Fuzzy Utility-Factor Assessments and Swarm Simulations on DRM Security Policies

Zhiyong Zhang, Jiexin Pu, Qingtao Wu, Lili Zhang, Danmei Niu
Electronics Information Engineering College,
Henan University of Science and Technology
Luoyang, P. R. of China
Email: {zhangzy, pjx}@mail.haust.edu.cn

***Abstract*—In recent decade, DRM (Digital Rights Management) has focused on security techniques for solving the issues as the malicious copy, free dissemination and unrestricted abuse of digital contents or assets. Whereas some increasingly enhanced security policies, which were implemented at contents provider-side or user-side, have not brought about optimal utilities for participants in the contents value chain. An analytic hierarchy structure and its algorithm on the assessment on utility factors' weights for DRM security policies were proposed based on Fuzzy Analytic Hierarchy Process, and then Swarm simulation experiments were further made on the adoptions of typical security policies in combination with the gained weight values. The simulation results show the proposed approach to fuzzy assessments effectively implements rational and optimal decision-making on security policies combinations.**

***Keywords*-Digital Rights Management; Fuzzy Analytic Hierarchy Process; Decision Theory; Security Policy; Swarm Simulation**

I. Introduction

In order to positively protect Intellectual Property and realize the legitimate and controlled usage on digital contents or assets, DRM has become a focus for the society as a whole, where the contents industry, academic realms, governments and even some civil liberty are involved in. Generally, DRM is an umbrella term involved both in business realizations of the contents industry and in valuable explorations on multiple scientific disciplines, for instance, information technology, economics and law [1]. Besides, recently Mobile DRM technology, which is oriented by a mobile network application scenario, has been paying more attention to the effective protection of digital contents in the whole life cycle for the mobile network environment. In North America and European Union, DRM-protected mobile contents service is listed among the four kinds of DRM killer application.

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 [2][3] and the contents usage permission that is accomplished by Rights Expression Language [4][5][6] and Usage Control [7][8], as well as on the digital watermark technology used for prosecuting pirate [9]. 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. Whereas we proposed the security-utility and game-theoretical analyses for DRM security policies from DRM-enabling contents value chain's perspective [10][11]. The main contribution of the paper focus on two aspects, one is to an effective analysis on utility-factors' weights based on Fuzzy Analytic Hierarchy Process (FAHP), and other is to further make Swarm simulation experiments on three-participant game in term of acquired factors' weights and security utilities.

II. Fuzzy Utility-Factor Assessment

A. Hierarchy Process Structure for DRM Security Policies

Analytic Hierarchy Process (AHP) is a systematic approach, by using the combination of quantitative and qualitative analyses, to make effective decisions on an object issue with a large-scale assessment factors. By virtue of making comparisons and normalized analyses on the mutual importance degree between any two factors, theses factors' weights and an optimal scheme are yielded from a group of optional strategies. But, when the number of object factors is considerable, the verification of the consistency of the judgement matrix has a high computational complexity for a general AHP as the inconsistent matrix need to repeatedly adjust and identify. To solve this issue, recent years have witnessed Fuzzy AHP based on the integrated fuzzy assessment methods. And it enables the computation of factors' weights much more compatible to a generic thinking process of human beings, meanwhile improving the correctness and rationality of quantitative and qualitative analyses by the marriage of the fuzzy estimation and AHP [12][13].

In term of multi-layer structure of AHP, We proposed a DRM-oriented four-layer one defined by Security Object-Policy-Component/Service-Influencing Factor, which is shown by Figure 1. Here, the top security goal is to safeguard the digital contents against illegally copying, spreading and abusing, as is the realization of DRM fundamental functionality. To realize the goal, there is a set of security policies for any participant in DRM ecosystem, moreover anyone of policies is composed of one or more Security Components (SC)/Security Services (SS) used for implementing the concrete security functions. Besides, the

