Intelligent Automation and Soft Computing, Vol. 17, No. 2, pp. 191-203, 2011

GAME-THEORETIC ANALYSES AND SIMULATIONS OF ADOPTIONS OF SECURITY POLICIES FOR DRM IN CONTENTS SHARING SCENARIO

ZHIYONG ZHANG[1, 2], QINGQI PEI[2], JIANFENG MA[2], AND LIN YANG[3]

[1]*Electronic & Information Engineering College*
Henan University of Science & Technology
Luoyang 471003
Henan, P.R. of China

[2]*Ministry of Education Key Laboratory of Computer Network & Information Security*
Xidian University
Xi'an 710071, Shannxi, P.R. of China

[3]*The Research Institute*
China Electronic Equipment & Systems Engineering Corporation
Beijing 100141
P.R. of China

ABSTRACT—A legitimate contents sharing is an essential functionality of DRM (Digital Rights Management)-enabling contents industry and its value chain extension. In order to effectively choose and deploy some typical security policies in a contents sharing scenario, we introduced game theory to analysis the mutual influence of adoptions of trusted computing enabling enhanced security policies on benefits of two stakeholders, which are DRM *Providers* and contents *Sharer* who is a category of consumers. A dynamic and mixed game and its algorithm were proposed, where *Sharer*'s strategies were whether to employ the trusted computing enabling devices and related components or not, as well as *Providers*' strategies included entirely general security, entirely enhanced security and dynamic security policies. We concluded from both game-theoretic analyses and Swarm simulation experiments that the number of acquired sharable digital rights and security cost have a direct effect on *Sharer*'s choices of the enhanced security policy, and also their different basic sharing modes including partial, modest and extensive sharing, further influence the choice of *Providers*. Besides, with respect to the mixed sharing mode far more similar to a real contents sharing scenario, Dynamic security strategy is superior to the entirely enhanced security in the context of limited sharable rights and higher security costs, but with the acquisition of much more rights and the decrease of enhanced security overhead, the latter strategy would be optimal and stable as a Nash Equilibrium for stakeholders, in combination with the exploitation of effective business models of contents industry.

Key Words: Digital Rights Management; Game Theory; Trusted Computing; Algorithm; Simulation

1. INTRODUCTION

The illicit copy, malicious dissemination and unauthorized usage of copyrighted digital contents have been still a common phenomenon, as contents like the electric book, image, music, movie and application software are easily duplicated without deterioration in qualities. As a result, digital contents industry would be heavily damaged, and even the value chain could also be interrupted. Digital Rights Management has emerged at the beginning of the 1990s, and it is an umbrella term involved both in the realization of the contents industry field and in the insights into multiple scientific disciplines, for instance, information technology, economics and law [1].

In the last decade, regardless of a general DRM or Mobile DRM, emphasis has been laid on the copyrights protection so as to resolve issues of digital assets' piracy and illegal usage, which mainly employs the cryptographic security and watermark technologies, as well as on usage permissions that are accomplished by Rights Expression Language (abbr. REL) and Usage Control. Note that a legitimate share of purchased contents is necessary for a complete DRM ecosystem and its contents value chain extension, where the digital rights transfer/delegation meets the requirements of consumers' contents sharing.

With respect to REL for digital rights sharing, OMA has not formally specified syntax and semantics of the rights transfer in OMA REL yet [2], which makes it difficult to unambiguously depict sharable permissions, conditions and constraints in the DRM system compliable for OMA DRM. Though other RELs, such as ODRL and XrML, specify several transferable permissions, such as Sell, Lend, Give of ODRL [3], Delegation of XrML [4], these definitions of the rights sharing are coarse-grained, and a fine-grained one is essential for some complicated business models. In combination with fundamental delegation characteristics and extensible ODRL, we proposed a fine-grained rights transfer policy and its trusted enforcements [5].

Generally, Contents Providers/Services Provider distributes usage licenses to a purchaser by using the binding of content-license-device (or user), consequently a rigorously restriction of contents usages make it impossible to share contents on multiple the front-end devices held by consumers and among users. Therefore, Digital Video Broadcasting Project was first to propose the concept on "Authorized Domain" for sharing contents at various kinds of rendering consumer electronics [6]. Subsequently, OMA DRM Specs have adopted the concepts, and realized the uniform domain management of RI (Rights Issuer), which refers to the devices' joining, leaving and registering domain, together with RO (Rights Object) acquisitions from RI [7]. The approach can implement the sharing behavior within the managerial domain, but RI obviously becomes the bottleneck of DRM system. An introduction of Domain Issuer in OMA DRM was proposed to organize a sharing domain that substitutes multiple Right Issuers with regard to a case that sharer could purchase contents from different contents vendors and share them on different devices [8]. So, a Domain Manager has already emerged in later version of OMA Specs. Nowadays, contents sharing scenarios primarily focuses on Home Network Domain [9] and Personal Entertainment Domain [10]. A secure domain architecture and related protocols for DRM were proposed, which, however, did not support RO transferring and contents sharing [11]. Kim et.al. [9] improved on this architecture for the home domain, and the Local Domain Manager he proposed substitutes RI to accomplish license distributions for domain membership devices, meanwhile Delegated RO and Proxy Certificate have realized rights delegations. This refined architecture is merely limited to home domain, and it is worthwhile to consider that how rights transfer/delegation-based contents sharing is achieved in a wider domain.

