Regular Article

Nilesh Marathe, Nikita Kulkarni, Nilesh Rathod*, Jyoti Jadhav, Pratik Kanani, and Sharmila Rathod

Adaptive multidimensional trust-based recommendation model for peer to peer applications

https://doi.org/10.1515/eng-2024-0049
received September 01, 2023; accepted May 27, 2024

Abstract: In today's world, the widespread utilization of services such as Nearby Share, Near Field Communication (NFC), and Wi-Fi Direct for deploying various applications has significantly bolstered the demand for reliable and secure distributed ad-hoc peer-to-peer networks. Yet, ensuring the trustworthiness of participating nodes remains a significant challenge. Trust among nodes plays a pivotal role in collaborative network applications, especially in environments like Mobile Ad-hoc Networks and VANET (Vehicular Ad-hoc Networks). Evaluating the trustworthiness of nodes is essential for promptly identifying misleading entities, thereby preemptively preventing their involvement in ongoing transactions. Attributes or characteristics exhibited by nodes, such as honesty, selfishness, or malicious behavior, serve as key factors in trust computation. The effectiveness of trust evaluation directly influences the encouragement of honest nodes and the deterrence of malicious ones, thereby nurturing a healthy and competitive network ecosystem. Recognizing the dynamic nature of network environments, trust computation methods must be adaptable and diverse. The adaptive multidimensional trust (AMT) model introduced in this article goes beyond simple reputation assessment. It offers three distinct methods such as Direct Trust ($\text{Direct}_{\text{Trust}}$), multiple security parameters, identification of qualified recommenders, which got selected dynamically as per change in trust ratings of peers. AMT advocates for an incentive-driven approach to identify legitimate peers, monitoring gradual increases in their performance ratings, whereas, spikes in performance alert to potential colluding peers or nodes displaying erratic behavior. This article evaluates the effectiveness of the AMT through a case study focused on an E-commerce application. It scrutinizes the model's performance across different percentages of malicious nodes within the network, providing a thorough analysis and discussion of the results based on the trust value of malicious and benign peers and efficiency by selecting genuine service for transaction.

Keywords: trust computation, transitive trust, trust model, trust vector, polling, transaction risk, trust mechanism, group recommend, collaborative, colluding, dynamic behavior

*** Corresponding author: Nilesh Rathod**, Department of AI-ML, Dwarkadas J. Sanghvi College of Engineering, Mumbai, India, e-mail: nilesh.rathod@djsce.ac.in
Nilesh Marathe: Department of CSE(DS), Dwarkadas J. Sanghvi College of Engineering, Mumbai, India, e-mail: nilesh.marathe@djsce.ac.in
Nikita Kulkarni: Department of Computer Engineering, K J College of Engineering and Management Research, Pune, India, e-mail: nikitakulkarni.kjcoemr@kjei.edu.in
Jyoti Jadhav: Department of Information Technology, Ramrao Adik Institute of Technology, D.Y. Patil Deemed to be University, Navi Mumbai, India, e-mail: jyoti.jadhav@rait.ac.in
Pratik Kanani: Department of AI-DS, Dwarkadas J. Sanghvi College of Engineering, Mumbai, India, e-mail: pratikkanani123@gmail.com
Sharmila Rathod: Department of Computer Engineering, MCTS Rajiv Gandhi Institute of Technology Andheri, Mumbai, India, e-mail: sharmila.gaikwad@mctrgit.ac.in

1 Introduction

The randomness in the node behaviors allows it to leave or join the groups with common interest anytime, which is the major challenge for trust computation. The community-based group formation misleads the reputation-based trust computation by giving collaborative feedback. The credibility factor proposed in the adaptive multidimensional trust (AMT) addresses these issues.

The proposed system is a collaborative and adaptive approach, which associates trust mechanism in P2P network model and weighted application-specific attributes, e-transaction characteristics. The resource selection for group-based applications is the key factor influencing secure successful communication. It has two major challenges that need to be addressed:

1) Trustworthy node selection that provides reliable service even though the selfish/malicious nodes exist in the network.
2) Encourage the resource nodes to provide reliable service as well as punish misbehaving nodes.

The proposed model can be used for any group-based application. The model is designed in the four levels. The peers are motivated to perform better by gradually increasing peer's trust value and intern upgrading the level and status, whereas in case of malfunction, it cut down sharply. The credibility and trust value are calculated by considering different parameters for different methods used. The situation-based dynamic switching is performed between these methods for using different ways of trust calculation.

This article is organized to elaborate the literature survey in Section 2, and Section 3 describes the details of the proposed adaptive multidimensional trust model. Section 4 discuss the results and analysis of the model. Section 5 concludes the article, and references are presented in Section 6.

2 Literature survey

In a trust paradigm, there are two ways to handle global information. One method is to create an administrative center to gather proof from all nodes (users), after which the center can compute the global trust and make it available to all users.

The Eigen Trust [1] reputation system is one example of a method to compute a distinct global trust for each user in a distributed manner that reflects the interactions of all users in the network with the user. An administration center is not required for such a global architecture, but it is challenging to ensure a quick and secure convergence when calculating the global trust.

Trust and reputation-based models have emerged as essential mechanisms to enhance the security and reliability of P2P networks. This literature survey seeks to provide an overview of the latest advancements in research pertaining to models focused on measuring the reliability of the peers for secure communication in P2P-based application environment.

TBMOR [2]: An efficient trust-oriented model designed to enhance secure routing in opportunistic networks. The article presents TBMOR, a lightweight and efficient model that evaluates trustworthiness among nodes and selects reliable routes. Through simulation-based evaluations, the authors demonstrate the model's effectiveness in mitigating malicious behaviors and improving message delivery rates in opportunistic networks. The proposed TBMOR model contributes to the advancement of secure routing protocols in challenging and dynamic communication environments.

Jiang *et al.* [3] proposed a novel approach to enhance the accuracy of recommendation systems for online shopping using a trust-based combination filtering. The algorithm leverages trust relationships between users to improve the quality of item recommendations. The article introduces a comprehensive evaluation of the proposed algorithm, demonstrating its effectiveness in providing personalized and trustworthy recommendations in E-commerce settings.

Jiang *et al.* [3] propose a novel approach that collaborate user with similar interest with slop algorithm to enhance the accuracy of E-commerce recommendation systems using trust-based collaborative filtering. The algorithm leverages trust relationships between users to improve the quality of item recommendations. The article introduces a comprehensive evaluation of the proposed algorithm, demonstrating its effectiveness using Amazon dataset in providing personalized and trustworthy recommendations in E-commerce settings. Still it can be more improved by considering the vector of attributes for recommendation calculations.

Wang *et al.* [4] perform the survey of recommender system and finds to have more granularity in consideration of given recommendation. The author is trying to address the question as "How much the recommendation is trustworthy?" He proposes the framework for the "Trustworthy Recommender Systems," which likely to explore the challenges in building recommender systems that prioritize trustworthiness and reliability. It covers the four-phase framework that process the data and obtain more accurate results. It also covers various approaches to integrate trust models into recommender systems, enabling users to receive more accurate and personalized recommendations. This framework will be very useful for customizing it according to application.

Ge *et al.* [5] highlight the need of building trustworthy recommender systems which provides a comprehensive, transparent mechanism. The survey encompass the classification of recommendations based on its prospective. User satisfaction and robust mechanism are key points highlighted in this article. It explores how trust factors, social relationships, and reputation metrics are integrated into the recommendation process. The article also discuss privacy and security concerns and propose methods for building transparent and fair recommender systems. By keeping in consideration of this need, it becomes necessary to have multiple dimensionality to consider for trust calculations.

Canturk *et al.* [6] propose that "trust-aware location recommendation" explores the challenges and methods for providing trustworthy location recommendations in location-based social networks (LBSNs). The survey investigates various graph-based algorithms and techniques used to incorporate trust information from the social network to enhance the accuracy of location recommendations. It delves into the use of trust relationships and

user interactions to build personalized recommendation models. The article also discusses the evaluation of the proposed graph-based approach through real-world experiments or simulations, demonstrating its effectiveness in generating reliable and relevant location suggestions. In addition, it could identify potential areas for future research in the domain of trust-aware location recommendation in LBSNs.

Nirmaladevi and Prabha [7] present a novel approach for addressing the challenges posed by selfish nodes in mobile ad hoc networks (MANETs) to achieve reliable routing. The literature survey explores the existing routing protocols and mechanisms to handle selfish nodes' behavior. It discusses trust-aware algorithms that evaluate node reliability based on their past behavior and interactions. The article introduces an optimized clustering technique to enhance the network's overall efficiency and reduce overhead. The survey demonstrates the effectiveness of the proposed protocol in mitigating selfish node behavior and improving the reliability of data routing in MANETs. In addition, it identifies potential future research directions to further improve the trust-aware and optimized clustering-based routing approach.

