Wireless Personal Communications (2021) 119:2147–2163
https://doi.org/10.1007/s11277-021-08323-4

Integrated Context-Based Mitigation Framework for Enforcing Security against Rendezvous Point Attack in MANETs

Sengathir Janakiraman[1] · M. Deva Priya[2] · A. Christy Jebamalar[3]

Accepted: 18 February 2021 / Published online: 14 March 2021

Abstract

Reliable communication in ad hoc networks necessitates mobile nodes to synchronize among themselves for cooperation. The cooperation in ad hoc networks is enforced through the implementation of encryption algorithms and intrusion detection systems. Most of the intrusion detection and encryption algorithms are not effective enough to address the extent to which a participative mobile node may trust other interacting mobile nodes for data forwarding. The existing mitigation frameworks consider packet forwarding capability as the single parameter for calculating trust values which cannot be appropriate for computing the accurate trust factor as reliable nodes are highly impacted by data rate, throughput, delay and energy consumption. An Integrated Context-based Mitigation Framework (ICMF) is proposed for facilitating effective mitigation of rendezvous point misbehavior and for enhancing the performance of the network. This proposed ICMF framework facilitates rendezvous point misbehavior detection by determining Grey theory Inspired Discriminating Factor (GTIDF) that is contextually derived from multiple factors including data rate, throughput, delay and energy consumptions using the benefits of the Grey theory. From the simulation results of the proposed ICMF framework, improved root node attackers survivability rate and root node attackers categorization rate are inferred when compared to the benchmarked baseline mitigation frameworks.

Keywords Rendezvous point node · Grey theory · Accurate trust factor · Grey Theory Inspired Discriminating Factor (GTIDF)

✉ M. Deva Priya
m.devapriya@skct.edu.in

Sengathir Janakiraman
j.sengathir@gmail.com

A. Christy Jebamalar
a.christyjebamalar@skct.edu.in

[1] Department of Information Technology, CVR College of Engineering, Mangalpally, Vastunagar, Hyderabad, Telangana, India

[2] Department of Computer Science & Engineering, Sri Krishna College of Technology, Coimbatore, Tamil Nadu, India

[3] Department of Information Technology, Sri Krishna College of Technology, Kovaipudur, Coimbatore, Tamilnadu, India

1 Introduction

Traditionally, security is considered as a challenging issue in the event of data dissemination in Mobile Ad hoc NETworks (MANETs) due to their decentralized characteristics and dynamic change of states of mobile nodes [1]. The dynamic changes in mobile nodes' behavior are either intentional or non-intentional introduced by the node itself or the attackers intruding into the network [2]. The predominant attacks that are possible include selfish node attack, rendezvous node attack, block hole attack, worm hole attack and flooding attack [3]. In specific, the root node or rendezvous attack on mobile nodes is considered to be significant that is highly possible during group communications [4]. The network performance under root node attack prevents data packets from being forwarded from one multicast tree to another. This attack negatively impacts the throughput of the network by increasing energy consumption and re-transmissions [5]. Further, when the selfish behavior is imposed over rendezvous nodes, the network performance is still highly degraded that leads to constant tree multicast partitions in the network. A number of predominant mitigation frameworks are formulated and contributed in the network for effective mitigation of rendezvous point nodes [6]. Most of the mitigation frameworks proposed for preventing root node attacks relies only on a single parameter. The parameters such as data rate, throughput, delay and energy consumptions are determined to be essentially investigated for designing a reliable framework [7]. Thus the mitigation of rendezvous point attack under selfish intent cannot be possible through the incorporation of a single parameter [8]. Hence, an integrated context-based multiple factor-based mitigation framework becomes necessary to be devised for mitigating the root node attack with selfish intent in a remarkable manner.

In this paper, an Integrated Context-based Mitigation Framework (ICMF) is formulated for preventing rendezvous point attacks through the computation of Grey theory Inspired Discriminating Factor (GTIDF) which is contextually derived using the multiple factors like data rate, throughput, delay and energy consumption using the benefits of the Grey theory. This proposed ICMF framework contextually computes the GTIDF factor by utilizing three categories of root node detection mechanisms that determines its trust value based on their history, conditional and forecasting methodologies respectively. The simulation experiments are also facilitated for quantifying the remarkable performance of the proposed ICMF framework using the survivability rate and categorization rate of root node attackers.

The forthcoming sections of the paper are arranged as follows. Section 2 highlights the potential review of the most recent frameworks contributed for effective detection of rendezvous point attack. Section 3 presents the detailed view of the proposed ICMF framework in addition to its suitability and applicability.

2 Related Work

In this section, some of the most recent frameworks contributed in the literature that focus towards effective and efficient prevention of the rendezvous point attack are detailed with their merits and limitations.

Initially, a Support Vector-based Trust Mitigation Framework (SVTMF) is proposed using Support Vector Machine (SVM) for effective prevention of malicious nodes in the network based on the concept of Tit-for Tat [9]. This SVTMF utilizes only a single factor of packet forwarding potentail for effective mitigation. This SVTMF framework possesses the limitation of not using multiple parameters that appropriately attribute towards the detection of rendezvous node attack in the network. This SVTMF is not capable of predicting the future probability of selfish-based rendezvous point attack under multicasting. Then, a Bayesian Trust (B-TRUST)-based root node attack mitigation framework is proposed for deriving the benefits of Bayesian probability in rendezvous point node detection process [10]. The Bayesian Probability is considered in B-TRUST for quantifying the influence of one factor over other factors such that accurate detection of root node attack is facilitated. This B-Trust mitigation framework also considers only a single parameter for making decisions towards the mitigation of selfish nodes in the network. Further, an effective mitigation framework called Feedback Aggregation in Collaborative Intrusion Detection Network (FACID) is proposed for mitigating the rendezvous point attack in a network [11]. This FACID framework is determined to be the contextual method that estimates the single parameter of throughput to be incorporated in the decision process. Furthermore, Multiple Trust-based Mitigation Framework (MTMF) is proposed for mitigating malicious activity of mobile nodes in the network [12]. This MTMF is the first framework approach that induces innovation of utilizing the benefits of multiple factors that could attribute towards the efficient detection of malicious nodes in the network. Finally, another SVM-based root node mitigation approach is contributed for superior performance of the network in terms of throughput and packet forwarding rate [13]. The energy consumptions and packet delay of the network are determined to be considerably minimized to a significant level in the network. This framework fails to compute the value of trust based on contextual application of parameters and hence the average overhead incurred in the process of data transfer is estimated to be maximum in the network.

