Fuzzy Risk Assessments on Security Policies for Digital Rights Management

Zhiyong Zhang [1,2]*; *Shiguo Lian* [3], *Qingqi Pei* [2], *Jiexin Pu* [1]

Abstract: In multimedia consuming, Digital Rights Management (DRM) is the important means to confirm the benefits of both digital contents/services providers and consumers. To keep the DRM system running in order, risk management should be adopted, which identifies and assesses the DRM system's security level. Now, the legitimate sharing of copyrighted digital content is still an open issue, which faces severe risks of propertied assets circumvention and copyright infringements. In this paper, we try to highlight a multi-disciplinary method for all-around examinations on risks to digital assets in the contents sharing scenario. The method is a qualitative and quantitative fuzzy risk assessment, which is used for estimating a novel concept called Risk-Controlled Utility (RCU) in DRM. Then, we emphasize on an application case of the emerging trusted computing policy, and analyze the influences of different content sharing modes. Finally, we address a business model with some simulation results. The comparison with other methods shows that the fusion of qualitative and quantitative styles can not only evaluate the RCU with uncertain risk events effectively, but also provide accurate assessment data for the security policies of DRM.

Key words: *Digital Rights Management; Risk Management; Fuzzy Risk Assessment; Security Policy; Trusted Computing; Qualitative and Quantitative Analysis*

Received: 2009, Jan
Revised and accepted: 2009, Jul

1. Introduction

The illicit copy, malicious dissemination and unauthorized usage of copyrighted digital contents have been still a common phenomenon, as the contents like the electric book, image, music, movie and application software are easily duplicated without deterioration in qualities. As a result, digital content industries would be heavily damaged, and even the value chain could also be interrupted. Digital Rights Management (DRM), which is an umbrella term involved in the multiple scientific

*Zhiyong Zhang
Electronic Information Engineering College, Henan University of Science and Technology[1], Chinese Ministry of Education Key Laboratory of Computer Network & Information Security, Xidian University[2], Human-Computer Interface Lab, France Telecom R&D[3], zhangzy@mail.haust.edu.cn

disciplines, for instance, information technology, economics and law [1], aims at resolving these above mentioned issues, and it covers the description, identification, trading, protecting, and tracking of all forms of usages over digital assets. In the last decade, an emphasis has been laid on the technical protections and restrictions by using the increasingly enhanced security policies/mechanisms. Besides, an emerging trend for the legitimate and flexible sharing of purchased contents is helpful to extend the content value chain and improving user experiences. However, copyrighted digital contents or assets are subject to complicated and severe risks of piracy and abuse in content sharing scenario, and digital content/services providers faced with these challenges should dedicate themselves to exploring on countermeasures as early as possible.

Risk management is an essential concept in the realm of finance and business, and allows business managers to balance operational and economic costs of protective measures and achieve benefits through protecting business processes that support business and enterprise objectives, even military missions [2]. Risk management is an integrated process used to identify, control, and minimize the impact of uncertain risky events, and is mainly made up of four distinct steps: risk analysis, risk assessment, risk mitigation, and risk control. The ultimate objective of the risk management program is to reduce the risk of performing some activities or functions to an acceptable level. In addition, recent attentions to information security breaches have led to an increased awareness of information security issues, and related security risk management is an effective approach to achieve the information assurance and to control risks to valuable assets and information systems in the case of the ubiquitous security vulnerabilities and hostile attacks [3]. Figure 1 depicts the security risk in a general *Sharers*' social network, in which the content sharing gives birth to the risks to copyrighted digital assets. And, these risks could be controlled by the security policies from *Providers*, which is composed of Content Provider (CP), Right Provider (RP) and Device Provider (DP). However, how to successfully assess these risks to copyrighted contents is still an unsolved issue for DRM nowadays.

In conducting the risk assessment, most of the considerations are should be given to the pros and cons of quantitative and qualitative assessments. The main advantage of the qualitative style of risk assessment is that it can prioritize different risks and resort to corresponding security actions. However, this kind of approach makes a cost–benefit analysis of risk controls more difficult. Differently, the quantitative risk assessment provides a measurement of the impacts' magnitude, as is suitable for the cost–benefit analysis. Since it depends on the numerical ranges used to express the measurement, the meaning of the quantitative risk assessment may be unclear, requiring the results to be interpreted in a qualitative manner [4]. In general, the decision of which to use should depend on what you are attempting to achieve. Nowadays, of the existing analytic styles, the qualitative data analysis enable us to keep the picture of risk as rich as possible for as long as possible. Therefore, risk assessment now tends to be moving toward the soft computing technology [5].

In this paper, we focus on the fuzzy risk assessments on the security policy for contents sharing scenario, and to our best knowledge, it is the first discussion on the risk evaluations in DRM. The main contribution of the paper is to employ the

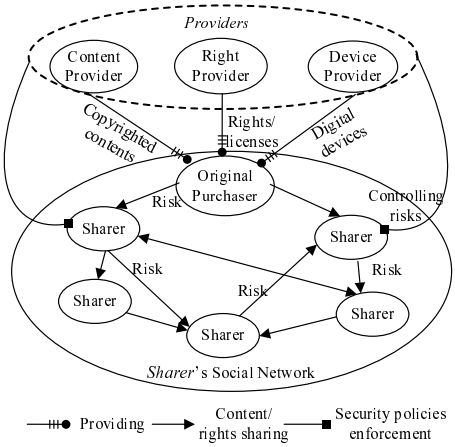

Fig. 1 *Security risks in a generic social network for content sharing*

risk management and multi-disciplinary method for all-around assessments on the risks in the contents sharing scenario, and further address a novel business model through analyzing the influences of consumers' sharing modes on risks to assets. The rest of the paper is organized as follows. Firstly, various content sharing schemes are reviewed in Section 2. Then, in Section 3, a systematic approach to fuzzy risk utility assessment is proposed based on qualitative and quantitative styles. The trusted computing-enabled security policy is analyzed in Section 4. In Section 5, some simulation experiments are given, and the related business models are analyzed. Finally, the conclusions are drawn, and future work is given in Section 6.

