GAME-THEORETIC ANALYSIS OF MAXIMUM-PAYOFF MULTIUSER COLLUSION

H. Vicky Zhao[*], *W. Sabrina Lin*[†] *and K. J. Ray Liu*[†]

[*] ECE Dept., University of Alberta, Edmonton, AB T6G 2V4 Canada
[†] ECE Dept., University of Maryland, College Park, MD 20742 USA

ABSTRACT

Multiuser collusion is an effective attack against traitor-tracing multimedia fingerprinting, where a group of attackers collectively mount attacks to reduce their risk of being detected. During collusion, each attacker wishes to maximize his or her own payoff. To resolve the conflict, colluders have to negotiate with each other and achieve fair collusion. An attacker also needs to decide with whom he or she wants to collude. Though colluding with more people helps further reduce the risk, it also makes an attacker share with more people the rewards from illegal usage of multimedia. This paper uses game theory to model the complex colluder dynamics and analyzes the tradeoff between the risk and the rewards. We study how the selection of fellow attackers affects each colluder's utility, and analyze the optimum strategies that maximize colluders' payoffs.

Index Terms— Multimedia forensics, security, game theory

1. INTRODUCTION

Digital fingerprinting is an emerging technology that offers proactive post-delivery protection of multimedia. It labels each distributed copy with the corresponding user's ID, known as a fingerprint, which can be used to trace traitors who use their copies illegally. Multiuser collusion attack is a powerful attack against digital fingerprinting, where a group of attackers collectively mount attacks to attenuate the identifying fingerprints. To design collusion-resistant fingerprints and provide reliable traitor-tracing performance, analysis of the strategies and the effectiveness of collusion is a crucial part of research in multimedia forensics.

Colluders form a special social network during collusion. They share the rewards from the illegal usage of multimedia content as well as the risk of being detected by the digital rights enforcer. Every colluder wishes to maximize his or her own payoff, and they have conflicting objectives. They negotiate with each other to resolve this conflict and achieve a notion of fairness [1]. A game-theoretic framework was proposed in [2] to analyze this complex dynamics among colluders, and the negotiation among colluders was modeled as a bargaining problem.

In addition to fairness, another important issue for colluders is to select with whom to collude and decide how many people to collude with. Most prior work considered the scenario where colluders aim to minimize their risk of being detected during collusion. In this scenario, when there are more colluders, the energy of each contributing fingerprint is reduced by a larger ratio, and thus, each attacker has a smaller probability of being detected [1]. Therefore, colluders should find as many colluders as possible to minimize their risk. However, a larger total number of colluders means sharing the rewards with more people and thus benefiting less from collusion. Thus, from reward maximization's point of view, attackers prefer to collude with fewer people. Colluders need to address this tradeoff between the risk and the rewards, which was seldom studied in the current literature.

This paper focuses on the tradeoff analysis between the risk and the rewards during collusion and analyzes the optimum strategies that an attacker should follow to select with whom to collude. We follow the game-theoretic modeling of colluder dynamics in [2], and consider both the colluders' probability of being detected and the rewards from illegal usage of multimedia when defining the utility functions. In this paper, we investigate the impact of the total number of colluders on each attacker's utility, and analyze the optimum fellow-attacker-selection strategies that maximize their payoffs.

The rest of the paper is organized as follows. Section 2 introduces the multimedia fingerprinting system model, and Section 3 discusses the game-theoretic formulation of the complex colluder dynamics. Section 4 studies the impact of the number of colluders on each attacker's utilities, and analyzes how an attacker should select with whom to collude in order to maximize his or her payoff. Conclusions are drawn in Section 5.

2. MULTIMEDIA FINGERPRINTING SYSTEM MODEL

2.1. Scalable Video Coding

With recent advances in networks, communications and multimedia, scalable video coding is widely adopted to accommodate heterogenous networks and devices with different storage and computing capability. It decomposes video sequence into different layers of different priority. The base layer contains the most important information of the video and is received by all users, and the enhancement layers gradually refine the reconstructed sequence at the decoder's side and are only received by users with sufficient bandwidth. Without loss of generality, in this paper, we consider two-layer temporal scalability, and we use frame skipping and frame copying to implement temporal decimation and interpolation, respectively [3]. For example, with MPEG-2 video coding, the base layer may include all the I frames, and the enhancement layer contains all the P and B frames.

