CHINESE WALL SECURITY MODEL AND CONFLICT ANALYSIS

T. Y. Lin
Department of Mathematics and Computer Science
San Jose State University
San Jose, California 9192
and
Berkeley Initiative in Soft Computing
Department of Electrical Engineering and Computer Science
University of California,
Berkeley, California 94720
tylin@cs.sjsu.edu, tylin@cs.berkely.edu

ABSTRACT

Brewer and Nash, and immediately updated by this author, introduced Chinese Wall security policy models for commercial security. Applying Pawlak's idea of conflict analysis, this paper introduced a practical way of computing an extended model.

1. INTRODUCTION

In 1988 May at the IEEE Symposium on Security and Privacy at Oakland, Brewer and Nash proposed a very interesting and intriguing commercial security model -- called Chinese wall security policy model [BrewerNash88]. The idea and the approach were fascinating and raised tremendous attentions at the conference. The problem they tried to address was essentially the following: To protecting its competing clients, a consulting company needs to have a very tight security policy among its agents. The model was called Chinese Wall security policy model in the sense that there is impenetrable wall among agents. The intuitive meaning of Chinese Wall is essentially the s[...] the current term "fire wall." One of the important results they obtained was: Let CIR be the binary rela[...] "conflict of interests"

意思是：在所有的代理商中存在着不可逾越的墙壁。

如果一个代理已经接触过一个对象（一个客户和他的数据），那么他能够接触到的其他数据就只能是同一个客户或者是其他的CIR类。

BN-Theorem 1. Once an agent has accessed an object (a client and its data), the only other objects accessible by that agent lie within the same client dataset or within a different CIR class.

一旦代理商接触了某个指定的对象，那么他所能够接触的其他对象就只有：同一个客户的数据集，或者，冲突集合以外的数据（冲突集合为集合中包含和指定对象存在利益冲突的对象）

This "theorem," however, is inaccurate; the authors implicitly assumed CIR is an equivalence relation that pa[...] the universe into mutually disjoint equivalence classes. Present author proposed a modification.

作者隐含地认为CIR是将所有关系划分为相互不相交的等价类的等价关系。 目前作者提出了一个修改。

THEOREM 1 Once an agent has accessed a particular object, the only other objects accessible by that agent li[...] within the same client dataset or outside of the *conflict neighborhood*, where conflict neighborhood consists of thos[...] objects whose interests are in conflict to that particular object.

These are the events of 1989; some how the security community has not developed these idea further or its practice[...] have not been well published. Both papers assumed the existence of "conflict of interests," denoted by CIR, and n[...] indications on how such CIR can be constructed. Completely from different directions, Pawlak, the creator of rough set theory, initiated a research on the conflict analysis in mid 80's. In his acceptance speech of the best paper award at JIC'98, he presented a talk on conflict analysis and hinted towards the possible applications to international affairs. Currently, e-business has experience enormous growth, developing a usable security model is quite essential. In this paper, we apply Pawlak's idea of conflict analysis, take the approaches of Chinese Wall models, and augment with uncertainty reasoning to explore a security model.

不管怎么说，安全社区已经不再深入研究这个想法，它的实践也没有很好的发表。同时，关于论文中提到的CIR，也没有任何指出如何建立CIR类的迹象。

在本文中，我们运用Pawlak的冲突分析思想，采用中国墙模型的方法，并用不确定性推理来扩充安全模型

2. CHINESE WALL SECUIRTY POLICY MODELS

We will recall some of our analysis from [Lin89]. "Conflict of Interest" is mathematically a binary relation, denoted by CIR, that is,

二元关系

一般来说，这不是等价关系。在现实世界中，脆弱的CIR几乎是不可能的，某种权重应该与每一对（u，v）相关联。每一对CIR都应该存在权值。

$$CIR = \{(u, v)\} \subseteq U \times U$$

In general, this is not an equivalence relation. In real world, a crispy CIR is almost impossible; some kind of weight should be associated to each pair (u, v). In other words, there is a map

F((u,v))可以被定义为：
1. 确定的概念
2. 信仰价值
3. 仅仅是客观的测评
在数学上，它是一个模糊的二元关系。

$$F: CIR \subseteq U \times U \rightarrow [0, 1]$$

in which the image F((u, v)) may be defined by (1) a probability, if the sample space is available, (2) belief value, if the necessary environment exists, or (3) it is merely a subjective estimation. Mathematically, this is a fuzzy binary relation. Since the numerical value F((u, v)) may have nothing to do with intuitive "fuzziness;" so we will called it weighted binary relation.

