ITERATIVE RATING THROUGH VOTING ALGORITHM-MULTI PARAMETER AGGREGATION

Manjula Pilaka, K V N Sunitha, Aruna Rao S L

Computer Science and Engineering, BVRIT Hyderabad College of Engineering for Women, India

ABSTRACT

With the rapid growth of academic search engines, the visibility and impact of scholarly articles depend heavily on how effectively they are ranked. While systems such as Google Scholar emphasize citation counts, community sentiment and other contextual attributes can also provide important signals of trustworthiness. Similarly, in professional platforms like LinkedIn, the credibility of recommendations depends not only on the recommender's opinion but also on their expertise and standing within the community. This paper introduces an Iterative Voting Algorithm with Multi-Parameter Aggregation (VMPA) that integrates multiple voter attributes into the ranking process. The algorithm is designed to mitigate individual collusion, group collusion, and biased voting, while ensuring that authentic but infrequent voters are not overlooked. Each voter is associated with measurable parameters such as academic experience, citation record, and organizational affiliation, which are incorporated into their voting weight. The method is evaluated using both real and synthetic datasets in the context of conference ranking. Results show that the algorithm successfully identifies colluders, preserves genuine contributions, and produces rankings consistent with credible benchmarks such as CORE. The findings suggest that multi-parameter aggregation improves robustness, enhances trustworthiness, and reduces the number of iterations required for convergence.

KEYWORDS

MPIA - Multi Parameter Identification and Aggregation VMPA - Voting with Multi Parameter Aggregation

1. INTRODUCTION

Trust is a cornerstone of digital interaction, particularly in environments where participants engage without direct personal or institutional assurances[9]. Online ecosystems such as e-commerce platforms, academic search engines, and social networks face ongoing challenges in preventing manipulation, ensuring fairness, and maintaining credibility. Unlike traditional paper-based trust mechanisms, digital systems operate at scale, where interactions can be replicated indefinitely and malicious behavior can spread quickly.

One significant challenge is the presence of spammers and colluders who distort voting or recommendation systems for personal gain[10]. These actors often produce misleading evaluations that deviate significantly from community consensus, reducing the reliability of aggregated outcomes. Consequently, detecting such behavior and reinforcing trustworthiness has become an essential area of research. Ranking algorithms play an important role in information retrieval and decision-making[3,6]. Users not only expect relevant results but also prefer outcomes derived from credible and authoritative sources. Ensuring that rankings reflect genuine

Bibhu Dash et al: EDU, EDUTEC, CCITT - 2026
pp. 57-68, 2025. IJCI – 2026 DOI:10.5121/ijci.2026.150106

sentiment while incorporating contextual factors such as expertise, experience, and reliability is key to preventing manipulation.

Recent work emphasizes these challenges in modern contexts such as federated learning and blockchain-based e-voting. For example, Chu & Laoutaris (2024) propose quadratic voting with trust-weighted budgets to resist poisoning in federated learning [1], while Somasekhar et al. (2024) and Rausch et al. (2025) show how blockchain and cryptographic primitives enhance verifiability and trust in digital voting [4,3]. In this paper, we propose an Iterative Voting Algorithm with Multi-Parameter Aggregation (VMPA) that incorporates community sentiment alongside quantifiable voter parameters. The approach aims to distinguish collusive and biased actors from authentic participants while safeguarding the influence of occasional but trustworthy voters.

In this section we define the basic terms we use in the following section. These terms may have various meanings depending on the area in which they are used. The following are the meanings we intend when using these terms. A Rating is the evaluation or assessment, in terms of quality (as with a critic rating a conference), quantity, or some combination of both. A Voter is the person who evaluates the product and provides feedback as evaluation for the product. A Voter Parameter is a numerical or other measurable factor forming one of a set that defines the person/product which sets the conditions of the operation/election. An Election process is all the raters will be provided a group/list of products and will be asked to provide their ranking as rating based on the goodness/quality of the product.Thus, in our technical usage, an election is the process of choosing a best describing rating level for a product. Trustworthiness of the rater can be taken as the voter has provided his voting how best or close to the sentiment of the community(most of the people voting to the genuine person or product) and other parameters identified like experience, age, skill level in rating, how long he/she is associated with this product/ person etc.. parameters improve the trust worthiness factor. Voting Scores are the scores which are produced by our system or other systems which we use for comparison purposes to reflect the quality of a product. We may use 'scores' or 'ranks' interchangeably to refer to such scores [1].

