计算机研究与发展
Journal of Computer Research and Development
ISSN 1000-1239/CN 11-1777/TP
44(4):598~605, 2007

TDDSS 中可信模型及其分析

田俊峰 肖 冰 马晓雪 王子贤
(河北大学数学与计算机学院 保定 071002)
(tjf@hbu.edu.cn)

The Trust Model and Its Analysis in TDDSS

Tian Junfeng, Xiao Bing, Ma Xiaoxue, and Wang Zixian
(*College of Mathematics and Computers, Hebei University, Baoding* 071002)

Abstract A new model—trusted distributed database server system (TDDSS) is presented in this paper. This new model breaks the situation in which trusted computing is always applied in PC. It introduces trusted mechanism from PC into distributed database server system (DDSS). And this model helps to find out a new application area for the trusted computing. Also set up are a complete model of TDDSS and the layers of trusted-chain in trusted distributed database server system with trusted computing technology. Trusted-chain presents assurance for the transfer of the trust. It transfers from the trusted root to the interior of the system. Role-based mechanism, which is recognized by more and more people, is posed in management in TDDSS. It defines a role for every client server, and role-based mechanism proposes a more flexible and scalable permission management model. At the same time, the mechanisms of authentication and log are improved in this system. Especially, two-level of logs is used in TDDSS. It improves the security and makes the information seeking much easier. In conclusion, a complete model for the application of trusted computing in computing systems is given. Furthermore the whole system model is evaluated with mathematics method, and its feasibility and efficiency are proved accurately.

Key words distributed database; trusted evaluation; role-based management

摘 要 可信分布式数据库服务器系统 TDDSS(trusted distributed database server system)顺应了目前可信计算的研究从单机到网络的研究趋势,在分布式数据库服务器系统 DDSS(distributed database server system)中引入可信机制. 分布式系统是一个正处于发展中的系统,许多机制有待进一步研究和完善. 在分布式系统中引入可信性存在许多困难,为此对分布式系统开展可信性研究具有重大意义. 利用可信技术,引入可信第三方,建立了完整的 TDDSS 模型和多层次系统信任链模型. 在系统管理方面使用了角色管理机制. 与此同时,改进了相应的系统认证和日志管理体系. 为今后可信在计算机系统中的应用提供了完整的可靠模型,并对建立的 TDDSS 模型进行了整体的数学评估和科学检测.

关键词 分布式数据库;可信评估;角色管理

中图法分类号 TP309

随着信息技术特别是攻防技术的发展,就信息系统本身而言,并不能完全做到对系统的全方位保护. 中国国家信息安全测评认证中心提供的调查结果显示,信息安全问题在很多情况下是由内部人员造成的,而非外来黑客和病毒引起. 合法用户很容易接触到计算机系统内部,对数据进行访问、修改甚至破坏,且事后不易被发现,造成比外部攻击更大的威胁. 为了保证计算机资源只能被合法用户合法地使用,2003 年 IBM, Intel, AMD, HP 和微软等共同倡导成立了可信计算组织 TCG(trusted computing group)[1-2],其目的是定义未来通用计算平台上的一种可信计算环境,通过建立这种可信计算环境来提

收稿日期:2006-07-17;修回日期:2007-01-12
基金项目:河北省自然科学基金项目(F2004000133)

供各种安全操作功能,解决各种安全问题. 现在已经有 200 多个企业加入了 TCG,可信计算机已经进入了实际应用的阶段[3-4].

目前,国内有关可信计算和可信计算平台的研究工作主要集中于单机,提出了多种新型可信计算机和可信软件[5-7]等.

本文利用可信技术,在分布式数据库服务器系统 DDSS(distributed database server system)[8]中引入可信认证第三方(即认证授权方),建立系统多层次信任链结构,改进系统存取控制方式,对客户端实行角色管理机制、认证机制,应用两级日志管理等技术,提出可信分布式数据库服务器系统 TDDSS(trusted DDSS)的完整模型.

具有的优点是能够提高系统资源(包括所有软件资源和硬件资源)的安全性和可靠性,有效防止非正常访问. 与此同时,不过多增加系统运行成本,更不影响到系统原有正常服务.

本文使用数学方法对 TDDSS 进行性能评估,并与 DDSS 进行比较,定量说明了应用可信技术、引入可信第三方之后,系统整体安全性和可靠性提高,对于非正常访问具有了比以前更强的抵御能力.

