Usage Control Model for Digital Rights Management in Digital Home Networks

Zhiyong Zhang, Tao Huang, Danmei Niu, and Lili Zhang
College of Electronics Information Engineering, Henan University of Science and Technology, Luoyang, China
Email: z.zhang@ieee.org

***Abstract*—The free distribution, unauthorized usage, and illicit sharing of copyrighted digital contents have become a common phenomenon with the rapid triple-play progress. The digital home network (DHN) is confronted with the open issue of digital rights management, and there is a lack of a formalized usage control model as well as some killer applications. The paper proposes a role-based cross-domain usage control model called the RCDUCM for DHN, which embraces two primary features of both role-based access control and security domain constraint management. RCDUCM is visually modeled by Unified Modeling Language to shorten the gap between the theoretical model and digital rights management applications. An application case denotes that the proposed model can implement consumer-contents-device license binding and transferring, the result of which is copyright protection of purchased digital contents against malicious piracy.**

***Index Terms*—computer security, Digital Rights Management, formal model, Digital Home Network, copyrights**

I. INTRODUCTION

The past few years have witnessed rapid developments in the fields of information technology and communications. There have been large-scale use and application of 3G/4G wireless mobile networks. Flexible and versatile network admission modes can enable a convenient connection "for anyone at any given time and anywhere" to existing and future digital resources. However, copyright infringements have also unfortunately increased alongside these rapid technological developments. For example, there exist the free distribution, unauthorized usage, and illicit sharing of copyrighted digital contents, including electric books, images, music, movies, and application software, mainly because of the ease with which these products can be duplicated while retaining high quality in their reproduction. These illegal practices negatively affect content protection and legitimate usage, and pose potential critical risks to the digital contents industry. Therefore, appropriate and efficient solutions are urgently needed, especially for eye-catching triple play in China. Digital rights management (DRM) refers to the right employed to cope with this controversial issue.

Manuscript received May 5, 2011; revised June 30, 2011; accepted July 1, 2011. Corresponding author: Zhiyong Zhang.

There are numerous and versatile digital devices in the digital home network (DHN) nowadays such as PCs, IPTVs, smart phones, PDAs, and MP3/MP4 players. General users want to play DRM content freely on their own devices, including the digital home network domain [1-3] and personal entertainment domain [4]. Reference [5] proposed the security domain architecture and corresponding protocols for DRM, but it did not support RO (Rights Object) transferring and content sharing. Consequently, Kim [1] improved on the above-mentioned architecture for a home domain, as well as the newly proposed LDM (Local Domain Manager) substituted Rights Issuer (RI) to accomplish the license distribution for domain membership devices. Meanwhile, the delegated RO and proxy certificate also realize the function of rights delegation. The scheme introduces a potential attack object, i.e., LDM, and increases some overheads. As far as the case wherein a consumer can purchase contents from different providers and share them on different devices is concerned, the introduction to Domain Issuer in OMA DRM instead of multiple Right Issuers is helpful in managing a sharing domain [6]. There remains, however, a lack of formalized usage control model and its visual modeling in DHN.

The paper proposes a role-based, cross-domain usage control model and its formalism, as well as highlights the corresponding visual modeling to shorten the gap between the theoretical model and some killer applications. The rest of the paper is organized as follows. Section 2 examines the authorization and delegation in DHN. Section 3 begins with the formalism of basic model components and defines the temporal properties and several constraint rules. Sections 4 and 5 address visual modeling and an application to the DHN system for DRM, respectively. The final section gives the concluding remarks and future research on secured protocols and security mechanisms.

II. RELATED WORKS

First, Rights Expression Language (REL) is employed by contents/rights providers to specify content usage policies, which involve a number of combined usage rules on rights/permissions under specified conditions and constraints [7]. Until now, there exist some specified REL (i.e., XrML [8], ODRL [9], and MPEG-21 [10]) that have gradually progressed and have been precisely represented in recent years. For example, the additional semantics of REL has been introduced by increasing new XML tags.

doi:10.4304/jmm.6.4.376-383

These constitute a primitive and underlying language that has such properties as flexibility, machine understandability, human readability, and expressivity. An unambiguous semantics is required to ensure that the REL-based rights specifications of copyrighted contents are non-conflicting. Besides, a framework for extensible DRM services by means of a simplified core REL was proposed based on the hierarchy DRM architecture [11]. Figure1 illustrates the separation mode of core REL and associated data with rights management, which is accomplished by the upper application-level transactional interaction.