Recent work in truth discovery and trust aware aggregation also tackles collusion and noisy sources by jointly estimating item quality and source reliability.Yin et al. study “truth discovery with multiple conflicting information providers” and show how iterative re-weighting can separate reliable and unreliable sources in Web data [14]. Li et al. survey a large family of truth-discovery methods, many of which use weighted voting schemes similar in spirit to our iterative voting, but often treat source reliability as a single latent parameter [15].More recent work exceeds these ideas to dynamic and numerical data, as well as privacy-preserving truth discovery[18].Complementarily ,truth, reputation and collusion focus on robust reputation scores and group rankings in adversarial environments[16][17][19][20][21]. In contrast to these approaches, our voting with Multi-Parameter Aggregation(VMPA) explicitly incorporates multi dimensional externally observable voter attributes(e.g citation counts, publication records, institutional profile) into the iterative voting process, while preserving community-sentiment signal.

The main contributions of the work are:

1. We formalise a multi-parameter voter model in which each voter is associated with measurable academic attributes and show how to aggregate them into a single trust weight.
2. We propose VMPA, an iterative rating through voting algorithm that integrates multi-parameter trust weights with community sentiment to resist individual, group and baited colluders

3. We provide empirical analysis on real and synthetic conference ranking scenarios and discuss how VMPA relates to state of art truth discovery and collusion resistant ranking methods.

The remainder of the paper is organized as follows: In Section 2 we define objectives and explain application scenarios in detail. In Section 3 we detail the related work. In Section 4 we propose our voting algorithm. Then we propose our 'Voting with Multi-Parameter aggregation method in Section 4.1. In Section 5 we explain implementation of our method and also discuss the results of evaluating our method and Section 6 concludes the paper with the future work reference.

2. Objective and Application Scenario

The specific problem that we target in this paper is the accurate identification of the top ranked Conference in a list of 10 top conferences identified in subject area networks and ranked by program committee members[8]. The program committee members are people who have academic background and their academic details are available on academic search engines like Microsoft research, google scholar etc. In this case the voters (program committee members) are not anonymous voters but voters whose academic record like their citation count, publication count, journal count, their associated university/organization publication count and journal count can be retrieved from popular academic search engines. The key parameters like citation count mentioned above emphasize the academic track record of that person. In this paper we explain the iterative rating method "Voting - Multi parameter aggregation" to obtain robust rating against any colluders and biased voters. The objective is to obtain high trustworthiness through multi parameter identification and aggregation and to obtain the highest rating in less number of iterations. This is based on the "Rating through Voting" algorithm [1]. The below algorithm can be applied not only to conference scenario but also scenarios like LinkedIn recommendations where the recommendations are treated as feedback provided by the recommender to the person being recommended and trust worthiness[9] factor can be treated as the sentiment of the community along with key parameters identified for recommender like experience, position in the company, skill level, experience of the person being recommended etc. This can also be applied to the book rating on Amazon if we are able to track their trustworthiness parameter's like how many more related books they have read and voted for, if their profession is the same as the book category etc. This can also be applied to any general election scenario where we have a list of people/products to be voted on and we have group or online systems or social networking sites where people can provide their feedback in the form of votes[10]. Parameters associated with people can be tracked through academic or professional search engines. In such cases the below algorithm can be used to identify the best voted person/product.

3. Related Work

In this section, we review four lines of research related to our work (i) rating through robust voting, (ii) social feeding ranking and engagement based algorithms, (iii)truth discovery and crowd sourced label aggregation and (iv) collusion-resistant reputation and ranking

3.1. Rating through Robust Voting

The Rating through Voting approach[1,13] addresses unfair manipulation in online rating systems by combining voting data with behavioural analysis. Reviewers' actions are modeled as feature vectors, and a fuzzy inference mechanism is used to compute trust scores. This enables the system to detect coordinated attacks and unfair evaluations. While effective, the method focuses mainly on behavioural features without incorporating external voter attributes such as expertise or credibility.Our work is inspired by this iterative re-weighting paradigm, but differs in that (i) we treat voter attributes (e.g., citation counts, institutional publication records) as first-class parameters, and (ii) we explicitly target academic and professional ranking scenarios rather than generic product reviews.

