

DRM 博弈控制分析

马国峻¹, 裴庆祺², 姜晓鸿¹

(1. 西安电子科技大学 计算机学院, 陕西 西安 710071; 2. 西安电子科技大学 综合业务网国家重点实验室, 陕西 西安 710071)

摘 要: 提出了一种博弈控制模型。博弈的控制者是全局理性的, 并依据控制目标来选择策略, 迫使被控者依据个体理性原则选择控制者期望的策略, 从而实现全局的优化控制。在此基础上, 分析了 DRM 价值链实体的关系和行为, 建立了 DRM 博弈控制模型, 讨论了内容提供商如何作为博弈的控制者选择全局优化策略, 以实现和用户之间稳定的互利共赢, 为 DRM 的合理应用提供了理论指导。

关键词: DRM; 博弈论; 控制; 纳什均衡; 全局优化

中图分类号: TP393

文献标识码: A

文章编号: 1000-436X(2012)Z1-0282-05

Analysis of DRM game control

MA Guo-jun¹, PEI Qing-qi², JIANG Xiao-hong¹

(1. School of Computer Science and Technology, Xidian University, Xi'an 710071, China;

2. The State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China)

Abstract: To overcome the limitations of individual rationality, a game control model was proposed. The controller of game is global rational. To achieve global optimization, the controller chooses strategies according to the control goal, and the controlled chooses the strategies according to the principle of individual rationality. Based on the model and the analysis of relationships and actions of DRM value chain, a model of DRM game control is presented. Content provider actions as the controller of the game, and the global optimization strategies which the content provider choose are discussed, which provides the guidance theory of rational DRM applications.

Key words: DRM; game theory; control; Nash equilibrium; global optimization

1 引言

数字版权管理(DRM, digital right management)技术是数字内容交易过程中对知识产权进行保护的技术、工具和处理过程的总称, 包括对数字资产各种形式的使用进行描述、识别、交易、保护、监控和跟踪等各个过程。

DRM 价值链由内容提供商、用户等多个实体构成, 实际中, 这些实体都具有“理性”的特点, 是以自我利益最大化为目标的。由于利益目标不同, 这些实体之间存在利益冲突和策略竞争的现象, 例如, 一方面, 用户总想以最低的代价来使用

数字内容, 于是出现了非法共享等行为。另一方面, 为了防止数字内容的非法共享, 内容提供商采用各种技术手段来控制、追查数字内容的使用^[1-3], 以维护自身的利益。然而, 技术保护的负面作用又加剧了用户非法共享数字内容的企图^[4]。DRM 价值链的这种矛盾现象, 使人们逐渐认识到发展 DRM 而应该从综合各方利益的角度出发, 需要寻求利益均衡的解决方案^[5,6]。

博弈论也称作“对策论”, 是研究决策主体的行为发生相互作用时的决策以及这种决策的均衡问题的理论, 是研究竞争场景下决策主体行为的重要工具。由于 DRM 价值链中实体的决策行为和利

益关系, 恰好属于博弈论的研究范围。因此, 一些学者开始从博弈论角度来分析 DRM 现象、探讨 DRM 价值链中各方利益均衡问题^[5-8]。和这些工作不同的是, 本文并不是单纯地用博弈论来解释 DRM 价值链内实体的行为, 也不热衷于纳什均衡点的寻求, 而是从非合作博弈的特性入手, 首次提出了博弈控制理论, 并以此为基础来探讨 DRM 价值链内实体选取策略的原则, 为 DRM 的合理发展提供了理论指导。

由于 DRM 价值链内的各个参与实体间难以形成一个稳定的协议, 因此, 本文认为 DRM 价值链内的各个参与实体间的利益关系和决策行为表现为非合作博弈。由于非合作博弈不一定有纯策略纳什均衡点, 并且纳什均衡点也不一定是全局最优点, 即个人理性和集体理性相矛盾。因此, 目前 DRM 价值链中参与实体之间难以达到一个全局优化的均衡点。非合作博弈的这一特点是当前 DRM 现状的一个根本解释。因此, DRM 的合理发展需要克服个体理性的局限, 实现全局优化。为此, 本文提出了控制博弈的概念和模型。控制博弈在基本博弈模型的基础上引入了控制者和控制目标, 控制者是全局理性的, 被控者是个体理性的。控制者依据控制目标来选择自己的策略, “迫使”被控者则依据自身利益最大化原则选择控制者期望的策略, 从而实现全局的优化控制。然后, 本文从 DRM 价值链的利益关系入手, 选取内容提供商和用户作为博弈的参与者, 并对他们的策略和效用进行了分析和建模, 建立了 DRM 控制博弈模型, 最后, 阐述了内容提供商如何作为博弈的控制者来选择全局优化策略, 以实现和用户之间的稳定的互利共赢。