2. Related Works

In decades, DRM technologies focus on the contents and relevant copyrights protections, which are based mainly on cryptographic security and watermark technologies, as well as on the restricted usage that is accomplished by Rights Expression Language (REL) and Usage Control. However, owing to the inherent vulnerability of general-purpose devices, we need to pay much more attentions on the security risk management of digital assets and DRM systems, especially for the contents sharing scenario in question. From a technical perspective, Figure 2 indicates the security policies, risk management and multi-participant trust, which together underlie two typical application scenarios in DRM.

In order to realize the content sharing, the first step is to propose or extend a REL with the rights transfer/delegation functionality. To date, Open Mobile Alliance (OMA) has not formally specified syntax and semantics of these functions in OMA REL yet [6], as makes it difficult to unambiguously depict sharable permission, condition and constraint in a DRM system adopting OMA DRM Specs. Though other RELs, such as Open Digital Rights Language (ODRL) and eXten-

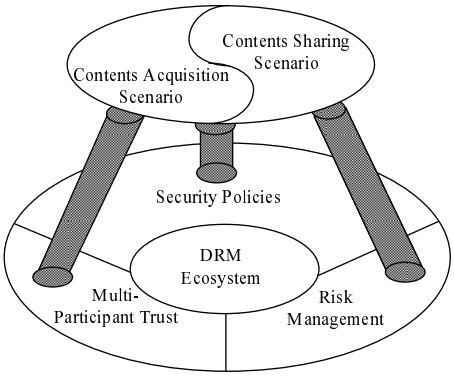

Fig. 2 *Security policies, risk management and multi-participant trust in DRM Ecosystem*

sible rights Markup Language (XrML), specify some transferable permissions of digital right, such as Sell, Lend, Give of ODRL [7], Delegation of XrML [8], these specifications of rights transferring are coarse-grained, and a fine-grained one is required in some business models. In combination with the remote attestation in the trusted computing, we [9] implemented the trusted distributions and enforcement of a fine-grained digital rights transfer policy. The new scheme is more advantageous than other relevant approaches in existence, as it did not restrict within the local domain environment, and accomplished the fine-grained rights transfer and contents sharing between users without direct participations of Rights Issuer and Local Domain Manager.

In addition, Rights Issuer (RI) generally distributes the usage permissions to a purchaser by binding of contents-license-device (or user), consequently results in a rigorously restriction of contents usage. Digital Video Broadcasting Project is an industry-led consortium, which was first to propose the concept "Authorized Domain" for sharing content at different rendering devices [10]. Subsequently, OMA DRM Specs [11] have adopted the concepts, and realized the uniform domain management of RI, including device's joining and leaving domain, registering and Rights Object (RO) acquisition from RI. The approach can implement content sharing within domain that is composed of different devices, but the increase of RI's burden becomes the bottleneck of the DRM system. An introduction of Domain Issuer in OMA DRM was proposed to manage a sharing domain that substitutes multiple Right Issuers with regard to a case that sharer could purchase contents from different providers and share them on different devices [12]. So, a Domain Manager was introduced in later version of OMA Specs. Nowadays, scenarios of content sharing are mainly involved in Home Network Domain [13] and Personal Entertainment Domain [14]. A secure domain architecture and the related protocols for DRM were proposed, which, however, did not support RO transferring and content sharing [15]. Kim et al. [13] improved this architecture for home domain, and the Local Domain Manager he proposed substitutes RI to accomplish license distribution for domain membership devices, meanwhile Delegated RO and Proxy

Certificate have realized rights delegation. This improved architecture is limited to home domain, and it is worthwhile to consider how content sharing based on rights transfer/delegation is achieved in wider domain.

Recent years have witnessed the application research on trusted computing technology in the field of DRM, which covers to trustworthily dissemination of license presenting usage policy, secure storage of contents and encryption key, and trusted execution of DRM Controller (i.e. DRM Agent) on the basis of several key techniques, such as remote attestation, seal approach and integrated trusted platform [16]. 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 relationships among participants in value chain. Nowadays, there exist several representative organizations, such as Trusted Computing Group (TCG), OpenTC in Europe and Chinese Trusted Computing Union, together with a series of Specs about trusted PC platform [17] and trusted mobile architecture [18], etc.

Besides, some several attempts to explore the multi-participant trust and benefit balance of DRM ecosystem have recently emerged. We [19, 20] made the systematic game-theoretic analysis with respect to the contents acquisition scenario, mainly referring to 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. To our best knowledge, it is the first game-theoretic discussion on the adoptions of typical security policies with different levels, including trusted computing-enabling enhanced policy, in DRM ecosystem. It should be noted that our done attempts are the base of the paper.

3. Qualitative and Quantitative Assessments on Risk-Controlled Utility of Security Policies

3.1 Risk-Controlled Utility of Security Policies

Through adopting proactive security policies, we gain the positive utilities and considerable benefits. The positive utility of security policies is categorized into two aspects: one is general utility, and the other is Risk-Controlled Utility (RCU). The former is the return of security investment, for instance, *Providers* acquires much more benefits owing to the increase of purchasing contents when providing consumers with enhanced security policies/mechanism, such as Java applications security and multi-factor user authentication in the contents transactions. And the latter denotes the expectancy positive utility that results from the adoptions of enhanced security policies controlling risks, and the expected risk utility is a potential benefit from *Providers*' perspective. In other words, if the occurrence rate of a security risk is little, or the severity factor of the risk is negligible, the risk utility is inconsiderable and the adoptions of corresponding security policies controlling the risk would be not cost-effective. So, RCU analysis is of significance for rational evaluations and adoptions of security policies.

