Cooperative and Non-Cooperative Game-Theoretic Analyses of Adoptions of Security Policies for DRM

Zhiyong Zhang, Qingqi Pei,
Jianfeng Ma
Key Laboratory of CNIS, M.O.E.
Xidian University
Xi' an, P.R. of China
zhangzy@mail.xidian.edu.cn

Lin Yang
The Research Institute
China Electronic Equipment &
Systems Engineering Corporation
Beijing, P. R. of China
yanglin61s@yahoo.com.cn

Kefeng Fan
Electronics & Equipments Center
China Electronics Standardization
Institute
Beijing, P.R. of China
fankf@cesi.ac.cn

Abstract—**Digital Rights Management ecosystem is composed of various participants, which adopt different security policies to meet their own security requirements, with a goal to achieve individual optimal benefits. However, from the perspective of the whole DRM-enabling contents industry, a simple adoption of several increasingly enhanced security policies does not necessarily implement an optimal benefit balance among participants. A game-theoretic analysis of adoptions of security policies was emphasized based on a proposed General DRM value chain ecosystem without the loss of generality. First, we formalized security policies and fundamental properties that include internal relativity and external one, together with multi-party game on adoptions of security policies. Also, a cooperative game among digital Contents Provider, Rights/Service Provider and digital Devices Provider, as well as a non-cooperative game between Providers and Consumers were presented. Final, a stable core allocation of benefits and Nash Equilibriums were found out, respectively. It is clearly concluded that the cooperative game has important super-addivitity and convexity, thus simultaneous adoptions of security policies with external relativity being helpful to achieve Pareto Optimality by using a pre-established cooperative relation; and that Pareto Optimality also exists between Providers and Consumer with the increase of users' purchase transactions when both have a repeated game.**

Keywords-Digtial Rights Management; Security Policy; Game Theory; Nash Equilibrium; Core Allocation

I. INTRODUCTION

In decade, illegal copy, free distribution and unauthorized usage of copyrighted digital contents have been a common phenomenon. The goal of Digital Rights Management (DRM) is to better solve these problems [1]. The digital contents value chain, or DRM ecosystem, is composed of relative participants and their fundamental functional components. In general, an entire value chain principally includes contents creators, intermediary distributors, rights holders/issuers, terminal platform vendors and end users. With regarding to some essential functionalities, Certification Authority, Clearing House that is responsible for license processing, financial and event managements, as well as DIMS (Distribution Information Management System) that supports a contractual mechanisms and maintains program for interoperability, were introduced in Lee's proposed distribution model [2]. A multi-party DRM ecosystem was presented to solve interoperability obstacle for DRM wider acceptability and adoption [3]. The ecosystem refers merely to four entities: Creator, Distributor, User and Authority, which are the essential elements of the simple and practical business model of DRM value chain. Gallery [4] introduced three new entities—device manufacturer, DRM Agent installer and CMLA (Content Management Licensing Administrator) —on the basis of OMA DRM architecture. If mobile operators and telecom companies were taken into account, Mobile DRM value chain would be more complicated than the traditional contents supply chain [5].

Nowadays, the main countermeasure of copyrights infringement is to look for positive security policies, even increasingly enhanced policies, at the standpoints of copyrights owner and contents provider. Consequently, owing to the higher cost and inconvenience of improved terminal platform and contents usage, digital consumers may reject DRM technology and DRM-protected digital products, as will interrupt the contents chain value. It is stated that DRM should balance interests of various stakeholders in value chain, to enable the IPR (Intellectual Property Rights)-enabling contents industry to flourish in [6]. Recently, several attempts to explore benefit balance of DRM ecosystem have emerged [7, 8]. Anderson et.al. [9] presented that an important tool to analyze economics of information security is Game Theory, where Nash Equilibrium is an essential concept that is an optimal and stable outcome of multi-party game on different strategies combinations. Under the circumstance, participants together acquire maximum and balance of benefits.

II. GENERAL DRM ECOSYSTEM AND FORMAL GAME

A. A General DRM Value Chain Ecosystem

We focused mainly on a General DRM Ecosystem (abbr. GDRM) composed of four basic active parties, which have their own security policies. In GDRM, Contents Provider (abbr. CP) could include contents creator/owners and intermediary distributors. Rights Provider (abbr. RP) denotes a participant distributing digital rights and may be a service provider/network operator. Generally, CP and RP have collaborative relationship for providing contents and corresponding usage rights, respectively. Device Provider

The work was sponsored by National Natural Science Foundation of China Grant No.60803150, No.60633020 and No. 60672112, "111" Project Grant No.B08038.

