Manipulation-Resistant Mechanism Design for Strategic Network Diffusion

Wen Shen[1], **Ke Yan**[2] and **Cristina V. Lopes**[1]
[1]University of California, Irvine, Irvine, CA 92697, USA
[2]China Jiliang University, Hangzhou 310018, China
wen.shen@uci.edu, yanke@cjlu.edu.cn, lopes@ics.uci.edu

Abstract

Strategic network diffusion, a marketing strategy that allows stakeholders to promote their desired outcomes by offering incentives to successful referrals, plays an important role in modern society. Unfortunately, existing incentive mechanisms for for strategic network diffusion are often vulnerable to manipulations such as false-name attacks and collusion. To address this problem, we introduce a new class of mechanisms called the *Generalized Contest Mechanism* (GCM). We show that the GCM are resistant to both false-name attacks and collusion. It also satisfies other desirable properties such as budget constraints, individual rationality, monotonicity, and subgraph constraints. Experiments on real-world social network datasets show that the GCM not only can beat the state-of-the-art mechanisms in terms of total efforts but is also more robust to false-name attacks and collusive manipulations. Our work brings new insights into how to counter manipulations with proper design of competitions.

1 Introduction

Strategic network diffusion refers to the marketing strategy in which a stakeholder (e.g., a seller, a task owner) incentivizes participants to spread the designated information across their social networks to achieve her desired outcomes [Galeotti and Goyal, 2009; Shen *et al.*, 2019]. Such viral marketing strategy is usually more efficient and effective than traditional advertisement because referral marketing is usually more credible to potential customers [Berman, 2016]. It can also have access to new customers that traditional marketing methods may not reach, and provide better matching of potential users' needs to a product or service [Berman, 2016]. Moreover, previous studies show that the value and contribution of participants acquired through referrals are higher than those of non-referred customers [Schmitt *et al.*, 2011]. Due to these benefits, strategic network diffusion has become a powerful tool for stakeholders to promote their agendas and has broad applications in many domains such as crowdsourcing [Pickard *et al.*, 2011], disaster management [Gao *et al.*, 2011; Besaleva and Weaver, 2013], health care [De Choudhury *et al.*, 2013], e-commerce [Constantinides *et al.*, 2008; Tiago and Veríssimo, 2014; Zhao *et al.*, 2018], economic diversification [Alshamsi *et al.*, 2018] and political campaigns [Enli, 2017].

To encourage early adoption and attract participation from influential players, stakeholders usually provide rewards (e.g., discounts, free products, event tickets or other monetary incentives) for both direct and indirect referral [Emek *et al.*, 2011; Pickard *et al.*, 2011]. For instance, if Alice has referred Bob and Bob has invited Dana, both Alice and Bob are rewarded for Dana's contributions (e.g., purchases, labor work) toward the stakeholders' goals. Mechanisms that provide incentives to the successful referral chains are often called *geometric mechanisms* [Emek *et al.*, 2011; Drucker and Fleischer, 2012].

Geometric mechanisms have many important applications ranging from disaster response to product promotion [Besaleva and Weaver, 2013; Shen *et al.*, 2019]. However, they are often vulnerable to manipulations such as false-name-attacks and collusion [Drucker and Fleischer, 2012]. In strategic network diffusion, a false-name attack refers to an agent's strategy to create multiple false identities in order to increase his diffusion rewards, while collusion is a manipulative strategy that a group of agents communicate to jointly limit the competition (e.g., reducing the task efforts). False-name attacks and collusion are pervasive in social networks since players may create multiple accounts with no or minimal cost, and may communicate with their social ties to reduce the competition if they can make profits [Drucker and Fleischer, 2012; Naroditskiy *et al.*, 2014; Ferrara *et al.*, 2016]. Nevertheless, Both manipulations are undesirable because they not only diminish stakeholders' ability to implement their goals but also reduce other honest players' payoffs [Drucker and Fleischer, 2012; Shen *et al.*, 2019]. Besides, agents' manipulative behaviors may crash the markets [Tang *et al.*, 2011].

Our contributions: To counter false-name attacks and collusion in strategic network diffusion, we introduce a new mechanism called the *Generalized Contest Mechanism* (GCM). In doing so, we first characterize a necessary and sufficient condition for a reward mechanism to be false-name-proof: the reward function should be superadditive in terms of the diffusion contributions. We then identify a sufficient condition for a mechanism to be collusion-proof: the total

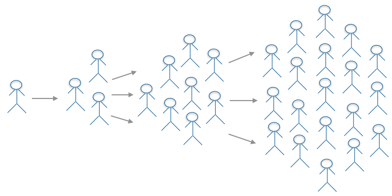


Figure 1: A simple illustration of strategic network diffusion.

diffusion rewards for the referrers of a player should be increasing and bounded above in terms of the total task efforts of the referrers. Finally, we integrate both conditions into a single mechanism. We demonstrate that the resulting mechanism is both false-name-proof and collusion-proof. It also satisfies other desirable properties such as budget constraints, individual rationality, monotonicity, and subgraph constraints. Numerical results demonstrate that the GCM can outperform the state–of-the-art multi-winner contests (MWC) mechanism [Shen *et al.*, 2019] in terms of total task efforts with a variety of supperadditive functions and increasing and bounded functions. The GCM is also more robust to false-name attacks and collusive manipulations than the MWC mechanism. Our work provides a systematic approach to manipulation-resistant mechanism design.

2 Strategic Network Diffusion

Before introducing the mechanism design problem, we first describe key notations.

2.1 Notations

We model referral processes with a *directed acyclic graph* (DAG) $G = (V, E)$. In a DAG G, nodes V represent the players that may voluntarily participate in the strategic diffusion to increase their utilities. To maximize their profits, the players need to both complete the principal's designated tasks (e.g., buying a product, collecting data, crowdfunding, manhunt, and software development) and invite their neighbors to participate. Edges E correspond to the referral relationships.

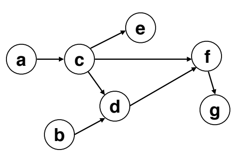


Figure 2: A typical directed acyclic graph for modeling strategic network diffusion.

