Utility-Analytic Approach and Swarm Simulations of Security Policies in Digital Rights Management

Zhiyong Zhang [1,2], Xinliang Liu [1], Jiexin Pu [1]
1 Electronics Information Engineering College, Henan University of Science and Technology, Luoyang, China
2 School of Management, Xi'an Jiaotong University, Xi'an, China
Email: {zhangzy, lxl, pjx}@haust.edu.cn

Abstract— **DRM (Digital Rights Management) Ecosystem to date lacks of a multi-participant trust for stakeholders, which are involved in Contents Provider, Rights Provider and End User, as has significantly negative impacts on DRM-enabled contents value chain's survivable. In order to establish the trust, a utility-analytic and non-cooperative game approach to the optimal adoption of cost-effective security policies was employed. A series of Swarm-based simulation experiments were highlighted, both considering a generic DRM application scenario on the contents acquisition, and discussing different sharing modes' influences on the adoption strategies of typical security policies for a much more complicated scenario on the contents sharing. The simulation results manifest that the enhanced security policies combination are not necessarily rational under any circumstance for the former scenario, and the optimal combination and its precondition are represented. Besides, the best modest sharing mode would spur consumer and contents provider to earn the maximum benefits, as is based on the given optimal security policies profile.**

Index Terms— **Digital Rights Management, Trust, Security Policies, Non-Cooperative Game Theory, Swarm Simulation**

I. INTRODUCTION

With the rapid development of communication network technologies, the Next-Generation Internet, 3G and 4G wireless mobile networks have been striding to the large-scale deployments and applications. As a result, by using multiple network admission methods, users could access to digital resources and services in anytime, at anywhere, which is much easier than ever before. Under this circumstance, the copyright infringement behaviors, such as the illicit copy, malicious distribution, unauthorized usage, free sharing of copyrights-protected digital contents, have already become a common phenomenon, as the contents like electric book, image, music, movie and application software are very easily duplicated without the deterioration in quality. Thus, the digital contents industry could be heavily damaged, and its value chain may also be interrupted. So, the copyrighted contents protections and legitimate usages are, therefore, crucial. To solve the issue, Digital Rights Management (DRM) technologies have emerged at the beginning of 1990s, and have a variety of applications from the end of 1990s. Recent years have witnessed the significant progress on DRM-enabling techniques, and we are faced with new challenges and opportunities to cope with the piracy much more effectively.

It should be noted that, in the last decades, regardless of general DRM or Mobile DRM, the emphasis has been primarily laid on the research on the contents protection, which is based mainly on cryptographic security and the contents usage permission that is accomplished by Rights Expression Language and Usage Control, as well as on the digital watermark technology used for prosecuting pirate. Apparently the above two roadmaps are both at the standpoints of the digital contents provider or digital rights provider, and the main countermeasure of copyrights infringement is to look for positive security policies, even further enhanced policies. Consequently, digital users may reject DRM technologies and DRM-enabled digital products, which will interrupt the contents chain value. It is stated that DRM should balance the interests of the various stakeholders in the value chain, and enable the IPR (Intellectual Property Rights)-enabling contents industry to flourish. Therefore, from the perspective of DRM value chain's survivability, DRM should embody not merely security policies but the interest balance of involved parties, especially for an establishment of the multi-party trust relationship.

Compared with the previous works, the paper's main contribution is to find out the cost-effective typical security policies combination and best contents sharing mode under a ceratin circumstance, by using holistic Swarm-based simulation experiments, both for a basic scenario on the contents acquisition and for a much more complicated one on the contents sharing, respectively. The the rest of the paper is organized as follows: in Section II, the state-of-the-art of DRM is represented, and Section III focuses on the utility-analytic and non-cooperative game-theoretical formalisms. A comprehensive Swarm simulation experiment is made in the following section, and the conclusive remarks are drew in Section V.

Manuscript received January 1, 2009; revised June 1, 2009; accepted July 1, 2009. Corresponding author: Zhiyong Zhang.

doi:10.4304/jmm.5.5.417-426

II. Related Works

In the DRM value chain, Contents Provider (CP)'s goal is to protect digital contents security, so security policies available are commonly categorized into two sorts: preventive and reactive one. Both employ different security mechanisms and approaches to protect digital contents against malicious piracy in DRM Ecosystem. Thereinto, the former is to employ the cipher-based encryption to meet the requirement of the contents protection [1], [2].

Howerver, cryptograph-based copyrights protection is not consummate. Under a certain circumstance, for example, an analogue environment, an attacker could record the signals of decrypted contents in the process of the contents rendering. Moreover, the emergence of more complicated attack approaches and tools also easily circumvents or disables cipher protections mechanisms sometimes [3]. To prosecute the illicit usage and copyrights infringement, digital watermarking is a reactive approach to authenticate the ownership of copyrighted contents and provide forensic proofs through the detection/decoding of the pre-embedded imperceptible watermark, so as to realize the contents' usage tracking and copyrights infringement authentication based on the watermark and biological features [4], [5].

In addition, In DRM value chain, other than CP-centered preventive and reactive policies for the copyrights protection, there also exist Rights Provider (RP)-centric digital rights expressions and usage control [6]. The former is involved in REL (Rights Expression Language), and the latter mainly implement the controlled usage of digital rights predefined by RP by using a certain REL. In a generally way, REL is employed to specify the contents usage policies, which are composed of a group of grant rules depicting some concrete rights/permissions under the given conditions and constraints. Existing representative RELs, for instance, XrML [7], ODRL [8] and MPEG-21 REL [9], have gradually progressed and been precisely specified in recent years. However, Jamkhedkar et.al. [10] addressed a significant issue of "language bloat". Some new DRM-related business models tend to be continuously introduced to DRM ecosystem, but the current RELs may be incapable of specifying material rights and their managements in any particular scenario, as a consequence, a certain REL would been extended on the basis of the original REL so that it could support multiple business models. The reason why the issue emerges is due largely to the lack of a separation of rights expression and rights management, directly resulting in REL being more complicated and even difficult to operate. Therefore, we still need much attempt to solve the issue.