Mahamune and Chandane [8] explore the challenges of secure communication in MANETs and proposed a trust-based co-operative routing approach to address them. The literature survey delves into the existing routing protocols and security mechanisms used in MANETs. It discusses the importance of trust in enhancing communication reliability and mitigating malicious behavior. The article introduces the trust-based co-operative routing model, where nodes collaborate based on trust levels to establish secure communication paths. Through simulations or real-world experiments, the survey demonstrates the effectiveness of the proposed approach in achieving secure communication and resilience against attacks in MANETs. In addition, it identifies potential future research areas to further enhance trust-based co-operative routing for secure communication.

Korir and Cheruiyot [9] present a comprehensive survey of the security challenges faced by current MANET routing protocols. The literature survey explores various existing MANET routing protocols, such as AODV, DSR, and OLSR, and assess their vulnerabilities to different types of attacks, including blackhole attacks, wormhole attacks, and selective forwarding. It discusses the importance of secure routing in MANETs and the impact of security breaches on network performance. The article also highlights the limitations of existing security mechanisms and propose potential solutions to address the identified security challenges. Through the survey, the author aims to provide valuable insights into the state-of-the-art research in MANET security, guiding future improvements and developments in secure routing protocols for MANETs.

Goel *et al.* [10] focus on improving malicious node detection in extensive networks to maximize throughput. The literature survey reviews existing methods for detecting malicious nodes in large-scale networks, such as wireless sensor networks or MANETs. It explores various techniques, including anomaly detection, trust-based approaches, and statistical analysis, used to identify malicious nodes attempting to disrupt network communication. The article proposes an improved detection method, possibly incorporating machine learning algorithms or data analytics, to enhance the accuracy and efficiency of detecting malicious nodes. Through simulations or real-world experiments, the survey demonstrates the effectiveness of the proposed method in achieving maximum throughput while ensuring network security. In addition, it identifies potential areas for further research and improvements in the domain of malicious node detection in extensive networks.

Gyawali *et al.* [11] explore and analyze existing research on misbehavior detection systems in vehicular networks, focusing on machine learning and reputation-based approaches. It investigates the challenges faced in securing vehicular networks against internal attacks and discuss the potential vulnerabilities of cryptographic methods. The survey also examines previous techniques for enhancing detection accuracy and reliability in vehicular networks and compare their performance against the proposed method. In addition, the survey discusses the application of Dempster-Shafer theory and the use of reputation-based mechanisms in other network security contexts to provide a broader understanding of their effectiveness. Overall, it would aim to situate the proposed machine learning and reputation-based MDS within the current state of research and highlight its contributions and advantages in enhancing security in vehicular communication networks.

The concept of multidimensional trust, also referred to as trust parameters, trust factors, or trust dimensions, is explored in various research works. Wang and Wu [12], for instance, introduces a three-dimensional trust model encompassing integrity, benevolence, and ability within the domain of e-commerce. This research highlights that distinct trust dimensions exhibit statistical differences and exert varying influences on e-commerce outcomes. In addition, Griffiths contributes to the field by offering a mechanism for agents to model multiple dimensions of trust and integrate them with other factors when making decisions regarding collaborative partnerships. It is worth noting that this work does not address recommendation trust (indirect trust) and does not facilitate the sharing of trust-related information.

Three fundamental trust parameters, two adaptive components [13], and a general trust metric are all part

of the PeerTrust model that Xiong and Liu [14] proposes. To the best of our knowledge, the majority of currently published research either treats each dimension separately or integrates them together to denote a single overall trust.

We aim to implement a customized and dynamically adaptive approach that increases the complexity of trust calculation in high-priority scenarios, while maintaining simplicity in environments with a lower impact of malicious nodes. This strategy allows for efficient resource allocation, ensuring robust trust evaluation where it is most needed and streamlined processing where the threat level is lower.

3 Objective and motivation

In an open ad-hoc environment, maintaining a fixed set of parameters can often be too rigid to adapt to application-specific challenges. Therefore, it is essential to propose a customized set of parameters tailored to address the specific demands of the application environment.

We expect to design a framework for distributed P2P applications and achieve the following objectives.

3.1 Motivate the economic and nonmalicious resources to provide the best services as possible: Incentive approach

The genuine resources have to be motivated to give the best service with the good economical rate. The model proposes the level structure that categorized the peer from lowest zeroth level to highest third level. These levels are designed to measure the credibility level of the peer. As high as level of the peer, it is more trustworthy and also allows getting more benefits per transactions. The trust value is gradually increased based on the ratio of successful versus total transactions that increase the credibility of the peer as per the level.

3.2 Reduce the impact that malicious resources have on the system as a whole; perish the nodes

As the trust value gradually increases for successful transaction rate, it slashed down for every unsuccessful transaction. We are keeping the eye on such peer if their success rate falls below threshold, or they continuously perform poor and then we put them in the black list. These black list ids are circulated among the groups to avoid transactions with such peers [15–19]. Even while selection of the peer, we consider the global feedback rating than relying on any one peer feedback.

3.3 Provide a facility for an economic user access the best resources possible: Try to provide benign service only

The users are allowed to select any resource group based on certain set of attributes as per the application. In our case, we have consider the E-commerce applications, and we have given asset cost, transaction cost, expected delivery time, incentives, and services as attributes for selection of the peer. So the economic user can select the resource peer according to his requirement where every transaction is monitored with eagle eyes regardless of transaction cost given to resource peer.

3.4 Allow per usage contracts for greater flexibility compared to long-term contracts: Evaluate every transaction as a whole

There is no such binding among the user and resource regarding the number of transaction to be performed with that resource peer. So for every new transaction, user can poll for available resource groups and select each time a new group. The system also keeps that eye on users peers to track the malicious users.

4 The proposed AMT

The proposed AMT is generalized solution applicable for P2P based application. For demonstrative and implementation purpose, P2P E-commerce-based applications are considered for the case study.

4.1 Brief

A unique identification of the node is achieved using global user identification number (GUID) associated with his

group. The model is designed in the four levels. The peer get introduced in the level 0, and based on their performance, peer dynamically switches between the levels. The credibility and trust value are calculated by considering different parameters for different methods used. The situation-based dynamic switching is performed for selection of the specific method, which follows different ways of trust calculation.

In this model, the roles of the peer or peer status can be categorized as user or client peers, resource or provider peers, and reference peers. The nodes which require service or utilize the network for their job are known as user or client peer. The peer who provides the service called resource or provider peer, and the peer who just give the suggested list of resource peers is called recommender. A peer say as I need some service it can poll or send the request to all resource providers. The "recommender" or "provider" peers can only provide the service, whereas the peers with status as "user" are not allowed to provide the service unless they become the "provider." So the interested provider who has required product will send the reply, and based on the calculated trust value, set of attributes (S_{Val}), or rating included in the certificate, user peer decides whether to transact with the peer. If the calculated trust value is above the threshold, then the peer is considered otherwise go for the next interested resource peer in the list. Once the transaction is completed, user peer recalculates the peer score and the trust value. These new values will be used to decide whether the peer is good peer or malicious peer.

The model uses a term called satisfaction value, which describes different attributes of the product and transaction demanded by the user. This will add multiple dimensions for peer selection.

Satisfaction value: The satisfaction value (S_{Val}) is calculated by considering different attributes according to the type of application. We can define the satisfaction value by formula (1).

$$S_{\text{Val}} = \sum_{k=0}^{n} (W_k) a_k, \tag{1}$$

where S_{Val} is a satisfaction value, W_k is the weight assign to attribute, and a_k is the product and transaction characteristics.

4.2 Trust model

A major of node reliability and credibility is represented by trust rating evaluated for each peer node against the previous transaction it has completed. The trust model proposed here have considered some basic principles:

1. The peers are classified in three roles or status: user, provider, or recommender. The peer can play any role but one at a time. Only user peers are not allowed to provide service, whereas requester can be anyone.
2. Each peer is bifurcated based on its trust value in four levels. The peers dynamically switched among the levels and its status based on the trust rating. The transaction cost per job may increase as moving toward higher levels.
3. The provider or recommender can provide the services to users peers who belong to same or lower level than the provider level.
4. A linear increase in peer's trustworthiness value is the reflection of his consistent good behavior, whereas it decreases exponentially for nasty or bad response even for one transaction.
5. The blacklisted node is the punishment for nodes that provided bad responses over the transactions.

The participant's direct interaction experiences, recommendation from others, and reference peer recommendation considered through multiple dimensions are the major parameters of trust calculations.

Figure 1 elaborates the concept of different levels in the proposed trust model. Each level is a representation of complexity of trust calculations and reliable environment. The increasing order of layers depicts.

- Increase in transaction cost.
- Harden the trust calculations.
- More secure environment.

The level of the peer is also mapped respectively to match proposed level architecture. The change in the trust value of peer slides it dynamically among the levels. The level wise distribution of trust range from 0 to 1 is bifurcated as follows:

- L0 (TrustValue range = 0.0–0.24)
- L1 (TrustValue range = 0.25–0.49)
- L2 (TrustValue range = 0.5–0.74)
- L3 (TrustValue range = 0.75–0.1)

Four trust methods per level were selected dynamically based on the application scenario.