2.1. Formalization of "Conflict of Interests"

这节的目的是要明确CIR在数学中的意义。首先，回忆早些时候的分析：O是一个对象的集合，一个对象就是一个公司的数据集。其次，我们假设CIR应该满足以下4个关系：
1.CIR是一个二元关系
2.CIR是对称的
3.CIR是不自反的，除非在特定情境下
4.CIR是不传递的，除非在特定场景下

在直觉上是清晰的：CIR是一个满足对称性盒非自反的二元关系。传递性指的是CIR内的传递型。

The goal of this section is to capture mathematically what is a "conflict of interests"? Fir earlier analysis [Lin89]: Let O be a set of objects; an object is a dataset of a company. Br assume that "conflict of interests" is an equivalence relation; we disagree. Instead, we interests," denoted by CIR, satisfies the following:

CIR-0 CIR is a binary relation
CIR-1 CIR is symmetric.
CIR-2 CIR is non-reflexive, except in special circumstances.
CIR-3 CIR is non-transitive, except in special circumstances.

It should be intuitively clear CIR is a binary relation that satisfies symmetric and not reflective. For CIR-3, let us examine the following example: Let O = {USA, UK, USSR}. Let CIR="in cold war with". If the relation "in cold war with" were transitive, then the following two statements:

USA is in cold war with USSR, and
USSR is in cold war with UK

would imply that

USA is in cold war with UK.

This is absurd; so CIR is, in general, non-transitive.

2.2. Alliance and Reflexive Closure of Conflicts

冲突的联盟与自反闭包

Very often we need to study the reflexive closure of CIR; in fact that is the relation studies by Brewer and Nash. A reflexive closure, denoted by R(CIR), is a minimal reflexive extension of CIR. Even with this extension, it is still not transitive, formally,

CIR-4 R(CIR) is non-transitive, except in special circumstances.

To validate this postulate, we need to introduce the "opposite" of CIR. Let the opposite be "in ally with" (denoted by IAR); intuitively, one represents "friend," and the other "enemy." The two relations are disjoint (as subsets of $O \times O$). Assume O consists of more than three objects, and IAR is non-trivial in the sense that at least one pair of two distinctive objects is in IAR. Now, we will proceed to the proof: Suppose R(CIR), contrary to the conclusion, is transitive. By non-triviality of IAR, there are two distinct objects, say A_1 and A_2, such that $(A_1, A_2) \in$ IJAR. Since O has more than three objects, there is one more object, say B, distinct from A_1 and A_2. By the assumption of transitivity of R(CIR), $(A_1, B) \in$ R(CIR) and $(B, A_2) \in$ R(CIR), implies $(A_1, A_2) \in$ R(CIR). Since A_1 and A_2 are distinct, $(A_1, A_2) \in$ CIR; this contradicts to the fact that IJAR and CIR are disjoint. So we conclude that R(CIR) can not be transitive.

为了验证这个假说，我么需要引入CIR的敌人的概念，让敌人描述为合谋，记为LAR，直观上一个代表朋友，另一个代表敌人。两个关系是不相交的。假定O含有至少3个对象，而IAR是不平凡的，即至少拥有一对两个互异的对象。
假设R(CIR)是传递的，对于IAR的非平凡性，存在A1和A2，A1和A2都在IJAR中。因为O有至少3个对象 ，所以存在一个对象B,不同与A1和A2。由于假设R(CIR)是传递的，因为(A1，B)属于R(CIR)，(B，A2)属于R(CIR)，可以推出(A1，A2)属于R(CIR)。因为A1和A2是不相同的，所以(A1，A2)属于CIR，这与IJAR和CIR是不相交的矛盾。

2.3. A Critical Review of Brewer and Nash Model

The top level of Brewer and Nash's model consists of "conflict of interest classes." In general, CIR is not an equivalence relation, such equivalent classes do not exist. Figure 1 of [BrewerNash88] implies that the collection of objects are partitioned to pair-wise disjoint sub-collections, hence the data organization cannot be derived from CIR; [Lin89] proposed to resolve their discrepancy by

(1) replacing CIR by a generalized conflict of interest (GCIR).
(2) keeping the mathematical notion of CIR and propose a new model.