The above mentioned approaches to the copyrights protection primarily focus on digital contents/services side. It should be noted that DRM trust has recent years been paid much more attentions from a novel perspective of contents value chain ecosystem.

A. DRM Trust Models

1) PKI-Based OMA DRM Trust Model: As a representative industry alliance engaging in DRM, OMA has ever proposed a trust model in DRM Architecture [11] and DRM Specification [12]. PKI being its basis, this model attempted to build a trust relationship between RI and DRM Agent run in the user device. If the Agent was verified to be a trusted component by using a non-revoked certificate that was issued by the TTP (Trusted Third Party) as CA, RI would trust the behaviors of the Agent. In other words, an Agent produced by a certain trusted manufacturer has the trustworthiness of the license enforcement. Similar to this case, DRM Agent could also trust a RI through the certificate-based authentication. Obviously, OMA DRM trust model mainly refers to trust relations between logical functional entities. However, this mutual trust is not sufficient for the general open terminal platforms and complicated network environment, because the certificate issued by CA could only ensure that the identity and origin of an entity is genuine without being able to guarantee the run-time behavioral trustworthiness, as it is a static trust.

Content Management License Administrator (CMLA), which is a Limited Liability Company sponsored by four distinguished IT companies, including Intel, Nokia, MEI/Panasonic and Samsung, has made an active effort to realize the trust model for OMA DRM V2.0. As a holistic objective of CMLA is to enable a wide and trusted distribution of DRM contents in a large digital ecosystem, it plays a role of the PKI creator and administrator, and proposes a hierarchy PKI system in order to build the trust [13]. The proposed PKI system is composed of some basic entities, such as Root CA, Device CA(s), RI CA and OCSP (Online Certificate Status Protocol) Responder, which is a key entity to provide the verification of the certificate validity in Internet X.509 PKI, as well as a series of certificate objects issued by various CAs. Meanwhile, CMLA represented some fundamental requirements of a robust DRM realization, and Certifications Principles for Service Provider and Client Adopter (device). These principles are used to justify whether consumers' devices including DRM Agent, applications and services, are well implemented or not, that is to say meeting CMLA Compliance and Robustness Rules. Note that CMLA does not replace or modify OMA DRM Specs, nor is it a prerequisite or requirement for the OMA DRM architecture. So there may be other trust models except CMLA in the DRM ecosystem. Though no doubt that CMLA supported and extended the trust model of OMA, both have the same disadvantages that the run-time trustworthiness of entities could not be guaranteed, and that they do not provide verification mechanisms and realization approaches to improving multi-party trust in the DRM ecosystem. Moreover, the overhead of establishing PKI also must be taken into account.

2) Web of Trust in DRM Ecosystem: Arnab [14] presented a standpoint that the trust in a DRM system is determined by how much confidence the Producer

and Consumer have in the implementations of DRM components and services. However, the trust relationship would be easy to break along with an increase of entities that need to be trusted, and the traditional trust chain is linear and not completely suitable for depicting the trust relations among DRM components. For this, a conceptual web architecture of the trust for DRM was proposed, and a key distribution scheme, including the contents decryption key and the license key, was designed based on the trust web.

The entities were categorized into three sorts in the trust web. The first sort is a set of several active entities such as Contents Producer and Consumer in the DRM value chain. The second one is a set of basic components/services indispensable to a DRM system, such as DRM Controller, License Server and Packaging Service. The last one includes Independent Verification Authority that is trusted by Producer and Consumer to verify the trustworthiness of DRM Controller, and Authentication & Credentials Service Producer which mainly implement access control functions and authentication mechanisms. And, both could be recognized as an active entity or a service affiliated to any active party like CMLA. In the web of trust, RP was not explicitly shown, but License Server should belong to an implicit RP similar to RI. Besides, there is only the conceptual multi-party trust architecture, and its trust was established on the basis of the secure key dissemination and storage, lacking a more practical trust mechanism other than the OMA trust model.

To the best of our knowledge, there is still a lack of benefit-centric multi-participant trust for DRM Ecosystem, not merely the consideration of security. The paper's goal is right to investigate on the open issue.

III. Non-Cooperative Game-Theoretical Adoptions of Security Policies

Utility and Game theory are a category of Decision Theory, with a goal to analyze a certain situation in which the payoffs of participants directly or indirectly depend on the mutual behaviors. Based on a fundamental assumption that every player is a rational agent, the optimal strategies combination (profile), that is Nash Equilibrium, can be achieved through the round mathematical and formal analysis. In this section, the utility and game theory were employed to accomplish a rational decision-marking in face of various security policies for DRM, and related formal definitions and propositions were presented.

A. DRM Security Policies and Properties

Definition 1 (Security Component/Service) In term of security requirements for participants, an atomic functionality security component could be a program, hardware/firmware unit and middleware, as well as a functional security service is realized to accomplish a group of related functions. Here basic security components/services are written by c^*/s^*, and optional ones denoted by c/s. Notations f, w, u, μ manifest a factor from the Factor Set F influencing the whole benefit of $\wp$ for an adoption of c/s, the factor weight value, the factor utility, as well as the positive/negative utilities sum when adopting c/s, respectively. Note that the weight's normalization is based on all factors' weights involved in c/s.

$$SecurityComponent = \{c_1^*,\ c_2^*,\ ...\ c_i^*, c_1,\ c_2,\ ...\ c_j\}$$
$$SecurityService = \{s_1^*,\ s_2^*,\ ...\ s_m^*,\ s_1,\ s_2,\ ...\ s_n\}$$
$$F(c_s) = \{f_{c1},\ f_{c2},\ ...\ f_{cp}\}$$
$$F(s_t) = \{f_{s1}\ ,\ f_{s2},\ ...\ f_{sq}\}$$
$$(1 \le s \le j, 1 \le t \le n)$$
$$\mu(c_s) = \sum_{i=1}^{p} u_i\ (\ w_i / \sum_{k=1}^{h} w_k)$$
$$\mu(s_t) = \sum_{j=1}^{q} u_j\ (\ w_j / \sum_{k=1}^{l} w_k)$$