The aforementioned limitations of the reviewed mitigation frameworks mechanisms induce the idea for formulating an effective and efficient ICMF framework for mitigating selfish-based rendezvous point attack in the network under multicasting.

3 Integrated Context-based Mitigation Framework (ICMF)

This proposed Integrated Context-based Mitigation Framework (ICMF) uses multiple factors and context-based reliability factors for classifying and mitigating rendezvous point with selfish misbehavior under multicasting. ICMF proves that mobile node's behavior cannot be effectively evaluated through a single input parameter like probability of reliable interactions. Hence, reliability factor in ICMF is calculated using closely related parameters including data rate, throughput, delay and energy consumptions. Grey theory is used in ICMF for employing the aforesaid multi-parameters for quantitative evaluation, classification and behavioral investigation of mobile nodes. ICMF uses the benefits of Grey theory as they are capable of analyzing the possible relation that exists between multiple factors based on the kind of data collected. They are potential in evaluating parameters that are not consistent with any distribution rules and are capable of handling multiple factors by preventing uncertainty through the computation of a Grey Theory Inspired Discriminating Factor (GTIDF).

ICMF framework depicted in Fig. 1 consists of three modules as follows:

(1) Multi-factor observation module

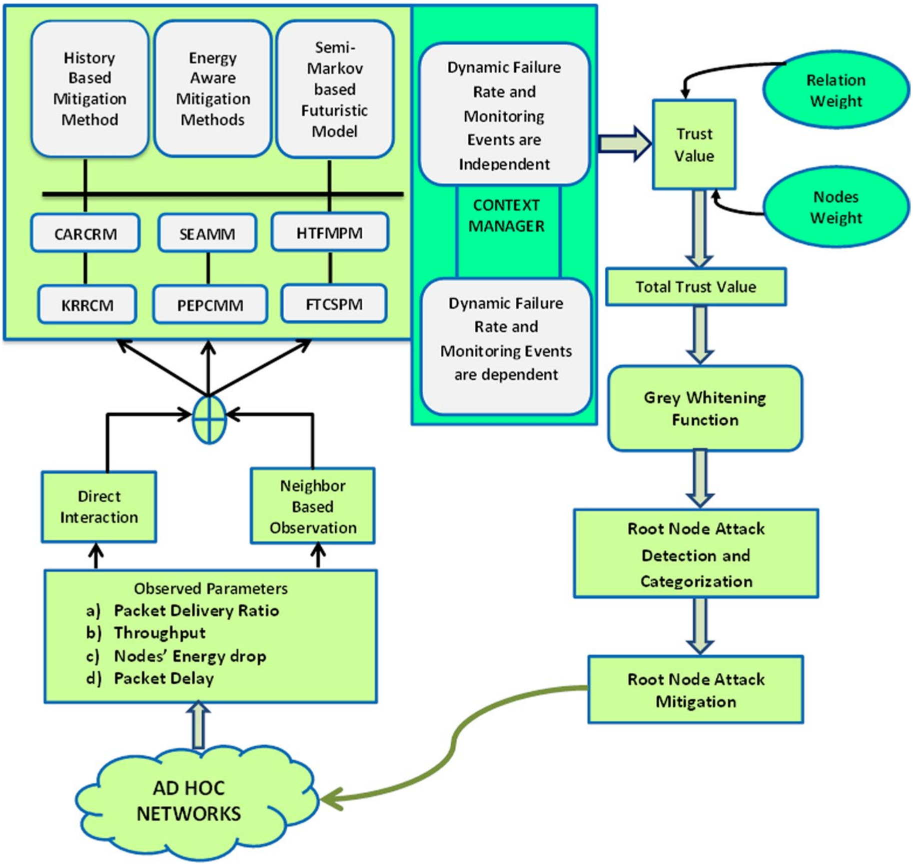
History Based Mitigation Method
Energy Aware Mitigation Methods
Semi-Markov based Futuristic Model
CARCRM
SEAMM
HTFMPM
KRRCM
PEPCMM
FTCSPM
Dynamic Failure Rate and Monitoring Events are Independent
CONTEXT MANAGER
Dynamic Failure Rate and Monitoring Events are dependent
Trust Value
Relation Weight
Nodes Weight
Total Trust Value
Grey Whitening Function
Root Node Attack Detection and Categorization
Root Node Attack Mitigation
Direct Interaction
Neighbor Based Observation
Observed Parameters
a) Packet Delivery Ratio
b) Throughput
c) Nodes' Energy drop
d) Packet Delay
AD HOC NETWORKS

Fig. 1 ICMF Mitigation Framework Architecture

(2) Multi-reliability factor computation and integration module
(3) Rendezvous Point Misbehavior classification and mitigation module

The detailed descriptions of each of the aforementioned modules are given below.

3.1 Multi-factor Observation Module

In this Multi-factor observation module, multiple factors such as data rate, throughput, delay and energy consumption are elucidated from the network. The elucidated multiple factors are gathered either through direct interaction or neighbour-based interactions. The multiple data is collected for computing GTIDF. This GTIDF aids in computing the contextual reliability factor that integrates three types of proposed mitigation schemes pertaining to co-operation, quantifying reliability factors based detection mechanisms viz., History-based approach (SPlit-half Reliability Factor-based Selfish Node Mitigation (SPRFSNM) [14] and Exponential Factor-based Selfish Node Mitigation (EFSNM)[15]), Conditional probability-based mitigation approaches (ERlang Reliability Conditional Factor-based Selfish Node Mitigation (ERCFSNM) [16] and Laplace Transform-based Selfish Node Mitigation (LTSNM) [17]) and forecasting mechanisms (Semi Markov Factor-based Selfish Node Mitigation (SMF-SNM) [18] and Hyper-Geometric Factor-based Selfish Node Mitigation (HGFSNM) [19]) respectively.

3.2 Multi-reliability Factor Computation and İntegration Module

In this multi-reliability factor computation and integration module, the reliability factor is computed either using SPRFSNM or EFSNM for collecting the trust from the neighbours depending on the suitability and application. ERCFSNM is used for computation when the difference between the elucidated multiple factors is minimum, and LTSNM is used when the deviation between the multiple factor is maximum. ICMF manipulates the energy based probabilistic reliability factor using SPRFSNM or EFSNM based on energy utilization rate of mobile nodes. ERCFSNM and LTSNM are used when the energy utilization rates of mobile nodes realized from collected multiple factors are maximum and minimum respectively. The alteration between ERCFSNM and LTSNM is facilitated through the contextual manager that analyzes the energy utilization rate of mobile nodes. In addition, the futuristic reliability forecasting factor of this framework is computed by using the SMFSNM and HGFSNM prediction mechanism.

