A Device Management and Credit Evaluation System in Home Network Domain

Xie Lanchi, Tian Chen, and Wang Xingjun
Shenzhen Key Lab. of Information Sci&Tech/Shenzhen Engineering Lab. of IS&DRM Department of Electronic Engineering/Graduate School at Shenzhen, Tsinghua University, Beijing, China
Email: xielanchi@139.com, livagain@sina.com,wangxingjun@tsinghua.edu.cn

***Abstract*—Many DRM systems were created to protect content rights, but controversy never ends on the necessity. Doubters believe that the loss of user experience will be greater than profit gained. The key point to be solved, is not proposing a method, but proving the expected revenue is satisfactory. In this paper, a centralized home network content protection system firstly proposed. The management part and evaluation part is built on a special designed intelligent home gateway. It supports multiple domains and functions, and has flexible features. Then, profits of operator and user are both taken into consideration. Proposed content protection scheme is proved practical by game theory. Compared with previous systems, the system has many advantages.**

***Index Terms*—Digital Rights Management (DRM), multi-media gateway, credit value, game theory**

I. Introduction

World of internet believes that content is the king in consideration of the enormous economic value. Therefore, digital right management becomes irreplacable method for content protection. Authorized domain is defined to management behavior of several equipments in particular area. Many systems were built to protect the safety of digital goods in home network based on this concept. In 2001,IBM corporation proposed the xCP cluster protocol, using symmetric encryption to share content between different computers. Compared with the public key encryption, it is of benefit in computational complexity. The cost of transmission sharply raises for broadcast encryption, when the amount of data and users booms. Thompson proposed SmartRight in 2003, naming the system personal private network (PPN).A smartcard is in demand for consistency check. Registration progress uses public key encryption, while a specific domain key shared between each member. Troubles appear, when a member is compromised which means the domain key must be changed.

Nowadays, the two most popular specifications involving domain are from Marlin [1] and OMA [2] in the industry. China also has its DRM architecture named China DRM [3]. OMA's specification defines content issuer to distribute the encrypted content and rights issuer to distribute rights object (RO).DRM agents in equipments are responsible to communicate with the server and process the target data. Problems come when number of users becomes larger or networks fail to connect. Definition of domain in Marlin's specification is more flexible. The server part and client part are both allowed to built management entity on. Heeyoul Kim proposed a local management system [4], named local domain manager (LDM), supporting many scenarios for home network. There an assumption exists that local administration device is trusted. However, the credibility is not so obvious.

To solve this problem, home gateway [5] embedded with security chip is necessary to link the identity of users with their behavior. Trust management through reputation mechanisms are summarized by G. Zacharia [6]. Loosely connected and highly connected communities were discussed separately, but it is focus on algorithm research. Yan's paper [7] evaluates devices in P2P network, but the credit scoring method is not detailed. Ben-Jye Chang's paper [8] constructs a Markov chain trust model, while trust value(TV) change when good or bad manners are observed. But the centralized certificate authentication (CA) is not fixed, which will bring more difficulty for communication. In order to build an excellent system, we can't only care the CSP's, but also the consumer's demand. Zhang analyses DRM system with game theory. Analysis based on game theory is just applicable to the problem of payoffs between multi- participants. Jin Zhang's paper [9] analysis DRM in P2P network by game theory provide great inspiration, while what we discuss in is a totally different scene.

The rest part of this paper is organized as follows. Section II we introduce a home DRM system responsible for content share and protection. A reputation evaluation mechanism is put forward in section III. Section IV details game theory analysis used to calculate payoffs of credit evaluation system for consumer and operator. Conclusions and ideas for further research are given in section VI.

II. DRM in Home Network Domain

In this entertainment-oriented era, intelligent terminals become popularized. We hold several or even dozens devices at home, and sharing between different devices conveniently turns into demand. On the other hand, elaborate high-definition TV programs contain enormous

Manuscript received January 28, 2013; revised March 30, 2013

doi: 10.12720/lnit.1.3.104-108

economic value. Effective protection method and appropriate payment mode seem the only way for the industry, which is proved by the success of HULU.

