可生存性MLS/DBMS中基于隐蔽通道的恶意事务检测

郑吉平[1], 秦小麟[2], 管致锦[2], 孙 瑾[3]
(1.清华大学计算机科学与技术系, 北京 100084; 2.南京航空航天大学计算机科学与技术系, 江苏南京 210016;
3.南京航空航天大学 民航学院, 江苏南京 210016)

摘 要: 多级安全数据库系统(MLS/DBMS)中并发控制协议并不能彻底消除所有的隐蔽通道.在隐蔽通道无法避免的情况下,已渗透的恶意事务可以利用隐蔽通道泄漏和篡改机密信息.为提高数据库的可生存性,首先分析了MLS/DBMS系统中的隐蔽通道,通过对真实情况的参数模拟和实验分析,结合恶意事务特征和隐蔽通道带宽的异常改变,给出可生存DBMS中的同谋事务和恶意事务的检测,并提出了同谋用户造成隐蔽通道传递性的机理以及恶意噪声事务对其的影响.

关键词: 多级关系模型; 隐蔽通道; 恶意事务; 同谋
中图分类号: TP392 文献标识码: A 文章编号: 0372-2112 (2009) 06-1264-06

Covert Channel based Malicious Transaction Detection in Survivable MLS/DBMS

ZHENG Ji-ping[1], QIN Xiao-lin[2], GUAN Zhi-jin[2], SUN Jin[3]
(1. *Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China;*
2. *Department of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, Jiangsu 210016, China;*
3. *College of Civil Aviation, Nanjing University of Aeronautics and Astronautics, Nanjing, Jiangsu 210016, China*)

Abstract: Current concurrency control protocols can not eliminate all covert channels in multi-level secure database management systems(MLS/DBMS). Existence of covert channels leads penetrated malicious transactions leak and interpolate confidential information. To improve database survivability, covert channels in MLS/DBMS are firstly analyzed. Then Conspired and malicious noise transactions can be detected based on malicious transaction characteristics and abnormal varieties of covert channel capacities by simulated parameters and experiments according to real systems. Further, transitive property of multi-conspiracies along with the influence of malicious noise transaction is analyzed.

Key words: multi-level secure model; covert channel; malicious transaction; conspiracy

1 引言

大多数安全数据库管理系统(DBMS)访问控制机制建立在多级关系模型基础之上[1,2].在多级安全(MLS)DBMS中,主体和客体被赋予不同的密级,并制定相关访问策略:作为数据库主体的事务不能读取高于其密级的数据客体;同时,事务主体只能修改同等安全级别的数据客体,即"向下读,同等写"[3].然而,共享数据客体,包括数据文件、记录和记录中的某个字段等,以及系统资源可能被不同安全级别事务利用以传递机密信息.已有的并发控制协议[4,5],如两段锁协议(2PL)、时间戳协议(TO)、带优先权的两段锁协议(2PL-HP)、乐观锁协议(OPT)、安全两段锁协议(S2PL)、多版本两段锁协议(MV2PL)、"双重"(Dual)方案等,在DBMS安全和性能上进行了平衡,即:为了确保安全性牺牲了DBMS性能.从并发控制角度,违反安全策略的信息流动即隐蔽通道难以避免.

另一方面,在信息战[7]前景下,传统DBMS安全机制的局限性以及攻击的智能性和协同性导致成功的攻击无法避免,数据库的可生存性已成为研究的热点[6].在"服务至上"的理念下,为确保事务在规定时间内或者关键核心事务的顺利完成,允许隐蔽通道存在[7~9].外

收稿日期: 2007-08-31; 修回日期: 2009-02-18
基金项目: 国家自然科学基金(No. 60673127); 国家863高技术研究发展计划(No. 2007AA01Z404); 江苏省支撑计划(No. BE2008135)

部非法攻击者以及潜藏在系统内部的滥用用户可能利用系统安全策略部分允许的隐蔽通道泄漏秘密信息, 为保证系统不被恶意行为进一步破坏并保证 DBMS 恢复到正常状态, 必须对已渗透的恶意用户行为进行检测.

本文研究可生存性 MLS/ DBMS 中系统安全策略部分受到破坏情况下存在的隐蔽通道, 根据必然存在的隐蔽通道检测恶意同谋事务和恶意噪声事务. 通过参数模拟以及实验分析, 为可生存性 MLS/ DBMS 中恶意事务的进一步隔离和感染事务的恢复打下理论基础和分析依据.