In risk management, Annualized Loss Expectancy (ALE) [21] is common quantitative analysis tool used for computing an expected loss for an annual unit, and

in general it includes the following elements:

- Asset Value (AV) denotes a tangible or intangible worth of digital assets by using monetary or other styles.
- Annual Rate of Risk Occurrence (AR^2O) is a prediction of how often a specific risk event is likely to happen each year.
- Exposure Factor (EF) indicates the impact of risks on a target system.

3.2 A Quantitative and Qualitative Analytic Approach to RCU Fuzzy Assessment

Considering the rational decision-making on the adoptions of security policies for DRM in the paper, our ultimate goal is merely to prioritize these policies based on the RCU analysis. Therefore, we integrated qualitative approach with quantitative one to estimate the security risks to valuable digital contents owing to copyrights infringements and abuse, further acquiring the corresponding risk utility owing to the adoption of enhanced security polices in the scenario.

With regard to such a risk severity factor as user demands for contents in DRM ecosystem, we refined the definition of ALE for DRM, written by ALE^{DRM}, through the introduction to User Demand (UD) as Formula (1)

$$ALE^{DRM} = AV * ARRO * EF * UD \tag{1}$$

Further, we formally defined RCU, which is a positive utility at controlled risk, by

$$\begin{aligned} RCU &= ALE^{DRM}_{after\_risk} - ALE^{DRM}_{before\_risk} \\ &= AV * |\Delta ARRO| * |\Delta EF| * UD \end{aligned} \tag{2}$$

where $ALE^{DRM}_{after\_risk}$ and $ALE^{DRM}_{before\_risk}$ denote the ALE^{DRM} after and before risks that are controlled by enhanced security policies, respectively. Also, we depicted the variations of two parameters of AR^2O and EF, written by $\Delta ARRO$ and ΔEF, after controlling risks.

For main parameters of ALE^{DRM}, Asset Value is easily acquired and depicted by the monetary value of digital contents, AR^2O is calculated by Poisson Distribution of the annual risk occurrence, and EF is yielded through the quantitative and qualitative fuzzy analytic approach.

3.2.1 VaR based Calculation on Maximum AR^2O

Value at Risk (VaR) [22] is an essential calculation method for estimating the maximum risk values based on a confidence degree $(1-\alpha)$ in a given time period, and it was defined as

$$Prob(L \leq VaR) = 1 - \alpha \tag{3}$$

where L is an expected risk loss, VaR is the maximum loss, and α is determined by Providers' opinions on risks to a specific DRM ecosystem, that is,

$$\begin{cases} 0 \leq \alpha < 0.5 & \text{Risk-averse Providers} \\ \alpha = 0.5 & \text{Risk-neutral Providers} \\ 0.5 < \alpha \leq 1 & \text{Risk-seeking Providers} \end{cases} \tag{4}$$

Taking it into consideration that the Poisson Distribution is a common probability function depicting the likelihood of random events occurrence, we attempted to employ the Poisson Distribution and VaR to calculate the AR^2O, that is an estimation on the maximum occurrence rate of a random copyrights infringement/illicit usage event CI. Thus, the maximum of CI occurrences, denoted by n_{CI}, is in line with Poisson Distribution with the parameter λ. And then, by using

$$Prob(x \leq n_{CI}) = 1 - \alpha \tag{5}$$

we can calculate n_{CI} in the given confidence α.

3.2.2 Fuzzy Assessments on EF and UD by using Triangular Fuzzy Number

With respect to two fundamental parameters EF and UD, we adopt the triangular fuzzy number-based subjection function to estimate these factors influencing RCU of *Providers*.

Definition 1 (Subjection Function) for any assessment target/factor $x \in X$, when the map function $x \rightarrow \varsigma_{si}(x) \in [0,1]$ hold, $\varsigma_{si}(.)$ is the subjection function and the resultant triple $(x, \varsigma_{s1}(x), \varsigma_{s2}(x), ..., \varsigma_{sn}(x))$ denotes Subjection Degree (SD) of x on every assessment scale $si(i = 1, 2, ..., n)$.

According to Definition 1, the triangular fuzzy number-based subjection function was piecewise defined as Formula (6) - (8). Here, if $1 < i < n$, Formula (6) holds:

$$\varsigma_{si}(x_{fi}^j) = \begin{cases} (s_{i-1} - x_{fi}^j)/(s_{i-1} - s_i) & s_i \leq x_{fi}^j \leq s_{i-1} \\ 1 & x_{fi}^j = s_i \\ (x_{fi}^j - s_{i+1})/(s_i - s_{i+1}) & s_{i+1} \leq x_{fi}^j \leq s_i \\ 0 & x_{fi}^j \geq s_{i-1}, x_{fi}^j \leq s_{i+1} \end{cases} \tag{6}$$

Besides, when$i = 1$, we obtained Formula (7)

$$\varsigma_{si}(x_{fi}^j) = \begin{cases} 1 & x_{fi}^j \geq s_i \\ (x_{fi}^j - s_{i+1})/(s_i - s_{i+1}) & s_{i+1} \leq x_{fi}^j \leq s_i \\ 0 & x_{fi}^j \leq s_{i+1} \end{cases} \tag{7}$$

And then, when $i = n$, the following Formula (8) yielded:

$$\varsigma_{si}(x_{fi}^j) = \begin{cases} 0 & x_{fi}^j \geq s_{i-1} \\ (s_{i-1} - x_{fi}^j)/(s_{i-1} - s_i) & s_{i+1} \leq x_{fi}^j \leq s_i \\ 1 & x_{fi}^j \leq s_i \end{cases} \tag{8}$$

where x_{ft}^j is the assessment score of the factor $f_t(t = 1, 2, ..., q)$ from jth judge $(j = 1, 2, ..., J)$. It should be noted that there exists a kind of an assessment target with the single factor under some circumstances, i.e. $i = 1$, we gained the subjection degree vector as

$$SD = (\varsigma_{s1}(x), \varsigma_{s2}(x), ..., \varsigma_{sn}(x)) \tag{9}$$

However, if $i > 1$, as is a multi-factor fuzzy assessment, for any factor $f_t$and any assessment scale s_i, the subjection degree is calculated as

$$\varsigma_{si}(x_{ft}) = (\sum_{k=1}^{J} \varsigma_{si}(x_{ft}^{k}))/J \tag{10}$$

where $i = 1, 2, ..., n$ and $t = 1, 2, ..., q$.