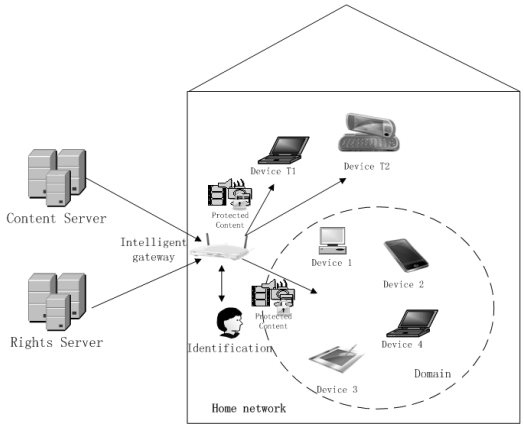

Figure 1. Device management architecture in home network

A. System Overview

In home network, more and more equipments need a management device to control consumption and distribution of digital content. Intelligent gateway is suitable to act the role as content distribution and rights management centre at home. User can customize domain-based services declaring scope and manner of sharing a certain domain. Temporary devices can also choose to not join a domain enjoying service of home gateway. Figure 1 shows the architecture how gateway as a DRM center works in home network.

Intelligent gateway is an "always on" device, equipped Android system with computing ability, which meets the basic requirements as a DRM center. In fact, the thought of local rights management has been proposed a long time ago, while operators don't stand behind it worrying rights abused by suspicious device.

Public key encryption is used in content distribution, and safety of private key determines the system possibility of being cracked. We solve this problem by hardware design .A security chip is embedded in our intelligent gateway. With keys stored in it, the stolen data can't be decrypted, thereby protecting commercial privacy and data security. Each user's identification is locked with the only hardware ID, so their behavior wouldn't be denied.

B. Gateway Centered Content Protection

Multi-media gateway is the management center for content and service protection (CSP). It receives protected content from Content Server, and receives rights objects including rights and restrictions to consume the data from Rights Server. The protected content is encrypted with a content encrypting key (CEK).

Intelligent gateway should also include the memory Entity. Operation history and interactive information of devices are all recorded in it, which will be uploaded to the server by a certain period.

When device enters home, a request message will be sent to the gateway. According to OMA DRM standard, a mutual authentication takes place between device and the gateway. Many access modes are available to choose from. One can join in a exist domain by password, or access as an independent device.

Consuming home content is the basic function of the proposed system. After user purchasing a program, the gateway translates the rights object into different domain rights objects, according to property and level of user who request the content. A domain rights object (DoRO) contains CEK encrypted by domain key(DK),while devices not in a domain will get device rights object (DeRO) including CEK encrypted by their individual public key.

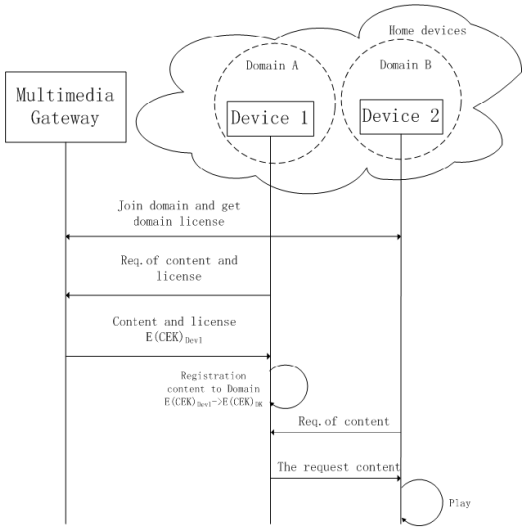

Figure 2. Typical functions of gateway centered domains

In proposed system, various functions are supported, including normal consumption, temporary consumption and super distribution. A typical domain content consumption and distribution example is showed in the following picture.

III. Trust Evaluation Model

Based on device management system, we build a trust evaluation entity to record and distinguish different user's credit situation. During the safety evaluation to home network devices, credit scores are usually binding with the ID of user and domain's. To avoid the attack of re-registration, the credit scores of the newly registered common users should be lowest, and the scores of users are both affected by objective performance of themselves and the scores marked by the others. $S_{i->j}$ represents the trust score given by user to user i to user j .Its value can be chose from 0,1 and 2.

$$S_{i->j} = \{s|0,1,2\}$$

Malicious device attempts to unfairly score others to damage trust evaluation scheme. To eliminate injustice, a score will be adjusted scores given by a certain group of persons.

$$S_{i->j} = \alpha \cdot S_{i->j} + (1-\alpha) \cdot \frac{\sum_{m \in g, m \neq i} S_{m->j}}{|M|}$$

α ($0<\alpha\leq 1$) is the weighted factor, and it has positive correlation with the scorer's own credit level. A user's final score is determined by their objective recording behavior and the scores of given by others. When trigger event takes place, the score changes described by the following formula :

$$S_j^{'} = S_j + \beta \cdot \frac{\sum_{n \in g} S_{n->j}}{|N|} + \gamma \cdot S_j^b$$

S_j is the previous score of j . β and γ are respectively influence factors of scoring and behavior. S_j^b represents score earned by behavior, which we divide into good manners and bad manners. Table I is a optional manner scoring standard. Obviously γ is positive when good manners happen, while it is negative when bad ones detected.