Definition 2 (Security Policy) *sp* is composed of a group of relevant security components/services, which include all c^*/s^* and some c/s that are adopted by $\wp$ with a specific security goal, where $\Im(.)$ denotes the set cardinality.

$$sp = \{c_1^*, ..., c_i^*, s_1^*, ..., s_m^*, c_1, c_2, ...c_s, s_1, s_2, ...s_t\}$$
$$(0 \le s \le j, 0 \le t \le n)$$
$$SP_i = \{sp_i^1, sp_i^2, ..., sp_i^{\Im(SP_i)}\}$$
$$(\Im(SP_i) = 2^{(j+n)}, i \in \{CP, RP, Consumer\})$$

Definition 3 (Utility of *sp*) Utility U of *sp* is a sum of utilities μ of all security components and services involved in *sp*.

$$U(sp_a^b) = \sum_{p=0}^{i}\sum_{q=0}^{m}(\mu(c_p^*) + \mu(s_q^*)) + \sum_{p=0}^{j}\sum_{q=0}^{n}(\mu(c_p) + \mu(s_q))$$

B. Non-Cooperative Game on Security Polices

Definition 4 (Payoff of *RA*) *RA* denotes a rational actor aiming at the benefit maximum, and makes decisions on adopting security policies. The payoff of *RA* denotes the acquired benefit under a security policy combination (profile) that is a vector of security policies adopted by *RA*s' actions. The payoff includes two aspects, one being from *RA* itself and the other being from other *RA*s' moves.

Definition 5 (Multi-Party Game on Security Policies) The game depicts a process of making decision on effective and rational adoptions of security policies, where participants' moves have effects on benefits one another. To achieve utility maximum and benefit balance, the game is formalized by a set of the three tuple as $< \wp, sp, payoff >$, where SP manifests a set of security policies.

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

Proposition 1 (Non-Cooperative Simultaneous-Move Game in Contents Acquisition Scenario) Contents acquisition (purchase) is a general DRM application scenario, where adoptions of security policies are considered

as a specific multi-player simultaneous-move game process game among CP, RP and Consumer.

Proof: In MPTA, there are RA_{CP}, RA_{RP}, $RA_{consumer}$ in term of Definition 5, and let SP_{CP}, SP_{RP} and $SP_{Consumer}$ be a security policies set, respectively. The game is further formalized as $G_{acquisition} =< RA_i, SP_i, Payoff(RA_i, RA_{-i}) >$, where $i = \{CP, RP, Consumer\}$. For the deployment and the initialization of a DRM system, any party needs to choose and active relative security components/services, which is to say, to adopt a specific *sp* from *SP*. In general, the contents acquisition process has temporal order characteristic, taking a DRM Pull model as an example, $RA_{consumer}$ acquires a corresponding license of the purchased content from RA_{RP} after acquiring contents from RA_{CP}. However, each *RA* adopts and initializes *sp* without knowing the moves of other *RA*s' *sp*, meanwhile the activeness of *sp* could not change after DRM system initialization for a contents transaction, so the whole process of all *RA*s' moves is a simultaneous-move game on security policies, not a sequential-move game. ■

Proposition 2 (Dynamic and Mixed Game in Contents Sharing Scenario) When transactional sessions of the contents sharing have implemented more times among multiple users, participants of DRM ecosystem become a multi-game behavior on adoptions of security policies. The new game is a dynamic and mixed game based on the former non-cooperative game and its result, and a new equilibrium could be gained.

Proof: In the given scenario, with the increase of contents transactions, the adoptions of security policies would correspondingly change. When RA_{CP}, RA_{RP}, and $RA_{Consumer}$ choose security policies over again, a repeated game occurs in combination with the former game and the concrete numbers of transaction sessions, and the newly gained security policies profile becomes a new Nash Equilibrium.

Contents Sharing is a typical user-centric scenario, and there is a dynamic and mixed game on security policies for any contents sharing tree. In the given scenario, without a loss of generality, CP, RP and DP are simplified considered as a whole, which is called $RA_{Providers}$. Thus only two participants $RA_{Providers}$ and $RA_{Consumer}$ are discussed. As contents sharing procedure is seen by a tree structure for any original contents purchaser C_0. For the tree, C_0 shares his/her contents with C_i, C_{i+1}, …,C_n via a branch of tree, and $RA_{Providers}$ and $RA_{Consumer}$ will accomplish a Simultaneous-Move Game on adoptions of security policies for every sharing action of C_i. There is also a repeated game between both parties from an entire branch, even sharing tree, and the previous sharing action has a direct effect on the later choice of security policies in the game. So a repeated dynamic game with mixed multiple simultaneous-move sub-games exists in contents sharing scenario of GDRM ecosystem. ■

IV. SWARM SIMULATIONS

A. Typical Security Policy Set

The subsection presents several typical security policies in a general DRM ecosystem, and a practical DRM application may include these policies, but are not limited to. But, it should be noted that there are two properties on security components/services and security policies. Thereinto, if two or more optional components/services that are from different parties need to be adopted simultaneously, otherwise the active c/s has a negative utility on corresponding parties, these components/services are of the external relativity, Futher, the security policies'external relative is deduced, that is if two or more different security policies refer to c/s with the external relativity [15].