Recent years have witnessed the some key applications of trusted computing technologies to DRM, which cover to the trustworthy dissemination of licenses presenting concrete usage policies, secure storage of contents and their encryption key, and trusted execution of DRM Controller (i.e. DRM Agent) on the basis of the remote attestation, seal approach and integrated trusted platform

[5, 12]. A trusted terminal platform provided by the device manufacturer is crucial for the general DRM system or Mobile DRM, and is also helpful for establishing and enhancing the trust relationship among participants in the contents value chain. Nowadays, there exist several representative organizations, such as TCG, OpenTC in Europe and Chinese Trusted Computing Union, together with a series of Specs on trusted PC platform [13] and trusted mobile architecture [14], etc.

Besides of existing researches on DRM security realizations and deployments, interestingly, attempts to explore the benefit balance of DRM ecosystem have recently emerged. Heileman et.al. [15] made a basic game-based analysis on how adoptions of DRM protections or not have significant effects on benefits for contents vendors and purchasers. And also, a game-theoretic approach to explore digital rights ownership was proposed for optimally balancing benefits between contents industry and individual consumer, not just benefiting the either of both [16]. In our opinion, from the perspective of the holistic DRM-enabling contents industry, a simple adoption of several increasingly enhanced security policies does not necessarily implement the optimal benefit equilibrium among participants. So, regarding the contents acquisition scenario, we made the systematic game-theoretic analyses on security policies for DRM [17].

The main contribution of the paper is to introduce the game theory to analyze and simulate a dynamic and mixed game on the alternative of a general baseline security and trusted computing enabling enhanced policy in contents sharing scenario. The remainder of paper is organized as follows. A dynamic and mixed game and related algorithm based on the contents sharing tree were presented in Section 2. And then, Section 3 gave simulation experiments and discussions. Finally, conclusions were drawn.

2. A DYNAMIC AND MIXED GAME ON TYPICAL SECURITY POLICIES

In a generic DRM ecosystem, each of stakeholders has a set of security policies and a practical choice as his/her strategy (or move) in the contents transaction. We presented two kinds of typical security policies and corresponding utilities in Subsection 2.1, respectively. And then, on the basis of a simplified tree structure regarding the contents sharing, a dynamic and mixed game was proposed in next Subsection. Finally, the game analyses and algorithm were given in detail.

2.1 Typical Security Policies Utilities of Participants

We mainly discussed two kinds of typical policies for both *Providers*, a unified logic entity including CP (Contents Provider), RP (Rights/Services Provider) and DP (Devices Provider), and *Sharer* that is a category of consumers with sharing behaviors. One is the general security policy that meets fundamental security requirements, and the other is the trusted computing enabling enhanced security, which provides participants with much more copyrights and private/sensitive data protections.

For *Providers*, the general security policy $sp^{G}_{\text{Providers}}$ denotes that CP implements basic cryptographic protection and package of digital contents, RP accomplishes the corresponding licenses dissemination by secure channels, and DP provides a common digital device or consumer electronics for *Sharer*. The acquired benefit of the adoption of the policy for *Providers* is written as $\mu^{baseline}_{\text{Providers}}$. The enhanced security $sp^{E}_{\text{Providers}}$ for *Providers* means a combination of higher contents security, the trusted distribution of RO created by RP based on sharers' Devices Attestation (DA) [5], as well as the trusted computing enabling commodity devices provided by devices vendors.

Undoubtedly, DA can implement the validation on the system bootstrap and running-time integrity of user terminal device, as well as on such key component as DRM Controller and contents rendering application. Thus enables RP to ensure that the issued licenses will be trustworthily interpreted and executed on the front-end consumer devices. Moreover, the Contents Encrypted Key can be also better protected by Trusted Platform Module that is a physical chip at trusted devices. Therefore, these factors above mentioned would yield the positive utility $u_{\text{Providers}}^{PoDA}$, and meanwhile DP would acquire $u_{\text{Providers}}^{PoTC}$ from users' purchase of the kind of devices. The other side of a coin, DA enforcement directly results in managerial overheads of DRM system, together with negative session-level utilities. The costs related to indispensable infrastructure like Integrity Management and Privacy CA are considered in the paper, we assume that *Providers* deploys them beforehand. These session-level impact-factors, such as the time delay of contents transactions, computing and storage were denoted by $f_{\text{Providers}}^{CoDA}$ as a whole, with its utility being $u_{\text{Providers}}^{CoDA}$.