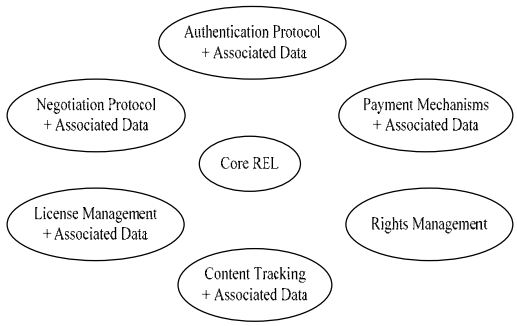

Figure 1. DRM extensible service architecture with an underlying simplified core REL

Some efforts have been focused on formal REL definitions such as the formal foundation for XrML and ODRL [12, 13]. The MPEG-21 REL ISO Standard with formal depictions was published in the realm of the multimedia contents industry [11]. Jamkhedkar proposed a formalized core model of digital rights as a basis of generic REL and clearly presented the map relations between the novel model and the above-mentioned XrML, ODRL, and Creative Commons License [14]. Due to the lack of formalized semantics of OMA REL, Reference [15] employed an executable algebra language called CafeOBJ to resolve the disadvantage, the main goal of which is to come up with automatic tools for the checking of the behavior of license sets. Sheppard discussed the issue on translation between XML-REL and virtual machine programs. A novel concept, Rights Expression Compiler, which is used for REL's formalized definitions and precise translations, was correspondingly proposed [16]. For the validation of digital rights, Sachana implemented an effective method for checking rights consistency [17, 18].

Second, some studies have ever conducted on a general usage control model and it capability or temporal-spatial extensions when typical DRM applications were introduced. A Usage Control basic framework, which integrated Authorization-oBligation-Condition and was also called $UCON_{ABC}$ [19]. Figure 2 (a) showed 4 combinations of $UCON_{ABC}$ models about the Auhthorization, oBligation and Condition, and Figure 2 (b)-(d) illustrated 16 possible basic $UCON_{ABC}$ models, where a notation of '0' denotes the case that all attributes are immutable, and one of '1', '2', and '3' presented the updates of some mutable attributes may happen before (pre), during (ongoing), or after (post) the rights is exercised, respectively.

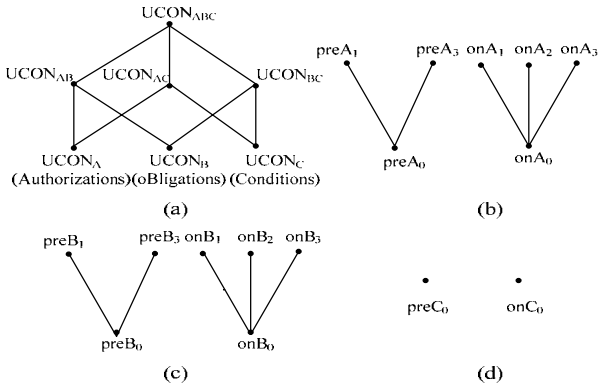

Figure 2. $UCON_{ABC}$ core models family

Due to the lack of the delegation characteristic in $UCON_{ABC}$, we [20] proposed a formal UCON model with the delegation capability, called UCOND, which is an extension of UCON with two important intrinsic properties remaining, as Figure 3.

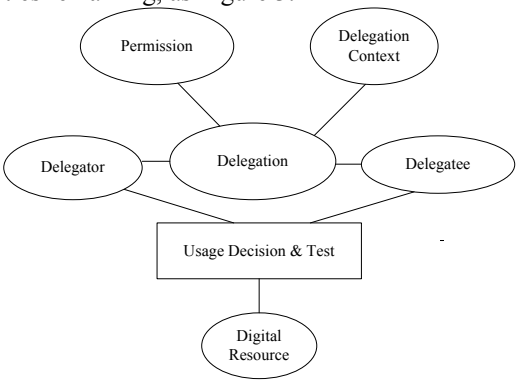

Figure 3. $UCON_D$ Model with the delegation capability

Muhlbauer [21] improved the traditional rights controls based on proposed location constraints by which consumers can access sensitive data resources with a spatial change in mobile terminals. In the scheme, a non-instantaneous display usage control was realized based on MPEG-21 REL in combination with HTTP-HELD protocol-supported and trusted location services. In addition, a complicated technical category of non-instantaneous access control was presented in his contributions. Interestingly, the issue of reply attack of rights object, including such dynamic rights as play period, print count, and expire time, was addressed in [22]. There is a novel mechanism for controlling and managing usage of consumable rights, which is a vital motivator to prevent malicious users from reusing an expired "old license" through backup, especially among domain devices.

Third, regarding usage control applications in DHN, a DRM system for the home network, which is based on the ID-based public key system and group signature protocol, was presented to enable access control of contents and protection of domain privacy by the anonymity characteristic of group signature [23]. Reference [24] introduced an Onion Policy Administration (OPA)-based DRM model by which both content creators and distributors can configure license with traceability; this leads to greater efficiency and security of rights sharing.

