Game-Theoretic Strategies and Equilibriums in Multimedia Fingerprinting Social Networks

W. Sabrina Lin, *Member, IEEE*, H. Vicky Zhao, *Member, IEEE*, and K. J. Ray Liu, *Fellow, IEEE*

***Abstract*—Multimedia social network is a network infrastructure in which the social network users share multimedia contents with all different purposes. Analyzing user behavior in multimedia social networks helps design more secured and efficient multimedia and networking systems. Multimedia fingerprinting protects multimedia from illegal alterations and multiuser collusion is a cost-effective attack. The colluder social network is naturally formed during multiuser collusion with which colluders gain reward by redistributing the colluded multimedia contents. Since the colluders have conflicting interest, the maximal-payoff collusion for one colluder may not be the maximal-payoff collusion for others. Hence, before a collusion being successful, the colluders must *bargain* with each other to reach agreements. We first model the bargaining behavior among colluders as a noncooperative game and study four different bargaining solutions of this game. Moreover, the market value of the redistributed multimedia content is often time-sensitive. The earlier the colluded copy being released, the more the people are willing to pay for it. Thus, the colluders have to reach agreements on how to distribute reward and risk among themselves as soon as possible. This paper further incorporates this time-sensitiveness of the colluders' reward and studies the time-sensitive bargaining equilibrium. The study in this paper reveals the strategies that are optimal for the colluders; thus, all the colluders have no inventive to disagree. Such understanding reduces the possible types of collusion into a small finite set.**

***Index Terms*—bargaining, collusion, game theory, multimedia fingerprinting, multimedia social network.**

I. Introduction

A social network is a social structure that ties individuals or organizations by one or more specific types of interdependency. A multimedia social network is a social network in which a group of users exchange or share multimedia contents, as well as other resources. The incentive for people to join a multimedia social network is to gain the reward/resource from others. But to gain reward, the users have to contribute their own resource as well as their cost. The utility of joining a multimedia social network can be considered as the difference between reward and cost. Intuitively, each user in a multimedia social network aims to maximize his/her own utility, and different users have different objectives which are often conflicting with other users' [1].

Since these multimedia social networks include millions of people, a crucial issue is to understand the user dynamics that influence human behavior [1], such as how users interact with and respond to each other. Research on human behavior provides fundamental guidelines to better design multimedia systems and to offer more reliable and personalized services. Since users might have conflicting objectives, the most-preferable decisions for one user may not be the most-preferable decisions for all other users. In such a scenario, game theory [2], [3] provides a fundamental tool to study the behavior dynamics among multimedia social network users and find the solution that can satisfy all users. By analyzing the human behavior in multimedia social networks, both the users and the system designer will have a clear picture of how much reward every user can get and what are the possible actions, thus ultimately leading to systems with more secure, efficient, and personalized services.

In this paper, we use the multimedia fingerprinting system to illustrate the modeling and analysis of user behavior in multimedia social networks. Digital fingerprinting tracks the distribution of multimedia data to protect multimedia from illegal usage by embedding a unique label, known as fingerprint, into every distributed copy [4], [5]. multiuser collusion is a cost-effective attack against digital fingerprinting system, where a group of attackers collectively mount attack to effectively remove or attenuate the identifying information. For example, by simply averaging all copies pixel by pixel, the fingerprint energy in the colluded copy can be reduced significantly without degrading the quality of the multimedia content. Multimedia fingerprinting should be designed to resist such multiuser collusion as well as attacks by a single adversary [6] to offer consistent and reliable protection.

During collusion, the colluders share reward from the illegal usage of multimedia as well as the risk of being captured by the digital rights enforcer. For example, if the multimedia content is a movie, then the reward is the profit by selling the pirate copy. The colluders in the digital fingerprinting system form a social network in which they contribute their own copies and share the reward and risk. In a colluder social network, users collaborate with each other to reduce their chance of being caught by the digital right enforcer and share the reward of redistributing the colluded multimedia signal. Most prior work assumes any types of collusion can happen. However, before collusion relationship can be established, an agreement must be reached regarding how to distribute risk and reward and if the collusion cannot satisfy

Manuscript received April 20, 2010; revised October 05, 2010 and December 02, 2010; accepted December 12, 2010. Date of publication December 30, 2010; date of current version March 18, 2011. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Ton Kalker.

W. S. Lin and K. J. R. Liu are with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742 USA (e-mail: wylin@umd.edu; kjrliu@umd.edu).

H. V. Zhao is with the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, Alberta T6G 2V4 Canada (e-mail: vzhao@ece.ualberta.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TMM.2010.2102345

all colluders, such an collusion will not exist. Nevertheless, each colluder prefers the collusion that favors his/her own payoff the most (lowest risk and highest reward), and different colluders have different preferences of strategies. To address such a conflict, a critical issue for the colluders is to decide how to fairly distribute the risk and the reward. It is of ample importance to understand how colluders bargain with each other to achieve fairness of the attack.

In the literature, there has been some prior works on the analysis and modeling of multiuser collusion [7]–[12]. The collusion behavior under equal-risk criteria in a scalable fingerprinting system was studied in [13], and the work in [14] investigated how a selfish colluder behaves if he/she wants to cheat during multiuser collusion in order to further decrease his/her risk. Based on the above investigations of colluder behavior, techniques from different disciplines, including error-correcting codes, finite-projective geometry, and combinatorial theories, have been used in the literature to design better collusion-resistant multimedia fingerprints [15]–[18]. However, all prior works assume that colluders only share the probability of being detected risk during collusion and they all decide to share the same risk. Such assumption neglects the fact that the colluders also share the reward of illegally redistributing multimedia contents, and different colluders have different resources that the colluders may not all agree with sharing the same risk.

To analyze how colluders bargain with each other to reach agreements, we model the user behavior as a noncooperative game where each colluder tries to maximize his/her individual payoff under the fairness constraint. We assume the colluders are willing to cooperate and the question to be answered is how do they reach agreements. In this paper, we consider different definitions of fairness and investigate how colluders share risk and reward. We will consider four different bargaining solutions: Absolute fairness, Nash-Bargaining, Max-Min, and Max-Sum solutions. Also, users in a colluder social network may have different social rankings; thus, some users may be willing to take higher risk and higher reward at the same time, while other users may be more concerned about risk and want to take lower risk and lower reward. We also take this phenomenon into consideration and study the proportional-fairness collusion.

One specific property of multimedia contents is that their market value is very time-sensitive. For instance, if the pirate version of a movie is released when the movie is in theater, it would have much higher market price than if it is released after the movie is available at DVD rental stores. Therefore, all colluders have the incentive to mount collusion as soon as possible. Since the total reward of redistributing the multimedia signal is the sum of all colluders' reward, the users in the colluder social network have to agree on how to distribute the risk and reward and achieve agreement of the collusion attack. If we consider the reward being a constant over time, thus the colluders can bargain for infinite stages to reach the equilibrium under different fairness constraints. However, since the reward is time-sensitive, the colluders must reach an agreement within a few stages to release the colluded copy with high market value.

In addition, on the other side of the fingerprinting system, the fingerprint detector also has to choose its optimal strategy according to various types of collusion. The colluders will agree on the bargaining solutions if and only if the bargaining solutions are the best strategies they can choose under the fairness criteria. Therefore, it is crucial for both colluders and the digital rights enforcer to investigate the optimal strategies for each other's choices and reach equilibriums for the multimedia fingerprinting social network.

Bargaining strategies and equilibriums in social networks have been studied and can be foreseen to be used in any social networks in which users have mutual interest. For example, in a peer-to-peer network in which peers are all interested in the same set of files or multimedia streams, users exchange pieces of the data that they have to help each other complete the file. In such a scenario, it is natural for the users to bargain with each other on how much data and when should each user upload to others. The performance of the peer-to-peer systems are dominated by how cooperative the users are. Therefore, the results in this paper can be applied to peer-to-peer systems and provide guidelines for the system designer about how to push the bargained cooperation strategies among peers to the optimal one that can maximize the system performance.

We first formulate the collusion as a bargaining process and find the fair collusion that colluders will all agree. Then we incorporate the time-sensitive property into the game-theoretical model and find the equilibrium that maximize the colluders' payoff. Section II introduces the multimedia fingerprinting systems that we consider in this paper. We propose the bargaining model in Section III and analyze the fair collusion, and the time-sensitive bargaining process is discussed in Section IV. The analysis of equilibriums for the colluder-detector game in the multimedia fingerprinting social networks is studied in Section V, and conclusions are drawn in Section VI.

II. System Model

In this section, we will introduce the structure and users involved in the colluder social network. As the very first study in the fairness analysis among colluders, we use Gaussian orthogonal fingerprint in the scalable video coding system as an example to demonstrate our analysis.

A. Temporally Scalable Video Coding Systems

With the heavy traffic of multimedia communication in the past decade, scalability in multimedia coding has become one of the most important properties for rich media access from anywhere by anyone [20]. Scalable video coding is widely adopted nowadays to accommodate heterogeneous networks and devices with different storage and computing capability: it decomposes the video sequence into different layers of different priority. The base layer contains the most important information of the video and is distributed to all users, and the enhancement layers gradually refine the reconstructed sequence at the decoder's side and are only distributed to the users with sufficient bandwidth. Such an encoding structure provides flexible solutions for multimedia transmission and offers adaptivity to heterogeneous networks, varying channel conditions and diverse computing capability at the receiving terminals.

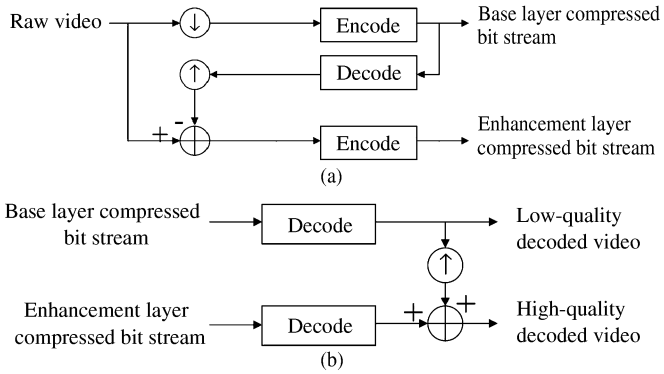


Fig. 1. Two-layer scalable codec. (a) Encoder. (b) Decoder.

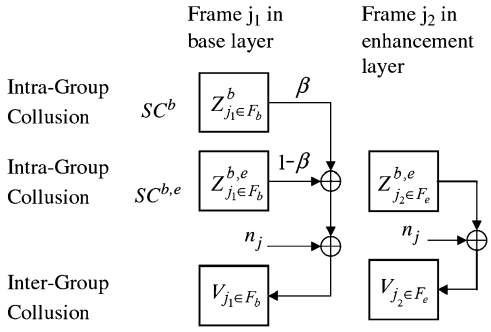


Fig. 2. Illustration of multiuser collusion in two-layer scalable video coding systems.

Fig. 1 shows a block diagram of a two-layer scalable video coding system. The encoder first down-samples the raw video and performs lossy compression to generate the base layer bit stream. Then, the encoder calculates the difference between the original video sequence and the up-sampled base layer, and applies lossy compression to this residue to generate the enhancement layer bit streams. At the receiver's side, to reconstruct a high-resolution video, the decoder has to first receive and decode both the base layer and the enhancement layer bit streams. Then the up-sampled base layer is combined with the enhancement layer refinements to form the high-resolution decoded video.

