Towards a Dynamic Multi-Policy Dissemination Control Model (DMDCON)

Zude Li, Xiaojun Ye
Institute of Information System and Engineering,
School of Software, Tsinghua University, Beijing, China 100084
li-zd04@mails.tsinghua.edu.cn, yexj@tsinghua.edu.cn

Abstract

Dissemination control (*DCON*) is a security policy of controlling digital resource access before and after distribution. It is an extension of traditional access control within client-side domain, digital rights management by payment-free applications, and originator control on recipients' re-dissemination rights allowance. Different application domains may adopt dynamically different resource dissemination policies, but current *DCON* models cannot solve the multi-policy coexistence and compatibility problems. A dynamic multi-policy dissemination control model (*DMDCON*) is proposed to express the dynamic and multi-policy nature existing in reality, which are indispensable for well formed resource dissemination control application. The goal of this paper is to de ne and extend formally some basic concepts related with resource dissemination (such as dissemination policy, chain, tree, etc.) and further, propose a comprehensive *DMDCON* model to describe universal resource dissemination applications through specifying temporal dissemination features, restrictions, and policy revocation (cascade or non-cascade). Finally, we brie y discuss the importance of *DCON* within the usage control domain.

Keywords

dissemination control, dissemination tree, active time range

1 Introduction

Dissemination control (*DCON*) is one of the most important and challenging goals for information security, which is concerned with controlling digital resource even after it has been delivered to a legitimate recipient [5].

DCON is formed beyond some well-known resource access, dissemination, and usage protection policies.

- *DCON* is an extension of traditional access control from the single server-side resource control to continuous resource access authentication, authorization and propagation along the dissemination path scatted over the decentralized and heterogeneous Internet environment [4, 15, 1, 9];
- *DCON* is an expansion of commercial digital rights management (*DRM*) that focuses on commercial copyrighted digital resource distribution by charging payment from recipients based on contracts subscribed in advance [6, 13]. Commercial *DRM* applications mostly concern the payment-based type (*PBT*) of resource dissemination but ignore the payment-free type (*PFT*). Our generic *DCON* model integrates the *PBT* and *PFT* type, and the new zero-payment type (*ZPT*) for universal resource dissemination applications.
- *DCON* is an enlargement of originator control (*ORCON*). *ORCON* is an access control policy that requires recipients to gain originators approval for resource re-dissemination [1, 9], but *DCON* breaks out this constraint and further, enriches the re-dissemination policies in dissemination chain context without security losing.

Based on the above discussion, *DCON* can be formally de ned as a security policy of controlling both digital resource access before distribution and resource usage even after distribution. The control scope of *DCON* described in the de nition indicates the *physical* resource distribution, and the *continuous* resource control along the dissemination chain.

Our contributions of this paper mainly focus on a formal analysis of *DCON* within the dynamic dissemination tree context, including (1) specifying rule-based automatic re-dissemination rights assignment and revocation (cascade or non-cascade); (2) supporting dynamic dissemination modelling with temporal activation and inactivation of dissemination policy; (3) purchasing a dynamic multi-policy *UCON* model based on the policy-compatible analysis and policy-con ict solutions.

Basic concepts related to resource dissemination are presented in session *2*. Two taxonomies of dissemination policy are described in session *3*. Multi-policy *DCON* and dynamic multi-policy *DCON* are proposed in session *4* and session *5* respectively. Finally, the importance of *DMDCON* within the usage control domain is discussed as a conclusion of the whole paper.

2 Basic Concepts

In most literature on resource dissemination (access, distribution, propagation, etc) [12, 13, 6, 5, 9, 3], some basic concepts such as dissemination certi cate, policy, chain, and resource dissemination decision, are introduced. For example, *DCON* means that the distributor or rights holder can control recipients' access to the digital information [12]. But there are no formal de nitions of these concepts to express their control domain boundaries and dynamical features. For the convenience of the latter extensive discussion, we need to formally de ne and extend those elements.