3.2. Social Feeding Ranking and Engagement based Algorithms

Facebook EdgeRank algorithms assigns scores to edges in a social graph based on affinity, edge weight and time decay , and uses these scores to rank content in the News feed[7]. Similar engagement-driven ranking models exist in other social media systems. While effective for personalisation, these methods largely optimize visibility and user engagement, not robustness to collusion. Consequently, they do not incorporate explicit notions of trustworthiness or multi-parameter expertise, and are therefore not directly suitable for our conference ranking and professional recommendation scenarios. Reddit's ranking algorithm, which combines up-votes, down votes and a time-decay factor via a logarithmic function, is another widely cited voting-based ranking baseline[4]. As with EdgeRank, Reddit's design trades off popularity and recency but does not explicitly estimate voter reliability, making it vulnerable to orchestrated voting campaigns[11].

3.3. Truth Discovery and Crowd Sourced Label Aggregation

The truth discovery literature is highly relevant to our setting because it also aims to infer trustworthy aggregated outcomes from noisy or even adversarial sources. Yin et al. introduced the problem of "truth discovery with multiple conflicting information providers" and proposed an iterative method that alternates between estimating the veracity of claims and the reliability of sources [14]. Their work established the idea that majority voting is insufficient when sources have different reliability.

Li et al. provide a comprehensive survey of truth discovery methods, covering web data integration, crowdsourcing and sensor networks, and categorise algorithms by how they model source reliability, object difficulty and data dynamics [15]. More recent work address dynamic truth discovery on numerical data and privacy-preserving truth discovery in distributed settings [18].

Wu et al. Propose label-confidence clustering for crowdsourcing, which groups workers according to confidence patterns and then infers task labels and worker reliability jointly[16]. In follow-up work, Wu et al. introduce a reliability driven multi view graph embedding framework that models multiple aspects of worker-task interaction and derives robust truth estimates[17]. These methods use sophisticated probabilistic or embedding models to infer worker reliability, but they typically treat worker quality as latent and do not exploit rich, externally available attributes like academic records.

Our VMPA algorithm can be viewed as complementary design choice: instead of inferring reliability only from label patterns, we construct multi-dimensional trust features from observable academic parameters (citation counts, publication history, institutional output) and integrate them into an iterative voting scheme. This makes VMPA particularly suitable in domains—such as academic conference ranking—where high-quality external signals about voter expertise are available.

3.4. Collusion-Resistant Reputation and Ranking

Collusion and spam in online rating systems are widely studied in both conference and journal venues. Early work on opinion spam and spammer detection focuses on identifying fake reviews at the content or reviewer level.Later work analyses fake reviewer groups and black-market driven collusion, showing the collusive groups can dominate ratings even in large platforms[21]. In the context of reputation and ranking, group level and reputation independent ranking systems remain robust under strategic manuplation. For example, Saúde et al. introduce a robust reputation-based group ranking system and study its resilience under several attack models [20]. Knowledge and Information Systems (KAIS) has also published multi-dimensional trust models that explicitly evaluate robustness to collusion in service recommendation scenarios, e.g., CA Trust, which uses context-aware multi-dimension trust and filters dishonest recommendations in highly hostile environments [19].

Our work is aligned with this line of research in aiming for collusion-resistant aggregation. However, VMPA differs along two axes (i) we operate directly on voting/rating matrices rather than network-structured interactions and (ii) we design the trust weight as an aggregation of multiple observable parameters per voter instead of a single latent reputational value. This design allows us to simultaneously use community sentiment(iterative voting over rating lists) and multi-parameter expertise signals (academic attributes) to seperate honest voters from colluders.