Without loss of generality, we consider a two-layer temporally scalable video coding system. Our analysis can also be applied to other types of scalability since the scalable codec in Fig. 1 is generic and can be used to achieve different types of scalability. In the following discussion, we define F_b and F_e as the sets containing the indices of the frames in base layer and enhancement layer, respectively; and let $f^{(i)}$ be the set of the indices of the frames that user $\mathbf{u}^{(i)}$ receives. U^b is the subgroup of users who receive the base layer only, and $U^{b,e}$ contains the indices of the users who subscribe to the high-quality version containing both layers.

B. Scalable Multimedia Fingerprinting and Collusion Attack

We consider a digital fingerprinting system that consists of three parts: fingerprint embedding, collusion attacks, and fingerprint detection.

1) Fingerprint Embedding: Spread spectrum embedding [21], [22] is a popular data hiding technique to embed fingerprints into the host multimedia signals because of the proven robustness against many single-copy attacks and common signal processing. Therefore, we use the spread spectrum embedding to embed fingerprints in the host signal. Let $\mathbf{S}_j$ be the jth frame in the video, and for each user $\mathbf{u}^{(i)}$ who subscribes to frame j, the content owner generates a unique fingerprint $\mathbf{W}_j^{(i)}$, with the same length as $\mathbf{S}_j$. The fingerprinted frame is $\mathbf{X}_j^{(i)} = \mathbf{S}_j + JND_j\mathbf{W}_j^{(i)}$, which is distributed to $\mathbf{u}^{(i)}$. JND [22] here is used to control the energy of the embedded fingerprints and make the fingerprinted copy be perceptually the same as the original one.

We consider orthogonal fingerprint modulation [5] in this paper, which means $\mathbf{W}_j^{(i)}\dot{\mathbf{W}}_j^{(j)} = \|\mathbf{w}_j\|^2\delta(i-j)$. We first generate independent vectors following Gaussian distribution $\mathcal{N}(0,\sigma_W^2)$, and then apply Gram-Schmidt orthogonalization to produce fingerprints that are strictly orthogonal to each other with equal energies.

2) Multiuser Collusion: During multiuser collusion, colluders collectively mount attacks to effectively attenuate the energy of the embedded fingerprints. Since nonlinear collusion can be modeled as averaging collusion with additive noise and all collusion attacks have similar performance with colluded copies of the same quality [23], in this paper, we focus on averaging-based collusion. Depending on the resolutions of the colluders' copies, during collusion, the colluders are divided into two non-overlapping subgroups. Let SC^b be the set with the indices of the colluders who receive the fingerprinted base layer only and $SC^{b,e}$ contains the indices of all colluders who subscribe to the high-resolution copy with both base layer and enhancement layer. $K^b = |SC^b|$ and $K^{b,e} = |SC^{b,e}|$ are the number of colluders in SC^b, $SC^{b,e}$, and SC^{all}, respectively. $K = K^b + K^{b,e}$ is the total number of colluders.

We consider the basic scenario where colluders who receive fingerprinted copies of the same resolution agree to share the same risk. Following the two-stage collusion model in [13] as illustrated in Fig. 2, colluders first apply intra-group collusion as follows: for each frame $j \in F_b$ in the base layer, colluders in SC^b generate $\mathbf{Z}_j^b = \sum_{k\in SC^b}\mathbf{X}_j^{(k)}/K^b$; and for each frame $j \in F_b \cup F_e$ that they receive, colluders in $SC^{b,e}$ calculate $\mathbf{Z}_j^{b,e} = \sum_{k\in SC^{b,e}}\mathbf{X}_j^{(k)}/K^{b,e}$. Then, colluders combine these two copies, $\{\mathbf{Z}_j^b\}_{j\in F_b}$ and $\{\mathbf{Z}_j^{b,e}\}_{j\in F_b\cup F_e}$, and apply inter-group collusion. For each frame $j \in F_b$ in the base layer, the colluded frame is

$$\mathbf{V}_j = \beta\mathbf{Z}_j^b + (1-\beta)\mathbf{Z}_j^{b,e} + \mathbf{n}_j \tag{1}$$

where $0 \le \beta \le 1$. For each frame $j_2 \in F_e$ in the enhancement layer, the colluded frame j is

$$\mathbf{V}_j = \mathbf{Z}_j^{b,e} + \mathbf{n}_j. \tag{2}$$

$\mathbf{n}_j$ is additive noise to further deter the detection performance.

During collusion, the colluders bargain to reach the agreement on how to choose the collusion parameter, β, to achieve fair collusion that balances every colluder's demand.

3) Fingerprint Detection: We consider a nonblind detection scenario where the host signal is first removed from the test copy before colluder identification. Upon receiving the colluded

copy, the detector first extracts the fingerprint $\mathbf{Y}_j$ from the jth frame $\mathbf{V}_j$ in the colluded copy. Here we adopt our prior work, the self-probing fingerprint in [24], as the fingerprint detector. It was shown that the self-probing fingerprint detector has approximately the same performance as the optimum detector, which has perfect knowledge of the means and always selects the detection statistics with the best performance.

To identify the colluders who received the higher resolution copy, $SC^{b,e}$, the self-probing detector first chooses the detection statistics.

- For every user $\mathbf{u}^{(i)}$ in $\mathbf{U}^{b,e}$, the detector first calculates $TN_{all}^{(i)}$, $TN_e^{(i)}$, and $TN_b^{(i)}$ by

$$TN_t^{(i)} = \left(\sum_{j \in F_t} \left\langle \mathbf{Y}_j, \mathbf{W}_j^{(i)} \right\rangle \right) / \sqrt{\sum_{j \in F_t} \left\| \mathbf{W}_j^{(i)} \right\|^2} \quad (3)$$

  where $t = b, e$, or $\{all\}$ and then obtains

$$\widehat{SC}_c^{b,e} = \left\{ i : TN_{all}^{(i)} > h_t \right\}, \quad \widehat{SC}_e^{b,e} = \left\{ i : TN_e^{(i)} > h_t \right\},$$
$$\widehat{SC}_b^{b,e} = \left\{ i : TN_{e1}^{(i)} > h_t \right\} \quad (4)$$

  for a given threshold h_t.
- The detector combines the above four sets of estimated colluders in $\mathbf{U}^{b,e}$ and lets $\widehat{SC}^{b,e} = \widehat{SC}_{all}^{b,e} \cup \widehat{SC}_e^{b,e} \cup \widehat{SC}_b^{b,e}$.
- Given $\widehat{SC}^{b,e}$, the detector estimates the means of the three detection statistics above

$$\hat{\mu}_{all} = \sum_{k \in \widehat{SC}^{b,e}} \frac{TN_{all}^{(k)}}{|\widehat{SC}^{b,e}|}, \quad \hat{\mu}_e = \sum_{k \in \widehat{SC}^{b,e}} \frac{TN_e^{(k)}}{|\widehat{SC}^{b,e}|},$$
$$\hat{\mu}_b = \sum_{k \in \widehat{SC}^{b,e}} \frac{TN_b^{(k)}}{|\widehat{SC}^{b,e}|}. \quad (5)$$

- The detector compares $\hat{\mu}_{all}$, $\hat{\mu}_e$, and $\hat{\mu}_b$ and selects the detection statistics with the largest estimated mean for final detection.

For each user $\mathbf{u}^{(i)}$ in $\mathbf{U}^b$, the detection statistics is

$$TN^{(i)} = \left(\sum_{j \in F^b} \left\langle \mathbf{Y}_j, \mathbf{W}_j^{(i)} \right\rangle \right) / \sqrt{\sum_{j \in F^b} \|\mathbf{W}_j^{(i)}\|^2}. \quad (6)$$

Finally, the self-probing detector compares these detection statistics with a threshold h, and outputs the estimated colluder set $\widehat{SC} = \{i : TN^{(i)} > h\}$.

III. Bargaining Model of Human Behavior in Colluders Social Network

In this section, we focus first on the scenario that the market value of the multimedia content is not time-sensitive. We propose the game-theoretical model of user behavior in a colluder social network, find the feasible set of the game, and analyze possible bargaining solutions under different fairness criteria. We define the cost of collusion to be a monotone decreasing function of his/her risk of being detected ($P_d^{(i)}$): the smaller the risk, the higher the payoff. In addition, when the colluded copy has higher resolution and better quality, colluders can redistribute the colluded copy with a higher price and thus receive higher profit. Consequently, $\pi^{(i)}$ is a monotonically increasing function of the colluded copy's resolution. Furthermore, colluding with more attackers reduces $\mathbf{u}^{(i)}$'s probability of being detected, while it also reduces the profit that $\mathbf{u}^{(i)}$ receives from the illegal redistribution of multimedia since he/she has to share it with more people.

A. Game Model

During collusion, every user in the colluder social network wants to minimize his/her own risk and maximizes his/her own reward. Hence, the payoff of each colluder can be considered as the difference between the expected value of risk and the reward.

First, the reward of redistributing the colluded multimedia signal depends on not only the quality of the colluded copy but also the time that the copy being released. The market value of colluded copy with lower quality decreases faster than higher-resolution copy. For instance, when the movie is still in theaters, people might want to watch the low-resolution colluded copy to catch the trend. But if the movie is out of the theaters and its DVD has been released, people might still want to purchase the high-resolution pirated copy since the cost would be lower than the DVD, but the incentive of paying for low-resolution pirated version is very little, since the DVD is easily accessible and not very costly. Also, if the colluded copy is the only pirated copy in the market, all the market value will go for it and not be shared with other copies. Therefore, the colluders are competing not only with the movie industry but also the other colluders over the speed of generating the pirated copy.

For colluder $\mathbf{u}^{(i)}$, his/her payoff function $\pi^{(i)}$ should be composed of two terms: colluder i's loss if being detected plus his/her reward. Here we adopt the exponentially decay model for the market value of the colluded copy [2]. The reward that player i gets in the next round of bargaining will be decayed by a constant $\delta_{(i)}$. Hence, the utility function of user i at the kth round can be defined as

$$\pi_k^{(i)} = -P_d^{(i)}(\beta_k) * L + \left(1 - P_d^{(i)}\right) \delta_{(i)}^{k-1} R^{(i)} \quad (7)$$

where $0 < \delta_b < 1$ and $0 < \delta_{b,e} < 1$ are the reward-decay constant of SC^b and $SC^{b,e}$, respectively, and β_k is the collusion parameter of the kth round. The market value of the high-resolution copy is more resistant to time than low-resolution copies. For instance, after the DVD of the movie is available at the rental stores, the low-resolution copies almost have no value in the market, but high-resolution copies still conserve parts of the value as long as their prices are lower than the rental fee. Therefore, a reasonable constraint of the decaying factors is $\delta_{b,e} \geq \delta_b$. In (7), $P_d^{(i)}$ and $L^{(i)}$ stand for colluder $\mathbf{u}^{(i)}$'s probability and loss of being detected, and $R^{(i)}$ is the reward that $\mathbf{u}^{(i)}$ gets after redistributing the colluded multimedia content and sharing with other colluders.