978-1-4244-2309-5/09/$25.00 ©2009 IEEE

(abbr. DP) provides digital device platform including consumer electronics for end user of the ecosystem. Obviously, end User is a set of subscribers/consumers of digital contents, and they could share purchased contents through superdistribution mechanisms. GDRM is shown in Figure 1.

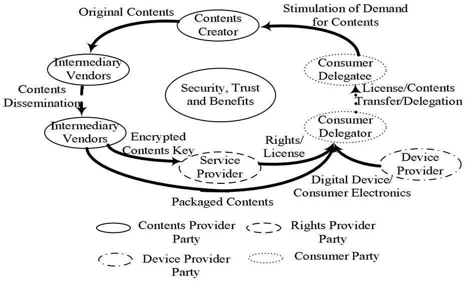

Figure 1. A General DRM Ecosystem

B. Formalized Security Policies and Properties

Definition 1(Party) Party $\wp$ denotes a set of some actors α playing the same functional role in DRM value chain.

$$\wp = \{\alpha \mid \textit{actor is responsible for a function}\}$$

$$GDRM = \{CP, RP, DP, Consumer, Contents, Rights\}$$

Definition 2(Security Component/Service) in term of fundamental security requirements of each party, an atomic component that may be a program, hardware unit and middleware, as well as a composite service, is realized to accomplish a specific functionality related to security. Security Components/ Services consist of two kinds of basic ones denoted by c^* / s^*, and optional ones written by c / s. Notation f, w, U and μ denote an actual factor influencing benefit of α when an adoption of c or s, the weight value of a factor, positive/negative utility of the factor and components/services, respectively.

$$SecurityComponent = \{\overset{*}{c}_1, \overset{*}{c}_2, \ldots \overset{*}{c}_i, c_1, c_2, \ldots c_j\}$$

$$SecurityService = \{\overset{*}{\mathrm{s}}_1, \overset{*}{\mathrm{s}}_2, \ldots \overset{*}{\mathrm{s}}_m, s_1, s_2, \ldots s_n\}$$

$$\mu(c_s) = \sum_{p=0}^{i} U_p \ (W_p / \sum_{k=0}^{i} W_k), \ \mu(s_t) = \sum_{q=0}^{j} U_q \ (W_q / \sum_{k=0}^{j} W_k)$$

Property 1(Internal Relativity of Basic Security Components/Services) for each participant, various c^* / s^* are combined to meet fundamental security requirements. The integrated adoption of c^* / s^* are referred to as internal relativity, which do not influence other participants' decision on adoptions of security policies.

Property 2(External Relativity of Optional Security Components/Services) If two or multiple optional components/services that are from different parties need to be adopted simultaneously, otherwise these active components have no positive effect on corresponding parties. These c / s are seen as external relative, which is formalized as follows:

$$Exter\_Relative\_Components \ \{\mathrm{c}_1, \mathrm{c}_2, \ldots, \mathrm{c}_\mathrm{p}\} \ \forall i, j (1 \le i, j \le p, 2 \le p \le \mathbb{C}(\wp))$$

$$\exists s, t (s, t \in \{CP, RP, DP, Consumer\})(\mathrm{c}_\mathrm{i} \in C_s, \mathrm{c}_\mathrm{j} \in C_t, i \ne j \rightarrow s \ne t)$$

$$Exter\_Relative\_Services \ \{\mathrm{s}_1, \mathrm{s}_2, \ldots, \mathrm{s}_\mathrm{q}\} \ \forall i, j (1 \le i, j \le q, 2 \le q \le \mathbb{C}(\wp))$$

$$\exists m, n (m, n \in \{CP, RP, DP, Consumer\})(s_\mathrm{i} \in S_m, \mathrm{s}_\mathrm{j} \in S_n, i \ne j \rightarrow m \ne n)$$

Definition 3(Security Policy) *sp* is a set of security components or services including all c^* / s^* and some optional c / s that are adopted by α . Here *sp* has upper abstract.

