price systems. This framework aided in global elucidation of reputation information pertaining to each node for establishing the detection of abnormal reputation information that might be attributed by each mobile node in the network with maximized accuracy. This framework also enabled the combination of pricing and reputation for enforcing maximized reputation node to pay less for their acquired services. This pricing strategy was not exhaustive, resulting in biased behavior of malicious nodes in the network. The throughput and detection rate facilitated by this RMS scheme was only substantial.

Further, Thorat et al. [14] proposed an uncertain exploration framework for computing the dimension of uncertainty, disbelief and belief values that are highly required during the process of enforcing cooperation under data dissemination. This framework combined different dimensions of trust such as global trust, direct and indirect trust together in determining the genuineness of the mobile nodes during data dissemination. It discovered different influences of trust models with respect to different mobility models considered for investigation. The experimental investigation confirmed an improvement in packet delivery rate of 3.48% and the network belief by 5.64%, compared to the existing trust-based routing protocols considered for analysis. This belief-based approach was not able to contextually apply the weights during the trust estimation process.

An Energy and Security-Aware Routing Scheme (ESARS) was proposed by Ali and Prasad [15] for reducing the complexity of communication incurred under selfish behaviour of mobile nodes during the process of data delivery. This security aware routing approach guarantees that genuineness of each and every node and thereby isolates the malicious nodes in the routing path with a rapid speed. This approach also utilized the benefits of self-configurable runs for all the mobile nodes such that the restricted energy sources can be optimally used in the routing process. It failed to incorporate complete set of exhaustive influential factors that attribute towards reliable data dissemination process. Garg et al. [16] proposed Fuzzy Rule-based Cooperation Enforcing Scheme (FRCES) for handling the issue of mobility and dynamic change in characteristics that hurdle their performance in the dimension of secure routing. This FRCES included the route stability into account in order to prevent frequent link breaks in the paths that are established between the source and destination mobile nodes. This approach was proposed with the merits of the existing AODV protocol, which is extended for constructing a secure path between the source and destination nodes. This fuzzy approach was completely proposed based on the values of Length of Trust and Trust Values for securing the route of data dissemination. It was also propounded for easy elimination of malicious nodes with the help of the trust values that confirm better trusted route in the network. The rate of malicious node detection facilitated by this FRCES is still marginal and requires the capability of more updating process during cooperation environment.

Furthermore, Feature Extraction-based Intruder Node Detection and Isolation Mechanism (FS-INDISM) was proposed by Kavitha et al. [17] for attaining secure routing and cooperation in the network. It utilized the benefits of feature extraction, optimization and classification for discriminating malicious nodes from genuineness nodes. In particular, the features corresponding to direct and indirect trust features are determined from each mobile node in order to estimate the features of trust that optimally combines them during the isolation process of malicious nodes in the routing path. This approach specifically optimized the trust features associated with each mobile node based on the optimization algorithm of particle swarm optimization (PSO) as the potential optimization technique. This approach also used the merits of Neural Network (NN) as the classifier that aided n precise identification of intruder nodes. The performance of this FS-INDISM was determined in terms of communication delay, energy consumptions and packet delivery success rate to assess its potential towards better malicious node isolation during data dissemination. A Subjective Trust Framework (STF) was proposed by Xia et al. [18] with the merits of least computation involved in the trust assessment and prediction process. It included the historical behaviour of nodes into account in the trust assessment for determined the sequence of trust data. It facilitated the prediction of node's trust based on a weighted Markov Chain (SCGM) measure that aided in better futuristic

decision-making process. It was developed based on the baseline on-demand routing protocol (ODMRP), which is improved by considering the trust into account. The results of FS-INDISM and STF confirmed its importance in successful packet delivery, throughput, network delay and control overhead. However, the prediction accuracy of this SCGM was 95.45% and hence, it still possesses a room of improvement.

In addition, Secure Routing using Energy Efficiency Framework (SREEF) was proposed by Ponguwala and Rao [19] for guaranteeing data integrity and security in ad hoc networks. This SREEF adopted an authentication scheme that included the benefits of certificate-based hash chain. It included the cluster formation of cluster integrated with secure verification process in order to enable the process of elliptic curve verification. It included the benefits of worst case PSO-based secure routing for security enhancement through the model of dual state Markov chain model. It also included a dual XOR-based Fuzzy Evaluating Cipher Encryption algorithm for guaranteeing maximized data integrity. This SREEF was considered to enhance the network performance in terms of packet delivery successful rate, residual energy and throughput compared to the benchmarked approaches.

3. Proposed gaussian trust factor-based grey decision-making technique (GTF-GDMT)

The GTF-GDMT is proposed based on the determination of direct and indirect trust modelled through the Gaussian distribution model. This Gaussian distribution model completely depends on the successful and the failed interactions possible between any mobile nodes existing in between the routing path established between the source and destination nodes. This proposed scheme derived the benefits of the Grey decision process that considers Gaussian distribution-based trust as the input in order to determine the degree of genuineness rendered by the mobile nodes during the data routing process. In this section, the detailed view of the proposed GTF-GDMT is presented as follows.

