Privacy-Preserving and Diversity-Aware Trust-based Team Formation in Online Social Networks

YASH MAHAJAN, JIN-HEE CHO, and ING-RAY CHEN, Virginia Tech, USA

As online social networks (OSNs) become more prevalent, a new paradigm for problem-solving through crowd-sourcing has emerged. By leveraging the OSN platforms, users can post a problem to be solved and then form a team to collaborate and solve the problem. A common concern in OSNs is how to form effective collaborative teams, as various tasks are completed through online collaborative networks. A team's diversity in expertise has received high attention to producing high team performance in developing team formation (TF) algorithms. However, the effect of team diversity on performance under different types of tasks has not been extensively studied. Another important issue is how to balance the need to preserve individuals' privacy with the need to maximize performance through active collaboration, as these two goals may conflict with each other. This research has not been actively studied in the literature. In this work, we develop a team formation (TF) algorithm in the context of OSNs that can maximize team performance and preserve team members' privacy under different types of tasks. Our proposed PRivAcy-Diversity-Aware Team Formation framework, called `PRADA-TF`, is based on trust relationships between users in OSNs where trust is measured based on a user's expertise and privacy preference levels. The PRADA-TF algorithm considers the team members' domain expertise, privacy preferences, and the team's expertise diversity in the process of team formation. Our approach employs game-theoretic principles *Mechanism Design* to motivate self-interested individuals within a team formation context, positioning the mechanism designer as the pivotal team leader responsible for assembling the team. We use two real-world datasets (i.e., Netscience and IMDb) to generate different semi-synthetic datasets for constructing trust networks using a belief model (i.e., Subjective Logic) and identifying trustworthy users as candidate team members. We evaluate the effectiveness of our proposed `PRADA-TF` scheme in four variants against three baseline methods in the literature. Our analysis focuses on three performance metrics for studying OSNs: social welfare, privacy loss, and team diversity.

Additional Key Words and Phrases: Team formation, online social networks, privacy-preserving, diversity, trust

ACM Reference Format:
Yash Mahajan, Jin-Hee Cho, and Ing-Ray Chen. 2024. Privacy-Preserving and Diversity-Aware Trust-based Team Formation in Online Social Networks. 1, 1 (April 2024), 25 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

1.1 Motivation

As online social networks (OSNs) or social media systems become prevalent, a new problem-solving paradigm by crowd-sourcing emerges. In the OSN platforms, users can post a problem, and then other members form a team to collaborate and solve the problem. For example, to complete a Human Intelligence Task (HIT) based on crowd-sourcing, such as Amazon Mechanical Turk, it is critical to form a team of people with relevant skills and knowledge. When a task requires experts in multiple domains to collaboratively solve the problem, how to form a team is a critical component that can affect team productivity and performance.

Authors' address: Yash Mahajan, yashmahajan@vt.edu; Jin-Hee Cho, jicho@vt.edu; Ing-Ray Chen, irchen@vt.edu, Virginia Tech, 7054 Haycock Rd, Falls Church, Virginia, USA, 22043.

Manuscript submitted to ACM

Our work is motivated by the need of many OSNs (examples to be given below), where a team consisting of diverse team members with different expertise in various domain areas is needed to solve a problem collaboratively. A major problem is that OSN users are not employees of a particular enterprise or company. Rather, they are just members of the OSN, each with their own objective (e.g., monetary gain or social welfare [1] gain) to stay in the OSN community. This is an intricate problem because, on the one hand, the OSN administrator must recruit members with diverse expertise to solve problems for the prosperity and growth of the OSN. On the other hand, it must incentivize participating members, knowing that individual members have their own objectives.

We list three OSN examples to illustrate how useful our proposed framework is. The first example of *Amazon Mechanical Turk* OSN would allow users to post a Human Intelligence Task (HIT), and workers receive a reward or payoff when completing the posted HIT. The second example is a *Multidisciplinary Co-authorship Collaboration* OSN. This allows a user to post a multidisciplinary problem, and the OSN administrator shall select qualified members to solve the problem in the form of an article co-authored by the selected members. The third example is a *Social Bookmarking* OSN for a posted multi-domain problem, and the OSN administrator shall select qualified users to collect, organize, share, and discover online resources related to the posted problem. Motivated by the three examples OSNs above, we propose to leverage trust to select a team formation that achieves high performance in terms of performance metrics defined by the OSN administrator, such as high social welfare and low privacy loss to OSN members and high team diversity.

Given a task T, a set of required domain expertise, and the number of required team members, we aim to form a team to maximize the team's performance based on the sum of individual members' utilities to the team. Many social scientists have shown that team productivity and successful task completion are closely related to the composition of a team in terms of relevancy and diversity of skill sets, team coherence, trust among members, information sharing, or shared mental model [33, 44]. However, depending on the nature of the task, the team may require diverse expertise or focus on high expertise in a single domain.

Diversity has been identified as one of the critical elements of team formation for generating high-quality solutions to somewhat complicated problems. Such problems may require creative and innovative thought processes with diverse domain expertise. Various thoughts or multidisciplinary approaches are known to be very creative and novel and bring more productive and beneficial outcomes in solving highly complicated problems, compared to methods relying on homogeneous, single discipline-based expertise [52]. Many researchers have scientifically and empirically proven the positive effect of high diversity on team or organization productivity [51]. However, in our real-world settings, high team diversity does not necessarily always produce high productivity due to the different natures of an assigned task [45, 63]. To the best of our knowledge, few studies have investigated such issues.

When collaborating with other team members, a member may care about how much she/he can preserve privacy while still contributing to the team's productivity. The primary reason is that collaboration often involves sharing sensitive information, which a malicious team member could use to perform targeted attacks. For instance, in the *Multidisciplinary Co-authorship Collaboration* OSN discussed earlier, a team member may share the technical details of an ongoing government-funded research project. However, this information used to solve a part of the multidisciplinary problem may not be disseminated without government approval. If a malicious member of the team was to spread misinformation, it could affect the individual's credibility and reputation. Privacy loss minimization techniques have been studied as a distributed constraint satisfaction (DCS) problem [23, 58] to preserve perfect privacy without trusting anyone in interactions while minimizing interactions. However, since minimizing privacy loss normally leads to less information

[1] In the context of 'Mechanism Design' within game theory, 'social welfare' is defined as the aggregate of the utilities of all individual players [59].

sharing, it may not be possible to achieve maximum team productivity that often requires more information sharing. In particular, it would be hard to complete a task that requires diverse expertise if there is less information sharing due to minimizing privacy loss. The relationship between privacy loss and team performance has been examined [26]. However, little work has studied how information sharing in a team affects team performance and privacy loss when the team is assigned to complete a task requiring expertise levels in multiple, diverse domains.

1.2 Research Goal & Contributions

This work proposes a framework PRivAcy-Diversity-Aware Team Formation, called PRADA-TF. PRADA-TF can be applied in an OSN where team members are selected based on trust relationships between them. Trust can be estimated based on their privacy preferences and expertise levels. PRADA-TF offers a mechanism design (MD)-based team formation algorithm that effectively considers the required level of team expertise and the privacy preservation preferences of team members. In addition, it identifies the optimal settings of key design parameters that maximize team productivity while maintaining a balanced level of team diversity, information sharing, and members' privacy preferences.

Our work makes the following **key contributions**:

(1) In our work, we introduce PRADA-TF, a game-theoretic strategy rooted in *Mechanism Design* (MD) [46], tailored for solving team formation issues. The MD framework was selected to orchestrate a strategic game involving a mechanism designer (i.e., a centralized authority) and numerous cooperative agents, potentially with divergent goals. This framework ensures that each participant, driven by the principle of individual rationality – where every entity is assumed to act in their best interest to maximize their utility [59] – can collectively reach their objectives. Through the application of MD, PRADA-TF delves into the impact of team diversity and the privacy preferences of team members on performance across a variety of collaborative endeavors within Online Social Networks (OSNs).

(2) We leverage a belief theory called *Subjective Logic*, which offers the capability of deriving trust relationships between two users with no direct relationships to select a set of team members as promising candidates. Although trust has been considered in various domains, we found little work considering prior trust relationships in the context of TF in the OSN, where the game-theoretic MD is used to form a team based on team diversity and privacy.

(3) Unlike any other approaches in the TF research, we consider two scenarios – 'expected' and 'actual' when executing any given task. In the 'actual' task execution, a team member's behavior is modeled based on the player's privacy preference revelation (see Section 5.4). Modeling this real-world scenario provides insightful details about the 'actual' performance of the team regarding social welfare and potential privacy loss, which is first studied in this work.

(4) Based on the generated trust network, we consider possible private information loss due to other team members' distrust (or dishonesty). This potential privacy loss directly affects team members' behaviors by affecting team performance and indicates trust in the team.

(5) We create two semi-synthetic datasets resembling two separate OSNs to test the feasibility of our approach based on real-world *Netscience* [49] dataset and *IMDb* [8] dataset. These two datasets, each containing thousands of members, realistically simulate a *Multidisciplinary Co-authorship Collaboration* OSN and an *artist* OSN following the paradigm of problem-solving by crowd-sourcing.

(6) We conduct an extensive experiment for the in-depth comparative performance analysis of the seven TF schemes consisting of four variants of our proposed PRADA-TF scheme and three state-of-the-art baseline schemes. We discuss the key findings of their performance in terms of potential private loss, actual/expected social welfare, team diversity, and asymptotic time complexity in Big-O notation.

The preliminary research of this work has been published in our prior work [40]. In [40], we proposed a team formation (TF) algorithm in the context of OSNs that can maximize team performance and preserve team members' privacy under different types of tasks. The present paper substantially extends [40] by providing the following **additional contributions**: (1) We substantially extended the discussions of the related state-of-the-art approaches and clarified the key differences between our work and the existing counterparts. (2) We provided the details of how a belief model (i.e., Subjective Logic, or namely SL) is used for the team leader (i.e., a mechanism designer) to select team members based on two operators provided by the SL (i.e., discounting and consensus operators [27]). This offers the estimation of trust between the team leader and candidate team members based on the expertise and privacy preference levels in a given OSN. (3) We conducted the algorithmic complexity analysis of the seven TF schemes, including our schemes and other counterparts, based on Big-*O* asymptotic time complexity analysis and simulation running time in Section 7.5. A TF problem is known as an NP-Hard problem [31]. Hence, this analysis can deliver insights into how the proposed heuristic approach can achieve at least acceptable complexity for its use in practice. (4) We conducted an in-depth sensitivity analysis to investigate the outperformance of the proposed PRADA-TF over other competitive counterparts by varying the values of the following key design parameters: (a) a different type of tasks requiring diverse skill sets and domain expertise; (b) a different level of the team members' privacy preferences; and (c) a different team size (i.e., the number of team members). These are addressed in Sections 7.1–7.3.

The rest of the paper is structured as follows. Section 2 provides an overview of the related literature. Section 3 describes the example scenario and the task, information, and adversarial models considered in this work. Section 4 describes the objective function of the problem we aim to solve. Section 5 provides the details of the proposed team formation approach based on the mechanism design and trust network modeled by a belief model called Subjective Logic. Section 6 gives the detailed experimental settings for the conducted experiments. Section 7 demonstrates numerical results and provides underlying reasons for the in-depth performance analysis of the compared schemes. Section 8 concludes the paper with key findings.

2 RELATED WORK

In this section, we discuss the overview of the existing related work, including collaborative team formation, team diversity, privacy-preserving in multi-agent systems, and trust-based applications for OSNs.

2.1 Collaborative Team Formation

Team formation (TF) research has proposed many approaches using various team member selection criteria, including domain expertise [32], cost of communications between team members [1, 32] or between team members and a leader [29], skill sets [1, 32], or fair workload among members [1]. In addition, a TF problem has been studied in social networks [9, 17, 66] in that close social relationships and homophily of team members can reduce communication costs but may not be desirable to derive novel ideas [9]. In addition, a game theory based on *Mechanism Design* (MD) is leveraged to solve the TF problem. In MD, a centralized entity called a *mechanism designer* aims to maximize the sum of all participating agents' utilities, known as *social welfare*. Each agent has its own utility function to maximize. The first formal MD framework for TF was presented [68] with the analysis of incentive compatibility, social welfare, and fairness. Liu et al. [39] solved a TF problem in a crowdsourcing market using the *pricing mechanism design* whereas Wang et al. [65] took a game-theoretic approach and modeled each worker in crowdsourcing as a selfish entity who did not necessarily cooperate with the request to join a social crowdsourcing team. However, little work has considered team diversity and privacy issues in TF problems, which are addressed in this work.

2.2 Team Diversity

Diversity is a subjective phenomenon created by group members based on the dissimilarity (or similarity) of social identities. The diversity in the workplace was investigated by an individual's visible (e.g., age, race, sex), non-visible (e.g., attitude or knowledge), and discretion (e.g., sexual orientation or hidden disability). In addition, diversity in team members' personality traits can impact team performance [2]. Gomez and Bernet [20], Pieterse et al. [54], van Veelen and Ufkes [64] reported the positive effect of cultural diversity on team performance. Moreover, Tasheva and Hillman [61] argued that individual-level diversity and team-level diversity are not independent. Ely and Thomas [15] found that the benefits of cognitive diversity can be seen in complex problem-solving rather than in performance. Cohen and Yashinski [6] showed that finding an optimal diverse team of people is an NP-Complete problem. Marcolinon et al. [41] studied how the team's diversity can beat the team's high expertise in team performance.

Most team diversity research has been conducted in the social sciences, while a few studies [6, 41] have theoretically examined how the diversity of team members can affect team performance in terms of the mechanism design perspective in game theory, which is studied in our work.

2.3 Privacy Preservation

Many studies proved that information sharing is an apparent driving force leading to high team performance and success [43, 67]. However, the adverse impact of information sharing via close interactions among team members has not been sufficiently explored. Privacy loss or minimization problems have been studied in distributed constraint satisfaction (DCS) problems [23, 58]. In the DCS problems, distributed negotiation or cooperation is studied while preserving perfect privacy by not trusting anyone in interactions. Both works [23, 58] showed a tradeoff between privacy and efficiency.

Dwork [13] first introduced a mechanism design-based ϵ-differential privacy (DP) to ensure a person's privacy cannot be compromised with the release of their data if the data is not present in the database. DP was extended to provide game-theoretic guarantees [42], including approximate truthfulness, collusion resistance, and repeatable play. External incentives are necessary for individuals to participate and report truthfully [50, 69]. There was a privacy-aware mechanism design model of efficient results [50] while highlighting how ignoring privacy awareness in the design of mechanisms may render it not incentive compatible. Xiao et al. [69] introduced a transformation of a truthful mechanism into a deferentially private mechanism that remains truthful based on the ideas for privately releasing histogram data. [24, 70] proposed a privacy-preserving framework in the context of crowdsourcing by using blockchain technology. However, mechanism design-based privacy research has not solved TF problems.

Du et al. [11] explored the application of game theory to user interactions and decision-making processes regarding privacy protection in SNs. This study underscored the critical role of incentive mechanisms, community influence, and evolutionary dynamics in shaping user privacy behavior. Concurrently, Du et al. [12] delved into the necessity of safeguarding privacy-sensitive information within Internet of Things (IoT) applications. It addresses this through the lens of privacy-conscious data analysis, secure data exchange, and trustworthy data aggregation. The paper elaborates on utilizing distributed Multi-Party Computation (MPC), auctions, and contractual agreements to mitigate security risks while advocating for continuous enhancements in IoT security frameworks, protocols, cryptographic methods, and privacy-preserving data management strategies.