Finally, the final subjected degree vector of the multi-factor assessment target is obtained by

$$\begin{aligned} SD &= (\varsigma_{s1}(x), \varsigma_{s2}(x), ..., \varsigma_{sn}(x)) \\ &= (w_{f1}, w_{f2}, ..., w_{fq}) * \begin{bmatrix} \varsigma_{s1}(x_{f1}), \varsigma_{s2}(x_{f1}), ..., \varsigma_{sn}(x_{f1}) \\ \varsigma_{s1}(x_{f2}), \varsigma_{s2}(x_{f2}), ..., \varsigma_{sn}(x_{f2}) \\ ..... \\ \varsigma_{s1}(x_{fq}), \varsigma_{s2}(x_{fq}), ..., \varsigma_{sn}(x_{fq}) \end{bmatrix} \end{aligned} \tag{11}$$

where w_{fi} is the normalized weight of the factor f_t, and it could be empirically given or calculated by FAHP(Fuzzy Analytic Hierarchy Process), as is out of the scope of the paper.

4. Trusted Computing-Enabling Security Policy and RCU Analysis

The emerging Trusted Computing (TC) aims to improve the security and trustworthiness of a general-purpose commodity devices held by end users, such as PC and Server. Therefore, TC-enabling enhanced security policies are suitable for DRM and copyrights content sharing. For this case, we present the related security policies, propose the risk-controlled positive utility, and analyze the influence of different sharing modes in the following content.

4.1 Typical Security Policies of Participants

Here, two kinds of typical security policies for both *Provider* and *Sharer* are considered. One is the general security policy that meets fundamental security requirements of DRM system, and the other is the trusted computing-enabling enhanced security policy, which provides participants much more security protections.

For *Provider*, the general security denotes that CP implements basic cryptographic protection of digital contents, RP accomplishes the secure dissemination of license related to a certain contents, and DP provides a common device or sharer electronics for *Sharer*. The acquired benefits of adoptions of security policies for two participants are written as $u_{Providers}^{baseline}$ and $u_{Consumer}^{baseline}$, respectively. The enhanced security policy for *Provider* means a realization of higher security of contents and cipher key packaged by CP, as well as the trusted distribution of RO created by RP based on remote attestation technology and trusted computing-enabling device platform provided by DP.

Device Attestation (DA) could implement the validation functionality on the system bootstrap and run-time's integrity of user terminal device and such key

component as DRM Controller. Therefore, it enables RP to ensure that an issued license will be trustworthily interpreted and executed. These factors would lead to the acquirement of positive utility $u^{PoDA}_{Providers}$. Moreover, the Content Encrypted Key could be also well protected by TPM (Trusted Platform Module) that is a chip welded on the motherboard of trusted device, and DP would acquire the benefit $u^{PoTC}_{Providers}$ from users' purchase of the kind of devices. The other side of a coin, the activeness of DA also directly increases overhead of DRM system, together with a transactional delay. These session-level impact-factors were denoted by $f^{CoDA}_{Providers}$ as a whole, with a corresponding utility being $u^{CoDA}_{Providers}$.

For *Sharer*, a general security policy (G-Strategy) or enhanced security policy (E-strategy) denotes the purchase and usage of common or trusted computing-enabling device/sharer electronics. The adoption of the latter device could implement enhanced security of DRM application and safeguard sharers' confidential and sensitive personal information from malicious collecting and disseminating.

When a sharer adopts trusted computing device, there are also positive and negative factors in a DA session, which were denoted by f^{PoDA}_{Sharer} and f^{CoDA}_{Sharer}, with corresponding utilities being u^{PoDA}_{Sharer} and u^{CoDA}_{Sharer}. Besides, u^{CoTC}_{Sharer} denotes the cost of purchasing the higher security device.

With regard to these factors above mentioned, we merely need to quantitatively analyze RCU of $u^{PoDA}_{Providers}$, when deploying trusted computing-enabling security policies. And, other factors could be evaluated by the scale-based qualitative approach or concrete monetary values.

4.2 Positive Utility of TC-Enabling Security Policy and Application Case

The aspects of the TC enhanced security superior to the general security policy were listed as follows:

- Assuring the integrity of DRM key components, which are located at such as general-purpose user devices as various PCs/Servers, or some special-purpose consumer electronics as Smart Phones and PDAs, based on TC-enabling front-end user devices and remote attestation schemes.
- Restricting the concrete type of and patch edition of DRM-contents rendering applications by using the enhanced security methods for the device integrity attestation.
- Protecting the cryptographic keys, such as Content Encryption Key (CEK) and the private key of devices, and related certificates from disclosing and circumventing, so that implement propertied contents protections.
- Keeping the tamper-proof closed environment and trusted I/O in combination with a trusted chip module, for example Trusted Platform Module (TPM) or Trusted Cryptography Module (TCM), and upper-layer Trusted Software Stack (TSS).

According to the essential functionality of TC enhanced security, its RCU can be calculated by $ALE^{DRM}$and the fuzzy analytic approach in Section 3.2. The

following case is an application of the proposed risk utility to TC-enabling security policy for DRM.