The peer roles are also change dynamically based on its trust value. If it is greater than the 60% of the trust range at respective level, the peer role will become the "provider," whereas if it is greater than 90%, the peer role will become the "recommender."

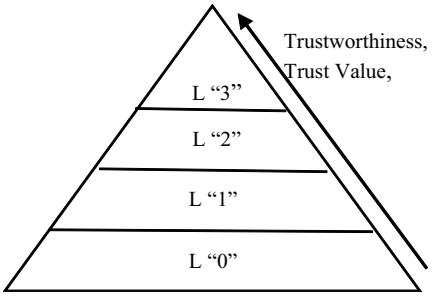

Figure 1: Proposed layered trust model.

4.3 Framework for trust value calculation

Trust value is the reflection of nodes consistency in performing the job. The proposed framework considers multiple parameters and applies different constraints for trust value calculation.

Majorly trust value calculation is depending on three parameters as given in Equation (2):

$$\text{Trust}_{\text{value}} = w_0 \times \text{Direct}_{\text{Trust}} + w_1 \times \text{Indirect}_{\text{Trust}} + w_2 \times \text{Trust}_{\text{parameters}}, \quad (2)$$

where w_0, w_1, and w_2 are the weights providing the flexibility for parameter weightage consideration with the condition as shown in Equation (3):

$$w_0 + w_1 + w_2 = 1. \quad (3)$$

In the proposed AMT, majors used for calculation of $\text{Direct}_{\text{Trust}}$ in each method are same, but for $\text{Indirect}_{\text{Trust}}$ and $\text{Trust}_{\text{parameters}}$, it varies based on the trust level and application requirement.

As most reliable peers gradually reach to the level 3 and 4, the complexity of trust calculations can be reduced by considering feedback of direct and indirect nodes, but for lower levels where the chances of malicious activities are more, multidimensional approach plays a crucial role. Let's define each parameter given in above Equation (3).

4.3.1 Direct trust ($\text{Direct}_{\text{Trust}}$)

The quality of service provided by participating peer (i, j) in the transaction is majored using $\text{Peer}_{\text{Score}(i,j)}$, which is a representation of direct trust as shown in Equation (4):

$$\text{Direct}_{\text{Trust}} = \left(\frac{\sum_{n=1}^{N} \text{Peer}_{\text{Score}(i,j)}}{N_{ij}} \right). \quad (4)$$

$\text{Peer}_{\text{Score}}$ depends on the satisfaction ratio of the product requested by the user peer and delivered product quality.

4.3.2 Indirect trust ($\text{Indirect}_{\text{Trust}}$)

The reliability of node is assured when it compared against indirectly calculated trust. The reflections of node consistency while behaving with different peers is measured based on nodes past transaction experiences with that nodes referred as indirect trust.

The proposed credibility factor confines the effect of indirect trust based on quality of node, which has participated in indirect rust calculations. The AMT model propose four different methods for the calculation of the credibility each consider different parameters according to the situations.

4.3.3 Trust parameters ($\text{Trust}_{\text{parameters}}$)

The proposed multidimensional approach insists to consider the application specific parameters to measure the quality of work done by the resource node. It is possible to define the multiple attributes with flexibility of weightage of each attribute to vary according to the application demand. The application specific parameters to be considered here are presented in the following sections:

4.3.3.1 Performance analysis

Monitoring and evaluation of the behaviors of the node in the participating transaction is the key for the reputation model. In the current ecommerce works, every stakeholder is participating in the feedback process seller as well as purchaser in the same manner, and every online services have to be rated and incentives to be given for successfully providing the service. It is always advisable to consider the feedback in different aspects and collect rating for different components of the service. Thus, the proposed model define a measure called satisfaction value (S_{Val}) (Equation (6)), which is a vector composed of the attribute factors to represent participant's performance. Along with the duration factor, we use this value to calculate $\text{Peer}_{\text{Score}}$ after every transaction. Let $\text{Peer}_{\text{Score}}(a, b)$ be a performance measure of transaction done between the participating node a and b computed as shown in Equation (5).

$$\text{Peer}_{\text{Score}} = [\beta \times (S_{\text{Val}}) + \alpha \times (\text{Deliverytime}_{\text{ratio}})] \times \text{Risk}_{\text{Value}}, \quad (5)$$

where $\beta + \alpha = 1.0$ are the weights assigned to the attributes S_{Val} and $\text{Deliverytime}_{\text{ratio}}$. S_{Val} is the satisfaction value (customized equation).

$$S_{\text{Val}} = \sum_{k=0}^{2} (W_k) a_k, \quad (6)$$

W_k is the weight assigned to attribute a^k. It is possible to generalize these attributes according to the application. For e-commerce applications, the model has considered the following attributes:

- a_0: Cost = Product_cost + Tran_cost
- a_1: Product category
- a_2: Incentives

where w_0, w_1, andw_2 are the weightages assigned to attributes a_0, a_1, and a_2, respectively, in such a ways as $w_0 + w_1 + w_2 = 1$.

Deliverytime_ratio:

$$\text{DeliverTime}_{\text{ratio}} = \frac{\text{Delivery}_{\text{Act}}}{\text{Delivery}_{\text{Exp}}}. \tag{7}$$

It is the ratio of the product ensured delivery time versus actual product delivery time.

4.3.3.2 Risk tolerance ($\text{Risk}_{\text{Value}}$)

Colluding attack is the major hurdle for genuine trust calculation, so it is always better to weigh the feedback given by the resource peer against its credibility. This increases the risk tolerance of the system rather than considering the feedback as it is.

The feedback of consistent peer will have high weightage rather than random behaving peers. So risk tolerance of each node is measured by Risk_Value that increases with experimentally justified value 0.04 if it satisfies following constraints:

- At lower level L0, reliable behavior is at least for 50% of participated transaction.
- At level L2, reliable behavior is at least for 60% of participated transaction.
- At level L3, reliable behavior is at least for 70% of participated transaction.
- At level L4, reliable behavior is at least for 90% of participated transaction.
- There is a decrease by 0.08 even for one bad performance.

The Risk_Value of every peer is updated for 10 recent individual transactions, and this verifies the consistency of node.

4.3.3.3 Deterioration factor

Trustworthiness of peer is need to be measured against the consistent behavior. The trust calculations should not be changed because of influence of one good transaction. It is necessary to control dynamic behavior of node or at least reflect it over that nodes trustworthiness. So a window of recent 10 transactions are considered as deterioration factor by which consistence of node can be observed. Track over the recent transaction will play the major factor to put eye on capricious nodes.

4.3.3.4 Credibility of feedback

It is always considerable to judge the feedback based on the credibility of node who is giving the feedback. The weightage of feedback given by evaluator is decided based on reliability of node. If its credibility is low, it is possible that the feedback is not considered. Because of this, peer can avoid itself suffering from bad peer's attack [4].

4.4 Trust calculation methods

Different factors considered for the trust calculation in the proposed method are defined in detail in previous section. This section incorporates different combinations of these factors in proposed multiple methods of trust calculation, which are adapted dynamically according to variation percentage of malicious nodes in the network and respective trust level. This will resist the colluding nodes from manipulating the trust value, as well as the flexibility of attribute selection makes it more appealing for any group-based application [20]. Let us have a look at the different method proposed, and the algorithm elaborated in next section will depict these method adaptability in our proposed secured environment.

4.4.1 Method 1 considers only Direct Trust ($\text{Direct}_{\text{Trust}}$)

Parameter for evaluation: It is most suitable at most trusted environment as Level 4 in ore model where rigorously evaluated resource peers only considered for participation. This is the elementary method where peer rely on direct feedback of the resource peer. The trust value is calculated based on his own experience with the resource peer. The peer which has good rating will be selected for performing the job. Here, the $\text{Trust}_{\text{value}}$ is calculated as shown in Equation (8).

$$\text{Trust}_{\text{value}} = w_1 \times \text{Tran}_{\text{sucessRatio}} + w_2 \times \left(\frac{\sum_{n=1}^{N} \text{Peer}_{\text{Score}(i,j)}}{N_{ij}} \right), \tag{8}$$

where the transaction success ratio $\text{Tran}_{\text{sucessRatio}}$ is calculated by considering the total number of transaction versus the total number of successful transactions.

The transaction will be considered as successful based on performance in current transaction, but also the difference between the old feedback score and new feedback score should be less than defined threshold value.

These trust values not only consider the feedback score given after every transaction but also consider the overall successful transaction performed by the peer. So even though we have a peer with average trust value if its success ratio is not good, it will be not get selected.

This method is selected when user peer has previously transacted with the provider peer (known peer), malicious peer ratio in the network is less than 20% of the total network size and the provider peer is not in the doubted list. So the risk involved to judge the peer only based on the direct trust is less.