$$sp = \{\overset{*}{c}_1 \ldots \overset{*}{c}_i, \overset{*}{s}_1 \ldots \overset{*}{s}_m, c_1, c_2, \ldots c_s, s_1, s_2, \ldots s_t\} \ 0 \le s \le j, \ 0 \le t \le n$$

Definition 4 (Utility of sp) Utility U of *sp* is a sum of utilities μ of all components and services involved in *sp*.

$$U(sp_i^j) = \sum_{p=0}^{i} \sum_{q=0}^{m} \mu(\overset{*}{c}_p) + \mu(\overset{*}{s}_q) + \sum_{p=0}^{s} \sum_{q=0}^{t} \mu(c_p) + \mu(s_q)$$

Property 3 (External Relativity of Security Policies) if two or multiple different security policies include c / s with external relativity, then these policies are also seen as external relative, formalized by

$$Exter\_Relative\_Policies \ \{sp_1, sp_2, \ldots, sp_\mathrm{n}\}$$

$$\forall i, j (1 \le i, j \le n, 2 \le n \le \mathbb{C}(\wp)) \ \exists s, t (s, t \in \{CP, RP, Consumer\})$$

$$(sp_i \in SP_s, sp_j \in SP_t, i \ne j \rightarrow s \ne t)$$

$$\exists p, q \ (p + q \ge n) \wedge ((c_1, c_2, \ldots, c_p \in Exter\_Relative\_Components) \vee$$

$$(s_1, s_2, \ldots, s_q \in Relative\_Services)) \ (c_p \in sp_i, s_q \in sp_j)$$

C. Formalized Game on Security Policies

Definition 5 (Rational Agent and Payoff) in GDRM, *RA* denotes a rational participant aiming at a maximum of benefits, and makes a decision on adopting a certain security policy. There are four *RA*s with respect to four parties, RA_{CP}, RA_{RP}, RA_{DP}, $RA_{Consumer,}$ respectively. The payoff of RA manifests the acquired benefits in participants' policies combination (profile).

Definition 6 (Multi-Party Game) Multi-Party Game for DRM denotes a process of making decision on an effective and rational adoption of security policies, as has effect on benefits each other. The game is depicted by a set of three tuple $< \wp, \ sp, payoff >$:

$$G = \{< RA_i, SP_i, Payoff(RA_i, RA_{-i}) > \mid \ i = \{CP, RP, DP, Consumer\}\}$$

Definition 7 (Nash Equilibrium of Non-Cooperative Game on Security Policies) for any *RA*, when the case that the *RA* adopt a security policy sp^* to acquire benefit greater than the benefit acquired by choosing any other *sp* occurs, the profile, called by Nash Equilibrium, of each *RA*'s sp^* is a balance of payoffs by adopting relatively dominant policies.

$$Payoff(RA_i^{sp^*}, RA_{-i}^{sp^*}) \ge Payoff(RA_i^{sp^j}, RA_{-i}^{sp^*})$$

$$j \in SP_i, \ j \ne *, \ i \in \{CP, RP, DP, Consumer\}$$

$$-i \in \{CP, RP, \ DP, Consumer\}, -i \ne i$$

Definition 8 (Cooperative Game on Security Policies) for the N-player game, if any subset S players of N constitute a cooperation coalition, and adopt a certain security policy, for the sake of implementing individual rationality and coalitional rationality of benefits allocation, then the N-player cooperative game is denoted by $< N, \nu >$, where ν is a function from 2^N to a real number set $\Re$ whose element is total payoff of the S coalition. In the cooperative game of GDRM, $N = \{CP, RP, DP\}$.

Property 4 (Super-Additivity and Convexity) the cooperative game $< N, \nu >$ has super-additivity, iff $\forall S, T \in 2^N$, $\nu(\mathrm{S}) + \nu(\mathrm{T}) \le \nu(\mathrm{S} \cup \mathrm{T}), \mathrm{S} \cap \mathrm{T} = \varnothing$; the game has convexity, iff $\forall S, T \in 2^N$, $\nu(\mathrm{S}) + \nu(\mathrm{T}) \le \nu(\mathrm{S} \cup \mathrm{T}) + \nu(\mathrm{S} \cap \mathrm{T})$. Here $S, T \in 2^{\{CP, RP, DP\}}$.