978-0-7695-3906-5/09 $26.00 © 2009 IEEE
DOI 10.1109/ICCCS.2009.23

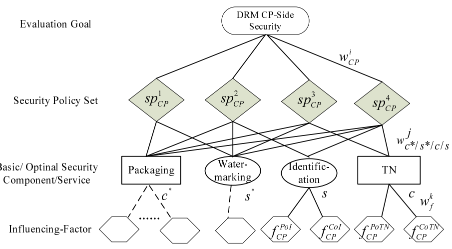

Figure 1. Analytic Hierarchy Structure for DRM Security Policies

bottom presents a serious of factor influencing the SC/SS' or OSC (Optional SC)/OSS (Optional SS)' utilities and these factors' weighs. The weights of the security policy, sc/sc and factor are written by $w^i_{CP} w^j_{c^*/s^*/c/s}$ and w^k_f, respectively.

B. FAHP-Based Fuzzy Assessment on Factors' Weights

Definition 1 [12] A set of target factors as $F = \{f_1, f_2, ..., f_n\}$ is given. If the matrix $R = (r_{ij})_{n*n}$ satisfies the following conditions: (1)$0 \leq r_{ij} \leq 1, (i = 1, 2, ..., n, j = 1, 2, ..., n)$, (2)$r_{ii} = 0.5$, (3)$r_{ij} + r_{ji} = 1$, then R is called by fuzzy complementary judgement matrix, where r_{ij} denotes the importance subjection degree of f_i superior to f_j, i.e., the greater r_{ij} is, the much more importance of f_i by comparisons with f_j. Obviously, when $r_{ij} = 0.5$, two factors are coequal.

Theorem 1 [12][13] If a fuzzy complementary judgement matrix $R = (r_{ij})_{n*n}$, for $\forall i, j, k = 1, 2, ..., n$, the equation $r_{ij} = r_{ik} - r_{jk} + 0.5$ holds, then R is called by fuzzy consistency judgement matrix. Especially, any element of R can be represented, by elements in the first row, as $r_{ij} = r_{1j} - r_{1i} + 0.5, i, j = 1, 2, ..., n$.

Theorem 2 [13] if $R = (r_{ij})_{n*n}$ is a fuzzy consistency judgement matrix, the weight of the target factor is acquired by

$$w_i = 1/n - 1/(2\alpha) + 1/(n\alpha) * \sum_{k=1}^{n} r_{ik}, (i = 1, 2, ..., n)$$

where let α be equal to $(n-1)/2$, with the goal to embody the significant importance between factors.

III. Utility-Factor Analysis and Assessment Algorithm for DRM Security Policies

In this section, we analyzed and calculated the factor weights vector by the computation method in Theorem 2, adjusting elements of the fuzzy judgement matrix in term of Theorem 1 related to FAHP, and the fuzzy subjection degree between any two factors is depicted based on the scale defined by Table 3 in [13]. According to typical security policies represented in [11] and the above mentioned theorems, we presented the following Algorithm 1 for fuzzy assessments on factor weights, with the objective to analyze the fuzzy weights of all utility factors, located at the bottom of DRM analytic hierarchy structure, for the target top layer.

Input: based on 0.1-0.9 scale and the comparison of the importance between any two typical security policies, components/services, or utility factors, all elements of i th layer of fuzzy complementary matrix $R = (r_{ij})_{n*n}$ are given.
Output: factor weights vector as W^{CP}_f, W^{RP}_f and $W^{Consumer}_f$ of participants.

for $p \in \{CP, RP, Consumer\}$ **do**
  for $AHP\_l \in policyLayer, CSLayer, factorLayer$ **do**
    while R *is a non-consistent judgement matrix* **do**
      Adjusting every element of the fuzzy judgement matrix $R = (r_{ij})_{n*n}$,and enabling the equation $r_{ij} = r_{1j} - r_{1i} + 0.5(i, j = 1, 2, ..., n)$ hold;
      Calculating the single-ordering weights of utility factors in the fuzzy consistent judgement matrix by the following equation as $R_{AHP\_l} = (r_{ij})_{n*n} w_i = 1/n - 1/2\alpha + (1/n\alpha) * \sum_{k=1}^{n} r_{ik}, (i = 1, 2, ..., n)$;
      For the $(AHP_l > 1)$th layer, in conjunction with the single-ordering factor weights b_{ij},calculating the composite-ordering weights b_i of the element a_j in the $(AHP_l - 1)$th layer, according to $b_i = \sum_{j=1}^{m} b_{ij} a_j, (i = 1, 2, \cdots, n)$;
      In combination with $w^p_{f_i}, (i = 1, 2, ..., n)$, yields W^p_f;
    end
  end
end
return $W^{CP}_f, W^{RP}_f, W^{Consumer}_f$;