Bhatt et al. developed a Personal DRM prototype of the Motorola E680i smart mobile phone [25]. Using the novel terminal, end consumers can set the digital license and flexibly transfer this among devices, resulting in personal content sharing. On temporal rights sharing, Lee made an interesting investigation on a re-distribution approach and secured protocol among front-end user devices. The effort is of significance in the extension of digital rights sharing [26]. Feng and Tang adopted Ergodic Encryption and machine authentication to share purchased license, significantly reducing the overhead due to dependence on the authorized domain [27].

The main disadvantage of the above-mentioned related works, however, is the lack of a generic, formalized model for DRM-enabling DHN. For this, the paper's main contribution is to propose a formalized model with several primary characteristics such as cross-domain security management, usage constraint rules, and rights transferring.

III. FORMALIZED ROLE-BASED, CROSS-DOMAIN USAGE CONTROL MODEL FOR DHN

A. Basic Components

To implement an effective usage control in DHN with versatile digital devices and multiple usage permissions on digital contents, a novel role-based, cross-domain usage control model called the RCDUCM for DHN was proposed based on role-based access control in combination with security domain management. The model embraces the indispensable usage constraints on intra-domain and inter-domain authorizations. The RCDUCM for DHN is composed of several basic components such as consumer, functionality role, device, and usage permission as shown in Figure 4.

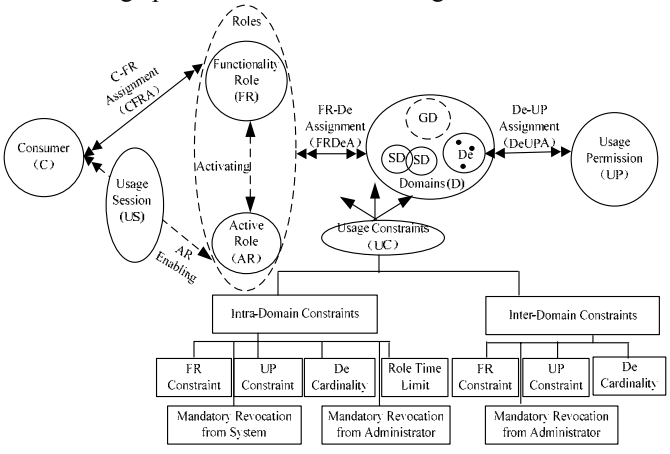

Figure. 4 RCDUCM for DHN

B. Main Formalism

Definition 1 (Consumer, C): It is an active entity that is intended to gain access to the purchased or shared digital contents in DHN. As a generic user, it is subdivided into two subsets, namely, ***Purchaser*** and ***Sharer***.

$$\boldsymbol{C}=\{c|c\in \boldsymbol{Purchaser} \vee c\in \boldsymbol{Sharer}\}$$

Definition 2 (Devices & Domain): The former is a platform set commonly specified as digital devices or consumer electronics by which a *consumer* can render or use digital contents. The later is a set of a group of devices, and it is called Security Domain (SD) when these devices are consistent with needed security requirements and goals. Otherwise, the domain belongs to General Domain (GD) which is not involved with security requirements and implementations.

$\forall\, d\ (d\in \boldsymbol{D})\ d=\{de_1, de_2, \ldots, de_n \mid de_i\in \boldsymbol{De}\}$

$\forall\, sd\ (sd\in \boldsymbol{D})\ sd=\{de_1, de_2, \ldots, de_m \mid de_j\in \boldsymbol{De}$, security goal $(de_j)\}$

Definition 3 (Functionality Role, FR): It denotes an abstract kind of *consumers* with the same usage requirements for a security domain. Further, Active Role (AR) is the only effective role for *consumer* in a usage session, where *c* represents access to digital content objects.

$$\boldsymbol{FR}\in 2^{\boldsymbol{C}},\ \mathrm{ar}\in \boldsymbol{FR}(c)(c\in \boldsymbol{C})$$

Definition 4 (Usage Permission, UP): It is formalized as an authorized operation available in an RO set for a security domain, including reading, writing, playing, pre-playing, license transferring, sharing, and so on.

$$\forall\, ro\ (ro\in \boldsymbol{RO})\ ro=\{up_1, up_2, \ldots, up_n \mid up_j\in \boldsymbol{UP}\}$$

Definition 5 (Set Relationship): There exist several important relationships in the RCDUCM for DHN as follows:

$CFRA\subseteq C\times FR$: It is a multiple-to-multiple assignment relationship between ***C*** and ***FR***.

$ARE\subseteq C\times AR$: Active Role Enabling (ARE) is a one-to-one function.

$FRDeA\subseteq FR\times De$: There exists a multiple-to-multiple assignment relationship, and it is a bidirectional function.

$DeUPA\subseteq De\times UP$: The multiple-to-multiple binding relationship indicates the assignment of usage permission(s) to a certain device.

Definition 6 (Consumer Functionality Role Assignment, CFRA): The authorization is a triple-tuple (c, fr, constraints), and it denotes that *c* would acquire *fr* when the assignment conditions are consistent with pre-defined constraints rules.