For any two nodes $u, v \in V (v \neq u)$, if a path from u to v exists, then u is a *predecessor* of v, and v is a *successor* of u. In this case, player v's decision to contribute to the principal's tasks is (partially) due to u's referral. We write the distance between u and v by $dist(u, v) \in \mathbb{Z}_{>0}$. The distance between v and itself is 0 (i.e., $dist(v, v) = 0$). If there is no path from u to v, then $dist(u, v) = +\infty$. If $dist(u, v) = 1$, we say u is a *direct predecessor* of v, and v is a *direct successor* of u. For each node $v \in V$, the number of its direct predecessors is its *indegreee* $deg^-(v)$, and the number of its direct successors is its *outdegree* $deg^+(v)$. The set of v's all predecessors $I_v^- = \{u \in V : 0 < dist(u, v) < +\infty\}$. Similarly, the set of v's all successors $I_v^+ = \{u \in V : 0 < dist(v, u) < +\infty\}$. The subgraph rooted at v includes node v and all its successors. That is, $G_v = (V_v, E_v)$, where $V_v = \{v\} \cup I_v^+$, and $E_v \subseteq E$.

In a referral DAG $G = (V, E)$, if a player v makes irreversible contributions to the principal's designated tasks (e.g., purchasing products without returns, collecting data, manhunt, and software development), then player v exerts task efforts $t_v \in \mathbb{R}_{\geq 0}$. Player v can choose to spread the information of the tasks to his successors and invite them to participate to maximize his profits. If one of his successors $u \in I_v^+$ also exert *task efforts* $t_u \in \mathbb{R}_{\geq 0}$, then we say player v makes *diffusion contributions* $d_v \in \mathbb{R}_{\geq 0}$. In strategic network diffusion, a player's decision to exert positive task efforts may be due to either a single referral chain or multiple referrals. This setting is more general than the tree setting where a player's decision to make contributions can be only traced from a single referral chain. For example, it is likely that a customer will use a mobile application only if more than one of his friends have actively used it and have sent invitations to him. Similar to the tree setting, a player in a referral network is also permitted to invite multiple neighbors to increase his diffusion contributions.

In practice, players' task efforts are usually measurable and verifiable to the principal. For instance, the principal can quantify a player's task efforts according to the pieces of the tasks or the amount of time spent on the tasks. We thus assume that players' task efforts are observable in our model. However, the diffusion contributions are often difficult or even unfeasible to verify because strategic players can generate fake referrals with no or minimal efforts by creating multiple false accounts or identities to form extra referral chains.

2.2 The Mechanism Design Problem

We consider a principal aims to maximize the aggregated task efforts via strategic network diffusion. At the beginning, the principal selects a number of participants $S \subseteq V$ in a social network $G = (V, E)$ as the seed nodes. The optimal selection of seed nodes in a social network falls into the broad categories of influence maximization problems [Kempe *et al.*, 2003]. The influence maximization problem is proven to be NP-hard even the diffusion model is known as a priori, but one can address it with approximation algorithms [Chen *et al.*, 2009]. Alternatively, the principal can choose the seed nodes arbitrarily if she has no prior knowledge of the social network.

The seed participants may voluntarily perform the tasks and invite their neighbors in the social network to participate. If a player $v \in G = (V, E)$ exerts task efforts t_v, he will receives a task reward $\pi_t(v)$ from the principal. If v also spread the information to his successors and one of his successors $u \in I_v^+$ also exerts task efforts, then the referrer v will also receive a diffusion reward $\pi_d(v, u)$. Let $\pi_d(v)$ denote the total diffusion rewards that v receives, we have $\pi_d(v) = \sum_{u \in I_v^+} \pi_d(v, u)$. Player v's total rewards $\pi(v) \in \mathbb{R}_{\geq 0}$ include both the task rewards and the diffusion rewards, i.e., $\pi(v) = \pi_t(v) + \pi_d(v)$.

In our model, we assume that the valuation of a player is linear in the rewards he receives and the cost he pays is linear in the efforts he has contributed. Let $c(v) \in \mathbb{R}_{\geq 0}$ denote the total cost for player v to exert task efforts t_v and diffusion contributions d_v, player v's total cost $c_v = t_v + d_v$. Let $\rho_v \in \mathbb{R}_{\geq 0}$ denote the parameter that measures the relative cost for player v to make a unit diffusion contribution compared with the cost of the unit task effort, we have $d_v = \rho_v \cdot t_v$. Hence, $c(v) = (1 + \rho_v) \cdot t_v$. Let Θ_v be player v's type space for the total cost c_v, then the type space for all the players in a social network $G = (V, E)$ is $\Theta = (\Theta_v)_{v \in V}$. In practice, the cost for information diffusion is relatively insignificant compared with the task efforts. That is, $0 \leq \rho_v << 1$. For example, a player share the information via mass messages to all the target neighbors.

Player v's utility $U(v) = \pi(v) - \zeta_v \cdot c_v$, where $\zeta_v \in \mathbb{R}_{\geq 0}$ is a private coefficient that quantifies player v's marginal cost for exerting extra unit effort. Let $\delta_v = \zeta_v \cdot (1 + \rho_v)$, we have player v's utility

$$U(v) = \pi(v) - \delta_v \cdot t_v \ , \tag{1}$$

where $\delta_v \in \mathbb{R}_{\geq 0}$ is a private parameter that quantifies player v's marginal cost for exerting extra unit effort. In practice, performing manipulations also incur costs. However, such cost can be incorporated into the private cost coefficient that is privately known to the player himself [Shen *et al.*, 2019].

In strategic network diffusion, the principal is interested in an incentive mechanism π that determines the rewards for each player that has exerted efforts (See Def. 1). In practice, an incentive mechanism must satisfy several constraints (e.g., budget feasibility, and voluntary participation) to be implementable. In this paper, we are particularly interested in a mechanism that is resistant to manipulations such as false-name attacks and collusion.