2 控制博弈

2.1 基本博弈模型

一个基本的博弈模型可表示为 $G=(P, S, U, \Gamma)$, 其中 P 表示参与者, S 表示策略集, U 表示效用函数。

1) P (参与者), 是参与博弈的直接当事人, 是博弈的决策主体和策略制定者。参与者具有“理性”的特征, 他们行动时都是以自身利益最大化目标的。参与者可以是个人也可以是为了一个共同目标或效用而参加博弈的集体。如果 G 有 n 个参与者, 用 $P=\{1, \dots, n\}$ 表示参与者集合。

2) S (策略集), 参与者可选择全部行动规则

的集合。如果 G 有 n 个参与者, 分别用 S_1, \dots, S_n 每个参与者的策略集, 用 $s_{ij} \in S_i$ 表示参与者 i 的第 j 个策略, 同时用 S_{-i} 表示除参与者 i 之外的其他参与者选择的策略集合。

3) U (效用函数), 用于计算特定的策略组合下各个参与者收益的大小, 如果 G 有 n 个参与者, 用 U_1, \dots, U_n 分别表示每个参与者的收益函数。

4) Γ 表示博弈的所有纳什均衡点集合, 即 $\Gamma=\{\tau_1, \dots, \tau_m\}$, 其中 τ_i 表示博弈 G 的第 i 个纳什均衡点。 τ_i 是一个策略组合, $\tau_i = \{\sigma_1^*, \dots, \sigma_n^*\}$ ($\sigma_i^* \in S_i$), 对于 $\forall i \in P, \forall \sigma_i \in S_i$ 有

$$U_i(\sigma_i^*, \sigma_{-i}^*) \geq U_i(\sigma_i, \sigma_{-i}^*)$$

其中, σ_i^* 称为参与者 i 在此均衡点的占优策略。

非合作博弈中, 个人理性和集体理性往往是相矛盾的, 理性的个体追求自身利益最大化的结果却实现不了集体利益的最大化, 从而也不能真正实现自身利益的最大化。因此, 非合作博弈不一定有纯策略纳什均衡点, 同时纳什均衡点往往不是全局最优点, 如典型的非合作博弈模型一囚徒困境模型。

2.2 博弈控制

2.2.1 模型

为了克服个体理性的局限, 实现全局的理性, 本文提出了控制博弈的概念。控制博弈在基本非合作博弈模型的基础上引入了控制者和控制目标, 控制者也是博弈的参与者, 但是控制者是全局理性的, 而被控者是个体理性的, 被控制的目标总是需求自身利益最大化的。控制者依据控制目标来选择自己的策略, “迫使”被控者则依据自身利益最大化原则选择控制者期望的策略, 从而, 实现全局的优化控制。

一个博弈控制可表示为 $CG=(P, S, U, C, A, \bar{C}, \bar{A}, W)$, 其中 P 表示参与者, S 表示策略集, U 表示效用函数, 这些和前面介绍基本博弈模型的含义相同。控制博弈的其他元素介绍如下。

1) C 表示控制者, 控制者是博弈的参与者的子集, 即 $C \subseteq P$, 控制者是全局理性的, 控制者会依据全局效用函数 W 来选择基于 W 全局优化的战略。

2) A 是控制策略的集合, A 是控制者实施控制的策略集合。

3) \bar{C} 表示被控者, 是博弈参与者中除了控制者的那部分参与者, 即 $\bar{C} \subseteq P$, 同时 $C \cap \bar{C} = \phi$,

$C \cup \bar{C} = P$ 。

4) \bar{A} 表示被控者的策略，是 \bar{C} 在 C 选择 A 的情况下，依据个体利益最大化原则选择的策略，即对于 $\forall i \in \bar{C}$ ，用 \bar{a}_i 表示被控者 i 的策略， $\bar{a}_i \in \bar{A}$ 。用 $S_{\bar{C}-i}$ 表示 \bar{C} 中除 i 外的被控者策略集合，则对于 $\forall \sigma_i \in S_i - \{\bar{a}_i\}$ 和 $\forall \sigma_{\bar{C}-i} \in S_{\bar{C}-i}$ ，有下式成立

$$U_i(A, \bar{a}_i, \sigma_{\bar{C}-i}) > U_i(A, \sigma_i, \sigma_{\bar{C}-i})$$

5) W 表示全局效用函数，是控制目标的体现。它是控制策略 A 和 \bar{A} 的函数，控制者选择控制策略的目标是使该函数的值最大，以实现全局的最优化。

2.2.1 必要条件

控制者要实现全局优化控制，需要满足以下基本条件。

1) 信息透明，控制者清楚地知道被控者的策略以及效用函数，这样控制者才能正确地选择全局优化的策略。

2) 控制先行，控制者先于被控者做出控制策略的行动。

3 DRM 博弈控制

为了从控制博弈的角度来研究 DRM 价值链中实体的决策行为及相互影响，并寻求全局优化的解决方案，在前面建立控制博弈的基础上建立 DRM 博弈控制模型，内容提供商作为控制者来实施全局优化的策略。