3.3 Rendezvous Point Misbehaviour Classification and Mitigation Module

Finally, ICMF integrates the three categories of estimated reliability factors. This integrated trust of mobile nodes called GTIDF is calculated during the time period 't' {t=1, 2,.., T}. GTIDF discrimination factor of each node 'i' at time 't' is denoted by 'd_{ij}'. Likewise, the discrimination factor of i's neighbour node 'j' at the same time 't' is 'd_{ji}'.

From the estimated discrimination factor, the GTIDF (μ_{ij}) is

$$\mu_{ij} = \frac{\min\left|d_{ij} - d_{ji}\right| + k\max\left|d_{ij} - d_{ji}\right|}{\left|d_{ij} - d\right| + k\left|d_{ij} - d_{ji}\right|} \tag{1}$$

In this context, the discrimination factor of each mobile node 'i' as estimated by its neighboring mobile nodes at time 't' is 'd_{ij}'. On the hand, the discrimination factor of each neighboring node as estimated by the originally monitored mobile nodes at the same time 't' is 'd_{ji}'. (For example, if nodes 'i' and 'j' are interacting nodes, then 'd_{ij}' refers to the trust judgement of node 'i' by mobile node 'j' and 'd_{ji}' refers to the trust judgement of node 'j' by the mobile node 'i', vice versa).

Here, $k = 1/2$ is mainly required for normalizing the discrimination factor that ranges from '0′and '1'.

The influence of rendezvous point misbehaviour classified into three discriminating Grey-theory groups $\left(G_1, G_2, G_3\right)$ with their associated weight functions $\left(wf_1, wf_2, wf_3\right)$ is given by

$$wf_1\left(\mu_{ij}\right) = -\mu_{ij} + 1, \text{ where } 0 \le \mu_{ij} \le 1, \alpha = 0 \tag{2}$$

$$wf_2\left(\mu_{ij}\right) = \begin{cases} 2\mu_{ij} & where\ \mu_{ij} < 0.5,\ \alpha_2 = 0.5 \\ -\mu + 2 & \text{where } \mu_{ij} > 0.5,\ \alpha_2 = 0.5 \end{cases} \tag{3}$$

$$\mathrm{wf}\left(\mu_{\mathrm{ij}}\right) = \mu_{\mathrm{ij}}, \quad \text{where } 0 < \mu_{\mathrm{ij}} < 1,\ \alpha = 1 \tag{4}$$

where $\left(\alpha_1, \alpha_2, \alpha_3\right)$ refers to the critical bounds for root node attack classification. Then, the integrated value of grey function (G_{ij}) aids in classifying the impact of root node attacks. The impact is said to be moderate if 'G_{ij}' lies between $\frac{\alpha_3+\alpha_1}{3}$ and $2\frac{\alpha_3+\alpha_1}{3}$. If G_{ij} is below $\frac{\alpha_3+\alpha_1}{3}$, the impact of root node misbehaviour is minimum and it is isolated from routing. In contrary, if 'G' is above $\frac{\alpha_3+\alpha_1}{3}$, the mobile node is co-operative and non-compromised by rendezvous point misbehaviour.

In addition, the proposed ICMF framework can be utilized for mitigating rendezvous point misbehaviour in critical ad hoc networks applications like Post disaster relief operation where co-operation among mobile nodes are highly essential.

4 Suitability of ICMF framework in Disaster Rescue Operation

Tsunami in 2011 and hurricane Sandy in 2012 have drawn great focus to improve the process of post disaster recovery operation. Disasters are unpredictable and may create great havoc by uprooting the entire communication system depending on their severity [20, 21]. Moreover, an infrastructure based network is adversely affected by disaster, and the disaster struck region suffers from degraded communication which hurdles the rescue operation. Thus, the application of ad hoc networks plays a vital role in disaster rescue operation as they can be quickly implemented in the disaster region without any fixed networking infrastructure. However, the application of ad hoc networks in a disaster struck region faces the challenge of co-operation that is necessary for maintaining reliable communication [22, 23]. The issue of co-operation is influenced by the energy constrained nature of mobile nodes because injudicious use of their energy may decrease the network lifetime and further hurdle the network connectivity during post disaster relief operation [24, 25]. Hence, the proposed ICMF framework can be incorporated during a post disaster relief operation for mitigating rendezvous point misbehaviour of multicast group leader in this critical environment.

The implementation of ICMF in post disaster relief operation can be achieved in the following aspects. A hybrid network architecture need to be used for maintaining connectivity between the Base Station (BS) and the mobile nodes of the disaster struck region. The hybrid network architecture has to alternate its mode from cellular network mode to ad hoc network mode when the link between the BS and the survivor's node fail. The route between survivor's nodes should be discovered only through neighbours' communication rather than broadcasting the route request packet. The hybrid network architecture must employ a dedicated MAC protocol based on Time Division Multiplexing (TDM) for reducing the delay during recovery. Rendezvous point misbehaviour mitigation of survivor's node have to achieved by calculating a trust value that integrates three types of context-aware reliability factors based detection techniques proposed in this research.

5 Performance Investigation of ICMF Framework

The performance of ICMF framework is investigated and it is compared with the benchmarked mitigation frameworks like MTFM and B-TRUST using ns-2.32. ICMF is deployed in the simulation area that contains 100 mobile nodes that arbitrarily move around the terrain area of 1000×1000 m in order to investigate the impact of small and large networks [26–30]. Simulations are carried out using a random waypoint model with CBR traffic rate of 40 packets per second and simulation time of 250 s.

Comparative performance of ICMF with MTFM and B-TRUST is initially evaluated based on the estimated trust value for proving its efficiency in effectively mitigating rendezvous point misbehavior. Then, ICMF framework is analyzed based on detection rate, average latency, average overhead, communication overhead, packet delivery rate and throughput by varying the number of mobile nodes and root node attackers. Finally, ICMF is studied based on newly contributed evaluation parameters like rendezvous point misbehavior categorization rate. Rendezvous point misbehavior categorization rate refers to the ratio of the number of mobile nodes actually found to be attacked root nodes to the number of mobile nodes expected to exhibit rendezvous point misbehavior. The rendezvous point misbehavior rate quantifies the fraction of the number of mobile nodes actually mitigated for exhibiting rendezvous point misbehavior to the actual number of mobile nodes exactly identified as rendezvous point misbehavior compromised.