4.4.2 Method 2 Multiple Security Parameters

This method involves multidimensional trust calculation [01, 02]. Here, we consider additional parameters for the calculation of trust value. These parameters are nothing but dimension of the trust, which we can consider separately without aggregating to one value. The trust value formula followed at this method is given in Equation (9).

$$\begin{aligned}\text{Trust}_{\text{value}} = {} & w_1 \times \text{Direct}_{\text{trust}} + w_2 \times \text{Prod}_{\text{Dimension}} \\ & + w_3 \times \text{Tran}_{\text{Dimension}}.\end{aligned} \tag{9}$$

- The product dimension (satisfaction value (S_{Val})) pertains to the particular good or service a user plans to buy. At this point, a user worries about the characteristics of the specific product or service the website promotes. The user may alter the weighting of the three criteria in our model that correspond to this dimension's durability, customization, and availability.
- The transaction dimension focuses on the process of delivery and the provision of after-sales services. In our model, we take into account three parameters associated with this dimension: payment options, refund policy, and promotions. It is important to note that the weighting of these parameters can be tailored to the preferences of the user.

This method is selected regardless of the fact that the user peer has previously transacted with the provider peer (unknown or known peer), and malicious peer ratio in the network is less than 40% of the total network size or the provider peer is in the doubted list. So the additional parameters help to mitigate the risk involved to judge the unknown or the peer present in the doubted list.

There are no sources in the current document.

4.4.3 Method 3 Identification of Qualified Recommenders

How many credible endorsers have suggested it determines its legitimacy. The recommenders are ranked according to the quantity of resource groups they have recommended and the amount of times they have been qualified recommenders. Expert recommenders in that trust area are those with the highest rankings. Their trustworthiness assessments are employed to guarantee the resource groups' dependability.

The majority of the resource peers are known by the qualified recommenders, who are chosen as qualified recommenders. A fresh list is made up of resource peers who have at least two qualified recommenders who know them. The requestor group can then use this list for other transactions.

The procedure for choosing qualified recommenders is summarized in **Algorithm 1**. The requester chooses the top N resource groups whose trust value exceeds a certain threshold before consulting the recommenders about their recommendations. To express whether the recommender r_i has direct trust experiences with the resource peer, a two-dimensional array RS is constructed with elements RS[i][j] that are either 1 or 0. Both recommenders who know fewer resource groups than TH_{rs_1} and recommenders who know less-resource groups than TH_{rc_1} are excluded. Based on the chosen resources and recommenders, a new RS array is created. As qualified recommenders, the top TH_{rc_2} recommenders who are familiar with the majority of the resource peers are chosen. Those resource peers with at least more than one qualified recommenders form new S. This list can then be used by the requestor group for further transactions. So the credibility is considered based on how many qualified recommenders have recommended it [4].

Algorithm 1. Identify Qualified Recommenders

1. Create a Recommender System (RS) table.
2. Calculate the total trust value $T[I]$ for each user i as the sum of trust values from all recommenders j.
3. Calculate the total trust value $S[j]$ for each recommender j as the sum of trust values from all users i.
4. Form a set R_c containing recommenders r_i, where $T[I] \geq \text{TH}_{rs_1}$.
5. Form a set S containing recommenders S_j, where $S[j] \geq \text{TH}_{rc_1}$.
6. Rebuild the RS table.
7. Recalculate the total trust value $T[I]$ for each user i as the sum of trust values from all recommenders j.
8. Sort the $T[I]$ values and select the top TH_{rc2} recommenders as R_c.
9. Forms a set S containing recommenders S_j, where QS[i][j] = 1

This method is selected regardless of whether the user peer has previously transacted with the provider peer (known or unknown peer), malicious peer ratio in the network is less than 60% of the total network size, and the provider peer is not in the doubted list. Here, we use opinions of more than one recommender to judge the reliability of the resource peers without relying on any one recommender.

4.5 Policy

Each peer group maintains three threshold values, Th_User Th_Provider and Th_Recommender. We are using different methods for calculation of the trust value of the peer group. Based on the network environment, any one of the method is dynamically selected. After calculation, the peers with trust value > Th_Recommender are treated as the most trusted peer referred as recommender in the group, which maintains the suggested list of peers who are genuine and consistently gives better performance. The peers with trust value < Th_user are treated as the malicious peer. The peers trust value > Th_Provider are selected for providing the service. If they provide the bad service, then they added in the doubted list. If the peer already present in doubted list and still it has provided the bad service, then it gets added in the black list. The peers with trust value > Th_User can be selected as the user peer even though they are provider or recommender. The user peer will join the peer group with the highest trust value.

The selected peer group also verifies the user peer while providing the service. If the user peer is totally new to the system, then the group allows it to join by assigning basic trust value and use the multidimensional trust method to obtain additional parameters to judge its trustworthiness.

Upon utilizing the service by affiliating with a specific host peer group, the user peer proceeds to reevaluate the trustworthiness of the host peer group. This assessment is grounded in the quality of service delivered by the host peer group and the satisfaction experienced by the client peer during service usage. The same methodology employed for calculating the user peer's own trustworthiness is applied.

Subsequently, the client peer updates the host peer's certificate with the revised trust value. Furthermore, the host or provider peer assigns a rating based on the payment received from the user peer.

After joining one of the host peer groups to use the service, the user peer recalculates the trust value based on the host peer group's service quality and the client peer's satisfaction with the service, using the same methodology used to determine the service's trustworthiness. The certificate with the revised trust value is issued by the client peer to the host peer. Furthermore, based on the payment collected for the user peer, the host or provider peer assigns the rating.

After every 20 transaction calculate average trust value(Trust_value$_{Avg}$) and the successful transaction ratio(Tran$_{Avg}$) of the peer, based on this, we track the malicious peer in the network and prepare the black list and doubted list that circulated among groups. **Algorithm 2** elaborates the policy applied to trust calculations to either give them reward or punish them.

Algorithm 2 Trust-based Peer Status Evaluation

$Trust_{valueAvg}$ ← "calculated after every 20 transactions"
$TH_{Provider}$, Th_{User} ← Initialize thresholds
if $Peer_{status}$ = "*Reference*" **or** $Peer_{status}$ = "*Resource*" **then**
  if *TrustvalueAvg* > *THProviderU* **and** *TranAvg* > *ThTran* **then**
    Assign average trust value ($Trust_{valueAvg}$) to the peer.
    $Peer_{status}$ = "*Recommender*"
  else
    Reduce its Risk Value by 0.8.
    Put the peer in the doubted list.
  end if
end if
if $Peer_{status}$ = "*Resource*" **or** $Peer_{status}$ = "*User*" **then**
  if *TrustvalueAvg* < *THProviderU* **and** *TrustvalueAvg* > *ThUser* **and** $Tran_{Avg} > Th_{Tran}$ **then**
    Assign average trust value ($Trust_{valueAvg}$) to the peer.
    $Peer_{status}$ = "*Resource*"
  else
    Reduce its Risk Value by 0.8.
    Put the peer in the doubted list.
  end if
end if
if $Trust_{valueAvg} < Th_{User}$ **and** $Trust_{valueAvg} > Th_{basic}$ **and** *TranAvg* > *TranThr* **then**
  if $Peer_{status}$ = "*User*" **and** $Peer_{status}$ = "*New*" **then**
    Assign average trust value ($Trust_{valueAvg}$) to the peer.
    $Peer_{status}$ = "*User*"
  end if
else
    Peerstatus = "Malicious peer"
    Include the name in the blacklist.
end if

The peer is taken off the list of those who are doubted, placed on the black list, and expelled from the organization if the trust value falls below the cutoff.

4.6 Working of the proposed adaptive multidimensional model

When a client peer requests a certain product, it notifies its neighbors. The product name, category, and projected cost are all included in the request along with the client peer's GUID. When a host peer wants to provide service to a client peer, they respond with information such their own GUID, the name of the product, its category, and its price. Each peer in the system that has completed a transaction, or provided the goods, has a rating on their certificate that was given by the client peer. The host peer's rating reflects how well the host peer has served the client peer. The algorithm for a proposed model is given in two parts.