Define F_b and F_e as the sets containing the indices of the frames that are encoded in the base layer and the enhancement layer, respectively. $|F_b|$ and $|F_e|$ are the number of frames in the base layer and the enhancement layer, respectively. For user $\mathbf{u}^{(i)}$, $F^{(i)}$ contains the indices of the frames that he or she receives from the content owner, and define $f^{(i)} = |F^{(i)}|/(|F_b| + |F_e|)$ as the normalized temporal resolution. If $F^{(i)} = F_b$ and $\mathbf{u}^{(i)}$ receives a low-resolution copy, then $f^{(i)} = f_b \triangleq |F_b|/(|F_b| + |F_e|) < 1$. If $\mathbf{u}^{(i)}$ receives both layers from the content owner, then $f^{(i)} = 1$.

2.2. Multimedia Fingerprinting

Fingerprint Embedding We use the spread spectrum embedding [4, 5] 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 $\mathbf{W}_j^{(i)}$ of the same

The author can be reached at vzhao@ece.ualberta.ca, {wylin, kjrliu}@umd.edu.

length as $\mathbf{S}_j$. We consider orthogonal fingerprint modulation [1], where fingerprints assigned to different users are orthogonal to each other and have the same energy. The fingerprinted frame j that $\mathbf{u}^{(i)}$ receives is $\mathbf{X}_j^{(i)} = \mathbf{S}_j + JND_j\mathbf{W}_j^{(i)}$. JND [5] here is used to control the energy of the embedded fingerprints and make the fingerprinted copy be perceptually the same as the original one.

Multi-user Collusion During collusion, a few attackers mount attack collectively and generate a new copy where the fingerprints are attenuated. Let F^c be the set containing the indices of the frames in the colluded copy, and $f_c = |F_c|/(|F_b| + |F_e|)$ is the normalized resolution of the colluded copy. $f_c = f_b$ when colluders generate a copy with the base layer only, and $f_c = 1$ when the colluded copy includes both layers.

In this paper, we consider the scenario where colluders wish to generate a high-resolution copy whenever possible. Following the two-stage collusion model in [6], colluders first divide into two non-overlapping subgroups: SC^b is the set including the indices of the colluders who receive the base layer only, and SC^{be} contains the indices of the colluders who subscribe to the high-quality version. $K^b = |SC^b|$ and $K^{be} = |SC^{be}|$ are the numbers of colluders in SC^b and SC^{be}, respectively. Then, colluders apply the intra-group collusion: for each frame j 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 the video sequence, colluders in SC^{be} calculate $\mathbf{Z}_j^{be} = \sum_{k\in SC^{be}}\mathbf{X}_j^{(k)}/K^{be}$. Finally, the colluders apply the inter-group collusion: for each frame j in the base layer, colluders generate $\mathbf{V}_j = \beta\mathbf{Z}_j^b + (1-\beta)\mathbf{Z}_j^{be} + \mathbf{n}_j$ where $0 \le \beta \le 1$ is the collusion parameter; and for each frame j in the enhancement layer, $\mathbf{V}_j = \mathbf{Z}_j^{b,e} + \mathbf{n}_j$. $\mathbf{n}$ is additive noise to further deter the detection performance.

Fingerprint Detection When identifying colluders, the fingerprint detector first extracts the fingerprint $\mathbf{Y}$ from the colluded copy $\mathbf{V}$. For each user $\mathbf{u}^{(i)}$, to measure the similarity between the extracted fingerprint $\mathbf{Y}$ and the original fingerprint $\mathbf{W}^{(i)}$, the fingerprint detector calculates the correlation-based detection statistic $TN^{(i)} = \langle\mathbf{Y}, \mathbf{W}^{(i)}\rangle/||\mathbf{W}^{(i)}||$, compares it with a pre-determined threshold h, and identifies $\mathbf{u}^{(i)}$ as a suspicious colluder if $TN^{(i)} > h$.