1 TDDSS

1.1 系统的结构模型

可信分布式数据库服务器系统 TDDSS(trusted distributed database server system)是在 C/S 模式下实现的一个可信分布式信息管理系统. TDDSS 主要由主服务器节点、多子服务器节点和可信授权机节点构成. 逻辑结构如图 1 所示:

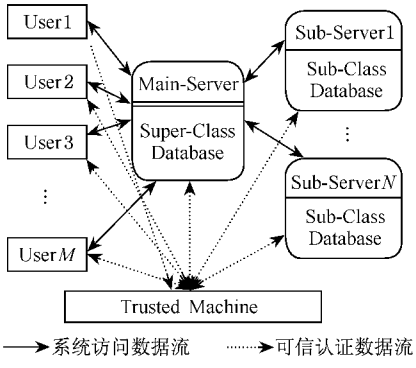


Fig. 1 The structure of TDDSS.

图 1 TDDSS 系统结构框图

1) 主服务器

主服务器是以同构双机热备份方式工作,存放的是一些基本的公共信息,其数据库的规模相对不是很大,但是访问频率较高,称为超类数据库[8]. 主服务器还生成一张关于 TDDSS 的结构映射表,其中有系统中各个服务器节点的基本信息.

结构映射表数据结构如下:

```
Structure Map_table_node
{int server_number ;/* 服务器标识 */
char IP_address ;/* 服务器的 IP 地址 */
int information_type ;/* 信息类型,与数据库相关 */
int backup_server_number ;/* 备份数据库标识 */
int status ;/* 该数据库当前状态 */
} ;Map_tabale[N] ;
```

2) 子服务器

子服务器中数据库存放的是大量的专用数据,称为子类数据库[8],其访问频率较低,但是数据规模一般较大. 系统中所有的子服务器是同构的,呈单向循环冗余备份关系.

3) 可信授权机

TDDSS 使用可信计算机作为可信授权机,主要功能用来验证系统中各节点(包括服务器和客户端)的可信性以及运行过程中操作的可信性,并管理系统 Request 权限表(Request 表记录系统中所有客户端的访问权限,是在客户端加入系统时写入). 特别指出,为了方便权限的管理,授权机采用的是可信角色管理机制[9]模型.

TDDSS 中所有客户端都拥有自己的访问权限,这些权限通过客户端对应的角色(role)来体现,并进行管理. 服务端定义并管理 role,同时根据 role 定制特定的安全策略. role 在这个框架中是一个具有权利和义务内容的实体. 每一个 role 自身包含两重映射.

映射 1:角色(role)→访问权限.

映射 2:客户端→角色(role).

角色存储管理采用的是邻接表的结构,使用 4 位二进制码来表示相应角色读写权限,其逻辑结构如图 2 所示:

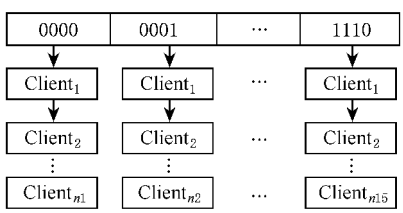


Fig. 2 The linklist of the roles.

图 2 TDDSS 角色链表

第 1 位表示是否有对主服务器读的权限. “0”表示有读主服务器中数据的权限;‘1’表示无法读取主服务器中数据. 第 2 位表示是否有对主服务器写的权限,第 3、第 4 位分别表示是否有对子服务器读、写的权限.

只利用邻接表并不能具体区分子服务器,所以我们使用读写矩阵来具体区分子服务器的读写权限. 读写矩阵中的行表示客户端 $1\sim m$,列表示服务器 $1\sim n$. 矩阵的元素为‘1’时,表示该元素所在行的客户端对该元素所在列的服务器有读/写操作的权限,为‘0’时说明没有访问的权限. 使用两个矩阵分别表示对子服务器的读和写的两种权限. 当服务器数量很多的时候,多数客户端一般只能访问个别服务器,这时该矩阵是稀疏矩阵,我们可以简化存储,只需存储元素‘1’所在位置. 其数据结构如图 3 所示,这种存储很直观,查找也很容易实现.

Role:

role	firstclient

```
typedef struct mode
 {
   char role[4];
   client_node * firstclient;
 } role_node;
```

(a)

Client:

client	next

```
typedef struct cnode
 {
   int number,
   struct cnode * next;
 } client_next;
```

(b)

Fig. 3 The data structure of roles and clients. (a) The data structure of roles and (b) The data structure of Clients.