Based on the literature review above, TF problems with privacy preservation have not been sufficiently explored where the TF is also diversity-aware in team composition.

2.4 Trust-based Applications for OSNs

Trust plays an increasingly important role in decision-making in OSNs [4]. Lai and Turban [30] provided evidence from virtual social groups that users tend to trust other members by expertise, identity, and personal information. Tang et al. [60] used a measure of trust to share and exchange information and aggregate or filter data. Trust also contributed to exhibiting the risk-taking behavior by users participating in OSNs [22]. Due to the lack of interactions between the majority of the users on any OSN platform, predicting and establishing trust between any two users is a difficult task [19]. Various approaches have been presented for trust prediction based on the following three categories: graph-based trust models [37, 38, 57], interaction-based trust models [55], and hybrid trust models [18, 57]. Lin et al. [34] leveraged graph convolutional neural networks (GCNs) to propose *Guardian* to learn latent factors in social trusts with GCNs. Nasir and Kim [47] proposed a framework based on transpose trust propagation and co-citation to evaluate the trust and distrust between two unconnected users in a network. Lin and Li [35] proposed a framework to predict dynamic social trust, which varies over time.

The above works discussed mainly focused on establishing and predicting trust between users and building social groups or communities with high trust in OSNs to provide trustworthy services. However, our work focuses on how trust can be leveraged to select a team formation that achieves high performance in terms of the expected/actual social welfare, expected/actual potential privacy loss, and team diversity.

3 PRELIMINARIES

In this section, we describe the following: an example scenario mainly considered in this work, task model (i.e., attributes of an assigned task), information model (i.e., properties to explain the value of information for the information shared by team members), and adversarial model (i.e., what adversarial behaviors a team member may exhibit).

3.1 Example Scenario

We assume a scenario where a team must be formed in OSN platforms to successfully complete a sufficiently complicated task. Imagine an online crowdsourcing system like Amazon Mechanical Turk, where a requestor wants to form a team to execute a given task. We assume that the task requires fairly diverse skills or knowledge and collaboration across team members to complete successfully. Thus, selecting qualified team members is the key to success.

A team will consist of members with diverse levels of domain expertise and privacy preferences. Each member's privacy preference will affect communication patterns among team members, in which the contribution of information naturally leads to high team productivity. In an OSN, a team leader aims to gather promising candidate team members to achieve a particular task by reaching out to his/her friends or friends of friends. We assume that each user is a trustor who can estimate trust in his/her friends, as trustees, based on domain expertise or willingness to share information available to a trustor through direct or indirect experiences. Through the chain of trust relationships between users, the team leader can gather a set of promising candidates for team members and select a group based on specific criteria. We describe how to calculate a user's trust in another user and how the team leader collects a group of promising candidates and accordingly selects the final team members in Section 5.5.

3.2 Task Model

We consider a multi-domain, multidisciplinary task posted in the OSN that requires a team of OSN users who have expertise in the relevant domains or disciplines. Those team users can complete the task and maximize the benefits of

OSN in terms of the performance metrics defined by the OSN administrator. Such a task is general and can range from a Human Intelligence Task (HIT) posted in the Amazon Mechanical Turk OSN, a technical multidisciplinary problem posted in the Multidisciplinary Co-authorship Collaboration OSN, to an online resource collection task posted in the Social Bookmarking OSN.

A prospective team is given a complex task composed of the following fundamental components:

- *Team size (m)*: Any given prospective team consists of m team members. Hence, the team leader will select m number of members for the team he/she aims to form.
- *Required domain expertise (E)*: We model the required domain expertise for a given task as a set, represented by $E = \{e_1, e_2, \ldots, \ldots, e_l\}$, where e_h is the extent of expertise in the domain h required to complete the task with $l \leq m$. Note that e_h refers to a real number where $\sum_{e_h \in E} e_h = \epsilon$, meaning that the sum of all expertise levels equals ϵ. Note that each domain expertise level can be filled by multiple members' expertise levels in the domain. Thus, each domain expertise is not necessarily met by a single person.

We conduct sensitivity analysis of the considered TF algorithms' performance when varying m and $|E|$ and discuss their overall trends in Section 7.

3.3 Information Model

A team member's expertise preference (θ_i^e) and contribution to the team performance may introduce a different level of impact to the team performance. We model how valuable the contributed information is to the team performance [56] by the so-called *Value-of-Information (VoI)*, which is quantitatively measured by real numbers in $[0, 1]$ in terms of the following key components:

- *Credibility* (crd_{ih}) represents the degree of information credibility player i provides based on his/her expertise level in domain h.
- *Usefulness* (uf_{ih}) indicates the usefulness (or relevance) of the information player i provides where player i has a certain level of expertise in the domain h.
- *Novelty* (nov_{ih}) indicates the degree of novel ideas the information player i provides based on his/her expertise in domain h.

VoI characterizes how much each team member can contribute to team performance through the quality of information they provide. We identify three key factors that determine the quality of information: *credibility*, *usefulness*, and *novelty*. These three factors can affect the team performance in different ways depending on a user's qualification, as the task may require different levels of information credibility [14], usefulness [36], and novelty (or creativity) [21, 36]. We formulate these three factors as a weighted sum, a common way to combine multiple factors into a single value [5]. In Eq. (1), we use this weighted sum to formulate the VoI, allowing each weight to be considered depending on the specific context.

We measure the VoI about the information player i provides based on his/her expertise in the domain h by:

$$\mathrm{VoI}_{ih} = w_{\mathrm{crd}} \cdot \mathrm{crd}_{ih} + w_{\mathrm{uf}} \cdot \mathrm{uf}_{ih} + w_{\mathrm{nov}} \cdot \mathrm{nov}_{ih}, \tag{1}$$

where each of crd_{ih}, uf_{ih}, and nov_{ih} is measured as a real number in $[0, 1]$ and we hold $w_{\mathrm{crd}} + w_{\mathrm{uf}} + w_{\mathrm{nov}} = 1$. If player i is a member of the team executing a task that requires expertise in E, player i's crd_{ih}, uf_{ih}, and nov_{ih} are obtained by:

$$\mathrm{crd}_{ih} = \theta_{ih}^e, \quad \mathrm{uf}_{ih} = \min\left[1, \frac{\theta_{ih}^e}{(e_i)}\right], \quad \mathrm{nov}_{ih} = \frac{\sum_{j \in \mathcal{T}, j \neq i} \max\left[0, \left(\sqrt{\theta_{ih}^e} - \sqrt{\theta_{jh}^e}\right)\right]}{|\mathcal{T}|}, \tag{2}$$

where θ^{e}_{ih} is represented by a real number in $[0, 1]$ exhibiting player i's truthful expertise type in domain h and $\mathcal{T}$ refers to a set of other players j's in a given context of team composition.

In Eq. (2), player i's VoI contains the following components: (a) Player i's actual (truthful) expertise in domain h, $\theta^{e}_{i}(h)$, means the information credibility player i can provide, denoted by crd_{ih}; (b) This metric evaluates the extent to which player i's expertise in domain h aligns with and contributes to the team's required expertise level (e_h), directly impacting team performance. A higher uf_{ih} indicates a stronger and more relevant contribution to the team's goals in that domain.; and (c) The novelty score assesses the uniqueness of player i's expertise in domain h relative to the expertise of other team members, with a higher nov_{ih} signaling that player i brings distinct and potentially innovative insights to the team's collective knowledge.

3.4 Adversarial Model

This section describes what adversarial behaviors a team member can exhibit by leaking other team members' private information to the outside. We model the so-called *potential privacy loss* (PPL) based on an individual team member's distrust level. To derive trust relationships between two entities, even if they are not directly connected (or known) to each other, we use a belief model called *Subjective Logic* (SL) [27]. SL is a well-known belief fusion theory that can model the propagation of a user's trust in a distributed OSN under uncertainty. In addition, SL provides the capability of deriving trust relationships between different entities without direct connection. Then, we use SL to measure a team leader (i.e., mechanism designer)'s trust in other users j's in a given OSN setting and denote it by P^{MD}_{j}, MD's projected trust probability in node j. We measure the team leader's distrust in user j by $1 - P^{MD}_{j}$, as detailed in Section 5.6.

We estimate the PPL level of player i (i.e., a team member) by:

$$pl_i = \exp\left(- \frac{\lambda}{\left(\sum_{h \in E}(1 - \hat{\theta}^{p}_{ih})\right)\left(1 - \prod_{j \in M, i \neq j} P^{MD}_{j}\right)} \right), \tag{3}$$

where pl_i is the level of PPL that team member i can leak out, and λ is a constant to scale the number of domain expertise (i.e., $\lambda = |E|$). We also denote the sum of team member i's shared information with the team based on $(1 - \hat{\theta}^{p}_{ih})$ in given domain h where the revealed privacy preference is denoted by $\hat{\theta}^{p}_{ih}$ (see Section 5.4). Note that the team leader (i.e., a mechanism designer) is only aware of the revealed value of player i's privacy preference. We also calculate the probability of other team members j's PPL by $\left(1 - \prod_{j \in M, i \neq j} P^{MD}_{j}\right)$. If $(\sum_{h \in E}(1 - \hat{\theta}^{p}_{ih}))(1 - \prod_{j \in M, i \neq j} P^{MD}_{j}) = 0$, team member i has zero privacy preference by sharing all information with the team, as $pl_i = 0$, assuming all other members have complete trust to member i. In this work, we assume that the team leader is fully trusted with no chance of leaking any private information of other team members to unauthorized parties.

We estimate PPL (i.e., pl_i) based on Eq. (3) to ensure that each team member's potential privacy loss is proportional to the amount of private information they share. Because a lower privacy preference means a member is more willing to share private information. More specifically, a higher PPL incurs when member i prefers more private information sharing with other team members j's (used as the denominator in the exponent part).

4 PROBLEM DESCRIPTION & OBJECTIVE FUNCTION

Our work leverages a game theory, called the *Mechanism Design* [16, 59], to solve a team formation problem in an OSN environment. The team can develop novel, useful, and credible solutions to a sufficiently complex task that demands diverse expertise. A sufficient level of information sharing with the team is necessary for high performance. However, it is often unavoidable to face a certain level of privacy exposure to the team or possible privacy leakout to unauthorized

parties due to irresponsible (or less trustworthy) team members. We model a mechanism designer as a team leader to select relevant team members with the criteria of candidates' diverse expertise and privacy preferences to ensure both maximum team performance and minimum privacy leakout.

In the team formation research [43, 67], information sharing and its impact on privacy preservation have been a challenging problem. In this work, the team leader, as a mechanism designer (MD), aims to enable all players to expose their truthful expertise and privacy types. This allows the team leader to select the most qualified team members to maximize team performance while maximally preserving their privacy preferences. Each team member i (i.e., a player in the Mechanism Design) has a utility, u_i, based on the level of team performance a member i contributes and the level of preserving i's privacy. The MD aims to maximize *social welfare*, estimated by the sum of all players' utilities [59]. The team leader's goal is by the following objective function:

$$\arg\max_{x \in X} \sum_{i \in \mathcal{T}_x} u_i(x, \hat{\theta}_i, \hat{\theta}_{-i} | \theta_i), \quad \forall \theta_i \in \Theta_i, \tag{4}$$

where Θ_i indicates a set of preferences and θ_i refers to member i's actual (true) expertise and privacy preferences. Given X as a set of team composition decisions, $x \in X$ is a particular decision. The revealed preferences to the team leader (i.e., MD) are denoted by $\hat{\theta}_i$ for player i and $\hat{\theta}_{-i}$ for other players $-i$ (i.e., except i). A set of team members chosen by team composition decision x is given by $\mathcal{T}_x$. Eq. (6) provides how $u_i(x, \hat{\theta}_i, \hat{\theta}_{-i} | \theta_i)$ is estimated.

The team leader aims to maximize social welfare by selecting a set of relevant team members in terms of their expertise and privacy preferences, where the social welfare is estimated based on Eq. (5).

OSN users may not always behave rationally. We consider two types of irrational actors: (1) a lying actor that exhibits a different privacy preference during task execution from the one revealed by the actor during team formation; (2) an adversarial member that leaks out one member's private information to other members. We dealt with these two types of irrational actors by dynamically changing the OSN administrator's subjective belief towards a user's trust so that for a future task posted, the administrator can select truly trustworthy actors for team formation. More specifically, since both lying and privacy leakout behaviors are considered distrustful behaviors that can impact a user's trust, we use a belief model called *Subjective Logic* to estimate the mechanism designer's subjective belief towards a user's trust.

5 PROPOSED PRADA-TF FRAMEWORK

In this section, our proposed PRADA-TF uses a game-theoretic approach Mechanism Design [46]. We describe a player's type, payoff computation, preference revelation, team selection process, and actual behavior modeled.

5.1 Mechanism Design for Team Formation

A set of players, $N = \{1, 2, \cdots, n\}$, participates in a team formation where a set of team choice $x \in X$ is given with $X = \{x_1, x_2, \ldots, x_n\}$. Each player i has a truthful private signal (i.e., type) $\theta_i \in \Theta_i$, representing preferences over outcomes. A set of truthful private signals by all players is denoted by $\theta = (\theta_1, \theta_2, \ldots, \theta_n)$, which describes the profile of all truthful types for the n players. The state θ is selected randomly from the state space $\Theta \equiv \Theta_1 \times \Theta_2, \ldots, \Theta_n$, representing the set of all possible profiles of types $\theta \in \Theta$. The MD aims to select x, a set of team members, to form a team based on the members' preferences, θ's (i.e., the decision rule by $x(\theta)$), to maximize the sum of the payoffs of all team members by:

$$\sum_{i \in \mathcal{T}_x} u_i(x, \hat{\theta}_i, \hat{\theta}_{-i} | \theta_i), \tag{5}$$

where $u_i(x, \hat{\theta}_i, \hat{\theta}_{-i}|\theta_i)$ refers to player i's utility when the MD selects x when player i's revealed preference type is $\hat{\theta}_i$, other players j's revealed preference types are denoted by $\hat{\theta}_{-i}$, and θ_i is player i's truthful preference. The $u_i(x, \hat{\theta}_i, \hat{\theta}_{-i}|\theta_i)$ is given in Eq. (6).

5.2 Types of Players

Type of each player θ_i is represented with two private signals (i.e., $\theta_i = \{\theta_i^e, \theta_i^p\}$):

- *Domain expertise* (θ_i^e): We represent the domain expertise of player i with a vector of real numbers in $[0, 1]$, $\theta_i^e = \{\theta_{i1}^e, \ldots, \theta_{io}^e\}$, given $\sum_{o \in M} \theta_{io}^e \leq |M|$ where M is a set of domain expertise whose subset is E as $E \subseteq M$. Recall that E is the required domain expertise for a given task, implying $\sum_{o \in E} \theta_{io}^e \leq |E|$. Note that the level of expertise can represent the types and levels of skill sets a user has.
- *Privacy preference* (θ_i^p): In a collaborative team setting, each member may have a different preference for sharing his/her private, sensitive information. We denote this player i's privacy preference as a vector $\theta_i^p = \{\theta_{i1}^p, \theta_{i2}^p, \ldots, \theta_{io}^p\}$, where θ_{io}^p represents player i's preference in revealing information in domain o with other team members j's. Note that higher θ_{io}^p means that the player prefers to share less information for his/her privacy loss protection in executing the given task. We follow the same concept of privacy used in the privacy-preserving team formation literature [13, 23, 26, 42, 50, 58, 69]. In those works, an individual's private information is defined as *any* information the individual shares with team members while executing a given task.