In this paper, we will generalize the second solution.

3. INFORMATION TABLES AND CONFLICT ANALYSIS

Following Pawlak, we will examine the conflict of interests via information tables, which is one format of rough set theory [Lin97].

3.1. Information Tables and Relations

The syntax of information tables in rough set theory (RS) is very similar to relations in Relational Database (RDB). Roughly, relation is the image f(x) of a knowledge representation $f : U \to Dom$, while information table is the graph (x, f(x)). Entities in RS are also represented by tuples of attribute values, however, the representation may not be faithful, namely, entities and tuples may not be one to one correspondence.

信息表的语法和关系型数据库的语法非常类似。

RS中的实体由属性值组成的元祖表示，但是这种表示方法不是很忠实，即可能存在实体和元祖不是一对一的关系。

一个关系R由一下部分组成：
1.U，实体的集合
2.T，属性的集合
3.Dom(Ai)，属性Ai可能取值的集合
4.每一个U中的实体都使用一个M唯一表示，Map为：
t: T -> Dom, t(A) 属于 dom(Ai)，Ai 属于 T

A relation R consists of

(1) U = {x, y,..}is a set of entities implicitly.
(2) T is a set of attributes $\{A_1, A_2, .. A_n\}$.
(3) $Dom(A_i)$ is the set of values of attribute A_i.

$$Dom = dom(A_1) \cup dom(A_2) \cup .. \cup dom(A_n),$$

(4) Each entity in U is represented uniquely by a map

$$t : T \to Dom,$$

where $t(A) \varepsilon\, dom(A_i)$ for each $A_i \varepsilon\, T$.

Informally, a relation is a table that consists of rows of elements. Each row represents an entity uniquely.

An information table (also known as information system, knowledge representation system) consists of

(1) U = {u, v,..}is a set of entities.
(2) T is a set of attributes $\{A_1, A_2, .. A_n\}$.
(3) $Dom(A_i)$ is the set of values of attribute A_i.

$$Dom = dom(A_1) \cup dom(A_2) \cup .. \cup dom(A_n),$$

(4) $\rho : U \times T \to Dom$, called description function, is a map such that $\rho(u, A_i)$ is in $dom(A_i)$ for all u in U and A_i in T.

Note that ρ induces a set of maps

$$t = \rho(u, \bullet) : T \to Dom .$$

Each map is a tuple:

$$t=(\rho(u, A_1), \rho(u, A_2),....,\rho(u, A_i), ..\rho(u, A_n))$$

Note that the tuple t is not necessarily associated with entity **uniquely**. In an information table, two distinct entities could have the same tuple representation, which is *not permissible* in relational databases.

3.2. Pawlak's Conflict Analysis

Pawlak used the information table to analyze the conflict. Let us recall the example from [Pawlak97] to illustrate his idea. He considered an example of the Middle East conflict, which was taken from [Casti89] with minor changes. Of course, Pawlak's remarked still holds that the example does not necessarily reflect present-day situation, it is used here only as an illustration of the basic ideas.

Assume there are six agents

1 -- Israel,
2 -- Egypt,
3 -- Palestinians,
4 -- Jordan,
5 -- Syria,
6 -- Saudi Arabia,

1.以色列
2.埃及
3.巴勒斯坦
4.约旦河沿岸
5.叙利亚
6.沙特阿拉伯

and five issues

a -- autonomous Palestinian state on the West Bank and Gaza,
b -- Israeli military outpost along the Jordan River,
c -- Israeli retains East Jerusalem,
d -- Israeli military outposts on the Golan Heights,
e -- Arab countries grant citizenship to Palestinians who choose to remain within their borders.

约旦河西岸和加沙地带自治的巴勒斯坦国
以色列在约旦河沿岸的军事哨所
以色列保留东耶路撒冷
以色列在戈兰高地的军事前哨
阿拉伯国家对选择留在本国境内的巴勒斯坦人给予公民身份。

The relationship of each agent to a specific issue can be clearly depicted in the form of a table, as shown below.

U	a	b	c	d	e
1	-	+	+	+	+
2	+	0	-	-	-
3	+	-	-	-	0
4	0	-	-	0	-
5	+	-	-	-	-
6	0	+	-	0	+

冲突分析最主要的目的是找到争论中代理之间的关系，并且去调查中间的冲突如何解决。
存在三种基本关系，冲突、同盟以及中立。前两者就像CIR和IJAR。

The notations "-", "+", "0" mean that an agent is against, favorable and neutral to the issue respectively. Each row of the table characterizes uniquely an agent by his opinion to the disputed issues.