Definition 1 (Incentive Mechanism)**.** *An incentive mechanism π for strategic network diffusion in a social network $G = (V, E)$ is a payment rule $\pi = (\pi(v))_{v \in V}$, where $\pi(v) : \Theta \to \mathbb{R}$ is the payment function for agent v.*

3 Design Constraints

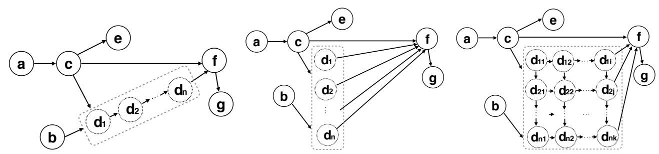
In this section, we formally introduce the two primary constraints for manipulation-resistant mechanism design: false-name proofness and collusion-proofness. We also discuss other constraints such as individual rationality, budget constraint, monotonicity and subgraph constraint.

3.1 False-Name Proofness

In strategic network diffusion, a strategic agent may create false identities (i.e., replicas) to form fake referrals to maximize his profits. In a referral graph $G = (V, E)$, a false-name attack for player $v \in G$ is a split at node v that results in a new graph $G' = (V', E')$ and a set of replicas $R \subseteq V'$. For the resulting graph G', if we collapse R into the single node v in G' we get the graph G.

Definition 2 (False-Name Attack)**.** *In a DAG $G = (V, E)$, we say a graph $G' = (V', E')$ and a set of replicas $R \subseteq V'$ are a* false-name attack *for player v in the graph G if $v \in V'$ and when we collapse R into the single node v in G' we get the graph G.*

In strategic network diffusion, there are generally three types of false-name attacks: *serial split*, *parallel split* and *hybrid split*. Serial split forms a long referral chain with one replica referring to another (See Fig. 4a). Parallel split duplicates the replicas in parallel to increase the count of referral relationships (See Fig. 4b). Hybrid split consists of both serial attacks and parallel attacks (See Fig. 3c). False-name attacks are detrimental to both the principal and other honest players. They can even crash the markets if most of the participants participate in the false-name attacks. Therefore, it is desirable that the incentive mechanism satisfies the *false-name-proofness* property.



(a) Serial split (b) Parallel split (c) Hybrid split

Figure 3: Three types of false-name attacks at node d.

An incentive mechanism is false-name-proof if under the mechanism false-name attacks are unprofitable for each player in the referral graph. Specifically, the total rewards that $v \in G = (V, E)$ receives are greater than or the same as the sum of the rewards obtained by the replicas of v due to a split of G at node v (See Def. 3).

Definition 3 (False-Name-Proofness)**.** *An incentive mechanism π is false-name-proof for all $v \in G : \pi(v) \geq \sum_{r \in R} \pi(r)$, where R is the set of replicas due to a false-name attack at node v.*

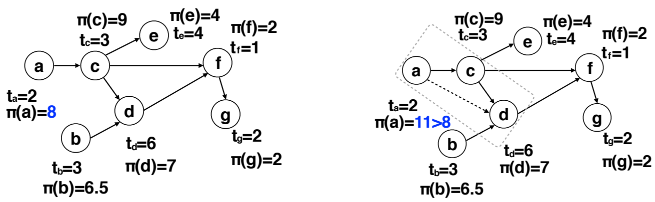
3.2 Collusion-Proofness

Different from false-name attacks, a collusion in a referral graph $G = (V, E)$ is a coalition strategy that makes at least one of the weakly connected players better off by changing the internal network structure (i.e., adding or removing the referral relationships) or reducing the task efforts of the coalition (See Def. 4).

Definition 4 (Collusion)**.** *A collusion is a coalition strategy of weakly connected players that makes at least one player in the coalition better off by changing the internal network structure or reducing the task efforts of the coalition. Formally, in a DAG $G = (V, E)$, we say a graph $G' = (V', E')$ and a set of players $P \subseteq V'$ are a collusive coalition if under the incentive mechanism π, we have*

- *for each pair $u, v \in P$, there exists either a directed path from u to v in G, or a directed path from v to u in G.*
- *for each $v \in V'$, we have $v \in V$.*
- *for each $u, v \in V \setminus P$, if $uv \in E$, then $uv \in E'$;*
- *for each $v \in V \setminus P$, the task efforts t_v remain unchanged.*
- *for each $v \in P$, the task efforts t_v do not increase.*
- *There exist at least one $v \in P$ such that we have $U(v) < U'(v)$, where $U(v)$ is player v's utility when there is no collusion, and $U'(v)$ is player v's utility when v is in*

a collusive coalition. Other members' utilities do not change.



(a) No collusion

(b) Collusion (a, c and d)

Figure 4: An example of strategic network diffusion with no collusion and with collusion under a typical geometric mechanism.

A group of players may reduce the task efforts, or change the internal network structure, or use combination of these two strategies to form a collusive coalition. Note that there may be coalitions that can increase the total efforts, which are usually beneficial to the principal. Such behaviors are typically not categorized as collusion.

Collusion is harmful to both the principal and other honest players. The collusive behavior depletes the principal's budgets with less task efforts. When the budget is fixed, under many mechanisms, the budget allocated to other honest players become less. Therefore, the incentive mechanism should satisfy the *collusion-proofness* property. An incentive mechanism is collusion-proof if under the mechanism no group of weakly connected players can collude to make at least one member of the group better off by changing the internal network structure or reducing the task efforts without making the remaining members worse off (See Def. 5).

Definition 5 (Collusion-Proofness)**.** *An incentive mechanism π is collusion-proof if no group of weakly connected players $P \subseteq V$ can increase the utilities for at least one player in the coalition without reducing the utilities for any other member in the group through changing the internal network structure or reducing the task efforts of the coalition.*

3.3 Other Constraints

To be implementable in practice, an incentive mechanism should also satisfy other desirable constraints, such as *voluntary participation*, *budget constraint*, *monotonicity*, and *subgraph constraint*.

A player should not be forced to participate in a mechanism. That is, a mechanism needs to incentivize or at least not penalize participation. An incentive mechanism satisfies the *voluntary participation* property if each player $v \in G = (V, E)$ receives positive (expected) diffusion rewards for each successful referral.

Definition 6 (Voluntary Participation)**.** *An incentive mechanism π satisfies voluntary participation if for each player $v \in G = (V, E)$ with $d_v \geq 0$, we have $U(v) \geq 0$, and $\pi_d(v, u) > 0$, where $u \in I_v^+$, and $U(v)$ is determined by Equation 1.*

To be economically feasible, an incentive mechanism should be budget constrained. In strategic network diffusion, the total rewards allocated to the players should not exceed a fixed portion ϑ of the total aggregated task efforts.