In experiment-1, the effectiveness of the ICMF framework in estimating genuine trust value is analyzed by emphasizing packet delivery rate, throughput, packet delay, energy consumption, data rate and packet loss rate varied over a period of time. It also evaluates the capability of the ICMF framework by using comprehensive trust value estimated by integrating the utilized multiple factors.

Figures 2 and 3 represent the results of accurate trust value of the ICMF framework when the packet delivery rate and throughput are emphasized in the implementation. Figure 2 shows that the ICMF framework estimates accurate trust value at an average rate of 9% and 14% superior to the MTFM and B-TRUST mitigation frameworks when the packet loss rate is emphasized during deployment. Figure 3 portrays that ICMF framework is accurate in estimating the trust value at a rate of 12% and 15% superior to MTFM and B-TRUST trust frameworks when throughput is emphasized during its application.

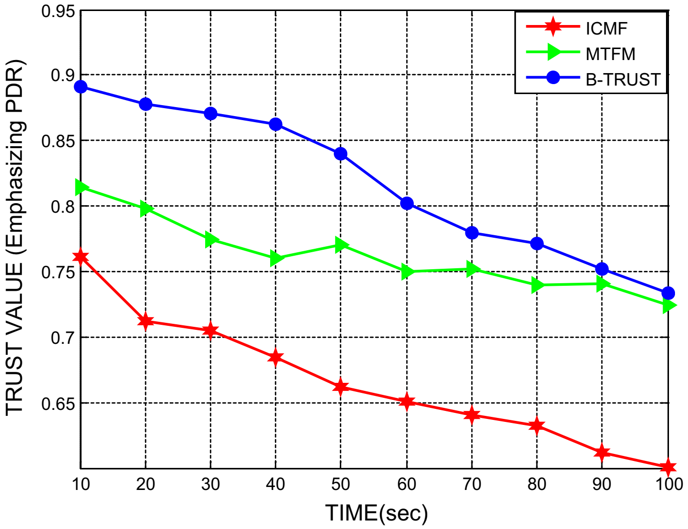

Fig. 2 Accurate Trust value emphasizing PDR of the Proposed Integrated Context-based Mitigation Framework

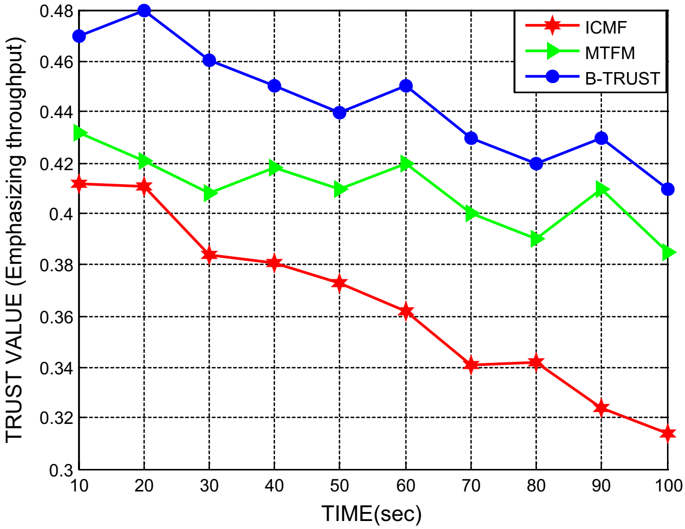

Fig. 3 Accurate Trust value emphasizing Throughput of the Proposed Integrated Context-based Mitigation Framework

Figures 4 and 5 depict the results of accurate trust value facilitated by ICMF framework when packet delay and energy consumption rate are emphasized during implementation. Figure 4 exhibits that when the packet delay is emphasized, the ICMF framework estimates the trust value at an accurate rate of 13% and 17% superior to the baseline mitigation frameworks. Figure 5 shows that ICMF framework estimates the trust value at an accurate

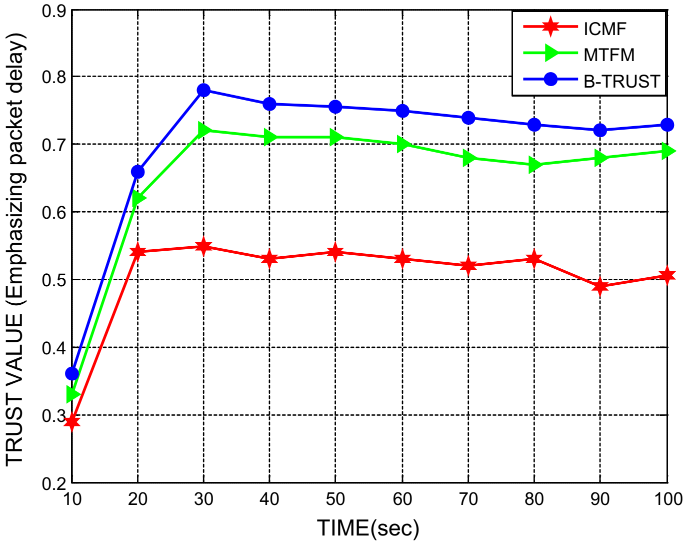

Fig. 4 Accurate Trust value emphasizing Packet Delay of the Proposed Integrated Context-based Mitigation Framework

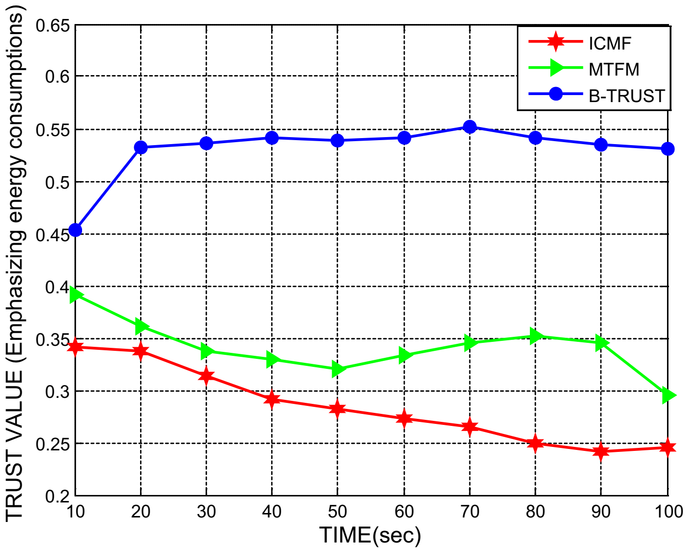

Fig. 5 Accurate Trust value emphasizing Energy consumption of the Proposed Integrated Context-based Mitigation Framework

rate of 11% and 20% superior to the MTFM and B-TRUST frameworks when energy consumption is emphasized.