3.1 参与者

为了便于从博弈角度对其进行研究，本文从 DRM 价值链的内在利益关系和价值目标不同的角度出发，将 DRM 价值链中的众多实体抽象为 2 个参与者：内容提供商和用户。内容提供商的利益目标是通过销售数字内容来最大程度地获利，用户的利益目标则是用最小的代价来使用数字内容。因此，在进行数字内容的销售和传播过程中，双方的利益目标是不同的。正是由于策略目标的不同而导致决策冲突的发生，成为需要用博弈理论来分析和优化原因。

实际中，内容提供商是通过 DRM 系统来实施各种保护措施和营销策略的，而用户是基于已有的 DRM 系统来购买数字内容的，因此，DRM 系统的策略是先于用户的购买策略的，内容提供商很适合作为控制博弈的控制者，而用户则作为被控者。所以，本文选择内容提供商作为 DRM 控制博弈的控

制者，用户则为被控者。

3.2 策略

策略是指参与人的行动规则，它表明了参与者在轮到自己行动的情形下，可以采取的行动。在深入分析内容提供商和用户决策行为的基础上，本文对用户和内容提供商的策略进行了抽象和总结。

3.2.1 用户策略

用户是数字内容的使用者，决策行为主要体现在是否使用合法数字内容，因此，用户有如下策略。

- 1) 合法购买数字内容，用 S_u_id 表示。
- 2) 使用盗版内容，用 S_u_id 表示。
- 3) 不使用数字内容，用 S_u_nu 来表示，当使用合法数字内容或盗版内容的代价太大时，用户会选择不使用数字内容。

用户策略集合用 S_u 来表示，即 $S_u = \{S_u_id, S_u_id, S_u_nu\}$ 。

3.2.2 内容提供商策略

内容提供商是数字内容的提供者，主要行为集中在提供数字内容是所采用的安全策略，以及销售价格。本文将内容提供商的行为抽象为如下策略。

1) 销售数字内容的价格，用 P_{dc} 来表示。销售价格是内容提供商进行行销的主要调控手段，直接关系到内容提供商的收益。

2) 共享策略，用 P_s 来表示。本文将内容提供商的各种技术保护策略统一为共享策略，因为内容提供商使用技术保护策略的主要目的就是限制用户的共享，以维护自身的利益。因此，数字内容和设备绑定的策略，可以理解为是一种最低限度的共享策略，该策略下，用户不能共享数字内容；而无技术保护策略，可以理解为是一种最大限度的共享策略，该策略下用户可以任意共享数字内容，且不承担技术保护的成。

3) 隐私保护级别，用 L_p 表示。用户隐私信息有助于内容提供商进行营销和技术保护，同时也关系到用户对 DRM 系统的满意度，因此，用户隐私信息保护是内容提供商的一个重要策略。 $0 \leq L_p \leq 1$ 指内容提供商对用户购买数字内容的隐私信息的保护级别， $L_p = 0$ 时，内容提供商不保护用户隐私， $L_p = 1$ 时，用户购买数字内容时无任何隐私信息泄漏。

4) 不销售数字内容，用 S_{msd} 来表示。当内容提供商销售数字内容的效用低于一定限额时，内容提

厂商将选择不销售数字内容。

用户和内容提供商的策略及其符号如表 1 所示。

参与者	策略符号	描述
用户	S_{cp}	
	S_{u_ld}	合法购买数字内容
	S_{u_id}	非法使用盗版数字内容
内容提供商	S_{u_nu}	不使用数字内容
	P_{dc}	数字内容的价格
	P_s	共享
	L_p	隐私保护级别
	S_{nsd}	不提供数字内容

3.3 效用函数

本节将讨论用户和内容提供商在不同策略下的效用,用 V_{dc} 表示一份数字内容的使用价值,用 P_{dc} 表示该数字内容的价格,用 V_s 表示无技术保护的情况下,用户合法共享数字内容的效用,用 V_p 表示用户隐私完全保护给用户带来的效用。