3.5. Recent Advances

Recent studies propose more robust frameworks. Chu & Laoutaris extend quadratic voting into federated learning, emphasizing trust-weighted budgets [1]. Kavner et al. analyze multi-issue iterative voting under uncertainty, demonstrating improved convergence [2]. Similarly, blockchain-based e-voting systems introduce verifiability and privacy-preserving designs [3–5]. Bai et al show how estimated trust weights affect the stability of weighted majority voting [6]. These works highlight the growing demand for resilient, trust-aware voting algorithms.

4. Voting - Multi Parameter Aggregation

There are 3 types of colluders. 1) Individual 2) group of colluders 3) biased voters. This algorithm is efficient in finding all the three colluder groups. This will also ensure the voting given by trustworthy random voters is considered to ensure their genuine votes are not lost. Input to this method is the list of conferences, list of voters and voting given as feedback from voters to the list of conferences. This method has 3 components 1. Multi-Parameter Identification.2. Rating Algorithm 3. Trustworthiness calculation. Output is the rating scores which show the top ranked conference in spite of collusion and biased rating by group of colluders.

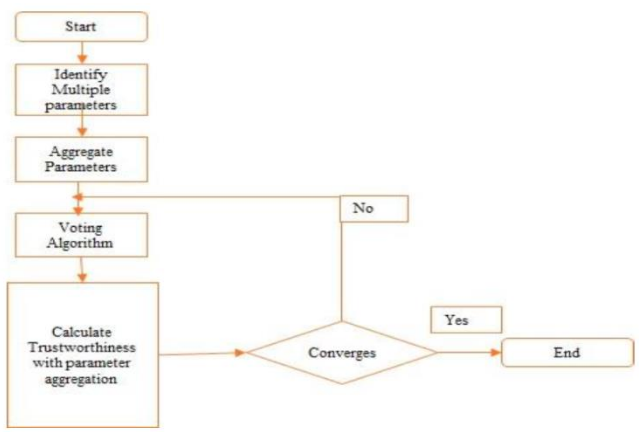

Fig. 1. Overview of Iterative Voting- Multi Parameter Aggregation Framework

4.1. Multi Parameter Identification and Aggregation(MLPA)

Identification of Multiple Parameters can improve the trust worthiness, an important factor in this method. In case of conference ranking we have considered Program Committee members as voters and taken their key associated parameters like citation count in the last 4 years (number of times their articles are being referenced in the last 4 years), Publication Count (total number of publications published in the last 4 years), Journal Count (total number of Journals published in the last 4 years), University Publication count in the last 4 years. University Journal count in the last 4 years. In this case we are considering 4 years of data. We are giving equal preference to all the voters. Also, we are considering that the voters should have at least 5 years of experience. Once the parameters are identified and data collected, the values should be aggregated by diving the value/average mean of the values and then summing up all the values. For colluders it is not possible to get valid data for their parameters or the data obtained might be faulty data we assign 0.01 as their parameter weight.

4.2. Voting with Multi-Parameter Aggregation(VMPA)

Once the parameters are aggregated we calculate the trust worthiness factor with Voting Algorithm. The Voting Algorithm calculates 1) scores of each of the voting item on the list 2) Trust worthiness factor which emphasis how reliable the scores are from the genuine voters as compared to the colluders. Below is Iterative voting algorithm that calculates the aggregation of identified parameters, calculate the score of each individual Voting product/person’s score by normalizing the values. Iterates until the algorithm converges. Convergence criteria is taken as the difference between iterations $<\varepsilon$, where ε is a threshold corresponding to some “reasonable” desired accuracy for the particular application

Some notation for the algorithm:

- nVotingLists = number of Voting lists
- nVotingItems = Items/Persons on the voting lists
- nTotalVoters = Total Number of Voters on lists
- hGroups = number of honest voters groups
- nHonestVoters = total number of honest voters
- nColluders = total number of colluding attackers
- nTotalVoters = NHonestVoters + nColluders
- VW = Voting weight for the list of parameters identified for the honest voters
- AWPM = Average Weight or Mean of values
- AWP = Average Weight of Parameter = Parameter Value / Average Mean of values
- P= Number of Iterations until the algorithm converges