A: algorithm for client peer. (**Algorithm 3(A) and Algorithm 3(B)**)

B: algorithm for resource provider peer. (**Algorithm 4**)

3(A): Proposed algorithm for client peer i (service needing peer):

Algorithm 3(A) Trust-based Algorithm for User(Service-Needing Peer i): **Step 1:**

$T_{priorTran}$ ← Basic provider value at that level.
$Th_{provider}$ ← Threshold value of the provider peer.
repeat
Step 1: Send request to a randomly selected peer *u* for (GUIDi, name of Product, category of Product, expected cost of product)
if *u* sends a reply **then**
  if *u* does not have any previous ratings received **then**
    Use Method II Multidimensional Trust and ask for additional parameters about the product and transaction.
    Calculate trust Tu on the supplied parameters.
    if $Tu > Th_{provider}$ **then**
      S val = calculate satisfaction value
      Goto Step 2.
    else
      Goto Step 1.
    end if
  else
    if *u* is blacklisted **then**
      suspicious reply so do not consider and jump back to Step 1.
    else
      Certificate Exchange between user peer i and Provider peer u.
      Client peer *i* extracts the ratings (trust values) from the certificate.
      if size of blacklist < 20% of network size **then**
        if *u* is in the trusted list **then**
          if *Tu* > *Thprovider* **then**
            S val = calculate satisfaction value.
            Goto Step 2.
          else
            Goto Step 1.
          end if
        else if *u is a* suspicious node **then**
          Tu = Apply Method II for Trust evaluation
          if *Tu* > *Thprovider* **then**
            S val = calculate satisfaction value
            Goto Step 2.
          else
            Goto Step 1.
          end if
        end if
      else if size of blacklist < 60% of network size **then**
        if *u* is in the trusted list or not in the blacklist **then**
          Tu = Apply Method III
          if *Tu* > *Thprovider* **then**
            S val = calculate satisfaction value.
            Goto Step 2.
          else
            Goto Step 1.
          end if
        end if
      end if
    end if
  end if
until all the neighbors have been requested

Algorithm 3(B) Trust-based Algorithm for User (Service-Needing Peer i): **Step 2**

Step 2: Complete the transaction with selected peer.
$S_{valaftertran}$ = Evaluate the transaction quality using S_{Val}
$PeerScore_{aftertran}$ = Calculate the Peer score after the transaction.
$Tu_{aftertran}$ = Reevaluate the trust based on S_{Val}.
Update the trust value in the certificate.
if($|TuAfterTrans - TuPriorTrans| > \varepsilon$ **OR** $TuAfterTrans < THB$) **Then**
  $Risk_{Value}$ = decrease the risk value by 0.8.
  if *u* already present in the doubted list **then**
    Remove *u* from the doubted list.
    Add *u* to the blacklist.
    $Tran_{factor}$ = 0.
  else
    Put u in the doubted list.
    Tu = *Tuaftertran*.
  end if
else

17: **if** $Tu_{AfterT\ rans} > THA$ **then**
18: Put u in the trusted list.
19: Add u to the suggested list of the recommender peer.
20: $Tran_{factor}$ = 1.
21: $Tu = Tuaftertran$.
22: **end if**
23: **end if**
24: Update Tu of the selected host peer u stored locally.
25: Issue the rating (Tu) to peer u.
26: After every 10 transactions, update the risk value if the peer consistently performs well.
27: After every 20 transactions, peers update their own trust value.
28: Also, update peer level and peer status by comparing with Th_{min} and Th_{max} for level change and comparing with $Th_{P\ rovider}$ and $TH_{Recommender}$ for status change.

Algorithm for Resource Peer u (Provider peer)

Algorithm 4 Resource Peer u (Provider Peer)

1: Tu: Request comes for user peer i.
2: Verify the peer I authenticity and its presence in black list.
3: **if** user peer i is blacklisted **then**
4: Do not transact with peer i.
5: **else**
6: Respond to peer i: (GUIDr, Prod_cost, Prod_cat, Tran_cost, Del_time, Incentives).
7: **end if**
8: After performing transactions, check the payment status.
9: **if** User peer i successfully pays the agreed amount then
10: Tran_factor = 1.
11: Ti = issue the trust value.
12: **else**
13: Risk_Value = decrease the risk value by 0.8.
14: Tran_factor = 0.
15: **if** i is already present in the doubted list **then**
16: Remove i from the suspicious list.
17: blacklist the user peer i.
18: **else**
19: Mark Peer .
20: Tu = Taftertran.
21: **end if**
22: **end if**

The terminology/abbreviations used in the algorithm are as:

THA = upper threshold value
THB = lower threshold value
THprovider = threshold value of the provider peer
GUID = Unique Identification
Tu = Peer trust
Ti = Peer trust
Tran_factor = transaction factor to judge the satisfaction ratio
Prod_cost = Product sell cost
prod_cat = Product category
Tran_cost = Transaction cost
Del_time = expected Delivery Time
Incentives = incentives provided by seller for the purchase
Risk_value = risk value for transacting with the peer
$T_{\text{priortran}}$ = Default Trust
$T_{\text{aftertran}}$ = Evaluated trust value
ϵ = permissible limit for consideration of transaction
Peerlevel = Peer level for 0–3 as explained in chapter 6
Peerstatus = Peer status either Provider or Recommender or User
$\text{Th}_{\text{mlevel}}$ = Respective level minimum threshold value
$\text{Th}_{\text{mxlevel}}$ = Respective level maximum threshold value
$\text{TH}_{\text{Recommender}}$ = Recommender threshold value >90% of the trust value range at that respective level
$\text{Th}_{\text{Provider}}$ = Provider threshold value >60% of the trust value range at that respective level

4.7 The peer details

In the proposed AMT model, global user identity (GUID), which is a distinct identifier, will be connected to each peer in the system. Client peers or user peers are peers who require a service or product, and host peers are peers who offer the service or product.

Each peer in the system maintains the following list with itself.

(1) Certificate
(2) PeerInfo
(3) BlackListInfo
(4) DoubtedListInfo
(5) TrustedPeerInfo
(6) SuggestedPeerInfo

4.7.1 Format of the certificate

Each peer in the system owns certificate in which digitally signed rating provided by the client peers as well as the host peers, and digitally signed feedback ratings given to host peers as well as the client peers are stored. Certificate contains the rating of the host peer and hence also called as rating certificate. Certificate contains the following information:

1. Peer's own GUID
2. Public key
3. Value of trust
4. Rating received from other peers
5. Feedback rating given to other peers
6. Number of times service used

There is upper threshold trust value and lower threshold trust value. Peers having reputation above the upper threshold are trusted peers, and peers having reputation below minimum threshold are malicious peers.

4.7.2 PeerInfo

Each peer maintains a list of neighbor peer called PeerInfo. PeerInfo contains information GUID and public key of neighbor peer. A peer always sends information to other peer in an encrypted form. Receiving peer decrypts the information using public key of the sender stored in its own PeerInfo list.

4.7.3 BlackListInfo

Information about the malicious peers encountered during transaction is stored in the BlackListInfo. BlackListInfo contains malicious peer GUID and its public key. Transaction with the peers in this list is avoided. The peer is added in this list if it provides the deviated service more than once.

4.7.4 DoubtedListInfo

DoubtedListInfo contains GUID and public key of the peer who have suddenly given deviated performance while providing product. Transaction is done with peers in the DoubtedListInfo by asking him to provide the additional parameters for validateing its trustworthiness, but if peers continue their deviated behavior then they are included in the BlackListInfo.

4.7.5 TrustedPeerInfo

TrustedPeerInfo contains GUID and public key of the peer who have always given best performance. Such peers are called as trusted peers. A peer always transacts with the peer in the TrustedPeerInfo list.

4.7.6 SuggestedPeerInfo

SuggestedPeerInfo is maintained by the recommender or reference peers, contains GUID and public key of the peer, who have always given best performance. A peer always transacts with the peer who is present in more than two qualified recommenders SuggestedPeerInfo list.

4.8 Details of algorithm

Client peer i randomly selects one of the host peers whose status is not "User." If the chosen host possesses the requested product with the specified attributes, the user peer requests a certificate. Upon confirming that the chosen peer is not in the BlackList, client peer i proceeds to verify the certificate. Subsequently, client peer i calculates trust using its prior experiences and the information obtained from the certificate. This calculation can be performed using any one of the four methods proposed in the model. The resulting trust value serves as the determinant for client peer i in deciding whether to engage in a transaction with the host peer. If the calculated trust value surpasses a predefined threshold, the host peer is deemed trustworthy, and the transaction proceeds. Otherwise, if trustworthiness is not established, client peer i selects another host peer offering the same product and continues the process.

Once the product is received from the host peer, client peer i rates the host peer based on their satisfaction level and the quality of service provided. This rating is transmitted to the host peer, complete with a timestamp and digital signature. A copy of the issued rating is also retained by the client peer for potential future reference. The digitally signed rating received from the client peer is updated in the host peer's own certificate.

Conversely, after delivering the product to the client peer, the host peer assesses and rates the client peer according to the payment strategies determined and the final payment received. Similar to the client peer's process, the host peer sends this rating to the client peer along with a timestamp and digital signature. A copy of the rating issued is kept by the host peer for possible future verification. The digitally signed rating received from the host peer is updated in the client peer's own certificate.

Each peer within the system maintains a record of the trust value following a transaction. In addition, every peer maintains a blacklist containing information about malicious peers. If a host peer or client peer chosen for service

is found to be malicious, their rating is downgraded, and they are added to the blacklist. The client peer is responsible for updating the blacklist. Furthermore, each peer in the system maintains a list of peers who deliver either exceptionally poor or exceptionally good service suddenly; this list is referred to as the doubted list. If a peer selected for providing the product deviates from their usual service, and they are already on the doubted list, they are subsequently added to the blacklist.