As a result, $R^{(i)}$ can be modeled as

$$R^{(i)} = \frac{\left(f^{(i)}\right)^{\gamma} D\left(P_d^{(i)}\right)}{\sum_{j=1}^{K} \left(f^{(j)}\right)^{\gamma} D\left(P_d^{(j)}\right)} \theta \quad (8)$$

where $f^{(i)}$ is the number of frames in $\mathbf{u}^{(i)}$'s copy, K is the total number of colluders, $D(\bullet)$ is a nondecreasing function, and θ' is a parameter to address the tradeoff between the risk that a colluder takes and the reward that he or she receives, and it has a smaller value when colluders emphasize more on risk minimization. $(f^{(i)})^{\gamma}$ illustrates colluders with higher-quality copies would have more reward since they already paid more money to subscribe to higher-resolution copies, and γ is the factor to control how much extra reward the colluders with higher-resolution copies should get. For example, if $\gamma = 0$, then the reward is equally distributed among the colluders with the same quality copies, and larger γ indicates the reward distribution favors the colluders with higher-quality copies more. Different colluders have different evaluations of their own risk. Therefore, some colluders might want to take higher risk, and in return, they would ask for more reward. $D(P_d^{(i)})$ allows the colluders who take higher risk to have higher reward.

Note that if the reward of redistributing multimedia content is not time-sensitive, which means $\delta_{(i)} = 1$, then (7) can be written as

$$\pi^{(i)} = -P_d^{(i)} * L^{(i)} + \left(1 - P_d^{(i)}\right) R^{(i)}. \tag{9}$$

In the following sections, to simplify the analysis, we assume the colluders who receive the same quality copies agree to share the same probability of being detected. Hence, the bargaining process during collusion can be modeled as the following game.

- **Players**: There are two players in the game. Colluders who receive low-resolution copies act as a single player in the game and they have the same utility π^b, while colluders who have high-resolution copies act as a single player during the bargaining process and they have the same utility $\pi^{b,e}$. Denote colluders in SC^b as SC^b, and colluders in $SC^{b,e}$ be $SC^{b,e}$ in this game.
- **Strategies**: The collusion parameter β controls the risk for both SC^b and $SC^{b,e}$. The control factors of the reward distribution (γ and $D(P_d^{(i)})$) are declared before the game. Therefore, the players' possible strategies are all the possible values of β.
- **Utility function**: The utility function is considered as the reward minus the expected cost as in (9). Note that each colluder is allowed to report different $L^{(i)}$ based on his/her own situation as long as $L^{(i)} \leq L^{max}$.

B. Bargaining Model

An illustration of the time-sensitiveness of the colluders' reward is shown in Fig. 3. The blue solid curve is the feasible region that the colluders can bargain with before the bargaining process, the green circled curve and the red dashed curve are the feasible region after the first and second bargaining rounds, respectively. As in Fig. 3, the colluders have to finish their bargaining process as soon as possible, to avoid the utility loss.

Under such circumstance, both groups of colluders, SC^b and $SC^{b,e}$, would want to reach agreement as soon as possible. We model the process of reaching agreement among colluders using the following bargaining model.

- In the first bargaining stage, $SC^{b,e}$ offers the collusion parameter β_1 that uniquely maps to the utility pair $(\pi_1^b, \pi_1^{b,e})$ on the Pareto-optimal set, in which both SC^b and $SC^{b,e}$ cannot increase their payoff without decreasing the other's. An example of Pareto-optimal set is illustrated in Fig. 4.
- Upon receiving the offer, SC^b has the choice to accept this offer and get the payoff π_1^b, or reject and offer back β_2, which corresponds to payoff pair $(\pi_2^b, \pi_2^{b,e})$ and continues to the second stage.
- If SC^b decided to offer back, $SC^{b,e}$ again has the choice to accept the offer $(\pi_2^b, \pi_2^{b,e})$ or offer back. The bargaining process would continue until both groups of colluders agree on one offer.

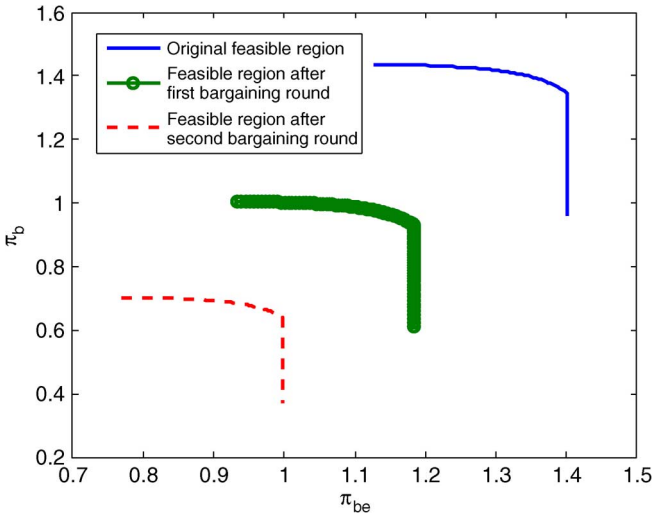


Fig. 3. Feasible region for bargaining after the first two rounds.

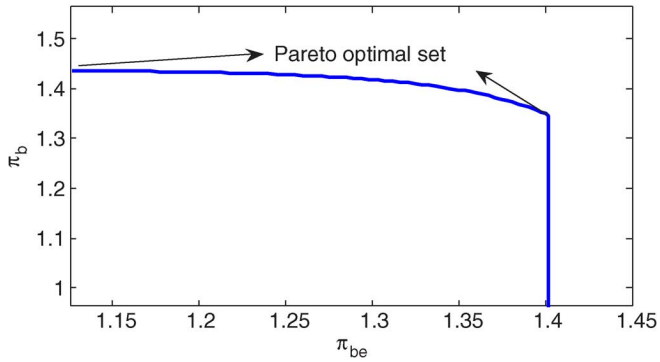


Fig. 4. Example of Pareto-optimal set for the bargaining problem in case one.

In this model, $SC^{b,e}$ makes offer first since colluders with higher-resolution copies take advantage during bargaining. This advantage comes from that even if $SC^{b,e}$ cannot reach agreement with SC^b, they can still release their high-resolution colluded copy with high market value, but on the other hand, SC^b themselves can only generate low-resolution colluded copy. Hence, $SC^{b,e}$ has more bargain power over SC^b, and should make the offer first.

The *equilibrium* in this time-sensitive bargaining game is the "offer pairs" that both players will agree immediately upon offered. From the offerer's point of view, he/she wants to make the offer attractive enough that the other player will agree on the offer and not offer back to reserve the full value of the colluded multimedia signal. On the other hand, the offerer also does not

want to make an offer that benefits the other player too much and hurt his/her own interest. Therefore, the equilibrium pair $((\pi_k^b, \pi_k^{b,e}), (\pi_{k+1}^b, \pi_{k+1}^{b,e})$ that the colluders would reach agreement at the kth bargaining stage has the following property: suppose $SC^{b,e}$ makes an offer $(\pi_k^b, \pi_k^{b,e})$ at the kth stage, then π_k^b should be large enough that SC^b will accept it, and no larger. On the other hand, SC^b should accept π_k^b if it is not smaller than the discounted payoff $-P_d^b(\beta_{k+1}) * L + \delta_b^k R^b$ that SC^b would receive if $SC^{b,e}$ accepts their counter offer. Therefore

$$-P_d^b(\beta_k) * L + \left(1 - P_d^b\right) \delta_b^{k-1} R^b = -P_d^b(\beta_{k+1}) * L + \left(1 - P_d^b\right) \delta_b^k R^b \quad (10)$$

and a similar consideration (for the dual game) for $SC^{b,e}$ gives

$$-P_d^{b,e}(\beta_{k+1}) * L + \left(1 - P_d^{b,e}\right) \delta_{b,e}^k R^{b,e} = -P_d^{b,e}(\beta_k) * L + \left(1 - P_d^b\right) \delta_{b,e}^{k-1} R^{b,e}. \quad (11)$$

We assume the worst-case scenario for the fingerprint detector that the colluders have perfect information about the detector's detection strategy. This is the widely adopted concept in the collusion analysis toward the best protection of multimedia. Thus, $P_d^{b,e}(\beta)$ and $P_d^b(\beta)$ are known to the colluders. So we have two linear-independent equations with two unknowns and the time-sensitive bargaining equilibrium can only be found numerically since $P_d^{b,e}(\beta)$ and $P_d^b(\beta)$ involve the Gaussian tail function.

C. Fairness Criteria

A special case of the above bargaining model is when the reward of redistributing the colluded copy is not time-sensitive, which means δ_k in (7) equals to 1. In such circumstance, any β_k can be the solution of equations (10) and (11), which means every solution is a time-sensitive equilibrium. When the time spent in the bargaining process is not a crucial factor during collusion, the colluders will bargain until both groups satisfy to reach a fairness solution. Depending on the definition of fairness and the objectives of collusion, colluders select different collusion strategies and aim to reach agreement under different fairness criteria. In this section, we demonstrate the behavior analysis of colluder social network by four commonly used fairness criteria during bargaining.

Absolute Fairness: The most straightforward fairness criteria is the absolute fairness, which means the utility of every user in the colluder social network is equal, where

$$\pi_{Absolute} = \pi^{(i)} = \pi^{(j)} \quad \forall i, j \in SC. \quad (12)$$

Moreover, since we have assumed colluders who receive the same quality copies have equal utility, (12) can be simplified to

$$\pi_{Absolute} = \pi^b = \pi^{b,e}. \quad (13)$$

Properties: Although absolute fairness solution is the simplest and seems the most fair criteria, depending on the parameter $L^{(i)}$, $|SC^b|$, and $|SC^{b,e}|$, absolute fairness solution does not always exist. Therefore, other fairness criteria have to be taken into account.

MaxMin Fairness: To guarantee the utility of every one who participates in the colluder social network, colluders might choose to reach the agreement to maximize the minimum utility over all the users in the social network, that is,

$$\pi_{maxmin} = \max_{\beta} \min_{i} \left\{ \pi^{(i)} : i \in SC \right\} \quad (14)$$

which can also be simplified to

$$\pi_{maxmin} = \max_{\beta} \min\{\pi^b, \pi^{b,e}\}. \quad (15)$$

Max Sum Fairness: Under some circumstances, all users in the colluder social network have the same goal so that they are willing to maximize the total utility over the whole social network. Mathematically, the Max-Sum fairness solution can be formulated as follows:

$$\pi_{maxsum} = \max_{\beta} \sum_{i \in SC} \pi^{(i)}. \quad (16)$$

Properties: Max-Sum solution has a desired property that if it is feasible, it is Pareto-optimal. Pareto optimality means no player can increase his/her payoff without decreasing others'. In a bargaining situation, players would always like to settle at a Pareto-optimal outcome. This is because if they select a point that is not Pareto-optimal, then there exists another solution with which at least one player can have larger payoff without hurting the interest of the other players.

Proof: If $\pi_{maxsum} = K^b \pi_{maxsum}^b + K^{b,e} \pi_{maxsum}^{b,e}$ is feasible but not Pareto-optimal, then there exists $(\pi_{maxsum}^b, \pi^{b,e'})$ or $(\pi^{b'}, \pi_{maxsum}^{b,e})$ in feasible set where $\pi^{b'} > \pi_{maxsum}^b, \pi^{b,e'} > \pi_{maxsum}^{b,e}$ by the definition of Pareto-optimal. Thus, there exists a feasible $\pi' > \pi_{maxsum}$, which contradicts the definition in (16).

Nash-Bargaining Solution: Nash-Bargaining solution, which is also always Pareto-optimal [2], [3], [25], is a famous bargaining solution in game theory. The definition of general Nash-Bargaining solution is as follows:

$$g(\pi^b, \pi^{be}) = (\pi^b - \pi^{b*})^{a_b} (\pi^{be} - \pi^{be*})^{a_{b,e}} \quad \text{where} \quad \pi^{b*} = \min_{\beta}\{\pi^b\}, \pi^{be*} = \min_{\beta}\{\pi^{be}\} \quad (17)$$

and $a_b, a_{b,e}$ are the bargaining power of SC^b and $SC^{b,e}$, respectively. When $a_b = a_{b,e} = 1$, Nash-Bargaining solution divides the additional utility between the two players in a ratio that is equal to the rate at which this utility can be transferred. If $a_b \neq a_{b,e}$, then the bargaining solution deviates from the proportional fairness solution and favors the player with higher bargain power.