Firstly, the basic concept, *dissemination chain* can be identi ed as a dissemination path consisting of a sequential list of resource dissemination relations from an originator (or agent) to recipients, denoted as a sequence N_1-N_2-$\cdots$-N_k, where any pair, i.e. N_i-N_{i+1} ($i<k$) is a dissemination relation indicating recipient N_i dissemi-

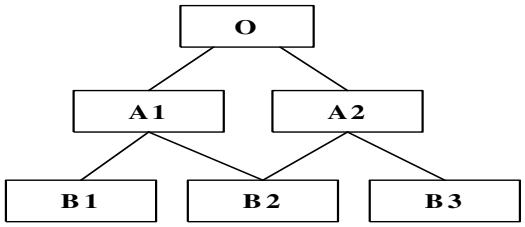

Figure 1. A dissemination tree T on resource $o1$

nates a resource to N_{i+1}. Mostly, a dissemination chain can form a linear-order lattice. Since the dissemination relation can be predened by host organizations, or existed after the resource has been disseminated, we can identify that there are two types of dissemination chain: *predened* chain and *existed* chain. The former indicates a chain is based on predened dissemination relations, which may not exist currently; The latter indicates all dissemination relations along a dissemination chain have been existed. Here we just concern the predened chain type from the view of modelling *DCON*.

Another, we introduce some new concepts elaborately for describing the detail dissemination control process. We define *re-dissemination certificate* as a label indicating whether a subject [1] has capability of re-disseminating resource to others. The *resource re-dissemination allowance* (*SRA*) function is a mapping that indicates whether a subject can re-disseminate specific resource to another one. This function can be formalized as, SRA: $C \times S \times S \times O \rightarrow \{true, false\}$, where C is a boolean parameter denotes whether a re-dissemination certificate is contained in the resource owner node or not by $true$ or $false$ value, S denotes subject set, O denotes object set (resource) and the return of the *SRA* function is a boolean value.

For example, $SRA(true, A1, B1, o1) = true$ denotes $A1$ has a re-dissemination certificate and disseminates $o1$ to $B1$. If the parameter C in the *SRA* function is *false*, then *SRA* always returns *false* no matter of other independent variables. Another, the *resource re-dissemination rights allowance*(*SRRA*) function is a mapping that returns a boolean value indicating whether a subject can grant the re-dissemination right on a specific resource to another subject. It can be formalized as, $SRRA$: $SRA \rightarrow true, false\}$, where *SRA* denotes the return value of a *SRA* function. In the above example, $SRRA(SRA(true, A1, B1, o1)) = true$ denotes $A1$ can grant $B1$ the re-dissemination right on $o1$. It should be noted that $SRRA(false)$ is always *false*.

Dissemination relation in the above dissemination chain definition is from a single subject to another one (one-to-one for short). For describing the one-to-many dissemination relation, we introduce the notion of dissemination tree, an extended version of dissemination chain. Informally, we can see a dissemination tree as the integration of several relative dissemination chains.

DEFINITION 1. Dissemination tree is a tree-shape resource dissemination structure integrated by several relative dissemination chains, where a node represents a subject and an edge between two related nodes represents a dissemination relation.

The root node of a dissemination tree always represents a resource originator (or agent), a dissemination path means a list of partial-order dissemination relations (represented as node pairs, said above) from the root to a specific node. A node is called the *parent* node if it disseminates a resource(or its re-dissemination right) to other nodes (called *son* nodes). The function $Parent$: $S \rightarrow \{S\}$, returns all parents of a node. In addition, we define a node's ancestors as all senior nodes from its parents up to the root node.

In *Fig*.1, root O is the ancestor of all nodes, $A1$ is the parent of both $B1$ and $B2$, $A2$ is the parent of both $B2$ and $B3$. In general, a dissemination tree expresses several dissemination chains or paths with different resource and different dissemination policies. Even, a dissemination tree can have more than one root, which can be called *dissemination network*(direct acyclic graph) or *multi-root* tree. Above all, the essence of a dissemination tree is to integrate various dissemination chains with some shared nodes (as node O and $B2$ in *Fig*.1), and to offer a larger environment for extended dissemination analysis than a single dissemination chain. Within dissemination tree environment, we can expose and solve the policy-conflict problems such as the *multi-parent* one, which is not discovered within single dissemination path but is real existed in many applications.

Similar to the dissemination chain category as described above, there are also two types of dissemination tree: *predened* and *existed* (dissemination) tree. (1) *Predened tree* is built on several related predened dissemination chains; (2) *existed tree* is built on related existed dissemination chains.