Definition 7 (Usage Control of RCDUCM): The control is an authorization assignment formalized as a six-tuple (c_i, fr_j, de_k, up_m, RTL, constraints), where c_i is a consumer, fr_j is a functionality role, de_k is a rendering device, up_m is a usage permission, and Role Time Limit (RTL) is the limitation of periodic or piecewise role action time. The semantic denotes that a generic user c_i is assigned by the DHN administrator to a role fr_j. This role has the whole explicit and implicit operation permission up_m on a consumer electronics device de_k, in the prerequisite conditions of RTL and constraints.

C. Temporal Properties for the Functionality Role

Definition 8 (RTL): The RCDUCM for DHN has a time limitation property, RTL={x | x=[τ bi, τ ei] (i=1,2…n)}, where τ bi is the begin time , and τ ei is the end time.

Definition 9 (States Set): Role states set ***S*** = {init, invoke, sleep, expire}, init is the beginning state, invoke is the active state, sleep is the sleepy state, and expire is the exiting state. Role's expire status is not equal to role revocation. If RTL expires, *fr* can set RTL afresh or be revoked.

Definition 10 (State Transitions in RTL): Let ST be a system time:

$\forall$ i (i$\in$N) ST$\notin$[τ bi, τ ei] $\wedge$ ST<τ b1 $\rightarrow$ S=init;

$\ni$ i (i$\in$N) ST$\in$[τ bi, τ ei] $\rightarrow$ S=invoke;

$\forall$ i (i$\in$N) ST$\notin$[τ bi, τ ei] $\wedge$(ST>τ b1)$\wedge$(ST<τ en) $\rightarrow$ S=sleep;

$\forall$ i (i$\in$N) ST$\notin$[τ bi, τ ei] $\wedge$ ST>τ en $\rightarrow$ S=expire.

D. Usage Constraints in the Security Domain

The RCDUCM for DHN strengthens usage permission assignments and management only in SD, not to GD, to prevent pirates from acquiring illegal usage licenses of digital contents. The essential rules include the non-conflicting constraint and cardinality constraint on several elements of ***FR***, ***UP***, and ***De***, which are defined as follows:

Definition 11 (Conflicting Functionality Role): Two functionality roles fr_i and fr_j are conflicting roles if they are not assigned to a consumer c_k at the same time in any security domain and if both are not sponsored in any session, as formalized by Cofl_FR(fr_i, fr_j, c_k).

Definition 12 (Conflicting Usage Permission): Two usage permissions up_i and up_j are conflicting permissions if they are not assigned to a general consumer c_k simultaneously in any security domain, as defined by Cofl_UP(up_i, up_j, c_k).

Constraint Rule 1 (FR/UP Constraints, FRC/UPC): Any two functionality roles or usage permissions that do not refer to the above assignment conflict with the ***FR*** and ***UP*** sets.

$\forall$ fr_i, fr_j (fr_i, fr_j $\in$ ***FR***, c_k $\in$ ***C***) Cofl_FR(fr_i, fr_j, c_k) = False

$\forall$ up_i, up_j (up_i, up_j $\in$ ***UP***, c_k $\in$ ***C***) Cofl_UP(up_i, up_j, c_k) =False

Constraint Rule 2 (Devices Cardinality Constraint, DeCC): the number of any consumer's devices does not exceed its pre-defined cardinality in any security domain, where the device's cardinality denotes the maximum number of the *consumer*'s owned devices.

Card(c_i, de_j, sd_k) = Max(de | for c_i and any security domain sd_k)

Constraint Rule 3 (Intra/Inter-Domain Constraint): Intra-domain constraint is independently effective only in any security domain, including FRC, UPC, and DeCC, whereas inter-domain constraints have a mutual effect on FRC, UPC, and DeCC. For instance, there is a user who merely has access to the minimum of devices' cardinality constraints when two or more security domains intersect.

Card(c_i, de_j, sd_m, …, sd_n) = Min{Max(de | for c_i and any security domain sd_i) $\wedge$ Intersect(sd_m, …, sd_n)}

Property 1 (Mandatory Revocation from the System): If the system time exceeds the RTL of *fr* or if other requisite conditions change, the RCDUCM for the DHN system would automatically revoke the authorizations, including all explicit and implicit usage permissions. The revocation would only affect intra-domain constraints.

Property 2 (Mandatory Revocation from the Administrator): If the DHN environments or the requisite usage conditions change, the RCDUCM for the DHN system administrator can discretionarily revoke the authority, including all explicit and implicit usage permissions. The revocation would be effective for both intra-domain and inter-domain constraints.