IV. Bargaining Analysis and Simulation Results

In this section, we take two different utility functions as examples to illustrate the human behavior dynamics of colluder social networks.

A. Scenario I: Reward is Not Proportional to Risk

To have a clear picture of the agreement that the four fairness criteria will achieve, we first use a simple utility function as follows:

$$\pi^{(i)} = -P_d^{(i)} * L^{(i)} + \left(1 - P_d^{(i)}\right) \frac{\theta}{K} \tag{18}$$

which is a special case of (8) with $\gamma = 0$ and $D(P_d^{(i)}) = 1$. With (18), the reward of redistributing the colluded copy is equally distributed to all colluders. Therefore, the utility functions of the two players, SC^b and $SC^{b,e}$, can be written as

$$\pi^b = R - (R + L^b)P_d^b \text{ and } \pi^{b,e} = R - (R + L^{b,e})P_d^{b,e} \quad \text{where } R = \frac{\theta}{K}. \tag{19}$$

In the following, we will analyze the feasible region, the Pareto-optimal set, and the bargaining solutions based on different fairness criteria. Moreover, since the loss term $L^{(i)}$ is a private information and is claimed by the colluders themselves, we will also discuss which value of $L^{(i)}$ would be optimal for each player.

1) Feasible Set: Given a N-person general-sum game, there is a certain subset S of $\mathbb{R}^N$ that is called the feasible set. It is feasible in the sense that, given any $(\pi_1, \pi_2, \ldots, \pi_N) \in S$, it is possible for the players $u_1, u_2, \ldots, u_N$, acting together to obtain the utilities $\pi_1, \pi_2, \ldots, \pi_N$, respectively.

The self-probing fingerprint detector has approximately the same performance as the optimal detector. Therefore, colluders should consider the worse-case scenario and assume that the fingerprint detector can always select the detection statistics with the largest mean. Following the analysis in [26], under the assumption that the detection noise is i.i.d. Gaussian $\mathcal{N}(0, \sigma_n^2)$

$$\begin{aligned} P_d^{(i)} &= Q\left(\frac{h - \mu_{max}^{(i)}}{\sigma_n}\right), \\ \mu_{max}^{(i)} &= \mu_b \triangleq \frac{\beta\sqrt{N_b}}{K^b}\sigma_w \quad \text{for } i \in SC^b, \\ \text{and} \quad \mu_{max}^{(i)} &= \mu_{b,e} \triangleq \max\left\{\mu_{b,e}^b, \mu_{b,e}^e, \mu_{b,e}^c\right\} \text{ for } i \in SC^{b,e}, \\ \text{where} \quad \mu_{b,e}^b &= \frac{(1-\beta)\sqrt{N_b}}{K^{b,e}}\sigma_w, \mu_{b,e}^e = \frac{\sqrt{N_e}}{K^{b,e}}\sigma_w, \\ \text{and} \quad \mu_{b,e}^c &= \frac{(1-\beta)N_b + N_e}{K^{b,e}\sqrt{N_b + N_e}}\sigma_w. \end{aligned} \tag{20}$$

$Q(x) = (1/sqrt2\pi)\int_x^\infty e^{-t^2/2}dt$ is the Gaussian tail function.

From (20), for a given β, μ_b is fixed while $\mu_{b,e}$ may take three different values. To find the feasible set of the game, we need to analyze the relationship between β and $\mu_{b,e}$ first.

- **Case 1** $\mu_{b,e} = \mu_{b,e}^b$: $\mu_{b,e} = \mu_{b,e}^b$ if and only if $\mu_{b,e}^b \geq \mu_{b,e}^e$, and $\mu_{b,e}^b \geq \mu_{b,e}^c$. So, from (20)

$$(1-\beta) \geq \max\left\{\frac{\sqrt{N_e}}{\sqrt{N_b}}, \frac{N_e}{\sqrt{N_b}(\sqrt{N_b + N_e} - \sqrt{N_b})}\right\}. \tag{21}$$

Note that $\sqrt{N_b} + \sqrt{N_e} \geq \sqrt{N_b + N_e}$. So the second upper bound in (21) is always larger or equal to the first one. Thus, we have

$$\mu_{b,e} = \mu_{b,e}^b \Leftrightarrow 0 \leq \beta \leq 1 - \frac{N_e}{\sqrt{N_b}(\sqrt{N_b + N_e} - \sqrt{N_b})}. \tag{22}$$

The two terms of the upper bound in (22) can be combined as

$$\frac{\sqrt{N_b}\sqrt{N_b + N_e} - N_b - N_e}{\sqrt{N_b}(\sqrt{N_b + N_e} - \sqrt{N_b})} = \frac{\sqrt{N_b + N_e}(\sqrt{N_e} - \sqrt{N_b + N_e})}{\sqrt{N_b}(\sqrt{N_b + N_e} - \sqrt{N_b})} < 0. \tag{23}$$

Hence, for all $N_b > 0$, the upper bound of β in (22) is always smaller than 0. Therefore, $\mu_{b,e} \neq \mu_{b,e}^b$ and $\mu_{b,e}^b$ cannot be the largest among the three $\mu_{b,e}^b$, $\mu_{b,e}^e$, and $\mu_{b,e}^c$. Based on the above analysis, scenario 1 can never happen in real cases.

- **Case 2** $\mu_{b,e} = \mu_{b,e}^e$: $\mu_{b,e} = \mu_{b,e}^e$ if and only if $\mu_{b,e}^e \geq \mu_{b,e}^b$ and $\mu_{b,e}^e \geq \mu_{b,e}^c$. Therefore, from (20)

$$(1-\beta) \leq \min\left\{\frac{\sqrt{N_e}}{\sqrt{N_b}}, \frac{\sqrt{N_e}(\sqrt{N_b + N_e} - \sqrt{N_e})}{N_b}\right\}. \tag{24}$$

Using the same analysis as in (22), the necessary and sufficient condition for scenario 2 is

$$\mu_{b,e} = \mu_{b,e}^e \Leftrightarrow 1 - \frac{\sqrt{N_e}(\sqrt{N_b + N_e} - \sqrt{N_e})}{N_b} \leq \beta \leq 1. \tag{25}$$

- **Case 3** $\mu_{b,e} = \mu_{b,e}^c$: Since scenario 1 has been proven to not exist, $\mu_{b,e}$ must equal to one of $\mu_{b,e}^e$ and $\mu_{b,e}^c$. Therefore, the necessary and sufficient condition for Scenario 3 must be the compliment of the necessary and sufficient condition for Scenario 2. Hence

$$\mu_{b,e} = \mu_{b,e}^c \Leftrightarrow 0 \leq \beta \leq 1 - \frac{\sqrt{N_e}(\sqrt{N_b + N_e} - \sqrt{N_e})}{N_b}. \tag{26}$$

From the above analysis on $P_d^{(i)}$, we can calculate the payoffs $\pi^{(i)}$ for all colluders for any given β. From the definition of the payoff function (9), colluders who receive fingerprinted copies of the same quality have the same payoff. We define $\pi_{b,e}$ as the payoff for colluders in $SC^{b,e}$, and π_b as the payoff for colluders in SC^b. Fig. 4 illustrates π_b versus $\pi_{b,e}$, and the feasible set is shown by the solid line. The straight line segment corresponds to scenario 2, in which $\mu_{b,e} = \mu_{b,e}^e = (\sqrt{N_e}/K^{b,e})$ and is independent of β. Therefore, $\pi^{b,e}$ remains the same value while π^b keeps decreasing with β increasing. Similarly, the curve segment in Fig. 4 corresponds to scenario 3, in which $\mu_{b,e} = \mu_{b,e}^c$ and $\pi^{b,e}$ increases as β increases, while π^b decreases as β increases.

2) Pareto Optimality: After finding the feasible set, it is important to find the set of Pareto-optimal points. A solution is Pareto-optimal if and only if no player in the game can increase his/her payoff without decreasing others' [2]. In a bargaining situation, players would always like to settle at a Pareto-optimal

outcome. This is because if the colluders select a point that is not Pareto-optimal, then there exists another solution where at least one player can have larger payoff without hurting the interest of other players. Therefore, the player who can have higher payoff without hurting others' has the incentive to push other players to deviate from the non-Pareto-optimal solution, and the other rational players will agree with him/her since their interests are not influenced. Therefore, if possible, the colluders will always look for Pareto-optimal solutions to satisfy all the users in the colluder social network. Also, Pareto-optimal solutions are not unique in most cases. In this subsection, we investigate the Pareto-optimal points and analyze the necessary and sufficient conditions for a point to be Pareto-optimal.

Note that from (20), colluders in SC^b can increase their payoff if and only if they select a smaller β. On the other hand, $\pi^{b,e}$ remains the same when scenario 3 happens. Therefore, we start our analysis of the Pareto-optimality by π^b.

- **Necessary Condition**: If a point is Pareto-optimal, then decreasing μ_b and increasing the payoff of those colluders in SC^b must increase $\mu_{b,e}$ and decrease $\pi_{b,e}$. Note that from (20), μ_b is an increasing function of β. Thus, if a point is a Pareto-optimal point, $\mu_{b,e}$ must be a decreasing function of β, which happens only when $\mu_{b,e} = \mu^c_{b,e}$. Consequently, if a point is Pareto-optimal, β must satisfy (26), and (26) is the necessary condition of a Pareto-optimal point.
- **Sufficient Condition**: If $\mu_{b,e} = \mu^c_{b,e}$, then to increase the payoff of those colluders in $SC^{b,e}$, colluders must decrease $\mu_{b,e}$ by selecting a larger β. However, a larger β implies a larger μ_b; thus, it decreases the payoff of those colluders in SC^b. Consequently, those points that satisfy (20) are Pareto-optimal points, and (20) is the sufficient condition of Pareto-optimal.

To conclude, the collusion is Pareto-optimal if and only if $\mu_{b,e} = \mu^c_{b,e}$ and (20) is satisfied, which is the curve segment in Fig. 4.

3) Bargaining Solutions:

- **Absolute Fairness Solution** There are many ways for colluders to share the risk and the reward, depending on their definition of "fairness". Absolute fairness is widely adopted in the literature and most straightforward, where all colluders have the same payoff. Based on the definition in (13) and the utility function in (18), the absolute fairness solution can be solved by

$$\frac{P_d^{b,e}(\beta)}{P_d^b(\beta)} = \frac{L^b + R}{L^{b,e} + R} \tag{27}$$

where $P_d^{b,e}(\beta)$ and $P_d^b(\beta)$ are the SC^b and $SC^{b,e}$'s probability of being detected defined as in (20), and L^b and $L^{b,e}$ are the loss term claimed by the two players, respectively. According to the feasible set definition, $P_d^{b,e}(\beta)$ is a non-increasing function of β, and $P_d^b(\beta)$ is a monotonically increasing function of β. Thus, $P_d^{b,e}(\beta)/P_d^b(\beta)$ is a monotonically decreasing function of β, and (27) can be easily solved by numerical method. Then the absolute fairness solution exists, where $\beta' = 1 - \sqrt{N_e}(\sqrt{N_b + N_e} - \sqrt{N_e})/N_b$.