On scope, *predened* tree contains *existed* tree, because existing dissemination should have satisfied predened dissemination relations. A *predened* tree frames and restricts the resource (with re-dissemination rights) dissemination flow, but a *existed* tree only describes the current status. In this paper, all dissemination trees proposed are *predened* ones, since they help to analyze possible resource dissemination flows in an integrated way, and policy-conflict problems much fully than any other dissemination tree.

Given a dissemination tree T (*Fig*.1), node $A1$ requires node O for disseminating resource $o1$ and its re-dissemination right, the policy of dealing such a request is as follows:

- for the resource re-dissemination: if O has the re-dissemination certificate and $SRA(true, O, A1, o1) = true$, then $A1$ can acquire $o1$;
- for the resource re-dissemination right: if $A1$ can acquire $o1$ and $SRRA(SRA(true, O, A1, o1)) = true$, then $A1$ can acquire the re-dissemination right on $o1$.

In the above, resource (with its re-dissemination rights) dissemination decision on a node can be performed only by its single parent node [2]. This policy is called *parent-priority*, which indicates that the parent node decides whether its son node can obtain a resource(with its re-dissemination rights). As the decision made above, the single node, O can decide whether $A1$ acquire the re-dissemination right on resource $o1$. More generally, if there is a node $B1$, the son of $A1$, which wants to require the re-dissemination right on $o1$ from $A1$, the formal decision expression is like:
$SRRA(SRA(true, A1, B1, o1)) = true \rightarrow SRRA(SRA(true, O, A1, o1)) = true \cap SRA(true, A1, B1, o1) = true$.
If $B1$ obtains re-dissemination right on $o1$, $A1$ must own $o1$ and its corresponding re-dissemination right firstly.

[1] In this paper, subjects include originators and recipients.

[2] There is no consideration of payment or identification requirement for the resource dissemination charged by the senior nodes.

3 Policy

Different applications may adopt dynamically different resource dissemination policies. There may be many parent nodes of $A1$, or $B1$ in the above, which means that there may be some con icts existing in the dissemination tree. For example, supposing $A1$, $A2$ are two parent nodes of $B2$ (*Fig*.1), $SRRA(SRA(true, A1, B2, o1)) = true$ and $SRRA(SRA(true, A2, B2, o1)) = false$ hold, now how to judge whether $B2$ should have the re-dissemination right on $o1$? For answering this kind of *multi-parent* con ict problems, we propose three policy types of con ict-solution as follows.

- Positive policy. if $\exists\ Ai \in Parent(B2)$, satis es $SRA(true, Ai, B2, o1) = true$, then $B2$ can acquire $o1$ from Ai; if $SRRA(SRA(true, Ai, B2, o1))=true$, then $B2$ can acquire the re-dissemination right on $o1$ from Ai;
- Negative policy. if $\exists\ Ai \in Parent(B2)$, satis es $SRA(true, Ai, B2, o1) = false$, then $B2$ can not acquire $o1$ from any parent; if $SRRA(SRA(true, Ai, B2, o1))=false$, then $B2$ can not acquire the re-dissemination right on $o1$ from any parent;
- Majority-voting policy. if $\exists\ Ai \in Parent(B2)$, $i = 1, 2, \cdots, m$, and $m \geq major(|Parent(B2)|)$ [3], satis es $SRA(true, Ai, B2, o1) = true$, then $B2$ can acquire $o1$ from any positive parent [4]; if $SRRA(SRA(true, Ai, B2, o1)) = true$, then $B2$ can acquire re-dissemination rights on $o1$ from any positive parent.

Beside, dissemination policy can be divided into three types based on the dissemination purpose of the host node that deploys it: Zero-Payment Type (*ZPT*), Payment-Based Type (*PBT*) and Payment-Free Type (*PFT*). The purpose of *ZPT* (deployed by the host node) is to set no control over resource dissemination, and consequently any subject can acquire the resource no matter payment, identi - cation and any other conditions; The purpose of *PBT* is to make pro t for the host node through resource dissemination transactions, and consequently, a payment function is required for monitoring the payment charging process; The purpose of *PFT* is to control the resource dissemination within limited domains, and no payment contact (and payment function) is required but dissemination of resource should be appropriately restricted by using special access mechanisms. Here it should be noted that payment represents more than the notion of money. It can include money (mostly), contracts, agreements, etc. And also the e-payment mechanisms are various within different applications.