3. GAME-THEORETIC FORMULATION OF COLLUDER DYNAMICS

During collusion, different attackers have different objectives, and an important issue is to reach an agreement regarding how to *fairly* distribute the risk and the rewards. Following [2], we model this complex dynamics among colluders as a bargaining problem, and use game theory [7] to analyze how colluders negotiate with each other.

3.1. Definition of the Utility Function

The first step in the game-theoretic formulation is to define the utility function π. Following [2], we consider a simple scenario where colluders who receive copies of the same resolution agree to have equal payoffs. Thus, there are two players in the game: colluders in SC^b act as a single player and they have the same utility π^b, while those in SC^{be} act as a single player and have the same utility π^{be}.

Taking into consideration both the risk and the rewards, a natural definition of the utility function is the expected payoff that $\mathbf{u}^{(i)}$ receives by participating in collusion, that is, $\pi^{(i)} = -P_d^{(i)}L^{(i)} + (1-P_d^{(i)})R^{(i)}$. Here, $P_d^{(i)}$ is $\mathbf{u}^{(i)}$'s probability of being detected, $L^{(i)}$ is his or her loss if $\mathbf{u}^{(i)}$ is captured by the fingerprint detector, and $R^{(i)}$ is the rewards that $\mathbf{u}^{(i)}$ receives if he or she successfully escapes being detected. In this paper, we normalize $L^{(i)} = 1$ for all colluders. Also, we let $R^{(i)}$ be an increasing function of the colluded copy's resolution f_c. This is because when the colluded copy has a higher resolution and better quality, colluders can redistribute the copy at a higher price and thus profit more from collusion. In addition, we consider the scenario where colluders receive more rewards if they contribute more, and let $R^{(i)}$ be an increasing function of $f^{(i)}$, the normalized resolution of the fingerprinted copy from $\mathbf{u}^{(i)}$.

Based on the above discussion, we define the utility function as

$$\begin{aligned}\pi^{(i)} &= -P_d^{(i)} + (1-P_d^{(i)})R^{(i)} \quad \text{where}\\ R^{(i)} &= (f_c)^\gamma \frac{(f^{(i)})^\gamma}{K^b(f_b)^\gamma + K^{be}}\theta^{(i)}. \end{aligned} \tag{1}$$

The denominator in (1) is the normalization term.

There are two parameters in (1), γ and $\theta^{(i)}$. γ describes the importance of the base layer to the the reconstructed video sequence. Let us consider an example where $|F_b| = |F_e|$ and $f_b = 0.5$. Even though the base layer includes only half of the frames in the sequence, it conveys more than 50% of information about the content. Those frames in the enhancement layer only help improve the quality of the reconstructed sequence. So we select γ such that $(f_b)^\gamma \ge f_b$. Since $0 < f_b < 1$, γ should be in the range $[0, 1]$ and a smaller value of γ indicates that the base layer contains more information of the video. In this paper, we use $\gamma = 1/3$ as an example, and the analysis for other values is similar. $\theta^{(i)}$ in (1) is a parameter for $\mathbf{u}^{(i)}$ to address the tradeoff between the risk and the rewards. A larger $\theta^{(i)}$ indicates that $\mathbf{u}^{(i)}$ prefers to benefit more from collusion at a cost of higher risk. In our paper, we consider a simple case where $\theta^{(i)}$ are the same for all colluders and $\theta^{(i)} = \theta$. In summary, if colluders generate a colluded copy of high resolution and $f_c = 1$, we have

$$\begin{aligned} R^{(i)} &= R^b \triangleq \frac{(f_b)^\gamma\theta}{K^b(f_b)^\gamma + K^{be}} \quad \text{for all } i \in SC^b\\ \text{and } R^{(i)} &= R^{be} \triangleq \frac{\theta}{K^b(f_b)^\gamma + K^{be}} \quad \text{for all } i \in SC^{be}. \end{aligned} \tag{2}$$

3.2. The Bargaining Process

The collusion parameter β determines the colluders' probability of being detected ($P_d^{(i)}$) and thus their utilities ($\pi^{(i)}$) [2]. Each colluder prefers the β that maximizes his or her own payoff. To resolve the conflict, they negotiate with each other on the selection of β.