2　理论基础

2.1　MLS/ DBMS 模型

定义　MLS/ DBMS 模型[1, 3], 包括: 数据对象集合 $D=(x_1, x_2, \cdots, x_m)$, 事务集合 $T=(T_1, T_2, \cdots, T_n)$, 以及一组偏序的安全级别集合 S, 偏序关系表示为 $<$, D 和 T 上的映射 $F: D\cup T \rightarrow S$. 对于数据 x, $x\in D$, $L(x)\in S$.

在 MLS/ DBMS 中, 事务以及数据对象被赋予一个特定的安全级别并满足以下两个基本属性:

向下读属性: 一个事务仅能读取其安全级别受此事务安全级别支配的客体信息;

同等写属性: 一个事务仅能向同等安全级别的客体写信息.

2.2　隐蔽通道分析理论基础

根据 Shannon 信息理论[8, 10], 假定信号源输出量是一个随机离散量 $X=(x_1, x_2, \cdots, x_{k-1})$, $i=1, \cdots, k-1$. 假设每一个分量 x_i 的输出概率是 P_i, 则随机变量 X 的熵为:

$$H(X)=\sum_{i=0}^{K-1}P_i \log\frac{1}{P_i}$$

假设 X 是输入变量, Y 是输出变量, 则条件熵为:

$$H(X\mid Y)=\sum_j p(y_j)H(X\mid Y=y_j)$$
$$=-\sum_i\sum_j P(x_i, y_j)\log P(x_i\mid y_j)$$

则两者之间共享的交互信息为:

$$I(X; Y)=H(X)-H(X\mid Y)$$
$$=-\sum_i P(x_i)\log P(x_i)+\sum_i\sum_j P(x_i, y_j)\log P(x_i\mid y_j)$$
$$=-\sum_i\sum_j P(x_i, x_j)\log P(x_i)$$
$$+\sum_i\sum_j P(x_i, y_j)\log P(x_i\mid y_j)$$
$$=\sum_i\sum_j P(x_i, y_j)\log\frac{P(x_i\mid y_j)}{P(x_i)}$$
$$=\sum_i\sum_j P(x_i, y_j)\log\frac{P(x_i, y_j)}{P(x_i)P(y_j)}$$

即:

$$I(X; Y)=\sum_i\sum_j P(x_i, y_j)\log\frac{P(x_i, y_j)}{P(x_i)P(y_j)} \quad (1)$$

发送者可以用不同的频率传送不同的信号, 同时输入变量 X 符合不同的分布, 通过改变信号的频率, 可以改变接收者接收到的信号量. 在 MLS/ DBMS 中, 高安全级别事务通常采用不同的执行速率, 传递二进制信息 "0" 和 "1".

3　可生存性 MLS/ DBMS 中隐蔽通道分析

实时系统中, 高优先权往往赋予执行期限较早的事务. 在安全 DBMS 中, 针对此种情况通常是对低级别事务设定高级别的优先权可以避免隐蔽通道的产生, 但是同时导致高级别的事务强行退出, 此种策略导致系统中高级别事务处于 "挨饿" 状态或者强行退出. 在高安全部门如军事部门, 此种情况的发生是不能容忍的. 从另一方面, DBMS 的可生存性要求关键事务必须最低限度执行, 因此高安全级别事务在特殊情况下, 例如恶意事务的肆意破坏下需要部分违反安全策略执行, 因而导致了隐蔽通道的产生.

3.1　基本隐蔽通道分析

为保证 DBMS 事务的可串行化, 基本的并发控制解决方案是采用严格 2PL 实现, 即事务开始执行时对相关数据进行加锁, 提交或者中断退出时刻释放锁. 然而当高级别事务 T_h 和低级别事务 T_l 按照以下序列执行时:

T_h: $r_{Th}[x]\ \cdots\cdots r_{Th}[y]\ c_{Th}$

T_l: $w_{Tl}[x]\ w_{Tl}[y]\ c_{Tl}$

由于 T_l 无法获取数据 x 的写锁, 同时 T_h 也无法获取数据 y 的读锁, 因此存在死锁. 通常有两种方法解决死锁: 阻塞 T_h 或者中断 T_l. 然而中断 T_l 使得低安全级别事务能够感知高安全级别事务 T_h 的存在, 因而可能会存在隐蔽通道. 在可生存环境下, 由于恶意事务的攻击或者内部合法用户权限的滥用, 事务往往被阻塞. 假定 T_l 受阻塞的概率为 p, 周期性的执行 T_h 以及 T_l 导致在 Δt 时间内 T_h 向 T_l 传输 1bit 的信息; 同时设定 T_h 的在速度 v 的概率服从时间 t 的泊松(poisson)分布, 即:

$$y_h=f(t\mid v)\sim\frac{v^t}{t!}e^{-v}$$

则 Δt 时间内高安全级别事务 T_h 通过隐蔽通道向低安全级别事务 T_l 泄漏的信息量为:

$$I_{leak}=y_h tp\ \Delta t \quad (2)$$

3.2　带噪声隐蔽通道分析

DBMS 中大量不同粒度的共享数据导致在同一个时间间隔内, 数据 x 可能被 2 个以上不同安全级别的事务同时访问, 针对单个高级别事务与低级别事务对[T_h, T_l], 第三方事务可能对其的信息的传递存在一定的干扰, 从信息论的角度, 相关的隐蔽通道带有噪声. 简单起

见,假定同一时间段存在 3 个事务:T_h、T_l 和 T_{noise},其中 T_{noise}是干扰 T_h 和 T_l 通过隐蔽通道泄漏信息的其他事务. 假定 T_h 和 T_l 以相同周期进行提交,且 T_h 的提交晚于 T_l 的开始执行时刻 t 后 Δ 时间,其中 $\Delta < e_l$(e_l 是 T_l 的执行时间). T_h 的提交引起的 T_l 中断退出是导致隐蔽通道泄漏信息原因所在. 噪声事务 T_{noise} 通过改变 T_l 的正常提交影响隐蔽通道的信息传递. 如图 1 所示. T_{noise}可能在以下 5 个时刻到达:T_l 执行之前,T_{noise}到达概率为 q_1;T_l 执行之后 T_h 到达之前的 Δ 时间内,到达概率为 q_2;T_h 执行之后 T_l 提交之前 T_{noise}的到达概率为 q_3;T_l 提交之后 T_h 提交之前到达概率为 q_4;T_h 提交之后 T_{noise}的到达概率为 q_5. 其中 $q_1+q_2+q_3+q_4+q_5=1$,且 $e_l < \Delta + e_h$. 如表 1 所示:

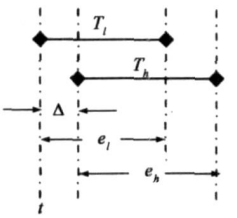

图1 带隐蔽通道的事务执行顺序

在无噪声事务 T_{noise} 存在的条件下,T_h 的执行导致 T_l 中断退出的概率为 p. 当 T_{noise}在不同时间段到达时,其中断正在执行的 T_h 和 T_l 的概率为 r,根据表 1 中 T_{noise}不同时间的到达概率,可以计算出 T_h 和 T_l 提交和中断的概率,如表 2 所示.

表1 噪声事务不同时间到达概率

符号	描述
q_1	$t_{noise} < t$
q_2	$t < t_{noise} < t + \Delta$
q_3	$t + \Delta < t_{noise} < t + e_l$
q_4	$t + e_l < t_{noise} < t + \Delta + e_h$
q_5	$t + \Delta + e_h < t_{noise}$

表 2 不同噪声事务到达概率下事务提交和中断的概率

T_{noise} 到达概率	高安全级别事务 T_h		低安全级别事务 T_l	
	提交(Commit)	中断(Abort)	提交(Commit)	中断(Abort)
q_1	p	$1-p$	$1-p$	p
q_2	p	$1-p$	$(1-r)(1-p)$	rp
q_3	$(1-r)p$	$r(1-p)$	$(1-r)(1-p)$	rp
q_4	$(1-r)p$	$r(1-p)$	$1-p$	p
q_5	p	$1-p$	$1-p$	p

