IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 1 December 2022, accepted 15 December 2022, date of publication 16 December 2022,
date of current version 22 December 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3230148

RESEARCH ARTICLE

An Uncertainty Trust Assessment Scheme for Trustworthy Partner Selection in Online Games

P SRIKANTH[1], ADARSH KUMAR[1], AND MUSTAPHA HEDABOU[2]
[1]Systemics Cluster, School of Computer Science, University of Petroleum and Energy Studies, Dehradun 248007, India
[2]School of Computer Science, Mohammed VI Polytechnic University, Ben Guerir 43150, Morocco

Corresponding authors: Mustapha Hedabou (mustapha.hedabou@um6p.ma) and Adarsh Kumar (adarsh.kumar@ddn.upes.ac.in)

ABSTRACT Purpose: An advances in technology, offline activities are moving toward online by creating the virtual environment (VE). The VE applications include video conferences, video chats, and massively multiplayer online games (MMOG) are interact to establish collaboration and resource sharing in VE by selecting random partners, which trigger various security challenges such as cheating in online games, uncertain behavior, and many others. Consequently, if the player acquires untrustworthy information from the selected partner, that exhausts untrustworthy information processing time as well as consumes the network bandwidth for transmission. Therefore, before establishing a collaboration with any selected partners, it is significant to assess the trustworthiness that enables fairness in online games and reduces untrustworthy information dissemination among the players. Method: the uncertainty trust assessment scheme, such as improved three valued subjective logic (I-3VSL), is leveraged to assess the trust among any two selected pairs. Further, the modified trustwalker (M-TW) algorithm is designed to discover the route from the trustor to the trustee that reduces the computational complexity by avoiding repeated computation once the longest search path is reached. Results: The experiment is conducted by establishing the arbitrary or bridge network. After that, the trust is assessed using I-3VSL with M-TW for various network sizes, depths, and iterations. The trust scores are compared with the assess trust (AT) and Trustwalker (TW) over the M-TW. The results show that the trust score increased $8-10\%$ over the AT and $7-9\%$ over the TW algorithm. Further, the computational complexity acquired as $O\left(n^2\right)$, which is optimized complexity compared to AT and TW. Conclusion: In MMOG, trustworthy partner selection is one of the most significant fields for artificial reasoning that assess uncertainty trust and represents the trust opinion in different forms. Therefore, the proposed work determines uncertainty trust more effectively compared to existing schemes.

INDEX TERMS Artificial reasoning, improved three valued subjective logic, massively multiplayer online game, uncertainty trust, virtual environment.

I. INTRODUCTION

Advances in Information and Communication Technology (ICT) and the immense evolution of online activities have progressed in Virtual Environment (VE) applications like Augmented Reality (AR) [1], virtual walkthroughs [2], [3], Massively Multiplayer Online Games (MMOG) [4], [5], [6] and many more. In MMOG, the players communicate with the other players' basis on content available to the neighbor players; from that, the opponent has selected randomly, which possesses the request contention problem, cheating in the online games, and uncertainty behavior [7], [8], [9]. Therefore, selecting a trustworthy partner by leveraging the trust assessment scheme is critical for the VE applications [10]. However, virtual games are initially devised using client-server communication. As a result, the partner selection relies on the server and preserves the trust ratings of the other peers based on their previous transactions. Besides, client-server communication is hampered by the service bottleneck and other problems. As a result, Peer-to-Peer (P2P) communication is leveraged in virtual gaming. In P2P, the peer's behavior changes over time since there is no central repository [11]. Besides that, in P2P virtual gaming, the information is shared among the players, including the players

The associate editor coordinating the review of this manuscript and approving it for publication was Kun Yang.

acquiring untrustworthy information from other players. The untrustworthy information processing and transmission consume the network bandwidth and cause the players' attention. Therefore, the proposed study focuses on creating VE that enables interaction and information sharing with other players by establishing trusting relationships among the players. Consequently, the players assess the trustworthiness of the received information based on the provider's trust. Additionally, it reduces untrustworthy information dissemination among the players.

The existing trust evaluation strategies are credential and reputation-based schemes. Credential-based schemes verify the user authentication before establishing the relations to access the desired content [12]. Reputation-based schemes assess the trustworthiness of opponents based on their reliability and service providers. Reputation-based schemes are widely employed in online forums where the participants are unfamiliar with each other. Hence, the unknown party's trustworthiness is determined based on the trust relationships with other parties' opinions and experiences [12], [13]. In other words, the selected players' trustworthiness is determined based on the recommendations of the other players with trusting relationships with trustors. The various reputation-based trust models are summation and average [14], topology-based models [3], [15], [16], [17], [18], PageRank [19], [20], [21], [22], [23], probabilistic [24], [25], [26], [27], [28], flow-based [29], [30], [31], and fuzzy models [32], [33], [34] that computes reputation based on the feedback. Conversely, the belief-based trust model, such as subjective Logic (SL), is the most prominent among all reputation models. The SL model evaluates the trust using direct and indirect trust interference. Further, this model characterizes interactions as trust, distrust, and uncertainty (neither trust nor distrust) [35], [36], [37], [38], [39], [40], [41], [42]. The SL model constantly preserves uncertain trust during the trustee's trust evaluation, implying that the uncertainty value never changes. Therefore, the three-valued subjective logic (3VSL) is designed to overcome the pitfalls of the SL model [43], [44], [45], [46], [47]. However, the 3VSL model requires enhancement in indirect trust assessment operations because the discount operation is not considering the distrust and posterior changes [45], [48], and the combining operations also require improvement. Therefore, the primary objective is to resolve the pitfalls of uncertainty trust more effectively and quantify trust between any pair of players based on their interactions.

The significant challenges in trust assessment

- ➢ The existing solutions to all-pair trust assessment approaches determine the trust among the players as a single quantity, such as trust or distrust. Nevertheless, it is impossible to judge whether the player is completely trusting or distrusting [45].
- ➢ Without a central repository, each peer must evaluate content providers' trustworthiness based on reputation systems. Hence, they have high computational and communication overhead [12].
- ➢ Cheating prevention and detection are the biggest challenge in a P2P environment [12].
- ➢ The SL trust assessment model produces inaccurate results for complex networks such as arbitrary or bridge networks [47], [48].
- ➢ The SL operation, such as the discount operation, does not support the association and cumulative rules that produce inaccurate results [41], [42], [43].
- ➢ The 3VSL indirect trust assessment operation, such as discounting, requires improvement since the trust opinions change over time. However, the discounting operation includes only the trust element and ignores other factors such as distrust and posterior. As a result, the changes in distrust and posterior do not influence the discount operation [48].
- ➢ The 3VSL combining operation also requires improvement because when the players' prior uncertainty opinions are equal to zero, the existing operation fails to derive the selected partner's trustworthiness
- ➢ All pair trust assessment schemes, such as assess trust (AT) and trustwalker (TW) algorithms, require improvement since they are slow in terms of execution time [45], [47], [49].

The main objective is to design the all-pair trust assessment scheme as the modified TW (M-TW) algorithm over the AT and TW. The M-TW algorithm significantly reduces the trust assessment execution time and provides accurate results for arbitrary networks. Moreover, the players' opinions are represented in the form of trust, distrust, and uncertainty. Further, the players establish interactions or trust relationships with other players based on the area of interest (AOI) and content availability through forming a network. The players' trust relationships are represented by leveraging the adjacent matrix. Thus, the adjacent matrix consists of the trust opinion, defined through the I-3VSL direct trust opinion. The trust of the selected partner is derived from the I-3VSL indirect trust assessment includes trust computation operations such as discounting and combining operations. Further, the trust computation complexity is optimized with M-TW over the AT and TW algorithm.

The main contributions of the proposed work are as follows

- ➢ The trustworthy partner selection is performed for an arbitrary or bridge network constructed by leveraging the Travian dataset.
- ➢ Devise the I-3VSL direct trust evaluation algorithm to determine the trust opinion based on the ratings.
- ➢ Devise the I-3VSL indirect trust assessment operations that determine the selected partners' trust opinion by leveraging the other trust partner's recommendations. Hence, the trust opinion of the selected partner is expressed as trust, distrust, posterior and prior trust.
- ➢ Develop the modified TW algorithm (M-TW) and analyze its computational complexity.

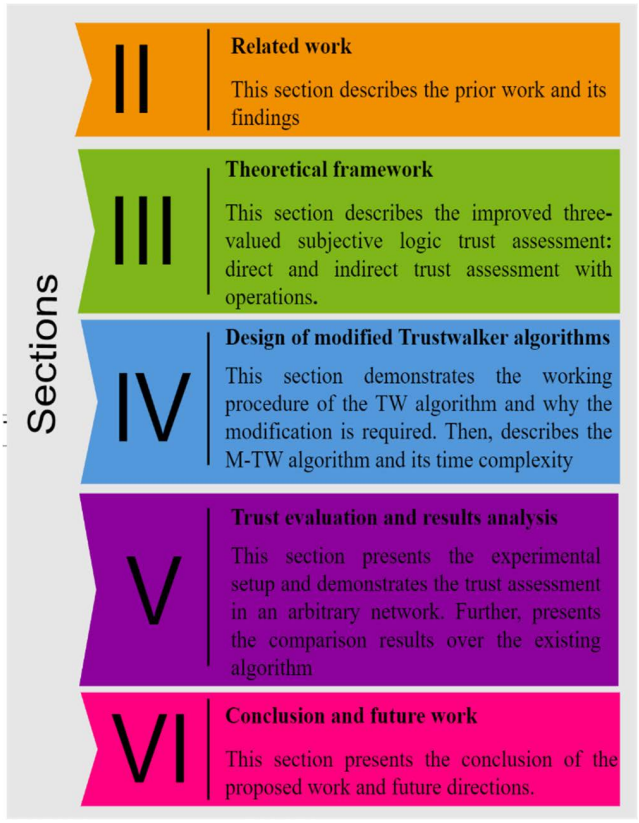


FIGURE 1. Working structure.

➢ The M-TW algorithm's performance is evaluated employing I-3VSL, and comparison results are demonstrated against AT and TW algorithms.

The article is structured as Section II describes the related work, and section III is the theoretical framework of the I-3VSL trust model. Section IV describes the M-TW Algorithm design based on the I-3VSL principles. Section V demonstrates the trust evaluation and analysis of comparison results, and Section VI includes a conclusion and future work. The working structure of the article is illustrated in Figure 1.

II. RELATED WORK

Trust assessment schemes are essential in computer science in a wide range of areas such as computer networks, distributed systems, game theory, and agent systems. Thus, it has acquired prominence in online-related decision-making at distinct the trustworthiness of web websites and services. Although, as technology advances, offline activities are migrated to the VE, including video conferences, virtual chats, and MMOG. These applications depend on interpersonal and trustor-trustee interactions virtually. Therefore, the trustees' trustworthiness in the virtual world is attracting the attention of the researchers [50]. The trust assessment schemes are classified as certainty and uncertainty models. The certainty trust assessment models express the degree of trust as a single quantity, such as trust or distrust. However, this is not possible to judge whether the player is trust or distrust in real-time applications such as autonomous vehicles and MMOG. Hence, the current study focuses on the uncertainty trust assessment schemes, and the comprehensive details are as follows.

The trust assessment scheme computes the trust based on its own experience and is referred to as direct trust. However, if the trustor never interacted with the trustee or service provider previously, then with recommendations or reputation, the trust is assessed, known as indirect. The direct trust opinion is private information, and the indirect trust opinion is public information which is second-hand information obtained from recommendations and reputation. Therefore, some of the reputation-based trust schemes such as summation and average [14], Bayesian systems [51], [52], [53], Discrete trust models [54], [55], Belief models [41], [42], [43], [45], [47], Fuzzy models [32], [33], [34], and flow-based [29], [30], [31].

- *The summation* form of assessment is the easiest way to compute the trust score by combining the ratings (positive and negative ratings). The advantage of the summation approach is that the logic behind the trust score computation is easy to understand. However, this scheme provides a low incentive rating and bias toward positive ratings. The *average assessment* scheme computes the average of all the reputations that produce the average trust score. However, the trust ratings can be repeated many times, which influences the false reputation values and has an inaccurate reputation score [56].
- *Bayesian systems* compute the reputation score based on the positive or negative input by leveraging the beta-probability density function (PDF). The PDF calculates the reputation score by combining the earlier score with a new rating and represents the score in the form of probability expected value. However, this approach cannot perform well in multiple conflicting beliefs and is not suitable for dynamic trust but provides better results theoretically [52], [57].
- *Discrete trust models* leverage the discrete verbal statements as very trust, trust, distrust, and very distrust. The trust score of personal experience with "x" is very trust, but the trust score derived from the referrals depends on the referring party, which may influence the trust score upwards or downwards. However, this scheme uses the heuristic formula for robust computation or look-up tables. The model is easy to understand and qualitative still, if theoretically considered, does not gives a concrete base [58].
- *Fuzzy models* express trust and reputation as fuzzy cognitive entities with similar measure function that describes how much the entity is honest or dishonest. This model uses the set of reasoning rules that determines the reputation. The reputation of an entity computed from private information is referred to as individual reputation, and reputation is derived from public information as social reputation [59], [60].