In this case, the DRM application has the specific annual occurrence rate of copyrights infringements threat to a target DRM system, as is compliant to Poisson Distribution with λ being equal to 5 in the case of adoptions of general security devices, and with λ being equal to 1.1 in the case of adoptions of TC enhanced security devices. So, the following formula holds in term of Poisson Distribution:

$$\begin{cases} Prob(x=k) = \dfrac{e^{-5}5^k}{k!}, & k=0,1,2,..., \text{General security policy} \\ Prob(x=k) = \dfrac{e^{-1.1}1.1^k}{k!}, & k=0,1,2,..., \text{Enhanced security policy} \end{cases} \tag{12}$$

Here, suppose that Provider is a risk-averse, and let α be equal to 0.03. And then, when $Prob(x \leq n_{CI})$ is equal to 0.97, we gained n_{CI} for two kinds of security policies:

$$\begin{cases} n_{CI} = 11, & \lambda = 5, \text{ General security policy} \\ n_{CI} = 5, & \lambda = 1.1, \text{ Enhanced security policy} \end{cases}$$

Obviously, the maximum of AR^2O decreases with the reduction ofλthat denotes the average AR^2O of random risky events.

With respect to fuzzy assessments of UD and EF, there were 8 judges participating in the risk utility assessments. In the case, we firstly presented the assessment scale and corresponding semantics of UD and EF, which is shown by Table 1. And then, a group of assessment values for parameters UD and EF were given in Table 2.

Level	Scale	UD Description	EF Description
1	90	Strong	High
2	70	Medium to Strong	Medium to High
3	50	Medium	Medium
4	30	Weak to Medium	Low to Medium
5	10	Weak	Low

Tab. I *Five-level scale descriptions of main utility-influencing factors*

According to the fuzzy assessment method presented in Section 3.2.2, UD and EF were calculated as follows:

As UD is a single-factor assessment participated by 8 reviewers, Formula (10) was deduced into $\varsigma_{si}(x) = (\sum_{k=1}^{8} \varsigma_{si}(x^k))/8, si \in \{90, 70, 50, 30, 10\}$. And then, the subjection degree vector of UD is $SD_{UD} = (0.2, 0.288, 0.213, 0.119, 0.125)$. In term of the principle for the maximum subjection degree, the optimal SD is 0.288, and UD is 70.

In similar way, the subjection degree vector of EF was yielded. Here, note that EF is a multi-factor fuzzy assessment procedure, and the final value of SD

Target/Factor(s)	Assessment Scores								Weights
	J_1	J_2	J_3	J_4	J_5	J_6	J_7	J_8	
UD	70	51	8	82	94	42	67	39	-
Controller	92	95	90	89	90	85	80	88	0.4
Application	82	87	90	75	78	94	88	92	0.3
Cipher Key	98	95	90	88	86	88	93	84	0.2
Platform	80	70	87	91	97	90	86	88	0.1
Generic Device	40	50	42	35	39	20	28	10	-

Tab. II *Subjective and qualitative assessments by using a worksheet*

should consider four factors' weights, which are shown in Table 2. Thus, we gained $SD_{EF\_TC} = (0.839, 0.215, 0, 0, 0)$, with EF_TC being equal to 90. Besides, with respect to adoptions general security devices, we obtain $SD_{EF\_GS} = (0, 0, 0.225, 0.45, 0.2)$ and $EF\_GS = 30$.

Finally, according to Formula (2), we further obtained $u^{PoDA}_{Providers} = RCU_{PoDA} = 252000$.

4.3 Sharing Modes and Maximum Benefits of Contents Provider

A content sharing tree among original purchaser and sharers is illustrated by Fig. 3, where a predefined w denotes the width of the tree, with a goal to restrict the user number of contents sharing for a sharer, the triple (al, m, n) presents the purchased/acquired sharing rights, as well as shareable rights when the enhanced or general security policy is adopted. Here we suppose that rights are averagely shared in accordance with present tree width, and any sharer only consumes one right. Besides, let d be the height of the tree.

In the content sharing tree, the dynamic width of every subtree embodies various sharing modes among users, for instance, the partial sharing, modest sharing and extensive sharing. In this section, we take it into account that different sharing modes have significant influences on such some aspects as the overhead of copyrights infringements track, denoted by C_T, and the loss C_L of risks resulted from security breaches based on the above analysis.

Typically, the following two content sharing trees are considered, which are illustrated by Fig. 4 and Fig. 5, respectively. In Fig. 4, an original purchaser shares his/her digital rights to a large number of other sharing users, i.e. $W_E = n = l_i - 1$, and the case belongs to a typical extensive sharing mode. In the scenario, if these exists an illegal sharer, the average overhead of the corresponding investigation on illicit actions is merely equal to 1 with respect to a premise that the path length from a root node (original purchaser) to the target node (malicious user) denotes the cost of the piracy tracking from CP/RP. Obviously, this an extreme instance. However, the total loss resulted from copyrighted contents circumventions and abuses would be considerable, as the number of sharers' adoptions of general security devices is max. In contrast with the extensive sharing, Fig. 5 depicts an extreme scenario of the partial sharing mode, and here every sharer acquires only

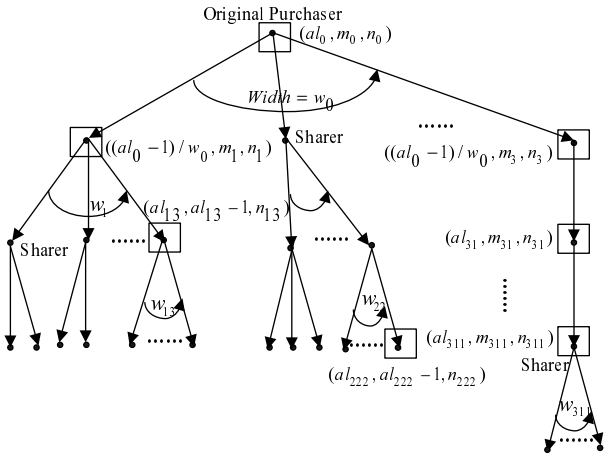

Fig. 3 *Contents sharing tree with dynamic widths*

one of digital rights, with W_P being equal to 1. So, the average cost of piracy tracks would significantly increase to a maximum, with being equal to $(n+1) * n/2$, but the copyrights infringements loss is fewer than the extensive sharing mode, only being $(n - i + 1) * loss_G$, where $loss_G$ denotes the loss yielded by the choice of general terminal devices.