从信息论的角度,作为发送方的高安全级别事务 T_h 的提交和中断表示传递信息"1"和"0",即 $x=i(i=1,0)$;同样,作为接收方的低安全级别事务 T_l 的提交和中断同样代表接收的信息为"1"和"0",即 $y=j(j=1,0)$,可以得到 T_h 和 T_l 之间信息传递的条件概率:

$$P(y=0|x=0)=q_1+q_2(1-p+rp)+q_3r+q_4(p+r-rp)+q_5$$

$$P(y=1|x=0)=2q_1(1-p)+q_2(1-p)(2-r)+q_3(1-p)+q_4(1-p)(1+r)+2q_5(1-p)$$

$$P(y=0|x=1)=q_1p+q_2p(1+r)+q_3p+q_4p(2-r)+2q_5p$$

$$P(y=1|x=1)=q_1+q_2(1-r+rp)+q_3(1-r)+q_4(1-rp)+q_5$$

进而,假定高安全级别事务 T_h 向低安全级别事务 T_l 发送"1"的概率为 ξ,则:$p(x=1)=\xi$,$p(x=0)=1-\xi$. 由贝叶斯(Bayes)公式,可以求得 T_h 和 T_l 之间信息传递的概率分布:

$$P(x=0,y=0)=(1-\xi)(q_1+q_2(1-p+rp)+q_3r+q_4(p+r-rp)+q_5)$$

$$P(x=0,y=1)=(1-\xi)(2q_1(1-p)+q_2(1-p)(2-r)+q_3(1-p)+q_4(1-p)(1+r)+2q_5(1-p))$$

$$P(x=1,y=0)=\xi(2q_1p+q_2p(1+r)+q_3p+q_4p(2-r)+2q_5p)$$

$$P(x=1,y=1)=\xi(q_1+q_2(1-r+rp)+q_3(1-r)+q_4(1-rp)+q_5)$$

$$P(y=0)=(1-\xi)(q_1+q_2(1-p+rp)+q_3r+q_4(p+r-rp)+q_5)+\xi(2q_1p+q_2p(1+r)+q_3p+q_4p(2-r)+2q_5p)$$

$$P(y=1)=(1-\xi)(2q_1(1-p)+q_2(1-p)(2-r))+q_3(1-p)+q_4(1-p)(1+r)+2q_5(1-p))+\xi(q_1+q_2(1-r+rp)+q_3(1-r)+q_4(1-rp)+q_5)$$

由式(1),T_h 和 T_l 之间交互信息 $I(T_h,T_l)$ 即 T_h 和 T_l 之间的隐蔽通道的带宽 $C_{h,l}$ 为:

$$C_{h,l}=I(T_h,T_l)=\sum_{i=0}^{1}\sum_{j=0}^{1}P(x_i,y_j)\log\frac{P(x_i,y_j)}{P(x_i)P(y_j)} \tag{3}$$

将上述 $P(x_i)=P(x=i)$、$P(y_j|x_i)=P(y=j|x=i)$ 以及 $P(x_i,y_j)=P(x=i,y=j)$ 代入式(3)所得结果即为 T_h 和 T_l 之间的隐蔽通道的带宽 $C_{h,l}$.

4 可生存性 MLS/DBMS 中基于隐蔽通道的恶意事务检测

建立可生存 DBMS 体系是确保 DBMS 在恶意事务的影响下能够保证系统最低限度的运行,即核心 DBMS 组件,如:并发控制管理器、缓冲区管理器以及恢复管理器等没有被颠覆或者被恶意用户完全控制[5,8,11]. 从另一个角度,如果并发控制管理器受到攻击,恶意事务可以改变事务的锁状态以及其他事务的到达时间等系统信息,相应的隐蔽通道分析参数 p、$q_{1\sim5}$、r 等被恶意篡改,机密信息可以通过隐蔽通道肆意泄漏. 在这种情况下,DBMS 无法最低限度运行,已处于崩溃状态. 因此,根据隐蔽通道的恶意事务检测假定恶意行为没有颠覆系统核心组件,即恶意用户只获得系统部分权限以及系统部分遭到破坏.