TABLE 1. Comparison of trust assessment schemes.

Model	Certainty	Uncertainty	Findings
Summation and average	√	×	The trust ratings can be repeated many times, impacting the false reputation values and producing an inaccurate reputation score.
Bayesian system	√	×	It cannot perform well in multiple conflicting beliefs and is unsuitable for dynamic trust.
Discrete trust model	√	×	The model is easy to understand and qualitative but, if theoretically considered, does not give a concrete base.
Fuzzy logic	√	×	This model suffers from computation and communication overhead.
Flow-based models	√	×	This approach only assigns the trust ratings to static network members. However, network members easily download unauthentic content from malicious peers.
Belief model	×	√	It supports the uncertainty trust assessment with various schemes but requires improvement.

- *Flow-based models* use the transitive rule that computes the trust by forming the chain from the trustor to the trustee. The trust or reputation score depends on the number of incoming and outgoing flows. The trust or reputation score increases if the number of incoming flows is high, and if the outgoing flow is low, the reputation score decreases and vice versa [29].
- *Belief models* use the probability theory, but the sum of overall probabilities is not necessarily 1, and the remaining probability is considered uncertainty.

According to these models, the summation and average model is ineffective in protecting against ballot stuffing or bad-mouthing attacks. Bayesian systems are widely used, but they are not considering uncertainty. Discrete trust and flow models do not provide the relevant mathematical background to compute trust. The fuzzy models are the combination of probability theory and predicate logic that allows for handling uncertainty but not uncertainty reasoning because they replace the truth values with approximate ones. Thus, fuzzy methods are not uncertain. The belief model inherently involves the node uncertainty behavior, which is considered an uncertainty trust model.

According to Table 1, the belief model supports the uncertainty trust assessment scheme using Dempster-Shafer theory (DST), subjective logic, and 3VSL. The DST is a mathematical and philosophical theory of evidence and an extension of Bayesian probability [61]. The DST works with a set of hypotheses named frame of discernment (FoD). The elements of FoD are a set of possible states that are mutually exclusive atomic events for the reasoning system. Therefore, a basic belief assignment (BBA) determines the belief in the range of [0, 1] to one of the subsets of frames. The DST approach uses a set of individual random variables: belief and plausibility. For instance, if 'X is a FoD and y is a BBA over X, then $\sum_{x\subset X} m(x) = 1$ then no mass is assigned to the empty set $m(\emptyset) = 0$. Then, the belief and plausibility are computed for a subset A of B as

$$b(A) = \sum_{B\subseteq A} m(B) \tag{1}$$

$$d(A) = \sum_{B\bigcap A} m(B) \tag{2}$$

$$u(A) = \sum_{\substack{B\bigcap A\neq\emptyset \\ B\nsubseteq A}} m(B) \tag{3}$$

Conversely, the BBA's have the two states then the observations are merged. For instance, m_1 *and* m_2 are two BBA's over the FoD of X is computed as joint mass m_{12}.

$$m_{12(A)} = (m_1 \otimes m_2) = \frac{1}{1-K} \sum_{B\cap C=A\neq\emptyset} m_1(B)\, m_2 \tag{4}$$

Here, K represents the number of conflicting beliefs among the m_1 *and* m_2 is represented in Eq. (5)

$$\sum_{B\cap C\neq\emptyset} m_1(B)\, m_2(C) \tag{5}$$

According to Zadeh [62], the Dempster rules produce counter-intuitive results when there is a high conflict between two mass beliefs. However, Josang A claimed that Dempster rules represent a method of preference combination while serving as an approximation for other belief combinations such as cumulative or average fusion of beliefs. Further, Pearl [63] claimed that it is misleading to interpret the belief functions as anything other than the probability proposition

that is provable from the set of other proposition probabilities. Therefore, Josang proposed various operators to combine the beliefs through the SL model [36].

The SL model is an extension of probability theory that resolves the DST challenges. Moreover, the SL model is used in various areas that are needed for uncertain reasoning, including trust network analysis [36], modeling trust on mobile ad-hoc networks, and arguing with evidence [64]. The SL model includes a wealth of operators for working with all classes of opinions (trust, distrust, uncertainty). The SL model uses the transitive rule that derives the functional trust by using the referral trust, performed through discounting operator. Further, if there exist multiple referral trusts to reach from $player_A$ to $player_B$ then the consensus operator is used to combine the opinions. The SL model operations are used to perform the uncertain reasoning, thereby allowing the intelligence analysis, Bayesian network analysis, and other actions that require reasoning when uncertainty is present. However, the SL model constantly preserves the uncertain trust during the trust assessment, implying that the uncertainty value never changes [35], [36], [37]. Therefore, the primary objective is to resolve the uncertainty trust more effectively and quantify trust between any pair of players based on their interactions by using 3VSL.

The 3VSL model is an enhanced version of the SL model, which further divides the uncertainty opinion into posterior and prior. The 3VSL model also uses the discounting and combining operations as the SL model. However, the SL model discounting operation does not support the cumulative and association rule, but combining operation supports both. In the 3VSL model, the association rule is supported but not cumulative, and both rules are supported in combining operations. Therefore, the SL and 3VSL models can be differentiated by association and cumulative law. However, the 3VSL discounting operation ignores the distrust and uncertainty opinions while deriving the trust opinion because, over time, the distrust and uncertainty changes do not influence the trust assessment. Similarly, the combining operation also required modification when the prior uncertainty opinions of two players are equal to zero. Therefore, the 3VSL model requires improvement in its operations, proposed in this work. Conversely, reputation is assessed by leveraging the various trust inference algorithms to establish trust between unknown users.

The DST approach challenge is cognitive rationally when the evidence fusion is highly conflicting belief [62]. Therefore, Smet [65], voorbraak [66], yager [67], Dubois [68], and Ma [69] methods are focused on handling the belief conflict evidence. Still, these methods fail to avoid the counter-intuitive caused by the original evidence error. Further, the data preprocessing approaches are employed before fusing the evidence according to DST. Murphy [70], Yong [71], Zhang [72], Yuan [73], Xiao [74], and Song [75] are performed the data preprocessing that eliminates the high conflict evidence fusion and avoids the problem of modifying the combination rule. However, DST-based approaches require optimization methods to provide effective solutions to real-time applications [76].

Further, Jøsang proposed SL based trust assessment model as Trust Network Analysis Subjective Logic (TNA-SL). This model computes the trust based on trust, distrust, neutral, and base rate opinions. The trust propagation and fusion mechanisms measure the final quantified trust value. However, this model forms the trusted network based on Direct Series Parallel Graph (DSPG) and expresses it in the canonical form, resulting in information loss [36], [37]. The TNA-SL model uses the matrix chain multiplication to compute the transitivity that consumes more time resulting in computational overhead. West et al. [77] proposed a modified TNA-SL model by representing the graph using a matrix with the trust opinions of ''n'' players. The trust is computed by applying a discount and combining operations of Kurdi [78] proposed an InterTrust model using the advantages of the TNA-SL and optimizes the matrix multiplications resulting in low computational overhead with more scalability. Golbeck et al. [79] proposed the tidal trust model that uses the transitivity rule to derive the trust opinion. The Tidal trust model uses a breadth-first search (BFS) fashion search that finds the shortest path from trustor to trustee. Hence, it reduces the number of hops interactions resulting the limited search space. However, the tidal trust fails to produce accurate results when more cycles and repeated edges are found in the search path. Massa et al [80] proposed a mole trust which considers all the routes based on the threshold and specific length. The mole trust model removes the loops in the network by transferring them into the directed acyclic graph (DAG). Then, it finds the path from a trustor to the trustee by verifying the trust value is more significant than the threshold value. Finally, it aggregates the selected trust values using the average weighted approach [81], [82], [83]. Cardoso et al. [41], [42] proposed a trust scheme for online games using BFS and a depth-first search (DFS) technique to discover the path. This model discovers the two paths from the trustor to trustee using BFS and DFS that provide balanced solutions for unknown party interactions. However, the BFS and DFS approaches have their own limitations when more cycles exist that produce inaccurate results and provide computational overhead. However, the SL model challenges are overcome with 3VSL, an extension of the SL model.

Liu et al. [45] proposed a multi-hop trust assessment scheme for arbitrary graphs using 3VSL with AT. The AT assesses the trustworthiness between any two players and produces accurate results. However, the AT trust assessment computational time increases exponentially while the hop-count increases, which creates the computational overhead.

Liu et al. [49] proposed OpinionWalk and Sohail et al [47] proposed Trustwalker algorithms to assess the trust based on depth-limited BFS fashion. Liu [45] and Sohail [47] algorithms produce accurate results and reduce computational complexity compared to AT algorithm. However, these approaches suffer computational overhead because, in the previous level, the longest path is reached. In the current

level, it also computes the trust value that is the same as the previous level.

Although the 3VSL model requires improvement in the discounting operation because this operation only depends on trust, remaining distrust and uncertain opinions are ignored in assessing the trust, producing inaccurate results. Srikanth et al. [48] proposed an I-3VSL trust assessment scheme based on the TW algorithm, which has accurate results but suffers computational overhead. Therefore, the proposed work intends to reduce computational complexity. Thus, the proposed work focused on developing the I-3VSL trust assessment scheme by modifying discount and combining. Further, designing the modified TW algorithm that reduces the computational overhead.

III. THEORETICAL FRAMEWORK

The term ''trust'' is described by various authors from different perspectives; according to the oxford dictionary, ''the person who has the belief or confidence in someone or something [84]''. In MMOG, the players interact based on content availability and AOI. Here, the content requestor has faith in the content provider and vice versa, which provides various benefits like risk mitigation, strong relationships among the players, and high productivity. Therefore, trust assessment is essential in MMOG. The existing trust assessment techniques are classified as absolute and uncertainty trust models. The absolute trust assessment model expresses trust in a single quantity, such as trust or distrust. The uncertainty trust models represent trust in multiple quantities, including trust, distrust, and uncertainty (neither trust nor distrust). Further, the uncertainty trust assessment is divided into two categories, such as direct and indirect assessment, the detailed description is provided in subsequent sections.

A. TRUST ASSESSMENT BASED ON PRIVATE OPINION OR DIRECT TRUST ASSESSMENT

In direct trust assessment, the $player_x$ is interacted with $player_y$ based on personal experience (direct interaction) is denoted as a trust rating. Then, the ratings are transformed into opinions by leveraging the direct trust assessment, as illustrated in Eq. (6).

$$\begin{cases} B_{xy} = \dfrac{p_{xy}}{p_{xy} + n_{xy} + u_{xy} + 3} \\ D_{xy} = \dfrac{n_{xy}}{p_{xy} + n_{xy} + u_{xy} + 3} \\ U_{xy} = \dfrac{u_{xy}}{p_{xy} + n_{xy} + u_{xy} + 3} \\ E_{xy} = \dfrac{3}{p_{xy} + n_{xy} + u_{xy} + 3} \end{cases} \tag{6}$$

Here, p_{xy}, n_{xy}, u_{xy} *and* 3 are positive, negative, posterior, and prior uncertainty. The prior uncertainty opinion is signified as 3 because of all three elements of opinion observation, such as positive, negative, and uncertain $(1 + 1 + 1 = 3)$. The interaction trust ratings are transformed into trust opinion that is represented in Eq. (7)

$$P_{xy} =< B_{xy}, D_{xy}, U_{xy}, E_{xy}, a_{xy} > \tag{7}$$

where $B_{xy}, D_{xy}, U_{xy}, E_{xy}, a_{xy}$ denotes the trust, distrust, posterior, prior trust opinions and base rate of $player_x$ on $player_y$.

TABLE 2. Nomenclature.