IV. Visual Modeling of the RCDUCM for DHN

A. Static Visual Modeling

The Object-Oriented Method is helpful in analyzing and designing object-oriented application systems using such main concepts as object, class, inheritance, encapsulation, aggregation, message transfer, and polymorphism. A visual modeling of the DHN usage control system adopting the object-oriented thinking and Unified Modeling Language shortens the gap between the abstract theoretical model and application implementations, further guiding the development and deployment of typical DRM applications based on the proposed model.

With regard to the static modeling of the RCDUCM for DHN, a use case diagram and entity class relationship diagram are mainly represented. System functions are introduced from the user's perspective using a use case diagram, as illustrated in Figure 5. Users are basically subcategorized into three kinds which fulfill different functionalities. The System Administrator manages the assignment of consumers, functionality roles, and usage permissions. The Security Officer takes charge of defining intra-domain and inter-domain constraint rules, thus carrying out FRC, UPC, and DeCC, as well as tracking and auditing the whole operations of the System Administrators' authorizations and managements. The General Consumer can access purchased or shared digital content resources.

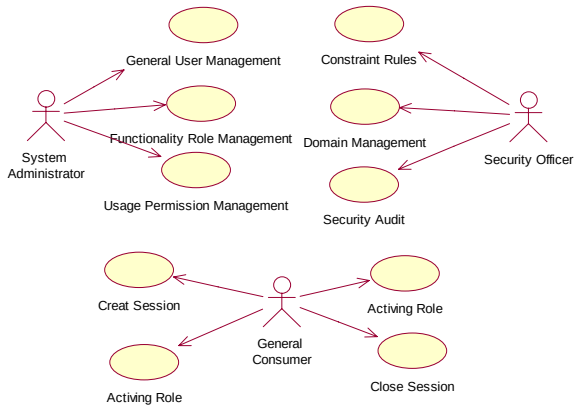

Figure. 5 Use case diagram of the RCDUCM for DHN

Some important entity class relationships, including their attributes and methods, can also be used to present the primary static features of the RCDUCM for DHN, as shown in Figure 6. These relationships mainly include

generalization, aggregation, and association. Role class is generalized into two subclasses: FR and AR. Constraint class is also generalized into Functionality Role Constraint, Usage Permission Constraint, Devices Cardinality Constraint, Role Temporal Limitation, and Revocation. These constraints have explicit effects on usage controls over functionality roles and usage permission assignments, respectively. In the association relationship, the cardinality characteristics between classes were presented such as many-to-many associations between consumer and functionality role classes, functionality role and device classes, device and usage permission classes, as well as one-to-one associations between consumer and active role classes. The class relationship between devices is a special aggregation into a domain through SD or GD.

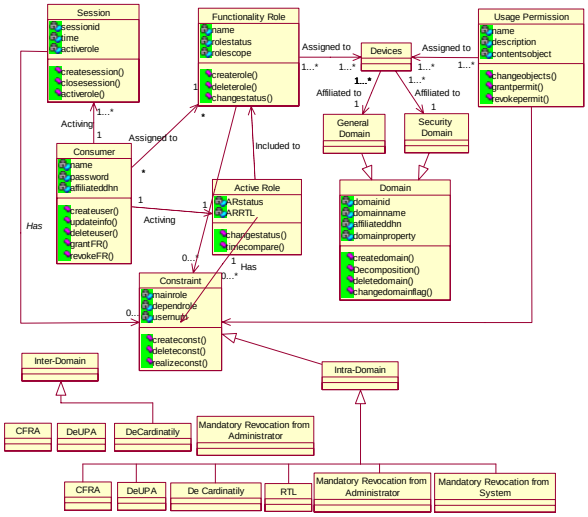

Figure 6. Classes relationship diagram of the RCDUCM for DHN

B. *Dynamic Visual Modeling*

With respect to dynamic modeling, the interaction diagram and object behavior diagram are shown in Figs. 4 to 6. All dynamic features are not described because of the length limitation of the paper, but a functionality role assignment and usage permission assignment (binding) sequence diagram (a kind of interaction diagram) is shown. The system administrator's CFRA and FRDeA are illustrated in Figure 7 and 8, respectively. In these two procedures, the corresponding constraints are implemented, and audit operations are also accomplished. The usage control of a generic consumer over digital contents is shown in Figure 9, in which the contents control, rendering, and auditing are represented in detail.