As Pawlak stated that primary goal in conflict analysis is to find the relationship between agents taking part in the dispute, and investigate how the conflict can be resolved. He introduced three basic relations, conflict, alliance and neutrality, first two are similar to our CIR and IJAR introduced in [Lin89]. We shall not go further, the purpose of this section is to give a soft introduction to the next section

5. WEIGHTED CONFLICT ANALYSIS FOR E-BUSINESS

In this section, we will illustrate the idea of constructing a weighted CIR. Suppose, there is a group of e-business shops, eshop1.com, eshop2.com, eshop3.com, eshop4.com and, eshop5.com. Their businesses are not identical, but do overlap. The type of business is indicated in the following information table.

Shops	e-Card%	e-Stock%	e-Chat%	e-Purchase%	Co_Asset(Millions)
eshop1.com	40%	0	0	60%	50

eshop2.com	10%	45%	45%	0	30
eshop3.com	70%	0	20%	10%	100
eshop4.com	0	80%	10%	10%	200
eshop5.com	5%	35%	30%	35%	10
Business_value(Millions)	93.5	177	56.5	63.5	390

Table 1 Types of Business

The table says that, for example, on e-Card business, eshop1.com, eshop2.com, eshop3.com, and eshop5.com have various degrees of market shares. The precise values are computed in Table 2; (we use -1 to indicate those shops that do not participate in that business)

Shops	e-Card	e-Stock	e-Chat	e-Purchase
eshop1.com	40%*50/93.5=0.21	-1	-1	0.47
eshop2.com	0.03	0.08	0.24	-1
eshop3.com	0.75	0.00	0.35	0.16
eshop4.com	-1	0.90	0.35	0.31
eshop5.com	0.01	0.02	0.05	0.06

Table 2 The Market Shares of Each Business

Those companies that have substantial market shares (≥10%) may have conflict of interests among themselves. Here is the information table of the "substantial market shares." The symbol "1", "0" and "-1" means positive, negligible, and none.

拥有大量市场份额的公司可能会有利益冲突。

Shops	e-Card	e-Stock	e-Chat	e-Purchase
eshop1.com	1	-1	-1	1
eshop2.com	0	0	1	-1
eshop3.com	1	0	1	1
eshop4.com	-1	1	1	1
eshop5.com	0	0	0	0

Table 3

So from the first column of Table 3, the CIR of e-Card business is represented in the table.

e-Card_th

eshop1	0	0	1	0	0
eshop2	0	0	0	0	0
eshop3	1	0	0	0	0
eshop4	0	0	0	0	0
eshop5	0	0	0	0	0
	eshop1	eshop2	eshop3	eshop4	eshop5

由表3变成表4，取第一列为例子，形成的表是关于对角线对称的。

Table 4

From second column, e-Stock business, the CIR is represented in the table

e-Stock_th

eshop1	0	0	0	0	0
eshop2	0	0	0	0	0
eshop3	0	0	0	0	0
eshop4	0	0	0	0	0
eshop5	0	0	0	0	0
	eshop1	eshop2	eshop3	eshop4	eshop5

Table 5

From the third column, e-Chat Room business, the CIR is represented in the table e_Chat_th

eshop1	0	0	1	0	0
eshop2	0	0	1	1	0
eshop3	0	1	0	1	0
eshop4	0	1	1	0	0
eshop5	0	0	0	0	0
	eshop1	eshop2	eshop3	eshop4	eshop5

Table 6

From the third column, e-Purchase business, the CIR is represented in the table

e-Purchase_th

eshop1	0	0	1	1	0
eshop2	0	0	0	0	0
eshop3	1	0	0	1	0
eshop4	1	0	1	0	0
eshop5	0	0	0	0	0
	eshop1	eshop2	eshop3	eshop4	eshop5

Table 7

If we consider total market shares, then by a proper computation (shown below), we have the table.