Given the utility function, colluders find the feasible set $\mathbf{S} = \{(\pi^b, \pi^{be}) \in \mathbb{R}^2\}$, where for every $(\pi^b, \pi^{be}) \in \mathbf{S}$, it is possible for colluders to act together and obtain the utilities π^b and π^{be}, respectively. Among all the possible solutions in the feasible set, those in the Pareto-Optimal set are of particular interest to colluders. A solution is Pareto optimal if no one can further increase his or her utility without decreasing others'. In a bargaining situation like this, colluders would always like to settle at a Pareto-Optimal point.

From [2], the Pareto-Optimal set of the colluder game corresponds to the solutions where colluders select $0 \le \beta \le \tilde{\beta} \triangleq 1 - (\sqrt{N_e \cdot N} - N_e)/N_b$. N_b and N_e are the lengths of the fingerprints embedded in the base layer and the enhancement layer, respectively, and $N = N_b + N_e$. It was shown in [2] that, when the additive noise $\mathbf{n}$ is i.i.d. Gaussian $\mathcal{N}(0, \sigma_n^2)$, given $0 \le \beta \le \tilde{\beta}$, colluder $\mathbf{u}^{(i)}$'s probability of being detected is

$$P_d^{(i)} = Q\left(\frac{h - \mu^{(i)}}{\sigma_n}\right), \quad \text{where}$$

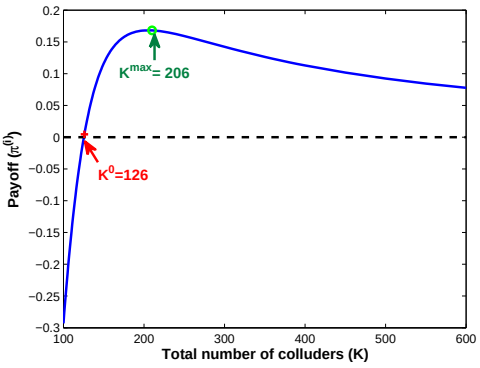

Fig. 1. $\tilde{\pi}$ when all colluders receive the high-resolution copies.

$$\begin{aligned}\mu^{(i)} &= \mu_b \stackrel{\triangle}{=} \beta\frac{\sqrt{N_b}}{K^b}\sigma_w \quad \text{if } i \in SC^b, \quad \text{and}\\ \mu^{(i)} &= \mu_{be} \stackrel{\triangle}{=} \frac{(1-\beta)N_b + N_e}{K^{be}\sqrt{N_b+N_e}}\sigma_w \quad \text{if } i \in SC^{be}. \end{aligned} \tag{3}$$

σ_w^2 is the variance of the fingerprint $\mathbf{W}^{(i)}$, and $Q(\cdot)$ is the Gaussian tail function. Thus, given $0 \le \beta \le \tilde{\beta}$ and $f_c = 1$, we have

$$\begin{aligned}\pi^b &= -Q\left(\frac{h-\mu_b}{\sigma_n}\right) + \left[1 - Q\left(\frac{h-\mu_b}{\sigma_n}\right)\right] R^b,\\ \text{and } \pi^{be} &= -Q\left(\frac{h-\mu_{be}}{\sigma_n}\right) + \left[1 - Q\left(\frac{h-\mu_{be}}{\sigma_n}\right)\right] R^{be} \end{aligned} \tag{4}$$

In game theory, a popular solution to the bargaining problem is the Nash Bargaining solution (NBS), which achieves proportional fairness. It divides the additional utility between the two players in a ratio that is equal to the rate at which this utility can be transferred [7]. Mathematically, the Nash Bargaining solution maximizes

$$\begin{aligned} g(\pi^b, \pi^{be}) &= \left(\pi^b - \pi^{b*}\right)^{a^b}\left(\pi^{be} - \pi^{be*}\right)^{a^{be}},\\ \text{where } \pi^{b*} &= \min \pi^b \quad \text{and} \quad \pi^{be*} = \min \pi^{be}. \end{aligned} \tag{5}$$

a^b and a^{be} are the bargaining powers of SC^b and SC^{be}, respectively. In this paper, we select $a^b : a^{be} = K^b : K^{be}$. The Nash Bargaining solution favors the player with a larger bargaining power and thus, in our problem, the subgroup of colluders with a larger size.