CP-centric security components/services include:

- **Packaging:**by using the functional component, digital contents are encrypted based on a specific cryptographic algorithm, and encapsulated as a distributable data object format. The component is dispensable to DRM system.
- **Watermarking (WM):** the basic security service provides a passive copyrights protection function and forensic proof, and is adopted to authenticate the ownership of contents through the detection/decoding of pre-embedded imperceptible watermarking.
- **Identification:** it is adopted to accomplish contents security, for instance, to validate by using a verification service provided by the third party whether a Java application is embedded into a section of malicious codes. Then, Consumer could acquire trustworthy contents when a certain trust level is authenticated. The function is also optional to CP, whether it is active or not is dependent on CP' security policy in a transaction.
- **Transaction-based Negotiation with RP (TN):** In a general value chain of DRM, CP and RP are respectively responsible for dissemination of digital contents and rights (or licenses). The service is advantageous to the distribution of contents/license, and to the creation of business trust relationship between CP and RP. Note that the trust negotiation is executed when each transaction begins, not when DRM system establishes.

As the set of CP's security components is {*Packaging**, *WM**, *Identification*, *TN*}, and obviously, the set of security policies include the following policies: {*Packaging**,*WM**}, {*Packaging**, *WM**, *Identification*}, {*Packaging**, *WM**, *TN*}, {*Packaging**, *WM**, *Identification*, *TN*}, denoted by $sp^1_{CP}, sp^2_{CP}, sp^3_{CP}, sp^4_{CP}$, respectively.

RP-centric security components/services are listed as follows:

- **Rights Expression and Issue (REI):** by the functional services, RP specifies and distributes a license of granting corresponding digital rights in term of purchased contents and payment, realizing persistent

usage control on contents. The services are considered to be essential to contents legitimate usage from RP's perspective.

- **Consumer's Identity Authentication (IA):** authentication provided by the basic component not only ensures the identity of purchaser, but provides a detailed log of the purchase.
- **User's Terminal Device Attestation (DA):** based on trusted computing-enabling device and remote attestation technology, RP could validate user device and key components' integrity, then, send a license to them. The functionality is not necessary for each transaction, but optional.
- **Transaction-based Negotiation with CP (TN):** as is above mentioned, it is optional.

Similarly, due to the set of RP's security components denoted by $\{REI^*, IA^*, DA, TN\}$, the set of security policies is $\{\{REI^*, IA^*\}, \{REI^*, IA^*, DA\}, \{REI^*, IA^*, TN\}, \{REI^*, IA^*, DA, TN\}\}$, denoted by $\{sp^1_{RP}, sp^2_{RP}, sp^3_{RP}, sp^4_{RP}\}$.

Finally, consumer's security functional components include:

- **DRM Controller:** this is a key component to effectively control content's legal usage by validating corresponding license and rights.
- **Contents Restricted Execution (CRE):** based on the optional service, consumer could restrict content's usage and execution in terminal device according to the trust level of contents, which is provided by CP.
- **Trusted Computing Device (TCD):** consumer could further implement enhanced security of DRM application and safeguard their confidential and sensitive personal information from collecting and disseminating.

Consumer's the set of security components is $\{Controller^*, CRE, TCD\}$, so security policies are composed of $\{Controller^*\}$, $\{Controller^*, CRE\}$, $\{Controller^*, TCD\}$ and $\{Controller^*, CRE, TCD\}$ denoted by $sp^1_{Consumer}$, $sp^2_{Consumer}$, $sp^3_{Consumer}$ and $sp^4_{Consumer}$, respectively.

B. Swarm Simulations in Contents Acquisition Scenario

Swarm project [16], sponsored by Santa Fe Institute in 1994, has an objective to develop a series of multi-agent simulation system and to provide researchers with the object-oriented programming feature and versatile tool kits, so that the modeling engineers could dedicate themselves to the essential characteristics of a modeling task, and not care the trivial details of the multi-agent programming. Swarm is a simulation environment suitable for the multi-agent system and modeling, and includes a conceptual framework for designing, describing, and conducting experiments on agent-based models. In last decade, Swarm has been successfully applied to intelligent system controls and processes in the realm of Artificial Intelligent, economics simulation and multi-participant game, etc.

We employ Swarm 2.2 for Java and MyEclipse 6.5 to make experiment on multiple agents' decision-making on adoptions of security policies, and there exist 100 Contents Provider agents (*CP*-agent), 100 Rights Provider agents (*RP*-agent) and 1600 Consumer agents (*Consumer*-agent) in the simulation. Besides, in the Swarm simulation, the concept of time step denotes the simultaneous-move game between three participants in the contents value chain.

A series of experiments were made on multi-party game and observed the changeable number of Agent adopting a certain security policy by using Swarm software package. Through these changes with temporal progress, we saw stable adoptions of security policies for participants, further acquiring the concrete Nash Equilibrium. In these experiments, four groups of initial values were given as Table 1. Besides, functions of main parameters, such as m, n, s, these parameters change in a linear way.

In term of Table 1, simulations results are illustrated by Figure 1- Figure 3.

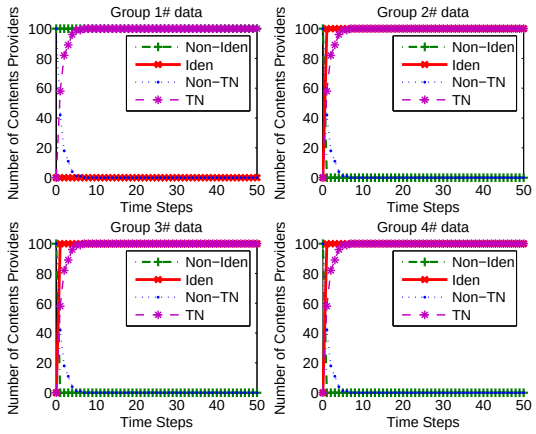

Figure 1. CP number change with time for different initial values

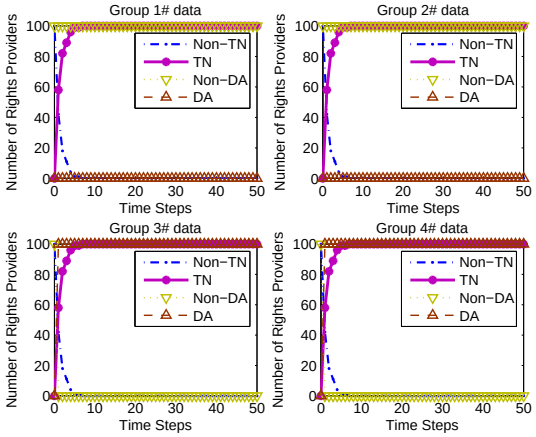

Figure 2. RP number change with time for different initial values

The above simulation results manifest that some strategies be gradually dominant with time, so we could find