图 3 角色表与客户端表的数据结构. (a) 角色表的数据结构;(b) 客户端表的数据结构

使用角色管理机制保证了 TDDSS 的快捷运行,同时每个客户端必须严格按照 role 进行访问,也使 TDDSS 的安全性得到了保障.

4) 数据访问中间件

主服务器节点、可信授权机节点和每个子服务器节点都设计有一个数据访问中间件[8],它定义了一系列应用程序接口,它的使用解决了系统的通信问题. 我们把节点发出认证请求和接受认证结果的部件也放到了数据访问中间件里,使其和计算机内部数据分离,保障数据的安全和结构的简明. 数据访问中间件的逻辑结构如图 4 所示:

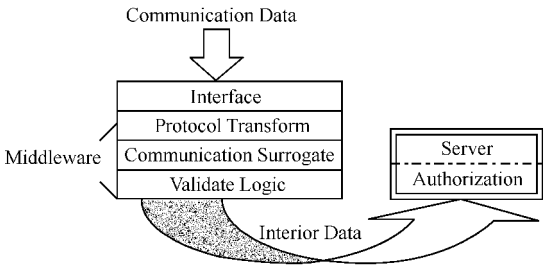


Fig. 4 The logic structure of the middleware.

图 4 数据访问中间件逻辑结构图

从图 4 中可以看出,有了数据访问中间件的保护,外界通信数据并不能直接进入系统内部,多了一层对外部攻击的防御,从而保证了系统安全性.

1.2 系统的运行模型

TDDSS 有可信认证内容,所以这里集中介绍当客户端需要对 TDDSS 进行访问时,系统进行认证的过程:

Step1. 客户端向 TDDSS 发出访问请求,主服务器接收到后(具体是由主服务器的数据访问中间件接收),向可信授权机发送一个查询请求,询问该客户端是否有访问 TDDSS 权限,发送的查询请求为二元组,数据结构如下:

```
typedef struct renode
 {
 int server;/* 主服务器标识 */
 int client;/* 客户端标识 */
 } request_node;
```

Step2. 授权机在 Request 权限表中进行核对,确定 Request 权限表中是否有该客户端的认证信息;

Step3. 如果有认证信息就返回‘Y’,主服务器允许进入 TDDSS,并开始由主服务器分析命令,否则,返回拒绝进入信息;

Step4. 允许进入 TDDSS 后,主服务器分析命令,确定其要访问的信息内容,然后通过查找 TDDSS 结构映射表,把命令转给拥有相应数据和服务的服务器去(由该服务器数据访问中间件接收);

Step5. 接到访问请求的服务器在被访问前,要先向可信授权机发送一个查询请求,询问发送访问请求的客户端是否有访问该服务器的读/写权限,此处的查询请求为三元组,数据结构如下:

```
typedef struct renode
 {
int server;/* 服务器标识 */
```

int *client*；/ * 客户端标识 * /

char *re*[4]；/ * 具体请求 * /

} *request_node*；

Step6. 授权机查找子服务器对应读/写矩阵，如果有相应访问权限，则返回“Y”，否则，返回拒绝访问信息；

Step7. 以上认证过程都通过后，客户端就可以进入正式的访问执行阶段.

在客户端的访问进行过程中，授权机还有监控的作用. 处于通话状态的服务端和客户端，如果有一方认为对方比较可疑，可以向授权机提出质疑，要求授权机对对方身份进行核对. 授权机通过对权限的核查，以及通过对其日志的审查来判断可疑方身份，如果断定是非法的，立即撤销通话，或者将其引入相应处理系统中(比如有陷阱系统的可以将其引入陷阱) 如果身份合法，就告知申请方可以继续通话.

1.3 系统信任链

TCG 提出“信任链”和“信任根”的概念，认为如果从一个初始的“信任根”出发，在平台计算环境下的每一次转换信任可以通过“信任链”以传递的方式保持下去不被破坏，那么系统平台就是可信的.

TDDSS 是分为 4 个模块来建立信任链的，分别为：

模块 1. 授权机模块.

模块 2. 主服务器模块.

模块 3. 子服务器模块.

模块 4. 客户端模块.

以这 4 个模块为基础，提出了 3 层信任链来保证 TDDSS 可信性.