For *Sharer*, a general security policy sp_{Sharer}^{G} or enhanced security policy sp_{Sharer}^{E} manifests the purchase and usage of the common or trusted computing enabling device/consumer electronics. Here assume that sharers could acquire the baseline utility $\mu_{\text{Consumer}}^{baseline}$ when they hold a general terminal. And, the employment of the enhancing security device could safeguard sharers against maliciously collecting, disseminating confidential and sensitive personal information.

When a sharer adopts trusted computing device, there are the positive and negative factors for a transactional session with DA functionality, which were denoted by f_{Sharer}^{PoDA} and f_{Sharer}^{CoDA}, with corresponding utilities being u_{Sharer}^{PoDA} and u_{Sharer}^{CoDA}. Besides, u_{Sharer}^{CoTC} denotes the expenditure of purchasing the higher security device.

2.2 Contents Sharing Tree and Dynamic and Mixed Game

After purchasing digital contents from CP/RP, an original purchaser could share the contents/rights to other users. Assume that rights delegatee can merely acquire transferable permissions from a sharer, thus a simplified contents sharing tree among original purchaser and sharers was illustrated by Figure 1, where a predefined *W* denotes the width of the tree, with a goal to restrict the user number of the contents sharing for a sharer, and three tuple (al, m, n) presents the purchased/acquired sharing rights, as well as shareable rights when the enhanced or general security policy is adopted. Generally, *m* is greater than *n* in combination with a practical business model. Further, assume that rights are averagely shared in accordance with the present tree width, and any sharer only consumes one of rights.

In term of the sharing tree, *Providers* need to consider a concrete strategy suitable for a whole share chain participated by a group of contents sharer, therefore, there is a dynamic and mixed game between *Sharer* and *Providers*. The former's strategy is equal to a move, which is the choice on whether or not to adopt of higher security devices/components, whereas the latter's one is a set of related moves for a succession of sharing processes. The game was illustrated by Figure 2, and here an ellipse denotes an Information Set, where any participant's move would be not observed by the other. In the game, for any sharer, he/she need to make decision on one of strategies, G-Strategy and E-Strategy, denoting the common or enhanced security policy, respectively. Owing to 2 times of sharing processes shown in Figure 2, there exist 16 kinds of move profiles for *Provider*. When the number is *n*, 2^{2n} move profiles yield. Significantly, two move profiles, (G, G, G, G) and (E, E, E, E), were defined as All-General-Security (All-G) Strategy and All-Enhanced-

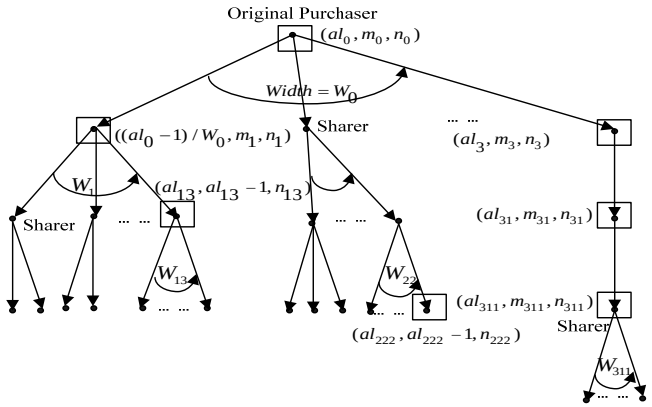


Figure 1. A Contents Sharing Tree with Dynamic Width

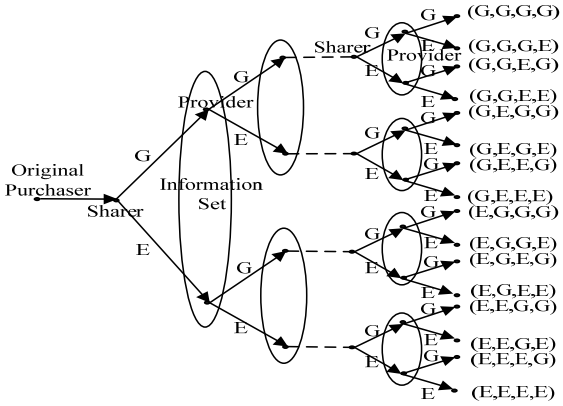


Figure 2. A Dynamic and Mixed Game between *Providers* and *Sharer* in Contents Sharing Scenario

Security (All-E) Strategy. Besides, other several profiles with the interesting consistency characteristic, which manifests that *Providers*' choices of security policies are dependent on *Sharer*' s adoptions, were seen as Dynamic Security Strategy for *Providers*.