Symbol and Notation	Meaning
B_{xy}	Belief on y in x perspective
D_{xy}	Distrust on Y in x perspective
U_{xy}	Posterior uncertainty on y in x perspective
E_{xy}	Prior uncertainty on y in x perspective
p_{xy}	Positive opinion among x and y
n_{xy}	Negative opinion among x and y
u_{xy}	Uncertain opinion among x and y
P_{xy}	Trust opinion on y in x perspective
$EB(P_{xy})$	Expected belief of P_{xy}
a_{xz}	Base rate
γ	The ration of base rates
$M[i][j]$	Opinion matrix
W_{ij}	Trust opinion weight
$\mathbb{O}$	No interaction among the players, i.e., Uncertain
$\mathbb{I}$	Self-interaction, i.e., Fully trust
$V[j]$	Individual opinion vector
V_x^d	Individual opinion vector x perspective at d depth
B^1	Boolean vector at depth 1
Δ	Discounting operation
Θ	Combining operation
$V_x^{d+1}[s]$	Individual vector of s, in x perspective at d+1 depth

The a_{xy} denotes the base rate of $1/2 = 0.5$ because the trust opinion is normalized to [0, 1], and the complete trust and distrust are designated as 1 and 0. Hence, according to the probability theory, the base rate lies at the center. Thus the sum of the trust opinions is equal to "1", as shown in Eq. (8)

$$B_{xy} + D_{xy} + U_{xy} + E_{xy} = 1 \tag{8}$$

For instance, the $player_x$ is interacted with $player_y$ then provides the rating for the interaction. The feedback is collected in the range 1 to 10. The rating is between 9 to 10 is positive, 0 to 6 is negative, and $7 - 8$ is uncertain. Therefore, based on the ratings, the sum of positive, negative, and uncertain rates are considered for assessing the trust. Let us assume that the $player_x$ *and* $player_y$ are interacted 10 times previously out of 4 are positive, 3 are negative, and 3 are uncertain. However, the prior observations are included as 3 (positive, negative, and uncertain). As a result, the trust opinion between $player_x to player_y$ is derived by leveraging Eq. (1), and the results are shown in Eq. (4).

$$\begin{cases} B_{xy} = \dfrac{4}{4+3+3+3} \\ D_{xy} = \dfrac{3}{4+3+3+3} \\ U_{xy} = \dfrac{3}{4+3+3+3} \\ E_{xy} = \dfrac{3}{3+3+3+3} \end{cases} \tag{9}$$

According to Eq. (9), $player_x$ trust opinion on $player_y$ is $P_{xy} =< 0.308, 0.231, 0.231, 0.231, 0.5 >$ and the sum of the opinions is equal to 1 according to Eq. (8). Thus, the $player_x$ is having the previous interactions with the $player_y$ then the trust opinions are determined with Eq. (6). In case the $player_x$ is not having the previous interactions with $player_y$. Then, the trust opinion of $player_y$ is determined through the indirect trust assessment by considering the trust recommendations from a friend of a friend.

B. TRUST ASSESSMENT BASED ON PUBLIC OPINION OR INDIRECT TRUST ASSESSMENT

The indirect trust assessment determines the trust of the selected partner by leveraging the discounting and combining operations. The discounting operation propagates trust by transforming a friend's trust opinion to another. Let's assume the $player_x$ is having the trust opinion on $player_y$ and $player_y$ is having the trust opinion on $player_z$. Then, the $player_x$ is never interacted with the $player_z$. In this case, the $player_x$ establishes the trust relationship with the $player_z$ through the $player_y$'s a recommendation as illustrated in Figure 2(a). The combining operation performs the trust fusion by combining different players' opinions. the $player_x$ is having the interaction with $player_y$ and $player_q$, these player's having the interaction with $player_z$. Therefore, the $player_x$ is establishing a trust relationship with $player_z$ by leveraging the recommendations of $player_y$ and $player_q$ as illustrated in Figure 2 (b).

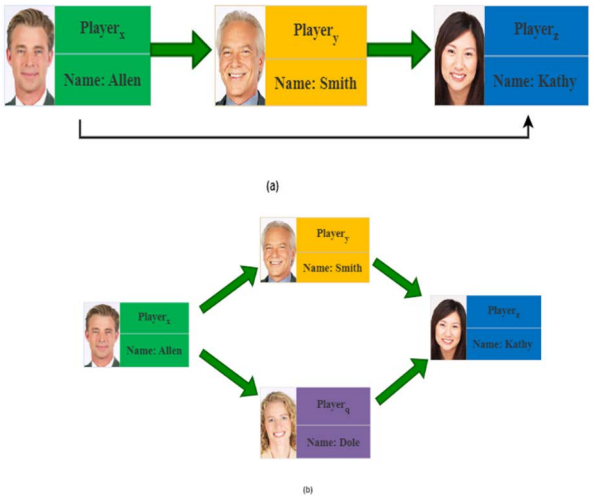


FIGURE 2. Players' interactions (a) single path (b) multiple paths.

According to Figure 2 (a), the trust relationship among the $player_x$ to $player_y$ and $player_y$ to $player_z$ are referral- trust. According to referral trust, the functional trust is determined from $player_x$ to $player_z$. Therefore functional trust is determined by leveraging the discounting operation. Similarly, Figure 2 (b) has multiple paths to assess the functional trust between $player_x$ to $player_z$. Initially, the discounting operation is applied between $player_x$ to $player_z$ via $player_y$ and $player_x$ to $player_z$ via $player_q$. Then, it performs the combining operations that determine the trust opinion between $player_x$ to $player_z$. The discount and combining operations are as follows.

1) DISCOUNTING OPERATION OR TRUST PROPAGATION

The discounting operation is used to transfer the trust opinion between the players that determine the trust opinion of the selected partner based on the trust recommendations of the friends. According to Figure 2 (a), let's assume the trust opinion between $player_x$ to $player_y$ as $P_{xy} =< B_{xy}, D_{xy}, U_{xy}, E_{xy} >$ and $player_y$ to $player_z$ as $P_{yz} =< B_{yz}, D_{yz}, U_{yz}, E_{yz} >$. Then, the trust opinion from $player_x$ to $player_z$ is determined using Eq. (10).

$$P_{xz} = \begin{cases} B_{xz} = EB\left(P_{xy}\right) B_{yz} \\ D_{xz} = EB\left(P_{xy}\right) D_{yz} \\ U_{xz} = 1 - \left(EB\left(P_{xy}\right)\left(B_{xz} + D_{xz} + E_{yz}\right)\right) \\ E_{xz} = E_{yz} \end{cases} \tag{10}$$

$$EB\left(P_{xy}\right) = B_{xy} + a_{xy} * U_{xy} + E_{xy} * 0.5 \tag{11}$$

In Eq. (10), $EB\left(P_{xy}\right)$ denotes the expected belief of the $player_x$ to $player_y$ which is computed by leveraging Eq. (11). In Eq. (11) the a_{xy} denotes the base rate of $1/2 = 0.5$ because complete trust and distrust are designated as 1 and 0. Hence, according to the probability theory, the base rate lies at the center.

2) COMBINING OPERATION OR TRUST FUSION

The combining operation is employed to aggregate the trust opinion of the multiple players that determines the functional trust. According to Figure 2 (b), the functional trust between the $player_x$ to $player_z$ is determined using Eq. (12) and (13). Let's assume the trust opinion between the $player_x$ to $player_z$ via $player_y$ is $P_{xz_1} =< B_{xz_1}, D_{xz_1}, U_{xz_1}, E_{xz_1}, a_{xz_1} >$. Similarly, the trust opinion between $player_x$ to $player_z$ via $player_q$ is $P_{xz_2} =< B_{xz_2}, D_{xz_2}, U_{xz_2}, E_{xz_2}, a_{xz_2} >$.

Case I: $E_{xz_1} + E_{xz_2} - E_{xz_1}E_{xz_2} \neq 0$

$$P_{xz} = \begin{cases} B_{xz} = \dfrac{E_{xz_2}B_{xz_1} + E_{xz_1}B_{xz_2}}{E_{xz_1} + E_{xz_2} - E_{xz_1}E_{xz_2}} \\ D_{xz} = \dfrac{E_{xz_2}D_{xz_1} + E_{xz_1}D_{xz_2}}{E_{xz_1} + E_{xz_2} - E_{xz_1}E_{xz_2}} \\ U_{xz} = \dfrac{E_{xz_2}U_{xz_1} + E_{xz_1}U_{xz_2}}{E_{xz_1} + E_{xz_2} - E_{xz_1}E_{xz_2}} \\ E_{xz} = \dfrac{E_{xz_1}E_{xz_2}}{E_{xz_1} + E_{xz_2} - E_{xz_1}E_{xz_2}} \end{cases} \tag{12}$$

Case II: $E_{xz_1} + E_{xz_2} - E_{xz_1}E_{xz_2} = 0$, *then compute* $\gamma = \frac{a_{xz2}}{a_{xz1}}$

$$P_{xz} = \begin{cases} B_{xz} = \dfrac{\gamma B_{xz_1} + B_{xz_2}}{\gamma + 1} \\ D_{xz} = \dfrac{\gamma D_{xz_1} + D_{xz_2}}{\gamma + 1} \\ U_{xz} = \dfrac{\gamma U_{xz_1} + U_{xz_2}}{\gamma + 1} \\ E_{xz} = 0 \end{cases} \tag{13}$$

For instance, $player_x$ opinion about $player_{z1}$ is $W_{xz1} =< 0.99, 0.01, 0, 0 >$ and $player_x$ to $player_{z2}$ is $W_{xz2} =< 0, 1, 0, 0 >$. Then the trustworthiness opinion from $player_x$ *to* $player_z$ is determined through Eq. (13) because the prior trust opinion of both the players (E_{xz1} *and* E_{xz2}) is 0. Accordingly, $\gamma = \frac{0.5}{0.5} = 1$, the $player_x$ trust opinion about $player_z$ is expressed through Eq. (14)

$$P_{xz} = \begin{cases} B_{xz} = \dfrac{1 * 0.99 + 0}{1 + 1} = 0.495 \\ D_{xz} = \dfrac{1 * 0.01 + 1}{1 + 1} = 0.505 \\ U_{xz} = \dfrac{1 * 0 + 0}{1 + 1} = 0 \\ E_{xz} = 0 \end{cases} \tag{14}$$

IV. DESIGN OF M- TW ALGORITHM

The trusted network is established based on the players' interaction using the Travian dataset. The constructed network is digraph G (V, E, W); in this, the vertices 'V' represent the players, their interaction represented with E and the trust opinion of the interaction represents the "W." The players establish trust relationships based on the distance and players' trust opinions. The number of hop counts controls the distance between the players, and trust opinions are generated through the I-3VSL trust model. Therefore, the trustwalker algorithm is designed to optimize the execution time without compromising performance. The graph G represents the adjacent list, which consists of the players' direct trust opinions. For instance, the $Player_x$ is having a direct interaction with $player_y$ then it is denoted with W_{xy} otherwise, it is prior uncertainty such as <0,0,0,1>, and the player has self the trust opinion as <1,0,0,0>. The prior uncertain and self-trust opinions are represented with O, I. Accordingly, the adjacent list is prepared for "n" players, which is illustrated in Eq. (15).

Algorithm 1 An Opinion Matrix Generation

Input: Digraph G and set of players P
Output: Adjacent Matrix M
Goal: To compute opinion matrix M
Adjacent_Matrix (G, P)

1. *for* $i \leftarrow 1$ *to n do*
2. *for* $j \leftarrow 1$*to n do*
3. *if* $i == j$ *then*
4. $M[i][j] = \mathbb{I}$
5. *else*
6. *if edge* $(i, j) \in E$
7. $M[i][j] = W_{ij}$
8. *else*
9. $M[i][j] = \mathbb{O}$
10. *end if*
11. *end if*
12. *end for loop*
13. *end for loop*

$$\begin{bmatrix} \mathbb{I} & W_{12} & W_{13} & \dots & W_{1n} \\ W_{21} & \mathbb{I} & W_{23} & \dots & W_{2n} \\ W_{31} & W_{32} & \mathbb{I} & \dots & W_{3n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ W_{n1} & W_{n2} & W_{n3} & \dots & \mathbb{I} \end{bmatrix} \tag{15}$$

Therefore, based on the player interactions, the initial adjacent matrix is illustrated in algorithm-1 through the G and players.

Algorithm1 is designed to generate the initial trust opinion between the players. The total number of players in the network depends on the input G and player set P. Thus, each player in the G interacted with "n" other players that produced the "$n \times n$" matrix. Line 1-2 presents each player in the G is interacting with all other players in the G and then verifying whether the player is having the interaction with itself. Thus, the opinion is completely trusted, as $\mathbb{I}$ shown in Lines 3-4. Line 6-9 verifies whether the player has interaction with other players, then the trust opinion is denoted with W_{ij} otherwise, the opinion is prior uncertain as $\mathbb{O}$.

According to Algorithm 1, the direct trust assessment measures the trust opinions among the players demonstrated in Algorithm 2.

Algorithm 2 Generating Direct Trust opinions

Input: Directed Trust G, Set of nodes P
Output: direct Trust opinion between the user "i" to "j."
Goal: Generating trust opinions from player "i" to "j" using direct trust relationships from G
Direct_ Trust (G, P)

1. initialize the opinion matrix M and individual opinion vector V with uncertain opinions O
2. *for* $i \leftarrow 1$ *to* n *do*
3. *for* $j \leftarrow 1$ *to* n *do*
4. *if* $edge(i, j) \in E$ *do*
5. $p_j \leftarrow 0$
6. $n_j \leftarrow 0$
7. $u_j \leftarrow 0$
8. end if
9. *for* $k \leftarrow 1$ *to* n *do*
10. *if* $edge(j, k) \in E$ *do*
11. *if* $k \in P$ *and* k *is trust*, *then*
12. $p_j \leftarrow p_j + 1$
13. *else*
14. *if* $k \in P$ *and* k *is distrust*, *then*
15. $n_j \leftarrow n_j + 1$
16. *else*
17. $u_j \leftarrow u_j + 1$
18. *end if*
19. *end if*
20. *end if*
21. *end for loop*
22. $B_{ij} \leftarrow \frac{p_j}{p_j+s_j+u_j+3}$
23. $D_{ij} \leftarrow \frac{n_j}{p_j+n_j+u_j+3}$
24. $U_{ij} \leftarrow \frac{u_j}{p_j+n_j+u_j+3}$
25. $E_{ij} \leftarrow \frac{3}{p_j+n_j+u_j+3}$
26. $M[i][j] \leftarrow (B_{ij}, D_{ij}, U_{ij}, E_{ij})$
27. $V[j] \leftarrow (B_{ij}, D_{ij}, U_{ij}, E_{ij})$
28. *end for loop*
29. *end for loop*
30. *return M*

Algorithm 2 is planned based on Algorithm 1; Line 1 initializes the adjacent matrix M and individual players' opinion vector"V." initially, the vector "V" consists of the uncertain opinion "$\mathbb{O}$." Line 2-8 specifies the interaction among the player "i" *to* "j" exists an edge, then their opinions are classified into positive, negative, and uncertain initialized to zero ($p_j = n_j = u_j = 0$). Further, Line 2- 21 presents how many interactions are established by the player "j" *to* "k" represents the outer loop, and inner loops indicate their interactions. After that, each interaction feedback is added to its classification as positive, negative, and uncertain. Further, assess the trust opinion between the players using Eq. (6) illustrated in lines 22-25. Lines 26-27 update the new trust opinions in the "M" *and* "V."