If there is an interaction between a node 'i' and node 'j' in the present mobile ad hoc network environment. Then, the node 'i' computes the trust value of and node 'j' in order to confirm the decision of interacting with it. Initially, the mobile node computes the direct trust value of node 'i' through the estimation of historical interaction information with respect to node 'j'. Further, the neighbor node of the mobile node 'j' is queried for determining the trust value of that node for the purpose of computing its indirect trust. Moreover, the direct and indirect trust is integrated for estimating the overall trust value of a specific mobile node. In this context, when the node 'i' and node 'j' interact with each other (c+d) times, then the number of successful and unsuccessful interactions visualized at a specific amount of time follows a Gaussian distribution [20] based on Eq. (1)

$$N=\left(\frac{c}{c+d},\frac{cd}{(c+d)^2}\right) \tag{1}$$

Where, 'c' and 'd' represents the number of successful and unsuccessful interactions.

3.1 Gaussian distribution-based modelling and updating of direct trust

Once the complete information associated with interactions is known, the trust value determined is modelled based on Gaussian Distribution. This modelling of trust value through the Gaussian distribution consists of expectation and variance presented in Eq. (2) and (3).

$$u=\sqrt{\frac{cd}{(c+d)^2}} \tag{2}$$

$$v=\frac{c}{(c+d)} \tag{3}$$

In this context, the distribution of reputation associated with the mobile node 'i' in relation to node 'j' is $R_{D(ij)}\sim N(\mu_J,\sigma_J^2)$. At this juncture, $\mu_{ij}\sim N(u^2,v)$ is the parameter of prior distribution represented through $(R_{D(ij)})_1,(R_{D(ij)})_2,.....(R_{D(ij)})_t$. Moreover, the Gaussian distribution-based reputation considered in the proposed model as is initialized through $N(0.5, 0.25)$.

3.2 Transfer of trust

If the mobile node 'i'and node 'j' is interacting ($c+d$) times, then the parametric conditional density ($P_{Cd}(\mu_J)$) in a time duration 't' are represented through Eq. (4)

$$P_{Cd}(\mu_J)=\frac{1}{\sqrt{2\pi\sigma_t^j}}exp(-\frac{\sum_{i=1}^{n}((X_i)_n-\mu_j)^2}{2\sigma_j^2}) \tag{4}$$

Where, the prior distribution $P_{Dist}(\mu_j)$ is estimated based on Eq. (5)

$$P_{Dist}(\mu_j)=\frac{1}{\sqrt{2\pi}u}\,exp\,(-\frac{(\mu_j-v)^2}{2u^2}) \quad (5)$$

At this juncture, the density of the posterior distribution is represented through Eq. (6).

$$\pi(\mu_j||((X_i)_1,(X_i)_2,(X_i)_3,....,(X_i)_n))=C\,exp\,(-\frac{(\mu_j-s)^2}{2\pi^2}) \quad (6)$$

Where, the value of 'π' and 's' is determined based on Eq. (7) and (8), respectively.

$$\pi=\frac{1}{\frac{1}{\delta_{ij}^2}+\frac{1}{u^2}} \quad (7)$$

$$s=\frac{(\frac{1}{\delta_{ij}^2}\bar{X}+\frac{1}{u^2})}{(\frac{1}{\delta_{ij}^2}+\frac{1}{u^2})} \quad (8)$$

Where, 'C' is the constant which is completely independent compared to the parameter of conditional density μ_j. It is also identified that density of the posterior distribution (π_j) is also satisfies the Gaussian distribution as similar to the parameter of conditional density μ_j.

In this situation, when the initial setting time is t=1, then the number of successful and failure interactions is determined to be unity with $\sigma_j=0.25$ and $\mu_j=0.50$ satisfying the properties of normal distribution ($N(0.5,0.25)$).

$$E=\frac{1}{\sigma_j}=\frac{1}{0.25} \quad (9)$$

$$F=\frac{(c+d)}{d} \quad (10)$$

$$G=\frac{(c+d)^2}{cd} \quad (11)$$

Where, $\bar{X}$ represents the mean number of successful interactions for the cumulative number of observations up to the preceding time slots to the total number of interactions (successful and failed) is represented in Eq. (12)

$$T_D=\frac{E\,\bar{x}+F}{E+G} \quad (12)$$

Further, the direct trust is defined through the utilized mathematical model developed based on the expectation of the Gaussian distribution is determined based on Eq. (13).

$$T_{Direct(i)}=Mean(\mu_j)=c \quad (13)$$

Moreover, the past observation and weightage associated with the age of the direct interaction is determined based on Eqs. (14) and (15)

$$S_{Int(ij)}^{New}=\alpha S_{Int(ij)}+1 \quad (14)$$

$$F_{Int(ij)}^{New}=\beta F_{Int(ij)}+1 \quad (15)$$

Where, $S_{Int(ij)}$ and $F_{Int(ij)}$ represents the count of successful and failed interactions identified as the specific point of time. α and β are used for incorporating weights in the computation of aging factors.