2.3 Game-Theoretic Analyses and Algorithm

Participants' payoffs for different move profiles were given as following Formula (1)-(4), and these payoffs were computing according to a group of formal definitions on security policies utility u and influencing-factor weight W for any RA (Rational Agent) [17]. Three payoff matrixes of the one-stage simultaneous-move game between *Providers* and *Sharer* was as Figure 3 (a)-(c). Here w' denotes the normalized weights.

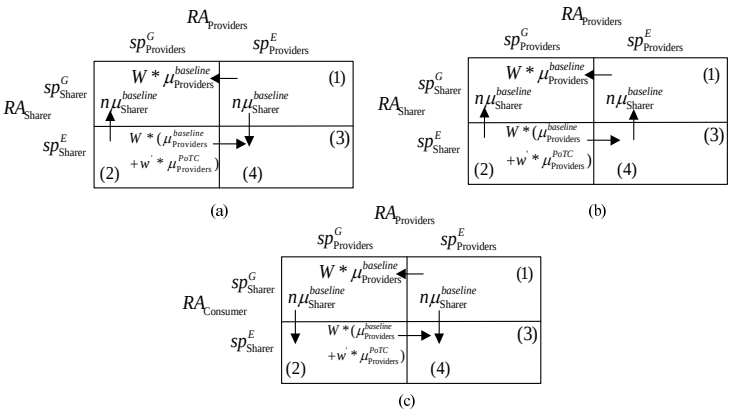


Figure 3. Payoff Matrixes of Simultaneous-Move Game between Providers and Sharer

$$Payoff(RA^{E}_{\text{Providers}}, RA^{G}_{Sharer}) = W * (\mu^{baseline}_{\text{Providers}} - u^{CoDA}_{\text{Providers}} * w^{CoDA}_{\text{Providers}} / \sum_{t=1}^{w(\text{Providers})} w_t) \quad (1)$$

$$Payoff(RA^{E}_{Sharer}, RA^{G}_{\text{Providers}}) = m * \mu^{baseline}_{Sharer} - u^{CoTC}_{Sharer} * w^{CoTC}_{Sharer} / \sum_{t=1}^{w(Sharers)} w_t \quad (2)$$

$$\begin{aligned} Payoff(RA^{E}_{\text{Providers}}, RA^{E}_{Sharer}) = W * (&\mu^{baseline}_{\text{Providers}} + u^{PoDA}_{\text{Providers}} * w^{PoDA}_{\text{Providers}} / \sum_{t=1}^{w(\text{Providers})} w_t \\ &- u^{CoDA}_{\text{Providers}} * w^{CoDA}_{\text{Providers}} / \sum_{t=1}^{w(\text{Providers})} w_t + u^{PoTC}_{\text{Providers}} * w^{PoTC}_{\text{Providers}} / \sum_{t=1}^{w(\text{Providers})} w_t) \end{aligned} \quad (3)$$

$$\begin{aligned} Payoff(RA^{E}_{Sharer}, RA^{E}_{\text{Providers}}) = m * (&\mu^{baseline}_{Sharer} + u^{PoDA}_{Sharer} * w^{PoDA}_{Sharer} / \sum_{t=1}^{w(Sharers)} w_t \\ &- u^{CoDA}_{Sharer} * w^{CoDA}_{Sharer} / \sum_{t=1}^{w(Sharers)} w_t) - u^{CoTC}_{Sharer} * w^{CoTC}_{Sharer} / \sum_{t=1}^{w(Sharers)} w_t) \end{aligned} \quad (4)$$

Here suppose that both *Providers* and *Sharer* have the tendency of adoptions of higher security mechanism in order to better protect digital contents and personal sensitive data. Thus, the following Formula (5)-(6) hold:

$$u^{PoDA}_{\text{Providers}} * w^{PoDA}_{\text{Providers}} / \sum_{t=1}^{w(\text{Providers})} w_t - u^{CoDA}_{\text{Providers}} * w^{CoDA}_{\text{Providers}} / \sum_{t=1}^{w(\text{Providers})} w_t > 0 \quad (5)$$

$$u^{PoDA}_{Sharer} * w^{PoDA}_{Sharer} / \sum_{t=1}^{w(Sharers)} w_t - u^{CoDA}_{Sharer} * w^{CoDA}_{Sharer} / \sum_{t=1}^{w(Sharers)} w_t > 0 \quad (6)$$