Definition 9 (Core Allocation) let χ be a benefits allocation vector of a cooperative game $< N, \nu >$ and $\chi \in \Re^n$. χ is a core allocation, iff $\forall S \in 2^N$, $\chi(S) \ge \nu(S)$. In GDRM, participants set S has collective rationality.

III. Typical Security Policies and Utilities

We presented some existing security components and compositive typical security polices of participants for contents acquisition application scenario as follows, also gave utilities of components and initial values in some security policies profiles, as Table 1. According to Property 1-3, we only need to consider the utilities of c / s.

- CP-centric c^* / s* include contents packaging and watermarking (abbr. WM), c / s consist of Transaction-based Negotiation with RP (abbr. TN) and trust computing-enabling Contents Identification (abbr. CI). Formally, the components/services set is {Packaging*, WM*, TN, CI}. And obviously, the set of security policies has {Packaging*, WM*}, {Packaging*, WM*, TN}, {Packaging*, WM*, CI}, {Packaging*, WM*, TN, CI}, denoted by $\{sp_{CP}^1, sp_{CP}^2, sp_{CP}^3, sp_{CP}^4\}$.

Contents Identification functionality is adopted to accomplish contents security, for instance, to validate by using a verification service whether or not a Java application is embedded into a section of malicious codes. Then, Consumer would execute the verified application based on trusted computing platform. These benefit-impacting factors mainly include the cost of identification, written by f_{CP}^{CoI} , and the acquire benefits of providing trusted contents to consumer, denoted by f_{CP}^{PoI} . The former is negative utility denoted by u_{CP}^{CoI}, and the latter is opposite, denoted by u_{CP}^{PoI}.

The activeness of TN is suitable for the establishment of a robust trust relationship between CP and RP, so it is a positive factor f_{CP}^{PoTN} , with its utility being u_{CP}^{PoTN} . The component would increase the time delay and computing complexity of digital transaction, as the function is transaction-driven. We depict the negative factor and its few utility as f_{CP}^{CoTN} and u_{CP}^{CoTN} , respectively. Note that the component needs to be simultaneously active by CP and RP. Otherwise, u_{CP}^{CoTN} and u_{CP}^{PoTN} would be none.

- RP-centric security components/services are listed as follows: c^* / s* have Rights Expression and Issue (abbr. REI) and Consumer's Identity Authentication (abbr. IA), and c / s have TN and User's Terminal Device Attestation (abbr. DA). Similar to CP, due to the set of RP's components/services is {REI*, IA*, TN, DA}, the adoptable security policies sp_{RP}^1 , sp_{RP}^2 , sp_{RP}^3 and sp_{RP}^4 denote {REI*, IA*}, {REI*, IA*, TN}, {REI*, IA*, DA} and {REI*, IA*, DA, TN}}.

DA is based on trusted computing platform and remote attestation, and it could implement the attestation of run-time integrity of user' terminal device and some key components, such as DRM Controller, as consequently enables RP to ensure that an issued license would be trustworthily interpreted and executed, thus acquiring payoff u_{RP}^{PoDA} . Therefore, the attestation function is a positive factor denoted by f_{RP}^{PoDA} .The other side of a coin, the usage of DA also directly increases the main overhead of integrity management and partial computation and storage costs of RP' system and These impacting-factors are together referred as f_{RP}^{CoDA} , and the corresponding utility being u_{RP}^{CoDA} .

- For DP, two security strategies mean that trusted computing-enabling platform or basic security one would be provided, denoted by $\{sp_{DP}^1, sp_{DP}^2\}$.

Device Provider provides trusted computing-enabling digital devices or consumer electronics for end user. Thus, the cost and profits of DP on trusted devices investments are denoted by u_{DP}^{PoTC} and u_{DP}^{CoTC} .

- For Consumers' perspective, security policy mainly denotes whether or not they use higher security device or active relative components/services, and two policies are written by $\{sp_{DP}^1, sp_{DP}^2\}$.