Likewise, Figs. 6 and 7 portray the result of accurate trust value facilitated by ICMF framework when data rate and packet loss rate are emphasized during deployment. Figure 6 depicts that when data rate is emphasized, ICMF framework estimates the trust value

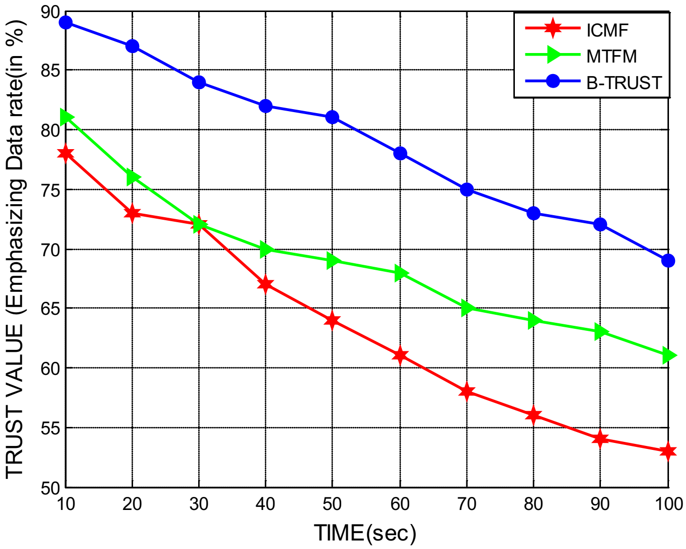

Fig. 6 Accurate Trust value emphasizing Data rate of the Proposed Integrated Context-based Mitigation Framework

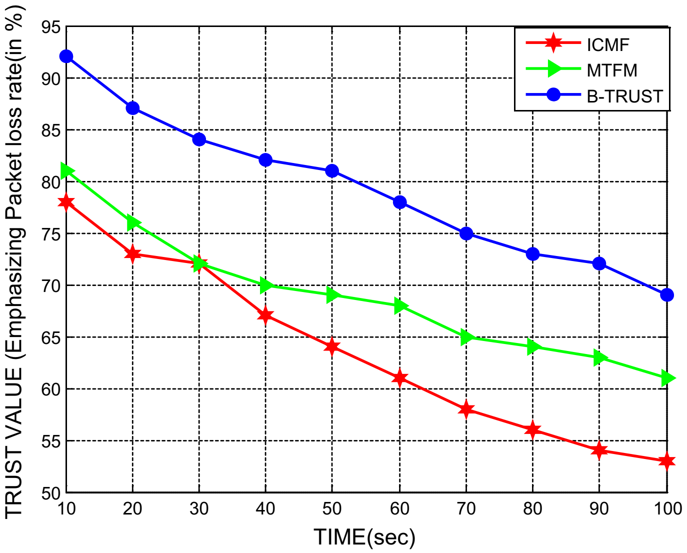

Fig. 7 Accurate Trust value emphasizing Packet Loss of the Proposed Integrated Context-based Mitigation Framework

at an accurate rate of 16% and 21% superior to the baseline mitigation frameworks. Figure 7 represents that ICMF framework that estimates the trust value at an accurate rate of 12% and 18% superior to the MTFM and B-TRUST frameworks when packet loss rate is emphasized.

Further, the effectiveness of ICMF is analyzed based on the false positive rate, average overhead and average latency by varying the number of root node attackers. Figures 8,

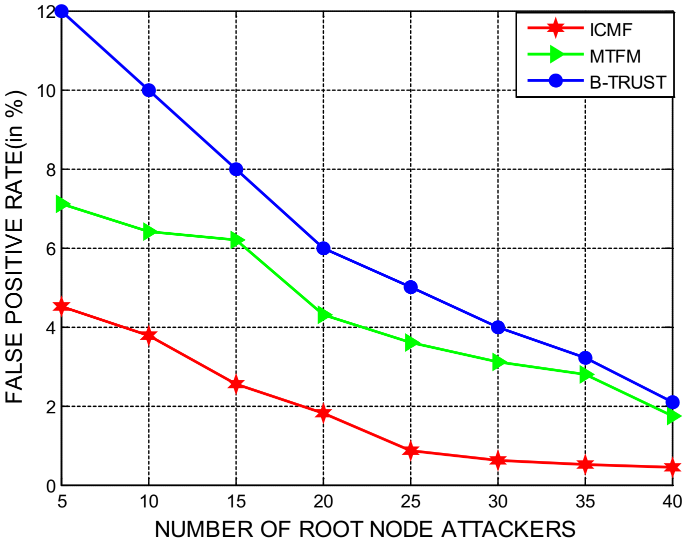

Fig. 8 False Positive Rate of the Proposed Integrated Context-based Mitigation Framework

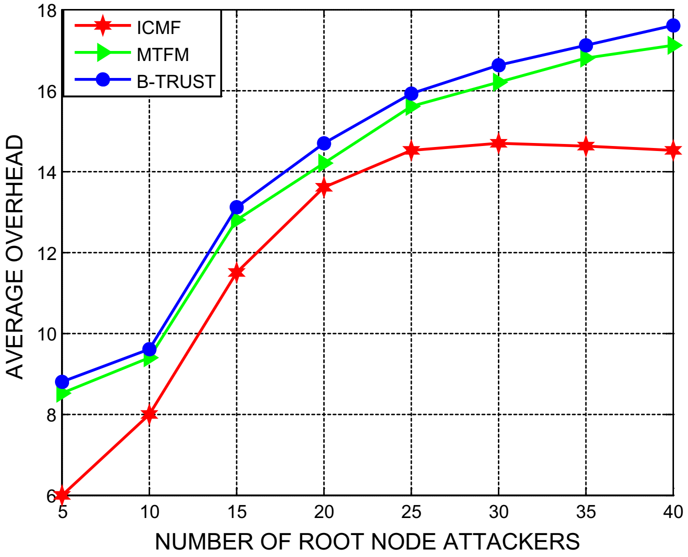

Fig. 9 Average Overhead of the Proposed Integrated Context-based Mitigation Framework