Since expertise is estimated by a given objective and quantifiable criteria (e.g., track record, publications, work experience, recommendations, etc.), a player cannot lie about their domain expertise. However, since a player's privacy preference cannot be known without direct experience, the preference might change depending on other team members, their privacy preferences, and a given task (e.g., what information is required to share). In particular, the player may want to use lower privacy preference to show the willingness to contribute more to the team. We assume that the players do not expose their privacy preference higher than their true privacy preference because the reluctance to share information with higher privacy preference may lead the player to be excluded from the member selection. That is, we assume $\theta_i^e = \hat{\theta}_i^e$ (i.e., revealing truthful expertise preferences) while allowing $\theta_i^p \geq \hat{\theta}_i^p$ (i.e., possible to reveal not truthful privacy preferences).

5.3 Player's Payoff

Recall that in game theory, each player receives a reward when an outcome is reached due to the combined decisions and strategies taken by all the players. The reward received by an individual player for taking an action leading to an outcome that helps the player achieve the objective is called a payoff.
After an outcome is generated, player i's payoff can be calculated by:

$$u_i(x, \hat{\theta}_i, \hat{\theta}_{-i}|\theta_i) = u_i^{\text{team}}(x, \hat{\theta}_i, \hat{\theta}_{-i}|\theta_i) + u_i^{\text{priv}}(x, \hat{\theta}_i, \hat{\theta}_{-i}|\theta_i) - pl_i, \tag{6}$$

where $u_i^{\text{team}}(x, \hat{\theta}_i, \hat{\theta}_{-i}|\theta_i)$ is the expected team performance when the MD decides to choose team x where $\hat{\theta}_i$ is player i's revealed type, $\hat{\theta}_{-i}$ is other players $-i$'s revealed types, and θ_i is player i's truthful type. The pl_i refers to i's potential privacy loss (PPL), and $u_i^{\text{priv}}(x, \hat{\theta}_i, \hat{\theta}_{-i}|\theta_i)$ reflects how much player i's privacy preferences is preserved.

We measure $u_i^{\text{team}}(x, \hat{\theta}_i, \hat{\theta}_{-i}|\theta_i)$ based on how much credible, useful, and novel information (i.e., VoI) can be influenced by player i's expertise and privacy preferences as:

$$u_i^{\text{team}}(x, \hat{\theta}_i, \hat{\theta}_{-i}|\theta_i) = \sum_{h \in E} VoI_{ih} \cdot (1 - \hat{\theta}_{ih}^p)^2. \tag{7}$$

This equation models the decrease of novelty when more information is shared as discussed in [62]. Furthermore, by utilizing the privacy paradox and leveraging Privacy Calculus Theory [53] and Communication Privacy Management Theory [7], we estimate the privacy-related utility as:

$$u_i^{\text{priv}}(x, \hat{\theta}_i, \hat{\theta}_{-i} \mid \theta_i) = \sum_{h \in E} (1 - VoI_{ih}) \cdot (\hat{\theta}_{ih}^p)^2. \tag{8}$$

The above utility reflects that sharing in less valuable information preserves player i's privacy more and introduces less adverse impact on team performance than sharing in more valuable information.

5.4 A Player's Preference Revelation

Unlike other TF research, we additionally validate the quality of TF algorithms when a task is actually executed by the selected team. Players do not have to reveal their truthful preferences, $\theta_i = (\theta_i^e, \theta_i^p)$, where $\theta_i^e = \{\theta_{i1}^e, \theta_{i2}^e, \ldots, \theta_{in}^e\}$ and $\theta_i^p = \{\theta_{i1}^p, \theta_{i2}^p, \ldots, \theta_{in}^p\}$. We denote player i's revealed preferences by $\hat{\theta}_i = (\hat{\theta}_i^e, \hat{\theta}_i^p)$. A player's actual behavior is modeled based on whether the player reveals his/her truthful privacy type considering the following two cases:

- *Case 1:* $\theta_i^p == \hat{\theta}_i^p$ where player i does not lie about his truthful type. In this case, the revealed preference is the same as the truthful preference and helps the MD make a fair decision.
- *Case 2:* $\theta_i^p \neq \hat{\theta}_i^p$ where player i's revealed preference is different from their truthful preference. In such a scenario, during the actual task execution, the player can choose to exhibit the revealed preference or the truthful preference based on the estimated utility. Player i's preference in an actual task is denoted by $\theta_i^{p'}$, and is determined by:

$$\theta_i^{p'} = \begin{cases} \hat{\theta}_i^p \text{ if } u_i(x^*, \hat{\theta}_i, \hat{\theta}_{-i} | \theta_i) \ > \ u_i(x, \theta_i, \hat{\theta}_{-i} | \theta_i), \\ \theta_i^p \quad \text{otherwise.} \end{cases} \tag{9}$$

  Here $u_i(x^*, \hat{\theta}_i, \hat{\theta}_{-i} | \theta_i)$ is the payoff when x^* decision is taken by the MD where $\hat{\theta}_i$ is the revealed type of the player i, $\hat{\theta}_{-i}$ is other players' revealed types, and θ_i is player i's truthful type. Thus, a player will compromise his/her privacy preference if and only if the payoff by compromising the truthful privacy preference, θ_i^p, using the revealed privacy preference, $\hat{\theta}_i^p$, brings a better payoff than using θ_i^p.

To determine the lower bound of how much a player can compromise its revealed preferences, we introduce a constant pc_i as a real number in $[0, 1]$. The player can then select a real number between $[pc_i \cdot \theta_i^p, \theta_i^p]$, as its exhibited privacy preference. Inherently, the higher the value of pc_i, the lower the willingness of the player i has to compromise the privacy preference and vice-versa. Note that when player i compromises his/her privacy preference, it implies that the player announces a lower privacy preference than θ_i^p to increase its benefit by sharing more information for team performance. We will investigate how pc_i affects a team's social welfare (i.e., team performance) in Section 7.

5.5 Trust-based Team Selection Process

5.5.1 Trust Definition. Trust is commonly defined based on *competence* and *willingness*, as identified in our prior extensive trust modeling survey work [4]. Since competence is closely related to the level of expertise and willingness commonly means how often one is willing to share information with others, trust therefore can also be defined by expertise and information sharing. Recognizing that information sharing is exactly the opposite of privacy preference, we define trust by expertise and privacy preference in this work.

5.5.2 Team Selection. Consider a bi-directional weighted social network of experts $V = \{v_1, \ldots, v_{12}\}$ in Fig. 1, where each expert is associated with an expertise level in $|M|$ knowledge domains. The weight of an edge from one expert (v_i) to another expert (v_j) represents the level of trust v_i has in v_j by t_{ij}. Then, this trust propagates to arrive at MD's trust in v_j using Subjective Logic [27], which will be discussed in the next Section 5.6.

The team leader (i.e., MD) aims to form a skilled and privacy-aware team that outperforms any other team composition regarding aggregated social welfare. The prospective members of the team are selected from the MD's *k-hop trust network*, where the MD is the central node, similar to a hub. All member candidates within k-hop distance from the MD are selected during team formation. Based on the network density, the value of k is adjusted. Innately, the higher the value of k, the higher the number of member candidates chosen is, and vice-versa. Given all the prospective team members in MD's k-hop trust network, the final team is chosen as follows: (1) For all the users in the network, direct trust is calculated between all adjacent users, which is then propagated to derive the indirect trust from the MD to any other users in the network; (2) All the member candidates whose direct/indirect trust from MD is above a particular threshold (e.g., 0.9) are selected. Our proposed PRADA-TF's candidate team selection methods are applied to it to select the top ϕ number of member candidates; and (3) Finally, the team of m members is selected by applying the social welfare function to select the top contributors for the required task, from the top ϕ from the previous step. The following sections describe the k-hop trust network, followed by the candidate team selection methods.

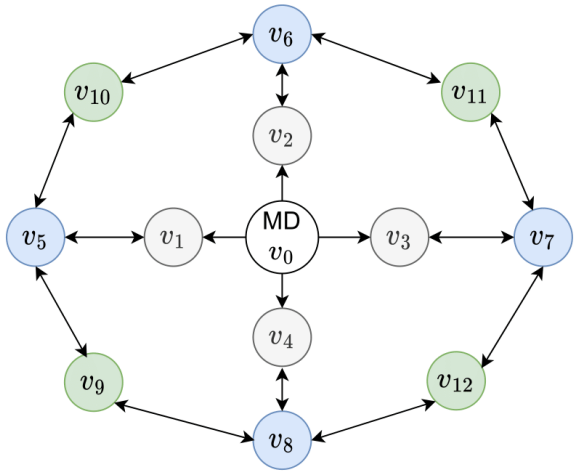


Fig. 1. The considered trust network where the gray, blue, and green nodes indicate 1st, 2nd, and 3rd hop nodes, respectively.

5.6 Building k-Hop Trust Network

As previously described, a k-hop trust network is built from the MD outwards, and the member candidates with trust values above a particular threshold (e.g., 0.9) are selected for further rounds. When two adjacent users in the OSN are connected, we calculate the *direct trust* between them based on objective and verifiable criteria. When two users are directly connected, they can accurately estimate each other's expertise and privacy preferences based on previous experiences. However, when users are not directly connected, the trust can be derived by propagating it along the trust chain with the direct trust values, as calculated earlier, with the help of the discounting operator. Since the MD can reach any user through indefinitely long trust chains, we limit the maximum length of these chains to reduce complexity and remove highly uncertain opinions. Finally, as the MD can reach the user through different trust chain paths (within the maximum length threshold), we combine these multiple opinions using the consensus operator to derive reasonably certain opinions about any user's expertise and privacy preferences.

In this work, we estimate the MD's trust in each user in a given trust network (e.g., an expert social network) based on a binomial opinion (i.e., trust or distrust) offered by SL [27]. We establish a k-hop trust network using the consensus and discounting operators. Due to the space constraint, we discuss them in Appendix B (Binomial Subjective Opinions and Their Fusion Operators) in the supplement document.

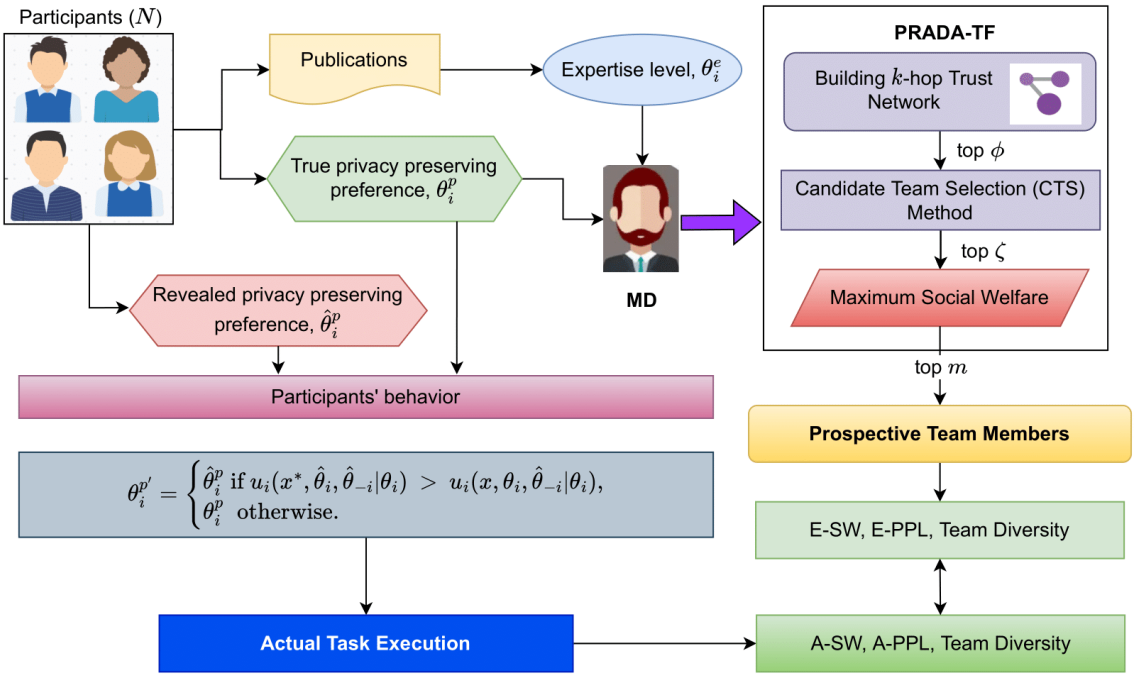


Fig. 2. PRADA-TF's Candidate Team Selection Process: E-SW and A-SW refer to expected or actual social welfare. E-PPL and A-PPL indicate expected or actual potential privacy loss. MD is a mechanism designer taking the role of a team leader.

5.7 Candidate Team Selection

As described in Section 5.5, using a sufficient value of k, a *k-hop* network is generated such that all the prospective team members are reachable from the MD. From the resulting network, trust is propagated using the *consensus* and *discounting* operators to arrive at a k-hop trust network, which is then leveraged to select the top ϕ players for the next selection.

To all the top ϕ selected candidate members, we apply Candidate Team Selection (CTS) methods to avoid high complexity and further cut down the number to ζ. From the ζ selected candidate members, the MD chooses the final m players to perform a given task based on the social welfare function. Considering all combinations of team x, the MD selects the team that maximizes the social welfare, as described in Eq. (14). Since the social welfare function is used to select a prospective team, the function's output is the expected social welfare and is not reflective of the social welfare achieved in an actual task execution where they may not be the same. In Fig. 2, we summarize the overview of our proposed PRADA-TF's candidate selection process described in this section.

6 EXPERIMENT SETUP

In this section, we describe performance metrics, datasets, parameterization, and the considered schemes used for the comparative performance analysis of our proposed PRADA-TF with the existing counterparts.

6.1 Metrics

Our proposed PRADA-TF variants are evaluated for performance against the following metrics:

- *Team Diversity ($\mathcal{TD}$)*: Team Diversity captures how diverse each team member's expertise background is, compared to the rest of the team. Team diversity, $\mathcal{TD}$, is calculated by:

$$\mathcal{TD} = \frac{\sum_{i \in \mathcal{T}} \mathcal{H}_i}{|\mathcal{T}|}, \tag{10}$$

where $\mathcal{T}$ refers to a set of all members in the team composition x and $\mathcal{H}_i$ measures the difference in team member i's expertise background to all other team members' expertise types. Based on the Hellinger distance [25], $\mathcal{H}_i$ is estimated by:

$$\mathcal{H}_i = \frac{\sum_{j \in \mathcal{T}, j \neq i} \mathcal{H}(\theta_i^e, \theta_j^e)}{|\mathcal{T}| - 1}, \tag{11}$$

where the difference between player i's background and player j's background, $\mathcal{H}(\theta_i^e, \theta_j^e)$, for given team $\mathcal{T}$ and $i, j \in \mathcal{T}$, is computed by:

$$\mathcal{H}(\theta_i^e, \theta_j^e) = \sqrt{\sum_{h \in \mathcal{E}} D_{ij}^e}, \tag{12}$$

$$\text{where } D_{ij}^e = \frac{\sum_{h \in E} \max\left[0, \theta_{ih}^e - \theta_{jh}^e\right]}{|E|}. \tag{13}$$

The θ_{ih}^e and θ_{jh}^e represent the truthful expertise types of player i and j in domain h, respectively.