Further, we got that one of Nash Equilibriums $(\text{sp}^{\text{E}}_{\text{Providers}}, \text{sp}^{\text{E}}_{\text{Sharer}})$ for a one-stage simultaneous-move game when the following Formula (7) or (9) holds, and the other Nash

Equilibrium $(sp^{G}_{\text{Providers}}, sp^{G}_{\text{Sharer}})$ exists when Formula (8) holds. Here $(\text{sp}^{\text{E}}_{\text{Providers}}, \text{sp}^{\text{E}}_{\text{Sharer}})$ is also a Nash Equilibrium with Pareto Optimality if Formula (7) holds.

$$\begin{cases} n\mu^{baseline}_{\text{Sharer}} - (2) > 0 \\ (4) - n\mu^{baseline}_{\text{Sharer}} > 0 \end{cases} \tag{7}$$

$$\begin{cases} n\mu^{baseline}_{\text{Sharer}} - (2) > 0 \\ n\mu^{baseline}_{\text{Sharer}} - (4) > 0 \end{cases} \tag{8}$$

$$\begin{cases} (2) - n\mu^{baseline}_{\text{Sharer}} > 0 \\ (4) - n\mu^{baseline}_{\text{Sharer}} > 0 \end{cases} \tag{9}$$

In term of the above analyses, with the change of parameters *m* and *n*, *Providers* and *Sharer* need to choose different moves in every stage of dynamic and mixed games for realizing their own optimal benefits. There is a rational assumption that the All-E Strategy is superior to Dynamic Security Strategy for *Providers* when all sharers adopt enhanced security devices, as the dynamic strategy can but increase the overhead of the strategy enforcement in the context.

An Algorithm for the game based on the contents sharing tree was presented as follows. Here W of each sub-tree indicates sharers' different sharing modes. For simplicity, we proposed three basic sharing modes as partial, modest and extensive sharing.

Algorithm "Dynamic and Mixed Game between *Providers* and *Sharer* based on Contents Sharing Tree"

Input & Initialization: Let al_0 be the acquired licenses of an original purchaser, and W denotes the present width of a sub-tree. Also, sl_i denotes the number of sharer s_i's sharable digital rights. Obviously, if s_i chooses the enhanced security device, $sl_i = m$, or else $sl_i = n$, meanwhile let *n* be *m*/2. Besides, $e = 0$ and general security $g = 0$, , and a counter, $i = 0$, of.

Output: A strategies profile of Nash Equilibrium between *Providers* and *Sharer*.

Begin

{ Sharable rights $sl_0 = m_0$; // Original purchaser C_0 generally adopts enhanced security devices.

$al_i = sl_0 / W_0$; // Every sharer s_i gains al_i rights, C_0 sharers sl_0 rights to W_0 sharers $s_i (i = 1, 2, ...W_0)$.

For Each s_i

{While $(sl_i > 1)$ // According to the payoff matrix of the one-stage game between *Providers* P_i and s_i.

{ If (Formula (7) holds) or (Formula (9) holds) then

{// $(sp^{E}_{Providers}, sp^{E}_{Sharer})$ is a Nash Equilibrium for the one-stage simultaneous-move game, and *Sharer* adopts sp^{E}_{Sharer}, meanwhile *Providers* adopts the move of $sp^{E}_{Provider}$.

Nash_Strategies [i+1] + = { sp^{E}_{Sharer} }; // *i* is a counter of the array.

$e += 1$; // Move E of *Providers*, and e is a counter.

$sl_{ij} = (al_i - 1)/W$; // s_i sharers sl_i rights to sharer s_{ij} $(j = 1, 2, ...W_i)$, and s_{ij} is a child of s_i.

if $(sl_i > 1)$ then

{ $s_i = s_{ij}$;

num + = 1;} // *num* is the number of sharers besides leaf-nodes.

} {end then}

Else if (Formula (8) holds) then

{// $(sp^{G}_{Providers}, sp^{G}_{Sharer})$ is a Nash Equilibrium for the simultaneous-move game, and *Sharer* adopts $sp^{G}_{Consumer}$, meanwhile *Providers* adopts the move of $sp^{G}_{Provider}$.

Nash_Strategies [i+1] + = { sp^{G}_{Sharer} };

$g = g + 1$; // Move G of s_i, and *g* is a counter.

$sl_{ij} = (al_i - 1)/2W$;

if $(sl_i > 1)$ then

{ $s_i = s_{ij}$;

num + = 1;}

} {Else if}

} {While}

} {For}

Comparing *g*/*e* with the value *num*, Nash_Strategies [i+1] + = {All-G / All-E / Dynamic}

}

End

3. SIMULATION EXPERIMENTS AND DISCUSSIONS

We made a series of Swarm simulation experiments on the two-player game and observed the continuously changeable number of Rational Agents adopting a certain strategy. Through these changes with the temporal progress, i.e. the multi-stage game, we saw stable adoptions of security policies for any participant, further acquiring concrete Nash Equilibriums in the specific contexts. For our experiments, four groups of initialized values of main parameters above mentioned were given as Table I.