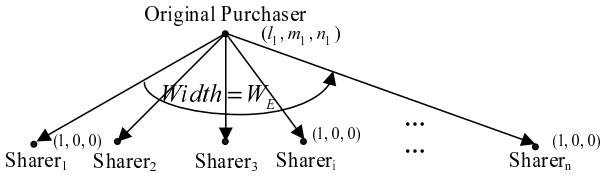

Fig. 4 *An extreme case of extensive sharing mode*

In addition, based on game-theoretic utility analysis in [20], the total RCU of Provider is presented as

$$TotalRiskUtility = (\sum_{i=1}^{n} payoff_i(sp_{Providers}, sp_{Sharer})) - C_T - C_L \qquad (13)$$

where i denotes a group of content sharing transactions from an identical original sharer, and it is also a subtree in the generic content sharing tree. In addition, C_T and C_L are calculated by Formula (14) and Formula (15) as follows:

$$C_T = O_i * averagePath \qquad (14)$$

where O_i denotes the overhead of investigating $Sharer_i$ for any step in the content sharing tree as Fig. 3, and $averagePath$ depicts the average steps of finding any

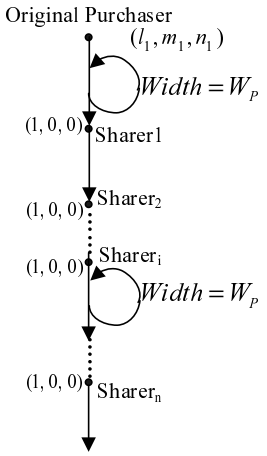

Fig. 5 *An extreme case of partial sharing mode*

tree node as $Sharer_i$.

$$C_L = ALE_G * N_G \tag{15}$$

where $ALE_G$and N_G is the annual loss expectancy when adopting generic devices and the number of *Sharer* holding the sort of devices.

Due to the direct impact of the tree width on three aspects as $payoff_i(sp_{Providers}, sp_{Sharer})$, C_T and C_L, *Providers*' goals are to find out the optimal sharing mode by which the sum of C_T and C_L is minimum, and to further gain a maximum total risk-controlled utility.

5. Simulation Experiments and Related Discussions

5.1 SWARM-based Simulation Experiments

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 [23]. The object-oriented programming capability and versatile tool kits were developed, and have been successfully applied to intelligent system controls and processes in the realm of artificial intelligent, economics simulation and multi-participant game, etc.

We employed Swarm 2.2 for Java and MyEclipse 6.5 to made a series of experiments on multiple rational agents (RAs), which are categorized into two kinds of $RA_{Providers}$ and RA_{Sharer}, and their rational decision-making on adoptions of security policies based on a dynamic and mixed game. In these experiments, there exist 16 $RA_{Providers}$ and 6400 RA_{Sharer}, together with three kinds of contents sharing styles, as are defined as follows: PSM (Partial Sharing Mode) manifests that the width of every subtree is not exceed to 3, the tree width of MSM (Modest

Sharing Mode) is a random integer from 4 to 10, and one of ESM (Extensive Sharing Mode) is less than and equal to 20. Besides, there are assumptions that every $RA_{Providers}$ adopts the dynamic strategy, that is to say compliances to sharers' security policies, and chooses PSM in the preliminary stage of the simulation.

In the experiment, four groups of utility and weight values were listed in Table 3, where initial values of all parameters besides $f^{PoDA}_{Providers}$ were qualitatively given based on the scale of 100. As the only enhanced security policy was considered without the demand for prioritizing utilities of different policies in the paper, we normalized $u^{PoDA}_{Providers}$ as an integer 25. Here, these given utility and weight values depict different application circumstances, for instance, the increases or reductions of some factors' utilities and weights would occur with security costs and overheads decreasing. Besides, assume that the number of original purchased rights is 41, with O_i and ALE_G being equal to 5.

Participant	$\mathrm{RA}_{Providers}$			RA_{Sharer}		
factor	$f^{PoDA}_{Providers}$	$f^{CoDA}_{Providers}$	$f^{PoTC}_{Providers}$	f^{PoDA}_{Sharer}	f^{CoDA}_{Sharer}	f^{CoTC}_{Sharer}
(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)

Tab. III *Four groups of initialized values of main parameters*

For any time step and any $RA_{Providers}$ in the Swarm simulation, its maximum benefits are calculated aiming at three sharing modes in term of Formula (13)-(15), respectively, so that the optimal sharing mode is obtained. The change curves of the number of *Providers* adopting three sharing modes yield with the time steps, as illustrated by Fig. 6 - Fig. 9, where the quantity of purchased digital rights/licenses increases step by step.