Algorithm 1: Fuzzy Weights Assessments Algorithm on Security Utility-Influencing Factors

Let R^{Policy}_{CP}, R^{Policy}_{RP} and $R^{Policy}_{Consumer}$ be fuzzy consistency judgement matrixes of three participants' typical security policies, respectively:

$$R^{Policy}_{CP} = \begin{bmatrix} 0.5000, 0.2070, 0.2476, 0.1000 \\ 0.7930, 0.5000, 0.5406, 0.3930 \\ 0.7524, 0.4594, 0.5000, 0.3524 \\ 0.9000, 0.6070, 0.6476, 0.5000 \end{bmatrix},$$

$$R^{Policy}_{RP} = \begin{bmatrix} 0.5000, 0.1738, 0.2416, 0.1000 \\ 0.8262, 0.5000, 0.5678, 0.4262 \\ 0.7524, 0.4322, 0.5000, 0.3584 \\ 0.9000, 0.5738, 0.6416, 0.5000 \end{bmatrix},$$

$$R_{Consumer}^{Policy} = \begin{bmatrix} 0.5000, 0.3000, 0.1738, 0.1000 \\ 0.7000, 0.5000, 0.3738, 0.3000 \\ 0.8262, 0.6262, 0.5000, 0.4262 \\ 0.9000, 0.7000, 0.5738, 0.5000 \end{bmatrix}.$$

According to Algorithm 1, we gain the fuzzy weight vector $W_{CP} = (0.0925, 0.2878, 0.2607, 0.3591)^T$ of CP's security policies set $\{sp_{CP}^1, sp_{CP}^2, sp_{CP}^3, sp_{CP}^4\}$.

Similarly, RP's weights vector is $W_{RP} = (0.0859, 0.3034, 0.2572, 0.3526)^T$, and Consumer's is $W_{Consumer} = (0.0957, 0.2290, 0.3131, 0.3623)^T$.

The utility weights of CP, RP and Consumer's OSS/OSC for Security Policy Layer are shown in Table 4.1, where $w_{c*/s*/c/s}^j$=0 when a certain c/s and sp_i^j are irrelevant, and $(i \in \{CP, RP, Consumer\}, 1 \leq j \leq 4)$.

We give a serious of fuzzy consistency matrixes of utility-influenced factor weights related to three participants' optional security components/services in DRM ecosystem.

$$R_{CP}^{Identification} = \begin{bmatrix} 0.5000, 0.7524 \\ 0.2476, 0.5000 \end{bmatrix},$$

$$R_{CP}^{TN} = \begin{bmatrix} 0.5000, 0.7930 \\ 0.2070, 0.5000 \end{bmatrix},$$

$$R_{RP}^{DA} = \begin{bmatrix} 0.5000, 0.8786, 0.7930 \\ 0.1214, 0.5000, 0.4144 \\ 0.2070, 0.5856, 0.5000 \end{bmatrix},$$

$$R_{RP}^{TN} = \begin{bmatrix} 0.5000, 0.7930 \\ 0.2070, 0.5000 \end{bmatrix},$$

$$R_{Consumer}^{CRE} = \begin{bmatrix} 0.5000, 0.700 \\ 0.300, 0.5000 \end{bmatrix},$$

$$R_{Consumer}^{TCD} = \begin{bmatrix} 0.5000, 0.9000, 0.8786 \\ 0.1000, 0.5000, 0.4786 \\ 0.1214, 0.5214, 0.5000 \end{bmatrix}.$$

Furtherwe gain the fuzzy weights assessment vector $W_f^{CP} = (0.0937, 0.0308, 0.0852, 0.0222)^T$ with respect to CP's utility-influenced factors set $\{f_{CP}^{PoI}, f_{CP}^{CoI}, f_{CP}^{PoTN}, f_{CP}^{CoTN}\}$ for the target layer.