TABLE I.
FOUR GROUPS OF INITIAL VALUES AND FUNCTIONS OF MAIN PARAMETERS

Party	RA_{CP}				RA_{RP}		
Factor	f_{CP}^{PoI}	f_{CP}^{CoI}	f_{CP}^{PoTN}	f_{CP}^{PoTN}	f_{RP}^{PoDA}	f_{RP}^{CoDA}	f_{RP}^{CoTC}
(u_1,w_1)	(10,3.5)	(50,2.5)	(30,2.1)	(15,1.9)	(25,2.1)	(15,2.0)	(50,2.5)
(u_2,w_2)	(20,3.7)	(30,2.2)	(35,2.5)	(12,1.6)	(30,2.5)	(10,1.8)	(45,2.3)
(u_3,w_3)	(35,3.9)	(20,1.5)	(45,3.0)	(8,1.6)	(40,3.1)	(8,1.5)	(30,2.0)
(u_4,w_4)	(50,4.0)	(10,1.3)	(60,3.7)	(3,1.0)	(65,3.7)	(5,1.2)	(20,1.7)
Party	RA_{RP}		$RA_{Consumer}$				
Factor	f_{RP}^{PoTN}	f_{RP}^{CoTN}	f_{Cons}^{PoCRE}	f_{Cons}^{CoCRE}	f_{Cons}^{PoDA}	f_{Cons}^{CoDA}	f_{Cons}^{CoTC}
(u_1,w_1)	(20,1.9)	(18,1.5)	(13,1.1)	(20,1.8)	(10,1.0)	(15,1.8)	(70,4.3)
(u_2,w_2)	(25,1.8)	(15,1.6)	(18,1.6)	(18,1.6)	(15,1.4)	(13,1.9)	(50,3.5)
(u_3,w_3)	(30,2.0)	(10,1.4)	(50,2)	(10,1.5)	(30,2.4)	(8,1.4)	(30,2.7)
(u_4,w_4)	(40,2.4)	(8,1.0)	(70,3.2)	(5,1.3)	(50,3.3)	(5,1.0)	(10,1.2)

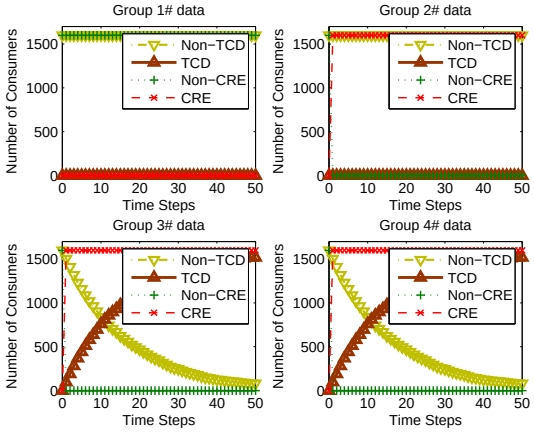

Figure 3. Consumer number change with time for different initial values

out the Nash Equilibrium of the multi-party game. Figure 1(1)-(4) illustrate sp_{CP}^3 including *TN* and sp_{CP}^2 having *Identification* are gradually dominant over sp_{CP}^1, thus CP would finally adopt sp_{CP}^4. With regard to RP, his adoption of security policies changes from sp_{RP}^3 to sp_{RP}^4 with the increase of m and n, together with the decrease of enhanced security overhead, as is shown by Figure 2(1)-(4). Note that RP firstly adopts sp_{RP}^3 including *TN* as Figure 2(1)-(2), which is consistent with the adoption of CP, and then begin employing *DA* in Figure 2(3)-(4), as Consumer also adopts *TCD* shown by the following Figure 3(3)-(4). It is seen from Figure 3(1)-(4) that Consumer would gradually adopts $sp_{Consumer}^4$ instead of other three kinds of security polices owing to the significant decrease of the enhanced security platform cost and its weight. When the weight is dominant over other weights, the adoption of enhanced RA functionality would bring the effective utilities for RP and Consumer, and the security policies including *DA*, for instance $sp_{Consumer}^2$ or $sp_{Consumer}^4$ is optimal strategy in any time. Here it is obvious that $sp_{Consumer}^4$ would become a dominant policy, as *CRE* is employed in Figure 3(1)-(2). To sum up, Nash Equilibrium would not be invariable with the increase of contents transactions, as well as change of impact factors and their weights, and $(sp_{CP}^4, sp_{RP}^4, sp_{Consumer}^4)$ becomes a optimal strategy combination for multi-party benefit balance in a certain preconditions after some time steps (repeated game).

C. Swarm Simulations in Contents Sharing Scenario

Based on the game-theoretic analysis on adoptions of security policies, we made a series of simulation experiments to explore on some interesting results related to dynamic and mixed game between *Providers* and *Sharer*. The Swarm simulation software kit, a representative simulation tool suitable for multi-agent systems and modeling, is employed to improve on our game-theoretic analysis or verify related theoretical conclusions. We simulate three scenarios in term of three kinds of contents sharing modes, respectively, and observe the consecutive changes of the quantity of agents adopting a certain move/strategy, further find out the optimal security policies (combination).