3.3.1 内容提供商效用

内容提供商效用取决于数字内容的价格和销售数字内容的成本。销售数字内容的成本主要包括以下几个方面。

- 1) 数字内容生产成本,用 C_{cdc} 来表示。
- 2) 共享策略成本,用 C_{cp-sp} 来表示。
- 3) 隐私保护成本,用 C_{cp-pp} 来表示。
- 4) 数字内容共享的负面作用,用 f_{cp-sp} 来表示。

用 σ_u 表示用户的策略。令内容提供商不销售数字内容时的效用为 0, 即

$$U_{cp}(S_{nsd}, \sigma_u) = 0 \quad (1)$$

假设技术成熟的条件下,隐私保护成本以及保护性共享的成本相对于整个营业成本来说是可忽略的,即 $C_{cp-s} = 0$ 以及 $C_{cp-pp} = 0$ 。则内容提供商提供数字内容,且用户购买数字内容时的效用表示为

$$U_{cp}(P_{dc}, P_s, L_p, S_{u_ld}) = P_{dc} - C_{cdc} - f_{cp-sp} \quad (2)$$

3.3.2 用户效用

用户效用主要取决于数字内容的使用价值和数字内容的成本。用户使用数字内容的成本分 2 种。

- 1) 用户使用合法购买的数字内容的成本,对比

用户使用非保护的数字内容的体验,本文将技术保护的负面作用分为以下 3 个方面。

a) 内容价格,数字内容是有销售价格 P_{dc} 的,用户购买合法数字内容是必须承担这个基本费用。

b) 共享限制负作用,用 f_{u-sp} 表示。包括用户使用 DRM 系统的投资,DRM 系统对用户终端设备系统性能的影响以及不能共享所带来的不便, f_{u-sp} 是内容提供商共享策略 P_s 的函数。

c) 隐私泄露负作用,用 f_{u-pp} 表示,用户使用 DRM 系统购买数字内容时,或多或少地都会泄漏用户的隐私信息, f_{u-pp} 是内容提供商隐私保护等级的函数, $f_{u-pp} = (1 - L_p) V_p$ 。

2) 用户使用非法盗版数字内容的成本,主要包括使用盗版数字内容所承受的法律、道德成本以及数字内容质量的损失等。用 V_{ed} 表示这部分成本。

用 σ_{cp} 表示内容提供商的策略,令用户不使用数字内容的效用为 0, 即

$$S_u(\sigma_{cp}, S_{u_nu}) = 0 \quad (3)$$

用 V_l 表示用户使用正版数字内容带来的正面心理效用,则用户购买正版数字内容的效用为

$$S_u(P_{dc}, P_s, L_p, S_{u_ld}) = V_{dc} + V_l + V_s + V_p - P_{dc} - f_{u-sp} - f_{u-pp} \quad (4)$$

同时,假设用户使用盗版数字内容时是可以完全共享数字内容的,自身的隐私信息也是完全安全的,则用户使用盗版数字内容的效用如下:

$$S_u(\sigma_{cp}, S_{u_id}) = V_{dc} + V_s + V_p - V_{ed} \quad (5)$$

3.4 控制目标

数字内容产业健康发展的基本要求是用户购买合法的数字内容,同时内容提供商能通过出售数字内容而获利,同时,要尽可能地提高内容提供商和用户的效用。因此,综合内容提供商和用户效用,给出全局效用函数为

$$W(\sigma_{cp}, \sigma_u) = (\alpha U_{cp}(\sigma_{cp}, \sigma_u) + \beta U_u(\sigma_{cp}, \sigma_u)) \gamma(U_{cp}(\sigma_{cp}, \sigma_u)) \mu(\sigma_u) \quad (6)$$

其中, σ_{cp} 是内容提供商的控制策略, σ_u 表示用户在内容提供商选择 σ_{cp} 的情况下,依据自身利益最大化而选择的策略。 α 和 β 表示用户和内容提供商的全局效用系数 $0 < \alpha \leq 1, 0 < \beta \leq 1$ 。 μ 和 γ 表示用户和内容提供商的策略效用系数函数。

$$\gamma(x) = \begin{cases} 1, & x > 0 \\ 0, & x \leq 0 \end{cases} \quad (7)$$

$$\mu(x) = \begin{cases} 1, & x = S_{u_ld} \\ 0, & x \neq S_{u_ld} \end{cases} \quad (8)$$