3.3 Decision on trust

In the process of deciding about trust, the method of grey theory is considered to be ideally suited for exploring the problems that involve bad information and small samples. It is determined to be frequently utilized for decision making in a context, where the limitation amount of information is available in the application. This grey theory-based trust, computed under the decision process attained even under limited information is considered to be quantitative in characteristics. While, fuzzy set-based trust factor is identified to be qualitative in property due to its capability in handling the issue of uncertainty. Hence, the proposed GTF-GDMT includes the merits of grey theory due to its quantitative nature as a trust factor estimated in a specific situation need to be more quantitative rather than qualitative. In specific, Grey theory is utilized for arranging the mobile nodes in the interaction process based on the quantitative characteristics for attaining the objective of selecting the neighbouring mobile nodes that are more reliable in data packet forwarding. Moreover, the trust management is integrated based on Grey-based decision-making process specified in [24] for initializing the parameters as specified below. In this proposed GTF-GDMT scheme, the input such as hops and trust value as transformed into input parameters as the input considered in the process of grey decision is linguistic in nature. Therefore, the input is converted into a Grey number by integrating the real values for attaining maximized decisions through the inclusion of Grey-based decision making. In addition, this proposed scheme inherits a novel strategy of gray likelihood [25] which is predominantly used for ranking the preference of candidates (mobile nodes under routing). This gray

likelihood strategy is also determined to be highly ideal for solving the problems associated with decision making that incurs maximized uncertainty.

In the network environment, the set of independent k candidates (mobile nodes) $M_n=\{M_{n(1)},M_{n(2)},M_{n(3)},....M_{n(k)}\}$ is assumed to be randomly deployed. The set of 'm' candidate attributes is considered in estimating the trust of independent k candidates (mobile nodes). However, the candidate attribute considered for evaluation is considered to be additive and independent. In this context, the candidate attributes considered for evaluation are packet forwarding rate, energy utilization, network coverage and mobility degree of mobile nodes. Moreover, attribute weight vector is also considered during the process of trust-based decision-making process. In the proposed GTF-GDMT scheme, the candidate (mobile nodes) ratings and weights of attributes is considered to be linguistic variable. At this juncture, Table 1 and 2 depicts the weights of attribute and achieved trust ratings that are respectively presented through the fractional range of 0-1 and integer interval of 0-10.

The complete steps involved in the proposed GTF-GDMT are detailed as follows.

Step 1: Estimate the candidate (mobile nodes) attribute weights by assuming a group of 'r' decision makers (each mobile node being monitored by different number of neighboring nodes in a time period) based on Eq. (16)

$$A_{W(Mn(ij))}=\frac{1}{r}\left[A^{1}_{w(Mn(ij))}+A^{2}_{W(Mn(ij))}+.....+A^{r}_{W(Mn(ij))}\right] \quad (16)$$

Table 1. Range of attribute weights

Attribute weights	Range
[0.0,0.1]	Very Low (VL)
[0.1,0.3]	Low (L)
[0,3,0,4]	Medium Low (ML)
[0.4,0.5]	Medium (M)
[0.5,0.6]	Medium High (MH)
[0.6,0.9]	High (H)
[0.9,1.0]	Very High (VH)

Table 2. Range used for attribute evaluation

Grade	Range
[0, 1]	Very Poor (VP)
[1, 3]	Poor (P)
[3, 4]	Medium Poor (MP)
[4, 5]	Medium (M)
[5, 6]	Medium Good (MG)
[6, 9]	Good (G)
[9, 10]	Very Good (VG)

Where, $A^{r}_{W(Mn(ij)}$ ($1\leq j\leq r$) represents the attribute weights corresponding to 'r^{th}' decision makers. It is represented in the grey numbers $A^{r}_{W(Mn(ij)}=[A^{r}_{W(Mn(ij)-Min},A^{r}_{W(Mn(ij)-Max}]$.

Step 2: Determine the values of attribute rating through the use of linguistic variables as specific in Eq. (17).

$$H_{W(Mn(ij))}=\frac{1}{r}[H^{1}_{w(Mn(ij))}+H^{2}_{W(Mn(ij))}+.....+H^{r}_{W(Mn(ij))}] \quad (17)$$

Where, $H^{r}_{W(Mn(ij)}$ ($1\leq j\leq r$) represents the values of attribute ratings corresponding to 'r^{th}' decision makers. It is represented in the grey numbers $H^{r}_{W(Mn(ij)}=[H^{r}_{W(Mn(ij)-Min},H^{r}_{W(Mn(ij)-Max}]$.

Step 3: Construct a Grey decision matrix as presented in Eq. (18)

$$G_{DM}=\begin{vmatrix} H_{11} & H_{12} & ..... & H_{1k} \\ H_{21} & H_{22} & ..... & H_{2k} \\ . & . & ..... & . \\ . & . & & . \\ H_{r1} & H_{r2} & ..... & H_{rk} \end{vmatrix} \quad (18)$$

Where, $H_{(ij)}$ is the linguistic variable determined based on gray numbers.

Step 4: Perform normalization operation over the constructed Grey decision matrix as presented in Eqs. (19) to (21)

$$G_{DM}=\begin{vmatrix} H^{N}_{11} & H^{N}_{12} & ..... & H^{N}_{1k} \\ H^{N}_{21} & H^{N}_{22} & ..... & H^{N}_{2k} \\ . & . & ..... & . \\ . & . & & . \\ H^{N}_{r1} & H^{N}_{r2} & ..... & H^{N}_{rk} \end{vmatrix} \quad (19)$$

$$H^{N}_{ij}=\left[\frac{H_{ij}}{H^{N(Max)}_{ij}},\frac{\bar{H}_{ij}}{H^{N(Max)}_{ij}}\right] \quad (20)$$

$$H^{N(Max)}_{ij}=\underset{1\leq i\leq n}{Max}\{\bar{H}_{ij}\} \quad (21)$$

If the attribute considered for observation refers to the cost attribute, then the cost incurred in data dissemination need to be reduced based on Eqs. (22) and (23).