Optimal Value of $L^{(i)}$: Suppose the absolute fairness solution exists, and SC^b wants to get more reward by falsely reporting the private information, the loss term L^b. Since π^b is a monotonically decreasing function of $P_d(\beta)$ and $P_d(\beta)$ is a monotonically decreasing function of $P_d^{b,e}(\beta)/P_d^b(\beta)$, π^b is a monotonically increasing function of $P_d^{b,e}(\beta)/P_d^b(\beta)$. Since $P_d^{b,e}(\beta)/P_d^b(\beta)$ satisfies (27) for the absolute fairness solution, it can easily be proven that if SC^b, instead of claiming the actual loss L^b, he/she cheats to claim a higher loss $L'^b > L^b$. The resulting absolute fairness solution will give a $P_d'^b < P_d^b$. Therefore, the bargained payoff π'^b by claiming higher loss is higher than the payoff π^b which is the absolute-fairness solution with honestly-reported loss L^b. Hence, SC^b can earn more payoff by cheating on his/her private information. The same analysis can be applied to $SC^{b,e}$ and is not repeated here. To conclude, reporting higher loss will increase the user's payoff under absolute fairness condition. Thus, any selfish and rational user is going to report the highest possible loss L_{max} to maximize his/her own interest. As a result, $L^b = L^{b,e} = L_{max}$, and based on (27), $P_d^{b,e} = P_d^b$ in absolute fairness solution.

- **Max-Min Solution** In this example, the players' payoffs is affine to risk; hence, the Max-Min solution can be rewritten as finding β_{maxmin} that

$$\beta_{maxmin} = arg \min_{\beta} \max \mu_b, \mu_{b,e} \tag{28}$$

where μ_b and $\mu_{b,e}$ are defined in (20).

The Max-Min fairness solution with payoff function defined in (18) has the following property.

Properties: Max-Min solution always exists, and at least one of the Max-Min solution is Pareto-optimal. If the Max-Min solution is unique and is not on the boundary, then absolute fairness solution exists and the Max-Min solution is also the absolute fairness solution.

Proof: First prove the existence: since both π^b and $\pi^{b,e}$ are continuous functions of β, then $\min\{\pi^b, \pi^{b,e}\}$ is also a continuous function of β. Also $0 \leq \beta \leq 1$; therefore, the Max-Min solution always exists.

Suppose $\pi(\beta')$ is a Max-Min solution which is not Pareto-optimal. Since $\pi^{b,e}$ remains the same in the feasible but not Pareto-optimal set, the largest π^b in the non-Pareto-optimal set is at the boundary to the Pareto-optimal set. Therefore, if $\pi(\beta') = \pi^{b,e}(\beta') \leq \pi^b(\beta')$ is a Max-Min solution in the non-Pareto-optimal set, the boundary $\beta'' = 1 - \sqrt{N_e}(\sqrt{N_b + N_e} - \sqrt{N_e})/N_b$ also gives a Max-Min solution because $\pi^b(\beta'') \geq \pi^b(\beta') >= \pi^{b,e}(\beta') = \pi^{b,e}(\beta'')$. On the other hand, if $\pi^{b,e}(\beta') > \pi^b(\beta') = \pi(\beta')$ is a Max-Min solution in the non-Pareto-optimal set, then there exists a small positive number ϵ that $\pi^{b,e}(\beta' - \epsilon) > \pi^b(\beta' - \epsilon) = \pi^b(\beta') > \pi^{b,e}(\beta')$ in the non-Pareto-optimal set which contradicts the assumption that $\pi(\beta')$ is the Max-Min solution.

If the Max-Min solution is unique and is not on the boundary, from the above proof, it can easily be shown that the solution must be Pareto-optimal. Since $\pi^b(\beta)$ is a monotonically decreasing function of β and $\pi^{b,e}(\beta)$ is a monotonically increasing function of β in the Pareto-optimal set, if

$\pi_{maxmin}(\beta) = \pi^b(\beta) < \pi^{b,e}(\beta)$ is the unique Max-Min solution in the Pareto-optimal set, then there exists a small positive number ϵ that $\pi^{b,e}(\beta'-\epsilon) > \pi^b(\beta'-\epsilon) = \pi^b(\beta'-\epsilon) > \pi^{b,e}(\beta')$ which contradicts the Max-Min assumption. Similarly, we can easily prove that $\pi_{maxmin}(\beta) = \pi^b(\beta) > \pi^{b,e}(\beta)$ also cannot be the unique Max-Min solution. As a result, the unique Max-Min solution must have the property that $\pi_{maxmin}(\beta) = \pi^b(\beta) = \pi^{b,e}(\beta)$ which is also the absolute fairness solution. □

Based on the above analysis, when the reward is evenly distributed among all colluders and Max-Min solution is unique, the Max-Min solution is similar to the absolute fairness solution with nice properties such as Pareto-optimal and existence. Solving Max-Min fairness is similar to solving absolute fairness, except the boundary points of the Pareto-optimal set have to be compared, too.

Optimal Value of $L^{(i)}$: If the Max-Min solution is unique, then it is the absolute fairness solution by the above proof. Therefore, under such circumstance, reporting higher loss gives the player higher payoff and both players SC^b and $SC^{b,e}$ have the incentive to report the highest loss L_{max}.

If the Max-Min solution is not unique, based on the above analysis, some of the bargained solutions give $\pi^b(\beta) > \pi^{b,e}(\beta) = \pi^{b,e}_{max}$, where $\pi^{b,e}_{max}$ is the maximal payoff of $SC^{b,e}$. Hence, the Max-Min solution gives maximal $\pi^{b,e}$ $(\beta = 1)$. In such circumstance, the Max-Min solution already gives $SC^{b,e}$ the most advantage. As the result, $SC^{b,e}$ has no incentive to cheat on the loss term $L^{b,e}$ since he/she cannot earn more utility than the Max-Min solution.

On the other hand, if SC^b reports his/her loss to be $L^b + L'^b$, it makes $\pi'^b(\beta) = \pi^b(\beta) - L'^b < \pi^{b,e}(\beta) < \pi^{b,e}_{max}$ for some $0 \le \beta < 1 - \sqrt{N_e}(\sqrt{N_b+N_e} - \sqrt{N_e})/N_b$. Thus, by reporting higher loss term $L^b + L'^b$, SC^b can push the bargained Max-Min solution from the boundary of the Pareto-optimal set to the absolute fairness solution inside the Pareto-optimal set. Apparently, from Fig. 4, any point inside the Pareto-optimal set gives higher payoff for $SC^{b,e}$ than the boundary point of the Pareto-optimal set. Therefore, SC^b can gain higher payoff for by cheating on private information, and SC^b has the incentive to report the highest loss $L^b = L_{max}$.

Based on the above analysis, SC^b always wants to report the highest loss, and sometimes $SC^{b,e}$ has the incentive to cheat (when the Max-Min solution is in the Pareto-optimal set) and sometimes does not. Since the loss L^b and $L^{b,e}$ are claimed before the bargaining process and $SC^{b,e}$ cannot predict whether the Max-Min solution will be Pareto-optimal before bargaining, the players should both claim L_{max} to ensure the highest possible payoff.

- **Max-Sum Solution:** The Max-Sum solution can be formulated as minimizing

$$C_{sum} = P_d^b(\beta)K^b(R+L^b) + P_d^{b,e}(\beta)K^{b,e}(R+L^{b,e}). \quad (29)$$

As shown in the previous section, the Max-Sum solution is always Pareto-optimal, and the Pareto-optimal set is concave and compact. Therefore, the minimizer of the above function is either on the boundary or at the zero-deviation point. Taking the first derivative of the above function versus β, then

$$\begin{aligned}\frac{\partial C_{sum}}{\partial \beta} = &\frac{\sigma_w}{\sqrt{2\pi}\sigma_n} \\ &\times \left[\frac{\sqrt{N_b}}{K^b} e^{-\frac{(h-\beta\sqrt{N_b}/K^b)^2}{\sigma_n^2}} K^b(R+L^b) \right. \\ &\quad - \frac{N_b}{K^{b,e}\sqrt{N_b+N_e}} \\ &\quad \times e^{-\frac{\left(h-((1-\beta)N_b+N_e)/K^{b,e}\sqrt{N_b+N_e}\right)^2}{\sigma_n^2}} \\ &\quad \left. \times K^{b,e}(R+L^{b,e}) \right]. \end{aligned} \quad (30)$$

The Max-Sum solution can be solved numerically by the above equation.

Optimal value of $L^{(i)}$: Depending on the original Max-Sum solution (both players report the loss honestly), the analysis of optimal value of $L^{(i)}$ can be divided into three cases: when $\beta = 1$, $\beta = 1-\sqrt{N_e}(\sqrt{N_b+N_e}-\sqrt{N_e})/N_b$, or $\partial C_{sum}/\partial\beta = 0$. From (30), the zero-derivation point is

$$\begin{aligned}\frac{\partial^2 C_{sum}}{\partial\beta\partial L^b} = &\frac{(K^b+C)\sigma_w}{\sqrt{2\pi}\sigma_n} \\ &\times \frac{\sqrt{N_b}}{K^b} e^{-\frac{(h-\beta\sqrt{N_b}/K^b)^2}{\sigma_n^2}} K^b > 0, \text{ and} \\ \frac{\partial^2 C_{sum}}{\partial\beta\partial L^{b,e}} = &-\frac{(K^{b,e}+C)\sigma_w}{\sqrt{2\pi}\sigma_n} \\ &\times \frac{N_b}{K^{b,e}\sqrt{N_b+N_e}} \\ &\times e^{-\frac{\left(h-((1-\beta)N_b+N_e)/K^{b,e}\sqrt{N_b+N_e}\right)^2}{\sigma_n^2}} \\ &\times K^{b,e} < 0 \text{ when } 0 \le \beta \le 1. \end{aligned} \quad (31)$$

Since the Pareto-optimal set is concave, SC^b can push the Max-Sum solution to a smaller β (lower P_d^b, thus getting higher payoff for SC^b) by reporting higher L^b. Similarly, $SC^{b,e}$ can also get higher payoff by reporting higher $L^{b,e}$. Hence, both players have incentive to claim the highest loss L_{max}.

- **Nash-Bargaining Solution**

Colluders may also select proportional fairness, where some colluders benefit more at a cost of higher risk. One popular solution is the Nash-Bargaining solution, which is based on the idea that players who can gain more will naturally ask for more in the bargain. The Nash-Bargaining solution is based on the definition of fairness that the additional payoff must be divided between the two players in a ratio equal to the rate at which this utility can be transferred.

The Nash-Bargaining solution is in the Pareto-optimal set and, therefore, it always satisfies (25). Consequently, (17) becomes

$$\begin{aligned} g(\beta) &= A(\beta)^{a_{b,e}} B(\beta)^{a_b}, \text{ where} \\ B(\beta) &= (R + L^b) \\ &\quad \times \left[Q\left(\frac{h - \frac{\sqrt{N_b}}{K^b}\sigma_w}{\sigma_n} \right) - Q\left(\frac{h - \frac{\beta\sqrt{N_b}}{K^b}\sigma_w}{\sigma_n} \right) \right], \\ A(\beta) &= (R + L^{b,e}) \\ &\quad \times \left[Q\left(\frac{h - \frac{\sqrt{N_b+N_e}}{K^{b,e}}\sigma_w}{\sigma_n} \right) \right. \\ &\quad \left. - Q\left(\frac{h - \frac{(1-\beta)N_b+N_e}{K^b\sqrt{N_b+N_e}}\sigma_w}{\sigma_n} \right) \right]. \end{aligned} \tag{32}$$

Note that Nash-Bargaining solution is always in the Pareto-optimal set, which is concave, and $g(\beta)$ is a concave function. Therefore, the above equation is maximized when the gradient of $g(\beta)$ equals to zero or when β is on the boundary.