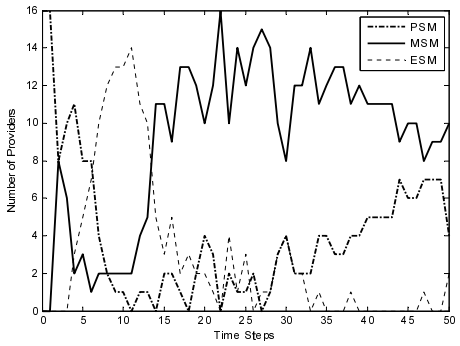

Fig. 6 *The change curve of number of Providers for Group 1# data*

From the simulation results in Fig. 6 - Fig. 9, it is found that MSM, under

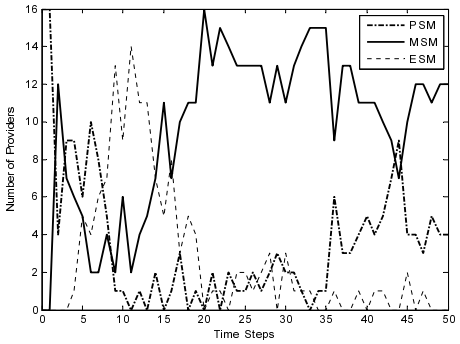

Fig. 7 *The change curve of number of Providers for Group 2# data*

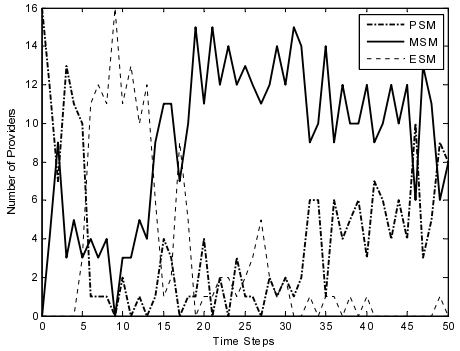

Fig. 8 *The change curve of number of Providers for Group 3# data*

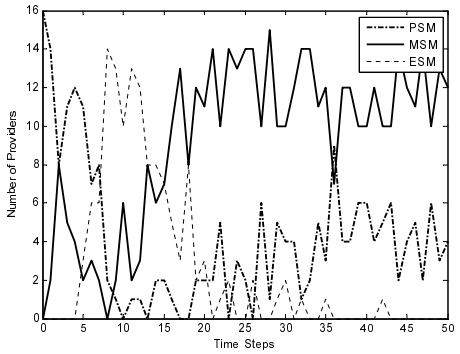

Fig. 9 *The change curve of number of Providers for Group 4# data*

different application circumstances, is obviously dominant over PSM and ESM step by step, that is to say that RA_{Sharer}'s adoptions of the modest sharing enables

$RA_{Providers}$ to acquire the maximum benefit in contents sharing scenario. Besides, note that ESM is a dominated mode than other two modes, and does not give birth to the optimal benefit for $RA_{Providers}$. The reason is that the extensive sharing enables much more sharers who only gain fewer shared rights to adopt the general security devices, and enhanced security policy controlling over risks to copyrighted contents has no influence on these sharers, thus directly resulting in significant risky losses and higher overheads used for copyright infringements tracking unauthorized usages and copyrights infringement. Further, for TC-enabling security policies, if they could successfully act on a majority of sharers, as is not to date a feasible scheme, it is possible that ESM becomes an optimal sharing style.

5.2 Related Discussions and Novel Business Model

The simulation experiment integrating the fuzzy risk assessment data concludes the dominant and dominated content sharing modes, and our approach is in essence different from the security risk assessment schemes available. A quantitative assessment methodology is proposed based on the monetary value of expected and unexpected losses due to security risk [24], but the approach including Expected Loss (EL) and VaR can not effectively evaluate risk utility of enhanced security policies. References [25, 26, 27] mainly focus on the specific cases, for instance the information system with all forms of critical data, a prototype supporting the National Institute of Standards and Technology (NIST) risk management standard, and an International Consequence Analysis Framework used for Intellectual Property theft. Besides, in order to find the structural origin of security risks in information systems, a conceptual modeling method for performing means-end analysis [28] and a framework incorporating the security policy pre-evaluation and enforcements [29] were addressed, and these emphasize some novel and comprehensive risk evaluation procedure. A mathematical model was represented based on the fuzzy set theory [30], in order to quantify the security characteristics of systems, but the model lacks the capability of risk utility analysis and estimation.

The fuzzy risk assessment on the enhanced security policy and a series of simulation experiments on the optimal choice of the content sharing mode show that the sharing style is an essential factor influencing the decision-making on the risk-controlling strategy, in a prerequisite that purchased digital rights of an original purchaser is given and each of sharers only consumes a specific quantity of digital rights/services. Therefore, these fuzzy risk assessments and game-theoretic decision-making on adoptions of security policies [19, 20] are integrated into the business model establishment and risk controlling process for the above mentioned content sharing tree, as shown by Fig. 10.

The process mainly includes some user considerations, the optimal adoption of contents sharing modes, security policies specifications and deployments, which are represented in detail as follows:

- A digital contents/services vendor should take the number of sharers adopting the generic security devices into consideration, and the inconsiderate investment on and deployment of enhanced security policies on every sharer is not cost-effective and optimal, as a certain quantity of sharers could access to

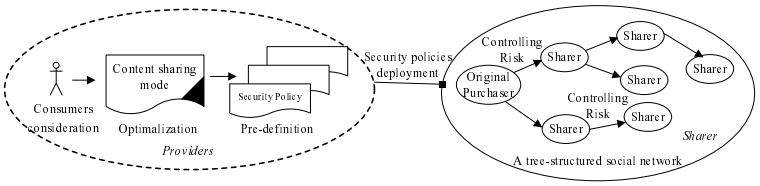

Fig. 10 *Business model establishment and risk controlling process*

shared contents in a generic devices or open terminal platform due to the limited the sharable digital rights and high cost of enhanced security devices.

- Based on the dynamic security policy, the contents provider can restrict and adopt the modest sharing style as a common model for the propertied contents sharing among consumers, who constitute a sort of social network, and users can share purchased contents/licenses with their relatives, friends or colleagues.

- The contents/services provider can enable intended shares to choose enhance security devices through effectively restricting the number of shareable digital rights in the case of users' adoptions of a general device. Thus, the devices vendors could acquire the increasing benefits by purveying the enhanced security devices.

- In the combination with the business model, contents/services providers implement and deploy the security policies so as to protect the digital contents/assets against illegally copying, abusing and disseminating in the whole life cycle of contents transaction, usage and sharing, and meanwhile to acquire considerable benefits.

6. Conclusions and Future Work

In the paper, we attempt to make a fuzzy assessment on a risk-controlled utility with regard to adoptions of enhanced security policies for DRM, and had an exploration on content sharing scenario oriented risk managements and total utility influences of different sharing modes. Our simulation experiments show that the modest sharing mode is dominant than other two modes, and is advantageous for contents/services providers to acquire the maximum benefit in combination with the proposed business model. Considering a generic social network composed of sharers, it is maybe depicted not merely as a simplified tree structure, but a directed graph in contents sharing scenario. Therefore, our future work is to have an in-depth examination on a cost-effective security strategy so as to control and mitigate risks of copyrighted contents piracy and abuse in the social network.