$$H^{N}_{ij}=\left[\frac{H^{N(Min)}_{ij}}{H_{ij}},\frac{H^{N(Min)}_{ij}}{\bar{H}_{ij}}\right] \quad (22)$$

$$H_{ij}^{N(Min)} = \underset{1 \le j \le n}{Min}\{\bar{H}_{ij}\} \quad (23)$$

Step 5: Determine a Grey decision matrix based on weighted normalization by utilizing different weights to each attribute into consideration as specified in Eqs. (24) and (25).

$$DG_{\&(WN)} = \begin{vmatrix} DG_{11}^{N} & DG_{12}^{N} & ..... & DG_{1k}^{N} \\ DG_{21}^{N} & DG_{22}^{N} & ..... & DG_{2k}^{N} \\ . & . & & . \\ . & . & ..... & . \\ . & . & & . \\ DG_{r1}^{N} & DG_{r2}^{N} & ..... & DG_{rk}^{N} \end{vmatrix} \quad (24)$$

$$DG_{(WN))ij)} = H_{ij}^{N} * W_{ij} \quad (25)$$

Step 6: Select a reference based on the concept of ideal choice of the possible number of candidate mobile nodes initialized to $G_{N(ID)} = \{G_{N(1)}, G_{N(2)}, ..., G_{N(n)}\}$ based on Eq. (26)

$$G_{NiID)}^{Max} = \{Max[DG_{WN(ij)}(G_{N(1)}, G_{N(2)}, ..., G_{N(n)})]\} \quad (26)$$

Step 7: The degree of likelihood is calculated among the mobile node candidates under comparison and the referenced candidate presented in Eq. (27)

$$P(G_{N(i)} \le G_{N(ID)}^{Max}) = \frac{1}{n} \sum_{j=1}^{n} P(G_{DM} \le G_{N(j)}^{Max}) \quad (27)$$

Step 8: Sort the candidates (mobile node potential) in increasing order but, when the condition $P(G_{N(i)} \le G_{N(ID)}^{Max})$ is minimized, then order of ranking need to be higher. Otherwise, order of ranking is determined to be lower.

Based on the aforementioned procedure, the order of ranking associated with the complete set of candidate mobile nodes can be determined and best mobile nodes are determined as highly trustworthy and the mobile nodes with least rank is identified as malicious node and isolated from the routing path. In addition, the flowchart of the proposed GTF-GDMT scheme in Fig. 1 is presented as follows.

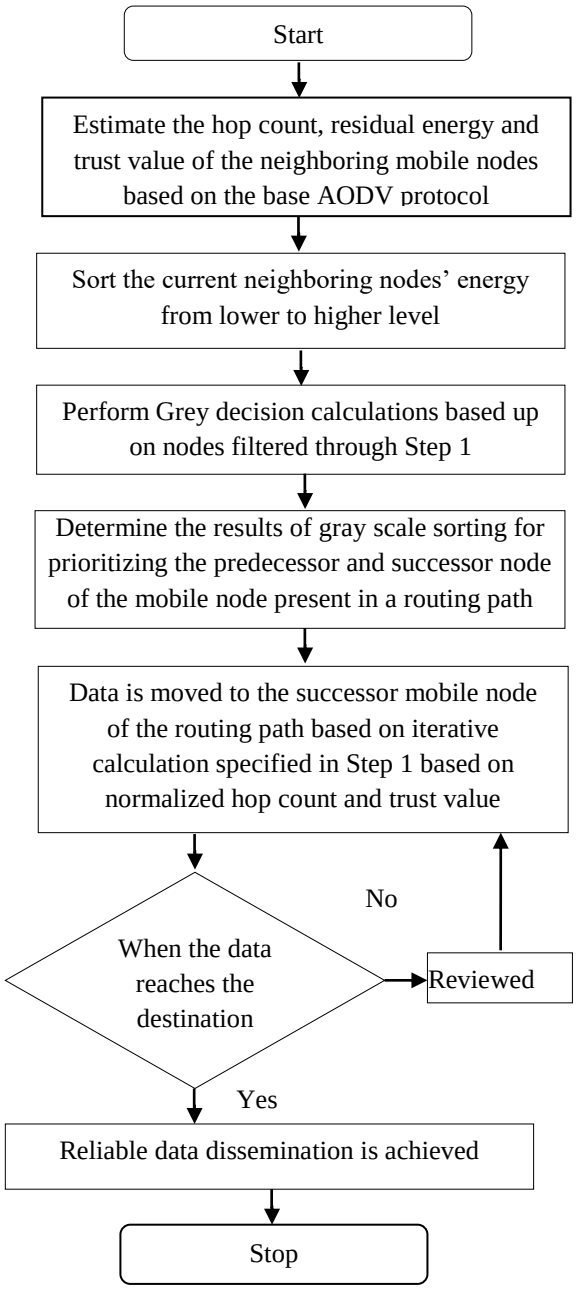

Figure. 1 Flowchart depicting the implementation process of the proposed GTF-GDMT in a specific routing path