Definition 7 (Budget Constraint)**.** *A reward mechanism is budget-constrained if we have $\sum_{v \in G} \pi(v) \leq \vartheta \cdot \sum_{v \in G} t_v$, where $\vartheta \in \mathbb{R}_{>0}$ is a predefined constant.*

A mechanism for strategic network diffusion should limit indirect referrals to prevent agents from forming unnecessarily long referral chains. That is, the mechanism should satisfy the *monotonicity* constraint to limit the scope of indirect referrals and facilitate the task completion.

Definition 8 (Monotonicity)**.** *An incentive mechanism π is monotonic if v_2 is a successor of v_1, adding a direct successor v_i to v_2 increases v_1's diffusion rewards $\pi_d^{'}(v_1)$ at least as much as the diffusion rewards $\pi_d^{''}(v_1)$ by adding a direct successor v_j to a successor of v_2, where $t_{v_i} = t_{v_j}$.*

In strategic network diffusion, players should have no incentives to delay performing the tasks to wait for a referral with a more rewarding position. That is, an incentive mechanism should determine the diffusion rewards for each player $v \in V$ based on the reverse subgraph G_v rooted at v.

Definition 9 (Subgraph Constraint)**.** *An incentive mechanism π is subgraph-constrained if $\pi(v)$ only depends on the rooted subgraph G_v.*

It is challenging for stakeholders to design a mechanism that satisfies all the constraints, especially false-name-proofness and collusion-proofness. A main reason is that in practice agents' identities are often costly to verify and the collusive communications are usually difficult or unfeasible to capture [Jin *et al.*, 2011; Yang *et al.*, 2014; Feldman and Chuang, 2005]. To tackle this challenge, a careful treatment is needed.

4 Generalized Contest Mechanism

In this section, we take a decomposition approach to manipulation-resistant mechanism design for strategic network diffusion. To do so, we first characterize the conditions for an incentive mechanism to satisfy both false-name-proofness and collusion-proofness. We then present a class of Generalized Contest Mechanism (GCM) that satisfy all the design constraints.

4.1 Superadditivity

We decompose the incentive mechanism into two payment rules: one for the task efforts and the other for the diffusion contributions. For task efforts, a posted price mechanism is used . Posted price mechanisms are both false-name-proof and collusion-proof because they determine the rewards for each agent based solely on the verifiable task efforts.

We now focus on the diffusion incentive mechanism $\pi_d(v)$. In order to satisfy the false-name-proofness requirement, the incentive mechanism should be supperadditive in the diffusion contributions d_v. That is, for any two diffusion contributions $d(v_1), d(v_2) \in \mathbb{R}_{\geq 0}$, we have $\pi_d(d(v_1) + d(v_2)) \geq \pi_d(d(v_1)) + \pi_d(d(v_2))$. The intuition is inspired from the superadditivity in functional analysis. The supperadditivity requirement of the mechanism brings a monotonicity in terms of the diffusion rewards that create extra incentives for the agent not to split.

Definition 10 (Superadditivity)**.** *Let $f : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}$, a function f is* supperadditive *if $f(x+y) \geq f(x) + f(y)$ for all x, $y \in \mathbb{R}_{\geq 0}$.*

Theorem 1. *An incentive mechanism is false-name-proof if and only if it is superadditive in terms of the diffusion contributions.*

Theorem 1 gives us a sufficient and necessary condition for an incentive mechanism to be false-name-proof when players' valuation is linear in the rewards and the costs he pays are linear in the task efforts. To design a false-name-proof mechanism, the principal needs to make the diffusion mechanism be superadditive in the diffusion efforts.

4.2 Increasing and Bounded Functions

In strategic network diffusion, a group of strategic players may collude to change the internal network structure or reduce the task efforts to benefit at least one member of the group without hurting the remaining members. To counter agents' such behavior, a mechanism should bound the total diffusion rewards for a referral. However, referrers will have no incentives to provide extra efforts if the number of the total diffusion rewards is fixed. To encourage the referrers to exert efforts, the mechanism needs to be monotonically increasing in the sum of total task efforts. Combining the two required conditions, the mechanism should be a monotonically increasing and bounded function in the sum of the referrers' task efforts.

Inspired by the monotone convergence theorem [Bibby, 1974] in real analysis, we demonstrate that if an incentive mechanism is monotonically increasing and bounded above in terms of the sum of the predecessors' task efforts, then the mechanism is collusion-proof.

Suppose a player $v \in G = (V, E)$ exerts task efforts $t(v)$ due to the referrals of his predecessors I_v^-. If the sum of the diffusion rewards due to the referral of player v is an increasing and bounded above function with respect to the sum of the task efforts of all the predecessors, the mechanism is collusion-proof.

Definition 11 (Increasing and bounded function)**.** *A function $f : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}$ is monotonically increasing and bounded above if the following two conditions hold: (1) for all $x, y \in \mathbb{R}_{\geq 0}$ such that $x \leq y$ one has $f(x) \leq f(y)$; (2) for all $x \in \mathbb{R}_{\geq 0}$ there exists $L \in \mathbb{R}$ where $L = \lim_{x \rightarrow +\infty} f(x)$.*

The diffusion rewards should be increasing in the sum of the task efforts because the task efforts of the players are verifiable. A group of players can only increase their diffusion efforts by increasing the sum of their total task efforts once the referral chains leading to v have established. The function should be bounded above due to the budget constraint requirement.

Theorem 2. *An incentive mechanism is collusion-proof if the mechanism is an increasing and bounded function in terms of the sum of the predecessors' task efforts $\sum_{u \in I_v^-} t(u)$.*

The increasing and bounded function provide incentives for referrers to increase their task efforts instead of colluding to reduce the task efforts. Meanwhile, it bounds the diffusion rewards. Note that the increasing and bounded function is not an necessary condition. To see this, we give an example. If the mechanism follows a uniform allocation rule, it is also collusion-proof. However, this rule violates the false-name-proofness constraint.