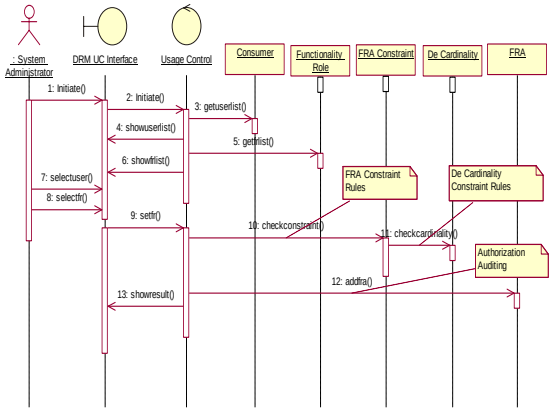

Figure 7. Sequence diagram of functionality roles assignment

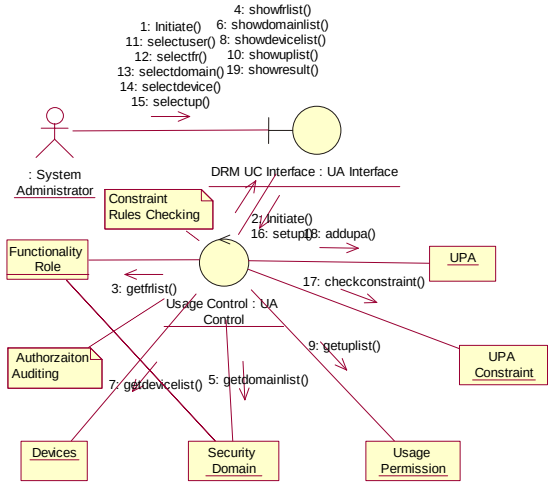

Figure 8. Collaboration diagram of usage permissions assignment

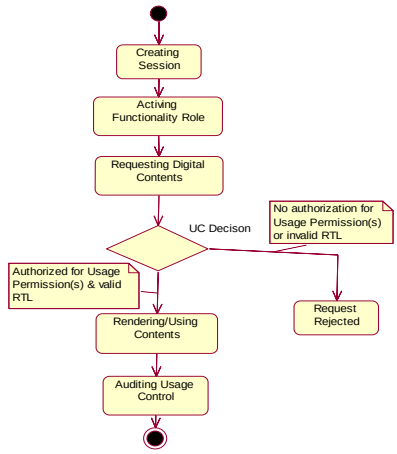

Figure 9. Activity diagram of usage control over consumer's rendering

V. AN APPLICATION CASE OF THE RCDUCM FOR DHN

For a usage control security subsystem for the DRM in a DHN application, the RCDUCM for DHN was employed, as shown in Figure 10. The architecture is composed of

consumer authentication, authorization, and usage control over digital contents. The authorization managements are mainly composed of centralized authorizations, usage control, and constraint rules management. In the application, the user is also categorized into system administrator, security officer, and general user using the basic security principle called Separation of Duty. In centralized authorization, the system administrator would assign a certain functionality role to a general user as a prerequisite for the above-mentioned constraint rules. The security officer administrates the rule database according to self-defined, application-level security policies.

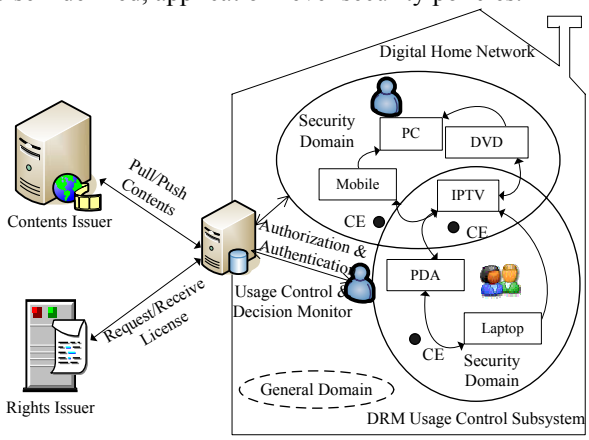

Figure 10. A DRM-enabling DHN application adopting RCDUCM

There is a specific procedure for a general user rendering purchased digital contents over one or more consumer electronics. First, the user is authenticated in the DRM usage control subsystem of DHN. The authentication is especially deployed by a bidirectional mechanism between the user and the security server. Second, the user is assigned a role that corresponds to the usage permissions listed in the purchased license, which depicts the content-device-consumer binding and transferring. Finally, at a specific time, the user gains access to the contents using the binding or transferable license, in realization of the usage control and sharing of contents. There is an intersection of the two security domains, namely, where the IPTV is located and a general domain. Note that Access Control and Decision Monitor makes the decisions on access requests based on valid authentication and authorization.

Analysis and comparison were made among the proposed approach and the existing representative DRM schemes, as shown in Table 1, where such symbols as "○," "×," and "-" show the possession of, no possession of, and not involving the corresponding characteristics or functionalities, respectively. The comparison results denote that the proposed scheme implements more security functionalities, including digital rights sharing, authorization constraint rules and digital rights revocation. In the aspect of system overhead, owing to OMA DRM, as a general standard specification and scheme, is not well involved with authorization and usage control applications for DHN, its overhead is medium. Whereas, the system overheads of the representative DRM approaches, including Ref. [1]'s, Ref. [23]'s, and the proposed scheme, are larger compared with OMA DRM, owing to the deployments and configurations of cipher key management and usage control server devices for home networks. Besides, as a generic formal usage control model for DHN, RCDUCM for DHN is consistent with the multimedia home networks standards or specifications available [28-30].