4. Simulation results and discussion

The performance of the proposed GTF-GDMT and the benchmarked FS-INDISM [17], SREEF [19] and FRCES [16] approaches are evaluated based onthe simulation conducted using ns-2.34 network simulator. In this simulation process, the MANET architecture is supported through the extensive use of AODV protocol [21-23]. This AODV protocol is used as the base protocol for the complete routing process as it is considered as one of the most widely renowned reactive protocols over which dynamic decision process can be achieved. The simulation environment of the proposed GTF-GDMT scheme comprises of 100 mobile nodes that randomly move around the terrain area of 1000 x1000 square meters. Among the 100 mobile nodes, the malicious nodes are varied from 5 to 50 in order to explore its impact on the implementation process of the proposed GTF-GDMT approach. The malicious nodes are made to drop the packets with a

packet dropping rate that ranges between 60% and 80%. In this simulation, source and destination

Table 3. Simulation parameters used in implementing GTF-GDMT scheme

Simulation parameters	**Values considered**
Number of mobile nodes	100
Base protocol used for routing	AODV protocol
Simulation time	13.45 minutes
Number of source and destination pairs	40
Packet dropping rate of mobile nodes	60%-80%
Size of the packets	512 Bytes
Pause time	50 Seconds
Mobility rate of nodes	15 meters per second
Area of simulation	1000 x1000 square meters
Range of transmission	250 meters
Capacity of transmission	2 Kbps
Node mobility model	Random Way Point model
Data traffic model	Constant Bit Rate (CBR)

node pairs, accounting to 40 are used for maintaining direct cooperation among the mobile nodes of the network. The traffic model and pause time considered for the simulation are constant bit rate (five packets per second as the constant flow rate) and 50 seconds, respectively. The complete simulation time considered for the implementation of the proposed GTF-GDMT scheme is 13.45 minutes. In addition, the simulation parameters considered for implementing the proposed GTF-GDMT scheme is presented in Table 3.

The comparative investigation of the proposed GTF-GDMT and the benchmarked FS-INDISM, SREEF and FRCES approaches are achieved with different number of mobile nodes, malicious nodes and increasing time of simulation. Initially, the proposed GTF-GDMT and the benchmarked FS-INDISM, SREEF and FRCES approaches are compared with respect to different number of mobile nodes.

Fig. 2 and 3 highlights the performance of the proposed GTF-GDMT and the baseline FS-INDISM, SREEF and FRCES approaches evaluated with respect to packet delivery rate and detection rate. The packet delivery rate of the proposed GTF-GDMT and the benchmarked approaches were visualized to get reduced with the number of mobile nodes. This decrease in the packet delivery rate is mainly due to the huge number of packets generated by the increasing number of mobile nodes and the necessity that enforces them to forward an increased number of data packets to their neighbors. However, the packet delivery rate of the proposed GTF-GDMT is kept up to the maximum level, even when

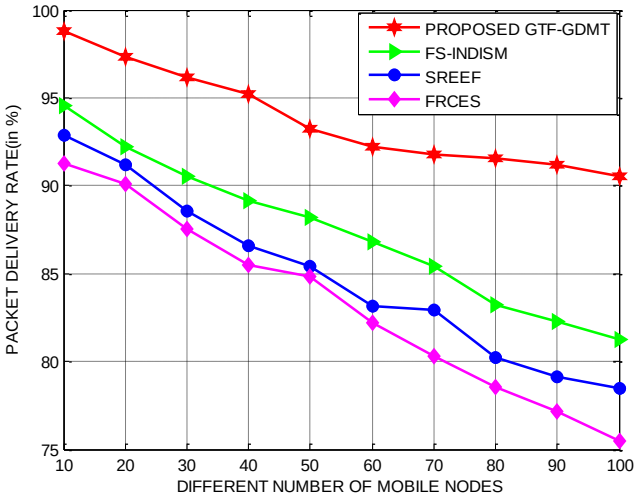

Figure. 2 Proposed GTF-GDMT-Packet delivery rate with different number of mobile nodes

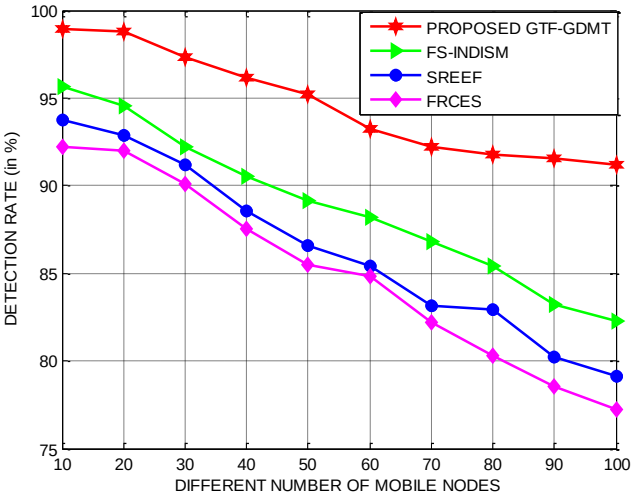

Figure. 3 Proposed GTF-GDMT-Detection Rate with different number of mobile nodes

the number of packets generated and need to be forwarded by the mobile nodes increases compared to the baseline schemes. The packet delivery rate of the proposed GTF-GDMT is determined to be improved by 12.38%, 14.91% and 17.74%, superior to the benchmarked FS-INDISM, SREEF and FRCES approaches.