In a similar waythe fuzzy weights assessment vector $W_f^{RP} = (0.1138, 0.0364, 0.0539, 0.0845, 0.0220)^T$ about RP's utility-influenced factors set $\{f_{RP}^{PoDA}, f_{RP}^{CoDA}, f_{RP}^{CoTC}, f_{RP}^{PoTN}, f_{RP}^{CoTN}\}$ for the target layer, and Consumer's is $W_f^{Consumer} = (0.1371, 0.0587, 0.1411, 0.0459, 0.0510)^T$ for its utility-influenced factors set $\{f_{Consumer}^{PoCRE}, f_{Consumer}^{CoCRE}, f_{Consumer}^{PoDA}, f_{Consumer}^{PoDA}, f_{Consumer}^{CoTC}\}$.

IV. Swarm Simulations and Discussions on Adoptions of DRM Security Policies

We employed 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 2. Besides, functions of main parameters, such as m, n, s, these parameters change in a linear way.

In term of Table 2, simulations results are illustrated by Figure 2-Figure 4.

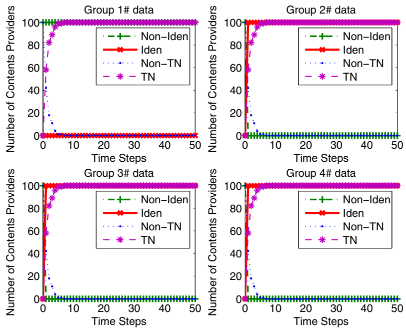

Figure 2. CP Number Changes with Time for different initial values

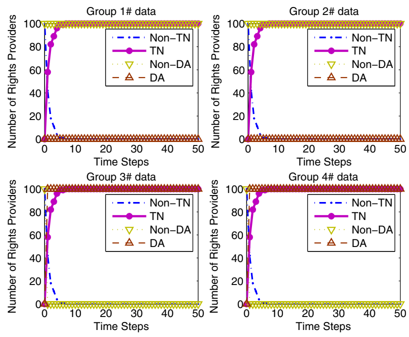

Figure 3. RP Number Changes with Time for different initial values

The above simulation results manifest that some strategies be gradually dominant with time, so we could find out the Nash Equilibrium of the multi-party game. Figure 2 (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

sp^i_{CP}	sp^1_{CP}	sp^2_{CP}	sp^3_{CP}	sp^4_{CP}	for SP_{CP}
c/s	0.0925	0.2878	0.2607	0.3591	$w^l_{c/s}$
Identification	0	0.2357	0	0.1579	0.1245
TN	0	0	0.2246	0.1358	0.1074
sp^j_{RP}	sp^1_{RP}	sp^2_{RP}	sp^3_{RP}	sp^4_{RP}	for SP_{RP}
c/s	0.0859	0.3034	0.2572	0.3526	$w^m_{c/s}$
DA	0	0.3334	0	0.2921	0.2042
TN	0	0	0.2476	0.1213	0.1065
$sp^k_{Consumer}$	$sp^1_{Consumer}$	$sp^2_{Consumer}$	$sp^3_{Consumer}$	$sp^4_{Consumer}$	for $SP_{Consumer}$
c/s	0.0957	0.2290	0.3131	0.3623	$w^n_{c/s}$
CRE	0	0.3666	0	0.3087	0.1958
TCD	0	0	0.5	0.2246	0.2380

Table I
UTILITY FACTORS' WEIGHTS OF TYPICAL SECURITY POLICIES' OSC/OSS

Party	RA_{CP}				RA_{RP}		
Factor	f^{PoI}_{CP}	f^{CoI}_{CP}	f^{PoTN}_{CP}	f^{PoTN}_{CP}	f^{PoDA}_{RP}	f^{CoDA}_{RP}	f^{CoTC}_{RP}
(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^{PoTN}_{RP}	f^{CoTN}_{RP}	f^{PoCRE}_{Cons}	f^{CoCRE}_{Cons}	f^{PoDA}_{Cons}	f^{CoDA}_{Cons}	f^{CoTC}_{Cons}
(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)