D. Basic Simulation Environment and Procedure

In the simulation, we continued to employ Swarm 2.2 for Java and MyEclipse 6.5 to make experiment on multiple agents' decision-making on adoptions of security policies, and there exist 16 *Providers* agents (P-agent) and 6300 *Sharer* agents (S-agent). With respect to Swarm simulation, the concept of time step denotes the dynamic and repeated game between two participants in the contents value chain. For any time step, we firstly randomly choose a *P-agent* that denotes an original purchaser, thus S-agent that is a sharer and related other S-agents constituting the contents sharing tree. And then, the game processes of all 16 *P-agents* are executed, and the number of agents adopting a specific security policy is also statistically given birth to. After multiple time steps, we gain the statistical curves with regard to the changeable quantity of agents, and as a result the optimal (dominant) security policy (combination) emerges clearly.

By Swarm simulation experiments on two-player game and observing the continuously changeable quantity of agents adopting a certain strategy. Through these changes with temporal progress, we saw stable adoptions of security policies for participants, further acquiring concrete Nash Equilibriums in specific conditions. In these experiments, four groups of initialized values of main parameters were given as Table 2.

TABLE II.
FOUR GROUPS OF INITIALIZED VALUES OF MAIN PARAMETERS

Participant	$RA_{Providers}$			RA_{Sharer}		
Factor	$f_{Providers}^{PoDA}$	$f_{Providers}^{CoDA}$	$f_{Providers}^{PoTC}$	f_{Sharer}^{PoDA}	f_{Sharer}^{CoDA}	f_{Sharer}^{CoTC}
(u_1,w_1)	(25,2)	(5,1)	(50,7)	(20,3)	(6,2)	(80,5)
(u_2,w_2)	(25,1)	(5,1)	(60,8)	(20,4)	(6,1)	(50,5)
(u_3,w_3)	(25,2)	(5,0)	(70,8)	(20,5)	(6,1)	(30,4)
(u_4,w_4)	(25,1)	(5,0)	(90,9)	(20,9)	(6,0)	(10,1)

The following simulation results manifest that adoptions of strategies are different in various sharing modes, as are shown by Figure 4- Figure 11. In our simulations, three basic sharing modes, including partial, modest and extensive, as well as the mixed, denote the scope of sharable consumers for an original purchaser, and have differently influences on the strategies of the security policies adoption for *Providers* and *Sharer*. These basic modes were presented by the above mentioned sharing subtree widths having the subjection to integer regions as [1,3], [4,10] and [11,20], respectively. Also, simulation results of corresponding four groups of initial values were illustrated by four sub-figures in every figure. Assume that initial strategies are All-G and G-Strategy for *Providers* and *Sharer*, respectively.

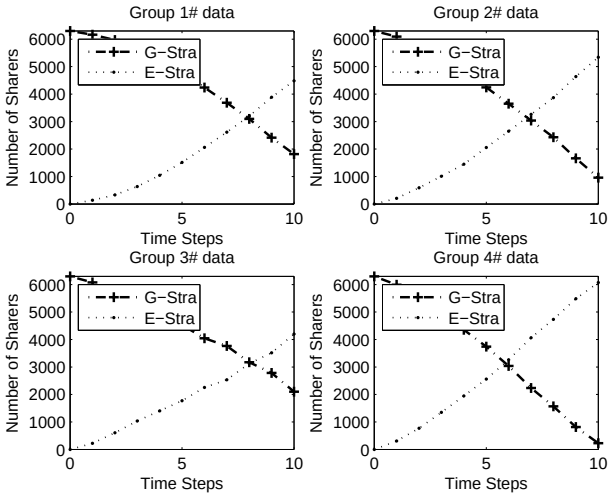

Figure 4. Sharers' moves change when adopting partial sharing mode

When all sharers choose partial sharing mode, it was seen that sharer's optimal move is gradually inclined to adoption of E-Strategy (Move) in Figure 4, and *Providers* correspondingly adopts All-E or a marriage of All-E and Dynamic Security strategy in Figure 5. This is because sharable licenses are only shared for a 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_{Sharer}^{CoTC} and related weight influencing total benefits of sharer. From *Providers*' perspective, Dynamic Security is superior to the entirely enhanced security strategy when limited sharable rights and higher security cost, as is shown in Figure 5(1)-(3). Therefore, *Providers* maybe adopts Dynamic strategy in limited repeated games because of the existence of some

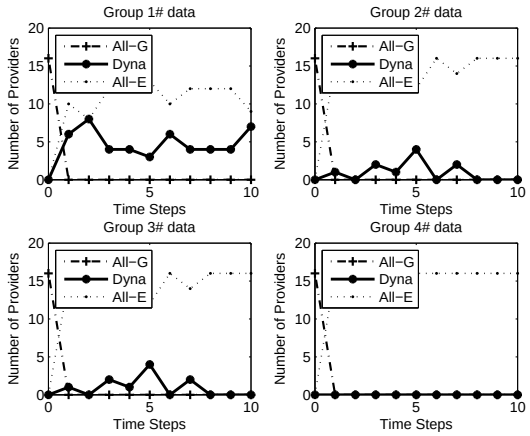

Figure 5. Providers' strategies change for Consumers' partial sharing mode

sharers adopting G-Strategy, but finally, All-E will still be dominant by other two strategies, as Figure 5(4).