From (32), if $\partial g(\beta)/\partial\beta = 0$, then

$$\begin{aligned} &\frac{N_b}{\sqrt{N_b+N_e}} a_{b,e} A'(\beta)B(\beta) = \sqrt{N_b} a_b A(\beta)B'(\beta), \text{ where} \\ &A'(\beta) = (R + L^{b,e}) \exp\left\{ -\frac{\left(h - \frac{(1-\beta)N_b+N_e}{K^{b,e}\sqrt{N_b+N_e}}\sigma_w \right)^2}{2\sigma_n^2} \right\}, \\ &B'(\beta) = (R + L^b) \exp\left\{ -\frac{\left(h - \frac{\beta\sqrt{N_b}}{K^b}\sigma_w \right)^2}{2\sigma_n^2} \right\}. \end{aligned} \tag{33}$$

Note that both $B(\beta)$ and $\partial A(\beta)/\partial\beta$ are increasing functions of β, while $A(\beta)$ and $\partial B(\beta)/\partial\beta$ are decreasing functions of β. Thus, the solution of (33) is a monotonically decreasing function of $a_b/a_{b,e}$. It implies that the subgroup of colluders with a larger bargaining power benefits more than the others by bargaining. Depending on the criteria of setting bargaining power in the Nash-Bargaining problem, the bargaining power may change in different colluder social networks. One of the most common bargaining powers is using the number of colluders, K^b and $K^{b,e}$.

Optimal Value of $L^{(i)}$: Note that in (33), both sides of the equation have the common term $(R + L^b)(R + L^{b,e})$ and can be eliminated. Hence, the Nash-Bargaining solution does not depend on the users' loss L^b and $L^{b,e}$. Therefore, the Nash-Bargaining solution can be considered as cheat-proof, that is, the bargained solution remains the same even the players cheat on the private information.

To conclude, both players SC^b and $SC^{b,e}$ can gain higher reward by reporting higher loss if the fairness criteria is absolute fairness, Max-Min, or Max-Sum. Also, the Nash-Bargaining solution is not influenced by the private information $L^{(i)}$ of each player. However, the loss is declared before the bargaining process, and at that time, the colluders do not know to which solution the bargaining process will converge. Therefore, both players SC^b and $SC^{b,e}$ have the incentive to report as much loss as possible, resulting in $L^b = L^{b,e} = L_{max}$ being the same for all colluders in the utility function definition (9).

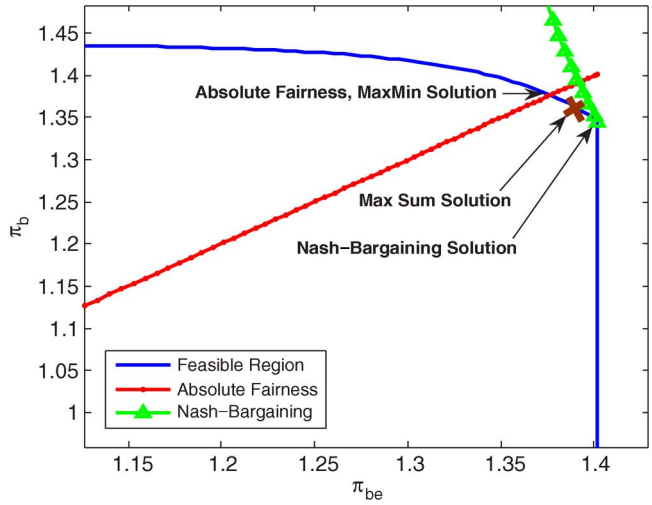


Fig. 5. Feasible region and bargaining solutions with utility function as in (18), $P_{fa} = 10^{-3}$, $N_b = N_e = 50\,000$, $K^b = 100$, $K^{b,e} = 150$, and $|U^b| = |U^{b,e}| = 250$.

4) Simulation Setting and Results: In our simulations, we first generate independent vectors following Gaussian distribution $\mathcal{N}(0,1)$, and then apply Gram-Schmidt orthogonalization to generate orthogonal fingerprints. The lengths of the fingerprints embedded in the base layer and the enhancement layer are $N_b = N_e = 50\,000$, and both two layers contain 20 frames, respectively. The total number of users is 500, where $U^b = U^{b,e}$. The probability of accusing an innocent user, P_{fa}, is 10^{-3}. Among the $K = 250$ colluders, $K^b = 100$ of them receive the fingerprinted base layer only, and the other $K^{b,e} = 150$ of the colluders receive fingerprinted copies of high resolution. Note that the feasible number of colluders depends on the fingerprint design. For example, if the fingerprint length is shorter or the colluders add larger noise during collusion, the attackers will choose less partners to collaborate with. But given any fingerprint setting, the same bargaining analysis can be applied.

Fig. 5 shows the feasible region and the four bargaining solutions in Section III-C with utility function as in (18), and bargaining powers in (17) are $a_b = 2$, $a_{b,e} = 3$, which is proportional to K^b and $K^{b,e}$. Compared to the absolute fairness solution, the Max-Sum solution gives the group with more people more utility, which is $SC^{b,e}$ in this case. The Nash-Bargaining with bargain power $a_b = 2$, $a_{b,e} = 3$ even more favors $SC^{b,e}$ since now the number of colluders works as the exponential term rather than the linear term in the Max-Sum solution. The other reason for such phenomenon is that in this simulation setting, K^b is much smaller than $K^{b,e}$ (2/3 of $K^{b,e}$); therefore, according to the definition of Nash-Bargaining solution in (17), the highest risk of SC^b, which can be considered as SC^b collude alone without $SC^{b,e}$, is much higher than that for $SC^{b,e}$. Therefore, the minimal payoff of SC^b, π^{b*}, is also smaller than the minimal payoff of $SC^{b,e}$, resulting in SC^b having more extra

payoff for bargaining, thus leading to better bargain position. Setting the bargaining power to be the number of colluders who receive different quality copies matches the real-world scenario: the group of colluders with more users acts together and should have more bargain power.

B. Scenario II: Reward is Proportional to Risk

In real-world social networks, reward is usually distributed unequally among the colluders. There are multiple reasons for the uneven reward distribution, for instance, each member has his/her own personal concern and position in the society. Therefore, some colluders might be more greedy and want to gain more reward in this collusion. Intuitively these colluders have to pay more cost (probability of being detected) to maintain fairness in the colluder social network. To address this issue, we also consider the more general utility function

$$\pi^{(i)} = -P_d^{(i)} * L^{(i)} + \left(1 - P_d^{(i)}\right) \times \frac{\theta}{\left(K^b (f^b)^{0.1} P_d^b + K^{b,e} (f^{b,e})^{0.1} P_d^{b,e}\right)/M} (f^{(i)})^{0.1} P_d^{(i)} \tag{34}$$

to illustrate the feasible region and the bargaining solution when the colluders distribute reward proportional to each copy's quality and risk (probability of being detected).

In this case, the reward each colluder gets is linear to his/her probability of being detected. Also, colluders who subscribe to higher resolution copy also gain more reward. The analysis of the four bargaining solutions are similar as in Section IV-A and not repeated here. Based on the same analysis, we can also conclude that both players have the incentive to report highest loss $L^b = L^{b,e} = L_{max}$ before collusion. Hence, we will show the bargaining solutions for this case by the simulations with both colluders claiming loss term L_{max}.

1) Simulation Setting and Results: To illustrate the feasible set and the bargaining solutions when the reward is proportional to risk, we run simulations with the same setting as in Section IV-B1. Fig. 7 shows the feasible region and the four bargaining solutions with utility function defined in (34). First, the whole feasible set is Pareto-optimal since π^b is a monotonically decreasing function of $\pi^{b,e}$ as shown in the figure. There is no non-Pareto-optimal feasible points as the straight line segment in Fig. 5. The reason for such result is that, although for all $\beta > 1 - \sqrt{N_e}(\sqrt{N_b + N_e} - \sqrt{N_e})/N_b$, $P_d^{b,e}$ is the same, but P_d^b keeps reducing as β increases. Hence, for all $u^{(i)}$ who receive higher-resolution copies, the denominator of the second term in the utility function (34) keeps increasing as β increases while the numerator is the same. As a result, unlike case 1 in which $\pi^{b,e}(\beta)$ is a constant for all $\beta > 1 - \sqrt{N_e}(\sqrt{N_b + N_e} - \sqrt{N_e})/N_b$, $\pi^{b,e}(\beta)$ is a decreasing function of β when $\beta > 1 - \sqrt{N_e}(\sqrt{N_b + N_e} - \sqrt{N_e})/N_b$ in case 2. Thus, all the points in the feasible set are also Pareto-optimal.

The four bargaining solution in Fig. 7 shows the same trend as in Fig. 5: the Max-Min solution is the same as the absolute fairness solution, the Max-Sum solution favors $SC^{b,e}$ better than that, and the Nash-Bargaining solution with $B_b = 2$, $B_{b,e} = 3$ gives $SC^{b,e}$ maximal utility. The same trend of the four bargaining solutions in these two cases shows our methodology can fit to different collusion problems once the utility function is defined since our analysis in on the bargaining level and the trend of the bargaining solutions are independent of utility function definitions. Nevertheless, the "absolute fairness solution" under proportional reward distribution also has proportional fairness characteristics.

Furthermore, comparing the feasible region in Figs. 5 and 7, it is clear that both the maximum utilities that SC^b and $SC^{b,e}$ can achieve are much higher if reward is distributed proportionally ($\pi^b_{max} = 1.441$ and $\pi^{b,e}_{max} = 1.403$ in Fig. 5 while $\pi^b_{max} = 2.182$ and $\pi^{b,e}_{max} = 1.947$ in Fig. 7). These maximal utilities happen for extreme β value when it approaches to 1 or $1 - \sqrt{N_e}(\sqrt{N_b + N_e} - \sqrt{N_e})/N_b$, under which one of P_d^b or $P_d^{b,e}$ is much higher than the other, and one of SC^b or $SC^{b,e}$ earn most of the reward resulting in high payoff.

C. Scenario III: Time-Sensitive Bargaining

In this section, we take the second utility functions as in Section IV as examples to illustrate the time-sensitive bargaining in the colluder social network. Since in real-world social networks, reward is usually distributed unequally because every member has different personal concern and position in the society, thus, we consider the general utility function as in (34) to illustrate the time-sensitiveness when the colluders distribute reward proportional to each copy's quality and the user's risk (probability of being detected). We apply our analysis to the real video data and verify our results.

D. Simulation Setting and Results

In our simulations, we test over the first 40 frames of "carphone", and use $F_b = \{1, 3, \cdots, 39\}$ and $F_e = \{2, 4, \cdots, 40\}$ as an example of the temporal scalability. The lengths of the fingerprints embedded in the base layer and enhancement layer are $N_b = 85\,938$ and $N_e = 85\,670$, respectively. We assume that there are a total of $M = 500$ users and $|\mathbf{U}^b| = |\mathbf{U}^{b,e1}| = 250$. We first generate independent vectors following Gaussian distribution $\mathcal{N}(0, 1/9)$, and then apply Gram-Schmidt orthogonalization to generate orthogonal fingerprints for different users.