In conclusion, the taxonomies of dissemination policy on its priority and on its purpose are connected with each other. For example, *PBT* often takes the *positive* policy but *PFT* always takes the *negative* policy. These elaborate connections should be described system-speci cally.

4 Multi-policy DCON

4.1 De nition

In reality, subjects who require a resource may have different purposes and different ways on its usage and re-dissemination. It results in the complexity of resource dissemination policy management. A multi-policy *DCON* model (*MDCON*) is proposed for solving this problem with convenience.

[3] $major(|Parent(B2)|)$ returns a number that indexes the major part of the whole one.

[4] positive parent denotes a parent node with a policy of allowing resource dissemination.

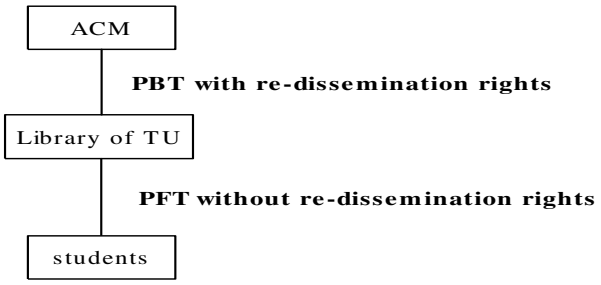

Figure 2. MDCON of PBT-PFT

DEFINITION 2. *MDCON* is a dissemination control model integrating multiple (more than one) dissemination policies within a dissemination tree (chain).

For example, as in the above *Fig*.2, the library of *Tsinghua* University (*TSU*) has brought *ACM*'s digital resource download service by money, and built a mirror site to store these resources, then legally, allows students on campus to share this service of accessing and downloading resource from the mirror site by the authentication on student-card *ID*. But students cannot share their acquired resource with any others. In this example, *ACM* is the originator and uses the *PBT* policy on resource dissemination. The library of *TSU* is a recipient that receives resources and corresponding re-dissemination rights from the originator by monetary contribution, and then takes the *PFT* policy on the resource sharing service oriented to students. But students can not propagate their owner resource any more since they have not re-dissemination rights from the library of *TSU*. In conclusion, there are two policies along the dissemination chain, *PBT* (with re-dissemination rights) and *PFT* (without re-dissemination rights).

4.2 Compatible vs. Con icting

Dissemination policies included in a dissemination tree are *policy-compatible* only if they can be real coexisted with reasonable application functions. For example, *PBT-PFT* is policy-compatible, since existing real applications (as the above example) that use *PBT* in a senior node and *PFT* in a junior node. Another, *ZPT-PFT* is not policy-compatible, since the second policy is meaningless and unnecessary, even illegally.

The policy-compatible analysis can introduce two kinds of compatibility relations: *before* and *after* relation, denoted by $beforeC$ and $afterC$ respectively, which are identi ed to describe the order-depended feature. Further, if $A1 \in beforeC(B1)$ holds, the dissemination relation $A1$-$B1$ is *upward-compatible*; if $B1 \in afterC(A1)$ holds, $A1$-$B1$ is *downward-compatible*; if both $A1 \in beforeC(B1)$ and $B1 \in afterC(A1)$ hold, $A1$-$B1$ is *full-compatible*. Mostly we only consider the full-compatible type and use the following constraint for normalizing $beforeC$ and $afterC$ relations :

- *If existing two policies, P, Q, and* $P \in beforC(Q)$*, then* $Q \in afterC(P)$*, and vice versa.*

From this point, we can de ne the following policy-compatible sets among the dissemination policies of different purposes (without interpretation) and conclude the dissemination policy compatibility theorem naturally. In reality, the general principles for normalizing its compatibility are as follows:
$beforeC(ZPT) = \{ZPT, PBT, PFT\}$;
$beforeC(PBT) = \{PBT, PFT\}$;

$beforeC(PFT) = \{PFT, PBT\}$;
$afterC(ZPT) = \{ZPT\}$;
$afterC(PBT) = \{PBT, PFT, ZPT\}$;
$afterC(PFT) = \{PFT, PBT, ZPT\}$.

THEOREM 1. In *MDCON*, two dissemination policies can *coexist* in a dissemination chain iff they are full-compatible.