TABLE I.
COMPARISON OF EXISTING REPRESENTATIVE SCHEMES

Functionality/ Overhead	Schemes			
	OMA DRM	Ref[1]'s	Ref[23]'s	RCDUCM for DHN
Usage Control	○	○	○	○
Security Domain	○	○	×	○
Constraints Rules	×	×	×	○
Rights Sharing	○	○	○	○
Rights Revocation	-	×	×	○
System Overhead	Medium	Local Domain Manager	Cipher Key Management Server	Usage Control Server

VI. CONCLUSIONS

The RCDUCM for DHN is a general and comprehensive DHN-oriented usage control reference model supporting functionality role assignment, device binding, and constraint rules implementation. Our visual modeling presented static and dynamic characteristics, and the theoretical model and visual modeling are adopted in the application case with the result of the model validation. Future works should focus on secure DHN admission protocols and mechanisms, aiming at the integration of a DRM security framework as a whole.

ACKNOWLEDGMENT

We would like to express our gratitude to the anonymous reviewers of this paper for their helpful comments and suggestions. The work was sponsored by the National Natural Science Foundation of China (Grant No.61003234), Program for Science & Technology Innovation Talents in Universities of Henan Province (Grant No.2011HASTIT015), China Postdoctoral Science Foundation (Grant No.20100471611), Henan Province Key Technologies R & D Program (Grant No.092102210295), and Henan University of Science & Technology Doctors Research Fund (Grant No.09001470).

REFERENCES

[1] H. Kim, Y. Lee, B. Chung, et al, "Digital Rights Management with Right Delegation for Home Networks,"

Lecture Notes in Computer Science 4296. Heidelberg, Germany: Springer Verlag Press, 2006, pp.233-245.
[2] J. Lee, Y. Jeong, K. Yoon, et al, "DRM applied contents share in digital home," In: Proceedings of the 13th IEEE International Symposium on Consumer Electronics. Piscataway, USA: IEEE Press, 2009, pp.64-66.
[3] H. Kim, Y. Lee, and Y. Park, "A robust and flexible digital rights management system for home networks," *Journal of Systems and Software*, 2010, vol.83, no.12, pp.2431-2440.
[4] P. Koster, F. Kamperman, P. Lenior, et al, "Identity-based DRM: personal entertainment domain," Lecture Notes in Computer Science 3677. Heidelberg, Germany: Springer Verlag Press, 2005, pp.104-122.
[5] B. C. Popescu, B. Crispo, F. Fkamperman, et al, "A DRM Security Architecture for Home Networks," In: Proceedings of 4th ACM Workshop on Digital Rights Management. New York, USA: ACM Press, 2004, pp.1-10.
[6] P. Koster, J. Montaner, N. Koraichi, et al, "Introduction of the domain issuer in OMA DRM," In: Proceedings of 4th Annual IEEE Consumer Communications and Networking Conference. Piscataway, USA: IEEE Computer Society Press, 2007, pp.940-944.
[7] Z. Y. Zhang, Q. Q. Pei, L. Yang, et al, "Security and trust of digital rights management: a survey," *International Journal of Network Security*, 2009, vol.9, no.3, pp.247-263.
[8] eXtensible rights Markup Language (XrML) 2.0 Specification. El Segundo: ContentGuard Inc, 2001.
[9] Open Digital Rights Language (ODRL) Version 2.0 Draft. ODRL Initiative, 2010.
[10] International Organization for Standardization and International Electrotechnical Commission. ISO/IEC 21000-5 Information technology—Multimedia framework Part 5: Rights Expression Language. Switzerland: 2004.
[11] P. Jamkhedkar, G. Heileman, and I. Ortiz, "The problem with Rights Expression Languages," In: Proceedings of 2006 ACM Workshop on Digital Rights Management. New York, USA: ACM Press, 2006, pp.1-9.
[12] J. Halpern and V.Weissman, "A formal foundation for XrML," *Journal of the ACM*, 2008, vol.55, no.1, pp.4-45.
[13] R. Pucella and V.Weissman, "A formal foundation for ODRL," In: Proceedings of 2004 IEEE Workshop on Issues in the Theory of Security. Piscataway, USA: IEEE Press, 2004.
[14] P. Jamkhedkar and G. Heileman, "A formal conceptual model for rights," In: Proceedings of the 8th ACM Workshop on Digital Rights Management. New York, USA: ACM Press, 2008, pp.29-38.
[15] N. Triantafyllou, I. Ouranos, and P. Stefaneas, "Algebraic specification for OMA REL licenses," In: Proceedings of 2009 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications. Piscataway, USA: IEEE Computer Society Press, 2009, pp.376-381.
[16] N. P. Sheppard and S. N. Reihaneh, "On the operational semantics of rights expression languages," In: Proceedings of the 9th ACM Workshop on Digital Rights Management. New York, USA: ACM Press, 2009, pp.17-27.
[17] A. Sachana, S. Emmanuela, A. Dasa, et al, "Privacy preserving multiparty multilevel DRM architecture," In: Proceedings of 2009 6th IEEE Consumer Communications and Networking Conference. Piscataway, USA: IEEE Computer Society Press, 2009.
[18] A. Sachana, S. Emmanuela, and M. S. Kankanhalli, "Efficient license Validation in MPML DRM Architecture," In: Proceedings of the 9th ACM Workshop on Digital Rights Management. New York, USA: ACM Press, 2009, pp.73-82.
[19] J. Park and R. Sandhu, "The $UCON_{ABC}$ Usage Control model,".ACM Transactions on Information and System Security, 2004, vol. 7, no.1, pp.128-174.
[20] Z. Zhang, L. Yang, and Q. Pei, et al, " Research on Usage Control model with delegation characteristics based on OM-AM methodology," In : Proceeding s of IFIP International Conference on Network and Parallel Computing & Workshop on Networks System Security, Sep, 2007.
[21] A. Muhlbauer, S. N. Reihaneh, F. Salim, et al, "Location constraints in digital rights management," *Computer Communications*, 2008, vol. 31, no.6, pp.1173-1180.
[22] I. M. Abbadi, M. Alawneh, "Replay attack of dynamic rights within an authorised domain," In: Proceedings of 3rd International Conference on Emerging Security Information, Systems and Technologies. Piscataway, USA: IEEE Computer Society Press, 2009, pp.148-154.
[23] Q. Q. Pei, J. F. Ma, J. X. Dai, et al, "Digital rights management for home networks using ID-based public key system and group signature," *China Journal of Electronics*, 2007, vol. 16, no.4, pp.653-669.
[24] T. Sans, F. Cuppens, and C. B. Nora, "OPA: onion policy administration model-another approach to manage rights in DRM," In: Proceedings of 2007 IFIP International Federation for Information Processing. Boston: Springer, 2007, pp.349-360.
[25] S. Bhatt, R Sion, and B. Carbunar. A Personal Mobile DRM Manager for Smartphones. *Computers & Security*, 2009, vol. 28, no.6, pp.327-340.
[26] S. Lee, J. Kim, and S. J. Hong, "Redistributing Time-based Rights between Consumer Devices for Content Sharing in DRM System," *International Journal of Information Security*, 2009, vol.8, no.4, pp.263-273.
[27] X. Feng, Z. Tang, and Y. Y. Yu, "An efficient contents sharing method for DRM," In: Proceedings of 2009 Consumer Communications and Networking Conference. Piscataway, USA: IEEE Computer Society Press, 2009.
[28] Multimedia home server systems - Conceptual model for domain management, IEC/TS 62579, Edition 1.0, May, 2010.
[29] Multimedia home server systems - Digital rights permission code, IEC 62227, Edition 1.0, Jun, 2008.
[30] Multimedia gateway in home networks - Guidelines, IEC 62514, Edition 1.0, May, 2010.