- *Social Welfare* ($\mathcal{SW}_{\mathcal{T}}$): This refers to a team's expected social welfare estimated based on Eq. (6), which is a sum of utilities of all the team members participating in a task:

$$\mathcal{SW}_{\mathcal{T}} = \sum_{i \in \mathcal{T}} u_i(x, \hat{\theta}_i, \hat{\theta}_{-i} | \theta_i). \tag{14}$$

Note that the actual SW is estimated by replacing revealed preferences, $\hat{\theta}_i$, with exhibited preferences, θ_i', at the execution time. Therefore, the experimental results show both expected and actual social welfare.

- *Potential Privacy Loss ($\mathcal{PPL}$)*: This metric refers to the amount of penalty a player may have because of a potential privacy leakout by other players. We use pl_i in Eq. (3) to measure it. We demonstrate the expected and actual PPL where a player's revealed preference estimates the expected PPL, $\hat{\theta}_i$, while the actual PPL uses the exhibited privacy level used by a player at task execution.
- *Complexity Analysis Metrics*: We analyze asymptotic time complexity using Big-O and simulation running time in sec.

6.2 Experimental Setup

6.2.1 Datasets. We create two semi-synthetic datasets resembling two separate OSNs to test the feasibility of our approach:

(1) A *N*etscience dataset is created from the real-world *N*etscience [49] dataset containing a network of 1,590 scientists working on Network Theory and Experiments. The *Netscience* dataset resembles a *M*ultidisciplinary Co-authorship Collaboration OSN where multidisciplinary collaboration is of utmost importance. We compile the reference lists of two review articles on networks [3, 48]. Using the Scopus API, the publication records and metrics are extracted for the top three subject areas (according to All Science Journal Classification, or ASJC) to determine the expertise of each author in the network using their corresponding publications and citations. We further consolidate the network into five categories: biology, biochemistry, science, arts, and engineering. Next, by creating edges whenever the cosine similarity of two authors equals or exceeds 0.9 in an expert level and subject area, this sparse network will be

Table 1. KEY PARAMETERS, MEANINGS, AND DEFAULT VALUES

Param.	Meaning	Value
N	Total number of users in the OSN	1,269
E	Total number of edges in the OSN	28,072
θ^e_{ik}	Strength in expertise in domain k	[0, 1]
θ^p_{ik}	Privacy-preserving preference in domain k	[0, 1]
$\hat{\theta}^p_{ik}$	Revealed privacy preserving preference in domain k	[0, 1]
pc_i	Extent to which a player can lie about its privacy-preserving preference	[0, 1]
w_e, w_s	Weights for expertise and privacy privacy preserving respectively	[0, 1]
ϕ	Number of candidates selected from the trust network	200
ζ	Number of participants selected using CTS schemes	40
m	Number of team members	20
$\|\mathcal{E}\|$	Number of expertise domains	5
$w_{\text{crd}}, w_{\text{uf}}, w_{\text{nov}}$	Weights for the three components of VoI	$[0, 1]$
ϵ	Sum of domain expertise levels required by a given task (i.e., $\sum_{e_i \in E} e_i = \epsilon$)	5
$\mathbf{L}$	A vector of domain expertise levels in a given task, $\{e_1, e_2, \ldots, e_l\}$	$[1, 1, 1, 1, 1]$
λ	A constant to scale pl_i in Eq. (3)	$\|E\|$

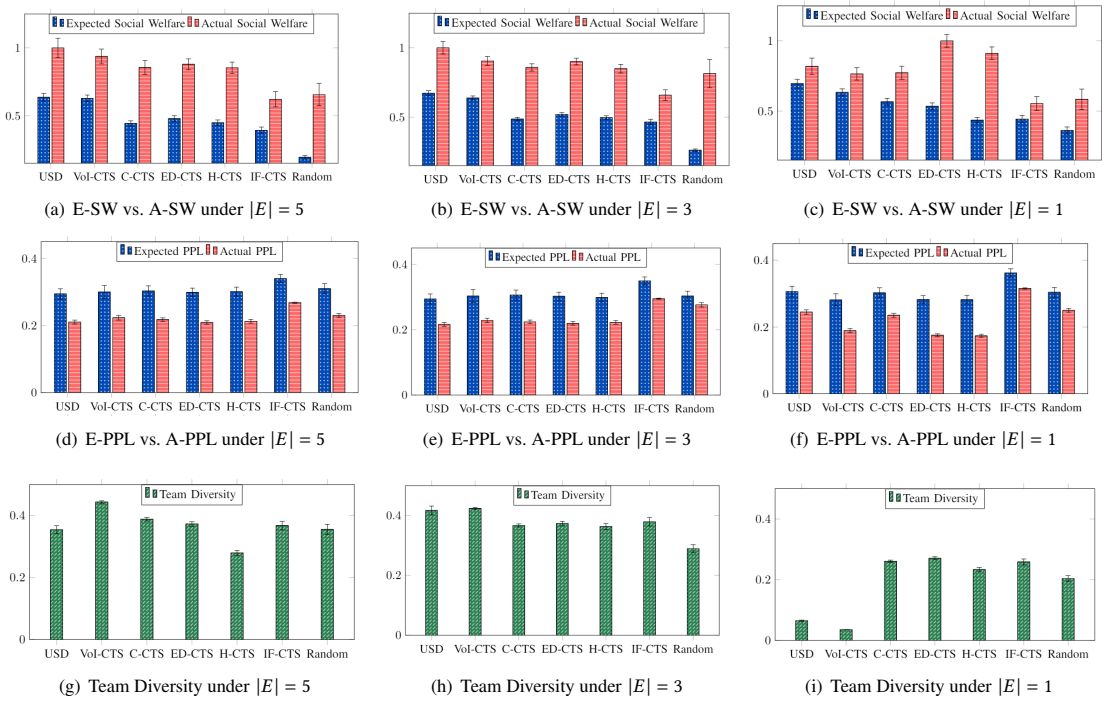
converted into a small-world network, easier for authors to reach through the MD. Based on the processed *Netscience* data, a network containing 1,269 nodes, 28,072 edges, and five subject-area specific communities is constructed. Subsequently, a Gaussian distribution draws the privacy preferences of each author with a mean of $\mu = 0.5$ and a standard deviation of $\sigma = 0.3$.

(2) An IMDb dataset is created from the real-world IMDb dataset [8], which contains a network of 1,021 artists acting in global entertainment industries. The co-star network, where an artist's expertise is publicly verified, is suitable for evaluating the effects of diversity and privacy in a collaborative setting. The IMDb dataset resembles an artist OSN as it contains sufficient details about an artist in the OSN: (1) different genres the artist has acted in; and (2) the number of times the artist has co-acted/collaborated with other artists in the past. Given that an artist can work in various domains, we pre-process the dataset to select the top three genres and rate the artists based on those genres. The top three genres in our dataset are *Drama, Comedy*, and *Crime*. Given the top three genres, the expertise of the artist in each of the genres is estimated by:

$$\theta_i^{\text{genre}} = \frac{\log|\text{genre}|}{\mathcal{D}} \times \frac{c_i}{c_m}, \tag{15}$$

where $\mathcal{D} = \log|\text{comedy}| + \log|\text{drama}| + \log|\text{crime}|$, genre $\in \{\text{drama, comedy, crime}\}$, c_i is the total number of movie credits an artist i has received throughout his career, and c_m is the average movie credits of all artists in the dataset. By comparing against the dataset's average, we obtain an accurate representation of the artist's expertise i in a genre between $[0, 1]$ using Eq. (15). Note that during evaluations of the expertise, if the expertise value exceeds 1, the artist is assigned full expertise in that genre. The privacy preferences of each artist are also drawn from a normal distribution with a mean of $\mu = 0.5$ and a standard deviation of $\sigma = 0.3$. From the data on the collaboration between artists, we form a graph where an edge exists if two artists have worked together in the past. The resulting graph has 1,021 nodes, 11,224 edges, and three different genres.

6.2.2 Parameterization. With 1,269 authors in the network, the author with the highest betweenness centrality value is selected as the team leader and also a Mechanism Designer. This highly dense network has over 28,000 edges, so a



(a) E-SW vs. A-SW under $|E| = 5$ (b) E-SW vs. A-SW under $|E| = 3$ (c) E-SW vs. A-SW under $|E| = 1$

(d) E-PPL vs. A-PPL under $|E| = 5$ (e) E-PPL vs. A-PPL under $|E| = 3$ (f) E-PPL vs. A-PPL under $|E| = 1$

(g) Team Diversity under $|E| = 5$ (h) Team Diversity under $|E| = 3$ (i) Team Diversity under $|E| = 1$

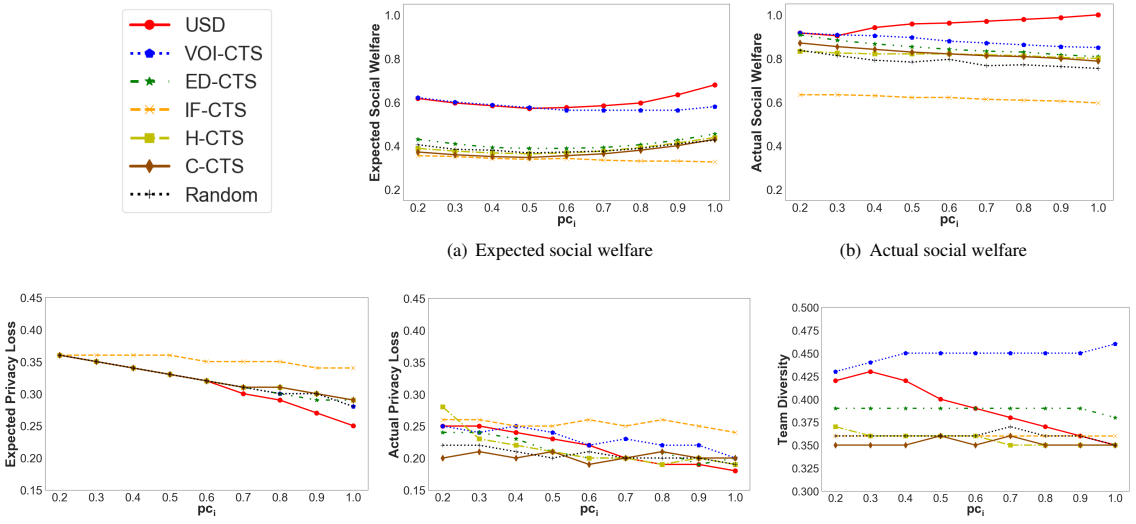
Fig. 3. Performance comparison of different candidate team selection (CTS) methods based on the five metrics, including expected social welfare (E-SW), actual social welfare (A-SW), expected potential privacy loss (E-PPL), actual potential privacy loss (A-PPL), and team diversity, when the number of domains varies with $|E| = 5, 3$ or 1 and the corresponding task composition, $\mathbf{L}(e_i) = [1, 1, 1, 1, 1], [5/3, 5/3, 5/3]$, or [5], respectively. (a), (d), and (g) are under $|E| = 5$, (b), (e), and (h) are under $|E| = 3$, and (c), (f), and (i) are under $|E| = 1$. The lower bound weight of a revealed privacy preference (pc_i) is set to $= 0.8$, the number of hops in an online trust network (k-hop) is set to 5, and the error bar represents the standard deviation.

value of 5 is chosen for k in $k - hops$, so most of the users in the network may be selected for recursive trust calculation in the trusted network according to Section 5. Since all independent paths from the MD to each user in the MD's trust network are examined, high-degree users are more likely to have higher trust values, as they can combine trust values from multiple directions using a consensus operator. Given that a task requires diverse and novel information, we weigh Credibility, Usefulness, and Novelty in VoI (Value of Information) as 0.2, 0.3, and 0.5, respectively. The w_e and w_s in Eq. (5) of the supplement document are equally weighted with $w_e = w_s = 0.5$. Top 200 ($= \phi$) players with the highest trust values are selected from which 40 ($= \zeta$) players are selected based on a given candidate team selection method described in 'Selection of Candidate Teams' of Section 5. A further shortlisting of 20 players is made from a list to 40 to maximize social welfare. Tabulated below are the default values for the key design parameters for our experiments. Results are calculated using the mean values from 1,000 simulation runs and the standard deviation at each point.

6.3 Comparing Schemes

In this work, we conduct a comparative performance analysis of the following schemes:

- *Utility-based Serial Dictatorship (USD)* where candidates are selected based on the output of the utility function for individual players (see Eq. (6)).



(a) Expected social welfare (b) Actual social welfare

(c) Expected PPL (d) Actual PPL (e) Team diversity

Fig. 4. Comparison of different candidate team selection (CTS) methods based on the five metrics under varying the lower bound weight of a revealed privacy preference (pc_i), where the environment is set as the number of domains ($|E|$) = 5, pc_i = 0.8, and task composition ($\mathbf{L}(e_i) = [1, 1, 1, 1, 1]$) under a 5-hop trust network (i.e., $k = 5$).

- *Expertise diversity-based CTS (ED-CTS)* where candidates are selected based on the uniqueness and diversity of the information to be contributed by the player given a task, similar to [41] (see Eq. (11)).
- *VoI-based CTS (VoI-CTS)* where candidate members are selected based on the value of information to be contributed by the player (Eq. (1)).
- *Information Sharing (IF-CTS)* where candidate members are selected solely based on their revealed privacy preference, $\hat{\theta}_i^p$. Players willing to share the most information are selected for the candidate team.
- *Homophily-based CTS (H-CTS)* where candidates are selected based on the homophily of the cosine-similarity metric [28] for the domain expertise of each player with the required expertise for a given task.
- *Centrality-based CTS (C-CTS)* [10] where candidates are selected based on the centrality value of the player in the trust network. To demonstrate the effectiveness, we leverage the betweenness centrality to identify the influential members in the network.
- *Random* where players are selected randomly from a given trust network.

USD, ED-CTS, VoI-CTS, and IF-CTS are the variants of our proposed PRADA-TF schemes. H-CTS and C-CTS are proven-and-effective schemes as comparable counterparts, while Random is a baseline scheme.