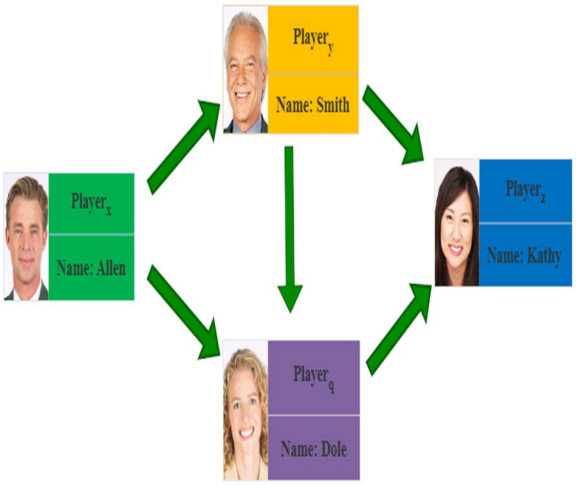


FIGURE 3. An arbitrary network.

A. CASE STUDY

For instance, serval players establish the trusted interaction based on their interests, illustrated as a trusted arbitrary network in Figure 3. Then, it applies algorithm1 and algorithm2 through assessing the direct trust assessment that is demonstrated below.

According to Figure 3, the adjacent matrix "M" is constructed using algorithm1, and the illustrated matrix is represented in Eq. (16).

$$M = \begin{bmatrix} \mathbb{I} & W_{xy} & W_{xq} & \mathbb{O} \\ \mathbb{O} & \mathbb{I} & W_{yq} & W_{yz} \\ \mathbb{O} & \mathbb{O} & \mathbb{I} & W_{qz} \\ \mathbb{O} & \mathbb{O} & \mathbb{O} & \mathbb{I} \end{bmatrix} \tag{16}$$

Further, algorithm-2 is employed that classifies the interactions as positive, negative, and uncertain based on the total interactions among the player one to all other players in the trusted network as shown in Eq. (16). After that, the interactions ratings are converted into trust opinion as "M" in Eq. (17) and 18. The individual trust opinion vector is fabricated as "V" based on $player_x$ concerning in Eq. (19).

$$M = \begin{bmatrix} \mathbb{I} & \begin{bmatrix} 12 \\ 1 \\ 2 \end{bmatrix} & \begin{bmatrix} 7 \\ 3 \\ 3 \end{bmatrix} & \mathbb{O} \\ \mathbb{O} & \mathbb{I} & \begin{bmatrix} 1 \\ 4 \\ 2 \end{bmatrix} & \begin{bmatrix} 13 \\ 5 \\ 1 \end{bmatrix} \\ \mathbb{O} & \mathbb{O} & \mathbb{I} & \begin{bmatrix} 1 \\ 2 \\ 8 \end{bmatrix} \\ \mathbb{O} & \mathbb{O} & \mathbb{O} & \mathbb{I} \end{bmatrix} \tag{17}$$

$$M = \begin{bmatrix} \begin{bmatrix}1\\0\\0\\0\end{bmatrix} & \begin{bmatrix}0.667\\0.056\\0.111\\0.167\end{bmatrix} & \begin{bmatrix}0.438\\0.188\\0.188\\0.188\end{bmatrix} & \begin{bmatrix}0\\0\\0\\1\end{bmatrix} \\ \begin{bmatrix}0\\0\\0\\1\end{bmatrix} & \begin{bmatrix}1\\0\\0\\0\end{bmatrix} & \begin{bmatrix}0.1\\0.4\\0.2\\0.3\end{bmatrix} & \begin{bmatrix}0.591\\0.227\\0.045\\0.137\end{bmatrix} \\ \begin{bmatrix}0\\0\\0\\1\end{bmatrix} & \begin{bmatrix}0\\0\\0\\1\end{bmatrix} & \begin{bmatrix}1\\0\\0\\0\end{bmatrix} & \begin{bmatrix}0.071\\0.143\\0.571\\0.215\end{bmatrix} \\ \begin{bmatrix}0\\0\\0\\1\end{bmatrix} & \begin{bmatrix}0\\0\\0\\1\end{bmatrix} & \begin{bmatrix}0\\0\\0\\1\end{bmatrix} & \begin{bmatrix}1\\0\\0\\0\end{bmatrix} \end{bmatrix} \tag{18}$$

$$V_x = \left[\mathbb{I}, W_{xy}, W_{xq}, \mathbb{O}\right] = \begin{bmatrix} \begin{bmatrix}1\\0\\0\\0\end{bmatrix} & \begin{bmatrix}0.667\\0.056\\0.111\\0.167\end{bmatrix} & \begin{bmatrix}0.438\\0.188\\0.188\\0.188\end{bmatrix} & \begin{bmatrix}0\\0\\0\\1\end{bmatrix} \end{bmatrix} \tag{19}$$

Although, Algorithm 2 assess the trust of known players since the unknown players' trust assessment is derived from the recommendations using an indirect trust assessment scheme. The indirect trust is evaluated in depth limited breadth-first search (DL-BFS) fashion, for the Trustwalker (TW) Algorithm is designed [48].

B. TRUSTWALKER (TW) APPROACH

The TW algorithm works based on the depth limitations that derive the unknown players' trust in the recommendations and reputations of their friends. The scheme starts from the trustor and searches the trustee player in the network according to the specific depth. Therefore, the trust computation is performed according to the discount and combined operations that are illustrated in Eq. (10), (11), and (12). However, the TW algorithm updates the trust of each player in every iteration by re-computing the trust opinion. For instance, the $player_x$'s trust opinion of all other players is preserved in the individual vector opinion V_x based on the depth as illustrated in Eq. (20).

$$V_x^d = \left[W_{x,1}^d, W_{x,2}^d, W_{x,3}^d, W_{x,4}^d \ldots W_{x,n}^d\right] \tag{20}$$

Here "d" represents the depth, x denotes the player and $W_{x,1}^d$ specifies the trust opinion of the $player_x$ about the $player_1$. Thus, the $player_x$ searches the trustworthy partner among all the players in the network at different depths through the TW algorithm. According to the TW algorithm, the trustor starts the trust computation from its neighbor players by leveraging the direct trust that specifies its trustworthy opinion about the neighbors. However, the neighbor players do not have the same opinion on the trustor because trust is the individual opinion about others; in other words, trust is asymmetric. Thus, the trust is determined using the following Eq. (21).

$$V_x^d = M^T \odot V_x^{d-1} \tag{21}$$

Here, M is the adjacent opinion matrix $\odot$ is an intuitional operator which performs the matrix multiplication. The standard matrix multiplication performs the summation and multiplication but performs the discount and combine operations here. The V_x^{d-1} is individual vector opinion concerning $player_x$ at depth $d-1$. The individual vector opinion is represented according to Fig. 3 in Eq. (19) at depth 1, and M is illustrated in Eq. (17). As TW updates the players' trust hop by hop, it reaches the trustee within the specified depth as the longest path. Thus, the TW algorithm is applied in Fig.3, and the trust evaluation steps are demonstrated.

For an instant, the trustor is $player_x$ and depth is $d = 1$, then the searching trustee. Thus the longest path from trustor to trustee is $player_x \rightarrow player_y$. Therefore, the trust opinion of $player_x$ about $player_y$ never changes further in the evaluation because it is the longest path. Similarly, the other longest path for $d = 1$ is $r_x \rightarrow player_q$. When d=2, the search path from $player_x$ finds the path as $r_x \rightarrow player_y \rightarrow player_z$, $layer_x \rightarrow player_q \rightarrow player_z$, $layer_x \rightarrow player_y \rightarrow player_q$. After that, d=3, then $r_x \rightarrow player_y \rightarrow player_q \rightarrow player_z$. The TW algorithm creates trust computation for various computational overheads at different depths. Hence, the modified TW (M-TW) algorithm is critical for quick trust evaluation to avoid computational overhead.

C. MODIFIED TRUSTWALKER (M-TW) APPROACH

The M-TW algorithm mitigates the number of updates in each iteration. As a result, it provides a quick trust assessment. Initially, the M-TW starts the computation from the trustor, and its neighbor interactions are represented in the individual opinion vector as described in Eq. (22).

$$V_x^1 = \left[W_{xx}, W_{xy}, W_{xq}, W_{xz}\right] = [I, W_{xy}, W_{xq}, O] \tag{22}$$

Then, it computes the next iteration individual opinion vector as V_x^2 from the previous iteration V_x^1. The computation of the next iteration is performed by the algorithm through the discounting (Δ) and combining ($\boldsymbol{\Theta}$) operations. According to Fig.3, the individual trust opinion vector is represented in Eq. (19). The next level computation is derived from Eq. (21) at d=2. The Eq. (22) consists of the $player_x$ opinion about the $player_y$ which is represented in the V_x^1, now $player_y$ to $player_z$ is derived that consists in V_x^2. However, the V_x^1 consist of the trust opinion of W_{xz} that is $\mathbb{O}$. The remaining opinions are not changing, and the opinion from $player_y$ to $player_z$ is changing that, is evaluated in Eq. (23).

$$W_{xz}^2 = \Delta\left(W_{xy}^1, W_{yz}\right) \tag{23}$$

Here, the W_{xy}^1 value is obtained from the previous level V_x^1 and W_{yz} is accessed from the trust opinion matrix "M." Similarly, the trust opinion of W_{xq} is determined as follows and W_{qz} is

exist, the resultant is shown in Eq. (24).

$$W_{xq}^2 = \Delta\left(W_{xx}^1, W_{xq}\right) = \Delta\left(I, W_{xq}\right) = W_{xq} \quad (24)$$

$$W_{xq}^2 = \Delta\left(W_{xy}^1, W_{yq}\right) \quad (25)$$

According to Eq. (24) and (25), the results are combined through the combining operation as Eq. (26).

$$W_{xq}^2 = \Theta\left(W_{xq}, \Delta\left(W_{xy}^1, W_{yq}\right)\right) \quad (26)$$

Therefore, the V_x^2 acquires the trust opinion from the previous iteration and updates the trust opinions of W_{xq} and W_{xz} remaining interactions will be the same. For that, a boolean vector is leveraged that preserves the updated information, as in Eq. (27).

$$B^1 = [0, 0, 1, 1] \quad (27)$$

Further, the trust assessed $player_x$ to $player_z$ at d=2, then the trust is assessed using Eq. (23), and Eq.(28) then performs the combine operation; that is trust opinions are updated in the boolean vector, which is shown in Eq.(27)

$$W_{xz}^2 = \Delta\left(W_{xq}, W_{qz}\right) (28) \quad (28)$$

$$W_{xz}^2 = \Theta\left(\Delta\left(W_{xy}, W_{yz}\right), \Delta\left(W_{xq}, W_{qz}\right)\right) \quad (29)$$

Similarly, at d=3, the boolean vector is illustrated in Eq. (30), and their respective computation is shown in Eq. (31).

$$B^2 = [0, 0, 0, 1] \quad (30)$$

$$W_{xz}^3 = \Theta\left(\Delta\left(W_{xy}, W_{yz}\right), \Delta\left(\Theta\left(W_{xq}, \Delta\left(W_{xy}, W_{yq}\right), W_{qz}\right)\right)\right) \quad (31)$$

According to Eq. (23) to Eq. (31), the individual trust opinion matrix for d=3 is defined in Eq. (32) and illustrated in the boolean vector in Eq. (33).

$$V_x^3 = \left[\mathbb{I}, W_{xy}, W_{xq}^2, W_{xz}^3\right] \quad (32)$$

$$B^3 = [0, 0, 0, 0] \quad (33)$$

Consequently, the longest path from the trustor to a trustee is acquired and stops the update process shown in Eq. (33). Accordingly, the algorithm is designed M-TW as Algorithm 3