Fig. 4 and 5 demonstrates the energy consumptions and the mean delay attained by the proposed GTF-GDMT and the benchmarked FS-INDISM, SREEF and FRCES approaches with different number of mobile nodes. The energy consumptions and the mean delay of the proposed GTF-GDMT and the benchmarked schemes is identified to get decreased with an increase in the number of malicious nodes as the number of packets dropped and time incurred for forwarding the original and the re-transmitted packets get increases in the network. However, the proposed GTF-GDMT

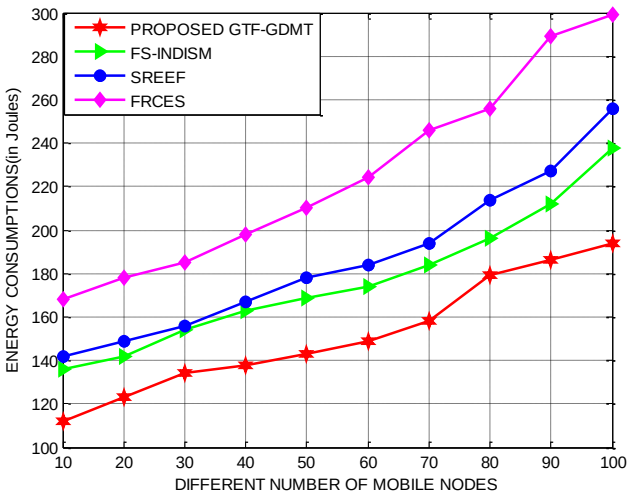

Figure. 4 Proposed GTF-GDMTEnergy Consumption with different number of mobile nodes

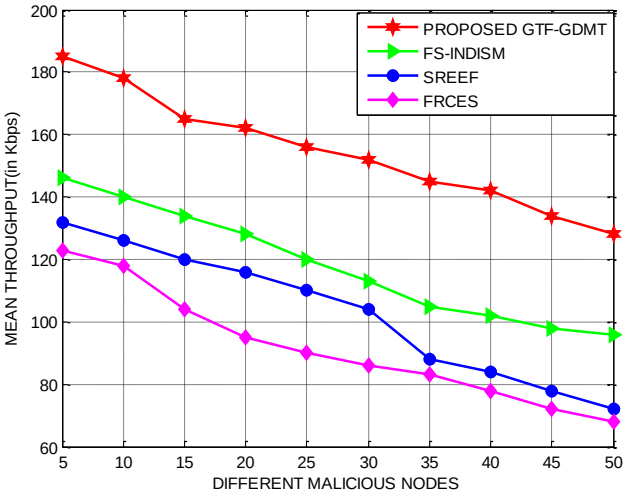

Figure. 6 Proposed GTF-GDMT-Mean Throughput with different number of malicious nodes

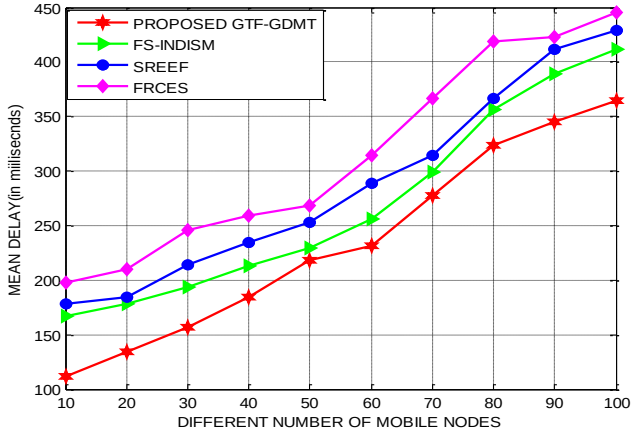

Figure. 5 Proposed GTF-GDMT-Mean Delay with different number of mobile nodes

adopted a flexible strategy inspired with the Gaussian trust factor and rapid detection rate that considerably gets enhanced depending in the number of malicious nodes gets introduced into the network scenario. The energy consumptions of the proposed GTF-GDMT with increasing mobile nodes is minimized by 11.28%, 13.84% and 15.82%, superior to the benchmarked FS-INDISM, SREEF and FRCES approaches. Likewise, the mean delay attained by the proposed GTF-GDMT with increasing mobile nodes is also reduced by 10.84 %, 12.19 % and 15.19 %, superior to the benchmarked FS-INDISM, SREEF and FRCES approaches.

Further, the potential of the proposed GTF-GDMT and the benchmarked FS-INDISM, SREEF and FRCES are explored based on mean throughput mean energy consumptions and the mean delay with respect to different number of malicious nodes.

Fig. 6 presents the mean throughput determined by the proposed GTF-GDMT and the benchmarked FS-INDISM, SREEF and FRCES approaches with different number of malicious nodes. The mean throughput of the proposed GTF-GDMT is estimated to get systematically decreased with respective increase in the number of malicious nodes. This systematic decrease in the mean throughput is mainly due to the number of packets dropped either intentionally or selfishly by the malicious mobile nodes growing in the network. However, the proposed GTF-GDMT is capable of maintaining the mean throughput to an acceptable level compared to the benchmarked FS-INDISM, SREEF and FRCES. This capability in maintaining mean throughput by the proposed GTF-GDMT is mainly due to the Gaussian trust factor that included the aging parameter and current operating behavior of mobile nodes into account. On the other hand, Fig. 7 presents the mean delay of the proposed GTF-GDMT and the benchmarked FS-INDISM, SREEF and FRCES techniques. The mean delay of all techniques is visualized to increase with respective increase in the number of malicious mobile nodes in the network, since the increase in the number of malicious nodes correspondingly increases the rate of packet drop that unnecessarily increases the time incurred for packet forwarding. However, the proposed GTF-GDMT facilitates rapid detection of malicious and selfish nodes based on the forecasting properties of Grey theory and supported in better sustenance in delay in the network on par with the baseline approaches used for comparison.