4.9 Peer selection strategy

The THA and THB threshold values are maintained by each peer in the system. THB equals 0.30 and THA is 0.80. A peer's trust value is determined when it is chosen (status is "Provider" or "Recommender") using any one of the four techniques chosen based on the circumstance. The chosen peer is regarded as the most trustworthy peer and its service can be accessed without a doubt if the calculated trust value, say T_u > = TH_A. Tu is a harmful peer, and its service is unquestionably not used if T_u < TH_B, or less than the minimal needed threshold value. If TH_A > T_u > TH_B, the chosen peer is neither the least harmful nor the least trusted, and therefore, its service may be used. A client peer typically selects the trustworthy peer r for service.

Following the use of a host peer's service, the client peer updates the trust value T_unew based on the host peer's service quality and the client peer's pleasure with the service. The host peer receives a rating from the client peer, which also changes the trust value. The following comparison is made between the computed trust values before and after the transaction:

$$|T_u^{\text{new}} - T_u^{\text{old}}| > \sum$$

where T_u^{new} is the evaluated trust based on performance, T_u^{old} is the previous trust value, and $\sum$ is the permissible limit for consideration of transaction.

This peer is added to the list of peers who are doubted if the gap between the old and new trust values is larger than $\sum$. With the help of this technique, system peers are compelled to gradually improve or decrease their level of service. The peer who exhibits a rapid shift in behavior is downgraded and added to the list of peers who are doubtful because they are seen as posing a threat to the system. If the peer performs differently once again, they are taken off the doubtful list and added to the blacklist. The risk value is crucial in identifying malevolent peers that behave erratically. This tactic aids in the gradual expulsion of peers whose bad behavior is based on a specific pattern.

The client peer then signs the newly calculated trust value and issues it to the host peer whose service it has utilized. A freshly arrived peer's default trust value is chosen at random by the system. A newly arriving peer is given the chance to establish their reliability by rendering excellent service.

A client peer chooses the reputable host peer using the peer selection approach. Following the transaction, the client peer reviews the host peers according to its satisfaction by giving the host peer the digitally signed rating. In addition, the client peer can identify harmful peers with dynamic personalities and lessen the impact of cooperating peers.

5 Result and analysis

The implementation framework comprises a network of 100 nodes facilitating approximately 950 transactions, amidst varying proportions of malicious nodes within the network. Each peer's trustworthiness dynamically varies based on their involvement in the latest 10 transactions.

The graph analysis presented in this section offers insights into the efficacy of our proposed approach across 10 and 90% of malicious node presence within the network. Rather than benchmarking against alternative research methods, we focus on comparing various scenarios within a malicious environment. Our analysis delves into trust values, service selection outcomes, and transaction success rates to provide a comprehensive understanding of the results.

5.1 Trust value

Trust Value is a pivotal parameter in assessing transaction. For instance, a "provider" peer must possess a trust value exceeding 60% of the trust range at that level, while "reference" or "recommender" peers should have trust values surpassing 90% of their respective trust ranges.

In the testing environment, the network initializes each node with randomly assigned roles and appropriate trust values. When a provider peer engages in its inaugural transaction, it must furnish additional transaction parameters and product attributes. If the user peer deems the node trustworthy based on these parameters, it provides positive ratings. Conversely, inadequate service prompts the inclusion of the service provider peer in the user peer's doubtful list, accompanied by a low rating. Subsequent

instances of subpar service lead to the service provider peer's placement on the blacklist, precluding future transactions with it. Conversely, exemplary service garners high ratings for the service provider.

Every peer updates its own trust value in the certificate after every 20 transactions, taking into account the latest 10 transactions. The updated trust value undergoes verification for any alterations in peer level and status. The following presents a comparison of average trust values between trustworthy peers and malicious peers after every 40 and 840 transactions.

5.1.1 Analysis: (10% malicious peers)

Figures 2 and 3 depict a comparative analysis of trust values between trustworthy peers and malicious peers after completing 40 and 840 transactions, respectively, while 10% malicious nodes is present in the network. In Figure 2, the trust values of trustworthy peers demonstrate a steady ascent, indicating an incremental build-up of trust following successful transactions. Conversely, in Figure 3, the punitive measures taken against misbehaving nodes are illustrated by the decline in their trust values. This gradual decrease effectively isolates the nodes from the network over time, serving as a mechanism to mitigate their negative influence.

5.1.2 Analysis: (90% malicious peers)

Figures 4 and 5 present a comparative examination of trust values between trustworthy peers and malicious peers after conducting 40 and 840 transactions, respectively, in an environment where 90% of the nodes exhibit misbehavior. Figure 4 vividly illustrates the gradual augmentation in the trust values of trustworthy peers, indicative of a consistent reinforcement of trust over time. Conversely, Figure 5 starkly portrays the sharp decline in trust values among malicious peers. This notable decrease underscores the severe consequences of misbehavior, highlighting the effectiveness of the system in penalizing and marginalizing nodes that deviate from acceptable behavior.

Figure 6 shows a concluding observation, demonstrating that even in the presence of 90% malicious peers within the network, there is a discernible and steady rise in trust values among good peers. Conversely, the conspicuous plummet in trust values among malicious peers underscores their effective isolation within the network. This finding highlights the resilience of the system in

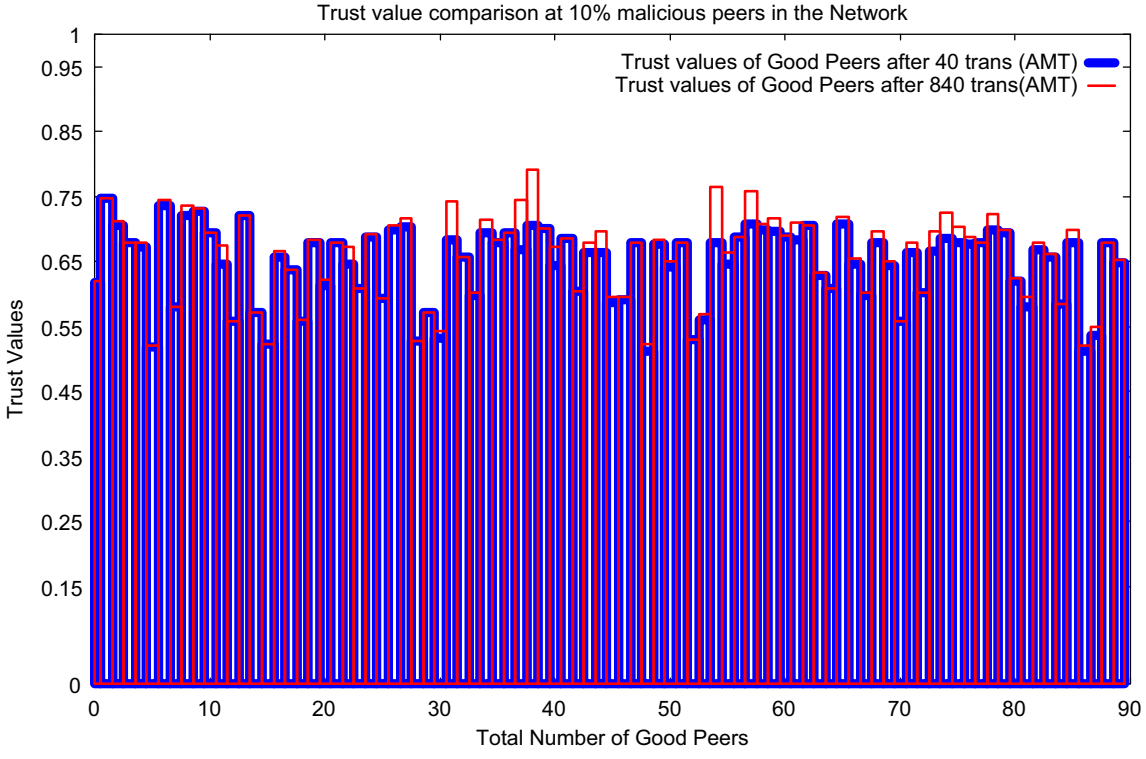

Figure 2: Trust values of good peers (10% malicious peers).