Algorithm 3 is designed to perform the quick trust assessment by minimizing the number of updates. Line 1-2 is used to initialize the opinion matrix M based on the G and initial depth at 1. Line 3-6 extracts the individual opinion vector from the opinion matrix M by concerning trustor x to all other players in the network at initial depth. Line 7-13 represents the interaction with all other players in the network, whose interactions are not the uncertain opinions in the opinion matrix and individual opinion vector. For them, the boolean vector value is assigned as "1", which means the trust opinion is derived in the future. Line 14 specifies the maximum depth limit to find the trustee partner. Line 15- 33 specifies the trust computation process of the next level based on the previous level and opinion matrix. The future computation updates are indicated in the boolean vector. Line 15 specifies the assignment of prior level trustworthiness concerning x about all the other players in the network. Line 16 verifies the $player_x$ like the other player, the boolean vector value is assigned as 1, then the next level opinion vector value is

Algorithm 3 Modified Trustwalker (M-TW) for Route Discovery

Input: A directed graph G, trustor x, player set P, and depth d

Output: performing the trust assessment quickly by reducing the number of updation

Goal: perform the trust assessment using depth-limited breadth-first search through M-TW

M-TW (G, P, x, d)

1. *Opinion matrix* $M = Direct\_Trust(G, P)$
2. *Initial depth* $d \leftarrow 1$
3. *for all the players trust opinion with* x *prespective where* $x \neq i$ *do*
4. $V_x^d[i] \leftarrow M[x][i]$
5. $B[i] \leftarrow 0$
6. *end for*
7. *for all players* $'s'$ *interaction with* x *in the network do*
8. *if* $V_x^d[s] \neq Othen$
9. *for all players* i *where* $M[s][i] \neq \mathbb{O}$ *do*
10. $B[i] \leftarrow 1$
11. *end for*
12. *end if*
13. *end for*
14. *while* $d < D$
15. $V_x^{d+1} \leftarrow V_x^d$
16. *for all players* $i \neq x$ *such that* $B[i] = 1$ *do*
17. $V_x^{d+1}[i] \leftarrow O$
18. *for all players* s *such that* $V_x^d[s] \neq \mathbb{O}$ *and* $M[s][i] \neq \mathbb{O}$ *do*
19. *if* $V_x^{d+1}[s] = \mathbb{O}$ *then*
20. $V_x^{d+1}[i] \leftarrow \Delta(V_x^d[s], M[s][i])$
21. *else*
22. $V_x^{d+1}[i] \leftarrow \Theta\left(V_x^{d+1}[i], \Delta\left(V_x^d[s], M[s][i]\right)\right)$
23. *end if*
24. *end for*
25. *end for*
26. *for all players* i *do*
27. $B[i] \leftarrow 0$
28. *end for*
29. *for all* $s \neq xsuchthatV_x^{d+1}[s] \neq V_x^d[s]$ *do*
30. *for all players* i *such that* $M[s][i] \neq \mathbb{O}$ *do*
31. $B[i] \leftarrow 1$
32. *end for*
33. *end for*
34. $d \leftarrow d + 1$
35. *end while*
36. *return* V_x^d

uncertain, as shown in line 17. Line 18-25 specifies the trust computation process; in the current depth, the $player_x$ to its neighbor players. Trust is not uncertain and from neighbor players to its neighbor players are not uncertain in the opinion matrix. Then it constructs the new opinion based on next-level depth; if there is no direct path, it derives a new trust opinion using discounting operation. However, if multiple routes exist, the combining operation (direct and indirect path trust opinions applies) applies. Line 26-33 updates the boolean vector $B[i]$ based on the current and previous level trust opinion vector. Line 29 verifies whether the trust opinion vector current and prior values differ, demonstrates that the opinion matrix value is not uncertain, and then updates the boolean vector. Like that, the process continues until it reaches the max depth and returns the individual opinion vector.

Further, the players are categorized into two groups, intra and inter, based on the players' identity. The players' identity is three types based on the M-TW trust computation algorithm. Accordingly, Algorithm 4 is demonstrated below.

Algorithm 4 describes the classification of players into the intra and inter-group. Thus, for the players belonging to the intra-group, the trust opinion never changes in the future because the searching depth is reached the longest path. Suppose the player belongs to the inter-group; then the player's trust will update in the future. Accordingly, algorithm 4 is designed. Line 1-5 describes the players' trust opinion vector values of $V_x^{d+1}[s]$ *and* $V_x^d[s]$ are identical, and the opinion is uncertain, then the player belongs to G_1. Line 6-10, the trust opinion vector values of $V_x^{d+1}[s]$ *and* $V_x^d[s]$ are identical, and the opinion is not uncertain, then the player belongs to G_3. Line 11-15, the opinion vector values of $V_x^{d+1}[s]$ *and* $V_x^d[s]$ are different, and the opinion is not uncertain; the player belongs to G_2. Therefore, G_1 players' opinion is uncertain, and their trust value is not changing. The boolean vector consists $B[i] \leftarrow 0$. G_2 players' opinion vector values of current and previous levels are different and not uncertain. The trust opinion vector is just updated, and the trust opinion value will change in the future. The G_3 players' trust opinion value is not yet updated, but the opinion value will be modified on different levels. According to the players' groups G_1, G_2 and G_3 The players are classified as intra and inter-groups. Line 16- 22, the player belongs to G_1 *and* G_2 which specifies the player is known because their trust opinion value is updated in the current or previous level, and the player is not interacting with any other players in the network. Thus, the player belongs to the intra-group, and the boolean vector value of these players is $B[i] \leftarrow 0$. Line 23-29, the G_2 *and* G_3 indicate they are unknown or known players. The trust value of these players is updated in the future because they interact with other players in the network. The players belong to the inter-group, and the boolean vector represents the $B[i] \leftarrow 1$. Therefore, the players belong to the intra-category, reach the longest path, and the trust value is not changing. In other words, intra-group players do not interact with inter-group members.

Algorithm 4 Classification of Players' Interactions

Input: opinion matrix M and Individual trust opinion vectors V_x^{d+1}*and* V_x^d.
Output: player's classification based on the groups
Goal: classifying the players as inter and intra groups
Inter_intra $\left(M, V_x^{d+1}, V_x^d\right)$

1. *for all* $x \neq s$ *such that* $V_x^{d+1}[s] = V_x^d[s]$ *do*
2. *for all the players i such that* $M[s][i] = \mathbb{O}$ *do*
3. $G_1 \leftarrow s$
4. *end for*
5. *end for*
6. *for all* $x \neq s$ *such that* $V_x^{d+1}[s] = V_x^d[s]$ *do*
7. *for all the players i such that* $M[s][i] \neq \mathbb{O}$ *do*
8. $G_3 \leftarrow s$
9. *end for*
10. *end for*
11. *for all* $x \neq s$ *such that* $V_x^{d+1}[s] \neq V_x^d[s]$ *do*
12. *for all the players i such that* $M[s][i] \neq \mathbb{O}$ *do*
13. $G_2 \leftarrow s$
14. *end for*
15. *end for*
16. *for all* $x \neq s$
17. *if* $s \in G_1 || s \in G_2$ *then*
18. *for all the players i such that* $M[s][i] = \mathbb{O}$ *do*
19. $Intra_{group} \leftarrow s$
20. $B[i] \leftarrow 0$
21. *end for*
22. *end if*
23. *if* $s \in G_2 || s \in G_3$ *then*
24. *for all the players i such that* $M[s][i] \neq \mathbb{O}$ *do*
25. $Inter_{group} \leftarrow s$
26. $B[i] \leftarrow 1$
27. *end for*
28. *end if*
29. *end for*
30. *return* $inter_{group}$ *and* $intra_{group}$

D. THE TIME COMPLEXITY ANALYSIS

The M-TW algorithm searches the trustee partner based on the DL-BFS manner. In the network maximum number of participants, players are 'n' among the one is trustor. Hence, the trustor has the maximum $n-1$ neighbor players and out-degree $n-1$ at depth d. Consequently, the mathematical formula is demonstrated in Eq. (34).

$$T(n) = d \times n((n-1) \times c_1 + c_2) \tag{34}$$

According to Eq. (34), the time complexity is $O\left(n^2\right)$ In Eq. (34), d is the constant depth, n is the number of players in the network, and $(n-1)$ is the maximum out-degree of the trustor. However, if the trustor out-degree is 1, then the complexity is $O(n)$; otherwise, the complexity is $O\left(n^2\right)$, which is illustrated in aglorithm3 Line 14-25.

Similarly, the complexity of algorithm4 is $O\left(n^2\right)$ because the maximum number of players is n in the network, one is

TABLE 3. Simulation setup.

Parameter	Specification
Players in VE	$10, 20, 50$ *and* 100
Area	$100 \times 100m^2$
Players movement	Random waypoint model
Community layout	Spring layout
Interaction range	$5m$

the trustor, and another is the trustee. Hence the mathematical formula is illustrated in Eq. (35)

$$T(n) = d \times ((n-1) \times (n-2)) \tag{35}$$

Here, d is the depth to search the longest path, the intermediate players among the trustor and trustee are $n-2$, and the out-degree of the trustor is a maximum $n-1$. Hence the complexity is $O\left(n^2\right)$

V. EVALUATION AND RESULT ANALYSIS

The performance of the proposed M-TW algorithm with I-3VSL is examined by conducting a simulation using python's Networkx package [85]. Thus, the Travian real-time dataset is leveraged to experiment, and the simulation setup is illustrated in Table 3. The Travian data set consists of the trustor and trustee and their trust ratings [6], [86]. The experimental platform is a laptop with windows 10, core i5-7200U CPU @ 2.50GHz 2.71 GHz, 8GB RAM, and 1TB HD.

The trust network formed from the Travian dataset consists of the attributes as the source, target, and time stamps. From the trusted network, self-loops and isolated nodes are removed then the alias names are assigned to each player as ids. Further, the players are moving freely in the trusted network, and the updated player's position information is distributed to all other players in the network. As a result, the use of network bandwidth is increasing. Hence, the trusted network is divided into small regions based on the players' interaction through community detection algorithms to minimize network bandwidth usage. However, many community detection algorithms require prior information, such as size and number of communities, but the information is not available to the players. Hence, the asynchronous label propagation algorithm (LPA) permits the formation of communities without prior knowledge and takes a linear amount of time [87]. The trusted arbitrary community network is designed based on the players' interactions within the community; the trust relationships are 30% and the outside community 2%. Further, each community consists of the players as 40%, 30%, and 30% of the total players in the network. The illustrated arbitrary trust network with the trust relationships is shown in Figure 3.

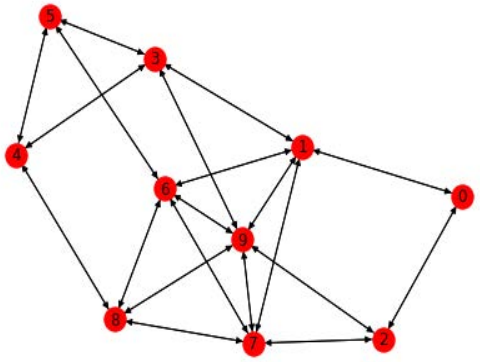


FIGURE 4. Sample arbitrary network with 10 players.

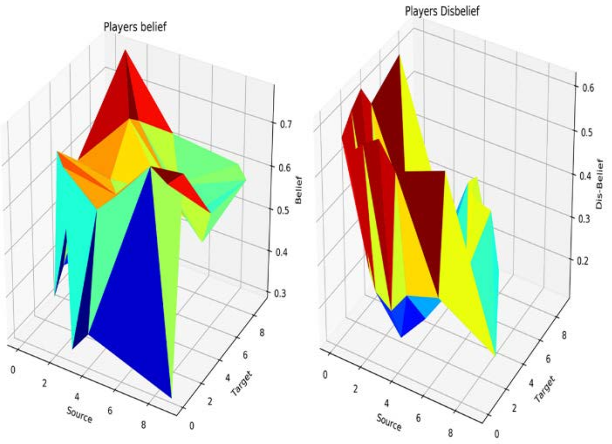


FIGURE 5. Player's trust opinion representation as belief and disbelief.

According to Figure 4, the trust relationships of the players' interaction and their trust ratings are converted into the uncertainty trust opinion using Gaussian probability. The Gaussian probability works based on the mean and standard deviation as 0.9 *and* 0.1. The trust opinion is standardized between [0, 1], and if the players' trust relationship value exceeds 1, then the mean and standard deviation are reassigned as 0.3 and 0.0001. However, 10% of malicious players are inserted into the network according to the size of the players. Therefore the generated belief and disbelief of the players are illustrated in Figure 5.

According to Figure 5, the direct trust opinion among the players is illustrated using algorithm 2. Here the X, Y, and Z-axis represent the source, target, and belief in Figure 5(a) and Figure 5(b), expressing the source, target, and disbelief among the players' interaction. The performance of the trust-assessed scheme is examined under network size 10 with searching depth limited to 4 through I-3VSL with the M-TW algorithm for various graph models over the numerous rounds, and the obtained results are shown in Figure 6.