WCIR

eshop1	0.00	0.00	0.49	0.20	0.00
eshop2	0.00	0.00	0.15	0.15	0.00
eshop3	0.40	0.15	0.00	0.29	0.00
eshop4	0.20	0.15	0.29	0.00	0.00
eshop5	0.00	0.00	0.00	0.00	0.00
	eshop1	eshop2	eshop3	eshop4	eshop5

Table 8: Weighted Conflict of Interests Relation

表8，表示的是shopX和shopY之间的利益冲突数值。
怎么计算呢？总之不是概论论中求到的概率。

Each element at (X, Y) of the Table 8 represents the weight of the conflict of interests between the eshopX and eshopY. For example, the third element in the first tuple means that eshop1 and eshop3 compete for customers, and the degree of competition is 0.49.

The original values, such as e-Card(eshop1), ... are probability values, however, we did *not* compute Table 8 according to the rule of probability theory , so the values in table 8 are no longer probability values. It merely a table of some sort of measurement or estimation. Mathematically, Table 8 is a fuzzy binary relation, however, the entries are semantically *not* measuring fuzzy-ness, so we call it weighted binary relation

Again, by considering only those substantial (≥ 10%) market shares, we have the table of CIR

CIR

eshop1	0	0	1	1	0
eshop2	0	0	1	1	0
eshop3	1	1	0	1	0
eshop4	1	1	1	0	0
eshop5	0	0	0	0	0
	eshop1	eshop2	eshop3	eshop4	eshop5

Table 9: Conflict of Interests Relation

In this section, we provide one practical way (not the only way) of finding a CIR for a given business environment. Once such a binary relation of a Conflict of Interests

是不是落了什么？

5.1. Computation of Table 8

The actual computation of the weight (Table 8) is not the main issue here; we merely indicate one possible way of providing numerical measurements. We will use function notations to indicate attribute values in the table: An attribute will be treated as a function, so the first column (of Table 2) means:

For simplicity, we will denote, 1 for eshop1, 2 for eshop2, ... Each element of Table 2 represents certain market share of a company on certain type of business; their computation is illustrated by an example below.

教你怎么求表2

e-Card(1)=0.21 =[e-Card%(eshop1)]*[Co_Value(shop1)]/[e-Card%(Business_value)]
e-Card(2)= 0.03
e-Card(3)= 0.75
e-Card(4)= 0
e-Card(5)= 0.01

The weight of conflict, say between eshopX and eshopY, will be computed as follows: Each sum, say e-Card(X) +e-Card(Y) is the total market share (percentage) of the companies X and Y. We could consider it as the "amount" of their conflict. The term, e-Card_th(X,Y), is the flag that indicates X and Y have conflict of interests (over the threshold). So the following amount is a reasonable measure of their conflict.

e-Card_th(X,Y)*(e-Card(X) +e-Card(Y))+
e-Chat_th(X,Y)*(e-Chat(X) +e-Chat(Y))+
e-Stock_th(X, Y)*(e-Stock(X) +e-Stock(Y))+
e-Purchase_th(X, Y)*(e-Purchase(X) +e-Purchase(Y))

教你怎么求表8：
1.eCard(X)+eCard(Y)表示X和Y公司在Card上共有的市场份额
2.eCard_th(X, Y)表示X和Y冲突类的flag标识（0或1）
3.开始讦算所有的业务并相加

1-2步骤的结果是关于对角线对称的矩阵

Some of the intermediate computations are kept in the following tables:

Table of (e-Card(X) +e-Card(Y))

eshop1	0.42	0.24	0.96	0.21	0.22
eshop2	0.24	0.06	0.78	0.03	0.04
eshop3	0.96	0.78	1.50	0.75	0.76
eshop4	0.21	0.03	0.75	0.00	0.01
eshop5	0.22	0.04	0.76	0.01	0.02
	eshop1	eshop2	eshop3	eshop4	eshop5

Table of (e-Chat(X) +e-Chat(Y))

eshop1	0	0.08	0	0.9	0.02
eshop2	0.08	0.16	0.08	0.98	0.1
eshop3	0	0.08	0	0.9	0.02
eshop4	0.9	0.98	0.9	1.8	0.92
eshop5	0.02	0.1	0.02	0.92	0.04
	eshop1	eshop2	eshop3	eshop4	eshop5

Table of (e-Stock(X) +e-Stock(Y))

eshop1	0	0.24	0.35	0.35	0.05
eshop2	0.24	0.48	0.59	0.59	0.29
eshop3	0.35	0.59	0.7	0.7	0.4
eshop4	0.35	0.59	0.7	0.7	0.4
eshop5	0.05	0.29	0.4	0.4	0.1
	eshop1	eshop2	eshop3	eshop4	eshop5