4.3 The GCM

Based on the Theorems 1 and 2, we introduce the generalized contest mechanism for strategic diffusion in social networks. The mechanism first constructs a superadditive function to determine the diffusion contributions for each player in the successful referral chain. It then uses an increasing and upper bounded function to determine the diffusion rewards.

For each player $v \in G = (V, E)$, if v exerts task efforts $t(v) > 0$ due to the referrals of his predecessors I_v^-. The task rewards for player $u \in G_v$ are computed by

$$\pi_t(u) = \mu \cdot t(u) \ , \tag{2}$$

where $\mu \in \mathbb{R}_{>0}$ is the reward parameter that characterizes to what extent the principal values agents' efforts.

The total diffusion rewards for the players in the subgraph G_v rooted at v is $\phi \cdot t(v)$ where $\phi \in \mathbb{R}_{>0}$. Let $D_v = \{u \in I_v^- : dist(u, v) = 1\}$ be the set of player v's direct predecessors. The virtual credits for player v are $b(v, v) = \eta \cdot f(t(v))$, where $f(\cdot)$ is a superadditive function in task efforts t. For each $u \in I_v^-$, the virtual credits for u's diffusion contributions due to v are determined by

$$b(u, v) = \eta \cdot f(t(u)) + t(u) \cdot \frac{\sum_{uu' \in p'} t(u')}{\sum_{uu' \in p} t(u')} \cdot t(v) \cdot (1 - \lambda) \tag{3}$$

The proportion of diffusion rewards allocated to each player $u \in G_v$ are calculated according to a ratio-form contest success function

$$h(b(u, v)) = \frac{(b(u, v))^\rho}{\sum_{u' \in G_v} (b(u', v))^\rho} \ , \tag{4}$$

where $\rho \in \mathbb{R}_{>0}$ is the noise factor.

The diffusion rewards for player u due to referring v are calculated by

$$\pi_d(u, v) = \begin{cases} h(b) \cdot t(v) \cdot \phi \cdot g(y) & u \neq v \\ h(b) \cdot t(v) \cdot \phi \cdot g(y) + t_v \cdot \phi (1 - g(y)) & u = v \end{cases} , \tag{5}$$

where $\lambda \in \mathbb{R}_{>0}$ is the proportion of diffusion credits given to the task worker v, and $0 \leq g(y) \leq 1$ is an increasing and bounded above in terms of y. Here, $y = \sum_{u \in I_v^-} t(u)$ are the total task efforts of player v's predcessors I_v^-.

The total rewards for player $u \in G_v$ are determined by

$$\pi(u, v) = \pi_t(u) + \pi_d(u, v) \ , \tag{6}$$

where $\pi_t(u)$ and $\pi_d(u, v)$ are computed by Eq. 2 and Eq. 5, respectively.

The GCM updates the diffusion rewards for each player in an anytime fashion, making it suitable for large-scale social networks. The social network $G = (V, E)$ can be implemented with adjacency lists. In the data structure, each

Algorithm 1 *Generalized Contest Mechanism*

```
    Input: S-seed nodes in a social network G.
    Output: π-payment for each node v ∈ G
    Initialize: π(v) = 0 for all v ∈ G
 1: while network propagation is true do
 2:     for each newly joined player v ∈ G and t(v) > 0 do
 3:         Assign diffusion credits b(v, v) ← η · (t(v))^2
 4:         Compute task efforts π_t(u) by Eq. 2
 5:         Update rewards π(u) ← π(u) + π_t(u)
 6:         for each u ∈ I_v^- and t(u) > 0 do
 7:             Compute diffusion credits b(u, v) by Eq. 3
 8:         end for
 9:         for each u ∈ G_v and b(u, v) ≥ η · f(t(u)) do
10:             Compute diffusion rewards π_d(u, v) by Eq. 5
11:             Update rewards π(u) ← π(u) + π_d(u, v)
12:         end for
13:     end for
14: end while
15: return π
```

node maintains a list of all its adjacent edges. It takes $O(|V|)$ time to allocate the diffusion credits, compute the task efforts, and update the rewards for all the newly joined players (See line 3-5 in Algo. 1). Computing diffusion credits for each player in the predecessors requires a depth-first search that takes $O(|V| + |E|)$ time (See line 7). To compute diffusion credits for all the players, it takes $O(|V| \cdot (|V| + |E|))$ time (See line 6-8). Similarly, it requires $O(|V| \cdot (|V| + |E|))$ time to compute the diffusion rewards and update the total rewards for each player in the social network (See line 9-12). Therefore, the total time complexity for updating the total rewards for all the players in Algo. 1 is $O(|V|^2 + |V||E|)$.

The GCM achieves false-name-proofness and collusion-proofness simultaneously by introducing a superadditive function to determine the diffusion contributions and a ratio-form contest success function to compute the proportion of diffusion rewards. The total diffusion rewards for all the referrers and the task worker are capped with an increasing and bounded above function in the total task efforts exerted by the referrers. For each player that has made successful referrals, he also receives a positive diffusion reward. Thus, the mechanism satisfies the voluntary participation constraints. The GCM is budget-constrained because it allocates a fixed portion of rewards for both task efforts and diffusion contributions. Under the GCM, direct referrals are given more diffusion rewards than indirect referrals through decayed diffusion credits. Therefore, the GCM is monotonic. For each newly joined player v, the GCM updates all the rewards of the players in the same subgraph rooted at v. Hence, the GCM satisfies the subgraph constraint.

Theorem 3. *The generalized contest mechanism satisfies false-name-proofness, collusion-proofness, individual rationality, budget constraint, monotonicity, and subgraph constraint.*

Apart from false-name attacks and collusion, a mechanism may be vulnerable to *collusion false-name attacks*: false-name attacks that are results of coordinated action by a group of players.

Corollary 1. *The generalized contest mechanism is resistant to collusion false-name attacks.*

When the superadditive function $f(t(u)) = (t(u))^2$ and $g(y) = 1$, the generalized contest mechanism corresponds to the multi-winner contests (MWC) mechanism [Shen *et al.*, 2019]. Note that the MWC mechanism is not collusion-proof as when referrers have the same cost coefficients, they could reduce their task efforts while still receiving the same level of diffusion rewards.