TABLE I. SCORES ACCORDING TO BEHAVIORS

S_j^b	Good Manners	Bad Manners
1	Scoring others	Abnormal application
2	Interaction with others	Frequently changing identity
3	Normal consumption	Malicious scoring
5	Real-name registration	Spoofing and attack
…	…	…
100		Captured piracy

Based on the scores at the moment, system divides all the users into five levels. Level 0 corresponds with users whose score is in the range from -10 to 10.We define it lowest level of all the normal users so as to prevent re-registration attack. People with bad record can't get a higher level of service by re-register a new account (score 0), because functions are in a restricted state for beginner level. Users with higher are considered as important customers, comprehensive service is obtainable. When score an account descends to -10, system label it as abnormal ID, and one will face with various restrictions and subsequent punishment. Especially a piracy caught by methods such as watermark detection, the ID will turn to abnormal level (level -1) directly showed in following picture.

Simply speaking, we sort users in 5 different score levels into 3 group. In view of profit and safety, VIPs get latest film and best service, while abnormal IDs are monitored .At the same time, system limit and guide beginner's manners.

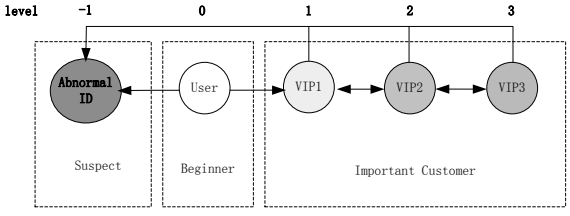

Figure 3. User's credit levels

In the content business model, usually 90% of the profit is gained by the 10% programs. For the more valuable content, it is necessary to take more strict protection measure.

We divided films into important ones and ordinary ones, with costs and benefits both taken into account. The simplest approach is ordinary films for newcomers and VIPs, and the star films are for VIPs only.

IV. GAME THEORY ANALYSIS

In the business world, the participating parties fight for maximum benefits, On the application scene of home network, consumers want better content and service, while operators pursuit high-income and low-cost. Game theory is suitable here to analyze weather the content protection scheme proposed is practical. Firstly we construct a general model.

To consumer, value of goods (G) and services (S) minus price (P) is the prospective earning of a piece of content.

$$\overline{E}_{User} = G + S - P$$

When the operator brings in content protection scheme proposed, the earning expression changed. Extra troubles make some users quit the system (the quit rate is q).After occurrence of turnover, rest customer will get better service and the impact factor is $(1-q)^{-\alpha}$ ($\alpha \geq 1$). Operator benefits from safety of the content, and impact factor β ($\beta \geq 1$) represents for corresponding service improvement.

$$E_{User} = G + \frac{\beta}{(1-q)^{\alpha}} S - P^{'}$$

$P^{'}$ is consumer's cost for content after protection. A film good (g) belongs to group of ordinary films (G_1) or group of important films (G_2).The proposed method not effect viewing ordinary films, so the price is unchanged for general users. $E_{User} \geq \overline{E}_{User}$, so users won't oppose the mechanism.

$$P^{'} \equiv \begin{cases} P, g \in G_1 \\ P + \Delta P, g \in G_2 \end{cases}$$

Restrictions on important movies increase the investment of time and energy for customers by ΔP . Equilibrium point acceptable to the users is $E_{User} = \overline{E}_{User}$ .Thus, $\Delta P = \left[\frac{\beta}{(1-q)^{\alpha}} - 1 \right] \cdot S$

To operator, a piece of film contributes an income of $\overline{E}_{Server}$. N is user number and C is the content cost . Content secure loss (L) caused by behavior of untrustworthy users takes place by a certain probability (p). $\overline{E}_{Server}$ can be characterized as follows:

$$\overline{E}_{Server} = P \cdot N - C - p \cdot L$$

After Configuration of the proposed system, the earning turns into E_{Server}.

$$E_{Server} = P^{'} \cdot (1-q)N - C$$

Operators wouldn't have motivation to build the system unless $E_{Server} > \overline{E}_{Server}$ and $E_{Server} > 0$ .For the important films, put $P^{;} = P + \Delta P$ into E_{Server} .We get

$$\frac{C}{(1-q)N} - \gamma \cdot S < P < \frac{(1-q)N \cdot \gamma \cdot S + p \cdot L}{q \cdot N}$$

, where $\gamma = \frac{\beta}{(1-q)^{\alpha}} - 1$.