Acknowledgement

The authors want to thank Prof. Yinghua Min (IEEE Fellow), from Institute of Computing Technology, Chinese Academy of Sciences, for his valuable suggestions on Game Theory. Also, the special thanks are given to anonymous reviewers for their valuable comments and suggestions. The work was sponsored by National Natural Science Foundation of China Grant No.60803150 and No.60633020, China National 111 Program of Introducing Talents of Discipline to Universities Grant No.B08038.

References

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

[2] Buckshaw D., Pamell G., and Unkenholz W.: Mission Oriented Risk and Design Analysis of Critical Information Systems, Military Operations Research, vol.10, no.2, 2005, pp.19-38.

[3] Evans S., and Wallner J.: Risk-based Security Engineering through the Eyes of the Adversary, In: Proceedings of the 2005 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 2005, pp. 158-165.

[4] Peltier T.: Information Security Risk Analysis 2^{nd} edition, Auerbach Publications, New York, 2005.

[5] Jones A., and Ashenden D.: Risk Management for Computer Security, Elsevier Inc Press, 2005.

[6] DRM Rights Expression Language Candidate Version 2.1. Open Mobile Alliance, Jul, 2007.

[7] Pucella R., and Weissman.V.: A formal foundation for ODRL, In: Proceedings of Workshop on Issues in the Theory of Security, 2004.

[8] Halpern J., and Weissman V.: A formal foundation for XrML, Journal of the ACM, vol. 55, no.1, 2008, pp.4-45.

[9] Zhang Z., Pei Q., Ma J., Yang L. and Fan K.: A Fine-grained Digital Rights Transfer Policy and Trusted Distribution and Enforcement, In: Proceedings of International Conference of Computational Intelligence and Security, IEEE Computer Society Press, Suzhou, China, Dec, 2008.

[10] Hibbert C.: 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.

[11] DRM Architecture Candidate Version 2.1.Open Mobile Alliance, Jul, 2007.

[12] Koster P., Montaner J., Koraichi N., and Iacob S.: Introduction of the domain issuer in OMA DRM, In: Proceedings of 2007 4th Annual IEEE Consumer Communications and Networking Conference, Las Vegas, NV, United States, 2007, pp.940-944.

[13] KIM H., Lee Y., Chung B., Yoon H., Lee J., and Jung K.: Digital Rights Management with right delegation for home networks, In: Proceedings of 9th International Conference on Information Security and Cryptology, M.S. Rhee and B. Lee (Eds.): LNCS 4296, 2006, pp.233-245.

[14] Koster P., Kamperman F., Lenoir P., and Vrielink K.: Identity-based DRM: personal entertainment domain, In: Proceeding of Transactions on Data Hiding and Multimedia Security, LNCS 4300, 2006, pp.104-122.

[15] Popescu, B. Crispo B., Tanenbaum A., and Kamperman F.: A DRM security architecture for home networks, In: Proceedings of 4th ACM Workshop on Digital Rights Management, Oct, 2004.

[16] Cooper A., and Martin A.: Towards an Open, Trusted Digital Rights Management Platform, In: Proceedings of 2006 ACM Workshop on Digital Rights Management. Alexandria, Virginia, USA, Oct, 2006.

[17] TCG PC Specific Implementation Specification Version 1.1, https://www.trusted computinggroup.org/specs/PCClient, Aug, 2003.

[18] TCG Mobile Reference Architecture Specification Version 1.0, https://www.trusted computinggroup.org/specs/mobilephone, Jun, 2008.

[19] Zhang Z., Pei Q., Ma J., Yang L. and Fan K.: Cooperative and Non-Cooperative Game-Theoretic Analyses of Adoptions of Security Policies for DRM, In: 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, U.S.A., Jan, 2009.

[20] Zhang Z., Pei Q., Ma J. and Yang L.: Establishing Multi-Party Trust Architecture for DRM by Using Game-Theoretic Analysis of Security Policies, Chinese Journal of Electronics, vol.18, no.3, 2009, pp.519-524.

[21] Landoll D.: The Security Risk Assessment Handbook, Auerbach Publications, New York, 2006.

[22] Dempster M.A.H.: Risk Management: Value At Risk and Beyond, Cambridge University Press, United Kingdom, 2002.

[23] Swarm Development Group. http://www.swarm.org

[24] Harmantzis, F., and Malek M.: Security risk analysis and evaluation, In: Proc. of 2004 IEEE International Conference on Communications, Paris, France, 2004, pp. 1897-1901, .

[25] Bernard R.: Information Lifecycle Security Risk Assessment: A tool for closing security gaps, Computers and Security, vol.26, no.1, 2007, pp. 26-30.

[26] Ekelhart A., Fenz S., and Neubauer T.: AURUM: A framework for information security risk management, In: Proc. of the 42nd Annual Hawaii International Conference on System Sciences, Waikoloa, HI, United states, 2009.

[27] Andrijcic E., and Horowitz B.: A macro-economic framework for evaluation of cyber security risks related to protection of intellectual property, Risk Analysis, vol. 26, no.4, 2006, pp. 907-923.

[28] Misra S., Kumar, V., and Kumar U.: A strategic modeling technique for information security risk assessment, Information Management and Computer Security, vol. 15, no.1, 2007, pp. 64-77.

[29] Yi H., Hori Y., and Sakurai K.: Security policy pre-evaluation towards risk analysis, In: Proc. of the 2nd International Conference on Information Security and Assurance, pp. 415-420, Busan, Korea, 2008.

[30] Halkidis S., Chatzigeorgiou A., and Stephanides G.: Quantitative evaluation of systems with security patterns using a fuzzy approach, Lecture Notes in Computer Science, vol. 4277, 2006, pp. 554-564.