[Proof Sketch]
(1) for the $\rightarrow$ direction, if two policies can coexisted in a dissemination chain, it indicates that this integration is meaningful for real *MDCON* application, so they are full-compatible according to the above interpretation;
(2) for the $\leftarrow$ direction, if two policies are full-compatible, it indicates that no con ict between them and so they can coexist in a dissemination chain.

In reality, building a dissemination model should consider the policy-con ict[5] solutions for administration convenience, since some newly inserted policies may be con icted with existing policies in a dissemination chain. We propose three policy-con ict solutions based on the policy priority.

- *senior-priority*, which indicates if two policies are con ict, then change the junior to be compatible with the senior;
- *junior-priority*, which indicates if two policies are con ict, then change the senior to be compatible with the junior;
- *senior-junior-priority*, which indicates the in-between policy should be changed to be compatible with both the senior and the junior policies.

4.3 Rule-based speci cation

The resource dissemination decision making in *DCON* and *MDCON* is complex and complicated. For easing this process, we build a set of rules for automatically making resource dissemination decisions. Now we use rules to specify dissemination policies, chains, trees, formally. For convenience, we don't consider the re-dissemination time point, policy taxonomy on priority.
-S: Subject set;
-O: Object set;
-P: Policy set, supposing $P = \{ZPT, PBT, PFT\}$;
-PF: $O \times S \times S \rightarrow P$, returns a policy over an object dissemination from a senior node to a junior one;
-$PBTDF : O \times S \times S \times Pay \rightarrow \{true, false\}$, denotes a dissemination allowance from a senior node to a junior one over a resource in PBT. Pay denotes a payment contract;
-$PBTDRF : O \times S \times S \times Pay \rightarrow \{true, false\}$, denotes a dissemination right allowance from a senior node to a junior one over a resource in PBT;
-$PFTDF$: $O \times S \times S \rightarrow \{true, false\}$, denotes a dissemination allowance from a senior node to a junior one over a resource in PFT;
-$PFTDRF : O \times S \times S \rightarrow \{true, false\}$, denotes a dissemination right allowance from a senior node to a junior one over a resource in PFT.

Now we take the above de nitions to describe the dissemination policies formally.

- For ZPT policy, $\forall\ s,\ r \in S,\ o \in O$, $PF(o,\ s,\ r) = ZPT \rightarrow SRA(true,\ s,\ r,\ o) = true$, $SSRA(SRA(true,\ s,\ r,\ o)) = true$;
- For PBT policy, $\forall\ s,\ r \in S,\ o \in O$, $PF(o,\ s,\ r) = PBT$, $PBTDF(o,\ s,\ r,\ \triangle)$ [6] $= true$, $PBTDRF(o,\ s,\ r,\ \triangle) = false$ $(true) \rightarrow SRA(true,\ s,\ r,\ o) = true$, $SSRA(SRA(true,\ s,r,\ o)) = false$ $(true)$;
- For PFT policy, $\forall\ s,\ r \in S,\ o \in O$, $PF(o,\ s,\ r) = PFT$, $PFTDF(o,\ s,\ r) = true$, $PFTDRF(o,\ s,\ r) = false$ $(true) \rightarrow SRA(true,\ s,\ r,\ o) = true$, $SSRA(SRA(true,\ s,\ r,\ o)) = false$ $(true)$.

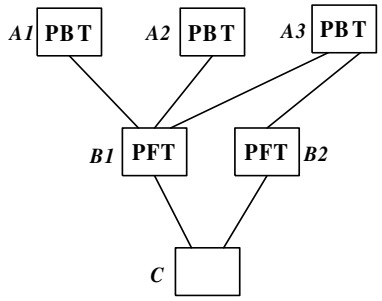

Figure 3. A dissemination tree

Any dissemination chain can be speci ed by combining the above rules. For example, A(PBT with re-dissemination rights according to contract c) - B(PFT without re-dissemination rights) - C can be speci ed as follows:

- On node pair $A(PBT)$-B, $PF(o, A, B) = PBT$, $PBTDF$ (o, A, B, c)=$true$, $PBTDRF(o, A, B, c)$=$true \rightarrow SRA(true, A, B, o) = true$, $SSRA(SRA(true, A, B, o)) = true$;
- On node pair $B(PFT)$-C, $PF(o, B, C)$=PFT, $PFTDF(o, B, C) = true$, $PFTDRF(o, B, C) = false \rightarrow SRA(true, B, C, o)$=$true$, $SSRA(SRA(true, B, C, o)) = false$.