内容提供商总是努力选择使 W 值最大的策略。

3.5 控制策略

现在，讨论内容提供商如何选择控制策略。

首先，用户购买数字内容的条件为

$$U_u(\sigma_{cp}, S_{u_ld}) > U_u(\sigma_{cp}, S_{u_nu}) \quad (9)$$

$$U_u(\sigma_{cp}, S_{u_ld}) > U_u(\sigma_{cp}, S_{u_id}) \quad (10)$$

由式(3)~式(5)得：

$$V_{dc} + V_l + V_s + V_p - P_{dc} - f_{u-sp} - f_{u-pp} > 0 \quad (11)$$

$$V_{dc} + V_l + V_s + V_p - P_{dc} - f_{u-sp} - f_{u-pp} > V_{dc} + V_s + V_p - V_{ed} \quad (12)$$

式(12)可化简为

$$P_{dc} + f_{u-sp} + f_{u-pp} - V_l < V_{ed} \quad (13)$$

其次，内容提供商选择出售数字内容的条件是 $U_{cp}(P_{dc}, P_s, L_p, S_{u_ld}) > 0$ ，即

$$P_{dc} - C_{cdc} - f_{cp-sp} > 0 \quad (14)$$

为了使目标函数 W 最大化，内容提供商控制策略如下。

首先，选择适当的出售价格 P_{dc} 、共享策略 P_s 和隐私保护等级 L_p ，以确保式(11)、式(13)和式(14)成立，在此基础上，内容提供商尽可能地提高隐私保护的等级，这样可以提高用户的效用，进而提高目标函数 W 的值，此外，内容提供商还通过选择适当的共享策略，以进一步提高用户或自己的效用，以提高目标函数 W 的值。

4 结束语

为了解决 DRM 价值链中个体理性与集体理性相矛盾现象的问题。本文提出了博弈控制的概念。博弈的控制者依据控制目标来选择策略，迫使被控者依据自身利益最大化原则选择控制者期望的策略，从而实现全局的优化控制。然后，对 DRM 价值链中的实体进行了提取，以内容提供商和用户为研究对象，建立了 DRM 博弈控制模型，分析了内容提供商如何作为博弈的控制者选择全局优化策略，为 DRM 的合理应用提供了理论指导。

参考文献：

[1] FAZIO N. On Cryptographic Techniques for Digital Rights Management[D]. Ph D Dissertation, New York University, 2006.

[2] CORIA L, NASIOPOULOS P, WARD R. A robust content-dependent algorithm for video watermarking[A]. Proceedings of 2006 ACM Workshop on Digital Rights Management[C]. Alexandria, Virginia, USA, 2006.

[3] MALIK H, KHOKHAR A, ANSARI R. Improved watermark detection for pread-spectrum based watermarking using independent component analysis[A]. Proceedings of 2005 ACM Workshop on Digital Rights Management[C]. Alexandria, Virginia, USA, 2005.

[4] ABIE H. Frontiers of DRM knowledge and technology[J]. IJCSNS International Journal of Computer Science and Network Security, 2007, 7(1):216-231.

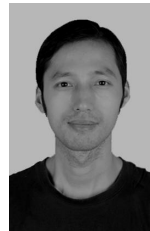
[5] HEILEMAN G, JAMKHEKAR P, KHOURY J, et al. The DRM game[A]. Proceedings of 2007 ACM Workshop on Digital Rights Management[C]. Alexandria, Virginia, USA, 2007.

[6] CHANG Y. Who should own access rights? a game-theoretical approach to striking the optimal balance in the debate over digital rights management[J]. Artificial Intelligence and Law, 2007, 15: 323-356.

[7] ZHANG Z Y, PEI Q Q, YANG L, MA J F. Game-theoretic analyses and simulations of adoptions of security policies for DRM in contents sharing scenario [J]. Intelligent Automation and Soft Computing, 2011, 17(2): 191-203.

[8] ZHANG Z Y, PEI Q Q, MA J F, et al. Cooperative and non-cooperative game-theoretic analyses of adoptions of security policies for DRM[A]. Proceedings of 5th IEEE International Workshop on Digital Rights Management Impact on Consumer Communications, Satellite Workshop of 6th IEEE Consumer Communications & Networking Conference[C]. Las Vegas, Nevada, USA, 2009.

作者简介：



马国峻 (1978-)，男，安徽无为，西安电子科技大学博士生，主要研究方向为信息安全、数字版权管理。

裴庆祺 (1975-)，男，陕西西安人，西安电子科技大学副教授，主要研究方向为信息安全、认知无线网络、数字版权管理。

姜晓鸿 (1966-)，男，陕西洛川人，西安电子科技大学教授，主要研究方向为光网络和无线网络的结构设计及网络协议开发、计算机网络层面、网络节点层面及 VLSI 芯片层面的互连网络结构设计。