An adoption of these enhanced security platform has positive and negative factors and relative utilities, denoted by $f_{Consumer}^{PoTC}$, $u_{Consumer}^{PoTC}$, $f_{Consumer}^{CoTC}$ and $u_{Consumer}^{CoTC}$. Here, $f_{Consumer}^{CoTC}$ mainly includes the purchase cost of trusted computing-enabling terminal device; $f_{Consumer}^{PoTC}$ denotes a positive effect on benefits of Consumer, for instance improvement of security for DRM application and personal confidential data. Here we assumed that CP and RP respectively acquire half of benefits $u_{Consumer}^{PoTC}$.

TABLE I. INITIAL VALUES OF IMPACTING FACTORS AND UTILITIES OF SECURITY POLICIES PROFILES

Party	RA_{CP}				RA_{RP}				RA_{DP}		$RA_{Consumer}$	
factor	f_{CP}^{PoI}	f_{CP}^{CoI}	f_{CP}^{PoTN}	f_{CP}^{CoTN}	f_{RP}^{PoDA}	f_{RP}^{CoDA}	f_{CP}^{PoTN}	f_{CP}^{CoTN}	f_{DP}^{PoTC}	f_{DP}^{CoTC}	$f_{Consumer}^{PoTC}$	$f_{Consumer}^{PoTC}$
(u, w)	(10,4)	(5,2)	(6,3)	(3,1)	(10,5)	(5,2)	(6,2)	(3,1)	(10,8)	(4,2)	(4,6)	(8,4)
1,1,1,1	5				5				5		5	
1,1,2,*	5				5				4.2		5, 1.8	
2,2,1,1	6.5				5.9				5		5	
4,2,1,1	6.5				5.9				5		5	
2,4,1,1	6.5				4.9				5		5	
2,2,2,*	6.5				5.9				4.2		5, 1.8	
2,4,2,2	6.5				9.9				12.2		2.1	
4,2,2,2	9.5				5.9				12.2		2.1	
4,4,1,2	5.5				4.9				5		5, 1.8	
4,4,2,1	5.5				4.9				4.2		5	
2,2,1,2	6.5				5.9				5		1.8, 5(repeated)	
4,4,2,2	9.5, 10.5(repeated)				9.9, 10.9(repeated)				12.2		4.2, 7.4(repeated)	

IV. COOPERATIVE GAME AMONG PROVIDERS

A. *Multi-Party Cooperative Game Model*

In GDRM, there is a three-player multi-strategy game model among CP, RP and DP with respect to adopting security policies, as is shown in Figure 2. Here the strategy denotes adoptable different security policies from participants' perspectives.

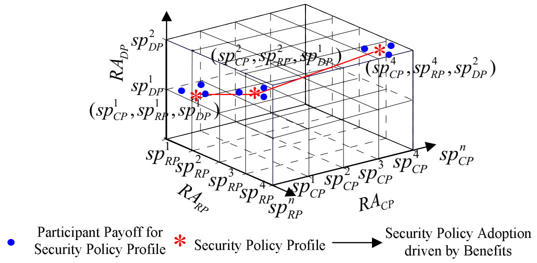
RA_{DP}
sp_{DP}^{2}
sp_{DP}^{1}
$(sp_{CP}^{2}, sp_{RP}^{2}, sp_{DP}^{1})$
$(sp_{CP}^{4}, sp_{RP}^{4}, sp_{DP}^{2})$
$(sp_{CP}^{1}, sp_{RP}^{1}, sp_{DP}^{1})$
sp_{RP}^{1}
sp_{RP}^{2}
sp_{RP}^{3}
sp_{RP}^{4}
sp_{RP}^{n}
RA_{RP}
sp_{CP}^{1}
sp_{CP}^{2}
sp_{CP}^{3}
sp_{CP}^{4}
sp_{CP}^{n}
RA_{CP}
● Participant Payoff for Security Policy Profile
* Security Policy Profile
Security Policy Adoption driven by Benefits

Figure 2. Three-Party Multi-Policy Game Model among Providers

If the game is non-cooperative, each participant merely has a rational attribute of pursuing maximum benefits based on a consideration of other parties' actions, that is to say personal rationality. So, in term of Table 1, there are two Nash Equilibriums of the non-cooperative game, security policies profile (2, 2, 1) and (4, 4, 2). Though every participant's payoff in the (4, 4, 2) scenario is much more than in (2, 2, 1), the final balance result is not security policies profile (4, 4, 2), with (2, 2, 1) owing to the essence of personal rationality.