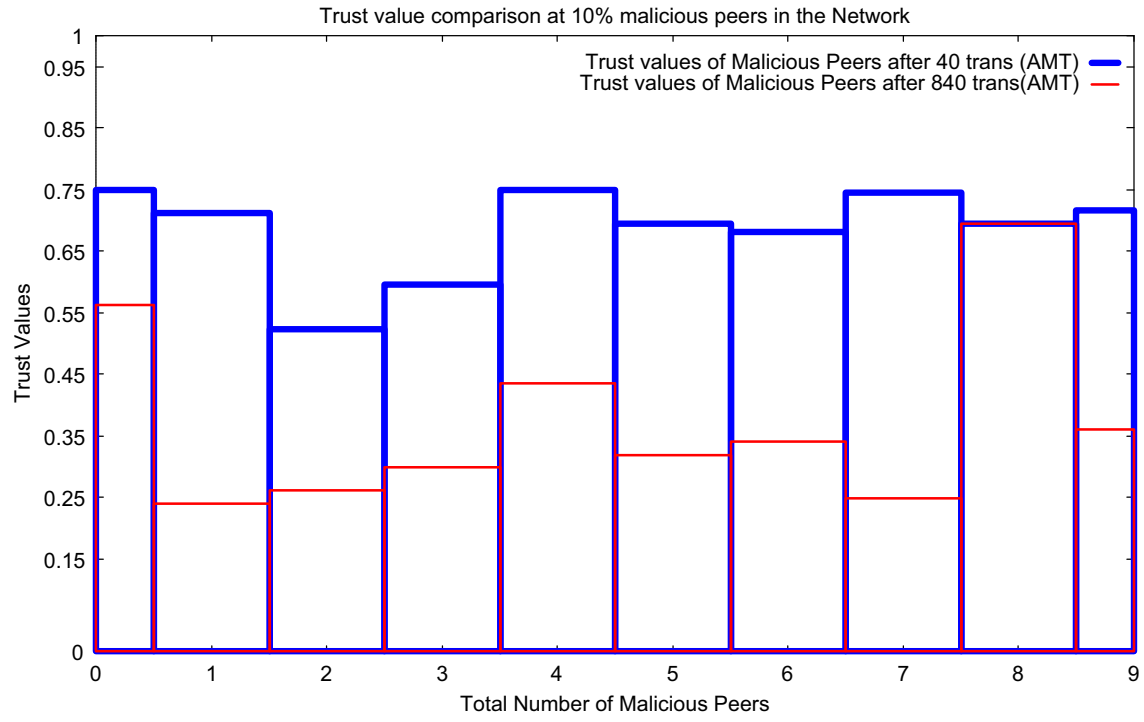

Figure 3: Trust Values of malicious peers (10% malicious peers).

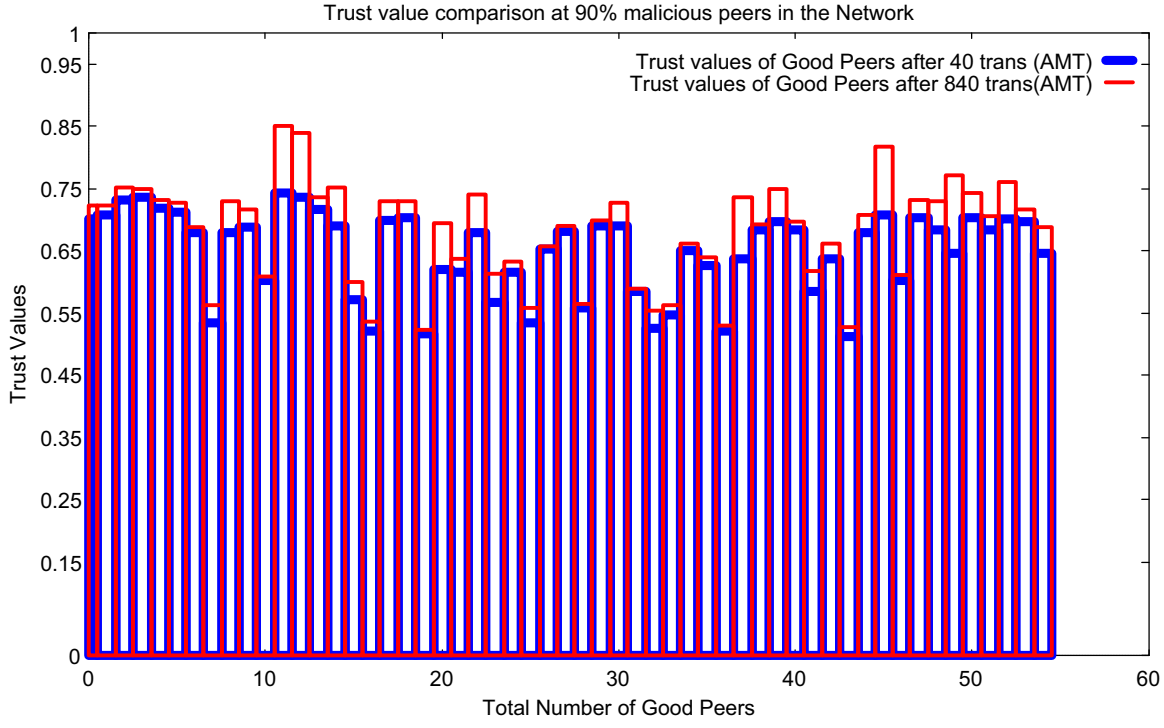

Figure 4: Trust values of good peers (90% malicious peers).

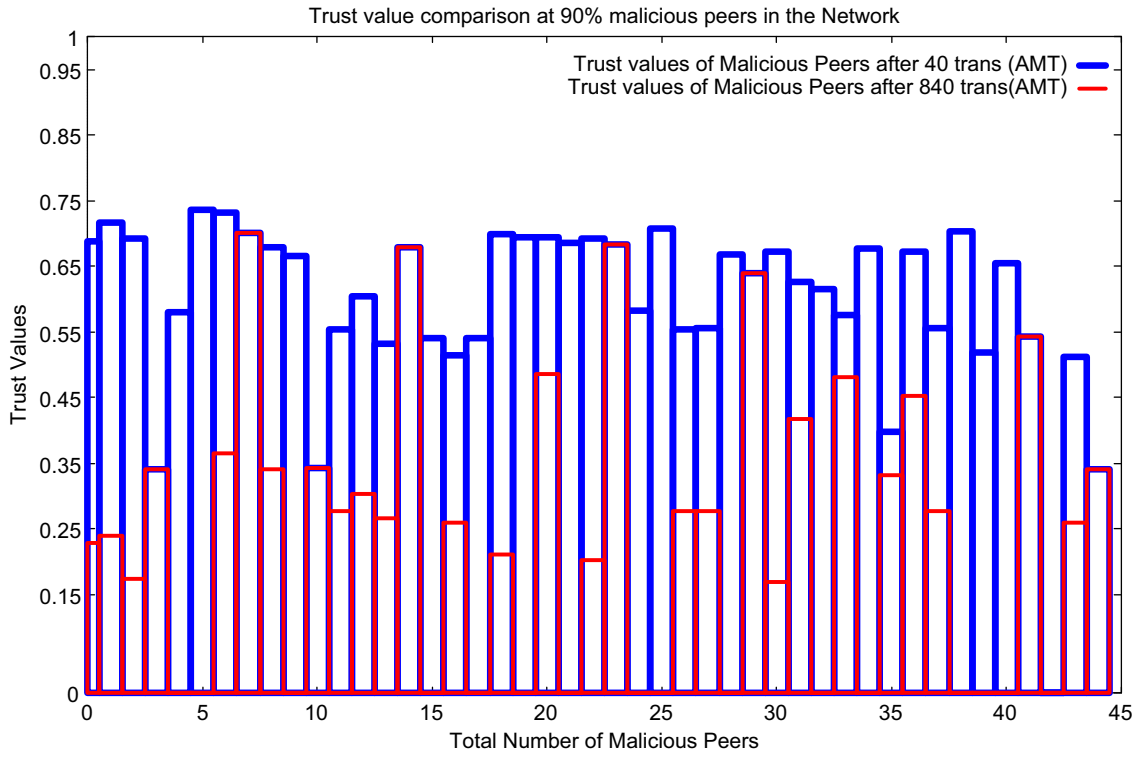

Figure 5: Trust Values of malicious peers (90% malicious peers).

Figure 6: Average trust values of the peers (90% malicious peers).