Now we take another instance to demonstrate the dissemination tree speci cation. Supposing $\{A1, A2, A3\}$(PBT with re-dissemination rights propagation according to contract c) - $\{B1, B2\}$(PFT without re-dissemination rights propagation) - $\{C\}$ is a dissemination tree ($Fig.3$) for resource o, and the PBT policy uses the *positive* policy and the PFT policy uses the *negative* policy against the dissemination policy con ict. The dissemination ow of resource o in the whole dissemination tree can be speci ed as follows:

- On node pair $\{A1, A2, A3\}$(PBT & positive policy)-$B1$, If $\exists\ Ai, i \in \{1, 2, 3\}$, $PF(o, Ai, B1) = PBT$, $PBTDF(o, Ai, B1, c) = true$, $PBTDRF(o, Ai, B1, c) = true \rightarrow SRA(true, Ai, B1, o) = true$, $SSRA(SRA(true, Ai, B1, o)) = true$;
- On node pair $A3(PBT)$-$B2$, $PF(o, A3, B2) = PBT$, $PBTDF(o, A3, B2, c) = true$, $PBTDRF(o, A3, B2, c) = true \rightarrow SRA(true, A3, B2, o) = true$, $SSRA(SRA(true, A3, B2, o)) = true$;
- On node pair $\{B1, B2\}$(PFT & negative policy)-C, If $\forall\ Bi, i = 1, 2$; $PF(o, Bi, C) = PFT$, $PFTDF(o, Bi, C) = false \rightarrow \forall\ Bi, i = 1, 2$; $SRA\ (true, Bi, C, o) = false$, $SSRA(\ SRA(true, Bi, C, o)) = false$;

[5] policy-con ict denotes two policies are not full policy-compatible.

[6] $\triangle$ denote a concrete contract value of the corresponding parameter.

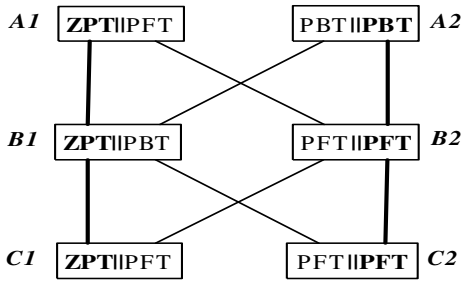

Figure 4. An instance of DMDCON

5 Dynamic Multi-policy DCON

5.1 De nition

In the above section, the dissemination structures (chains and trees) are all static and can not describe dynamical policy mutability, which is necessary and indispensable in real applications. So we propose the dynamic multi-policy *DCON* model (*DMDCON*) to specify continuous policy mutability.

Firstly, we de ne *dynamic dissemination modelling* as the dynamic process of updating the dissemination structure by some operations. From this de nition, some operations can be listed as dynamic dissemination modelling factors, which include inserting, appending a new node, removing an existing node, implementing new policies on existing or new nodes, updating or removing existed dissemination policies on existing nodes etc.

DEFINITION 3. *DMDCON* is an *DCON* model with the following features: (1) Allowing dynamic dissemination modelling; (2) Allowing more than one policy coexisted and activated in the same dissemination chain; (3) Using active time range constraints to express the dynamic features; (4) Using rules to specify the whole resource dissemination process.

The main purpose of *DMDCON* is to describe the dynamic and multi-policy nature of real *DCON* environment. Two attractive features of *DMDCON* are the dissemination decision continuity and dynamic resource dissemination by the activation and inactivation of relative dissemination policies.

5.2 Dynamic features of DMDCON

The dynamic features in our *DMDCON* context refer to the regular activation mutability of dissemination nodes. Factors resulting in this feature include temporal features and special attributes of recipients. For example, in some applications, a dissemination site is active just for some recipients who have special certi cates. Here we take the former factor to demonstrate the dynamic features.

Temporal features of *DMDCON* are expressed mainly by the notion of *active time range*, which is a period of time denoting policy activation and inactivation.