1) 授权机内部信任链

本文在 TDDSS 中使用的是一台可信计算机来做授权机，所以系统第 1 层次信任链(授权机内部信任链)实际上就是可信计算机内部信任链. 这个层次信任链是 TDDSS 可信的基础，如果没有实体本身物理上的可信，就不可能将信任进行传递，那么系统的可信也就不能保证.

2) 模块内部的信任链

每个模块内部都包括一条自己的信任链，这样就把授权机的信任传递到系统中的每个模块里. 在这个层次上，4 个模块产生 3 条信任链：

信任链 1. 授权机→主服务器.

信任链 2. 授权机→子服务器.

信任链 3. 授权机→客户端.

同时产生对应 3 个认证：

认证 1. 授权机对主服务器的认证.

认证 2. 授权机对子服务器的认证.

认证 3. 授权机对客户端的认证.

这里是由可信授权机模块直接认证主服务器模块、子服务器模块和客户端模块，信任就从授权机模块内部传递到了 TDDSS 每一个模块中. 这个层次信任链传递模型如图 5 所示：

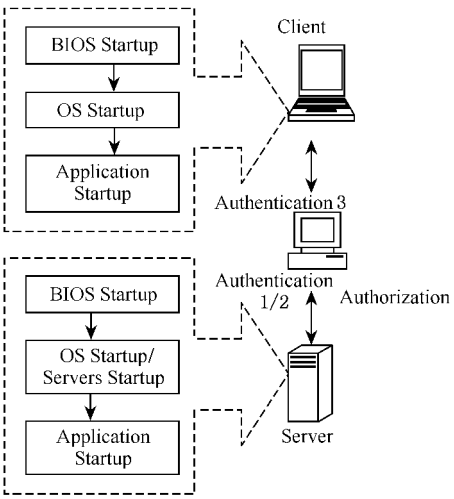


Fig. 5 The second layer of trusted chain.

图 5 TDDSS 第 2 层次信任链逻辑结构

3) 整体模块之间的信任链

这一层次信任链主要是将第 2 层次 3 条信任链整合在一起，也就是让主服务器、子服务器和客户端不仅与授权机有信任关系，它们之间也存在信任传递. 通过加入第 3 层次信任链，把 TDDSS 的各个模块串成了一个有机整体，也使信任能够从可信计算机的可信根传递到 TDDSS 的各个部分，从而生成整个系统的完整信任链. 这个层次信任链逻辑结构如图 6 所示：

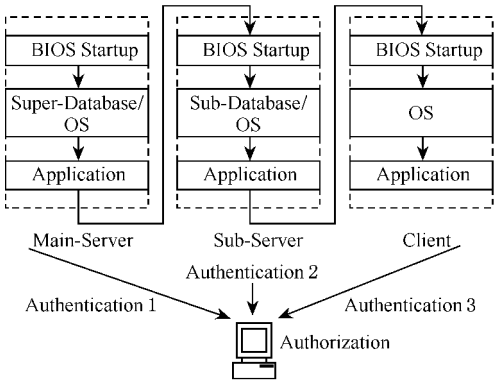


Fig. 6 The trusted chain of TDDSS.

图 6 TDDSS 第 3 条信任链逻辑结构

在以上介绍的 3 层信任链中，第 1 层次信任链是可信的物理保证；第 2 层次信任链是可信的延伸

和初步传递;第 3 层次信任链是可信的贯穿,它使 TDDSS 成为可信的整体. 通过这 3 层信任链一级认证一级、一级信任一级,最终将可信扩展到整个系统.

2 可信性分析与比较

我们对 TDDSS 的安全性进行数学上的证明,希望通过对系统整体定量分析得出更精确的可以广泛接受的描述. 不仅仅使系统的安全性、可信性停留在一个定性的阶段.

目前,关于信任的度量主要有基于概率统计的可信模型,基于模糊数学的数学模型[10],基于主观逻辑、证据理论的可信模型,以及基于如软件行为学的可信模型[11]等. 本文采用概率统计的可信度量模型进行分析研究.

2.1 系统可信性分析

为了方便说明问题,先给出如图 7 所示整个可信授权流程:

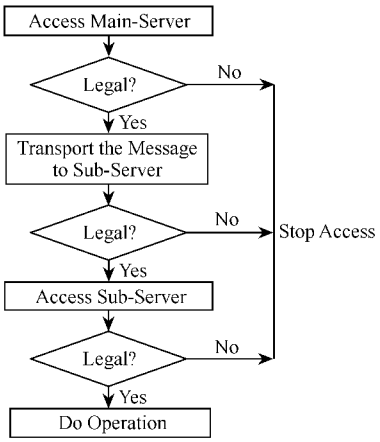


Fig. 7 The flow chart of TDDSS.