4. MAXIMUM-PAYOFF COLLUSION

Given fixed K^b and K^{be}, Section 3 analyzes how colluders negotiate with each other and select the collusion parameter β. During collusion, in addition to β, attackers can also select the total number of colluders K and select with whom they want to collude. In this paper, we consider the scenario where colluders not only want to minimize their risk, they also wish to maximize their rewards received from collusion. Taking into consideration both the risk and the rewards in the definition of the utility functions, this section investigates how the number of colluders affects each attacker's utility and finds the optimum K that maximizes their payoffs.

4.1. Non-Scalable Multimedia Fingerprinting

We start with the simple scenario where all users receive the high-resolution version. Since all the copies have the same resolution, there is no bargaining in collusion. Colluders agree to have the same probability of being detected $\tilde{P}_d$ and the same utility $\tilde{\pi}$, where

$$\begin{aligned}\tilde{P}_d &= Q\left(\frac{h - \sqrt{N}\sigma_w/K}{\sigma_n}\right), \text{ and}\\ \tilde{\pi} &= -\tilde{P}_d + \left(1-\tilde{P}_d\right)\theta/K, \end{aligned} \tag{6}$$

respectively. Figure 1 plots $\tilde{\pi}$ versus the total number of colluders K. Here, we assume that the length of the embedded fingerprints is 100,000. $\sigma_w = \sigma_n = 1$ and $\theta = 50$ in (6). h is selected so that the probability of falsely accusing an innocent user is 10^{-3}.

When K is small, $\tilde{P}_d$ has large values and colluders' chance of being detected is huge. Therefore, $-\tilde{P}_d$ is the dominating term in $\tilde{\pi}$, which results in a negative payoff as shown in Figure 1. In this scenario, colluders may not want to redistribute multimedia illegally since it is too risky. Attackers only collude and redistribute multimedia if they can find more than $K^0 = 126$ fellow attackers and receive positive payoffs from collusion. As K continues to increase above 126, colluders' risk of being detected decreases and, therefore, their payoffs increase.

However, colluding with more attackers does not necessarily always increase their payoffs. From Figure 1, when K is larger than 206, $\tilde{\pi}$ becomes a decreasing function of K. This is because in this scenario, $\tilde{P}_d$ is very small and the dominating term in $\tilde{\pi}$ is $(1-\tilde{P}_d)\theta/K$. Note that during collusion, colluders share the rewards from the illegal usage of multimedia and $R^{(i)}$ is a decreasing function of K. So when colluders are sure that their risk of being caught is small, they tend to prefer a smaller K and share the rewards with fewer people. Thus, in the example in Figure 1, attackers might prefer $K = 206$ in order to maximize their payoffs, and $\tilde{\pi}_{max} = \max_K \tilde{\pi} = 0.1682$ when $K = 206$.

Define $K^{max} \stackrel{\triangle}{=} \arg\max_K \tilde{\pi}$ as the optimal K that maximizes colluders' payoffs. We solve the problem $\partial\tilde{\pi}/\partial K|_{K=K^{max}} = 0$ to find K^{max}, where

$$\begin{aligned}\frac{\partial\tilde{\pi}}{\partial K} &= -\left(1+\frac{\theta}{K}\right)\frac{\partial\tilde{P}_d}{\partial K} - (1-\tilde{P}_d)\frac{\theta}{K^2}, \text{ and}\\ \frac{\partial\tilde{P}_d}{\partial K} &= -\frac{\sqrt{N}\sigma_w}{\sqrt{2\pi}K^2\sigma_n}\exp\left\{-\frac{1}{2}\left(\frac{h-\sqrt{N}\sigma_w/K}{\sigma_n}\right)^2\right\}. \end{aligned} \tag{7}$$

Figure 2 plots K^{max} versus θ and it shows that K^{max} is a decreasing function of θ. This is because, when θ has a larger value, that is, when colluders are willing to take a higher risk in order to benefit more from collusion, they prefer to collude with fewer people (thus a smaller K) to increase their rewards.