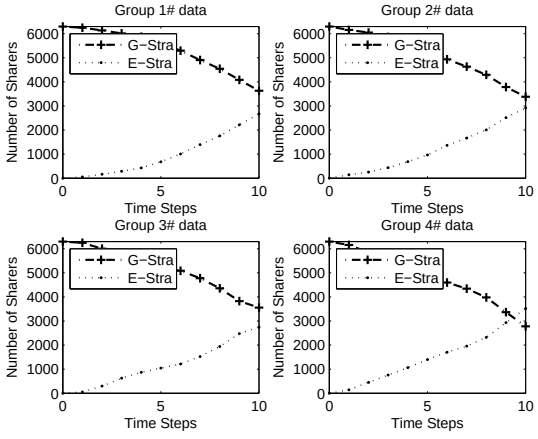

Figure 6. Sharers' moves change when adopting modest sharing mode

When a large number of shares belonging to Sharer participants adopt modest sharing mode, the number of acquired licenses for every shared sharer change to be limited. There are a portion of sharers that gain adequate licenses would choose E-strategy according to security polices' utility. 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-strategy. So, there are obviously two kinds of sharers whether or not to adopt trusted computing-enabling enhanced secu-

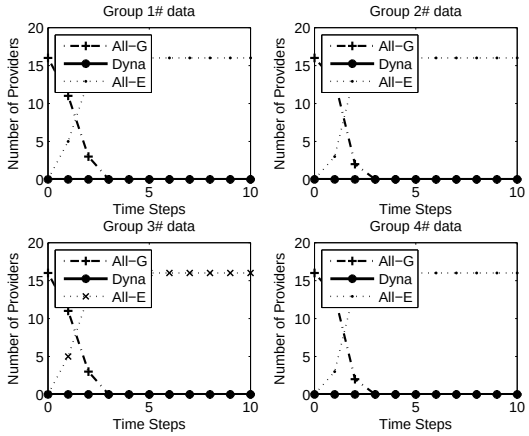

Figure 7. Providers' strategies change for Consumers' modest sharing mode

rity, as is shown by Figure 6. From Provider's perspective, we see from Figure 7 that All-E strategy is dominant over other two strategies after repeated games, and there is no adoptions of Dynamic-Security strategy, which is similar to Figure 5(4). Besides, it should be noted that after 3 time steps in Figure 6 and Figure 7, All-E for Provider is optimal when a portion of shares still choose G-strategy, because not all *sharer* agents participate any game with *Providers* in our designed simulation experiment.

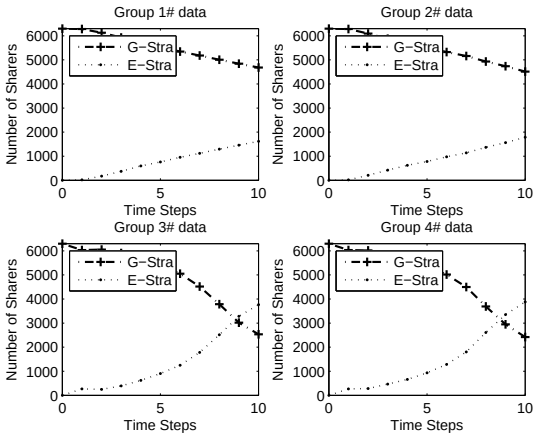

Figure 8. Sharers' moves change when adopting extensive sharing mode

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 in much more time steps, as is shown by Figure 8(1)-(2). But, Figure 8(3)-(4) denote that with the change of time step, the linear increase of sharable licenses and obvious decreases of enhanced security platform cost would directly result in the dominant E-Strategy. And also, with respect to the sharing mode, *Providers* adopting All-G strategy change none after 7 times steps as Figure 9, which is different from one time step in Figure 5 and Figure 7. However, we see the adoption of Dynamic Security strategy is none

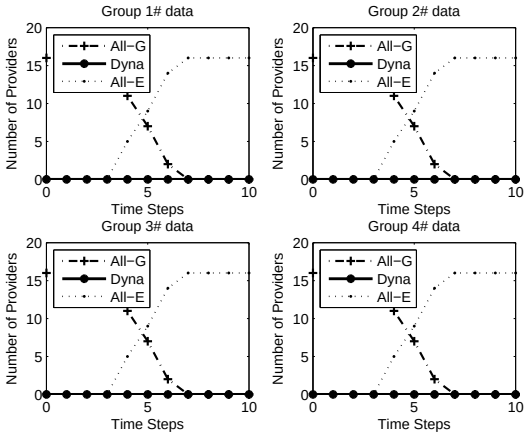

Figure 9. Providers' strategies change for Consumers' extensive sharing mode

all the time, which is similar to Figure 7.

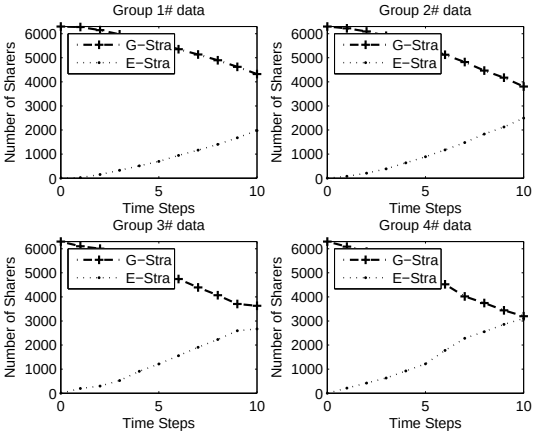

Figure 10. Sharers' moves change when adopting mixed sharing modes

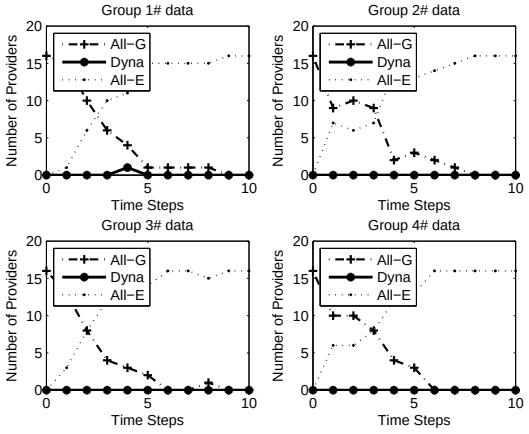

Figure 11. Providers' strategies change for Consumers' mixed sharing modes

Dynamic width manifests the choices of contents sharing modes are different for sharers, and it is consistent

with a 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 10- Figure 11. Firstly, in Figure 10(1)-(4), it is clearly shown that the G-Strategy is gradually dominated over E-Strategy for sharers, with the increase of acquired sharable rights and decrease of *TCD* cost. In addition, Dynamic Security Policy for *Providers* could also exists when limited sharable rights and higher security cost as Figure 11(1), but All-E strategy by degrees change much more advantageous to gain maximum benefits than other two strategies, as is shown by Figure 11(2)-(4). There is a much clearer change procedure after 6 time steps or so, and the implementation of enhanced security policy on every sharer is an optimal and stable strategy for a generic DRM ecosystem and its contents sharing scenario. It should be noted that the employment of dynamic security policy is fundamental under a specific contents value chain and DRM system, which is refined based on the introduction of the request-response of the active trusted computing devices/service prior to the remote attestation in a trusted computing-enabled user terminal platform.