7 NUMERICAL RESULTS & ANALYSIS

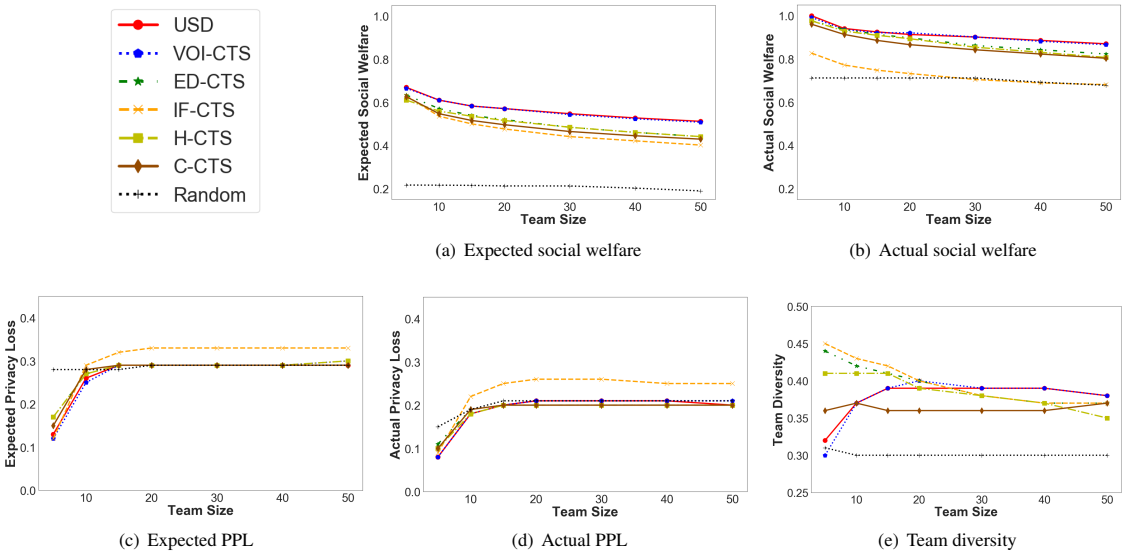
In this section, we demonstrate the simulation results and analyze their overall trends regarding the effects of different task types, compromising privacy, team sizes, and candidate team sizes. In addition, we analyze the algorithmic complexity of the considered TF algorithms based on both Big-O asymptotic time complexity analysis and simulation running time in sec.

Due to space constraints, we only report results on the *Netscience* dataset. The results on the *IMDb* dataset are consistent with those on the *Netscience* dataset and can be found in Appendix A of the supplement document.

7.1 Effect of Different Task Types

Fig. 3 shows the effect of different task types on the performance of the seven different candidate team selection (CTS) methods based on the five metrics in Section 6.1. From Fig. 2, in the team selection process, we first select the top ϕ participants from the k-hop trust network, from which the top ζ candidates are chosen based on the CTS methods proposed. Finally, from the top ζ candidates, the top m players are chosen based on the social welfare function. For consistency and ease based on selecting the top m candidates, we used $\zeta = 2m$ under different m values. Figs. 3(a)-3(c) show the performance comparison of seven different team selection methods based on Expected Social Welfare (E-SW) and Actual Social Welfare (A-SW). In Figs. 3(a)-3(c), we observe that in actual task execution, players tend to maximize their utilities by compromising their privacy and thereby increasing their information-sharing behavior (i.e., lowering the privacy preference level). Consequently, we observe that A-SW is likely higher than E-SW for the same reason. In a task requiring a fairly diverse skill-set, i.e., $L(e_i) = [1, 1, 1, 1, 1]$ with $|E| = 5$, from Fig. 3(a), we observe that the performance of the CTS methods is in the following order: USD > VoI-CTS > C-CTS ≃ ED-CTS ≃ H-CTS > Random ≃ IF-CTS. This is aligned with the trend observed for both A-SW and E-SW. We find that players chosen from the IF-CTS scheme tend to curb their privacy sacrifice to compensate for the consequent privacy loss, especially compared to C-CTS, ED-CTS, and H-CTS. We observe a similar trend in the performance of the CTS methods in a task requiring adequately diverse skill sets, i.e., $|E| = 3$ and $L(e_i) = [5/3, 5/3, 5/3]$. Similar to Fig. 3(a), Fig. 3(d) shows that USD performs the best among all, whereas IF-CTS performs the worst. However, this trend changes when a task requires domain-specific expertise, e.g., $|E| = 1$ and $L(e_i) = [5]$. In Fig. 3(g), contrary to the previous trends from the task compositions with $|E| = 3$ and $|E| = 5$, ED-CTS tends to perform the best, followed by H-CTS and USD. From the trends, we infer that a certain level of diversity is important for promoting team performance in a collaborative setting. However, when a task requires high expertise in a relatively less number of domains, the diversity in expertise and the novelty of the information contributed introduce a more vital impact on team diversity, as in Figs. 3(c), 3(f), and 3(i), specifically for ED-CTS and IF-CTS.

Figs. 3(d)-3(f) demonstrate the effect of different task types on Potential Privacy Loss (PPL). With the same reasoning as that of the difference in A-SW and E-SW, we observe that the actual PPL (A-PPL) is lower than the expected PPL (E-PPL). This is because, in actual task execution, a player might either stick to its revealed privacy preference or switch to its actual privacy preferences (see Section 5.2, which would be higher, which would, in turn, lead to less information shared and less privacy loss. This directly affects the utility, and we can observe the effects on the A-SW and E-SW values, as discussed before. Observing Fig 3(d), we notice that IF-CTS has the highest A-PPL, whereas USD has the lowest. That is, there exists a trade-off between information sharing and privacy. Sharing more information, regardless of its value (VoI), will naturally lead to higher privacy loss. As observed in Figs. 3(a), 3(b), and 3(c), information sharing (as shown in IF-CTS) is not a driving factor to maximize SW because of its high PPL. On the other hand, all the VoI-CTS, C-CTS, ED-CTS, and H-CTS show similar levels of PPL, indicating that all players act similarly in a selfish manner to protect their privacy, irrespective of the scheme used. In Fig. 3(e), we observe a similar trend wherein IF-CTS has the highest A-PPL, whereas all the rest of the CTS methods have comparable A-PPL values (except for Random). Notice that this directly affects the SW (see Fig. 3(b)). In addition, in Fig. 3(f), the performance order in terms of A-PPL is observed as ED-CTS > H-CTS > USD > Random > VoI-CTS > C-CTS > USD > IF-CTS. This is particularly interesting because, from Fig. 3(c), we can see that ED-CTS, followed by H-CTS, performs the best. From these comparisons, we can conclude that an inverse relationship exists between privacy loss and team performance estimated by SW.



(a) Expected social welfare (b) Actual social welfare

(c) Expected PPL (d) Actual PPL (e) Team diversity

Fig. 5. Comparison of different candidate team selection (CTS) methods based on the five metrics under varying team size, where the environment is set as the number of domains ($|E|$) = 5, pc_i = 0.8, and task composition ($\mathbf{L}(e_i) = [1, 1, 1, 1, 1]$) under a 5-hop trust network.

Figs. 3(g)-3(i) show the diversity of the team formed using the seven different CTS methods under three different types of tasks. For tasks requiring a fairly diverse skill-set (i.e., $|E| = 5$ or 3), we can see a clear trend between the best performing CTS schemes and team diversity, e.g., USD or VoI-CTS in Figs. 3(g) and 3(h). In Fig 3(h), team diversity is a standout factor that leads to higher utility, which can be clearly observed in USD and VoI-CTS. However, we also observe relatively high diversity for poor-performing schemes (see IF-CTS and Random). To further ensure our findings, from Fig. 3(i), we can observe that high team diversity is aligned with increased social welfare. From this observation, team diversity is important when the task requires subject-area-specific expertise. However, under a task requiring diverse domain expertise, it is unclear that having a certain level of diversity is closely related to high team performance (i.e., high social welfare), as shown in Fig. 3(i).

7.2 Effect of Compromising Privacy

Fig. 4 shows the effect of varying the lower bound of compromising a team member's privacy preference (pc_i) under the seven different CTS methods based on the five metrics. Like Fig. 3, USD performs the best, followed by VoI-CTS amongst all the E-SW and A-SW, as in Figs. 4(a) and 4(b). In Fig. 4(a), we observe that as pc_i increases (revealing more truthful privacy preferences), E-SW decreases when pc_i ranges from 0.2 to 0.5 whereas it increases when pc_i increases from 0.5 to 1. That is when $pc_i = [0.2, 0.5]$, the utility achieved by compromising the privacy is less than the privacy loss suffered as E-SW decreases for $pc_i = [0.5, 1]$. Unexpectedly, overall A-SW decreases as pc_i increases except for USD, which increases as pc_i increases. Although A-SW is always higher than E-SW, fewer players choose to compromise their privacy because the utility achieved by compromising its privacy compared to the privacy loss is less when pc_i increases and players' revealed privacy types become closer to their true types. In USD, players are selected based on the utility function. Thus, as pc_i increases, E-SW and A-SW increase.

Table 2. ASYMPTOTIC TIME COMPLEXITY OF THE SEVEN DIFFERENT CTS METHODS

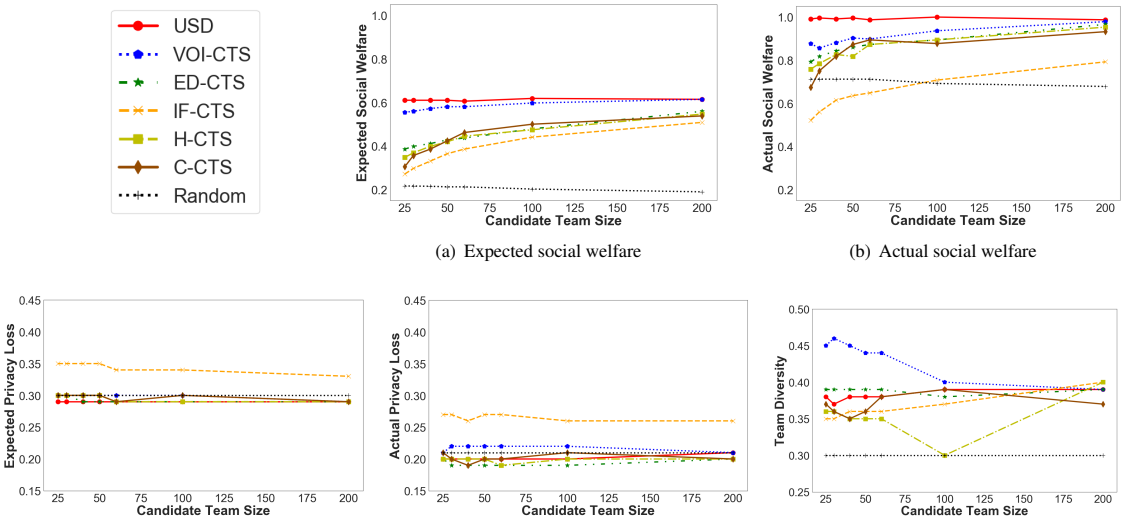
Scheme	**Big-O**	**Scheme**	**Big-O**
USD	$\mathcal{O}(\|V\|\|\mathcal{E}\|)$	ED-CTS	$\mathcal{O}(\|V\|^2\|\mathcal{E}\|)$
VoI-CTS	$\mathcal{O}(\|V\|^2\|\mathcal{E}\|)$	H-CTS	$\mathcal{O}(\|V\|)$
C-CTS	$\mathcal{O}(\|V\|\|E\|)$	IF-CTS	$\mathcal{O}(\|V\|)$

Note that V is a set of players, $\mathcal{E}$ is a set of expertise domains, and E is a set of edges.

In Fig. 4(c), we can see that the E-PPL decreases relatively sharply for USD, whereas IF-CTS has the highest value across all values of pc_i. Overall we observe that the E-PPL decreases as pc_i increases. In Fig. 4(d), we notice that except for USD, which follows the general trend, the rest of all the CTS methods remain unchanged (e.g., C-CTS) or have a slight decrease in their value of A-PPL as pc_i increases. The decreased A-PPL is because as pc_i increases, players start reporting higher privacy preference (less information sharing but revealing more truthful information), leading to less potential privacy loss. In addition, in actual task execution, players may revert to their true privacy preferences, further increasing their privacy preservation. Fig. 4(e) shows the trend in diversity as pc_i varies. We interpret that VoI-CTS has the highest increase in team diversity as pc_i increases. On the other hand, team diversity decreases under USD. For all the rest of the methods, the team diversity follows an almost zero incline. Additionally, compared to Fig. 4(a), A-SW increases as the team diversity increases for USD, whereas the A-SW decreases when the team diversity increases under VoI-CTS. This implies that although a certain level of team diversity can contribute to high team performance (i.e., higher social welfare), it is not necessarily true that higher team diversity produces higher social welfare based on the linear relationship.

7.3 Effect of Different Team Sizes

In Fig. 5, we show how different team sizes affect the performance of different CTS methods in terms of the five metrics. When comparing Figs. 5(a) and 5(b) against Figs. 5(c) and 5(d), respectively, we can infer the following. First, as the team size increases, PPL increases, consequently decreasing the player's utility. Looking at Figs. 5(b) and 5(d), as the team size increases, A-PPL increases while A-SW decreases, which is reasonable as higher PPL makes lower A-SW. Second, there exists a trade-off between information sharing and privacy, which directly affects the utility received by the team player. We have already discussed the poor performance of IF-CTS. Unlike the general trend observed, as the team size increases, the utility from collective information sharing predominates the risk of privacy loss, and consequently, utility increases steadily. Lastly, C-CTS selects influential candidates in the network. From Fig. 5(d), when the team size is small, a team with influential players has high A-PPL, which increases as the team size increases. However, after examining Fig. 5(b), we notice that although A-PPL increases, A-SW also increases. This implies that the valuable information shared by these influential members outweighs A-PPL. Fig. 5(e) shows the effect of different team sizes on team diversity under the seven CTS methods. The team diversity for USD and VoI-CTS increases as the team size increases because more task-specific candidates are selected, increasing expertise diversity. However, the team diversity decreases for ED-CTS, H-CTS, and C-CTS as the team size increases. This is because although players are chosen based on diversity or homophily (i.e., ED-CTS, H-CTS) and influence (i.e., C-CTS), the team consisting of highly diverse individuals cancels each other out considering diversity. Overall as the team sizes increase, all metrics converge to certain points. This implies that the CTS method is more important in promoting team performance under a smaller team size.



(a) Expected social welfare (b) Actual social welfare

(c) Expected PPL (d) Actual PPL (e) Team diversity

Fig. 6. Comparison of different candidate team selection (CTS) methods based on the five metrics under varying candidate team size, with the number of domains ($|E|$) = 5, pc_i = 0.8, and task composition ($\mathbf{L}(e_i)$ = $[1, 1, 1, 1, 1]$) under a 5-hop trust network.

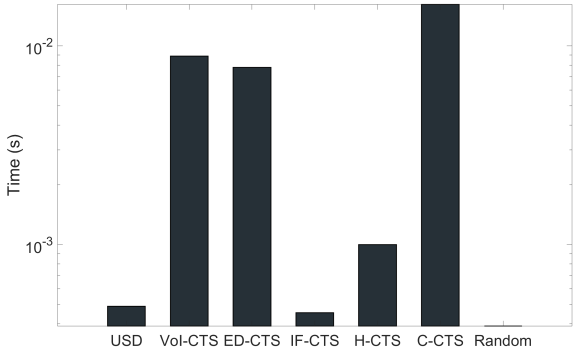


Fig. 7. Comparison of different candidate team selection (CTS) methods based on running time, where the environment is set as the number of domains ($|E|$) = 5, pc_i = 0.8 and task composition ($\mathbf{L}(e_i)$ = $[1, 1, 1, 1, 1]$).