5 Experiments

There are different ways to construct the superadditive functions and the increasing and bounded functions. GCM variants with different functions may perform differently. It is desirable to identify the variants that have the best performance and compare their performance with the state-of-the-art mechanisms for strategic network diffusion. In our work, we conducted numerical simulations to show the promise of the generalized contest mechanism on four real-world social network datasets.

5.1 Experimental Settings

Datasets In our experiments, we used four real-world social network datasets: Twitter [Hodas and Lerman, 2014], Flickr [Cha *et al.*, 2009], Flixster [Goyal *et al.*, 2011], and Digg [Hogg and Lerman, 2012]. We estimated the influence probabilities for simulating the diffusion process using the learning algorithms with the Bernoulli distribution under the static model [Goyal *et al.*, 2010]. We next used the general threshold model [Kempe *et al.*, 2003] to simulate the influence diffusion process with the estimated probabilities. After that, each dataset generated a largest weakly connected component of the entire social networks.

We estimated the efforts according to a "S"-shaped sigmoid curve $1/(1 + e^{-(deg^-(v)-0.8*MD)})$ and the cost coefficient is calculated by $\delta_v = -0.1 * 1/(1 + e^{-(deg^-(v)-0.8*MD)}) + 0.2$.

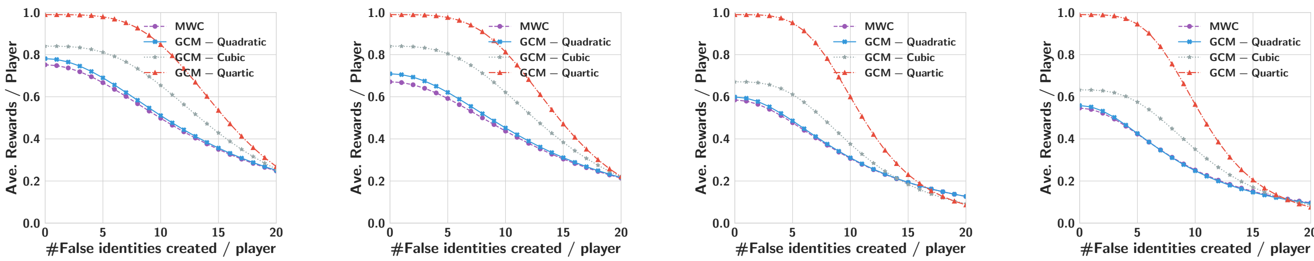
Method We measured the total efforts, the average individual efforts, the number of participates, and the social welfare. We used the multi-winner contests mechanism [Shen *et al.*, 2019] as the benchmark. We ran all the experiments 20 times on the same 3.7GHz 6-core machine.

Parameters In our experiments, we set the noise factor as $\rho = 0.55$ because moderate noise factors typically can expect the highest efforts [Shen *et al.*, 2019]. As standard in many geometric mechanisms, we set $\lambda = 0.5$. For fair comparison, we choose $\phi = 0.1$, $\mu = 0.9$, and $\eta = 0.25$.

We selected the superadditive functions. We considered the following functions: (1) quadratic: $(t(u))^2$, (2) cubic: $(t(u))^3$, and (3) quartic: $(t(u))^4$. We varied the increasing and bounded above functions. We considered the following functions: (1) linear: $\frac{g(y)}{1+g(y)}$; (2) quadratic: $\frac{(g(y))^2}{1+(g(y))^2}$; (3) exponential: $\frac{e^{g(y)}-1}{e^{g(y)}+1}$; (4) logarithmic: $\frac{\log(g(y)+1)}{1+\log(g(y)+1)}$. This resulted in 12 GCM variants. We compared their performance with the MWC mechanism.

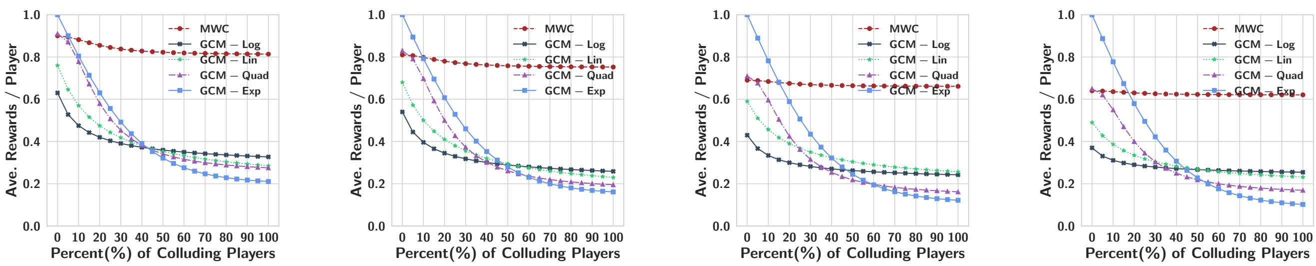
	GCM - Log			GCM - Lin			GCM-Quad			GCM-Exp			MWC
	Quadratic	Cubic	Quartic	Quadratic	Cubic	Quartic	Quadratic	Cubic	Quartic	Quadratic	Cubic	Quartic	
Twitter	1,992	2,966	3,320	4,119	4,471	5,780	5,041	5,888	6,673	7,142	8,963	9,327	4,080
Flickr	261	303	377	499	581	709	976	1,190	1,483	1,752	1,985	2,324	491
Flixster	120	178	268	391	434	499	650	732	806	945	1,069	1,177	379
Digg	113	170	196	211	242	275	389	418	472	513	603	691	207

Table 1: A comparison of the total task efforts for different groups.



(a) Twitter. (b) Flickr. (c) Flixster. (d) Digg.

Figure 5: Average rewards (normalized by the highest number in each dataset) for each player that creates different false identities.



(a) Twitter. (b) Flickr. (c) Flixster. (d) Digg.

Figure 6: Average rewards (normalized by the highest number in each dataset) for each player that is in different level of collusion.

5.2 Results

We compared the social welfare, the average individual efforts, and the total efforts. Our results indicate that the general contest mechanisms outperform the multi-winner contests mechanism consistently.