4.2. Scalable Multimedia Fingerprinting

Now, we consider the more complicated scenario where different colluders receive fingerprinted copies of different resolutions. In this scenario, colluders in SC^b act as a single player when negotiating, and those in SC^{be} act as one player. Note that one possible outcome of this bargaining is that they do not reach an agreement. If so, colluders only collude with their fellow attackers in the same subgroup, and the two subgroups SC^b and SC^{be} do not cooperate with each other during collusion. In this scenario, those colluders in subgroup SC^b generate a colluded copy with the base layer only. Similar to the analysis in Section 4.1, colluders in SC^b receive a payoff of

$$\begin{aligned}\pi_{nc}^b &= \max\left\{-P_{d,nc}^b + (1-P_{d,nc}^b)(f_b)^\gamma\theta/K^b, 0\right\}\\ \text{where } P_{d,nc}^b &= Q\left(\frac{h-\sqrt{N_b}\sigma_w/K^b}{\sigma_n}\right). \end{aligned} \tag{8}$$

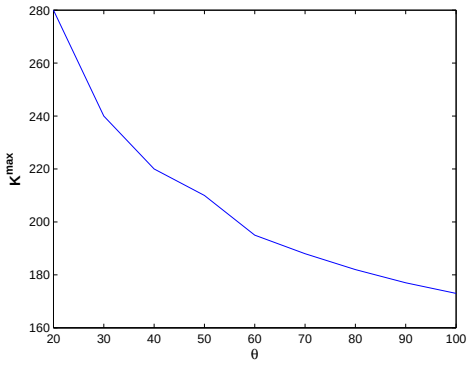

Fig. 2. K^{max} versus θ when $N = 10^5$.

Here, the maximum operator indicates that they will collude only if they receive positive payoffs from collusion. Similarly, for those colluders in SC^{be}, they generate a high-resolution copy and

$$\begin{aligned} \pi_{nc}^{be} &= \max\left\{-P_{d,nc}^{be} + (1 - P_{d,nc}^{be})\theta/K^{be}, 0\right\}, \\ \text{where } P_{d,nc}^{be} &= Q\left(\frac{h - \sqrt{N}\sigma_w/K^{be}}{\sigma_n}\right). \end{aligned} \quad (9)$$

If they reach an agreement regarding the distribution of the rewards and the risk, we use π_c^b to denote the utilities of the colluders in SC^b and π_c^{be} is the payoff of those colluders in SC^{be}. We consider the scenario where colluders select the Nash Bargaining solution in (5). Note that colluders in the two subgroups will cooperate with each other if and only if cooperation increases both subgroups' utilities, that is, when $\pi_c^b \geq \pi_{nc}^b$ and $\pi_c^{be} \geq \pi_{nc}^{be}$.

Figure 3 shows the results of the bargaining process. In Figure 3, K^{be} is fixed as 150, and we assume that these 150 colluders could not find any others who also receive high-resolution copies. Figure 3 analyzes how K^b affects the colluders' payoffs.

In this example, similar to that in Section 4.1, colluding with attackers in SC^b help colluders in SC^{be} further reduce their chance of being detected. However, colluding with more attackers does not always increase the payoffs. In Figure 3, when $K^b > 108$, $\pi_c^{be} < \pi_{nc}^{be}$ due to the sharing of the rewards with more people, and cooperation with attackers in SC^b does not benefit colluders in SC^{be} but rather decreases their utilities. Consequently, when $K^b > 108$, colluders only collude with their fellow attackers in the same subgroup, and the two subgroups do not cooperate with each other. From Figure 3, for colluders in SC^{be}, π_c^{be} reaches the maximum of 0.1681 when $K^b = 77$. Thus, in this example, for those 150 colluders in SC^{be} to maximize their utilities, if they cannot find any other attackers who receive high-resolution copies, the best strategy for them is to find another 77 attackers who receive the low-resolution copies.