Table I. Four Groups of Main Parameters' Initialized Values

Party	$RA_{Providers}$			RA_{Sharer}		
factor	$f^{PoDA}_{\text{Providers}}$	$f^{CoDA}_{\text{Providers}}$	$f^{PoTC}_{\text{Providers}}$	f^{PoDA}_{Sharer}	f^{CoDA}_{Sharer}	f^{CoTC}_{Sharer}
(u_1, w_1)	(10, 2)	(5, 1)	(30, 7)	(8, 3)	(6, 2)	(80, 5)
(u_2, w_2)	(10, 1)	(5, 1)	(30, 8)	(8, 3)	(6, 3)	(80, 4)
(u_3, w_3)	(10, 2)	(5, 0)	(40, 8)	(8, 5)	(6, 1)	(40, 4)
(u_4, w_4)	(10, 1)	(5, 0)	(60, 9)	(8, 8)	(6, 0)	(10, 2)

The simulation is designed for 16 $RA_{Providers}$ agents and 6300 RA_{Sharer} agents with regard to three basic sharing modes and a mixed mode. Due to the limited length of the paper, the simulation results of the mixed mode were merely illustrated by four sub-figures. For any contents sharing sub-tree, three basic sharing modes were presented by widths being equal to 3, 10 and 20, respectively. Assume that initial strategies are All-G and G-Strategy for *Providers* and *Sharer*, respectively.

When all sharers choose partial sharing mode, it was seen that sharer's optimal move is gradually inclined to adoption of E-Strategy (Move), and *Providers* correspondingly adopts All-E or a combination of All-E and Dynamic Security strategy. This is because sharable licenses are only shared for few users, and each user could acquire much more license. Besides, a majority of sharers would adopt optimal move of E-Strategy with the decrease of f^{CoTC}_{Sharer} and related weight influencing total benefits of sharers. From *Providers*' perspective, Dynamic Security is superior to the entirely enhanced security strategy when limited sharable rights and higher security cost. Therefore, *Providers* maybe adopts Dynamic strategy in limited multi-stage games because of the existence of some sharers adopting G-Strategy, but finally, All-E will still be dominant by other two strategies.

When a large number of sharers adopt modest sharing mode, the number of acquired licenses for every sharer change a certain extent. There are a portion of sharers that gain adequate licenses would choose E-strategy according to the payoff matrixes in Fig 3. Whereas, the other portion of sharers only adopt G-strategy as their optimal choice, as limited licenses are not enough to enable users to adopt E. So, there are obviously two kinds of sharers whether or not to adopt trusted computing-enabling enhanced security. From *Providers*' perspective, we see that the early adoption of Dynamic Security Strategy is finally substituted with All-E strategy after several time steps. Moreover, there needs a necessary interpretation that All-E for Provider is rational when a portion of sharers still choose G-strategy, because not all *Consumer* Agents participate every game with *Providers* in our designed experiments.

If all sharers adopt extensive sharing mode, each would gain fewer shared licenses, which leads to an early dominant adoption of G-Strategy for Sharer. But, with the progress of time step, the linear increase of sharable licenses and decreasing cost of enhanced security platform would directly result in a new choice of the optimal E-Strategy. Also, with respect to the sharing mode, none of *Providers* adopts All-G strategy after a few times steps, which is different from the former sharing modes. And then, *Providers* begins to dominantly adopt All-E. Note that the adoption of Dynamic Security strategy is none all the time.

The mixed Sharing mode, that is the dynamic width, manifests the choices of contents sharing modes are different for sharers, and the case is consistent with real contents value chains and sharing scenarios. A Nash Equilibrium of our proposed dynamic and mixed game between *Providers* and *Sharer* was illustrated by Figure 4-5. It is obviously shown that with the increase of acquired sharable rights and the decrease of enhanced security overhead, the adoption of E-

Strategy is gradually dominant for *Sharer* as Figure 4(1)-(4). Also, Dynamic Security for *Providers* could also exists when limited sharable rights and higher security cost as Figure 5(1)-(2), but All-E strategy by degrees change much more advantageous to gain maximum benefits than Dynamic Security strategy, as is shown by Figure 5(3)-(4). Note that the procedure change clearer after two time steps, as is also different from the above mentioned simulations of three single sharing modes. So, with the gradual increase of consumers' sharable rights/contents and significant increase of enhanced security cost, the implementation and deployment of the enhanced security policy on every sharer is a cost-effective and stable strategy in a generic DRM ecosystem and its contents sharing scenarios.