Table II
FOUR GROUPS OF INITIAL VALUES AND FUNCTIONS OF MAIN PARAMETERS

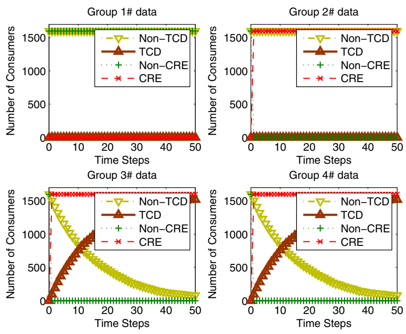

Figure 4. Consumer Number Changes with Time for different initial values

n, together with the decrease of enhanced security overhead, as is shown by Figure 3 (1)-(4). Note that RP firstly adopts sp^3_{RP} including *TN* as Figure 3 (1)-(2), which is consistent with the adoption of CP, and then begin employing *DA* in Figure 3 (3)-(4), as Consumer also adopts *TCD* shown by the following Figure 4 (3)-(4). It is seen from Figure 4 (1)-(4) that Consumer would gradually adopts $sp^4_{Consumer}$ 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 plicies including *DA*, for instance $sp^2_{Consumer}$ or $sp^4_{Consumer}$ is optimal strategy in any time. Here it is obvious that $sp^4_{Consumer}$ would become a dominant policy, as *CRE* is employed in Figure 4 (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 $(sp^4_{CP}, sp^4_{RP}, sp^4_{Consumer})$ becomes a optimal strategy combination for multi-party benefit balance in a certain preconditions after some time steps (repeated game).

V. Conclusion

We proposed an analytic hierarchy structure and its algorithm on the evaluation on utility-factors' weights for DRM security policies based on Fuzzy Analytic Hierarchy Process, and then made Swarm simulation experiments on the adoptions of optimal security policies in combination with the gained weight values. The simulation results show the proposed approach to fuzzy weights assessments effectively implement the rational decision-making on adoptions of security policies combinations, and further refined our game-theoretical analysis for DRM.

Acknowledgment

The authors want to thank anonymous reviewers for their valuable comments and suggestions. The work was sponsored by National Natural Science Foundation of China Grant No. 60803150, Henan Province Key Technologies R & D Program Grant No. 092102210295, and Henan University of Science & Technology Young Scholar Fund Grant No. 2008QN010.

References

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

[2] N. Jho, E. Yoo, and J. Cheon, et al, "New Broadcast Encryption Scheme Using Tree-Based Circle," In: Proceedings of 2005 ACM Workshop on Digital Rights Management, Alexandria, Virginia, USA. Nov, 2005.

[3] N. Fazio, "On cryptographic techniques for Digital Rights Management," Ph.D. Dissertation, New York University, Sep, 2006.

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

[5] Open Digital Rights Language (ODRL) version 1.1, http://www.w3.org/TR/odrl, 2002.

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

[7] A. Arnab and A. Hutchison, "Persistent access control: a formal model for DRM," In: Proceedings of 2007 ACM Workshop on Digital Rights Management, Alexandria, Virginia, USA. Oct, 2007.

[8] J. Park and R. Sandhu, "The UCON$_{ABC}$ Usage Control model," ACM Transactions on Information and System Security, vol.7, no.1, pp. 128-174, 2004.

[9] P. Wolf, M. Steinebach, and K. Diener, "Complementing DRM with digital watermarking: mark, search, retrieve," Online Information Review, vol.31, no.1, pp. 10-21, 2007.

[10] Z. Zhang, Q. Pei, and J. Ma, et al, "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., Jan, 2009.

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

[12] Y. Lu, "Weight Calculate Method of Fuzzy Analytical Hierarchy Process," *Fuzzy Systems and Mathematics*, vol.16, no.2, pp.79-85, 2002.

[13] J. Lan, Y. Xu, and L. Huo, et al, "Research on the Priorities of Fuzzy Analytical Hierarchy Process," *Systems Engineering - Theory & Practice*, vol.9, pp. 107-112, 2006.