It is noted that the profile (4, 4, 2) is rational and stable in a cooperative game among Providers, as personal rationality and collective rationality are both highlighted. Moreover, when the profile (4, 4, 2) is achievable, the participants' payoffs are maximum, also having Pareto Optimality. Security policies profile (4, 4, 2) embodies a cooperative relation of three parties to adopt enhanced security polices together, and single action or two-party cooperation is not optimal.

B. *Coalitions, Convexity and Core Allocation*

According to Table 1, we presented total payoffs of the cooperative game under different cooperation circumstances, which include single action, two-party and three-party cooperation for trusted computing-enabling enhanced security. When all participants do not cooperates, acquired utilities of CP, RP and DP are 6.5, 4.9 and 4.2, respectively; when cooperation exists, utilities obviously change, as (1)-(4).

$$v(\{\text{RACP, RARP}\}) = 15.4 \tag{1}$$

$$v(\{\text{RACP, RADP}\}) = 27.6 \tag{2}$$

$$v(\{\text{RARP, RADP}\}) = 28.6 \tag{3}$$

$$v(\{\text{RACP, RARP,RADP }\}) = 31.6 \tag{4}$$

From above Equations, it is clear that the total payoff of three-party cooperation is much more than all payoffs of single action and two-party cooperation. According to Property 4, the cooperative game has super-addivitity and convexity. Beside, in the game, each gains maximum benefits at the viewpoint of individual rationality, collective rationality and coalitional rationality, (9.5, 9.9, 12.2) is also a rational and stable core allocation that has the participants' acceptability.

C. *Discussions*

The security policy profile influencing the cooperative relation and total payoffs is $\{sp_{CP}^{3}, sp_{RP}^{3}, sp_{DP}^{2}\}$, though sp_{i}^{2}, where $i = \{CP, RP\}$, has two-party external relativity. Note that whether to adopt sp_{i}^{2} or not does not result in a negative utility for CP and RP, so both would together adopt sp_{i}^{2}, which does not a pre-established cooperative relation. But, single adoption of sp_{i}^{3} can give birth to a negative one for the active party, as well as a two-party cooperative action on sp_{i}^{3} does not also gain the maximum payoffs for Providers. So, the fulfillment of $\{sp_{CP}^3, sp_{RP}^3, sp_{DP}^2\}$ and optimal coalition requires contractual agreements on cooperation in advance.

V. Non-Cooperative Game Between Providers and Consumers

A. Non-Cooperative Game Model

In this section, based on the above cooperative game analysis, CP, RP and DP are seen as an actor Providers, denoted by $RA_{Providers}$. The relation between Providers and Consumer is in essence different from the cooperative one among three providers. $RA_{Providers}$ and $RA_{Consumer}$ have their own personal rational goal to pursue optimal profits or benefits, thus a consideration of collective rationality is unpractical. There is not a cooperative relation, and the relation can be not established by preliminary contractual agreement or negotiation. Therefore, we only need to look upon the relation as a non-cooperative two-player multi-strategy game model for adoptions of security policies.

B. Non-cooperative Game Analysis and Nash Equilibrium

First, through the above analysis of these given utility values in Table 1, it is clear that sp_{CP}^2 and sp_{RP}^2 would been simultaneously adopted. Second, according to participants' payoffs in different strategy profiles in Figure 3(a), $sp_{Consumer}^2$ is a strictly dominated strategy, by which it only acquires fewer benefit, 1.8 or 4.2, than benefit values 5 by $sp_{Consumer}^1$. Further, if $RA_{Providers}$ chooses $sp_{Providers}^1$, which denotes a non-cooperative adoptions of enhanced security, it would similarly gain 17.4 interests greater than 14.6, Thus, we easily found out a Nash Equilibrium $(sp_{Providers}^1, sp_{Consumer}^1)$. Obviously, we also gain a four-party Nash Equilibrium $(sp_{CP}^2, sp_{RP}^2, sp_{DP}^1, sp_{Consumer}^1)$ that could satisfy relative benefits balance for a one-stage game or few-stage game, where users only have limited purchase transactions.