Performance without Manipulations When there were no manipulations, all the GCM vairants except the GCM-Log groups outperformed the MWC mechanism. Among them, the GCM-Exp groups performed the best, followed by the GCM-Quad groups and the GCM-Lin groups (See Table 1). The underline reason is that the generalized contest mechanisms with exponential and quadratic form of increasing and bounded functions increased greater than the linear form. The MWC used the linear form. It had a higher increase rate than the logarithmic form. GCMs with quartic functions performed better than the cubic and quadratic form because the quartic forms offered higher incentives for the players to exert task efforts.

Robustness to False-Name Attacks With the same increasing and bounded function (linear), we studied how the selection of superadditive function affects the performance in presence of different levels of false-name attacks. Results show that the degree of polynomials increase the resistance false-name attacks (See Fig. 5). This is because higher degree of polynomials provides higher diffusion credits and rewards. Players who have performed false-name attacks suffer from a higher loss of rewards.

Robustness to Collusion With the same superadditive function (quadratic), we compared how the selection of increasing and bounded function affects the performance in presence of different levels of collusion. Results show that MWC experienced the smallest degree of reduction in the rewards, while the GCM-Exp group had the biggest reduction (See Fig. 6). This indicates that GCM variants are more resistant to collusion because players would receive substantially less rewards if they colluded under the GCM variants.

Discussion In summary, the generalized contest mechanism can achieve performance on par with the state-of-the-art mechanisms that is resistant to false-name attacks. It provides a higher level of flexibility for stakeholders to tune the parameters to tailor for their specific needs.

6 Conclusion

To counter both false-name attacks and collusion, we introduce a class of generalized contest mechanism. We take a decomposition approach to design the manipulation-resistant mechanisms. The GCM satisfies desirable properties such as individual rationality, budget constraint, monotonicity and subgraph constraint. We compare variants of GCM with the state-of-the-art mechanism for strategic network diffusion empirically. Results show that the GCMs are more robust to manipulations and outperform the MWC mechanism in terms of performance as well. Our work provides a new approach to design manipulation-resistant mechanisms.

In our work, we assumed that the budget grows linear in task efforts. This requires an rising market. It will be interesting to study if the budget is fixed or shrinks. Another fruitful problem is to study how to address the challenges when players learn (e.g., their marginal cost coefficients adapt). Another important problem is design manipulation-resistant mechanisms to maximize individual efforts.

References

[Alshamsi *et al.*, 2018] Aamena Alshamsi, Flávio L Pinheiro, and Cesar A Hidalgo. Optimal diversification strategies in the networks of related products and of related research areas. *Nature communications*, 9(1):1328, 2018.

[Berman, 2016] Barry Berman. Referral marketing: Harnessing the power of your customers. *Business Horizons*, 59(1):19–28, 2016.

[Besaleva and Weaver, 2013] Liliya I Besaleva and Alfred C Weaver. Applications of social networks and crowdsourcing for disaster management improvement. In *2013 International Conference on Social Computing*, pages 213–219. IEEE, 2013.

[Bibby, 1974] John Bibby. Axiomatisations of the average and a further generalisation of monotonic sequences. *Glasgow Mathematical Journal*, 15(1):63–65, 1974.

[Cha *et al.*, 2009] Meeyoung Cha, Alan Mislove, and Krishna P Gummadi. A measurement-driven analysis of information propagation in the flickr social network. In *Proc. of WWW 2009*, pages 721–730, 2009.

[Chen *et al.*, 2009] Wei Chen, Yajun Wang, and Siyu Yang. Efficient influence maximization in social networks. In *Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 199–208. ACM, 2009.

[Constantinides *et al.*, 2008] Efthymios Constantinides, Carlota Lorenzo Romero, and Miguel A Gómez Boria. Social media: a new frontier for retailers? In *European Retail Research*, pages 1–28. Springer, 2008.

[De Choudhury *et al.*, 2013] Munmun De Choudhury, Michael Gamon, Scott Counts, and Eric Horvitz. Predicting depression via social media. *ICWSM*, 13:1–10, 2013.

[Drucker and Fleischer, 2012] Fabio A Drucker and Lisa K Fleischer. Simpler sybil-proof mechanisms for multi-level marketing. In *Proceedings of the 13th ACM conference on Electronic commerce*, pages 441–458. ACM, 2012.

[Emek *et al.*, 2011] Yuval Emek, Ron Karidi, Moshe Tennenholtz, and Aviv Zohar. Mechanisms for multi-level marketing. In *Proceedings of the 12th ACM conference on Electronic commerce*, pages 209–218. ACM, 2011.

[Enli, 2017] Gunn Enli. Twitter as arena for the authentic outsider: exploring the social media campaigns of trump and clinton in the 2016 us presidential election. *European journal of communication*, 32(1):50–61, 2017.

[Feldman and Chuang, 2005] Michal Feldman and John Chuang. Overcoming free-riding behavior in peer-to-peer systems. *ACM sigecom exchanges*, 5(4):41–50, 2005.

[Ferrara *et al.*, 2016] Emilio Ferrara, Onur Varol, Clayton Davis, Filippo Menczer, and Alessandro Flammini. The rise of social bots. *Communications of the ACM*, 59(7):96–104, 2016.

[Galeotti and Goyal, 2009] Andrea Galeotti and Sanjeev Goyal. Influencing the influencers: a theory of strategic diffusion. *The RAND Journal of Economics*, 40(3):509–532, 2009.

[Gao *et al.*, 2011] Huiji Gao, Geoffrey Barbier, Rebecca Goolsby, and Daniel Zeng. Harnessing the crowdsourcing power of social media for disaster relief. Technical report, Arizona State Univ Tempe, 2011.

[Goyal *et al.*, 2010] Amit Goyal, Francesco Bonchi, and Laks VS Lakshmanan. Learning influence probabilities in social networks. In *Proc. of WSDM 2010*, pages 241–250, 2010.

[Goyal *et al.*, 2011] Amit Goyal, Francesco Bonchi, and Laks VS Lakshmanan. A data-based approach to social influence maximization. *Proc. of the VLDB Endowment*, 5(1):73–84, 2011.

[Hodas and Lerman, 2014] Nathan O Hodas and Kristina Lerman. The simple rules of social contagion. *Scientific Reports*, 4:4343, 2014.