Algorithm – Voting – Multi Parameter Aggregation

//Calculate the aggregation or sum of all parameter values based on their mean.

$$AWPM1 = Round[\sum_{l=1}^{nHonestVoters} VW[[l,1]]/nHonestVoters\ ,.1];$$

//Repeat for all parameters

$$Do[AWP[tt] += Round[VW[[tt,1]]/AWPM1\ ,.1], \{tt, 1, nHonestVoters\}];$$

//Assign 0.01 to all colluders as getting their parameters is not possible or faulty

$$Do[AWP[tt] = 0.01, \{tt, 16, 60\}];$$

//Caluclate scores and Trustworthiness with voting algorithm

$$TW[v_{,0}] := 1;$$

$$TW[v\_, p\_] := TW[v,p] = N[\sum_{l=1}^{nVotingLists} r[VW[l][[v]], l, p-1]] + AWP[v];$$

$$rr[j\_, l\_, p\_] := rr[j,l,p] = N[\sum_{v=1}^{nTotalVoters} TW[v,p]^{kPower}(1 - Sign[Abs[VW[l][[v]] - j]])];$$

$$r[j\_, l\_, p\_] := r[j,l,p] = \frac{rr[j,l,p]}{\sqrt{\sum_{m=1}^{iVotingItems} rr[m,l,p]^2}};$$

//For the algorithm to converge iterate until it converges or the difference between the iterations < ε

$$While[Max[Table[Abs[r[j,l,p+1] - r[j,l,p]], \{j, 1, iVotingItems\}, \{l, 1, nVotingLists\}]] > 10^{-3}, p++]$$

The below diagram shows how initially genuine voters vote for a genuine product/person and colluders vote for a faulty product/person. But after the iterative algorithm has been applied the genuine voter's choice for genuine product/person stands out.

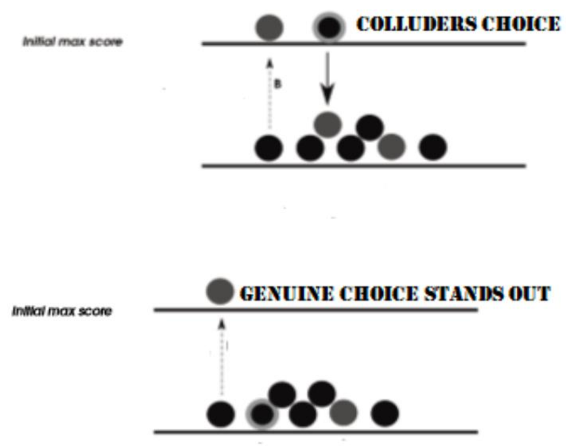

Fig. 2. After Iterative algorithm has been applied the genuine voter's choice stands out

5. Experiments and Results

To conceptualise our results, we discuss how VMPA relates to standard baselines used in truth discovery and collusion resistant ranking, even though our primary experiments focus on the robustness of VMPA itself.

1. Majority Voting(MV): Each conference's rank is determined by simple majority across voters, without weighting. MV is the most widely used baseline in truth discovery and label aggregation because of its simplicity, but it fails when colluders are in the majority[14][15].
2. Unweighted Iterative Rating through Voting(RTV): This is the original Rating through Voting algorithm that updates voter trustworthiness and item ratings iteratively, but does not incorporate external parameters such as citation counts or institutional statistics.
3. Single Parameter Truth discovery(TD-SP): Methods such as the Truth discovery framework of Yin et al maintain a single reliability weight per source and iteratively re-estimate source reliability and item truth[14]. When applied to our setting, each program committe member would have one latent reliability score ,independent of their academic profile.

In contrast, VMPA initialises each voter with a multi-parameter aggregate weight derived from measurable academic indicators(citation count, publication volume, journal activity, and institutional output), and then refines the effective influence of each voter through iterative trustworthiness updates coupled to community sentiment. As shown in Scenarios 1 and 2, even when colluders are three times as many as honest voters, VMPA recovers the genuine top conference(C1) and assigns substantially lower trustworthiness to colluders.