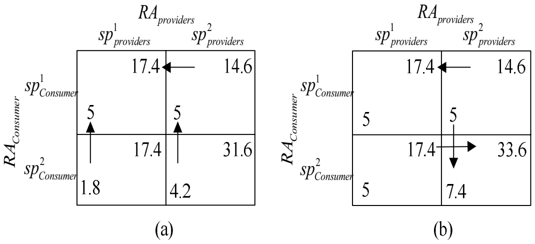

Figure 3. Payoffs Matrix of Non-Cooperative Game

If there is a dynamic repeated game between both, then a new Nash Equilibrium $(sp_{Providers}^2, sp_{Consumer}^2)$ holds, where $sp_{Providers}^2$ denotes a cooperative adoptions of enhanced security. As under the given scenario, the loss led by the adoption of $sp_{Consumer}^2$ would be compensated by gained benefits with an increase of transactions when the repeated game, and payoffs matrix is shown in Figure 3(b). Consumer's payoff changes from 4.2 to 7.4 for the new Nash Equilibrium, so $RA_{Consumer}$ would consider $sp_{Consumer}^2$. When the number of transactions increasingly grows and exceeds to $\left\lceil (u_{Consumer}^{CoTC} w_{Consumer}^{CoTC} - u_{Consumer}^{PoTC} w_{Consumer}^{PoTC}) / u_{Consumer}^{PoTC} w_{Consumer}^{PoTC} \right\rceil$, the acquirable benefit of $RA_{Consumer}$ much more than benefit baseline. If both parties have a repeated game, the new Nash Equilibrium occurs.

As a rational participant, not doubt that $RA_{Consumer}$ would choose $sp_{Consumer}^2$ at the beginning of the game by sacrificing short-term benefits and acquiring long-term ones, thus the expected result $(sp_{CP}^4, sp_{RP}^4, sp_{DP}^2, sp_{Consumer}^2)$ being achieved. In other words, if a rational user is intended to continually purchase contents, he/she will adopts higher security device, such as trusted computing-enabling platform or consumer electronics. For the adoption of Consumer, Providers would also provide trusted platform, actualize and deploy relative higher security policies in a real DRM ecosystem.

VI. Conclusive Remarks

We laid emphasis on the cooperative game among Providers and the non-cooperative game between Providers and Consumer. It is clearly concluded that Pareto Optimality respectively exists when a cooperative relationship among providers and a repeated game occur with the increase of purchase transactions.

References

[1] B. Rosenblatt, “DRM, law and technology: an American perspective,” Online Information Review, vol.31, no.1, pp.73–84. 2007.

[2] J. Lee, S. Hwang, S. Jeong, K. Yoon, C. Park and J. Ryou, “A DRM Framework for Distributing Digital Contents through the Internet,” ETRI Journal, vol. 25, no.6, pp.423–436, Dec. 2003.

[3] B. Vassiliadis, V. Fotopoulos, A.N. Skodras, “Decentralising the Digital Rights Management value chain by means of distributed license catalogues,” In: Proceeding of 2006 IFIP Artificial Intelligence Applications and Innovations, eds. Maglogiannis, I., Karpouzis, K., Bramer, M., (Boston: Springer), Vol. 204, pp. 689–696.

[4] E. Gallery and C.J. Mitchell, “Trusted mobile platforms,” In: Proceedings of Foundations of Security Analysis and Design, LNCS 4677, Aldini and R. Gorrieri (Eds.), pp. 282–323, 2007.

[5] E. Furregoni, A. Rangone, F. Renga and M. Valsecchi, “THE mobile digital contents distribution scenario,” In: Proceedings of Sixth International Conference on the Management of Mobile Business, 2007.

[6] H. Abie, “Frontiers of DRM knowledge and technology,” Intel. J. of Comput. Sci. and Network Security., vol.7, no.1, pp. 216–231, 2007.

[7] G. Heileman, P. Jamkhedkar, J. Khoury and C. Hrncir, “The DRM game,” In: Proceedings of 2007 ACM Workshop on Digital Rights Management, Alexandria, Virginia, USA. October 29, 2007.

[8] Y. Chang, “Who should own access rights? A game-theoretical approach to striking the optimal balance in the debate over Digital Rights Management,” Artifi. Intelli. & Law, no.15, pp.323–356, 2007.

[9] R. Anderson and T. Moore, “The Economics of Information Security,” Science, 314 (5799), pp. 610–613, 2006.