In the example in Figure 3, we fix the number of colluders who receive the high-resolution copies as $K^{be} = 150$, and analyze how K^b affects the utilities of those colluders in the subgroup SC^{be}. Now, with the two-stage collusion model in Section 2.2 and the bargaining process in 3, colluder $\mathbf{u}^{(i)}$ is interested in the optimum values of K^{be} and K^b that maximize his or her utility $\pi^{(i)}$, that is,

$$(K^{be*}(i), K^{b*}(i)) = \arg \max_{K^{be}, K^b} \pi^{(i)}. \quad (10)$$

To find $K^{be*}(i)$ and $K^{b*}(i)$, we solve the problem

$$\frac{\partial \pi^{(i)}}{\partial K^{be}}|_{K^{be}=K^{be*}, K^b=K^{b*}} = \frac{\partial \pi^{(i)}}{\partial K^b}|_{K^{be}=K^{be*}, K^b=K^{b*}} = 0. \quad (11)$$

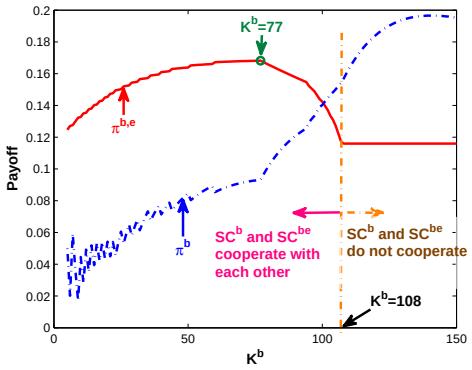

Fig. 3. π^b and π^{be} versus K^b. $N_b = N_e = 50,000$. $\sigma_w^2 = \sigma_n^2 = 1$, $\gamma = 1/3$, and $\theta = 50$. $K^{be} = 150$ is fixed.

With $N_b = N_{be} = 50,000$, $\gamma = 1/3$ and $\theta = 50$, for colluder $\mathbf{u}^{(i)}$ who receives a high-resolution copy, our analysis show that $K^{be*}(i) = 175$ and $K^{b*}(i) = 52$ give $\mathbf{u}^{(i)}$ a maximum payoff of 0.1744. Thus, if possible, to maximize π^{be}, $\mathbf{u}^{(i \in SC^{be})}$ should find 174 more attackers who also have the high-resolution copies and another 52 colluders who receive the base layer only. For colluder $\mathbf{u}^{(k)}$ who has the low-resolution copy only, the best strategy is to select $K^{b*}(k) = 141$ and collude with attackers in SC^b only. It helps $\mathbf{u}^{(k \in SC^b)}$ achieve a maximum payoff of 0.1966.

5. CONCLUSIONS

This paper studies the game-theoretic modeling of the complex dynamics among colluders, and analyzes the impact of colluder selection on attackers' payoffs. We consider both the colluders' risk of being detected and the rewards that they receive from collusion when defining the utility function, and model the colluder dynamics as a bargaining problem. Our analysis show that even though colluding with more attackers helps a colluder reduce his or her risk of being detected, it does not always increase his or her payoff, since he or she has to share the rewards with more people. Attackers will cooperate with each other if and only if cooperation helps all colluders further increase their utilities. We also investigate the optimum strategies that a colluder should follow when selecting fellow attackers in order to maximize his or her own payoff.

6. REFERENCES

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

[2] W. S. Lin, H. V. Zhao, and K. J. R. Liu, "Multi-user collusion behavior forensics: game-theoretic formulation of fairness dynamics," *IEEE Int. Conf. on Image Processing*, vol. 6, pp. 109–112, Sept. 2007.

[3] Y. Wang, J. Ostermann, and Y. Zhang, *Video Processing and Communications*, Prentice Hall, 1st edition, 2001.

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

[5] C. Podilchuk and W. Zeng, "Image adaptive watermarking using visual models," *IEEE Journal on Sel. Area in Comm.*, vol. 16, no. 4, pp. 525–540, May 1998.

[6] H. Zhao and K. J. R. Liu, "Behavior forensics for scalable multiuser collusion: fairness versus effectiveness," *IEEE Tran. on Information Forensics and Security*, vol. 1, no. 3, pp. 311– 329, Sept. 2006.

[7] G. Owen, *Game Theory*, Academic Press, 3rd edition, 1995.