图 7 TDDSS 可信授权流程

由流程图可以看出,对于一次访问,系统共有 3 次认证,而 DDSS 只提供了一次(相当于 TDDSS 第 3 次认证).

虽然 TDDSS 的认证为 3 层,但是没有绝对安全的系统,同样可能被攻击者破坏. 下面就用数学方法具体分析系统的安全性,并与 DDSS 作比较. 在分析比较之前,需要如下假设.

假设 1:攻击的产生服从 Poisson 分布.

假设 2:所有攻击造成的危害程度只与其攻破的认证级数有关,而与攻击本身性质或攻击者身份等无关.

对于可信性的比较,可以从能够成功检测出非正常访问的能力的角度来讨论. 为了方便考察,需要在 DDSS 和 TDDSS 运行过程中,分别提取一个系统被访问的样本,样本中系统接收到的访问的数量设为 N(其中包括正常访问和非正常访问). 同时还需要作相应假设:

假设 3:在样本中出现非法用户访问或者合法用户的非法访问(统称非正常访问)总体概率为 $P(0\leqslant P\leqslant 1)$,则出现的非正常访问的次数可以用 $N\times P$ 表示.

假设 4:DDSS 能够成功阻止的非正常访问数量为 m_1,不能够成功阻止的数量为 n_1,可知 $m_1+n_1=N\times P$.

假设 5:TDDSS 能够成功阻止的非正常访问数量为 m_2,不能够成功阻止的数量为 n_2,同样可知 $m_2+n_2=N\times P$.

为了表述,还需要引入以下变量.

变量 1:用 β_1 和 β_2 来分别表示 DDSS 和 TDDSS 检测非正常访问成功的概率的期望. 我们希望成功检测的真正概率要$\geqslant\beta_1(\beta_2)$(即希望真正的概率要高于概率的期望).

变量 2:用 α_1 和 α_2 来分别表示 DDSS 和 TDDSS 成功检测非正常访问的期望. 可以知道成功的期望值越高,说明检测成功的能力越大. 计算如下:

$$\begin{aligned}\alpha_1 &= (m_1+n_1)\beta_1,\\ \alpha_2 &= (m_2+n_2)\beta_2.\end{aligned}\tag{1}$$

变量 3:用 V_a 和 V_b 来分别表示 DDSS 和 TDDSS 成功检测非正常访问的概率分布. 由概率分布公式可以得出:

$$\begin{aligned}V_a &= \sum_{l=1}^{m_1} C_{m_1+n_1}^{l}\beta_1^{l}(1-\beta_1)^{m_1+n_1-l},\\ V_b &= \sum_{l=1}^{m_2} C_{m_2+n_2}^{l}\beta_2^{l}(1-\beta_2)^{m_2+n_2-l}.\end{aligned}\tag{2}$$

变量 4:TDDSS 因为有 3 次认证,所以 β_2 是由 3 部分组成,即第 1 级认证成功的概率、第 2 级认证成功的概率和第 3 级认证成功的概率,分别用 P_1,P_2 和 P_3 来表示. 分析 TDDSS 层次模型,得到如下表达式:

$$\beta_2 = P_1+(1-P_1)P_2+(1-P_1)(1-P_2)P_3.\tag{3}$$

DDSS 的认证层次仅一层,相当于 TDDSS 的第 3 层认证,有如下表示:

$$\beta_1 = P_3.\tag{4}$$

现在需要做的是比较 TDDSS 对于 DDSS 来说,系统能够成功拦截非正常访问的概率是否有所提

高,从而证明可信机制对计算机系统的作用. 为了更明显看出概率之间的关系,对式(3)(4)两式作差,进行相应推导结果如下:

$$\beta_2 - \beta_1 = P_1 + (1 - P_1)P_2 + (1 - P_1)(1 - P_2)P_3 - P_3 = (1 - P_2)(1 - P_3)P_1 + (1 - P_3)P_2 > 0. \tag{5}$$

设 $P_1 = P_2 = P_3 = p$,由式(3)(4)得出如图 8 所示的比较曲线图:

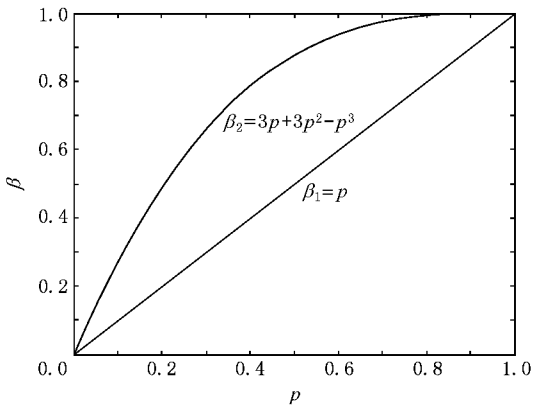


Fig. 8 The graph of β_1 and β_2.

图 8 β_1,β_2 比较曲线图

从图 8 可以看到,β_1 曲线在区间(0,1)内一直处于 β_2 曲线下方. 即 $P_1 = P_2 = P_3 = p$ 时,在区间(0,1),始终有 $\beta_1 < \beta_2$.

由式(5)和图 8 就得出了 β_1 和 β_2 大小关系,即 $\beta_1 < \beta_2$. 既然 β_1 和 β_2 大小关系已经确定,由式(1)可知,在(0,1)内始终有 $\alpha_1 < \alpha_2$.

这样就直接用数学方法证明了两系统抵御非法访问能力的不同,TDDSS 明显高于 DDSS. 说明引入可信机制之后,计算机系统成功拦截非正常访问的概率有了显著提高.

还可以从另外的角度,更进一步证明 TDDSS 安全性提高. 由于认证层数的分别,每次认证起的作用也有所不同,为了区分这些不同,定义危险系数概念:

定义 1. 我们把某一级认证失效造成的危害程度称为危险系数,使用符号 K 来表示,其中 $K \in [0,1]$. $K = 0$ 表示对系统没有危害;$K = 1$ 表示系统保护完全被突破,即最大危害程度.

如表 1 所示,对于 TDDSS,设第 1 级认证失效时危险系数 $K_1 = 0.25$,第 2 级认证失效时危险系数 $K_2 = 0.5$,第 3 级认证失效时危险系数 $K_3 = 1$,是递增关系.(攻击越接近中心,说明这次攻击被识破越晚,危害越大;越是靠近中心的层次,失效后对整个系统的危害就越大).

Table 1 The Hazard Coefficient of TDDSS

表 1 TDDSS 认证级数以及对应危险系数

Trusted Level	Hazard Coefficient(K)
The first certification	0.25
The second certification	0.5
The third certification	1

对于 DDSS 只有一层认证,保护失效后系统就处于危险,所以设 $K = 1$.

利用危险系数分别计算 DDSS 和 TDDSS 危险性的变化,提出相应变量.

变量 5:分别设 W_1 和 W_2 为 DDSS 和 TDDSS 的总体危险量.

使用危险系数作为参数,求出 DDSS 和 TDDSS 总体危险量,结果如下:

$$W_1 = 0.25 + 0.5 + (1 - P_3) \times 1 = 1.75 - P_3, \tag{6}$$

$$W_2 = (1 - P_1) \times 0.25 + (1 - P_1)(1 - P_2) \times 0.5 + (1 - P_1)(1 - P_2)(1 - P_3) = 1.75 - 1.75P_1 - 1.5P_2 + 1.5P_1P_2 - P_3 + P_1P_3 + P_2P_3 - P_1P_2P_3. \tag{7}$$

将式(6)(7)作差,经过相应数学推导结果如下:

$$W_1 - W_2 = (1.75 - P_3) - (1.75 - 1.75P_1 - 1.5P_2 + 1.5P_1P_2 - P_3 + P_1P_3 + P_2P_3 - P_1P_2P_3) = (1 - P_1)P_2(1.5 - P_3) + P_1(1.75 - P_3) > 0. \tag{8}$$

设 $P_1 = P_2 = P_3 = p$,由式(6)(7)得出如图 9 所示的比较曲线图:

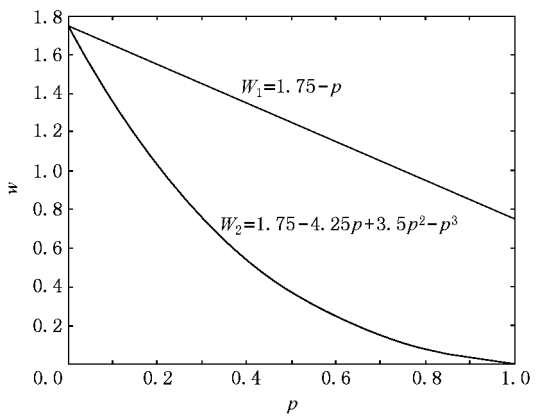


Fig. 9 The graph of W_1 and W_2.