Table of (e-Purchase(X) +e-Purchase(Y))

eshop1	0.94	0.47	0.63	0.78	0.53
eshop2	0.47	0	0.16	0.31	0.06
eshop3	0.63	0.16	0.32	0.47	0.22

eshop4	0.78	0.31	0.47	0.62	0.37
eshop5	0.53	0.06	0.22	0.37	0.12
	eshop1	eshop2	eshop3	eshop4	eshop5

该模型是一个明确拒绝（或否定授权）优先于授权的访问矩阵模型的修改

6. CHINESE WALL SECURITY MODEL

Following [Lin89], we will build a mathematical model for e-business. The model is a modification of an access matrix model with explicit denials (or negative authorization) taking precedence over authorizations [Lunt88]. The Chinese Wall security policy is a set of rules such that [BrewerNash88],

"no person (agent) can ever access data (objects) on wrong side of that wall."

没有人可以在错误的墙的一面上访问数据。要求，中国墙必须建在正确的位置，也就是说让不可获得的数据集的集合变得最小。
意思应该是，删除多余的无用的数据。

Moreover, the Chinese Wall has to be built in the right place, that is, the set of inaccessible datasets has to be minimal.

6.1. Binary relations and nearest neighborhoods

多媒体数据库或模式识别中一个非常流行的概念就是—最近邻居。
1.一个最近邻居系统：对于每一个点P，最近邻居是一组距离p非常接近的元素。
2.一个点P和它的所有最近邻居组成一个最近邻居系统。

One of a popular notion in multimedia databases or pattern recognition is the "nearest neighborhoods," which is equivalent to a binary relation:

1. a nearest neighborhood system: To each point p, we associate a nearest neighborhood that is a set of elements that are very "near" to p. The association of a point with its nearest neighborhoods is called a nearest neighborhood system.
2. a binary relation $B \subseteq U \times U$ defines a "nearest neighborhood" for each point

   $p \rightarrow Np=\{ u \mid (u. p) \in B\}$ (= the "nearest neighborhood").

   Conversely given a nearest neighborhood system, a subset can be defined, namely, 具体的表现形式。

   $B = \{ (u, p) \mid u \in Np\}$

   B is a binary relation, $B \subseteq U \times U$.

To indicate the close relationship between binary relations and nearest neighborhood systems 没说明白+1

6.2 Database Organization

On the top level, our data organization is different from that of [BrewerNash88]. Let CIR be the conflict of interests relation (e.g., provided by Table 9)

(a) "At the lowest level, we consider individual items of information, each concerning a single corporation." "We will refer to the files in which such information is stored as objects."

(b) "At the intermediate level, we group all objects which concern the same corporation together into what we call a company dataset."

(c) At the highest level we associate with each company dataset, say X, a nearest neighborhood, called Conflict of Interest Neighborhood of X,

$CIN(X) = \{ Y \mid (X, Y) \in CIR\}$, the set of all company datasets that are "in weighted conflict of interest to" X.

1.在最低层次上，我们考虑单独的信息项目，每一项都涉及单个公司。我们将存储信息的文件称为对象。
2.在中间层，我们将所有于同一个公司相关的对象组合在一起，并称之为公司的数据集。
3.在最高层，我们将每一个公司的数据集成为X，一个最近邻居成为X的利益冲突邻居。CIN(X) 表示X的所有利益冲突

6.3. Chinese Wall Security Policy Model

S：表示集合；
O：表示对象集合；
Oj：表示一个对象；
X(Oj)：表示Oj的公司数据集；如果X是可以理解的，我们可以简洁的使用X表示。
N：矩阵N表示代理S和对象集合O的关系矩阵，矩阵中的元素的所有可能取值为{0,1,-1}。
R(Si, Oj)：表示代理Si请求访问Oj的信息集。

We recall the new Chinese security policy model from [Lin89]. Let S be a set of agents, and O a set of objects. Let Oj be an object. Let X(Oj) [or simply Xj] be the company dataset of object Oj. When the object is understood, we may simply use X. Let N be a matrix with element N(i,j) corresponding to the members of $S \times O$, where the value of N(i,j) belongs to $\boxed{M=M=\{-1, 0, 1\}}$. Let a request to access an object Oj by the agent Si be denoted by R(Si,Oj), or R(i,j).