In a dissemination tree, a node is *available* if there is no senior/junior node that is policy-con ict with it. Formally, for node n, its *parent* node set S and *son* node set J, possible dissemination chain set Ch including node n. Node n is available only if, $\forall\, s \in S$, $j \in J$, $\exists\, ch \in Ch, < s, n > \in ch \rightarrow s \in beforeC(n) \cap n \in afterC(s)$; $\forall\, j \in J$, $\exists\, ch \in Ch, < n, j > \in ch \rightarrow j \in afterC(n) \cap n \in beforeC(j)$.

A policy p on node n is *active* if there exist a junior node j, the dissemination of resource o from n to j is available in the current time range tr. Supposing TR denotes time range, and $T(TR, S, S, O, P) \rightarrow \{true, false\}$ denotes an activation test function, $T(tr, A, B, o, p) = true$ denotes node A can disseminate resource o to node B within the time range tr through the active policy p. A node n is *active* only if existing a senior node s and a junior node j are both available, and in the current time range tr, $T(tr, s, n, o, p) = true \cap T(tr, n, j, o, p) = true$ holds. So that function T returns *true* should be a precondition for resource dissemination. Such as in the above example (*Fig*.1), given a dissemination tree T, node $O(p)$-$A1$ is a two-tier model for disseminating resource $o1$ (p is a policy on O). $A1$ can acquire $o1$ iff O has re-dissemination certi cate and $SRA(true, O, A1, o1) = true \cap T(tr, O, A1, o1, p)$ [7] $= true$; $A1$ can acquire the re-disseminate right on $o1$ iff $SRRA(SRA(true, O, A1, o1)) = true \cap T(tr, O, A1, o1, p) = true$.

Furthermore, we take a typical *DMDCON* instance, which contains four multi-policy dissemination chains (*Fig*.4), to demonstrate the above feature.
$A1(ZPT)$ - $B1(ZPT)$ - $C1(ZPT)$;
$A1(PFT)$ - $B2(PFT)$ - $C1(PFT)$;
$A2(PBT)$ - $B1(PBT)$ - $C2(PFT)$;
$A2(PBT)$ - $B2(PFT)$ - $C2(PFT)$.

We de ne that the active time range of an available dissemination chain is the intersection of all of policies within the chain. Supposing the active time range of the ZPT policy on node $A1$ to all junior nodes is (6:00-24:00), it of the PFT policy on $B2$ to $C1$ is (9:00-15:00), and it of the PFT policy on $C1$ to a junior node is (8:00-14:00), So we can calculate easily the active time range of the dissemination chain $A1(PFT)$-$B2(PFT)$-$C1(PFT)$ is (9:00-14:00).

5.3 Revocation: cascade vs. non-cascade

A policy is *revoked* or in the status of *revocation* if it is inactive. Considering the in uence by the revocation of an active policy in a dissemination tree, we divide it into two types:

- *Non-cascade*, which indicates the revocation of a policy just in uences the stand-alone node in a dissemination tree, but not all junior nodes;
- *Cascade*, which indicates the revocation of a policy results in all revocations of junior policies (nodes) in a dissemination tree, which have obtained resource from that node with that policy.

In another way, considering what should be in uenced by a policy revocation, there are two situations: on *resource* or on *re-dissemination rights*. The former indicates that if a policy is revoked, dissemination of both resource and re-dissemination rights [8] should be stopped immediately; the latter indicates what a revoked policy can in uence is re-dissemination rights granting but not resource propagation. In short, there are four types of policy revocation by the combination of the above two taxonomies:
(1) non-cascade revocation on re-dissemination rights;
(2) non-cascade revocation on resource dissemination;
(3) cascade revocation on re-dissemination rights;
(4) cascade revocation on resource dissemination.

[7] p is a speci c policy on O used in this example.

[8] since re-dissemination rights should based on resource dissemination. There are no re-dissemination rights can be granted without resource itself.

Every type has its application domains. For example, Intelligence community needs cascade revocation on resource dissemination: if a le among the community has some error, its copies should not be propagated again. *B2C* e-commerce needs non-cascade revocation on resource: if a senior sale agency has no store of a brand of goods, but a junior has, the senior should not prevent the junior's selling.

5.4 DCON within usage control

Recently, the notion of usage control (*UCON*) is proposed as a comprehensive security service of encompassing traditional access control, trust management, and digital rights management [10, 14]. $UCON_{ABC}$ model family is seen as a new approach for next generation information security solutions [11].