7.4 Effects of Different Candidate Team Sizes

Fig. 6 shows the effects of varying the candidate team size for the seven different CTS methods in terms of the five metrics described in Section 6.1. By keeping the team size fixed at 20, we vary the candidate team size from 25 to 200 to analyze its effect on team formation and performance. Although the team size is fixed, each CTS method has a higher player pool to choose from as the candidate team size increases. Figs. 6(a) - 6(e) explain that although the performance change is not drastic, it is nevertheless insightful. From Figs. 6(a) and 6(b), we can infer that as the candidate team size increase, the social welfare of the team in both actual and expected SW increases gradually. As the number of candidates increases, the CTS methods have more access to high utility-yielding players, and thus the actual and expected SW values increase. Interestingly, the utility of USD does not show much change by maintaining the highest throughout all candidate team sizes. This means that the USD outperforms all, regardless of any other constraints.

Figs. 6(c) and 6(d) show the effect of candidate team size on the E-PPL and A-PPL values. Based on the reasonable inference of an inverse relationship between information sharing and privacy, the E-PPL and A-PPL values show the highest for IF-CTS, where players are chosen based on their information-sharing behaviors. However, the candidate team size is consistent and has no apparent effect on the PPL values. Privacy is affected by the final team formed. Although more players with varied backgrounds are considered, the overall risk of privacy loss remains the same as long as the team size remains the same (also see Figs. 5(c) and 5(d)). With the same reasoning from Fig. 6(e), we can see team diversity remains consistent with the increase in candidate team size. Except for VoI-CTS and C-CTS, there is a slight upward trend in team diversity, which is expected because more candidates are available for the MD to form the final team.

7.5 Complexity Analysis

Table 2 shows the asymptotic time complexity of all the CTS methods in Big-O. From Table 2, we can observe that ED-CTS has the highest algorithmic complexity, whereas H-CTS and IF-CTS incur the lowest complexity. ED-CTS needs to calculate the expertise diversity by comparing each player with all other players in the network, which increases the complexity. On the other hand, IF-CTS simply selects candidates based on their reported privacy-preserving preferences, which makes the complexity linear. Although USD incurs higher complexity than H-CTS and IF-CTS, compared to its outperformance in social welfare, PPL, and team diversity, its complexity, $O(|V||\mathcal{E}|)$, is not as high as VoI-CTS and C-CTS where $|E| >> |\mathcal{E}|$ (i.e., $|E| = 28,072$ and $|\mathcal{E}| = 5$).

To capture the cost of hidden operations in asymptotic complexity analysis, we also show Fig. 7 to explain the actual simulation running times of all the seven CTS methods. We can see that the running times for all seven methods are quite close and in the range $10^{-1.5}$. Aligned with the results discussed in Table 7, the running times of USD and IF-CTS are significantly low, while H-CTS shows relatively good performance compared to VoI-CTS, ED-CTS, and C-CTS.

8 CONCLUSIONS

8.1 Key Findings

We obtained the following **key findings** in this study:

- Among utility components, utility-based team selection (UTS) can best balance privacy preservation and team performance.
- Due to potential privacy loss (PPL), telling truthful privacy preferences does not always lead to low team performance, even if high privacy preferences result in less information sharing. This was clearly observed with higher actual social welfare (SW) than expected SW, while there was higher expected PPL and lower actual PPL.
- Higher team diversity does not always lead to higher team performance because it may introduce higher challenges in understanding between team members and may provide a shallow level of domain expertise (e.g., a member with multiple domain expertise but with a shallow level). In addition, under low information sharing, even if the information shared is diverse, it does not necessarily directly contribute to high team performance.
- An excessively large team can suffer from a lack of domain expertise and diversity due to overlapping expertise between team members.
- Although the team formation (TF) problem is known NP-Hard, we solved the TF problem heuristically in a polynomial time to identify a close-to-optimal solution that can meet multiple criteria of team members selection. It is particularly noticeable that all seven TF algorithms show similar running times in the range of $10^{-1.5}$ in sec.

8.2 Limitations & Future Research

We discuss the limitations and future research directions to address the limitations as follows:

- Our work is limited in investigating the effect of privacy preservation and team diversity on team performance. Team coherence was not explicitly considered. A future research direction is to analyze the effect of trust among team members on team coherence and investigate the effect of team coherence on team performance.
- In this work, a player's privacy preference is not changed. In reality, a player's privacy preference may continuously evolve over the duration of the task. Another future research direction is a dynamically changing privacy model that can analyze the impact of various factors. They may affect a player's privacy preference during task execution.
- In this work, we simulated each player's privacy preference. A future research direction is to model each individual player's privacy preference more accurately by first-party data (collected directly from users in a target OSN).

9 ACKNOWLEDGMENTS

This work is partly supported by the NSF Grant 2107450. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

REFERENCES

[1] Aris Anagnostopoulos, Luca Becchetti, Carlos Castillo, Aristides Gionis, and Stefano Leonardi. 2012. Online Team Formation in Social Networks. In *Proceedings of the 21st WWW*. 839–848.

[2] Myriam Bechtoldt, Carsten De Dreu, and Bernard Nijstad. 2007. Team Personality Diversity, Group Creativity, and Innovativeness in Organizational Teams. *Available from Internet: http://www.susdiv.org/uploadfiles/RT3.2_PP_Carsten.pdf/* (2007).

[3] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D.-U. Hwang. 2006. Complex networks: Structure and dynamics. *Physics Reports* 424, 4 (2006), 175–308. https://doi.org/10.1016/j.physrep.2005.10.009

[4] Jin-Hee Cho, Kevin Chan, and Sibel Adali. 2015. A Survey on Trust Modeling. *ACM Comput. Surv.* 48, 2, Article 28 (Oct. 2015), 40 pages. https://doi.org/10.1145/2815595

[5] Jin-Hee Cho, Yating Wang, Ing-Ray Chen, Kevin S. Chan, and Ananthram Swami. 2017. A Survey on Modeling and Optimizing Multi-Objective Systems. *IEEE Communications Surveys Tutorials* 19, 3 (2017), 1867–1901. https://doi.org/10.1109/COMST.2017.2698366

[6] Sara Cohen and Moran Yashinski. 2017. Crowdsourcing with Diverse Groups of Users. In *Proceedings of the 20th International Workshop on the Web and Databases (WebDB'17)*. 7–12. https://doi.org/10.1145/3068839.3068842

[7] Mary J. Culnan and Pamela K. Armstrong. 1999. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science* 10, 1 (1999), 104–115. https://doi.org/10.1287/orsc.10.1.104

[8] IMDb Datasets. [n. d.]. IMDb Datasets. ([n. d.]). https://datasets.imdbws.com/ Last Accessed on May 10, 2023.

[9] Samik Datta, Anirban Majumder, and K.V.M. Naidu. 2012. Capacitated Team Formation Problem on Social Networks. In *Proceedings of the 18th ACM KDD '12*. 1005–1013.

[10] Paramita Dey, Maitreyee Ganguly, and Sarbani Roy. 2017. Network centrality based team formation: A case study on T-20 cricket. *Applied Computing and Informatics* 13, 2 (2017), 161 – 168. https://doi.org/10.1016/j.aci.2016.11.001

[11] Jun Du, Chunxiao Jiang, Kwang-Cheng Chen, Yong Ren, and H. Vincent Poor. 2018. Community-Structured Evolutionary Game for Privacy Protection in Social Networks. *IEEE Transactions on Information Forensics and Security* 13, 3 (2018), 574–589. https://doi.org/10.1109/TIFS.2017.2758756

[12] Jun Du, Chunxiao Jiang, Erol Gelenbe, Lei Xu, Jianhua Li, and Yong Ren. 2018. Distributed Data Privacy Preservation in IoT Applications. *IEEE Wireless Communications* 25, 6 (2018), 68–76. https://doi.org/10.1109/MWC.2017.1800094

[13] Cynthia Dwork. 2006. Differential Privacy. In *Automata, Languages and Programming*, Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener (Eds.). 1–12.

[14] P Christopher Earley. 1985. Influence of information, choice and task complexity upon goal acceptance, performance, and personal goals. *Journal of Applied Psychology* 70, 3 (1985), 481.

[15] Robin J Ely and David A Thomas. 2020. Getting serious about diversity. *Harvard Business Review* 98, 6 (2020), 114–122.

[16] Arthur G. Erdman and George N. Sandor. 1997. *Mechanism Design (3rd Ed.): Analysis and Synthesis (Vol. 1)*. Prentice-Hall, Inc., USA.

[17] Amita Gajewar and Atish Das Sarma. 2011. Multi-Skill Collaborative Teams based on Densest Subgraphs. In *Proceedings of the 2012 SIAM International Conference on Data Mining*. 165–176.

[18] Mohssen Ghafari, Shahpar Yakhchi, Amin Beheshti, and Mehmet Orgun. 2018. *Social Context-Aware Trust Prediction: Methods for Identifying Fake News*. 161–177. https://doi.org/10.1007/978-3-030-02922-7_11

[19] Seyed Mohssen Ghafari, Amin Beheshti, Aditya Joshi, Cecile Paris, Adnan Mahmood, Shahpar Yakhchi, and Mehmet A. Orgun. 2020. A Survey on Trust Prediction in Online Social Networks. *IEEE Access* 8 (2020), 144292–144309. https://doi.org/10.1109/ACCESS.2020.3009445

[20] L.E. Gomez and Patrick Bernet. 2019. Diversity improves performance and outcomes. *Journal of the National Medical Association* 111, 4 (2019), 383–392. https://doi.org/10.1016/j.jnma.2019.01.006

[21] Yaping Gong, Tae-Yeol Kim, Deog-Ro Lee, and Jing Zhu. 2013. A multilevel model of team goal orientation, information exchange, and creativity. *Academy of Management Journal* 56, 3 (2013), 827–851.

[22] Sonja Grabner-Kräuter and Sofie Bitter. 2015. Trust in online social networks: A multifaceted perspective. *Forum for Social Economics* 44, 1 (2015), 48–68. https://doi.org/10.1080/07360932.2013.781517

[23] Rachel Greenstadt, Jonathan P. Pearce, and Milind Tambe. 2006. Analysis of Privacy Loss in Distributed Constraint Optimization. In *Proceedings of the 21st National Conference on Artificial Intelligence (AAAI'06)*, Vol. 1. AAAI Press, 647–653.

[24] Yu Guo, Hongcheng Xie, Yinbin Miao, Cong Wang, and Xiaohua Jia. 2022. FedCrowd: A Federated and Privacy-Preserving Crowdsourcing Platform on Blockchain. *IEEE Transactions on Services Computing* 15, 4 (2022), 2060–2073. https://doi.org/10.1109/TSC.2020.3031061

[25] David Hand. 2008. Statistical Decision Theory: Estimation, Testing, and Selection. *International Statistical Review* 76 (Feb. 2008), 450–450. https://doi.org/10.1111/j.1751-5823.2008.00062_15.x

[26] Maaike Harbers, Reyhan Aydogan, Catholijn M. Jonker, and Mark A. Neerincx. 2014. Sharing Information in Teams: Giving up Privacy or Compromising on Team Performance?. In *Proceedings of the 2014 International Conference on Autonomous Agents and Multi-Agent Systems (AAMAS '14)*. 413–420.

[27] Audun Jøsang. 2016. *Subjective Logic: A Formalism for Reasoning Under Uncertainty* (1st ed.). Springer Publishing Company, Incorporated.

[28] I. Kamel, Zaher Al Aghbari, and Kareem Kamel. 2016. SmartRecruiter: A Similarity-based Team Formation Algorithm. *International Journal of Big Data Intelligence* 3 (01 2016), 228–238. https://doi.org/10.1504/IJBDI.2016.079975

[29] M. Kargar and A. An. 2011. TeamExp: Top-k Team Formation in Social Networks. In *IEEE 11th ICDM Workshops*. 1231–1234.

[30] Linda Lai and Efraim Turban. 2008. Groups Formation and Operations in the Web 2.0 Environment and Social Networks. *Group Decision and Negotiation* 17 (09 2008), 387–. https://doi.org/10.1007/s10726-008-9113-2

[31] Theodoros Lappas, Kun Liu, and Evimaria Terzi. 2009. Finding a Team of Experts in Social Networks. In *Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. New York, NY, USA, 467–476.

[32] Cheng-Te Li, Man-Kwan Shan, and Shou-De Lin. 2015. On team formation with expertise query in collaborative social networks. *Knowledge and Information Systems* 42, 2 (01 Feb 2015), 441–463.

[33] Beng-Chong Lim and Katherine J. Klein. 2006. Team mental models and team performance: a field study of the effects of team mental model similarity and accuracy. *Journal of Organizational Behavior* 27, 4 (2006), 403–418. https://doi.org/10.1002/job.387 arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/job.387

[34] Wanyu Lin, Zhaolin Gao, and Baochun Li. 2020. Guardian: Evaluating Trust in Online Social Networks with Graph Convolutional Networks. In *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*. 914–923. https://doi.org/10.1109/INFOCOM41043.2020.9155370

[35] Wanyu Lin and Baochun Li. 2021. Medley: Predicting Social Trust in Time-Varying Online Social Networks. In *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications*. 1–10. https://doi.org/10.1109/INFOCOM42981.2021.9488814

[36] Shyhnan Liou and Xuezhao Lan. 2018. Situational salience of norms moderates cultural differences in the originality and usefulness of creative ideas generated or selected by teams. *Journal of Cross-Cultural Psychology* 49, 2 (2018), 290–302.

[37] Guanfeng Liu, Yan Wang, and Mehmet A. Orgun. 2012. Social Context-Aware Trust Network Discovery in Complex Contextual Social Networks. *Proceedings of the AAAI Conference on Artificial Intelligence* (2012).

[38] Guanfeng Liu, Yan Wang, Mehmet A. Orgun, and Huan Liu. 2012. Discovering Trust Networks for the Selection of Trustworthy Service Providers in Complex Contextual Social Networks. In *2012 IEEE 19th International Conference on Web Services*. 384–391. https://doi.org/10.1109/ICWS.2012.47

[39] Q. Liu, T. Luo, R. Tang, and S. Bressan. 2015. An efficient and truthful pricing mechanism for team formation in crowdsourcing markets. In *2015 IEEE International Conference on Communications*. 567–572.

[40] Yash Mahajan and Jin-Hee Cho. 2021. PRADA-TF: Privacy-Diversity-Aware Online Team Formation. In *2021 IEEE International Conference on Web Services (ICWS)*. 493–499. https://doi.org/10.1109/ICWS53863.2021.00069

[41] Leandro Soriano Marcolinon, Albert Xin Jiang, and Milind Tambe. 2013. Multi-Agent Team Formation: Diversity Beats Strength? *IJCAI International Joint Conference on Artificial Intelligence*, 279–285.

[42] F. McSherry and K. Talwar. 2007. Mechanism Design via Differential Privacy. In *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07)*. 94–103.