Zhang Zhiyong received his Master,Ph.D. degrees in Computer Science from Dalian University of Technology and Xidian University, China, in 2003 and 2009, respectively, and post-doctoral fellowship at Xi'an Jiaotong University, China.

He is currently associate professor with College of Electronics Information Engineering, Henan University of Science & Technology, and research interests include digital rights management and soft computing, trusted computing and access control. Recent years, he has published over 40 scientific papers on the above research fields, and held 3 patents.

Dr. Zhang is IEEE Senior Member, IEEE Systems, Man, Cybermetics Society Technical Committee on Soft Computing, Membership for Digital Rights Management Technical Specialist Workgroup Attached to China National Audio, Video, Multimedia System and Device Standardization Technologies

Committee, Guest Editor of International Journal of Digital Content Technology and Its Applications. Besides, he is Chair/Co-Chair for several international workshops/sessions on Digital Rights Management, as well as TPC Member for numerous International Conferences. Due to efforts and contributions on academic activities, he was conferred the Award of Outstanding Organization Works for 2009 Int'l Conf. Computational Intelligence and Security in Dec. 2009.

HUANG Tao received his Master degree of Computer Science at Northwestern Polytechnical University. He is currently experimentalist with College of Electronics Information Engineering, Henan University of Science & Technology. His research interests include Access Control and modelling.

NIU Danmei received her Master degree of Computer Science at Wuhan University. She is lecturer with College of Electronics Information Engineering, Henan University of Science & Technology. Her research interests include Digital Rights Management and Usage Control.

ZHANG Lili received his Master degree of Cryptography at Xidian University. She is currently lecturer with College of Electronics Information Engineering, Henan University of Science & Technology, and her research interests include cryptographic algorithm in DRM.