这表达形式实在是让人看不懂

中国墙安全策略模型是一个四元组集合：
1.初始化，N的所有元素取值为-1
2.如果R(i,j)允许，N(i,j) = 1
3.如果R(i,j)不允许，N(i,j) = 0
4.如果R(i,j)允许，且N的第i行发生以下变化：
a.N(i,j) = 1
b.N(i,h) = 0, if N(i,h) =-1 and X(Oh) in CIR(X(Oi)).

Oo表示所有净化信息的数据集，Oo可以被任何S代理/主体访问，为了避免间接破坏中国墙安全策略，我们强制增加以下条件：
代理Si可以访问任意对象Ob，当且仅当N(i,b)不为0，且并不存在对象Oa（N(i,a)不为0），且a不和b或o相同。

Definition A Chinese Wall Security Policy Model is a 4-tuple (S, O, N, l
satisfied.

(CW1) Initially N(i,j) = -1 for all i, j.
(CW2) If N(i,j) =1, R(i,j) is granted
(CW3) If N(i,j) =0, R(i,j) is denied
(CW4) If N(i,j) = -1, R(i,j) is granted and at the same time the i-th row of N h

a. N(i,j) = 1,
b. N(i,h) = 0, if N(i,h) = -1 and X(Oh) in CIR(X(Oi)). [Explicitly encoding the denials of authorization]

As in [BrewerNash88], we will use object Oo to denote the dataset of all sanitized information; Oo is accessible to any Subject. To avoid the indirect violation of Chinese Wall security policy, we impose the following axiom

(CW5) Write access to any object Ob by an agent Si is permitted if and only if $N(i,b) \neq 0$,
and there is no object Oa such that $N(i,a) \neq 0$, where a is not equal to either b or o.

Remark:

(1) If all N(*,*) are not equal to -1 (i.e. after all agents have accessed some objects), then N(*,*) is just like the usual access matrix with denials taking precedence.

(2) Note that the model does not allow the system to update the N(i,j) if Si has authorized to access Oj. However, in practice, we may "sanitize" the agent Si (if after a long period of time the agent Si has never accessed Oj again) and reinitialize the row N(i,*).

(CW6) Unless sanitized by authority, the only value of N(i,j) can be updated is N(i,j) = -1.

除非被权威机构净化，否则N(i,j)的值只能被更新为-1

We quote, as an example, some theorems of [Lin89].

THEOREM 6.3.1. Once a subject Si has accessed an object Oj, the only other objects accessible by Si lie outside of CI(Xj), or equivalently, lie within the same company dataset or outside of CIN(Xj).

6.4. Weighted Version of Chinese Wall Secuirity Policy Model

We some weighted version of [Lin89] and [BrewerNash88].

6.4.1. Weighted binary relations and weighted neighborhood systems

We will focus on a particular binary relation, namely, weighted conflict of interests relation (WCIR) and weighted conflict of interests neighborhood system (WCIN)

1. A weighted binary relation is a map

$$WCIR: U \times U \rightarrow [0, 1]$$

2. A weighted nearest neighborhood at p is a map

$$WCINp: U \rightarrow [0, 1]$$

3. A weighted nearest neighborhood system: To each point p, we associate a weighted nearest neighborhood

$WCIN: p \to WCINp$

4. A weighted binary relation defines a weighted nearest neighborhood system,

$p \to WCINp$; $WCINp(u) = WCIR(u, p)$

and vice versa

$WCIR: U \times U \to [0, 1]$; $WCIR(u, p) = WCINp(u)$

Mathematically, these weighted objects are equivalent to fuzzy objects. Since no values are used for measuring fuzziness, we use "weighted" terms.

6.4.2. The Model

All organization is basically the same as classical case. We only have to change the notion of binary relations and neighborhoods to the weighted forms. Let S be a set of agents, and O a set of objects. Let Oj be an object. Let X(Oj) [or simply Xj] be the company dataset of object Oj. When the object is understood, we may simply use X. To each company dataset, say X, a weighted nearest neighborhood, denoted by WCIN(X) (Weighted Conflict of Interest Neighborhood of X) is associated. Let N be a matrix with element N(i,j) corresponding to the members of $S \times O$, where the value of N(i,j) belongs to M={-1, 0, 1}. Let a request to access an object Oj by the agent Si be denoted by R(Si,Oj), or R(i,j). A Weighted Chinese Wall Security Policy Model is nearly the same as un-weighted one. The axiom looks the same with minor adjustments, howevere, it is based on a weighted binary relation.