[Hogg and Lerman, 2012] Tad Hogg and Kristina Lerman. Social dynamics of digg. *EPJ Data Science*, 1(1):5, 2012.

[Jin *et al.*, 2011] Lei Jin, Hassan Takabi, and James BD Joshi. Towards active detection of identity clone attacks on online social networks. In *Proceedings of the first ACM conference on Data and application security and privacy*, pages 27–38. ACM, 2011.

[Kempe *et al.*, 2003] David Kempe, Jon Kleinberg, and Éva Tardos. Maximizing the spread of influence through a social network. In *Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 137–146. ACM, 2003.

[Naroditskiy *et al.*, 2014] Victor Naroditskiy, Nicholas R Jennings, Pascal Van Hentenryck, and Manuel Cebrian. Crowdsourcing contest dilemma. *J R Soc Interface*, 11(99):20140532, 2014.

[Pickard *et al.*, 2011] Galen Pickard, Wei Pan, Iyad Rahwan, Manuel Cebrian, Riley Crane, Anmol Madan, and Alex Pentland. Time-critical social mobilization. *Science*, 334(6055):509–512, 2011.

[Schmitt *et al.*, 2011] Philipp Schmitt, Bernd Skiera, and Christophe Van den Bulte. Referral programs and customer value. *Journal of marketing*, 75(1):46–59, 2011.

[Shen *et al.*, 2019] Wen Shen, Yang Feng, and Cristina V. Lopes. Multi-winner contests for strategic diffusion in social networks. In *Proceedings of the 33rd AAAI Conference on Artificial Intelligence (AAAI-19)*. AAAI Press, 2019.

[Tang *et al.*, 2011] John C Tang, Manuel Cebrian, Nicklaus A Giacobe, Hyun-Woo Kim, Taemie Kim, and Douglas Beaker Wickert. Reflecting on the darpa red balloon challenge. *Communications of the ACM*, 54(4):78–85, 2011.

[Tiago and Veríssimo, 2014] Maria Teresa Pinheiro Melo Borges Tiago and José Manuel Cristóvão Veríssimo. Digital marketing and social media: Why bother? *Business Horizons*, 57(6):703–708, 2014.

[Yang *et al.*, 2014] Zhi Yang, Christo Wilson, Xiao Wang, Tingting Gao, Ben Y Zhao, and Yafei Dai. Uncovering social network sybils in the wild. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 8(1):2, 2014.

[Zhao *et al.*, 2018] Dengji Zhao, Bin Li, Junping Xu, Dong Hao, and Nicholas R Jennings. Selling multiple items via social networks. In *Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems*, pages 68–76. International Foundation for Autonomous Agents and Multiagent Systems, 2018.

Appendix

Proof of Theorem 1

Proof. $\Rightarrow$ We prove it by contradiction. Suppose, to the contrary, that the mechanism is not superadditive. We have $\pi(v_1+v_2) < \pi(v_1)+\pi(v_2)$. Since $\pi_{v_1} = \pi_t(t_{v(1})+\pi_d(d_{v_1})$ and $\pi_{v_2} = \pi_t(t_{v_2}) + \pi_d(d_{v_2})$, we get $\pi_t(t(v_1 + v_2)) + \pi_d(d(v_1 + v_2)) < \pi_t(t(v_1)) + \pi_t(t(v_2)) + \pi_d(d(v_1)) + \pi_d(d(v_2))$. Since the π_t is posted-price, we have $\pi_t(t(v_1 + v_2)) = \pi_t(t(v_1)) + \pi_t(t(v_2))$. Therefore, we get $\pi_d(d(v_1 + v_2)) < \pi_d(d(v_1)) + \pi_d(d(v_2))$. Let $l = \pi_d(d(v_1)) + \pi_d(d(v_2)) - \pi_d(d(v_1 + v_2))$, we have that $l > 0$. That is, a player has a positive incentive to split his diffusion contributions. Thus, the incentive mechanism π is not false-name-proof, which contradicts the supposition that π is false-name-proof. Therefore, if an incentive mechanism is false-name-proof, then it is superadditive.

$\Leftarrow$ If the mechanism π is superadditive, then we have $\pi(v_1 + v_2) \geq \pi(v_1) + \pi(v_2)$. Since $\pi_{v_1} = \pi_t(t_{v_1}) + \pi_d(d_{v_1})$ and $\pi_{v_2} = \pi_t(t_{v_2}) + \pi_d(d_{v_2})$, we get $\pi_t(t(v_1 + v_2)) + \pi_d(d(v_1 + v_2)) \geq \pi_t(t(v_1)) + \pi_t(t(v_2)) + \pi_d(d(v_1)) + \pi_d(d(v_2))$. Since the π_t is posted-price, we have $\pi_t(t(v_1 + v_2)) = \pi_t(t(v_1)) + \pi_t(t(v_2))$. Therefore, we get $\pi_d(d(v_1 + v_2)) \geq \pi_d(d(v_1)) + \pi_d(d(v_2))$. Therefore, there is no incentive for a player to split the diffusion efforts.

This completes the proof. □

Proof of Theorem 2

Proof. There are three types of collusion:

- Reducing the task efforts: Since the incentive mechanism π is an increasing and bounded above function in the sum of the predecessors' task efforts $\sum_{u \in I_v^-} t(u)$. If v reduce the task efforts, then the diffusion rewards for both v and it predecessors reduce. If one or more predecessors reduce the task efforts, then the total diffusion rewards for the coalition that contains the players that have reduced the task efforts also decrease. Therefore, no groups of players can benefit from reducing the task efforts.
- Changing the internal network structure: If the task efforts do not reduce, but the internal network structure changes, the total diffusion rewards do not change. Suppose that the collusive coalition adds an additional referral relationship (as shown in Fig. 4), it will increase the diffusion rewards for one agent (e.g., player a in Fig. 4), but reduce the diffusion reward for another agent (e.g., player c in Fig. 4). According to the definition of collusion (See Def. 4), a collusive strategy should not make the remaining agents worse off.
- A combination of the previous two strategies: it suffices that a combination of the two previous two strategies do not make at least of the member in the collusive coalition better off without making the others worse off.

This completes the proof. □