Three main aspects of this model/algorithm are

1. Random Genuine Voter's voting should not be lost.
2. High Trustworthiness
3. Less number of Iterations.

Scenario1:

We use genuine voting data

Let's consider the dataset given below. In this scenario we are ranking a group of conferences identified in a particular subject area.

Election/Voter			V1,	V2,	V3,	V4,	V5
E	[1]	=	{1,	2,	1,	2,	2}
E	[2]	=	{2,	1,	2,	3,	2}
E	[3]	=	{2,	4,	4,	4,	2}
E	[4]	=	{1,	3,	3,	3,	1}
E	[5]	=	{2,	1,	1,	1,	1}
E	[6]	=	{1,	2,	1,	1,	1}

E [7] = {1, 1, 1, 1, 1}

In the first scenario, we analyzed a dataset representing genuine voting behavior. Five voters (V1-V5) participated in seven elections (E1-E7) to evaluate five conferences (C1-C5). The dataset reflects varied outcomes across the elections. For instance, in E1, voters V1 and V3 supported C1, while voters V2, V4, and V5 favoured C2. By contrast, in the final election (E7), all voters unanimously selected C1, indicating a strong consensus. This scenario demonstrates how community sentiment evolves across multiple voting rounds and highlights the importance of preserving the contributions of genuine voters, even when they participate infrequently.

Scenario 2:

In this experiment, a synthetic dataset was constructed consisting of 60 voters participating in 7 elections, each election including 10 conferences (C1-C10). Among these, the first 15 participants were modeled as honest voters, consistently providing fair evaluations. These voters and their ballots were generated by replicating the profiles of voters V1-V5 three times, yielding the set V1-V15. In contrast, the remaining 45 participants were designated as unfair voters, each casting a random vote on a single item in every election except the final round. Thus, the number of colluding voters was deliberately set at three times the number of honest ones. In the 7th election, the colluders coordinated their votes to favour conference C5, whereas all honest voters supported C1. Under a simple majority voting scheme, C5 would inevitably emerge as the winner, since its votes outnumber those of its genuine competitor C1 by a factor of three.

In both the scenarios in this method or algorithm we have identified parameters for the Voters (Program Committee members who voted for these conferences. The Identified parameters are Citation Count, Publication Count, Journal Count, University Publication count, University Journal Count.These parameters are identified from Microsoft Research website for anonymous program committee members. These parameters are identified and aggregated and the aggregated value is added to the voting algorithm to improve the performance of algorithm and also trustworthiness factor. Below is the parameter dataset.

Identified for the 15 honest voters (program committee members who have voted for the conference).

{{20,10,12,700,140},{15,35,9,500,170},{45,12,23,680,230},{10,22,6,220,156},{20,10,10,230,98},{30,20,789,300,100},{20,10,10,270,198},{20,10,12,980,150},{20,10,12,290,140},{20,10,11,220,140},{20,10,18,190,140},{20,10,30,780,140},{20,10,40,545,140},{20,26,12,670,140},{20,9,12,560,140}};

We calculate the aggregate of these scores for each Voter = Sum (P1/AP1+…..PN/APN) where P1 is the parameter value and AP1 is the average mean of parameter 1 value and finally calculate their sum. These can be taken as a trustworthiness factor of each voter although he/she should still vote to the sentiment of the community. This factor will ensure the random genuine voters are not lost. All the colluders are assigned 0.01 value.

Following are the results obtained from above data set after calculation

{4.2,5.4,6.2,3.7,2.9,15.9,3.6,4.9,3.3,3.2,3.2,4.5,4.2,5.2,3.8,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01,0.01}

In the initialization process of the voting algorithm with the aggregated parameters, item C1, having obtained 15 votes, gets the initial ranking score ≈ 0.42; on the other hand, item C5 gets an initial score of ≈ .94. However, after we run our algorithm, the scores are essentially reversed and C1 wins the election, as we would expect from a robust voting system. Below table shows the ranks produced by our algorithm in Scenario1

Scenario1:

Table. 1. Ranks produced by Iterative voting algorithm in Scenario 1

	C1	**C2**	**C3**	**C4**	**C5**
E1	0.814	0.580	0	0	0
E2	0.172	0.667	0.180	0	0

E3	0	0.728	0	0.686	0
E4	0.728	0	0.686	0	0
E5	0.862	0.507	0	0	0
E6	0.989	0.147	0	0	0
E7	1	0	0	0	0

A high trustworthiness rank will be given only to voters who often chose candidates favoured by many other members of the community, thus voting in accordance with the prevailing sentiment. Such voters can be considered as “reliable voters”, choosing candidates in accordance with the sentiment. But the ranks should be based not only on the sentiment but should be based on other parameters which emphasize the trustworthiness factor of the voters. Now we recalculate the ranks of items thus each received vote is now worth the present trustworthiness rank of the voter giving such a vote. We continue such iterations until the ranks stop changing significantly, ie., we stop when difference between iterations <ε, where ε is a threshold corresponding to some “reasonable” desired accuracy for the particular application; in our experiments it was in the range 10−3 − 10−6 with the algorithm terminating after 5 − 11 iterations.

Scenario2:

Table. 2. Ranks produced by Iterative voting algorithm in Scenario 2

	C1	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**C8**	**C9**	**C10**
E1	0.810	0.581	0.003	0.002	0.00	0.001	0.002	0.005	0	0.08
E2	0.172	0.967	0.186	0	0.03	0.02	0.01	0.01	0.01	0
E3	0.02	0.725	0.02	0.688	0.04	0.02	0.06	0.01	0.01	0
E4	0.732	0	0.680	0.003	0	0.01	0.002	0.002	0.003	0.009
E5	0.858	0.512	3.07E	0.007	0.003	0.002	4.49E	0	0.005	0.002
E6	0.988	0.147	0.001	0.002	0.001	0.001	0.006	0.006	0.003	0.001
E7	1	0	0	0	0.286	0	0	0	0	0

Observed Results:

Our experiments show that as the number of elections increases the sentiment of the community increases which in turn increases the trustworthiness factor. Similarly as the number of parameters of voters increases the Trustworthiness factor increases. Also, the colluders are identified with a clear distinction between the values of honest voters and colluders. Below are the minimum trustworthiness factors obtained for the honest voter and maximum trustworthiness factor obtained for colluder.
{7.74, 3.79}

There is a significant difference in value between the least trustworthy honest voter and most trustworthy colluder which clearly differentiates that the values provided are genuine. Also, the number of iterations in which the difference between the iterations <ε is close to 5 if the range is

10−3 and 11 if the range is 10−6. With the increase in number of parameters and the increase in the number of elections these iterations further reduce which improves the efficiency of the algorithm.

6. CONCLUSION

This paper presented an Iterative Voting Algorithm with Multi-Parameter Aggregation (VMPA). By incorporating community sentiment with measurable voter parameters, the algorithm effectively resists collusion, preserves genuine but infrequent voters, and converges quickly. Recent advances in quadratic voting, blockchain-enhanced e-voting, and stability analyses of weighted voting align with our approach and suggest pathways for extending the model. Future work will explore integrating item-level attributes (e.g., credibility of candidates or products) for two-sided trust modeling. Beyond the current experiments, VMPA can be seen as a specialisation of truth discovery and crowdsourced label aggregation methods to domains with rich side information on voters.They can also be extended to social media platforms, product reviews, or larger academic settings. Our results suggest that explicitly encoding multi-parameter voter attributes into an iterative voting scheme yields a simple yet effective mechanism for academic and professional ranking tasks. An interesting direction for future work is to integrate VMPA with recent graph-embedding-based truth inference models and to evaluate it on large-scale datasets derived from citation networks and professional platforms.

REFERENCES

[1] Tianyue Chu, Nikolaos Laoutaris. FedQV: Leveraging Quadratic Voting in Federated Learning. arXiv preprint, 2024

[2] Joshua Kavner, Reshef Meir, Francesca Rossi, Lirong Xia. Convergence of Multi-Issue Iterative Voting under Uncertainty. IJCAI, 2023.