图 9 W_1,W_2 比较曲线图

在区间(0,1),W_1 曲线始终位于 W_2 上方($W_1 > W_2$). 即 $P_1 = P_2 = P_3 = p$ 时,DDSS 危险量高于

TDDSS.综合式(8)和图9可以得出TDDSS相对于DDSS其总体危险量明显减小.说明了可信技术的引入,使得服务器系统被非法访问的危险性降低,提高了系统可靠性、安全性.

从以上两个方面证明知道,虽然增加了认证层次,TDDSS比DDSS运行系统开销要相对增大,但可信性与DDSS比较却得到明显提高.

2.2 系统测试分析

1)整体检测的数据采集

对系统(包括DDSS和TDDSS)进行整体检测,目的主要是为了验证DDSS和TDDSS对非正常访问的屏蔽作用.在人工测试时,使用探测器对系统工作进行追踪,分别取7次数据如表2、表3所示:

Table 2 The Test Data of DDSS

表2 DDSS测试数据结果

Access	Time(s)	Normal Access	Abnormal Access	Attack
10000	302	9901	99	5
10000	1032	9856	144	8
10000	654	9847	153	19
10000	698	9922	78	1
10000	1385	9900	100	7
10000	236	9734	266	12
10000	850	9803	197	17

Table 3 The Test Data of TDDSS

表3 TDDSS测试数据结果

Access	Time(s)	Normal Access	Abnormal Access	Attack
10000	587	9786	214	5
10000	796	9847	153	0
10000	1420	9920	80	1
10000	982	9863	137	0
10000	1002	9901	99	3
10000	976	9910	90	2
10000	890	9874	126	0

2)检测数据分析

由于攻击产生服从Poisson分布,可以认为7次采集是来自参数分别为λ_1,λ_2的Poisson分布样本,求λ矩估计量如下:

因为$\overline{X}$是λ是无偏估计

所以 $\hat{\lambda}=EX=\overline{X}=\frac{1}{n}\sum_{i=1}^{n}X_i$,

得 $\hat{\lambda}_1=\frac{1}{7}\sum_{i=1}^{7}X_i=\frac{69}{7}=9.857\approx10$,

及 $\hat{\lambda}_2=\frac{1}{7}\sum_{i=1}^{7}X_i=\frac{11}{7}=1.571\approx1.5$.

对于DDSS其万次访问中产生攻击的次数期望约为10次,而TDDSS仅约1.5次,相差幅度达到一个数量级.通过查表可知对于DDSS其万次访问中没有形成攻击的概率为0.000045,而TDDSS为0.223130.

3 结束语

本文用数学的方法,具体说是概率统计的可信性度量模型,精确地给出DDSS和TDDSS可信性评估,评估结果证明了可信机制的作用.它在一定程度上解决了分布式数据库系统在开放环境下非正常访问的问题,在不改变系统正常工作前提下,提高了系统可信性.虽然可信机制增加了系统访问开销,但是在现今这个对于网络安全要求很高的大环境中,还是有相当大的适用空间.这种思想不仅可以应用于TDDSS系统,对于大多数开放式系统都有参考价值.

今后工作:

1)需要继续改进角色管理机制,合理安排冗余,减少存储空间,提高搜索效率,通过应用更合理的机制使得角色管理更为安全.

2)继续完善本文可信思想,使其发展成为一种可以广泛应用的思想.并且能够扩展到可信网络[12]中去.