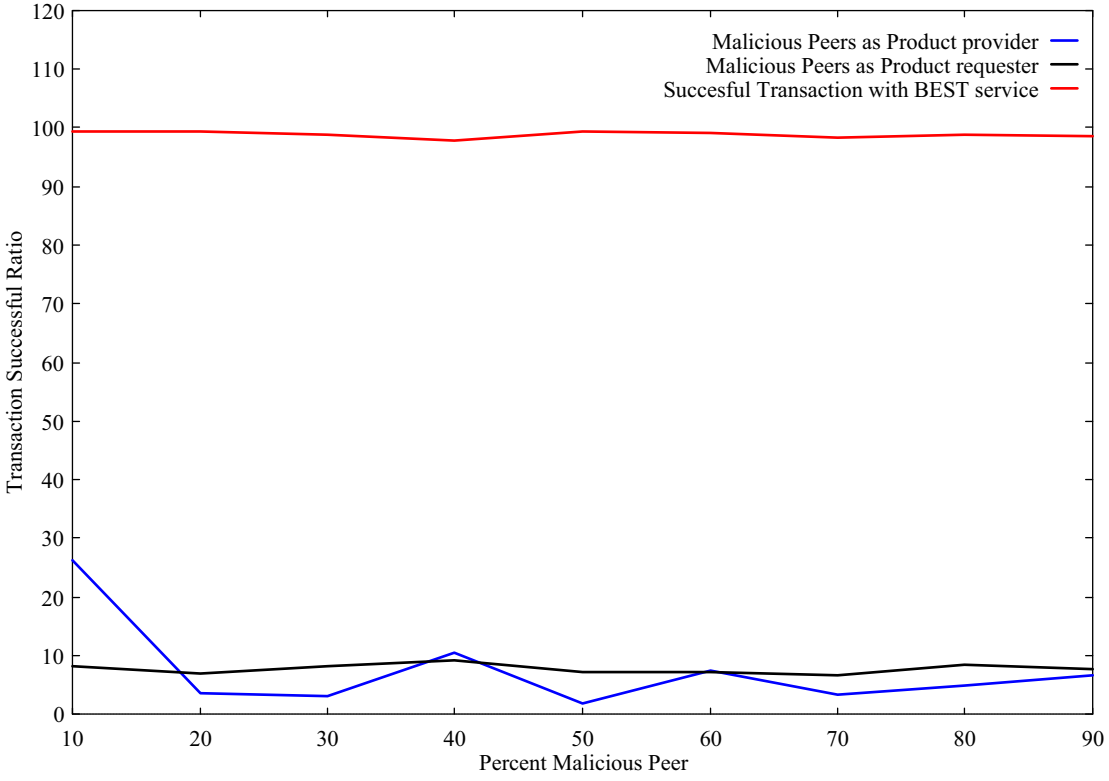

Figure 7: Best service selected (10–90% malicious peers).

fostering trust among cooperative peers while effectively containing and marginalizing disruptive elements, thereby ensuring the integrity and functionality of the network.

5.2 Transaction successful ratio

Figure 7 illustrates the simulation results across a spectrum of gradually increasing percentages of malicious peers within the network, ranging from 10 to 90%. The graph portrays the number of instances where the best service is provided during transactions, the occurrences of bad peers successfully serving other peers, and the instances where bad peers manage to utilize the services of other peers.

The metric of "best service" signifies the successful delivery of high-quality products, reflected by its proximity to 100%. In addition, the dotted line representing malicious requesters indicates their average usage pattern irrespective of the number of malicious peers in the network. Conversely, the inability of malicious providers to conduct successful transactions is evident, emphasizing their inefficacy within the network.

6 Conclusion and future scope

The proposed multilevel multidimensional adaptive trust model effectively identifies and monitors malicious peers within the network. Adaptability is a key feature, as the model dynamically selects an appropriate trust calculation method based on the prevailing circumstances when selecting peers for transactions.

Incentives are provided to good peers through a gradual increase in their trust values, thereby promoting trust-building within the network. Conversely, malicious peers face swift repercussions in the form of sharp decreases in their trust values, ensuring their accountability and discouraging disruptive behavior. Both providers and requesters are closely monitored to maintain network integrity.

The implementation of this trust model is underway using the Peersim simulator, which provides a solid foundational framework. While the model is currently tailored for e-commerce applications, its principles can be generalized to other domains by adjusting certain parameters related to satisfaction values, paving the way for broader applicability in future endeavors. The work can be further extended by implementing real-time simulations across various

applications such as file sharing, cryptocurrency transactions, and more. The results produced by these simulations can be analyzed to determine the percentage of genuine services selected over malicious ones, providing deeper insights into the effectiveness of the proposed trust evaluation method.

Funding information: Authors state no funding involved.

Authors contribution: All authors have accepted responsibility for the entire content of this manuscript and consented to its submission to the journal, reviewed all the results, and approved the final version of the manuscript. NM played a pivotal role in the conception and development of the research, foundation for defining the research problem and objectives, and proposed a comprehensive methodology. NK and NM were in bridging the gap between theoretical research and practical application, proposed adaptive layered trust model with a real-time case study in the eCommerce domain, and involved the meticulous validation, identification, and selection of parameters necessary for evaluating model's performance. NR played a crucial role in the publication process of the research, contributed significantly to the methodology by identifying an effective approach for measuring the credibility of nodes and validation. JJ played a vital role in ensuring the clarity and presentation of the research paper (formatting of the manuscript, adhering to the specific guidelines and standards), undertook the task of rewriting and revising the paper. PK provided invaluable insights into the dynamic and ad-hoc nature of the research environment, contributed by refining the performance metric parameters to better suit the specific needs of wireless sensor networks, played a key role in addressing reviewer feedback and implementing necessary changes, and validating the robustness of the model. SR was instrumental in the finalization of the manuscript through review process, conducted a thorough technical review, ensuring that the scientific content was accurate, coherent, and aligned with the research objectives.

Conflict of interest: The authors state no conflict of interest.

Data availability statement: The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.

References

[1] Su C, Zhang H, Ming Bi F. P2p-based trust model for e-commerce. 2006 IEEE International Conference on e-Business Engineering (ICEBE'06); 2006. p. 118–22.

[2] Su B, Hao Zhu B. Tbmor: A lightweight trust-based model for secure routing of opportunistic networks. Egypt Inform J. 2023;24(2):205–14.

[3] Jiang L, Cheng Y, Yang L, Li J, Yan H, Wang X. A trust-based collaborative filtering algorithm for e-commerce recommendation system. J Ambient Intell Humaniz Comput. 2019;10:3023–34.

[4] Wang S, Zhang X, Wang Y, Liu H, Ricci F. Trustworthy recommender systems. ACM Trans Intell Syst Technol. Accepted (October 2023). https://doi.org/10.1145/3627826.

[5] Ge Y, Liu S, Fu Z, Tan J, Li Z, Xu S, et al. A survey on trustworthy recommender systems. doi: 10.48550/arXiv.2207.12515.

[6] Canturk D, Senkul P, Kim S-W, Toroslu IH. Trust-aware location recommendation in location-based social networks: A graph-based approach. Expert Syst Appl. 2022;213:119048.

[7] Nirmaladevi K, Prabha K. A selfish node trust aware with optimized clustering for reliable routing protocol in manet. Meas: Sens. 2023;26:100680.

[8] Mahamune AA, Chandane M. Trust-based co-operative routing for secure communication in mobile ad hoc networks. Digital Commun Netw. 2023. doi: 10.1016/j.dcan.2023.01.005.

[9] Korir FC, Cheruiyot W. A survey on security challenges in the current manet routing protocols. Glob J Eng Technol Adv. 2022;12:78–091.

[10] Goel SS, Basha SM, dos Reis MC, de Albuquerque VHC, Lathar P, Alkhayyat A. Improved malicious node detection method for detecting a bait in an extensive network for getting the maximum throughput. IET Commun. 2022;1–8.

[11] Gyawali S, Qian Y, Hu RQ. Machine learning and reputation based misbehavior detection in vehicular communication networks. IEEE Trans Veh Technol. 2020;69(8):8871–85.

[12] Wang G, Wu J. Multi-dimensional evidence-based trust management with multi-trusted paths. Future Gener Comput Syst. 2011;27:529–38.

[13] Xiong L, Liu L. A reputation-based trust model for peer-to-peer ecommerce communities [extended abstract]. In ACM Conference on Economics and Computation; 2003.

[14] Lu Z, Mu H. A group-recommend based p2p e-commerce trust model. 2008 IEEE International Conference on Service Operations and Logistics, and Informatics. Vol. 1, 2008. p. 677–9.

[15] Sears W, Yu Z, Guan Y. An adaptive reputation-based trust framework for peer-to-peer applications. Fourth IEEE International Symposium on Network Computing and Applications; 2005. p. 13–20.

[16] Risan HK, Serhan FM, Al-Azzawi AA. Management of a typical experiment in engineering and science. In AIP Conference Proceedings. Vol. 2864, No. 1. AIP Publishing; 2024, January.

[17] Al-Zwainy F, Al-Marsomi M. Structural equation modeling of critical success factors in the programs of development regional. J Proj Manag. 2023;8(2):119–32.

[18] Al-Marsomi MSK, Al-Zwainy FMS. Assessing obstacles in construction-phases for regional development programs RDPs. Asian J Civ Eng. 2023;24(8):3425–36.

[19] Khan Q, Hayder G, Al-Zwainy FM. River water suspended sediment predictive analytics using artificial neural network and convolutional neural network approach: A review. In: Salih GHA, Saeed R.A. (eds). Sustainability challenges and delivering practical engineering solutions. Advances in Science, Technology & Innovation. Cham: Springer; 2023.

[20] QaraMohammed HN, Al-Zwainy FM. Strategic evaluation plan and improvement of cement plants (Iraqi Kurdistan Region-as a Case Study). Tikrit J Eng Sci. 2021;28(2). p. 124–36.