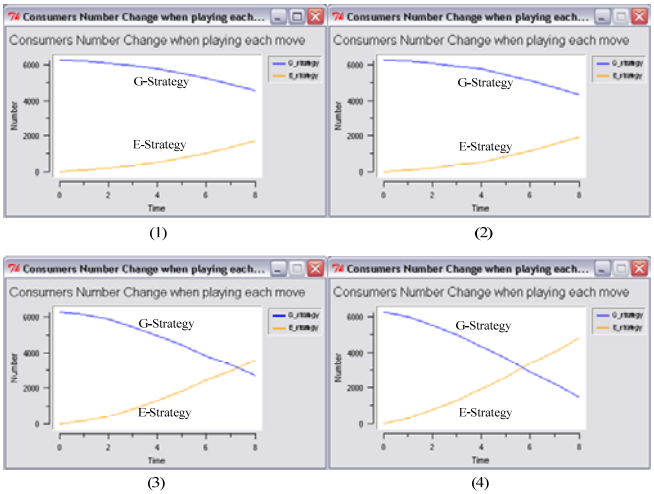


Figure 4. Sharers' Moves Change when Adopting Mixed Sharing Mode

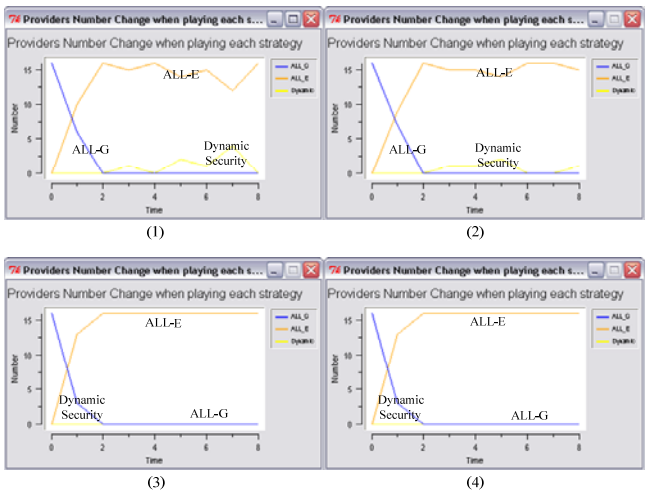


Figure 5. Providers' Strategies Change for Consumers' Mixed Sharing Mode

4. CONCLUSIVE REMARKS

We proposed a game-theoretic analysis and simulations of mutual influences of benefits on DRM *Providers* and *Sharer* when they are faced with security policies having different levels in the contents sharing scenario. It is concluded from our simulation experiments that several main factors, such as the number of acquired sharable digital rights, enhanced security overhead and different sharing modes, have a direct effects on two participants' adoptions of practical strategies in the game. For the mixed sharing mode similar to a real contents sharing scenario, with the increase of acquired sharable rights and the significant decrease of higher security cost, All-E Strategy is optimal. Besides, the exploitation of effective business models is essential to the benefit equilibrium among stakeholders in the contents value chain, for instance, much more digital rights could be shared, and the digital contents in better quality are provided for sharers adopting enhanced security devices.

ACKNOWLEDGMENTS

We are very grateful to Professor Yinghua Min, who is an IEEE Fellow from Institute of Computing Technology, Chinese Academy of Sciences, for his valuable suggestions. Also, we would like to show gratitude to anonymous reviewers for their helpful comments and suggestions. The work is supported by National Natural Science Foundation of China Grant No. 60803150 and No.61003234, the Key Program of National Natural Science Foundation of China Grant No. 60633020, National High Technology Research and Development Program of China Grant No. 2007AA01Z429, and China National 111 Program of Introducing Talents of Discipline to Universities Grant No.B08038.