参 考 文 献

[1] Hu Huaping, Jin Shiyao, Wang Zhaofu. Dependability study of distributed computer systems [J]. Comprter Engneering and Science, 1998, 20(1): 48-53 (in Chinese)
(胡华平,金士尧,王召福.分布式系统的可信性研究[J].计算机工程与科学,1998,20(1):48-53)

[2] Trusted Computing Platform Alliance (TCPA). Main Specification Version 1.1b [OL]. http://www.trustcomputinggroup.or/home, 2005-04-03

[3] Intel Corporation. Lagrande technology architectural overview [OL]. http://www.intel.com/technology/security/, 2005-05-01

[4] Microsoft. Trusted platform module servises in windows longhorn [OL]. http://www.microsoft.com/resources/ngscb/, 2005-04-25

[5] Chen Jun, Hou Zifeng, Wei Wei. Trusted computing platform architecture [J]. Journal of Wuhan University (Natural Science Edition), 2004, 50(S1): 23-26 (in Chinese)

(陈军，侯紫峰，韦卫. 可信赖计算平台体系结构[J]. 武汉大学学报(理学版)，2004，50(S1)：23-26)

[6] Huang Tao，Shen Changxiang. A trusted bootstrap scenario based trusted server [J]. Journal of Wuhan University (Natural Science Edition)，2004，50(S1)：12-14 (in Chinese)
(黄涛，沈昌祥. 一种基于可信服务器的可信引导方案[J]. 武汉大学学报(理学版)，2004，50(S1)：12-14)

[7] Zhang Huanguo，Wu Guoqing，Qin Zhongping，*et al*. A new type of secure microcomputer [J]. Journal of Wuhan University (Natural Science Edition)，2004，50(S1)：1-6 (in Chinese)
(张焕国，毋国庆，覃中平，等. 一种新型安全计算机[J]. 武汉大学学报(理学版)，2004，50(S1)：1-6)

[8] Tian Junfeng. The model of a distributed database server system [J]. Computer Engineering and Application，2003，39(23)：176-179 (in Chinese)
(田俊峰. 一种基于 c/s 模式的分布式数据库服务器系统模型[J]. 计算机工程与应用，2003，39(23)：176-179)

[9] Wang Yuan，Xu Feng，Lü Jian. Arts：A role-based trust-management system [J]. Journal of Wuhan University (Natural Science Edition)，2004，50(S1)：57-61 (in Chinese)
(王远，徐锋，吕建. Arts：一个基于角色的信任管理系统[J]. 武汉大学学报(理学版)，2004，50(S1)：57-61)

[10] Tang Wen，Chen Zhong. Research on subjective trust management model based on the fuzzy set theory [J]. Journal of Software，2003，14(8)：1401-1408 (in Chinese)
(唐文，陈钟. 基于模糊集合理论的主观信任管理模型研究[J]. 软件学报，2003，14(8)：1401-1408)

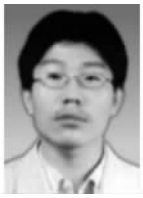
[11] Qu Yanwen. Software Behavior [C]. Beijing：The Electronic Industry Press，2004 (in Chinese)
(屈延文. 软件行为学[C]. 北京：电子工业出版社，2004)

[12] Lin Chuang，Peng Xuehai. Trusted network research [J]. Chinese Journal of Computers，2005，28(5)：751-758 (in Chinese)
(林闯，彭雪海. 可信网络研究[J]. 计算机学报，2005，28(5)：751-758)

Tian Junfeng，born in 1965. Professor and Ph. D. His main research interests include distributed computing and network technology.
田俊峰，1965 年生，博士，教授，主要研究方向为分布计算、网络技术.

Xiao Bing，born in 1982. M. S. candidate. Her main research interests include network technology and trusted computing.
肖　冰，1982 年生，硕士研究生，主要研究方向为网络安全、可信计算(xxbing@126.com).

Xa Xiaoxue，born in 1974. Master and assistant professor. Her main research interests include network technology and trusted computing.
马晓雪，1974 年生，硕士，助教，主要研究方向为网络技术与可信计算.



Wang Zixian，born in 1980. M. S. candidate. His main research interests include network technology and trusted computing.
王子贤，1980 年生，硕士研究生，主要研究方向为网络安全、可信计算.

Research Background

This project is sponsored by the Hebei Province Natural Science Foundation of China under grant No. F2004000133. The project is mainly on trusted computing. Its mission is to assure that the computer system resource should be use only by the legal user on the legal way，and to avoid that the illegal user to make use of the system at will. Nowadays，the work on the trusted computing centralizes on PC. However，this project imports trusted mechanism into distributed database server system for the first time.

In this paper，we present a model of TDDSS，and set up trusted third party for the system. Its aim is to make the trust transfer from the trusted root to the whole system by the trusted-chain. Simultaneity，mathematic way is employed to analyze the security and the reliability of the system.