Conditions to guarantee the existence of the above solutions are

$$\frac{C}{(1-q)N} - \gamma \cdot S < \frac{(1-q)N \cdot \gamma \cdot S + p \cdot L}{q \cdot N}$$

Which is equivalent with

$$C > \frac{(1-q) \cdot \left[N \cdot \gamma \cdot S + p \cdot L\right]}{q}$$

We can draw a conclusion. When C is greater than a certain value, it exist an range of P that operator can get more profits if content protection system gets used. Namely, protection mechanism only should be adopted in specific high value films under limitation of normal customs' interest not violated. It has been proved by analysis above that proposed user classification and scoring mechanism is of validity.

V. Comparison with Exist System

In this section, we compared the proposed system with other domain DRM systems: xCP (IBM, 2001), Smart Right (2003), OMA (Open Mobile Alliance, 2004), and DVB-CPCM (2009). The result of comparison is presented in Table II.

TABLE II. Functionality Comparisons Between Systems

DRM Systems	Network Dependence	Home Access Control	Hardware Protection	Personal Content Service
SmartRight	Low	×	×	×
xCP	High	△	×	×
OMA	High	△	×	×
DVB-CPCM	Low	×	×	×
Proposed	Low	○	○	○

All these systems supported content consumption in a sharing domain. Systems of OMA and IBM are centralized, rights are all managed by server causing a high network dependence. Proposed system supports multiple domains that each one enjoys different privileges. OMA's and IBM's partly include content about multi-domains, but flexible management of access control is not mentioned. Security chip embedded in home gateway provides hardware protection to the security of encryption and decryption. Credit evaluation entity classifies customers into several levels, so operator can be aware of the trust situation in time.

By comparing with other DRM systems, the proposed system has the advantage in privacy and safety. Novel function of credit scoring creates space for personal service.

VI. Conclusion

In this paper, a device management and credit evaluation system for DRM in home network has been presented. In proposed system, intelligent gateway with security chip acts as brain of home application. Multiple functions and more flexible service guarantee the system more practical.

Many DRM systems have been raised, but few of them come into products. The reason behind is that people ignored the profit what is the prerequisite of motivation to a company. Game theory analysis is an excellent tool to calculate profits. This paper presents a method to evaluate credit and classify users, which is proved effective. Detailed analysis will be taken in further work.

References

[1] Marlin Architecture Overview. (2007). *Marlin Developer Community*. [Online]. pp. 6-20. Available: http://www.marlin-community.com/public/MarlinArchitectureOverview.pdf

[2] *OMA2.0 DRM Specifications*, Open Mobile Alliance, OMA-TS-DRM-DRM-DRM- V2_1 -20070724-C, 2007.

[3] *China DRM Forum Home Network Standard Architecture*, China DRM Forum, Unpublished V2.0, 2009.

[4] H. Kim, Y. Li, and Y. Park, "A robust and flexible digital rights management system for home networks," *Journal of Systems and Software*, vol. 83, no. 12, pp. 2431-40, Dec.2010.

[5] L. Zhu, X. Wang, W. Ren, and Y. Hu, "A new domain management system for home network," *Electrical and Control Engineering*, Yichang, 2011, pp. 1905-1908.

[6] G. Zacharia and P. Maes, "Trust management through reputation mechanisms," *Applied Artificial Intelligence*, vol. 14, no. 9, pp. 881–907, Oct. 2000.

[7] F. Yan, "Research of PC video content protection method," Master dissertation, Dept. Elect. Eng., Tsinghua Univ., Beijing, 2010.

[8] B. Chang and S. Kuo, "Markov chain trust model for trust-value analysis and key management in distributed multicast MANETS," *IEEE Trans. on Vehicular Technology*, vol. 58, no. 4, pp. 1846-63, May 2009.

[9] J. Zhang and W. Lou, "The digital rights management game in Peer-to-Peer streaming systems," *IEEE International Conference on Computer Communications*, Shanghai, 2011, pp. 416-420.

Wang Xingjun received the M.S. degree in electronic and communication system and Ph.D. degree in signal and information processing from Tsinghua University, China, in 1994 and studied in University of Michigan, USA, from 1994 to 1996. His major studies are in digital TV, electronic and communication system.

In China, he is a famous expert in digital TV. He invented USB2.0-card technique and set up related national technology standard. Recently, he is the headman of the national digital right standard and family network workgroup.

Xie Lanchi received the B.S. degree in science and technology of electronic information from Tsinghua University, Beijing, China, in 2010. She will receive M.S. degree in information and communication from Tsinghua University, Beijing, China, in 2013. Her major studies are in digital right management of family network and digital watermarking for videos.

Tian Chen received the B.S. degree in technique and instrumentation of measurements from Harbin university of science and technology, Harbin, China, in 2010. He will receive M.S. degree in electronic and communication engineering from Tsinghua University, China, in 2013. His major studies are in reliability modeling and digital right management in media industry.