During collusion, the colluders apply the intra-group collusion followed by the inter-group collusion, and follow the above analysis when choosing the collusion parameters. In our simulations, we adjust the power of the additive noise such that $\|\mathbf{n}_j\|^2 = \|JND_j \mathbf{W}_j^{(i)}\|^2$ for every frame j in the video sequence. The probability of accusing an innocent user, P_{fa}, is 10^{-3}. Among the $K = 250$ colluders, $K^b = 100$ of them receive the fingerprinted base layer only, and the other $K^{b,e} = 150$ of the colluders receive fingerprinted copies of high resolution.

Fig. 6 shows the bargaining equilibrium versus the number of stages that the colluders need to make agreement (Section III-C) with utility function as in (34), and different discount factors: Fig. 6(a) uses $\delta_b = 0.7$, $\delta_{b,e} = 0.85$, and Fig. 6(b) is the result of $\delta_b = 0.7$, $\delta_{b,e} = 0.85$. The feasible region and the Pareto-optimal set with the same utility function for the first stage of the game is shown in Fig. 3. It is clear from Fig. 6 that both colluders have incentive to finish the bargaining process as soon as possible under both settings of discount constants, especially

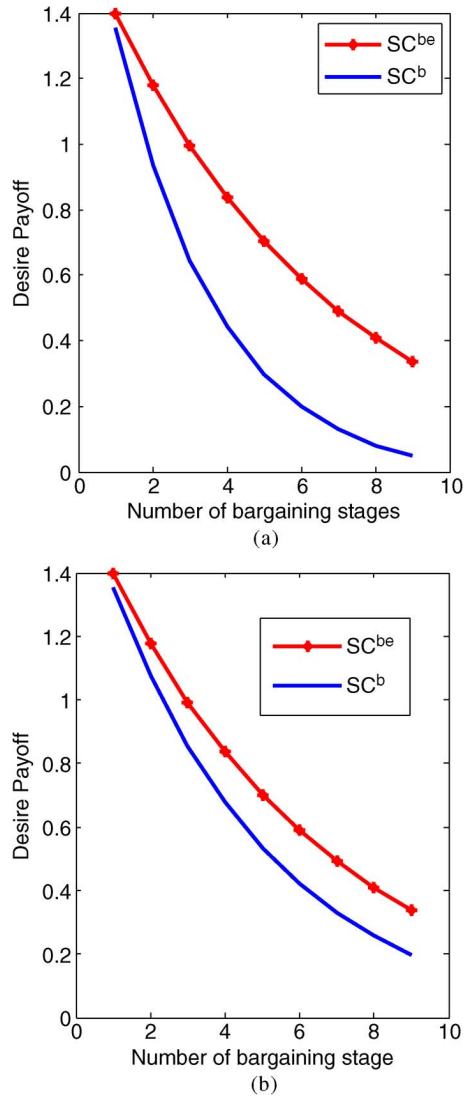


Fig. 6. Utilities of SC_b and $SC^{b,e}$ versus number of bargaining rounds. $P_{fa} = 10^{-3}$, $N_b = N_e = 50000$, $K^b = 100$, $K^{b,e} = 150$, and $|U^b| = |U^{b,e}| = 250$ with different discount factors. (a) $\delta_b = 0.7$ and $\delta_{b,e} = 0.85$. (b) $\delta_b = 0.8$ and $\delta_{b,e} = 0.85$.

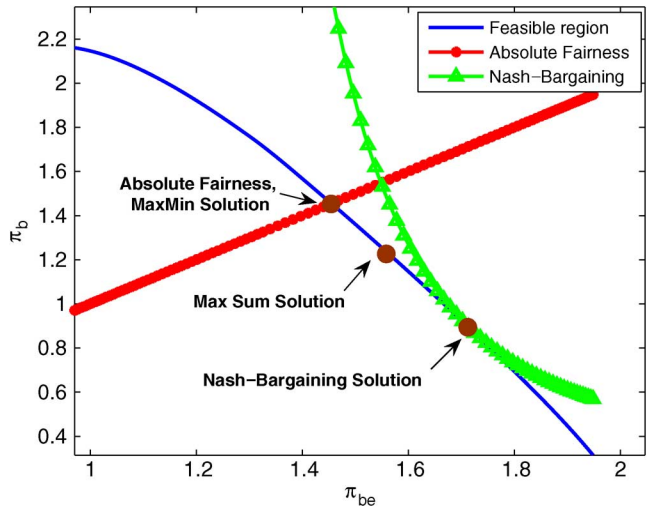


Fig. 7. Feasible region and the four fairness solutions with utility function as in (34), $P_{fa} = 10^{-3}$, $N_b = N_e = 50000$, $K^b = 80$, $K^{b,e} = 170$, and $|U^b| = |U^{b,e}| = 250$.

for SC^b whose utility decays faster than $SC^{b,e}$. Therefore, at the very first bargaining stage, the first-mover will offer based on the equilibrium by solving (10) and (11). Thus, SC^b would let $SC^{b,e}$ to take the advantage of offering first. It is clear by comparing Fig. 6(a) and (b) that higher discount factor results in higher payoff. The discount factors $\delta_b, \delta_{b,e}$ can also be considered as the power of bargaining for SC^b and $SC^{b,e}$. For instance, if the two groups of colluders cannot make agreement and they decide to collude within groups and generate two colluded copy with different qualities, then apparently SC^b would get much less reward than $SC^{b,e}$ since their colluded copy has lower quality. Thus, SC^b has much more intention to cooperate with $SC^{b,e}$, and this intention leads to less bargaining power.

V. Equilibriums of the Detector-Colluder Game

In the previous sections, we have discussed how the colluders bargain with each other and what are the fair types of collusion that can satisfy all colluders and lead to a successful collusion. A successful collusion must not only be fair to all colluders but also maximize all colluders' utility under the fairness constraint. On the other hand, the fingerprint detector also has to adjust its strategy according to the collusion type to achieve the highest probability of detection. Therefore, there exists complex dynamics among the colluders and the fingerprint detector, and they altogether also form a social network, called the multimedia fingerprint social network [26]. Hence, the bargaining solutions that the colluders are willing to follow have to be the best response to the detector's optimal strategy and form equilibriums between the fingerprint detector and the colluders.

Hence, in this section, we will prove that the bargaining solutions we discussed in Sections III and IV are also the equilibria strategies for the colluders in the detector-colluder game, thus being the best move for the colluders under different fairness constraints.

A. Stackelberg Game Model of Dynamics Between Colluders and Fingerprint Detector

To capture users' behavior in strategic situations, in which an individual's success in making choices depends on the choices of others, Game Theory [2], [3] is a useful tool to model the complex dynamics among multimedia social network members. Therefore, to analyze the optimal strategies of both fingerprint detector and the colluders under the fairness constraints, we formulate the interaction between the two groups of the multimedia fingerprinting social network users as a game with two players: the colluders acting as one single player and the fingerprint detector as the other [26].

Game between colluders and fingerprint detector

- **Players**: There are two players: colluders who make the move first as the leader, followed by the follower, who is the fingerprint detector that applies detection after receiving a suspicious copy.

- **Payoff Function**: In this game, what colluders gain is the lost of the detectors; thus, the two groups of users, colluders and the fingerprint detector in the fingerprinting social network, have totally conflicting objectives. Therefore, the sum of the utilities of all colluder equals to the utility of the digital right enforcer with negative sign. Based on the utility of each individual colluder during bargaining as in (9) and the assumption that all the colluders, the payoff functions of the colluders, and the fingerprint detector can be defined as

$$\pi_C = R_{sum} - P_d^b K^b (L_{max} + R^b) - P_d^{b,e} K^{b,e} (L_{max} + R^{b,e}) \quad \text{and} \quad \pi_D = -\pi_C \tag{35}$$

  where R_{sum} is the total reward of redistributing the colluded copy, and π_C and π_D are the utility functions for colluders and the fingerprint detector, respectively.
  Based on the utility function definition as in (35), all colluders has the same goal of minimizing his/her risk of being detected $P^{(i)}$ under fairness constraint. From the detector's point of view, the colluder's gain is the loss of the digital right enforcer, so we can define the detector's payoff as $\pi_D = -\pi_C$. Therefore, to maximize his/her own payoff, the fingerprint detector also has the incentive to maximize the probability of catching colluders in both groups, P_d^b and $P_d^{b,e}$.
- **Colluders' Strategies**: The colluders' strategies are the set of all possible collusion parameter $\boldsymbol{\beta}$ that achieves fairness, for each colluder leads to one strategy for the colluders in the colluder-detector game. Therefore, the colluders have an uncountably infinite number of strategies.
- **Detector's Strategies**: Since the fingerprinting is Gaussian and orthogonal and the noise added by colluders is Gaussian, the best detector is the correlation detector. Upon receiving the suspicious copy, the correlation-based fingerprint detector can decide which part of the suspicious copy he/she is going to use for detection. Note that for users in SC^b, since their copies only contain the base layer, the detector only has one choice, which is utilizing the whole base layer for identification.
  Hence, as discussed in the previous work [26], the detector's strategies includes the collective detector, single-layer detector, and the self-probing detector. The collective detector uses the whole sequence to identify $SC^{b,e}$; the single-layer detector uses either base layer or enhancement layer to identify $SC^{b,e}$; the self-probing detector probes the side information (the mean of the detection statistics) first, and then chooses to use the collective detector or the single-layer detector for detection.

In this game, there are multiple detection statistics that the fingerprint detector can use to identify colluders. However, by the analysis and simulation results shown in our previous work [26], the self-probing detector can always achieve better or equal performance as all other detectors (collective detector and single-layer detector). Thus, to maximize his/her payoff, the fingerprint detector always probes side information about collusion and selects the detection statistics that have the largest chance of successfully capturing colluders.

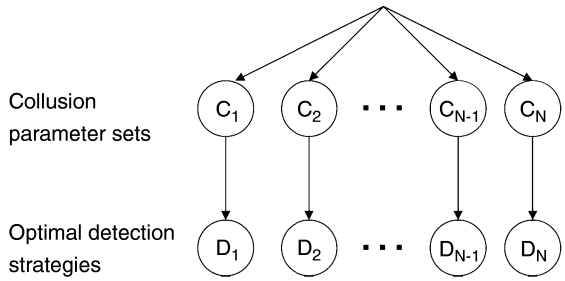


Fig. 8. Game tree illustration of the colluder-detector dynamics. $C_1, C_2, \cdots, C_N$ are the N possible sets of collusion parameters that achieve bargaining solutions under various fairness constraints when the fingerprint detector uses the optimal detection statistics to identify colluders, while $D_1, D_2, \cdots, D_N$ are the corresponding optimal fingerprint detection strategies.

From the angle of game theoretical analysis, probing side-information is equivalent to observing the colluders' action. The near-optimal performance of the self-probing detector implies the detector (follower in this game) can observe the colluders' action completely. Furthermore, to provide the best protection of multimedia content, here we assume the worst-case scenario that the colluders know exactly the detector's strategy, which means the colluders (leader) know that the detector observes their action. Hence, colluders as the leader have perfect knowledge of the detection strategies that the fingerprint detector will use, because the detector has no incentive to deviate from the self-probing detector. Therefore, the detector has no means of committing to a follower action that deviates from the self-probing detector, which is the best response, and the colluders know this. Therefore, the colluder-detector game is a Stackelberg game [3] with perfect information.