The performance of I-3VSL with M-TW is illustrated in Figure 6. The minimum trust probability of 70.53, the

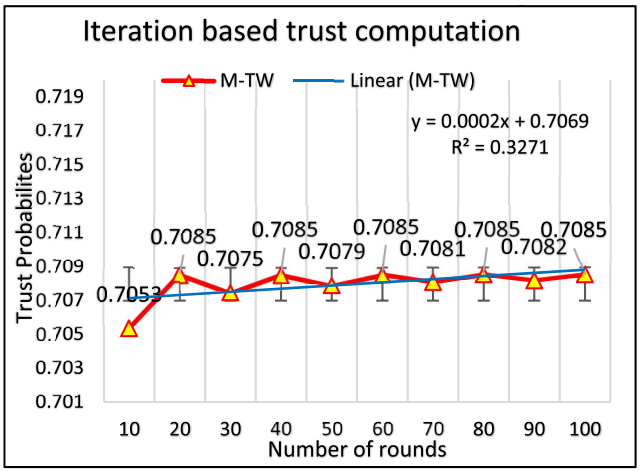


FIGURE 6. Trust computation with I-3VSL_M-TW.

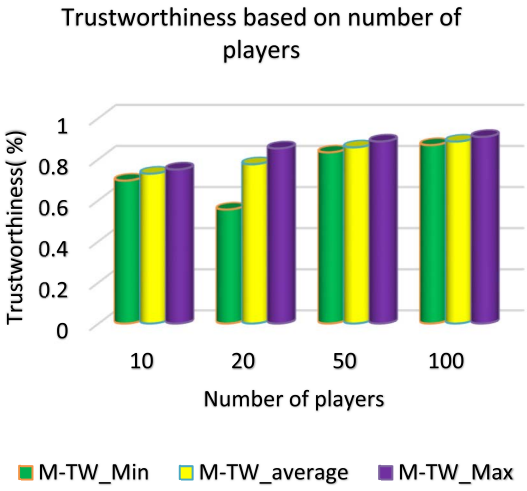


FIGURE 7. Trustworthiness of players.

maximum probability of 70.85, and an average probability of 70.85 for 10 to 100 iterations. However, the trust computation probabilities are linearly increased with $y = 0.0002x + 0.7069$ and R-square (R^2) value as 0.3271. Moreover, the trust probability opinion is fractionally changed after the 60 iterations. Subsequently, the network size increases gradually to 10, 20, 50,100, and the performance of the M-TW algorithm is analyzed in Figure 7.

The trustworthiness of players is assessed based on numerous sizes shown in Figure 7. The trustworthiness of the players is shown as min, max, and average according to the dimensions. The network sizes with 10, 20, 50 *and* 100 and randomly generate various graph representations, then the minimum, average and maximum trust opinions are computed. From Figure 7, it is examined that when the network size is 10, the min, average, and max trust value is 0.7, 0.73 *and*, 0.75. The network size is 100, then the min, average, and max trust values are 0.87, 0.89, *and*, 0.91.

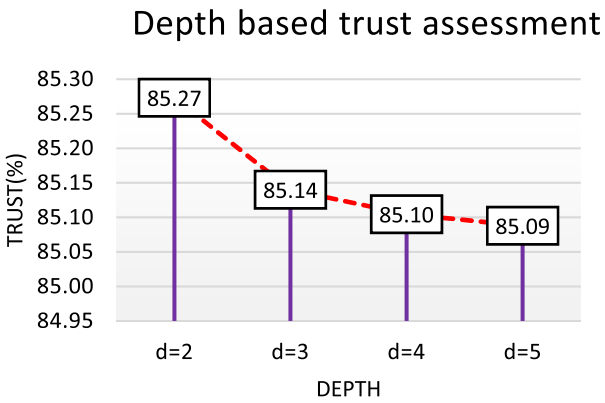
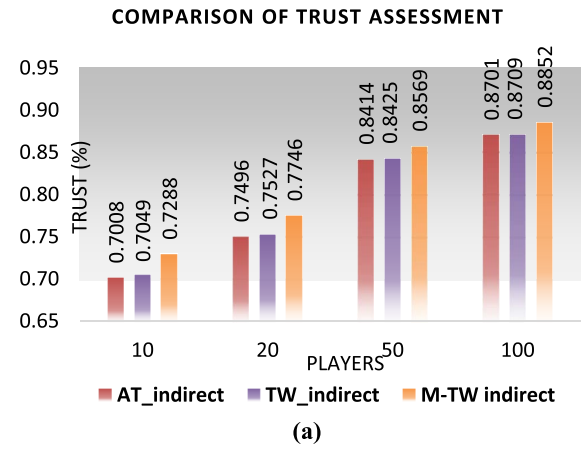


FIGURE 8. Depth-based trust assessment.

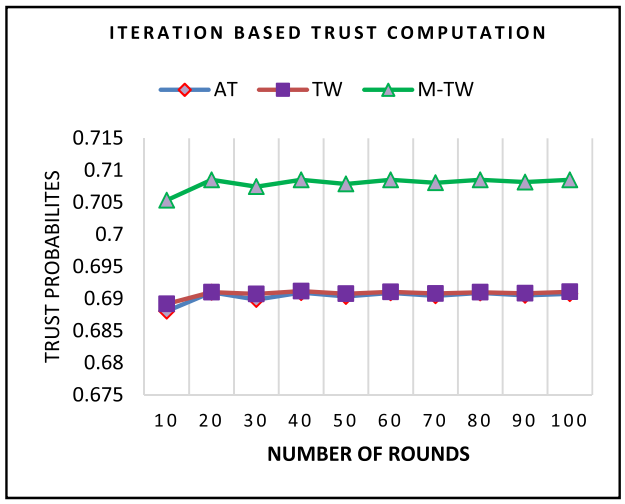
Therefore, when the network size increases, the trust opinions of the players also increase by $10-15\%$ overall. However, the network size is 100 the produced min, average, and max trust opinions provide a slight difference, i.e., $\cong$ 0.02. The performance of the proposed algorithm is analyzed depth-wise because the M-TW algorithm works in a DL-BFS fashion, and the results are shown in Figure 8.

The trust is assessed based on the depth; the plotted results are illustrated in Figure 8. Initial depth started from $d = 2$ produces the trust opinion as 85.27. While the depth is slowly increased, examine the trust opinion decreasing slightly. According to Figure 8, when the depth increases, the trust opinion value decreases because the trust is assessed based on the recommendations of the other players' opinions—the opinion of players changes based on context. Moreover, the proposed scheme uses the boolean vector that manages the opinion changes. Once the assessment reaches the longest path, trust opinion is not changed. Therefore in Figure 8, the trust opinion value for $d = 4$ *and* 5 produces approximately the same opinion. Likewise, the proposed trust assessment scheme, such as I-3VSL with M-TW, is compared with AT [45]. The TW trustworthiness computation according to the number of players and iterations results are shown in Figures 9 (a) and (b).

The trust opinion concerning the number of players as 10, 20, 50, *and* 100 is represented in Figure 9 (a). The trust assessment with AT produces the trust opinion values significantly less compared to the TW [47] and M-TW. The M-TW has a higher trust opinion compared to the TW algorithm. However, M-TW enhances the trust assessment by $8-10\%$ over the AT trust assessment and $7-9\%$ over the TW algorithm. Similarly, the Figure 9 (b) shows the better trust assessment results with the M-TW algorithm for numerous iterations and after 50^{th} iteration, the trust opinion values are changed slightly, but the AT and TW algorithm are constantly producing. Besides, the M-TW algorithm provides the enhanced trust opinion over the AT and TW as $10-12\%$ for each iteration. Further, the execution time of M-TW compared with AT [45] and TW [47] and shown in Figure 10.



(a)



(b)

FIGURE 9. Comparison of trust assessment.

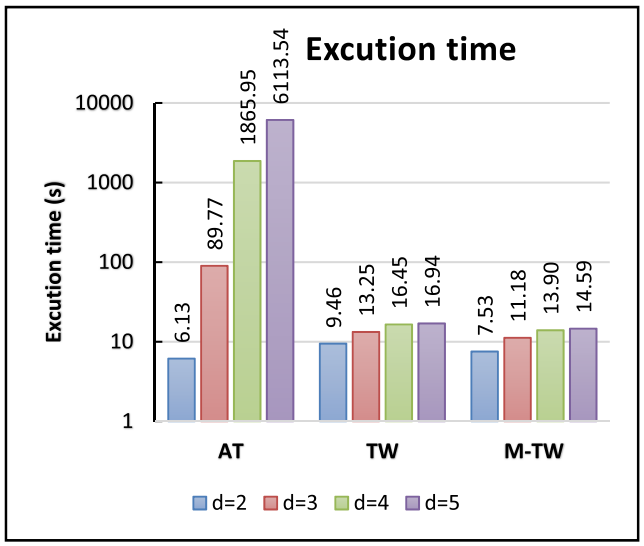


FIGURE 10. Trust assessment execution time comparison.

According to Figure 10, the trust execution time is compared with AT [45] and TW [47] algorithms over the M-TW. The obtained results show that when the depth is in a smaller range, the AT produces better results compared to TW and M-TW. However, the depth and execution time increase exponentially in AT. Similarly, in the comparison among the TW and M-TW trust assessment, the trustor to trustee finds the longest path then there is no change in its trust opinion value. Hence, M-TW produces quicker results than TW, as shown in Figure 10. Further, the mean absolute error (MAE) and accuracy of the AT, TW, and M-TW algorithms are evaluated using Eq. (36), (37), and (38).

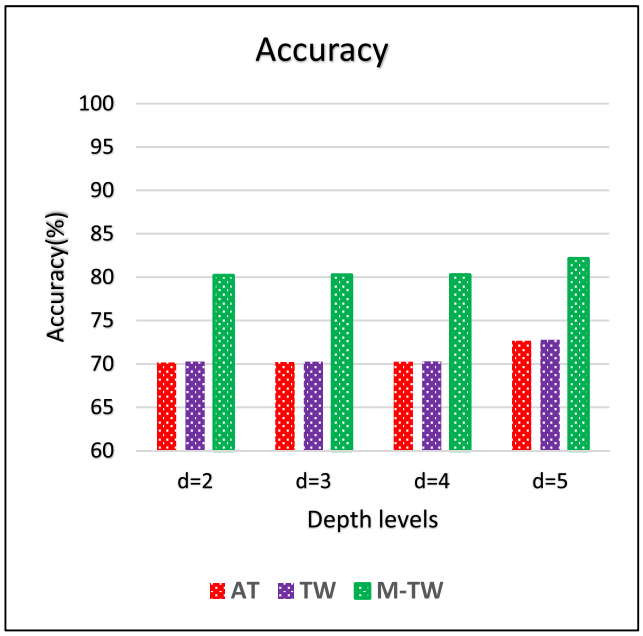


FIGURE 11. Comparison of accuracy.

$$Error = (predicted\ trust - actualtrust) \tag{36}$$

$$MAE = \frac{\sum_{i=1}^{n} Error_i}{\sum_{i=1}^{n} actualtrust\_i} \tag{37}$$

$$Accuracy = (1 - Error\_rate) \tag{38}$$

According to Eq. (36), (37), and (38), the MAE and Accuracy are assessed for various depths using AT [45], TW [47], and M-TW algorithms. The accuracy of the proposed scheme is compared with the AT and TW, which is illustrated in Figure 11.

The accuracy of the proposed scheme is compared with the existing approaches. The results show that the AT with M-TW provides a 10% enhancement, and the M-TW algorithm offers a 9% enhancement over the TW approach. Similarly, the TW improves the 0.07% over the AT algorithm.

VI. SUMMARY AND CONCLUSION

The internet-based applications are increasing, leading to numerous VE applications, especially MMOG. In MMOG, the players interact and share resources among the virtual game players. However, these players' behavior is uncertain, and without assessing the trustworthiness of the resource, it enables various security challenges. Therefore, the proposed work performs the trust assessment by leveraging

I-3VSL and the route from trustor to trustee through M-TW. The M-TW algorithm is designed to optimize the computation complexity over the existing algorithms, and the experiment uses the Travian dataset and establishes the arbitrary or bridge network. The performance of the proposed approach is compared with the existing AT, TW. The results demonstrate that the proposed work improves the trust assessment score by $8-10\%$ over the AT t and $7-9\%$ over the TW algorithm. Further, the computation time of the proposed approach is evaluated for multiple depths that reduce the 2% over the TW algorithm. Therefore, the proposed method is more efficient than AT and TW. The future work will improve the I-3VSL operations by including Monte Carlo principles. Further, the I-3VSL performance is verified with a complicated topology.

REFERENCES

[1] S. Bueno, M. D. Gallego, and J. Noyes, "Uses and gratifications on augmented reality games: An examination of Pokémon go," *Appl. Sci.*, vol. 10, no. 5, p. 1644, Mar. 2020, doi: 10.3390/app10051644.

[2] B. Sanchez, R. Ballinas-Gonzalez, and M. X. Rodriguez-Paz, "BIM and game engines for engineering online learning," in *Proc. IEEE Global Eng. Educ. Conf. (EDUCON)*, Mar. 2022, pp. 1467–1472, doi: 10.1109/EDUCON52537.2022.9766711.