[43] Jessica R. Mesmer-Magnus and Leslie A. DeChurch. 2009. Information Sharing and Team Performance: A Meta-Analysis. *Journal of Applied Psychology* 94, 2 (1 Mar. 2009), 535–546. https://doi.org/10.1037/a0013773

[44] Susan Mohammed and Brad C. Dumville. 2001. Team mental models in a team knowledge framework: expanding theory and measurement across disciplinary boundaries. *Journal of Organizational Behavior* 22, 2 (2001), 89–106. https://doi.org/10.1002/job.86

[45] Susan Mohammed and Erika Ringseis. 2001. Cognitive Diversity and Consensus in Group Decision Making: The Role of Inputs, Processes, and Outcomes. *Organizational behavior and human decision processes* 85 (08 2001), 310–335. https://doi.org/10.1006/obhd.2000.2943

[46] Y. Narahari, Ramasuri Narayanam, Dinesh Garg, and Hastagiri Prakash. 2009. *Foundations of Mechanism Design*. Springer London, London, 1–131. https://doi.org/10.1007/978-1-84800-938-7_2

[47] Safi Ullah Nasir and Tae-Hyung Kim. 2020. Trust Computation in Online Social Networks Using Co-Citation and Transpose Trust Propagation. *IEEE Access* 8 (2020), 41362–41371. https://doi.org/10.1109/ACCESS.2020.2975782

[48] Mark Newman. 2003. The structure and function of complex networks. *SIAM Rev.* 45 (08 2003). https://doi.org/10.1137/S003614450342480

[49] M. E. J. Newman. 2006. Finding community structure in networks using the eigenvectors of matrices. *Phys. Rev. E* 74 (Sep 2006), 036104. Issue 3. https://doi.org/10.1103/PhysRevE.74.036104

[50] Kobbi Nissim, Claudio Orlandi, and Rann Smorodinsky. 2012. Privacy-Aware Mechanism Design. In *Proceedings of the 13th ACM Conference on Electronic Commerce (EC '12)*. 774–789. https://doi.org/10.1145/2229012.2229073

[51] Scott E. Page. 2007. *The Difference: How The Power of Diversity Creates Better Groups, Firms, Schools, and Societies*. Princeton University Press, Princeton, NJ.

[52] Scott E. Page. 2010. *Diversity and Complexity*.

[53] Sandra Petronio. 2006. Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information between Marital Couples. *Communication Theory* 1, 4 (03 2006), 311–335. https://doi.org/10.1111/j.1468-2885.1991.tb00023.x

[54] Anne Pieterse, Daan Knippenberg, and Dirk Van Dierendonck. 2012. Cultural Diversity and Team Performance: The Role of Team Member Goal Orientation. *Academy of Management Journal* 56 (07 2012), 782–804. https://doi.org/10.5465/amj.2010.0992

[55] Owen Sacco and John G. Breslin. 2014. In users we trust: towards social user interactions based Trust Assertions for the Social Semantic Web. *Social Network Analysis and Mining* 4 (2014), 1–15.

[56] Reijo Savolainen. 2011. Judging the quality and credibility of information in Internet discussion forums. *Journal of the American Society for Information Science and Technology* 62, 7 (2011), 1243–1256.

[57] Wanita Sherchan, Surya Nepal, and Cecile Paris. 2013. A Survey of Trust in Social Networks. *ACM Comput. Surv.* 45, 4, Article 47 (Aug. 2013), 33 pages. https://doi.org/10.1145/2501654.2501661

[58] M. C. Silaghi and D. Mitra. 2004. Distributed constraint satisfaction and optimization with privacy enforcement. In *Proceedings. IEEE/WIC/ACM International Conference on Intelligent Agent Technology*. 531–535.

[59] Steven Tadelis. 2013. *Game theory: an introduction*. Princeton university press.

[60] Jiliang Tang, Huiji Gao, Xia Hu, and Huan Liu. 2013. Exploiting Homophily Effect for Trust Prediction. In *Proceedings of the Sixth ACM International Conference on Web Search and Data Mining (WSDM '13)*. 53–62. https://doi.org/10.1145/2433396.2433405

[61] Sabina Tasheva and Amy J. Hillman. 2019. Integrating Diversity at Different Levels: Multilevel Human Capital, Social Capital, and Demographic Diversity and Their Implications for Team Effectiveness. *Academy of Management Review* 44, 4 (2019), 746–765. https://doi.org/10.5465/amr.2015.0396

[62] Denis Trapido. 2015. How novelty in knowledge earns recognition: The role of consistent identities. *Research Policy* 44, 8 (2015), 1488 – 1500. https://doi.org/10.1016/j.respol.2015.05.007

[63] Gerben S Van Der Vegt and J Stuart Bunderson. 2005. Learning and performance in multidisciplinary teams: The importance of collective team identification. *Academy of management Journal* 48, 3 (2005), 532–547.

[64] Ruth van Veelen and Elze G Ufkes. 2019. Teaming up or down? A multisource study on the role of team identification and learning in the team diversity–performance link. *Group & Organization Management* 44, 1 (2019), 38–71.

[65] W. Wang, J. Jiang, B. An, Y. Jiang, and B. Chen. 2017. Toward Efficient Team Formation for Crowdsourcing in Noncooperative Social Networks. *IEEE Transactions on Cybernetics* 47, 12 (Dec 2017), 4208–4222.

[66] X. Wang, Z. Zhao, and W. Ng. 2016. USTF: A Unified System of Team Formation. *IEEE Transactions on Big Data* 2, 1 (Mar. 2016), 70–84.

[67] A. R. Wellens. 1989. Effects of telecommunication media upon information sharing and team performance: some theoretical and empirical observations. In *Proceedings of the IEEE National Aerospace and Electronics Conference*, Vol. 2. 726–733.

[68] Mason Wright and Yevgeniy Vorobeychik. 2015. Mechanism Design for Team Formation. In *Proceedings of the Twenty-Ninth AAAI Conference on Artificial Intelligence (AAAI'15)*. AAAI Press, 1050–1056.

[69] Xiaokui Xiao, Guozhang Wang, and Johannes Gehrke. 2011. Differential Privacy via Wavelet Transforms. *IEEE Trans. on Knowl. and Data Eng.* 23, 8 (Aug. 2011), 1200–1214. https://doi.org/10.1109/TKDE.2010.247

[70] Xiaolong Xu, Qingxiang Liu, Xuyun Zhang, Jie Zhang, Lianyong Qi, and Wanchun Dou. 2019. A Blockchain-Powered Crowdsourcing Method With Privacy Preservation in Mobile Environment. *IEEE Transactions on Computational Social Systems* 6, 6 (2019), 1407–1419. https://doi.org/10.1109/TCSS.2019.2909137

Supplement Document: Privacy-Preserving and Diversity-Aware Trust-based Team Formation in Online Social Networks

YASH MAHAJAN, JIN-HEE CHO, and ING-RAY CHEN, Virginia Tech, USA

ACM Reference Format:
Yash Mahajan, Jin-Hee Cho, and Ing-Ray Chen. 2024. Supplement Document: Privacy-Preserving and Diversity-Aware Trust-based Team Formation in Online Social Networks. 1, 1 (April 2024), 7 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

A ADDITIONAL NUMERICAL RESULTS & ANALYSIS

In this appendix, we discuss the experimental results on the IMDb dataset [1] (Section VI-B). We demonstrate the simulation results and analyze their overall trends regarding the effects of different task types, compromising privacy, and different team sizes when the IMDb dataset [1] is used.

A.1 Effect of Different Task Types

Fig. 1 shows the effect of different task types on the performance of the seven different candidate team selection (CTS) methods based on the five metrics. Confirming the trend observed with the *Netscience* dataset, we observe that with the *IMDB dataset* ASW is still found to be higher than ESW, as players try to maximize their utility by compromising their privacy during the actual task execution. Similarly, with the same reasoning as that of the *Netscience* dataset (see Appendix A.1), APPL is lower than EPPL for all the different CTS methods. Interestingly, we observe that USD still performs the best, however contrarily IF-CTS performs equally with USD. IF-CTS has the highest ASW as well as the lowest APPL indicating that information sharing behaviour is beneficial to the players, given the players are rewarded appropriately.

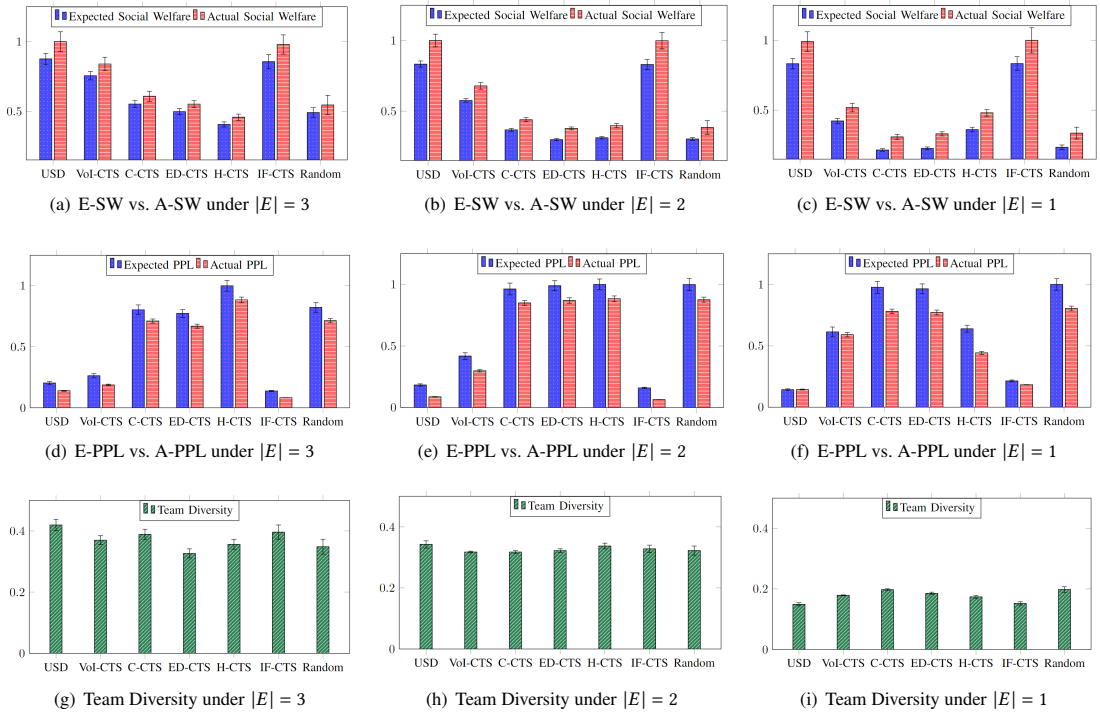
Comparing Fig 1(i) with 1(c) and 1(f), we can see that high diversity is inversely proportional to the team performance when the number of domains is equal to 1 ($|E| = 1$). The inverse proportionality is because in a single domain or less domain task, high diversity leads to higher potential privacy loss (see Fig. 1(f)) as team members are localised into a single domain.

A.2 Effect of Compromising Privacy

Fig. 2 shows the effects of varying the lower bound of compromising a team member's privacy preferences (pc_i) under the seven different CTS methods based on the five metrics. Like with the previous dataset, USD performs the best, followed by IF-CTS in terms of ESW and ASW, as seen in Figs 2(a) and 2(b). Interestingly, IF-CTS outperforms USD when the pc_i decreases, which is when the players have a higher margin to be dishonest when reporting their privacy preferences. From Fig. 2(b), we can see that when $pc_i \in [0.2, 0.6]$, IF-CTS performs better than USD, but as pc_i keeps increasing,

Authors' address: Yash Mahajan, yashmahajan@vt.edu; Jin-Hee Cho, jicho@vt.edu; Ing-Ray Chen, irchen@vt.edu, Virginia Tech, 7054 Haycock Rd, Falls Church, Virginia, USA, 22043.

Manuscript submitted to ACM



(a) E-SW vs. A-SW under $|E| = 3$ (b) E-SW vs. A-SW under $|E| = 2$ (c) E-SW vs. A-SW under $|E| = 1$

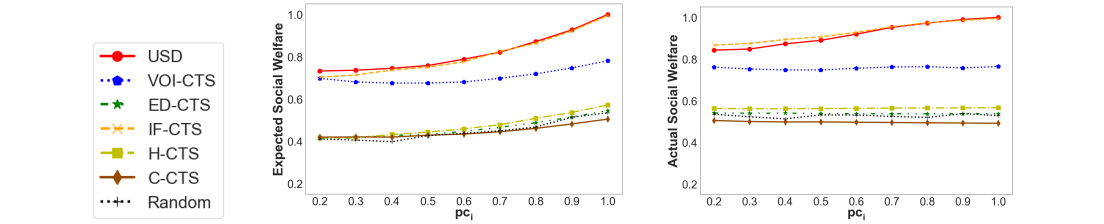
(d) E-PPL vs. A-PPL under $|E| = 3$ (e) E-PPL vs. A-PPL under $|E| = 2$ (f) E-PPL vs. A-PPL under $|E| = 1$

(g) Team Diversity under $|E| = 3$ (h) Team Diversity under $|E| = 2$ (i) Team Diversity under $|E| = 1$

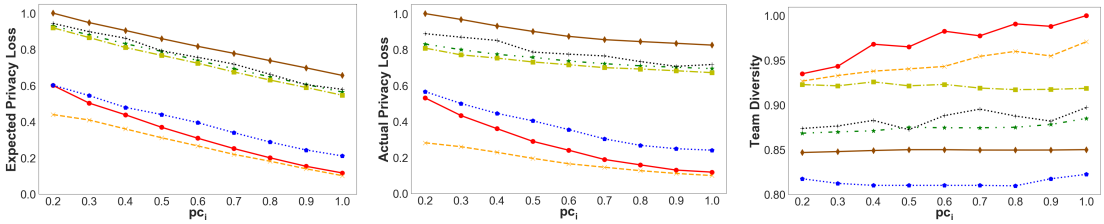
Fig. 1. Performance comparison of different candidate team selection (CTS) methods based on the five metrics, including expected social welfare (E-SW), actual social welfare (A-SW), expected potential privacy loss (E-PPL), actual potential privacy loss (A-PPL), and team diversity, when the number of domains varies with $|E| = 3, 2$ or 1 and the corresponding task composition, $\mathbf{L}(e_i) = [1, 1, 1]$, $[3/2, 3/2]$, or [3], respectively. (a), (d), and (g) are under $|E| = 3$, (b), (e), and (h) are under $|E| = 2$, and (c), (f), and (i) are under $|E| = 1$. Note that the lower bound weight of a revealed privacy preference (pc_i) is set to $= 0.8$, and the number of hops in an online trust network (k-hop) is set to 5.

USD starts performing better, indicating that players tend to compromise their privacy more if the equivalent reward is higher. Moreover, comparing the IF-CTS scheme, where the final team is selected based on the participant's privacy preferences, in terms of SW and PPL, we observe that the slope for IF-CTS is the highest in Figure 2(d), which shows the effect of pc_i on PPL. The overall trend for ESW, as well as ASW, is that as pc_i increases and players report a privacy preference close to their actual privacy preferences, we notice that both ESW and ASW increase, similar to what we observe with the Netscience dataset.