B. Equilibrium Analysis

With the self-probing fingerprint detection process, for each type of collusion, the fingerprint detector can always choose the detection statistics that give the best probability of detection performance for $SC^{b,e}$. Such phenomenon can be illustrated as the game tree shown in Fig. 8. In this game, assuming that there are N possible collusion strategies under the fairness constraint (can be either absolute fairness, Max-Min fairness, Max-Sum fairness, Nash-Bargaining, or the time-sensitive bargaining), the colluders first choose the fair collusion strategy based on Section III-C, and then the fingerprint detector selects the optimal detection statistics.

Since the follower (detector) can observe the leader's (colluders') strategy, the equilibrium of the game model can be solved by backward induction. By backward induction, since both the colluders and the fingerprint detector know that the optimal detection statistics will be used to identify colluders, once attackers determine the collusion strategy, their payoff is fixed and the colluders can accurately estimate their payoff. The colluders consider what the best response of the detector is, i.e., how the detector will respond once he/she observes the leader's strategy. The colluders then pick a strategy that maximizes its payoff, anticipating the predicted response of the detector. The detector actually observes this by using the self-probing detector and in equilibrium picks the expected quantity as a response.

Hence, the equilibrium of the detector-colluder game is as follows: during collusion, colluders should always consider the self-probing detector as the detector's strategy, and find the bargaining solutions under the fairness constraint. On the other hand, the detector always uses the self-probing detector. Since the bargaining solutions discussed in Sections III and IV are based on the self-probing detector, they are the equilibria strategies of the colluders.

VI. Conclusions

This paper studies the bargaining behavior of colluders after they agree to form a social network. We first model the fairness dynamics among colluders as a noncooperative game, in which each colluder aims to maximize his/her own utility through bargaining to achieve fair agreement. We discuss a more general model of utility functions which allows uneven reward-distribution, and analyze human behavior by four bargaining criteria: absolute fairness, Max-Min, Max-Sum, and Nash-Bargaining solution. Then we extend our model to address the special time-sensitive property of multimedia contents, analyze the colluders' behavior by modeling collusion as a time-sensitive bargaining process, and find the equilibrium of the bargaining game. Our analysis shows that in the colluder social network, the colluders will make agreement at the first bargaining stage and reach equilibrium; and if the market value of the colluded copy is not time-sensitive, colluders choose different points in the feasible set, depending on the colluders' definition of "fairness" and their agreement on how to distribute the risk and the reward among themselves. Furthermore, we also prove that all the bargaining solutions that satisfy the fairness criteria are also the equilibrium in the colluder-detector game. Such result shows the bargaining solutions are the best strategies for the colluders under the fairness criteria with the corresponding optimal correlation-based detector that all colluders would satisfy and not deviate from. Therefore, the possible types of collusion and the possible number of colluders can be reduced to the set of these feasible bargaining solutions. This paper provides a methodology that can fit human behavior analysis in different social networks.

References

[1] H. Zhao, W. S. Lin, and K. J. R. Liu, "Behavior modeling and forensics for multimedia social networks: A case study in multimedia fingerprinting," *IEEE Signal Process. Mag.*, to be published.

[2] G. Owen, *Game Theory*, 3rd ed. New York: Academic, 1995.

[3] D. Fudenberg and J. Tirole, *Game Theory*. Cambridge, MA: MIT Press, 1991.

[4] F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video," *Signal Process.*, vol. 66, no. 3, pp. 283–301, 1998.

[5] K. J. R. Liu, W. Trappe, Z. J. Wang, M. Wu, and H. Zhao, *Multimedia Fingerprinting Forensics for Traitor Tracing*, ser. EURASIP Book Series on Signal Processing and Communications. New York: Hindawi, 2005.

[6] I. Cox and J. P. Linnartz, "Some general methods for tampering with watermarking," *IEEE J. Select. Areas Commun.*, vol. 16, no. 4, pp. 587–593, May 1998.

[7] G. Doerr, J. L. Dugelay, and L. Grange, "Exploiting self-similarities to defeat digital watermarking systems: A case study on still images," in *Proc. 2004 ACM Multimedia and Security Workshop*, 2004.

[8] Z. J. Wang, M. Wu, H. Zhao, W. Trappe, and K. J. R. Liu, "Anti-collusion forensics of multimedia fingerprinting using orthogonal modulation," *IEEE Trans. Image Process.*, vol. 14, no. 6, pp. 804–821, Jun. 2005.

[9] F. Ergun, J. Killian, and R. Kumar, "A note on the limits of collusion-resistant watermarks," in *Proc. Advances in Cryptology—EuroCrypto '99, Lecture Notes in Computer Science*, 2001, vol. 1592, pp. 140–149.

[10] H. Stone, Analysis of Attacks on Image Watermarks With Randomized Coefficients, NEC Research Inst., Tech. Rep. 96-045, 1996.

[11] D. Kirovski and M. K. Mihcak, "Bounded Gaussian fingerprints and the gradient collusion attack," in *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing*, Mar. 2005, vol. II, pp. 1037–1040.

[12] M. Holliman and N. Memon, "Counterfeiting attacks and blockwise independent watermarking techniques," *IEEE Trans. Image Process.*, vol. 9, no. 3, pp. 432–441, Mar. 2000.

[13] H. Zhao and K. J. R. Liu, "Behavior forensics for scalable multiuser collusion: Fairness versus effectiveness," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 3, pp. 311–329, Sep. 2006.

[14] H. V. Zhao and K. J. R. Liu, "Traitor-within-traitor behavior forensics: Strategy and risk minimization," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 4, pp. 440–456, Dec. 2006.

[15] F. Zane, "Efficient watermark detection and collusion security," in *Proc. Financial Cryptography, Lecture of Notes in Computer Science*, Feb. 2000, vol. 1962, pp. 21–32.

[16] J. Dittmann, P. Schmitt, E. Saar, J. Schwenk, and J. Ueberberg, "Combining digital watermarks and collusion secure fingerprints for digital images," *SPIE J. Electron. Imag.*, vol. 9, no. 4, pp. 456–467, Oct. 2000.

[17] Z. J. Wang, M. Wu, W. Trappe, and K. J. R. Liu, "Group-oriented fingerprinting for multimedia forensics," *EURASIP J. Appl. Signal Process., Special Issue on Multimedia Security and Rights Management*, vol. 2004, no. 14, pp. 2142–2162, Nov. 2004.

[18] S. He and M. Wu, "Joint coding and embedding techniques for multimedia fingerprinting," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 2, pp. 231–247, Jun. 2006.

[19] W. S. Lin, H. V. Zhao, and K. J. R. Liu, "Fairness dynamics in multimedia fingerprinting social networks," in *Proc. IEEE Int. Conf. Image Processing*, Oct. 2008, to be published.

[20] Y. Wang, J. Ostermann, and Y. Zhang, *Video Processing and Communications*, 1st ed. Englewood Cliffs, NJ: Prentice-Hall, 2001.

[21] I. Cox, J. Killian, F. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673–1687, Dec. 1997.

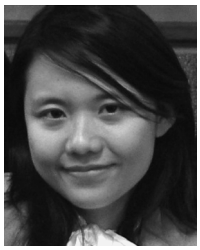
[22] C. Podilchuk and W. Zeng, "Image adaptive watermarking using visual models," *IEEE J. Select. Areas Commun.*, vol. 16, no. 4, pp. 525–540, May 1998.

[23] H. Zhao, M. Wu, Z. J. Wang, and K. J. R. Liu, "Forensic analysis of nonlinear collusion attacks for multimedia fingerprinting," *IEEE Trans. Image Process.*, vol. 14, no. 5, pp. 646–661, May 2005.

[24] W. S. Lin, H. V. Zhao, and K. J. R. Liu, "Scalable multimedia fingerprinting forensics with side information," in *Proc. IEEE Int. Conf. Image Processing*, Oct. 2006, pp. 2293–2296.

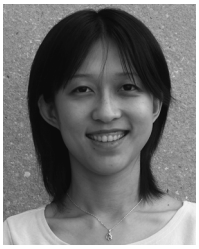
[25] M. J. Osborne and A. Rubinstein, *A Course in Game Theory*. Cambridge, MA: MIT Press, 1994.

[26] W. S. Lin, H. V. Zhao, and K. J. R. Liu, "Behavior forensics with side information for multimedia fingerprinting social networks," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pp. 911–927, Dec. 2009.



W. Sabrina Lin (M'06) received the B.S. and M.S. degrees in electrical engineering from National Taiwan University, Taipei, in 2002 and 2004, respectively, and the Ph.D. degree from the Electrical and Computer Engineering Department, University of Maryland, College Park, in 2009.

She is a Research Associate at the University of Maryland, College Park. Her research interests are in the areas of information security and forensics, multimedia signal processing, and multimedia social network analysis. She received the University of Maryland Future Faculty Fellowship in 2007.



H. Vicky Zhao (M'05) received the B.S. and M.S. degrees from Tsinghua University, Beijing, China, in 1997 and 1999, respectively, and the Ph.D. degree from University of Maryland, College Park, in 2004, all in electrical engineering.

She was a Research Associate with the Department of Electrical and Computer Engineering and the Institute for Systems Research, University of Maryland, College Park, from January 2005 to July 2006. Since August 2006, she has been an Assistant Professor with the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, AB, Canada. Her research interests include information security and forensics, multimedia social networks, digital communications, and signal processing.

Dr. Zhao received the IEEE Signal Processing Society (SPS) 2008 Young Author Best Paper Award. She co-authored the book *Multimedia Fingerprinting Forensics for Traitor Tracing* (New York: Hindawi, 2005). She is an Associate Editor for the IEEE SIGNAL PROCESSING LETTERS and the *Journal of Visual Communication and Image Representation*.

K. J. Ray Liu (F'03) was named a Distinguished Scholar-Teacher of the University of Maryland, College Park, where he is Christine Kim Eminent Professor in Information Technology, in 2007. He leads the Maryland Signals and Information Group conducting research encompassing broad aspects of wireless communications and networking, information forensics and security, multimedia signal processing, and biomedical engineering. His recent books include *Cognitive Radio Networking and Security: A Game Theoretical View* (Cambridge, U.K.: Cambridge Univ. Press, 2010); *Behavior Dynamics in Media-Sharing Social Networks*(Cambridge, U.K.: Cambridge Univ. Press, to be published); *Handbook on Array Processing and Sensor Networks* (Piscataway, NJ: IEEE-Wiley, 2009); *Cooperative Communications and Networking* (Cambridge, U.K.: Cambridge Univ. Press, 2008); *Resource Allocation for Wireless Networks: Basics, Techniques, and Applications* (Cambridge, U.K.: Cambridge Univ. Press, 2008); *Ultra-Wideband Communication Systems: The Multiband OFDM Approach* (Piscataway, NJ: IEEE-Wiley, 2007); *Network-Aware Security for Group Communications* (New York: Springer, 2007); and *Multimedia Fingerprinting Forensics for Traitor Tracing* (New York: Hindawi, 2005).

Dr. Liu is the recipient of numerous honors and awards including IEEE Signal Processing Society Technical Achievement Award, Distinguished Lecturer, and various Best Paper Awards from IEEE and EURASIP. He also received various teaching and research recognitions from the University of Maryland including university-level Invention of the Year Award; and Poole and Kent Senior Faculty Teaching Award and Outstanding Faculty Research Award, both from the A. James Clark School of Engineering. He is recognized as an ISI Highly Cited Author in Computer Science. He is a Fellow of AAAS. He is President-Elect and was Vice President—Publications of the IEEE Signal Processing Society. He was the Editor-in-Chief of the IEEE SIGNAL PROCESSING MAGAZINE and the founding Editor-in-Chief of *EURASIP Journal on Advances in Signal Processing*.