[3] B. C. Ooi, K. L. Tan, A. Tung, G. Chen, M. Z. Shou, X. Xiao, and M. Zhang, "Sense the physical, walkthrough the virtual, manage the metaverse: Adata-centric perspective," Jun. 2022, *arXiv:2206.10326*.

[4] S. Müller, R. Ghawi, and J. Pfeffer, "Using communication networks to predict team performance in massively multiplayer online games," in *Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining (ASONAM)*, Dec. 2020, pp. 353–360, doi: 10.1109/ASONAM49781.2020.9381481.

[5] L. V. Fernandes, C. D. Castanho, and R. P. Jacobi, "A survey on game analytics in massive multiplayer online games," in *Proc. 17th Brazilian Symp. Comput. Games Digit. Entertainment (SBGames)*, Oct. 2018, pp. 21–2109, doi: 10.1109/SBGAMES.2018.00012.

[6] A. Hajibagheri, G. Sukthankar, K. Lakkaraju, H. Alvari, R. T. Wigand, and N. Agarwal, "Using massively multiplayer online game data to analyze the dynamics of social interactions," in *Social Interactions in Virtual Worlds, An Interdisciplinary Perspective*, G. Sukthankar, K. Lakkaraju, and R. T. Wigand, Eds. Cambridge, U.K.: Cambridge Univ. Press, 2018, pp. 375–416, doi: 10.1017/9781316422823.015.

[7] T. V. Kornilova, M. A. Chumakova, and S. A. Kornilov, "Tolerance and intolerance for uncertainty as predictors of decision making and risk acceptance in gaming strategies of the Iowa gambling task," *Psychol. Russia*, vol. 11, no. 3, p. 86, 2018.

[8] V. Nae, A. Iosup, and R. Prodan, "Dynamic resource provisioning in massively multiplayer online games," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 3, pp. 380–395, Mar. 2011, doi: 10.1109/TPDS.2010.82.

[9] H. R. Maamar, A. Boukerche, and E. Petriu, "MOSAIC—A mobile peer-to-peer networks-based 3D streaming supplying partner protocol," in *Proc. IEEE/ACM 14th Int. Symp. Distrib. Simul. Real Time Appl.*, Oct. 2010, pp. 61–68, doi: 10.1109/DS-RT.2010.16.

[10] M. Salovaara-Hiltunen, K. Heikkinen, and J.-M. Koivisto, "User experience and learning experience in a 4D virtual reality simulation game," *Int. J. Serious Games*, vol. 6, no. 4, pp. 49–66, Nov. 2019, doi: 10.17083/ijsg.v6i4.305.

[11] J.-H. Kim, "Bandwidth analysis of massively multiplayer online games based on peer-to-peer and cloud computing," *J. Inst. Internet Broadcast. Commun.*, vol. 19, no. 5, pp. 143–150, 2019, doi: 10.7236/JIIBC.2019.19.5.143.

[12] A. Qureshi, H. Rifa-Pous, and D. Megias, "State-of-the-art, challenges and open issues in integrating security and privacy in P2P content distribution systems," in *Proc. 11th Int. Conf. Digit. Inf. Manag. (ICDIM)*, Sep. 2016, pp. 1–9, doi: 10.1109/ICDIM.2016.7829784.

[13] H. Akrout, "Trust in buyer-supplier relationships: Evidence from advanced, emerging, and developing markets," in *New Insights Trust Business-to-Business Relationships*, vol. 26. Bingley, U.K.: Emerald Publishing Limited, 2019, pp. 1–5, doi: 10.1108/S1069-096420190000026004.

[14] F. Hendrikx, K. Bubendorfer, and R. Chard, "Reputation systems: A survey and taxonomy," *J. Parallel Distrib. Comput.*, vol. 75, pp. 184–197, Jan. 2015, doi: 10.1016/j.jpdc.2014.08.004.

[15] Z. Gong, H. Wang, W. Guo, Z. Gong, and G. Wei, "Measuring trust in social networks based on linear uncertainty theory," *Inf. Sci.*, vol. 508, pp. 154–172, Jan. 2020, doi: 10.1016/j.ins.2019.08.055.

[16] Y. He, C. Liang, F. R. Yu, and Z. Han, "Trust-based social networks with computing, caching and communications: A deep reinforcement learning approach," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 1, pp. 66–79, Jan. 2020, doi: 10.1109/TNSE.2018.2865183.

[17] G. Yang, Q. Yang, and H. Jin, "A novel trust recommendation model for mobile social network based on user motivation," *Electron. Commerce Res.*, vol. 21, no. 3, pp. 809–830, Sep. 2021, doi: 10.1007/s10660-019-09344-9.

[18] M. R. Frank, D. Wang, M. Cebrian, and I. Rahwan, "The evolution of citation graphs in artificial intelligence research," *Nat. Mach. Intell.*, vol. 1, no. 2, pp. 79–85, Feb. 2019, doi: 10.1038/s42256-019-0024-5.

[19] T. Fan and Y. Wang, "Visual social network group consensus method with improved PageRank algorithm," *Kybernetes*, Apr. 2022. [Online]. Available: https://www.emerald.com/insight/content/doi/10.1108/K-12-2021-1301/full/html, doi: 10.1108/K-12-2021-1301.

[20] M. Hosseinzadeh, K. G. Delarestaghi, and M. Momeni, "Developing the page rank algorithm in social network analysis for cross-docking location problem," *J. Prod. Oper. Manag.*, vol. 11, no. 2, pp. 69–88, Jul. 2020, doi: 10.22108/jpom.2020.123719.1278.

[21] K. M. Frahm and D. L. Shepelyansky, "Ising-PageRank model of opinion formation on social networks," *Phys. A, Stat. Mech. Appl.*, vol. 526, Jul. 2019, Art. no. 121069, doi: 10.1016/j.physa.2019.121069.

[22] E. Bautista and M. Latapy, "A local updating algorithm for personalized PageRank via Chebyshev polynomials," *Social Netw. Anal. Mining*, vol. 12, no. 1, p. 31, Feb. 2022, doi: 10.1007/s13278-022-00860-5.

[23] R. Islam, M. K. Devnath, M. D. Samad, and S. M. J. A. Kadry, "GGNB: Graph-based Gaussian naive Bayes intrusion detection system for CAN bus," *Veh. Commun.*, vol. 33, Jan. 2022, Art. no. 100442, doi: 10.1016/j.vehcom.2021.100442.

[24] Y. S. Alsenani, G. V. Crosby, K. R. Ahmed, and T. Velasco, "ProTrust: A probabilistic trust framework for volunteer cloud computing," *IEEE Access*, vol. 8, pp. 135059–135074, 2020, doi: 10.1109/ACCESS.2020.3009051.

[25] I. P. Bodala, B. C. Kok, W. Sng, and H. Soh, "Modeling the interplay of trust and attention in HRI: An autonomous vehicle study," in *Proc. Companion ACM/IEEE Int. Conf. Hum.-Robot Interact.*, Mar. 2020, pp. 145–147, doi: 10.1145/3371382.3378262.

[26] S. Afroogh, "A probabilistic theory of trust concerning artificial intelligence: Can intelligent robots trust humans?" *AI Ethics*, vol. 2, pp. 1–16, Jun. 2022, doi: 10.1007/s43681-022-00174-4.

[27] V. Khattar and A. Eskandarian, "Stochastic reachable set threat assessment for autonomous vehicles using trust-based driver behavior prediction," *SAE Int. J. Connected Automated Vehicles*, vol. 6, no. 2, pp. 1–15, Jul. 2022, doi: 10.4271/12-06-02-0008.

[28] A. Molina-Markham and J. J. Rushanan, "Probabilistic inference for trust," *Notices Amer. Math. Soc.*, vol. 67, no. 5, pp. 710–711, May 2020, doi: 10.1090/noti2081.

[29] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The EigenTrust algorithm for reputation management in P2P networks," in *Proc. 12th Int. Conf. World Wide Web*, 2003, pp. 640–651.

[30] H. A. Kurdi, "HonestPeer: An enhanced EigenTrust algorithm for reputation management in P2P systems," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 27, no. 3, pp. 315–322, Jul. 2015, doi: 10.1016/j.jksuci.2014.10.002.

[31] A. Bojchevski, J. Klicpera, B. Perozzi, A. Kapoor, M. Blais, B. Rozemberczki, M. Lukasik, and S. Gunnemann, "Scaling graph neural networks with approximate PageRank," in *Proc. 26th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2020, pp. 2464–2473.

[32] H. Shirgahi, M. Mohsenzadeh, and H. H. S. Javadi, "A new method of trust mirroring estimation based on social networks parameters by fuzzy system," *Int. J. Mach. Learn. Cybern.*, vol. 9, no. 7, pp. 1153–1168, Jul. 2018, doi: 10.1007/s13042-017-0638-z.

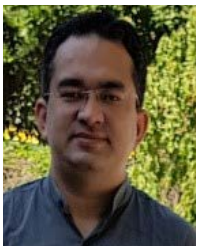
[33] Y. Atif, K. Al-Falahi, T. Wangchuk, and B. Lindström, "A fuzzy logic approach to influence maximization in social networks," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 6, pp. 2435–2451, Jun. 2020, doi: 10.1007/s12652-019-01286-2.

[34] M. Nilashi, E. Yadegaridehkordi, O. Ibrahim, S. Samad, A. Ahani, and L. Sanzogni, "Analysis of Travellers' online reviews in social networking sites using fuzzy logic approach," *Int. J. Fuzzy Syst.*, vol. 21, no. 5, pp. 1367–1378, Jul. 2019, doi: 10.1007/s40815-019-00630-0.