From Figs. 2(c) and 2(d), we also observe that the general trend for both EPPL and APPL is the same as that of the Netscience dataset, which decreases as pc_i increases. Corroborating the results from both datasets, we can confirm that 'privacy preference' is a significant factor in overall social welfare, and each individual participating acts selfishly to maximize their reward given their privacy preferences. Additionally, from all the rest of the CTS schemes, VoI performs the best, whereas H-CTS, ED-CTS, and C-CTS are relatively less affected by the increase in pc_i, which is expected given the fact that all the above schemes don't consider the privacy preferences, and consequently the pc_i when selecting the final team. The low variance observed is due to the difference in candidate pools available due to the increase in pc_i.

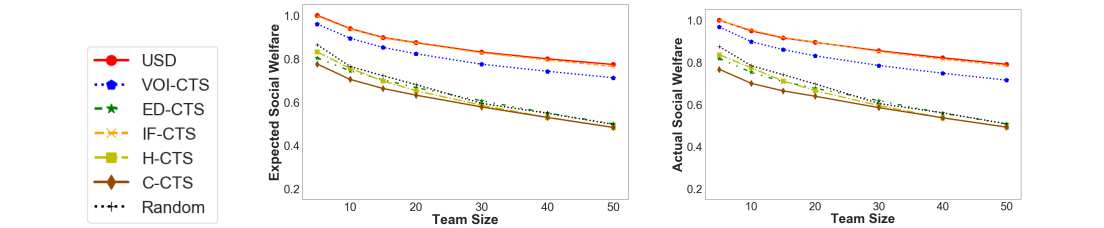


(a) Expected social welfare (b) Actual social welfare

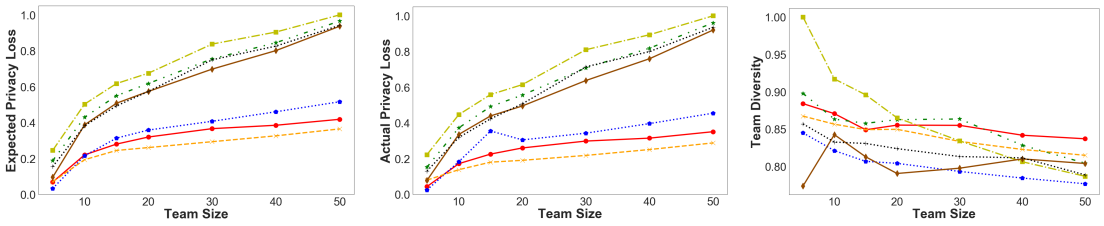


(c) Expected PPL (d) Actual PPL (e) Team diversity

Fig. 2. Comparison of different candidate team selection (CTS) methods based on the five metrics under varying the lower bound weight of a revealed privacy preference (pc_i), where the environment is set as the number of domains ($|E|$) = 3, pc_i = 0.8, and task composition ($\mathbf{L}(e_i) = [1, 1, 1]$) under a 5-hop trust network (i.e., $k = 5$).



(a) Expected social welfare (b) Actual social welfare

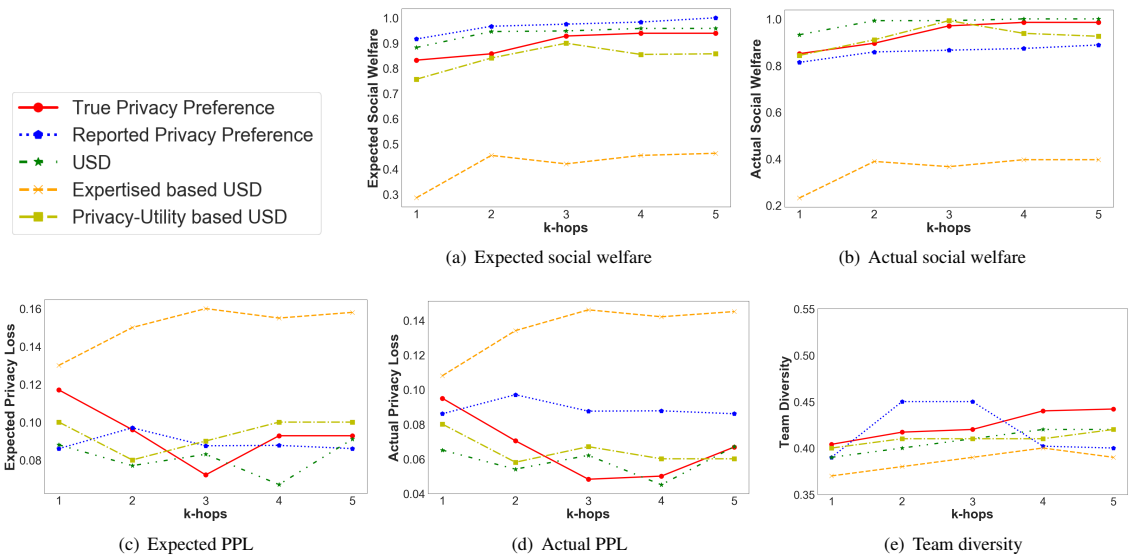


(c) Expected PPL (d) Actual PPL (e) Team diversity

Fig. 3. Comparison of different candidate team selection (CTS) methods based on the five metrics under varying team size, where the environment is set as the number of domains ($|E|$) = 3, pc_i = 0.8, and task composition ($\mathbf{L}(e_i) = [1, 1, 1]$) under a 5-hop trust network.

A.3 Effect of Different Team Sizes

In Fig. 3, we show how different team sizes affect the performance of different CTS methods in terms of the five metrics. Comparing ESW and ASW against EPPL and APPL (Figs 3(a)-3(d)), we can infer the following observation. The overall



(a) Expected social welfare (b) Actual social welfare

(c) Expected PPL (d) Actual PPL (e) Team diversity

Fig. 4. Comparison of various ablation methods based on the five metrics under varying k in k-hops for network exploration, where the environment is set as the number of domains ($|E|$) = 3, pc_i = 0.8, and task composition ($\mathbf{L}(e_i) = [1, 1, 1]$)

trend for both ASW and ESW is that as the team size increases, the social welfare decreases. This is expected as a larger team for the same task requirement will distribute its reward amongst more team members, consequently leading to lower social welfare. Moreover, the general trend observed with respect to EPPL and APPL is that the potential privacy loss increases exponentially as the team size increases and more individuals have potential access to sensitive information. From the given figures, USD and IF-CTS perform the best, followed by VOI-CTS, with the rest of the CTS schemes performing comparably.

Fig. 3(e) shows the effect of team size on the diversity. From the figure, we can infer that team diversity decreases with increased team size. This decrease is directly correlated with the team size, as with a larger team, the diversity of individuals decreases, and consequently, the team diversity decreases. To confirm this, we can observe the H-CTS scheme, which forms the final team based on the cosine similarity of the expertise with the required expertise. H-CTS decreases drastically as more and more similar players are selected and the team size increases. Overall, ED-CTS has the highest team diversity, as expected, followed by USD and IF-CTS. By comparing the results of varying pc_i, we can confirm a direct correlation between team diversity and social welfare.

Fig. 4 illustrates the impact of varying the exploration depth (k-hops) on network analysis, employing five distinct metrics used in this work. The methods evaluated include adherence to true privacy preferences, reported privacy preferences, and three variations of the Utility-based Serial Dictatorship (USD) Coordination and Trust Scheme (CTS) – specifically focusing on combined expertise and privacy utilities, expertise-based social welfare, and privacy-based social welfare. The observations from Fig. 4(a)-(e) as k increases reveal a nuanced interplay between social welfare, privacy preservation, and network exploration dynamics. Specifically, the USD scheme outperforms others in achieving the highest Actual Social Welfare while ranking second for Expected Social Welfare. This indicates its efficacy in balancing utility gains against privacy risks. Increasing the number of explored participants generally enhances social welfare; however, it concurrently raises the likelihood of privacy breaches. This leads to a decrease in players' Privacy Preference

Levels (PPL), reflecting a heightened prioritization of privacy with increasing privacy risks. Furthermore, the exploration extension results in greater team diversity, underscoring the trade-off between expansive network exploration and privacy preservation. Notably, the expertise-based USD method lags in performance, suggesting a predominant player preference for privacy over expertise in social welfare considerations. Paradoxically, adherence to reported privacy preferences results in higher privacy losses, highlighting discrepancies between reported and actual preferences. Lastly, the minimal distinction between 4-hop and 5-hop explorations suggests a plateau in network coverage efficiency beyond a certain threshold, with approximately 95% of the network being explored within 4 hops. This consolidation underscores the complex dynamics at play in optimizing social welfare within privacy-aware network explorations.

B BINOMIAL SUBJECTIVE OPINIONS AND THEIR FUSION OPERATORS

This appendix elucidates the binomial subjective opinion framework within Subjective Logic (SL) alongside two pivotal fusion operators deployed in the k-hop trust network, as delineated in Section V.F of the main manuscript.

In this framework, a binomial opinion represented by $\omega_B^A = (b_B^A, d_B^A, u_B^A, a_B^A)$ encapsulates the extent to which entity A trusts (b_B^A), distrusts (d_B^A), or remains uncertain (u_B^A) about entity B's trust in a given context, ensuring that $b_B^A + d_B^A + u_B^A = 1$. The term a_B^A denotes the base rate probability, reflecting A's initial belief or inclination towards B, typically set as $a_B^A = 1/2$ to represent an equitable prior distribution for both trust and distrust components. The projected probability of A's trust in B is thus calculated as:

$$P_B^A = b_B^A + a_B^A u_B^A. \tag{1}$$

This model also infers A's distrust in B as $d_B^A + a_B^A u_B^A$, equivalently rendered as $1 - P_B^A$, given the sum of $b_B^A + d_B^A + u_B^A$ equals 1. In scenarios requiring the assessment of a Mechanism Designer's (MD) trust in a user within an Online Social Network (OSN) through indirect trust chains (e.g., A trusts B, B trusts C, and C trusts D), we aim to calculate the MD's (denoted as A) trust in a distantly connected user (D). This process utilizes the concept of referral trust and the discounting operator as follows:

The discounting operator facilitates the determination of indirect trust by amplifying the uncertainty component in the trust calculation, adhering to the formula in Eq. (1). Considering three agents A, B, and C, with A's referral trust in B denoted by ω_B^A and B's functional trust in C by ω_C^B, the indirect trust of A in C, through B, is calculated using $\omega_C^{A:B} = \omega_B^A \otimes \omega_C^B$, where $\otimes$ signifies the discounting operator. The resulting indirect trust $\omega_C^{A:B}$ is defined by $(b_C^{A:B}, d_C^{A:B}, u_C^{A:B}, a_C^{A:B})$, with the expressions:

$$\begin{aligned} b_C^{A:B} &= b_B^A b_C^B, \quad d_C^{A:B} = b_B^A d_C^B, \\ u_C^{A:B} &= d_B^A + u_B^A + b_B^A u_C^B, \quad a_C^{A:B} = a_C^B. \end{aligned} \tag{2}$$

When faced with multiple direct trust assessments from users familiar with the target user, the MD utilizes the consensus operator proposed in SL to amalgamate these diverse trust valuations into a unified trust decision. This operator ensures a comprehensive and balanced trust evaluation by integrating multiple perspectives.

The *consensus operator* is used to obtain trust by combining two beliefs into one with reduced uncertainty in the expectation value. Assuming A's trust in C to be $\omega_C^A = (b_C^A, d_C^A, u_C^A, a_C^A)$ and B's trust in C to be $\omega_C^B = (b_C^B, d_C^B, u_C^B, a_C^B)$, the

consensus between ω_C^A and ω_C^B is denoted by $\omega_C^{A\oplus B} = (b_C^{A\oplus B}, d_C^{A\oplus B}, u_C^{A\oplus B}, a_C^{A\oplus B})$ with

$$b_C^{A\oplus B} = \frac{b_C^A u_c^B + b_C^B u_C^A}{\beta}, \quad d_C^{A\oplus B} = \frac{d_C^A u_c^B + d_C^B u_C^A}{\beta}$$
$$u_C^{A\oplus B} = \frac{u_C^A u_c^B}{\beta}, \quad a_C^{A\oplus B} = a_C^A \tag{3}$$

where $\beta = u_C^A + u_C^B - u_C^A u_B^A$.

With the help of the discounting and consensus operators [2], the MD's opinion in B, $\omega_B^{MD} = \{b_B^{MD}, d_B^{MD}, u_B^{MD}, a_B^{MD}\}$, can be obtained to derive the MD's trust based on Eq. (**??**). From the trust derived and calculated, the top ϕ candidate members based on Eq. (**??**) are selected for the next round of selections. Note that the considered paths are restricted to only those independent paths where no user appears more than once.

For simplicity, we initialize each user's trust value based on both expertise preference and willingness to share information based on privacy preference. For example, the MD's belief in trusting B via direct experience, in terms of whether B will be relevant for the given task requiring E set of expertise domains, is formulated by:

$$b_B^{MD} = \frac{\sum_{h\in E}\left(w_e \theta_h^e + w_s(1-\theta_h^p)\right)}{|E|}, \tag{4}$$

where $w_e + w_s = 1$. Assuming with a fairly small uncertainty u_B^{MD} (e.g., $K/(N+K)$ where $K = 2$ is commonly assumed for a binomial opinion and N is sufficiently large), we simply derive $d_B^{MD} = 1 - (b_B^{MD} + u_B^{MD})$ based on the requirement of additivity with $b_B^{MD} + d_B^{MD} + u_B^{MD} = 1$.

To elucidate the computation of indirect trust and the aggregation of trust evidence using the consensus operator, we have meticulously detailed the procedures in Algorithm 1.

REFERENCES

[1] IMDb Datasets. [n. d.]. IMDb Datasets. ([n. d.]). https://datasets.imdbws.com/ Last Accessed on May 10, 2023.

[2] Audun Jøsang. 2016. *Subjective Logic: A Formalism for Reasoning Under Uncertainty* (1st ed.). Springer Publishing Company, Incorporated.

Algorithm 1 Compute Indirect Trust and Aggregate via Consensus

Require: Trust network graph G, source node A, target node D, hop limit k
Ensure: Aggregated trust opinion of A towards D

function ComputeIndirectTrust(A, D, k)
  if $k = 0$ **then**
    return Direct trust opinion of A towards D if available
  end if
  Initialize an empty list *opinions*
  for each node B that A trusts directly **do**
    $\omega_B^A \leftarrow$ direct trust opinion of A towards B
    for each node C that B trusts **do**
      $\omega_C^B \leftarrow$ direct trust opinion of B towards C
      $\omega_C^{A:B} \leftarrow$ Discount(ω_B^A, ω_C^B) ▷ Apply discounting operator
      if $C = D$ or further hop possible **then**
        opinions.append($\omega_C^{A:B}$)
      end if
    end for
  end for
  aggregatedOpinion $\leftarrow$ Consensus(*opinions*)
  return *aggregatedOpinion*
end function
function Discount(ω_B^A, ω_C^B)
  Extract $b_B^A, d_B^A, u_B^A, a_B^A$ from ω_B^A
  Extract $b_C^B, d_C^B, u_C^B, a_C^B$ from ω_C^B
  Compute $b_C^{A:B}, d_C^{A:B}, u_C^{A:B}$ using given formulas
  return $(b_C^{A:B}, d_C^{A:B}, u_C^{A:B}, a_C^B)$
end function
function Consensus(*opinions*)
  Aggregate all opinions in *opinions* list according to consensus rules
  return Aggregated opinion
end function