Fig. 8 demonstrates the mean energy consumptions of the proposed GTF-GDMT and the benchmarked FS-INDISM, SREEF and FRCES with an increase in the time of simulation. The results confirmed that the energy consumptions incurred by

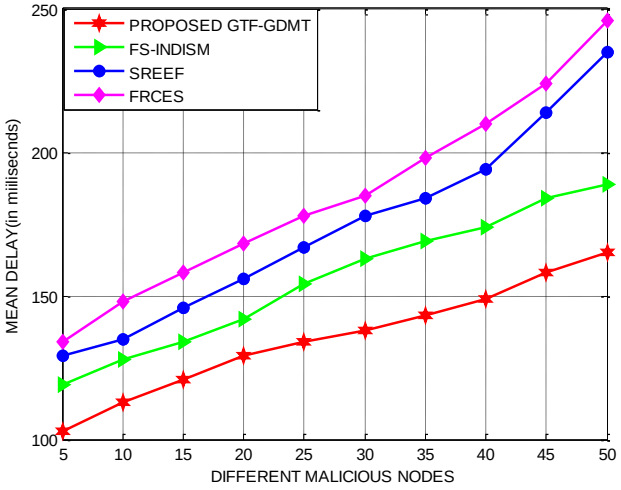

Figure. 7 Proposed GTF-GDMT-Mean delay with different number of malicious nodes

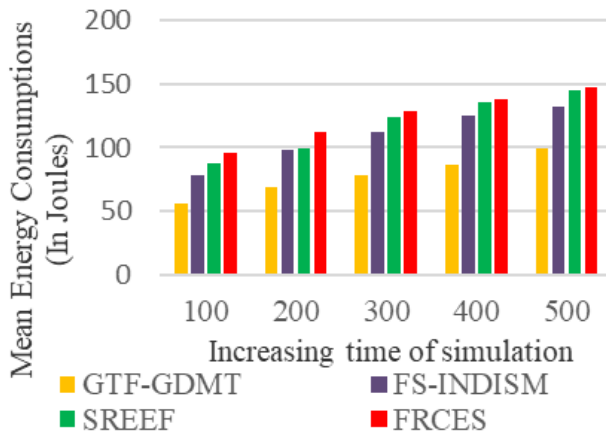

Figure. 8 Proposed GTF-GDMT-Mean energy consumptions with increasing time of simulation

the proposed GTF-GDMT is always lower independent to the increase in the simulation time. This reduced energy consumption rate facilitated by the proposed GTF-GDMT is mainly due to the rapid selection of genuine nodes based on the computation of Gaussian trust that aided in better forecasting of mobile node behavior in the routing path. The proposed GTF-GDMT minimized the mean energy consumptions with increasing time of simulation is minimized by 4.68%, 5.94% and 6.82%, compared to the benchmarked FS-INDISM, SREEF and FRCES approaches.

5. Conclusion and future work

In this paper, GTF-GDMT was proposed as reliable cooperation enforcing methodology developed based on the inspiration derived from Grey theory and Gaussian trust factor. It was proposed for detecting and isolating malicious mobile nodes based on the aging factor with the objective of sustaining network lifetime and performance. It explored the past, present and future exploration behavior of each and every mobile node into account in order to model them into the Gaussian distribution trust factor. It mitigated malicious nodes based on the computation of Gaussian distribution-based trust factor through the combination of link stability and node reputation factors attained through direct and indirect monitoring process. It facilitated the results of gray scale sorting for prioritizing the predecessor and successor node of the mobile node present in a routing path. The simulation results proved that the packet delivery rate and detection rate of the proposed GTF-GDMT with different mobile nodes is improved on an average by 15.18% and 15.88%, superior to the benchmarked FS-INDISM, SREEF and FRCES approaches. Further, the mean throughout of the proposed GTF-GDMT with increasing malicious nodes is improved by 11.28%, compared to the benchmarked FS-INDISM, SREEF and FRCES approaches. In addition, the proposed GTF-GDMT with increasing simulation time minimized the mean energy consumptions and mean packet delay, on an average by 6.28% and 5.92%, compared to the benchmarked FS-INDISM, SREEF and FRCES approaches. As the part of future scope, mitigation scheme using Demspter Shafer Theory can be developed and evaluated with the proposed GTF-GDMT to determine their contextual predominance. Further, different cooperation approaches using statistical reliability such as kohen kappa, Richardson kappa and Bates coefficient can be formulated and its comparative analysis can be further done for determine their significance during implementation.

Conflicts of Interest

"The authors declare no conflict of interest."

Author Contributions

S. Srinivasulu and S. Ramakrishna conceived of the presented idea and developed the methodology and performed the computations and S. Srinivasulu has performed the simulation conducted using ns-2.34 network simulator under the supervision of S. Ramakrishna. And both the authors discussed the results and contributed to the final manuscript.

References

[1] S. Vassilaras, D. Vogiatzis, and G. S. Yovanof, "Security and Cooperation in clustered mobile

ad hoc networks with centralized supervision", *IEEE Journal on Selected Areas in Communications*, Vol. 24, No. 2, pp. 329-342, 2006.