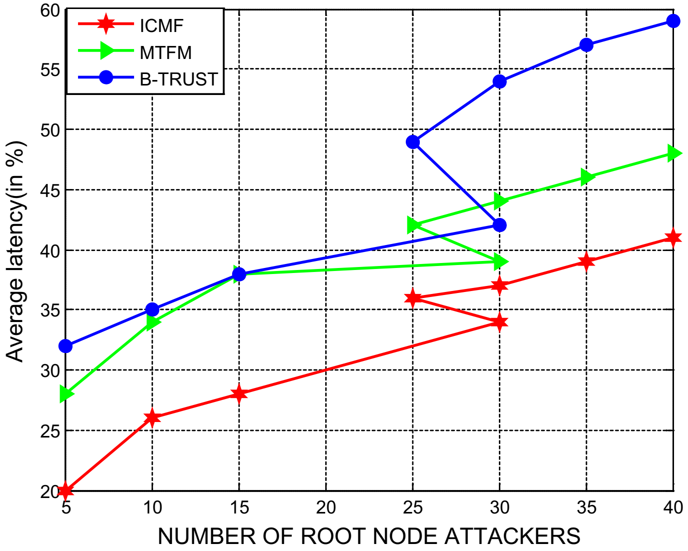

Fig. 10 Average Latency of the Proposed Integrated Context-based Mitigation Framework

9 and 10 exhibit the results of false positive rate, average overhead and average latency demonstrated by ICMF framework when evaluated for varying number of root node attackers. Figure 8 shows that ICMF framework offers reduced false positive rate at an average rate of 13% and false positive rate of 10% and 13% on par with MTFM and B-TRUST respectively.

Figure 9 represents that ICMF framework decreases the average overhead by an average rate of 17% and decreases the average overhead on par with MTFM and B-TRUST by 15% and 19% respectively. Figure 10 represents that ICMF framework decreases the average latency by an average rate of 14% and decreases the average latency in comparison with MTFM and B-TRUST by 12% and 16% respectively.

Finally, ICMF is also evaluated based on Rendezvous point misbehavior categorization rate and survivability rate as portrayed in Figs. 11 and 12. From Fig. 11, it is proved that Rendezvous point misbehaviour categorization rate of ICMF is 14% and 19% higher than the categorization rate as exhibited by MTFM and B-TRUST. From Fig. 12, it is evident that Rendezvous point misbehavior survivability rate of ICMF is 5.8% and 8.6% better than the survivability rate of MTFM and B-TRUST respectively.

The analytical validation of the proposed ICMF framework is presented based on the critical bounds of root node attack detection $\left(\alpha_1, \alpha_2, \alpha_3\right)$, different values of ‘k’ used for normalization and different weight functions $\left(\mathrm{wf}_1,\ \mathrm{wf}_2,\ \mathrm{wf}_3\right)$ used in the detection process. In the first part of analytical validation, the predominance of the proposed ICMF framework is explored using detection accuracy by changing the critical bounds of root node attack detection under $\alpha = 0.25$,$\alpha = 0.5$ and $\alpha = 1$, respectively.

The aforementioned results in Table 1 clearly prove that the detectıon accuracy of the proposed ICMF framework is determined to be comparatively improved with the critical bounds of root node attack classification value set to $\alpha = 0.5$. The performance of the proposed ICMF framework at $\alpha = 0.25$ and $\alpha = 1$ is also significant but not to the maximum level attained by the implemented scheme at $\alpha = 0.5$. Moreover, the detection accuracy on an average is visualized to be improved by 4.59% at $\alpha = 0.5$ in contrast to the critical bounds of root node attack detection estimated at $\alpha = 0.25$ and $\alpha = 1$, respectively.

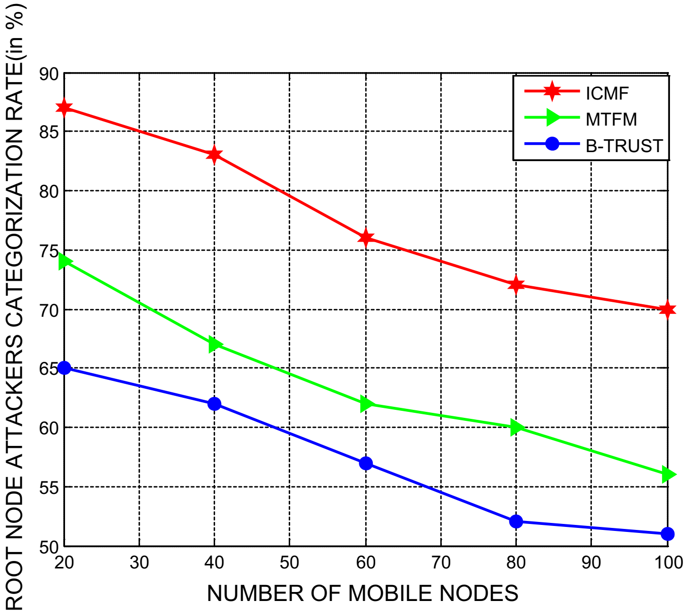

Fig. 11 Rendezvous Point Misbehavior Categorization Rate of the Proposed Integrated Context-based Mitigation Framework

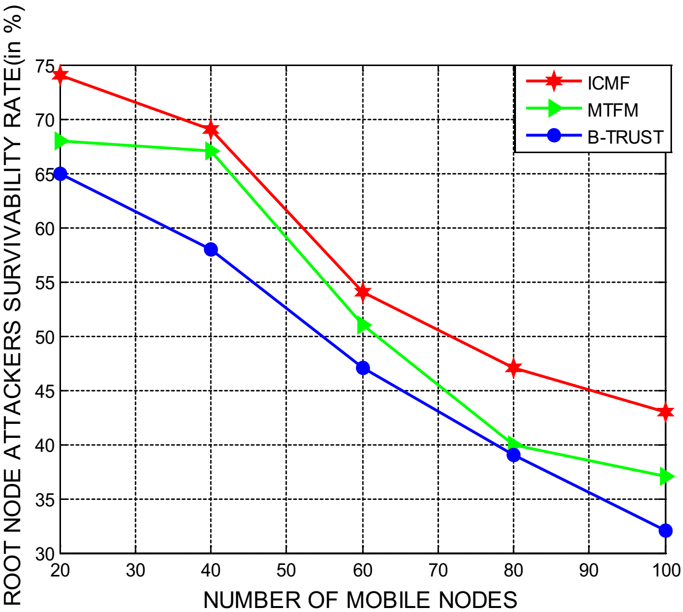

Fig. 12 Rendezvous Point Misbehavior Survivability Rate of the Proposed Integrated Context-based Mitigation Framework