DCON is one of the generic and key concerns of *UCON*, which enables dissemination and re-dissemination outside of a closed system environment where central control authority such as central reference monitor is hard to control.

The *DMDCON* model greatly integrates and expresses the dynamic dissemination conditions in *UCON* with the special mechanisms of the temporal restrictions on dissemination based on active time range, and continuous dissemination management within predened dissemination tree existed in real applications generally. In addition, the *DMDCON* model take a set of rules to describe the complex dissemination decision, which sets a good example for automatized dissemination management within *UCON* model.

6 Conclusion

In this paper, we rstly de ne and extend some basic concepts related with resource dissemination, including dissemination chain, tree. Then, we propose dynamic dissemination modelling and based on this notion, we build the comprehensive *DMDCON* model, which has two attractive features, dissemination decision continuity and dynamic resource dissemination. Finally, we brie y discuss the importance of *DCON* within the usage control domain.

Further research of *DMDCON*, integrating the secure resource initiation and transmission mechanisms, can form our ongoing distributed security model, Secure Resource Management (*SRM*), which elaborately considers trust management [2, 8, 16] and privacy protection [17, 7] as well as the all above mechanisms for achieving a secure resource control (including dissemination and usage separately) lifecycle in open system.

7 References

[1] Abrams, Marshall, and etc. Generalized framework for access control: Towards prototyping the orcon policy. *Proceedings of the 14th National Computer Security Conference*, pages 257 266, 1991.

[2] M. Blaze, J. Feigenbaum, and J. Lacy. Decentralized trust management. *Proceeding of IEEE Conference on Security and Privacy. Oakland, CA.*, 1996.

[3] Dwork, Cynthia, and etc. The mathematics of information coding, extraction, and distribution. *The IMA Volumes in Mathematics and its applications*, 107:31 47, 1999.

[4] D. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli. Proposed nist standard for role-based accesscontrol. *ACM Transactions on Information and System Security*, 4(3):224 274, 2001.

[5] R. K.Thomas and R. Sandhu. Towards a multi-dimensional characterization of dissemination control. *Proceedings of the 5th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'04)*, 2004.

[6] R. Lannella and P. Higgs. Driving content management with digital rights management. *IPR systems whitepaper series*, 2003.

[7] K. Lefevre, R. Agrawal, V. Ercegovac, and R. Ramakrishnan. Limiting disclosure in hippocratic databases. *Proceedings of the 30th VLDB conference, Toronto, Canada*, 2004.

[8] N. Li and J. C. Mitchell. Rt: a role-based trust-management framework. *In DARPA Information Survivability Conference and Exposition (DISCEX), Washington, D.C.*, 2003.

[9] J. Park and R. Sandhu. Originator control in usage control. *Proc. 3rd IEEE International Workshop on Policies for Distributed Systems and Networks, Monterey,California*, pages 60 66, 2002.

[10] J. Park and R. Sandhu. Towards usage control models: Beyond traditional access control. *In Proceedings of 7th ACM Symposium on Access Control Models and Technologies*, 2002.

[11] J. Park and R. Sandhu. The $ucon_{ABC}$ usage control model. *ACM Transactions on Information and System Security*, 7(1):128 174, 2004.

[12] J. Park, R. Sandhu, and J. Schifalacqua. Security architectures for controlled digital information dissemination. *IEEE*, 2000.

[13] Ryotuv and T. Neuman. The set and function approach to modeling authorization in distributed systems. *Proceedings of the Workshop on Mathematical Methods and Models and Architecture for Computer Networks Security*, 2001.

[14] R. Sandhu and J. Park. Usage control: A version for next generation access control. *Proc. Mathematical Methods, Models and Architectures for Computer Networks Security, Saint Petersburg, Russia*, 2003.

[15] R. Sandhu, R. S., and etc. Role-based access control models. *IEEE Computer*, 29(2):38 47, 1996.

[16] J.-M. Seigneur and C. D. Jensen. Trading privacy for trust. *iTrust2004, LNCS2995*, pages 93 107.

[17] J. won Byun, E. Bertino, and N. Li. Purpose-based access control of complex data for privacy protection. *SACMAT'05, Stockholm, Sweden*, Jun.