V. Conclusion

In order to establish the multi-participant trust in DRM Ecosystem, a utility-analytic and non-cooperative game approach were proposed and formalized. And then, we made a series of Swarm-based simulation experiments on adoptions of typical security policies for such two general scenarios as contents acquisition and content sharing. We finally find out the optimal security policies profile(s), this is Nash Equilibrium, and their preconditions. Besides, the best content sharing mode as the modest sharing, not merely meet users' common requirements for flexible and convenient usages of copyrighted digital contents, and but enable contents provider to obtain the optimal benefits. Inspired by the idea of security risk management, our future work aims at the copyright infringement risk identification, evaluation and controlling in user's social network.

Acknowledgment

The authors thank Shuailei Fang for his assistance on Swarm simulation experiments, and anonymous reviewers for their detailed comments and suggestions. The work was sponsored by National Natural Science Foundation of China Grant No. 61003234 & No. 60803150, China Postdoctoral Science Foundation Grant No. 20100471611, Henan Province Key Technologies R & D Program Grant No. 092102210295, and Henan University of Science & Technology Young Scholar Fund Grant No. 2008QN010.

References

[1] K. M.Ak and A. A. Selcuk, "Optimal Subset-Difference Broadcast Encryption with Free Riders," *Information Sciences*, vol. 179, no. 20, 2009.

[2] S. Lian, "Secure Video Distribution Scheme Based on Partial Encryption," *International Journal of Imaging Systems and Technology*, vol. 19, no. 3, 2009.

[3] P. Wolf, M.Steinebach, and K. Diener, "Complementing DRM with digital watermarking: mark, search, retrieve," *Online Information Review*, vol. 31, no. 1, 2007.

[4] T. Thomas, S. Emmanuel, and e. a. A. V. Subramanyam, "Joint Watermarking Scheme for Multiparty Multilevel DRM Architecture," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 4, 2009.

[5] H. T. Poon, A. Miriand, and J. Y. Zhao, "An Improved Watermarking Technique for Multi-user, Multi-right Environments," *Multimedia Tools and Applications*, vol. 42, no. 2, 2009.

[6] A. Pretschner, M. Hilty, and e. a. F. Schtz, "Usage Control Enforcement: Present and Future," *IEEE Security & Privacy*, vol. 6, no. 4, 2008.

[7] "eXtensible rights Markup Language (XrML) 2.0 Specification," ContentGuard Incorporation, Nov. 2001.

[8] "Open Digital Rights Language (ODRL) version 1.1," http://www.w3.org/TR/odrl.

[9] "Information technology—Multimedia framework Part 5: Rights Expression Language," ISO/IEC 21000-5, 2004.

[10] P. Jamkhedkar, G. Heileman, and I. Ortiz, "The problem with Rights Expression Languages," in *Proceedings of 2006 ACM Workshop on Digital Rights Management*, Oct. 2006.

[11] "DRM Architecture Candidate Version 2.1," Open Mobile Alliance, July 2004.

[12] "DRM Specification Candidate Version 2.1," Open Mobile Alliance, July 2006.

[13] T. C. M. L. A. L. L. Company, "CMLA: Client adopter agreement. Revision," University of California, Berkeley, Technical Report V1.2-070326, Mar. 2007.

[14] A. Arnab, "Towards a general framework for Digital Rights Management," Ph.D. Dissertation, University of CAPE TOWN, Dec. 2008.

[15] Z. Zhang, Q. Pei, J. Ma, and L. Yang, "Establishing Multi-Party Trust Architecture for DRM by Using Game-Theoretic Analysis of Security Policies," *Chinese Journal of Electronics*, vol. 18, no. 3, 2009.

[16] "Agent- and Individual-based Modeling Resources," http://www.Swarm.org.

Zhiyong Zhang was born in Xinxiang city, Henan Province, P. R. of China, in Oct, 1975. He received his Master,Ph.D. degrees in computer science from Dalian University of Technology and Xidian University in 2003 and 2009, respectively.

He is currently an associate professor at Henan University of Science & Technology, China, and a post-doctoral fellowship at Xi'an Jiaotong University, China. Recent year, he has published over 30 scientific papers on the above research fields. His research interests include Digital Rights Management and multimedia contents protection, trusted computing and access control.

Dr. Zhang is a technical specialist of Digital Rights Management Workgroup Attached to China National Audio, Video, Multimedia System and Device Standardization Technologies Committee, as well as Membership for IEEE (2006)and ACM (2008), Senior Member of China Computer Federation (M04, S08). Besides, he is a Chair/Co-Chair for IAS 2009 Invited Session on Digital Rights Management, CIS 2009 Workshop on Digital Rights Management & Contents Protection, HPCS 2010 Special Session on Trusted Ubiquitous Networks & Multimedia Contents Protection, ICGEC 2010 Invited Session on Security and Trust in Ubiquitous Networks, MINES 2010 Special Session on Security, Privacy and Copyright in Multimedia Social Network, as well as TPC Member for numerous international conferences.

Xinliang Liu received his MS degree in computer science from Wuhan University of Technology, China, in 2004. He is currently an associate professor at Henan University of Science & Technology. His research interests include information system management and security.

Jiexin Pu is currently a professor in computer science at Henan University of Science & Technology, China. His current research interests include computational intelligence and security.