[3] Daniel Rausch, Nicolas Huber, Ralf Küsters. Verifiable E-Voting with a Trustless Bulletin Board. Cryptology ePrint Archive, Paper 2025/841.

[4] G. Somasekhar, S. Jinka, C. Kanekal, A. Marouthu. Digital Voting with Blockchain using IPFS and pBFT. ETASR, 2024.

[5] "An Efficient and Versatile E-Voting Scheme on Blockchain." Cybersecurity, Springer, 2024.

[6] Shaojie Bai, et al. Stability of Weighted Majority Voting under Estimated Weights. arXiv preprint, 2022.

[7] Facebook News Feed Ranking. http://edgerank.net/

[8] Guofei Gu. Computer Security Conference Ranking and Statistic Ranking.

[9] R. Falcone, C. Castelfranchi. Social Trust: A Cognitive Approach. In Y.-H. Tan (Ed.), Trust and Deception in Virtual Societies.

[10] E.-P. Lim, V.-A. Nguyen, N. Jindal, B. Liu, H. W. Lauw. Detecting Product Review Spammers Using Rating Behaviors. CIKM '10, ACM.

[11] R.S. Boyer, J.S. Moore. A Fast Majority Algorithm.

[12] Michael Taylor, Hugo Zaragoza, Nick Creswell. Optimization Methods for Ranking Functions with Multiple Parameters.

[13] Mohammad Allahbakhsh, Aleksandar Ignjatovic. Robust Evaluation of Products and Reviewers in Social Rating Systems.

[14] X. Yin, J. Han, and P. S. Yu, "Truth Discovery with Multiple Conflicting Information Providers on the Web," IEEE Transactions on Knowledge and Data Engineering (TKDE), 2008.

[15] Y. Li, J. Gao, C. Meng, Q. Li, and J. Han, "A Survey on Truth Discovery: Concepts, Methods, and Applications," ACM SIGKDD Explorations, 2016

[16] G. Wu, L. Zhou, J. Xia, et al., "Crowdsourcing Truth Inference Based on Label Confidence Clustering," ACM Transactions on Knowledge Discovery from Data (TKDD), 2023.

[17] G. Wu, X. Zhuo, X. Bao, et al., "Crowdsourcing Truth Inference via Reliability-Driven Multi-View Graph Embedding," ACM Transactions on Knowledge Discovery from Data (TKDD), 2023.

[18] S. Zhi, F. Yang, Z. Zhu, Q. Li, Z. Wang, and J. Han, "Dynamic Truth Discovery on Numerical Data," in Proc. IEEE International Conference on Data Mining (ICDM), 2018.
[19] C. Miao, Y. Liu, Z. Shen, et al., "Multi-Dimensional Trust for Context-Aware Services Computing," Knowledge and Information Systems (KAIS), 2021.
[20] J. Saúde, F. Neves, and B. Ribeiro, "A Robust Reputation-Based Group Ranking System and Its Applications," ACM Transactions on Knowledge Discovery from Data (TKDD), 2022.
[21] H. S. Dutta, S. Chakraborty, A. Goyal, and A. Goyal, "Blackmarket-Driven Collusion on Online Media: A Survey," ACM Transactions on Knowledge Discovery from Data (TKDD), 2022.

AUTHORS

Manjula Pilaka is a Professor of Practice at BVRIT Hyderabad College of Engineering for Women. She completed her MPhil in Computer Science and Engineering at University of New South Wales and an MBA from Indian Institute of Management(IIM), India. She worked in Industry for 25 years in various roles in Australia, USA, UK and India.

Dr K V N Sunitha is a Professor and Principal at BVRIT College of Engineering for Women. She completed her PhD in Computer Science and Engineering at Jawaharlal Nehru Technological University. She completed her MTech in Computer Science and Engineering from NIT Warangal. She has 33years of Teaching experience and 16 years of Research Experience

Dr Aruna Rao SL is a Professor and HoD of Department of Computer Science and Engineering Department at BVRIT College of Engineering for Women. She completed her PhD in Computer Science and Engineering from Jawaharlal Nehru Technological University. She completed her MTech in Network and Internet Engineering from VTU, Belgaum. She has 22 years of Teaching experience