(CW1) Initially N(i,j) = -1 for all i, j.
(CW2) If N(i,j) =1, R(i,j) is granted
(CW3) If N(i,j)=0, R(i,j) is denied
(CW4) If N(i,j) = -1, R(i,j) is granted and at the same time the i-th row of N has to be updated as follows:

a. N(i,j) = 1,
b. N(i,h) = 0, if N(i,h) = -1 and WCIR(X(Oh),(X(Oj)) $\geq$ threshhold.
[Explicitly encoding the denials of authorization]

(CW5) Write access to any object Ob by an agent Si is permitted if and only if N(i,b) $\neq$ 0, and there is no object Oa such that N(i,a) $\neq$ 0, where a is not equal to either b or o.

(CW6) Unless sanitized by authority, the only value of N(i,j) can be updated is N(i,j) = -1.

THEOREM 6.1. Once an agent Si has accessed an object Oj, the only other objects Ok accessible by Si have the weight WCIR(Ok, Oj)$\leq$ threshold.

Theorem 2 of [BrewerNash88] is a corollary of its Theorem 1. In this new setting, Theorem 2 cannot be true literally. However, we can proceed analogously. We say a company dataset X is accessible to a agent S if an object O in X is accessible to S. Then we can paraphrase Theorem 2 of [BrewerNash88] as follows.

THEOREM 6.2. If Xj is accessible to agent Si, then Si cannot access any other company dataset Xk provided WCIR(Xj,Xk) $\geq$ the threshold.

We cannot carry Theorem 3 of [BrewerNash88] over here. We have the following estimation:

THEOREM 6.3. If there are n company datasets in WCIN(X), then the minimum number of agents which will allow every object to be accessed by at least one agent is n.

THEOREM 6.4. The flow of unsanitized information is confined to its own company data set; sanitized information may, however, flow freely through the system.

6.5. The Model for the E-business Example

6.5.1. Weighted Example

(1) The set of all objects

U = {eshop1.com, eshop2.com, eshop3.com, and eshop4.com, eshop5.com }.

(2) The set of weighted Conflict of Interest Neighborhoods WCIN(-) can be read from table 8 for example, WCIN(eshop1.com) is a map, that is read from the first row,

eshop1 $\rightarrow$ 0
eshop2 $\rightarrow$0.04
eshop3 $\rightarrow$0.20
eshop4 $\rightarrow$0.08
eshop5 $\rightarrow$0.07

(3) The company datasets = the universe

6.4.2 De weighted Example

This model is the model after evaluation with thresholds:

(1) The set of all objects

U = {eshop1.com, eshop2.com, eshop3.com, eshop4.com, eshop5.com }.

(2) The set of Conflict of Interest Neighborhoods CIN(-) can be read from Table 9 for example, CIN(eshop1.com) is a set, that is read from the first row,

CIN(eshop1.com) ={eshop3.com}
CIN(eshop2.com) ={eshop3.com, eshop4.com, eshop5.com }.
CIN(eshop3.com) ={eshop1.com, eshop2.com, eshop4.com}.
CIN(eshop4.com) ={eshop2.com, eshop3.com}.
CIN(eshop5.com) ={eshop2.com}.

(3) The company datasets = the universe

6. CONCLUSIONS

The idea behind Brewer and Nash was an excellent approach to the commercial security problem. Their innovation is still enlightening. In this paper, we use Pawlak's style of analysis to get a weighted conflict of interests relation. By "defuzzification" using threshold, we get a honest conflict of interest relation.

REFERENCES

[BrewerNash88] David D. C. Brewer and Michael J. Nash: "The Chinese Wall Security Policy" IEEE Symposium on Security and Privacy, Oakland, 1988, pp 206-214,

[Casti89] Casti, J.L. (1989). "Alternative Realities -- Mathematical Models of Nature and Man", John Wiley and Sons.

[Lin89] T. Y. Lin, "Chinese Wall Security Policy--An Aggressive Model", Proceedings of the Fifth Aerospace Computer Security Application Conference, December 4-8, 1989, pp. 286-293.

[Lunt88] Teresa F. Lunt : Access Control Polices for Database Systems, the 1988 Workshop on Database Security, Kingston, Ontario, Canada, Oct, 1988