Table 1 Detectıon Accuracy for Different Critical Bounds of Root Node Attack Classification

Number of mobile nodes	Detectıon Accuracy for Different Critical Bounds of Root Node Attack Classification		
	$\alpha = 0.25$	$\alpha = 0.5$	$\alpha = 1$
20	0.9724	0.9921	0.9832
40	0.9521	0.9916	0.9818
60	0.9432	0.9913	0.9732
80	0.9356	0.9906	0.9631
100	0.9288	0.9902	0.9649

Table 2 Detectıon Accuracy for Different Critical Bounds of Root Node Attack Classification

Number of mobile nodes	Detectıon Accuracy for Different Value of 'k' used for Normalization			
	$k = 0.25$	$k = 0.5$	$k = 0.75$	$k = 1$
20	0.9732	0.9942	0.9531	0.9341
40	0.9724	0.9938	0.9518	0.9312
60	0.9703	0.9934	0.9504	0.9256
80	0.9631	0.9921	0.9501	0.9214
100	0.9612	0.9913	0.9458	0.9204

The results presented in Table 2 evidently confirms that the detectıon accuracy of the proposed ICMF framework is determined to be comparatively improved with the critical bounds of root node attack classification value set to $k = 0.5$. The detection accuracy of the proposed ICMF framework at $k = 0.25$, $k = 0.75$ and $k = 1$ is visualized to be comparatively lower than the detection accuracy attained by the implemented scheme at $k = 0.5$. In addition, the detection accuracy of the proposed ICMF scheme on an average is visualized to be improved by 5.68% at $k = 0.5$ when compared to the critical bounds of roort node attack detection estimated at $k = 0.25$, $k = 0.75$ and $k = 1$, respectively.

The above mentioned results in Table 3 prove that the performance of the proposed ICMF framework evaluated in terms of detectıon accuracy is remarkable with the weights set to $wf_1 = 0.33$, $wf_2 = 0.33$ and $wf_3 = 0.33_{,}$ on par with the other weight assignments considered for mitigating attacks. The main reason behind this is mainly due to the importance of Grey theory considered for detecting attacks. Moreover, the performance of the proposed ICMF framework with $wf_1 = 0.33$, $wf_2 = 0.33$ and $wf_3 = 0.33$ is superior in detecting rendezvous point attack on an average by 5.62% and 6.83% when compared to other possible assignments of weights considered for rendezvous point attack detection.

Table 3 Detectıon Accuracy for Different Weights utilized during Detection of Root Node Attack

Number of mobile nodes	Detectıon Accuracy for Different Weights utilized during Detection of Root Node Attack		
	$wf_1 = 0.33$	$wf_2 = 0.33$	$wf_3 = 0.33$
20	0.9821	0.9843	0.9817
40	0.9815	0.9841	0.9813
60	0.9812	0.9828	0.9811
80	0.9806	0.9823	0.9806
100	0.9803	0.9817	0.9804
Number of mobile nodes	Detectıon Accuracy for Different Weights utilized during Detection of Root Node Attack		
	$wf_1 = 0.40$	$wf_2 = 0.3$	$wf_3 = 0.3$
20	0.9621	0.9529	0.9312
40	0.9614	0.9513	0.9307
60	0.9611	0.9508	0.9266
80	0.9605	0.9504	0.9254
100	0.9602	0.9501	0.9241
Number of mobile nodes	Detectıon Accuracy for Different Weights utilized during Detection of Root Node Attack		
	$wf_2 = 0.20$	$wf_2 = 0.5$	$wf_3 = 0.3$
20	0.9126	0.9451	0.9626
40	0.9112	0.9428	0.9622
60	0.9098	0.9356	0.9615
80	0.9054	0.9344	0.9611
100	0.9042	0.9326	0.9606

6 Conclusion

The proposed ICMF framework is formulated and presented as a trustworthy attempt that focuses on the reliable detection of selfish-based rendezvous point attack of mobile nodes under multicasting process. The merits of Grey theory are used in the of the proposed Integrated Context-based Mitigation Framework (ICMF) in order to understand the role of factors used for preventing the root node attack in a multicasting based network. The simulation results of the proposed ICMF framework are presented to exhibit its predominance in reducing packet latency, energy consumptions and average overhead in the network. The results of the proposed ICMF framework also confirm a mean superior Rendezvous point misbehaviour categorization rate and Rendezvous point misbehavior survivability rate of 16% and 6.5% respectively when compared to the MTFM and B-TRUST frameworks considered for investigation. In the near future, Dempster Shafer Evidence-based Trust Framework is planned to be formulated for mitigating the root node attack in the network.

Funding This research work has not received any funding from any organization.

Data Availability Statement The data that support the findings of this study are available from the corresponding author upon reasonable request.

Declaration

Conflicts of interest The authors declare that ther is no conflict of interest.

References

1. Verma, A., & Khare, A. (2013). TFT Technique with Adaptive Thresholding for Selfish Attack Prevention in MANET. *International Journal of Computer Applications, 63*(16), 1–4.
2. Lamba, G. K. (2016). Varying Number of Selfish Nodes based Simulation of AODV Routing Protocol in MANET using Reputation Based Scheme. *International Journal Of Engineering And Computer Science, 1*(2), 89–97.
3. Priya, M. D., Sengathir, J., & Valarmathi, M. L. (2010) Root node attack in a WiMAX 802.16e network. Trendz in Information Sciences & Computing(TISC2010), 1(1) 34–45.
4. Sengathir, J., & Manoharan, R. (2013). Security Algorithms for Mitigating Selfish and Shared Root Node Attacks in MANETs. *International Journal of Computer Network and Information Security, 5*(10), 1–10.
5. Kariya, S. L., & Panchal, B. B. (2012). Selfish Nodes Detection in MANETs: Acknowledgement Based Approach. *International Journal of Scientific Research, 2*(5), 216–217.
6. Rukhande, S., & Shete, P. (2015). Optimized Routing by Excluding Selfish Nodes for MANET. *Communications on Applied Electronics, 3*(5), 43–49.
7. Khoshabi Nobar, S., & Musevi Niya, J. (2014). Robust Mitigation of Selfish Misbehavior In Wireless Networks. *Security and Communication Networks, 8*(9), 1772–1779.
8. Xia, H., Jia, Z., Li, X., Ju, L., & Sha, E. H. (2013). Trust prediction and trust-based source routing in mobile ad hoc networks. *Ad Hoc Networks, 11*(7), 2096–2114.
9. Li, W., Joshi, A., & Finin, T. (2011). SAT: an SVM-based automated trust management system for Mobile Ad-hoc Networks. 2011-MILCOM 2011 Military Communications Conference, 1(1), 45–57.
10. Li, P. P. (2016). Trust portfolio toward an integrative framework: the emerging themes of trust context and trust complexity. *Journal of Trust Research, 6*(2), 105–110.
11. Fung, C. J., & Zhu, Q. (2016). FACID: A trust-based collaborative decision framework for intrusion detection networks. *Ad Hoc Networks, 53,* 17–31.