REFERENCES

1. B. Rosenblatt, "DRM, law and technology: an American perspective," *Online Information Review*, vol.31, no.1, pp.73-84, 2007.
2. DRM Rights Expression Language Candidate Version 2.1.Open Mobile Alliance, 2007.
3. R. Pucella and V. Weissman, "A formal foundation for ODRL," *Proceedings of Workshop on Issues in the Theory of Security*, Barcelona, Spain, 2004.
4. J. Halpern and V. Weissman, "A formal foundation for XrML," *Journal of the ACM*, vol. 55, no.1, pp.4-45, 2008.
5. Z. Y. Zhang, Q. Q. Pei, J. F. Ma, L. Yang, and K. F. Fan, "A Fine-grained Digital Rights Transfer Policy and Trusted Distribution and Enforcement," *Proceedings of International Conference of Computational Intelligence and Security*, Suzhou, China, 2008.
6. C. Hibbert, "A copy protection and content management system from The DVB. The DVB Consortium," http://www.dvb.org/documents/newsletters/DVB-SCENE-05-CopyProtection Article.pdf, 2005.
7. DRM Architecture Candidate Version 2.1.Open Mobile Alliance, 2007.
8. P. Koster, J. Montaner, N. Koraichi, and S. Iacob, "Introduction of the domain issuer in OMA DRM," *Proceedings of 2007 4th Annual IEEE Consumer Communications and Networking Conference*, Las Vegas, Nevada, USA, pp.940-944, 2007.
9. H. KIM, Y. Lee, B. Chung, H. Yoon, J. Lee, and K. Jung, "Digital Rights Management with right delegation for home networks," *Proceedings of 9th International Conference on Information Security and Cryptology*, M.S. Rhee and B. Lee (Eds.): LNCS 4296, pp. 233-245, 2006.

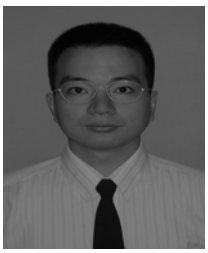
10. P. Koster, F. Kamperman, P. Lenoir, and K. Vrielink, "Identity-based DRM: personal entertainment domain," *Proceeding of Transactions on Data Hiding and Multimedia Security*, LNCS 4300, pp. 104-122, 2006.
11. B. Popescu, B. Crispo, A. Tanenbaum, and F. Kamperman, "A DRM security architecture for home networks," *Proceedings of 4th ACM Workshop on Digital Rights Management*, Alexandria, Virginia, USA, pp. 1-10, Oct. 2004.
12. A. Cooper and A. Martin, "Towards an Open, Trusted Digital Rights Management Platform," *Proceedings of 2006 ACM Workshop on Digital Rights Management*, Alexandria, Virginia, USA, 2006.
13. TCG PC Specific Implementation Specification Version 1.1, https://www.trusted computinggroup.org/specs/PCClient, 2003.
14. TCG Mobile Reference Architecture Specification Version 1.0, https://www.trusted computinggroup.org/specs/mobilephone, 2008.
15. G. Heileman, P. Jamkhedkar, J. Khoury, and C. Hrncir, "The DRM game," *Proceedings of 2007 ACM Workshop on Digital Rights Management*, Alexandria, Virginia, USA. 2007.
16. Y. Chang, "Who should own access rights? A game-theoretical approach to striking the optimal balance in the debate over Digital Rights Management," *Artificial Intelligence and Law*, no.15, pp. 323-356, 2007.
17. Z. Y. Zhang, Q. Q. Pei, J. F. Ma, L. Yang, and K. F. Fan, "Cooperative and Non-Cooperative Game-Theoretic Analyses of Adoptions of Security Policies for DRM," *Proceedings of 5th IEEE International Workshop on Digital Rights Management Impact on Consumer Communications*, Satellite Workshop of 6th IEEE Consumer Communications & Networking Conference, Las Vegas, Nevada, USA, 2009.

ABOUT THE AUTHORS

Z. Zhang received his BSc, MEng degree in Computer Science from Henan Normal University and Dalian Univ.of Technology, China, in 1998 and 2003, respectively. He is now a Ph.D. Candidate in Ministry of Education Key Laboratory of Computer Network & Information Security (CNIS), at Xidian University. He is also an associate professor at Henan University of Science & Technology, Professional Memberships of IEEE (M'06), ACM (M'08) and IEICE (M'08), and Senior Member of China Computer Federation (M'04, S'08). His research interests include Digital Rights Management, trusted computing and access control.

Q. Pei received his BEng, MEng and Ph.D. degrees in Computer Science and Cryptography from Xidian Univ, in 1998, 2005 and 2008, respectively. He is an associate professor, and Professional Memberships of IEEE, ACM and IEICE. His research interests focus on digital contents protection and trusted computing.

J. Ma received his BSc degree in Mathematics from Shannxi Normal Univ. in 1985, and acquired his MEng, PhD degrees in Computer Science and Cryptography from Xidian Univ., in 1988 and 1995, respectively. He was a visiting researcher at Nanyang Technological Univ., Singapore, from 1999 to 2001, and now is a doctorial supervisor at Xidian Univ. and director of CNIS. He is also a Senior Member of Chinese Institute of Electronics and Member of IEEE. His research interests include cryptography and wireless network security.



L. Yang received the BEng, MEng and PhD degrees from National Univ. of Defense Technology of China in 1993, 1996 and 1998, respectively. He is a research fellow in China Electronic Equipment & Systems Engineering Corporation, and doctorial supervisor of Xidian University and National University of Defense Technology. His research interests include system security and network security.