[35] C. J. Fung, J. Zhang, I. Aib, and R. Boutaba, "Dirichlet-based trust management for effective collaborative intrusion detection networks," *IEEE Trans. Netw. Service Manag.*, vol. 8, no. 2, pp. 79–91, Jun. 2011.
[36] A. Jøsang and T. Bhuiyan, "Trust network analysis with subjective logic," in *Proc. 2nd Int. Conf. Emerg. Secur. Inf., Syst. Technol.*, Aug. 2008, pp. 85–94.
[37] A. Jøsang and T. Bhuiyan, "Optimal trust network analysis with subjective logic," in *Proc. 2nd Int. Conf. Emerg. Secur. Inf., Syst. Technol.*, Aug. 2008, pp. 179–184, doi: 10.1109/SECURWARE.2008.64.
[38] Y. Yang, L. He, and X. Cai, "A dynamic trust evaluation algorithm based on subjective logic in pervasive computing environment," in *Proc. 10th Int. Conf. Control, Autom., Robot. Vis.*, Dec. 2008, pp. 1078–1083, doi: 10.1109/ICARCV.2008.4795669.
[39] J. Al Muhtadi, R. A. Alamri, F. A. Khan, and K. Saleem, "Subjective logic-based trust model for fog computing," *Comput. Commun.*, vol. 178, pp. 221–233, Oct. 2021, doi: 10.1016/j.comcom.2021.05.016.
[40] N. B. Akhuseyinoglu, M. Karimi, M. Abdelhakim, and P. Krishnamurthy, "On automated trust computation in IoT with multiple attributes and subjective logic," in *Proc. IEEE 45th Conf. Local Comput. Netw. (LCN)*, Nov. 2020, pp. 267–278, doi: 10.1109/LCN48667.2020.9314808.
[41] R. C. Cardoso, A. J. P. Gomes, and M. M. Freire, "A user trust system for online games—Part I: An activity theory approach for trust representation," *IEEE Trans. Comput. Intell. AI Games*, vol. 9, no. 3, pp. 305–320, Sep. 2017, doi: 10.1109/TCIAIG.2016.2592965.
[42] R. C. Cardoso, A. J. P. Gomes, and M. M. Freire, "A user trust system for online games—Part II: A subjective logic approach for trust inference," *IEEE Trans. Comput. Intell. AI Games*, vol. 9, no. 4, pp. 354–368, Dec. 2017, doi: 10.1109/TCIAIG.2016.2593000.
[43] G. Liu, Q. Yang, H. Wang, X. Lin, and M. P. Wittie, "Assessment of multi-hop interpersonal trust in social networks by three-valued subjective logic," in *Proc. IEEE Conf. Comput. Commun.*, Apr. 2014, pp. 1698–1706.
[44] T. Cheng, G. Liu, Q. Yang, and J. Sun, "Trust assessment in vehicular social network based on three-valued subjective logic," *IEEE Trans. Multimedia*, vol. 21, no. 3, pp. 652–663, Mar. 2019, doi: 10.1109/TMM.2019.2891417.
[45] G. Liu, Q. Yang, H. Wang, and A. X. Liu, "Trust assessment in online social networks," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 2, pp. 994–1007, Mar. 2021, doi: 10.1109/TDSC.2019.2916366.
[46] M. Sohail and L. Wang, "3VSR: Three valued secure routing for vehicular ad hoc networks using sensing logic in adversarial environment," *Sensors*, vol. 18, no. 3, p. 856, Mar. 2018, doi: 10.3390/s18030856.
[47] M. Sohail, L. Wang, S. Jiang, S. Zaineldeen, and R. U. Ashraf, "Multi-hop interpersonal trust assessment in vehicular ad-hoc networks using three-valued subjective logic," *IET Inf. Secur.*, vol. 13, no. 3, pp. 223–230, May 2019, doi: 10.1049/iet-ifs.2018.5336.
[48] P. Srikanth and A. Kumar, "A trustworthy partner selection for MMOG using an improved three valued subjective logic uncertainty trust model," *PalArchs J. Archaeol. Egypt Egyptol.*, vol. 18, no. 4, pp. 5677–5698, Mar. 2021. [Online]. Available: https://archives.palarch.nl/index.php/jae/article/view/7160
[49] G. Liu, Q. Chen, Q. Yang, B. Zhu, H. Wang, and W. Wang, "OpinionWalk: An efficient solution to massive trust assessment in online social networks," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, May 2017, pp. 1–9, doi: 10.1109/INFOCOM.2017.8057106.
[50] N. Sun and J. Botev, "Intelligent autonomous agents and trust in virtual reality," *Comput. Hum. Behav. Rep.*, vol. 4, Aug. 2021, Art. no. 100146, doi: 10.1016/j.chbr.2021.100146.
[51] A. I. A. Ahmed, S. H. A. Hamid, A. Gani, S. Khan, and M. K. Khan, "Trust and reputation for Internet of Things: Fundamentals, taxonomy, and open research challenges," *J. Netw. Comput. Appl.*, vol. 145, Nov. 2019, Art. no. 102409, doi: 10.1016/j.jnca.2019.102409.
[52] M. J. Dupre and F. J. Tipler, "New axioms for rigorous Bayesian probability," *Bayesian Anal.*, vol. 4, no. 3, pp. 599–606, 2009.
[53] Y. Xiao, L. Zhu, and X. Li, "A review on trust and reputation management systems in E-commerce and P2P network," in *Proc. 2nd Int. Conf. E-Commerce Internet Technol. (ECIT)*, Mar. 2021, pp. 58–62, doi: 10.1109/ECIT52743.2021.00020.
[54] M. Carbone, M. Nielsen, and V. Sassone, "A formal model for trust in dynamic networks," in *Proc. 1st Int. Conf. Softw. Eng. Formal Methods*, 2003, pp. 54–61, doi: 10.1109/SEFM.2003.1236207.
[55] Y. Wang and M. P. Singh, "Evidence-based trust: A mathematical model geared for multiagent systems," *ACM Trans. Auto. Adapt. Syst.*, vol. 5, no. 4, pp. 1–28, Nov. 2010, doi: 10.1145/1867713.1867715.
[56] A. Josang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decis. Support Syst.*, vol. 43, no. 2, pp. 618–644, 2007. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167923605000849
[57] W. T. L. Teacy, J. Patel, N. R. Jennings, and M. Luck, "TRAVOS: Trust and reputation in the context of inaccurate information sources," *Auto. Agents Multi-Agent Syst.*, vol. 12, no. 2, pp. 183–198, Mar. 2006, doi: 10.1007/s10458-006-5952-x.
[58] V. Cahill, E. Gray, J.-M. Seigneur, C. D. Jensen, Y. Chen, B. Shand, N. Dimmock, A. Twigg, J. Bacon, C. English, W. Wagealla, S. Terzis, P. Nixon, G. D. M. Serugendo, C. Bryce, M. Carbone, K. Krukow, and M. Nielsen, "Using trust for secure collaboration in uncertain environments," *IEEE Pervasive Comput.*, vol. 2, no. 3, pp. 52–61, Jul. 2003.
[59] H. Lin, X. Wu, and H. Lin, "Hierarchical fuzzy trust management for peer-to-peer network," in *Proc. Int. Colloq. Comput., Commun., Control, Manag. (ISECS)*, Aug. 2009, pp. 377–380, doi: 10.1109/CCCM.2009.5270416.
[60] J. Sabater and C. Sierra, "Social ReGreT, a reputation model, based on social relations," *ACM SIGecom Exchanges*, vol. 3, no. 1, pp. 44–56, 2001, doi: 10.1145/844331.844337.
[61] A. Bhargava and S. Verma, "DEIT: Dempster shafer theory-based edge-centric Internet of Things-specific trust model," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 6, p. e4248, Jun. 2021, doi: 10.1002/ett.4248.
[62] L. A. Zadeh, "A simple view of the Dempster–Shafer theory of evidence and its implication for the rule of combination," *AI Mag.*, vol. 7, no. 2, p. 85, Jun. 1986, doi: 10.1609/aimag.v7i2.542.
[63] J. Pearl, "Reasoning with belief functions: An analysis of compatibility," *Int. J. Approx. Reason.*, vol. 4, nos. 5–6, pp. 363–389, Sep. 1990, doi: 10.1016/0888-613X(90)90013-R.
[64] B. Tripathy, P. Bera, and M. Rahman, "Analysis of trust models in mobile ad hoc networks: A simulation-based study," in *Proc. 8th Int. Conf. Commun. Syst. Netw.*, 2016, pp. 1–8, doi: 10.1109/COMSNETS.2016.7440007.
[65] P. Smets, "The combination of evidence in the transferable belief model," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 12, no. 5, pp. 447–458, May 1990, doi: 10.1109/34.55104.
[66] F. Voorbraak, "On the justification of Dempster's rule of combination," *Artif. Intell.*, vol. 48, no. 2, pp. 171–197, 1991, doi: 10.1016/0004-3702(91)90060-W.
[67] R. R. Yager, "On the Dempster–Shafer framework and new combination rules," *Inf. Sci.*, vol. 41, no. 2, pp. 93–137, Mar. 1987, doi: 10.1016/0020-0255(87)90007-7.
[68] D. Dubois and H. Prade, "Representation and combination of uncertainty with belief functions and possibility measures," *Comput. Intell.*, vol. 4, no. 3, pp. 244–264, Sep. 1988, doi: 10.1111/j.1467-8640.1988.tb00279.x.
[69] W. Ma, Y. Jiang, and X. Luo, "A flexible rule for evidential combination in Dempster–Shafer theory of evidence," *Appl. Soft Comput.*, vol. 85, Dec. 2019, Art. no. 105512, doi: 10.1016/j.asoc.2019.105512.
[70] C. K. Murphy, "Combining belief functions when evidence conflicts," *Decis. Support Syst.*, vol. 29, no. 1, pp. 1–9, Jul. 2000, doi: 10.1016/S0167-9236(99)00084-6.
[71] D. Yong, S. WenKang, Z. ZhenFu, and L. Qi, "Combining belief functions based on distance of evidence," *Decis. Support Syst.*, vol. 38, no. 3, pp. 489–493, Dec. 2004, doi: 10.1016/j.dss.2004.04.015.
[72] Z. Zhang, T. Liu, D. Chen, and W. Zhang, "Novel algorithm for identifying and fusing conflicting data in wireless sensor networks," *Sensors*, vol. 14, no. 6, pp. 9562–9581, May 2014, doi: 10.3390/s140609562.
[73] K. Yuan, F. Xiao, L. Fei, B. Kang, and Y. Deng, "Conflict management based on belief function entropy in sensor fusion," *SpringerPlus*, vol. 5, no. 1, p. 638, May 2016, doi: 10.1186/s40064-016-2205-6.
[74] F. Xiao, "Multi-sensor data fusion based on the belief divergence measure of evidences and the belief entropy," *Inf. Fusion*, vol. 46, pp. 23–32, Mar. 2019, doi: 10.1016/j.inffus.2018.04.003.
[75] Y. Song and Y. Deng, "A new method to measure the divergence in evidential sensor data fusion," *Int. J. Distrib. Sens. Netw.*, vol. 15, no. 4, Apr. 2019, Art. no. 1550147719841295, doi: 10.1177/1550147719841295.
[76] K. Zhao, L. Li, Z. Chen, R. Sun, G. Yuan, and J. Li, "A survey: Optimization and applications of evidence fusion algorithm based on Dempster–Shafer theory," *Appl. Soft Comput.*, vol. 124, Jul. 2022, Art. no. 109075, doi: 10.1016/j.asoc.2022.109075.
[77] A. G. West, A. J. Aviv, J. Chang, V. S. Prabhu, M. Blaze, S. Kannan, I. Lee, J. M. Smith, and O. Sokolsky, "QuanTM: A quantitative trust management system," in *Proc. 2nd Eur. Workshop Syst. Secur. (EUROSEC)*, Nuremburg, Germany, 2009, pp. 28–35, doi: 10.1145/1519144.1519149.

[78] H. Kurdi, A. Alfaries, A. Al-Anazi, S. Alkharji, M. Addegaither, L. Altoaimy, and S. H. Ahmed, "A lightweight trust management algorithm based on subjective logic for interconnected cloud computing environments," *J. Supercomput.*, vol. 75, no. 7, pp. 3534–3554, Oct. 2018. [Online]. Available: https://dspace.mit.edu/handle/1721.1/131530
[79] J. Golbeck and J. Hendler, "FilmTrust: Movie recommendations using trust in web-based social networks," in *Proc. 3rd IEEE Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, 2006, pp. 282–286, doi: 10.1109/CCNC.2006.1593032.
[80] P. Massa and P. Avesani, "Controversial users demand local trust metrics: An experimental study on epinions. com community," in *Proc. AAAI*, vol. 1, Pittsburgh, PA, USA, Jul. 2005, pp. 121–126.
[81] M. Hedabou, "Cryptography for addressing cloud computing security, privacy, and trust issues," in *Computer and Cyber Security*. New York, NY, USA: Auerbach Publications, 2018.
[82] I. Zakaria and H. Mustaha, "FADETPM: Novel approach of file assured deletion based on trusted platform module," in *Proc. 3rd Int. Conf. Cloud Comput. Technol. Appl. (CloudTech)*, Oct. 2017, pp. 1–4, doi: 10.1109/CloudTech.2017.8284727.
[83] M. Hedabou, "A Frobenius map approach for an efficient and secure multiplication on Koblitz curves," *Int. J. Netw. Secur.*, vol. 3, no. 3, pp. 239–243, 2006.
[84] *Trust Definition & Meaning-Merriam-Webster*. Accessed: Dec. 25, 2021. [Online]. Available: https://www.merriam-webster.com/dictionary/trust
[85] *NetworkX-NetworkX Documentation*. Accessed: Nov. 11, 2021. [Online]. Available: https://networkx.org/
[86] C.-Y. Huang and W. C. B. Chin, "Distinguishing arc types to understand complex network strength structures and hierarchical connectivity patterns," *IEEE Access*, vol. 8, pp. 71021–71040, 2020, doi: 10.1109/ACCESS.2020.2986017.
[87] U. N. Raghavan, R. Albert, and S. Kumara, "Near linear time algorithm to detect community structures in large-scale networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 76, no. 3, 2007, Art. no. 036106, doi: 10.1103/PhysRevE.76.036106.

P SRIKANTH received the B.Tech. degree in information technology and the M.Tech. degree in computer science with a specialization in parallel computing from JNTU Hyderabad, India, in 2006 and 2012, respectively, and the Ph.D. degree in computer science and engineering from the University of Petroleum and Energy Studies, Dehradun, India. He is currently an Assistant Professor-Selection Grade with the School of Computer Science, University of Petroleum and Energy Studies. He has been associated with the Department of Computer Science and Engineering, Maheshwara Institute of Technology, Hyderabad, India, where he worked as an Assistant Professor. His main research interests include trust assessment, social networks, information security, cryptography, mobile ad-hoc networks, and blockchain technology. Many of his research publications have appeared in reputed journals and conferences at the international and national levels. He has Indian, Australian, and German patents in his research.



ADARSH KUMAR received the M.Tech. degree in software engineering from Thapar University, Patiala, Punjab, India, the Ph.D. degree from the Jaypee Institute of Information Technology, Noida, Uttar Pradesh, India, and the Ph.D. degree from the Software Research Institute, Athlone Institute of Technology, Ireland. From 2005 to 2016, he was associated with the Department of Computer Science Engineering and Information Technology, Jaypee Institute of Information Technology, where he worked as an Assistant Professor. He is currently an Associate Professor with the School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India. He has many research papers in reputed journals, conferences, and workshops. He has participated in one European Union H2020-sponsored research project. He is currently executing two research projects sponsored by the UPES SEED Division and one sponsored by Lancaster University. His main research interests include cybersecurity, cryptography, network security, and ad-hoc networks.

MUSTAPHA HEDABOU received the M.Sc. degree in mathematics from the University of Paul Sabatier, Toulouse, France, and the Ph.D. degree in cryptography from the INSA de Toulouse, France, in 2006. He is currently an Associate Professor at the School of Computer and Communication Sciences, Mohammed VI Polytechnic University. Prior to assuming his current position, he was a Research Scientist in digital security industry. His research interests include cryptography, information security, the IoT security, blockchain, and cloud computing security.