12. Guo, J., Marshall, A., & Zhou, B. (2017). A Multi-Parameter Trust Framework for Mobile Ad Hoc Networks. *Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications, 1*(1), 245–277.
13. Gopal, D. G., & Saravanan, R. (2016). Selfish node detection based on evidence by trust authority and selfish replica allocation in DANET. *International Journal of Information and Communication Technology, 9*(4), 473.
14. Sengathir, J., & Manoharan, R. (2013). A split half reliability coefficient based mathematical model for mitigating selfish nodes in MANETs. 2013 3rd IEEE International Advance Computing Conference (IACC), 2(1), 45–54.
15. Sengathir, J., & Manoharan, R. (2015). Exponential Reliability Coefficient based Reputation Mechanism for isolating selfish nodes in MANETs. *Egyptian Informatics Journal, 16*(2), 231–241.
16. Sengathir, J., & Manoharan, R. (2016). An Erlang factor-based conditional reliability mechanism for enforcing co-operation in MANETs. *Serbian Journal of Electrical Engineering, 13*(2), 265–284.
17. Sengathir, J., & Manoharan, R. (2014). Laplace Stleltjes Transform based Conditional Survivability Coefficient Model for mitigating Selfish Nodes in MANETs. *Egyptian Informatics Journal, 15*(3), 149–157.
18. Sengathir, J., & Manoharan, R. (2015). A futuristic trust coefficient-based semi-Markov prediction model for mitigating selfish nodes in MANETs. *EURASIP Journal on Wireless Communications and Networking, 2015*(1), 1–13.
19. Parthiban, S., & Rodrigues, P. (2016). A Hyper-Geometric Trust Factor Based Markov Prediction Mechanism for Compromised Rendezvous Point in MANET. *Arabian Journal for Science and Engineering, 41*(8), 3187–3199.
20. Yan, S., Liu, S., & Liu, X. (2016). Dynamic Grey Target Decision Making Method with Three-Parameter Grey Numbers. *Grey Systems: Theory and Application, 6*(2), 169–179.
21. Umar, R., & Mesbah, W. (2017). Throughput-Efficient Coalition Formation of Selfish/Altruistic Nodes in ad hoc Networks: A Hedonic Game Approach. *Telecommunication Systems, 67*(1), 95–111.
22. Chuang, Y., & Lee, Y. (2018). Defense Mechanism for Malicious and Selective Forwarding Attacks in Large and Mobile Wireless Networks. *The Computer Journal, 1*(1), 34–49.
23. Kumar, S., & Dutta, K. (2018). Trust Based Intrusion Detection Technique to Detect Selfish Nodes in Mobile Ad Hoc Networks. *Wireless Personal Communications, 101*(4), 2029–2052.
24. Waqas, A., & Mahmood, H. (2017). A Game Theoretical Approach for Topology Control in Wireless Ad Hoc Networks with Selfish Nodes. *Wireless Personal Communications, 96*(1), 249–263.
25. Roles, A., & ElAarag, H. (2017). Coexistence with malicious and selfish nodes in wireless ad hoc networks: A Bayesian game approach. *Journal of Algorithms & Computational Technology, 11*(4), 353–365.
26. Mohamed Musthafa, M., Vanıtha, K., Zubaır Rahman, A. M. J. M. and Anıtha, K. (2020) "An Efficient Approach to Identify Selfish Node in MANET," *2020 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, 2020, pp. 1–3
27. Jim, L. E., and Gregory, M. A. (2019). "Improvised MANET Selfish Node Detection using Artificial Immune System based Decision Tree," *2019 29th International Telecommunication Networks and Applications Conference (ITNAC)*, Auckland, New Zealand, pp. 1-6
28. Mao, Y., Zhou, C., Qi, J., et al. (2020). A Fair Credit-based Incentive Mechanism for Routing in DTN-based Sensor Network with Nodes' Selfishness. *Journal on Wireless Communication and Networking, 2020,* 232.
29. Janakiraman, S., & Jayasingh, B. B. (2019). A Hyper-Exponential Factor-Based Semi-Markov Prediction Mechanism for Selfish Rendezvous Nodes in MANETs. *Wireless Personal Communications, 108,* 1493–1511.
30. Roy, A., Acharya, T., & Das Bit, S. (2020). Social-based reputation-aware data forwarding for improved multicast delivery in the presence of selfish nodes in DTNs. *International Journal of Communication Systems, 33,* e4235.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Dr. Sengathir Janakiraman is currently working as an Associate Professor in the Department of Information Technology at CVR College of Engineering, Mangalpally, Telangana, India. He received his B.Tech degree in Computer Science and Engineering, M.Tech degree in Information security and Ph.D degree in Mobile ad hoc Networks from Pondicherry Engineering College, Pondicherry University, Puducherry, India. He is the recipient of the Pondicherry University Gold Medal in the year 2010. He has more than 15 years of teaching experience in handling courses like Automata Languages and Computation, Information Security and Compiler Design. His fields of interest include Mobile Ad hoc Networks and Software Engineering.

Dr. M. Deva Priya is currently working as Associate Professor in the Department of Computer Science & Engineering at Sri Krishna College of Technology, Coimbatore, Tamil Nadu, India. She received her Master’s degree in the year 2007 and her Ph.D degree in the year 2015 from Anna University, Chennai, Tamilnadu, India. She has 14 years of teaching experience. Her research interests include Wireless networks, IoT Networks and Machine Learning. She has published more than 60 papers in reputed Journals and Conferences. She is a life member of ISTE, ISRD, member in IAENG and Senior Member in UACEE.

Dr. A. Christy Jebamalar is currently working as Associate Professor in the Department of Information Technology at Sri Krishna College of Technology, Coimbatore, Tamil Nadu, India. She received her Master’s degree from Anna University, Coimbatore, Tamilnadu, India in the year 2009 and her Ph. D in the year 2019 from Anna University, Chennai, Tamilnadu, India. She has 14 years of teaching experience. Her research interests include Pervasive Computing and wireless indoor localization systems.