[2] G. Dhananjayan and J. Subbiah, "T2AR: trust-aware ad-hoc routing protocol for MANET", *SpringerPlus*, Vol. 5, 995, 2016.

[3] M. S. Khan, M. I. Khan, S. Malik, O. Khalid, M. Azim, and N. Javaid, "MATF: A multi-attribute trust framework for MANETs", *EURASIP Journal on Wireless Communications and Networking*, 2016.

[4] Y. Li and X. Wu, "Cooperative packet-forwarding strategies in mobile ad hoc networks with unreliable channels: An evolutionary game approach", *International Journal of Distributed SensorNetworks*, 2019.

[5] K. RahimiZadeh and P. Kabiri, "Trust-based routing method using a mobility-based clustering approach in mobile ad hoc networks", *Security Comm. Networks*, Vol. 7, pp. 1746-1763, 2014.

[6] S. NageswaraRao and C. Shobabindu, "Uncertain Rule Based Fuzzy Logic QoS Trust Model in MANETs", *International Conference on Advanced Computing and Communications -ADCOM*, pp. 55-60, 2015.

[7] A. Dorri, "An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET", *Wireless Netw*., Vol. 23, pp. 1767-1778, 2014.

[8] L. G. Delgado, E. P. Segarra, and A. M. Mezher, "A novel dynamic reputation-based source routing protocol for mobile ad hoc networks", *J Wireless Com Network 2019*, Vol. 77, 2019.

[9] S. NageswaraRao and C. S. Bindu, "A Novel QoS Trust Computation in MANETs Using Fuzzy Petri Nets", *International Journal of Intelligent Engineering and Systems*, Vol. 10, No. 2, pp 116-125, 2017.

[10] B. K. Tripathy, S. K. Jena, and P. Bera, "An Adaptive Secure and Efficient Routing Protocol for Mobile Ad Hoc Networks", *Wireless Pers Commun*., Vol. 114, pp. 1339-1370, 2020.

[11] Z. Li and H. Shen, "Game-Theoretic Analysis of Cooperation Incentive Strategies in Mobile Ad Hoc Networks", *IEEE Transactions on Mobile Computing*, Vol. 11, No. 8, pp. 1287-1303, 2012.

[12] J. Manoranjini, A. Chandrasekar, and S. Jothi, "Improved QoS and avoidance of black hole attacks in MANET using trust detection framework", *Automatika*, pp. 274-284, 2019.

[13] H. Shen and Z. Li, "A Hierarchical Account-Aided Reputation Management System for MANETs", *IEEE/ACM Transactions on Networking*, Vol. 23, No. 1, pp. 70-84, 2015.

[14] S. A. Thorat and P. J. Kulkarni, "Uncertainty analysis framework for trust-based routing in MANET", *Peer-to-Peer Networking and Applications*, pp. 1101-1111, 2017.

[15] S. S. Ali and B. V. V. S. Prasad, "Secure and energy aware routing protocol (SEARP) based on trust-factor in Mobile Ad-Hoc networks", *Journal of Statistics and Management Systems*, Vol. 20, No. 4, pp. 543-551, 2017.

[16] M. K. Garg, N. Singh, and P. Verma, "Fuzzy rule-based approach for design and analysis of a trust-based secure routing protocol for MANETs", *Procedia Computer Science*, pp. 653-658, 2018.

[17] T. Kavitha, K. Geetha, and R. Muthaiah, "India: Intruder Node Detection and Isolation Action in Mobile Ad Hoc Networks Using Feature Optimization and Classification Approach", *J Med Syst*., Vol. 43, 2019.

[18] H. Xia, Z. Li, Y. Zheng, A. Liu, Y. Choi, and H. Sekiya, "A Novel Light-Weight Subjective Trust Inference Framework in MANETs", *IEEE Transactions on Sustainable Computing*, Vol. 5, No. 2, pp. 236-248, 2020.

[19] M. Ponguwala and S. Rao, "E2-SR: a novel energy-efficient secure routing scheme to protect MANET-IoT", *IET Communications*, Vol. 13, No. 19, pp. 3207-3216, 2019.

[20] J. A. Josephine and S. Senthilkumar, "Tanimoto Support Vector Regressive Linear Program Boost Based Node Trust Evaluation for Secure Communication in MANET", *Wireless Pers Commun*, 2020.

[21] S. Janakiraman and B. B. Jayasingh, "A Hyper-Exponential Factor-Based Semi-Markov Prediction Mechanism for Selfish Rendezvous Nodes in MANETs", *Wireless Pers Commun.*, Vol. 108, pp. 1493-1511, 2019.

[22] 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.

[23] W. G. Kumar, K. S. Kumar, and S. K. Mutto, "Trust framework for attack resilience in MANET using AODV", *Journal of Discrete Mathematical Sciences and Cryptography*, pp. 209-220, 2020.

[24] A. A. A. Silva, E. Pontes, F. Zhou, and S. T. Kofuji, "Grey model and polynomial regression for identifying malicious nodes in MANETs",

IEEE Global Communications Conference, Austin, TX, pp. 162-168, 2014.
[25] W. Alnumay, U. Ghosh, and P. Chatterjee, "A Trust-Based Predictive Model for Mobile Ad Hoc Network in Internet of Things", *Sensors (Basel, Switzerland)*, 2019.