4.1 基于带宽的恶意事务检测

可生存 DBMS 中利用隐蔽通道进行检测主要根据以下两点:恶意用户特征和恶意事务对隐蔽通道异常改

变. 通常情况下,“无威胁”隐蔽通道建立在以下基础之上[5]: 隐蔽通道带宽过窄, 需要很长时间传递一定量的信息; 机密信息经过隐蔽通道泄漏后失去了原有的价值, 已变成垃圾信息; 机密信息经过隐蔽通道传输的时间过长, 已被相关检测机制发现; 消除隐蔽通道的代价远远超过隐蔽通道泄漏的机密信息价值本身. 因此, DBMS 中的恶意事务为了在低带宽情况下传递一定量的信息, 并且防止操作时间过长而被检测到, 最直接的方法就是加大隐蔽通道的带宽. 在式(1)中, 为了在 Δt 时间内传递更多的信息, 恶意事务改变 y_h 和 p 的值, 即加快执行的频率或者使得 T_l 受阻塞的概率增加. 图 2 显示了当 T_h 在执行速度 v= 100trans/ s、Δt= 1s 条件下, T_h 和 T_l 之间的带宽随 T_l 被中断概率的变化情况, 其中 T_h 在 v 的概率服从时间 t 的泊松分布. 图 2 显示, 隐蔽通道的带宽 I_{leak}不仅跟 p 的分布有关, 而且跟泊松分布的特征有关, 恶意事务通过改变相应概率分布 y_h 或者 p 的大小增加隐蔽通道带宽.

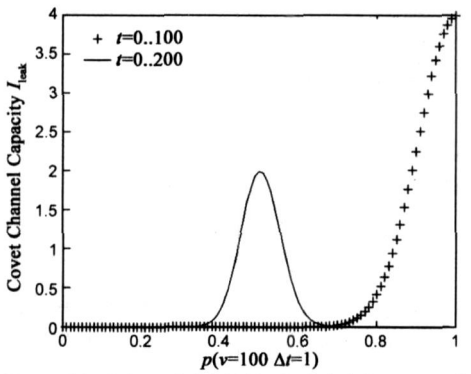

图2　不同分布下隐蔽通道带宽随中断概率的变化

(1) 高、低安全级别事务同谋以改变 p 和 ξ 值;

(2) 噪声事务恶意篡改 r、$q_{1\sim5}$的大小.

4.1.1　同谋事务检测

通常, 同谋事务是由事务对$[T_h, T_l]$组成, 且决定之间的信息量 $I[T_h, T_l]$ 的参数可由 T_h 与 T_l 共同决定. 在 MLS/ DBMS 中, 根据无干扰理论[12], 不同安全级别事务之间无信息流动. 给定高安全级别事务 T_h 以及低安全级别事务T_l, 彼此的运行是独立的, 即 $I[T_h, T_l] \sim 0$. 然而, 在隐蔽通道存在的前提下, T_h, T_l 可以改变与其关联的参数p 和 ξ, 相应的, T_h 和 T_l 之间的信息量也随之改变, 表示为:

$$I[T_h, T_l] \sim p, \xi \tag{4}$$

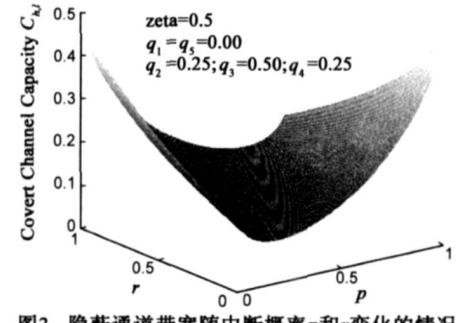

图3　隐蔽通道带宽随中断概率p和r变化的情况

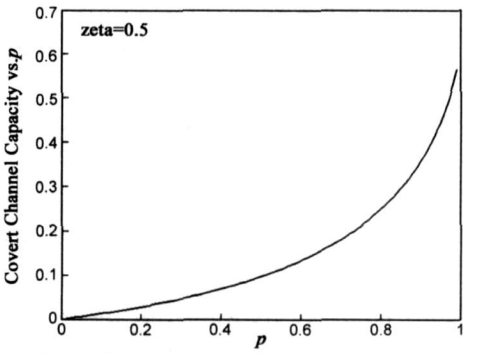

图4　无噪声情况下隐蔽通道带宽随p的变化

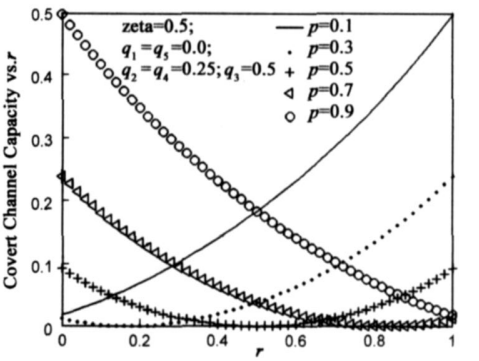

图5　噪声下隐蔽通道带宽随中断概率r的变化

图 4, 5 分别表示了无噪声事务和有噪声事务 T_{noise} 的影响下, 隐蔽通道带宽随高级别事务 T_h 中断低级别事务T_l 的概率的变化情况. 图 4 中隐蔽通道带宽随 p 增大而变大. 图 5 中当 p 从小到大依次取不同值时, 隐蔽通道带宽随 T_{noise}中断概率 r 的变化曲线向负斜率方向发展. 因此, T_h 和T_l 同谋改变p 值大小可以改变隐蔽通道的带宽. 无噪声情况下, 如果系统允许带宽为 0. 1, 当 p= 0. 8 时, T_h 和 T_l 为异常或恶意同谋事务; 有噪声情况下, p 值由 0. 5 增加到 0. 9, 隐蔽通道带宽由 0 改变到 0. 18, 同样判断 T_h 和 T_l 为异常或恶意同谋事务.

在 MLS/ DBMS 中, 信息被分为不同密级, 处于不同密级的信息泄漏对 DBMS 所造成的破坏往往不同, 处于高安全级别的事务的信息泄漏对 DBMS 的威胁远远大于低安全级别事务的信息泄漏. 而当同谋事务存在时, 机密信息通过中间载体向低安全级别事务泄漏信息.

定理　不同安全级别同谋事务间隐蔽通道满足传递性.

证明　设定 MLS/ DBMS 中存在三种相邻安全级别的事务 T_s(秘密)、T_c(机密)和 T_p(公开), T_s 与 T_c 之间有共同的参数p_1 和 ξ_1、T_c 与 T_p 之间有共同参数p_2 和 ξ_2, 即:

$$I[T_s, T_c] \sim p_1, \xi_1 \tag{5}$$

$$I[T_c, T_p] \sim p_2, \xi_2 \tag{6}$$

由式(5), (6)得:

$$I[T_s, T_c, T_p] \sim p_1, p_2, \xi_1, \xi_2 \quad (7)$$

式(7)说明秘密事务 T_s 与公开事务 T_p 之间通过参数 p_1, p_2, ξ_1, ξ_2 传递信息.

从并发控制角度, T_s 与 T_c 由于同时访问数据项 x_1, 而 T_c 与 T_p 同时访问数据项 x_2. T_p 由于 T_c 的执行被迫中断从而感知 T_c 的存在; 同时 T_c 由于 T_s 的执行被迫中断而感知 T_s 的中断, 由于 T_c 为中间同谋用户, 从而 T_p 可以感知 T_s 的存在. 因此, DBMS 的事务并发控制机制同样说明了同谋用户导致的隐蔽通道具有传递性.

4.1.2 恶意噪声事务检测

带噪声的隐蔽通道分析中, 噪声事务的影响决定了带宽的大小. 如果噪声事务有意识的中断 T_h 或者 T_l, 隐蔽通道带宽受其影响很大, 甚至威胁系统的正常运行. 图 6 显示了隐蔽通道在不同的 T_{noise} 中断概率 r 情况下带宽随 T_h 中断 T_l 的概率 p 的变化情况. 当 r 由小到大取不同的值时, 隐蔽通道带宽在 p 较小的时候随 r 的增大而变大; 当 p 增大时, 带宽随 r 的增大而变小. 因此, 如果噪声事务恶意篡改 r 值大小, 例如 r 从 0.5 增大到 0.9, 在 p = 0.2 时带宽相差 0.19, 当系统允许的带宽改变少于此值时, 噪声事务 T_{noise} 为恶意事务.

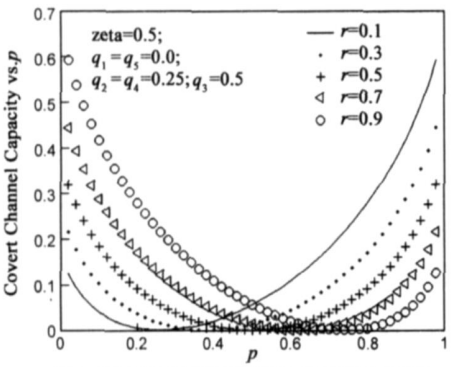

图6 噪声隐蔽通道带宽随 p 的变化(r 不同)

图 7 显示了在 T_{noise} 的不同到达概率情况下隐蔽通道带宽随其中断 T_h, T_l 概率的变化情况. 当 q_1= q_2= q_5 = 0 时, 隐蔽通道带宽为零, 当 q_3= q_4= 1 时, 带宽在噪声事务中断的小概率和大概率的情况下变大. 因此, 噪

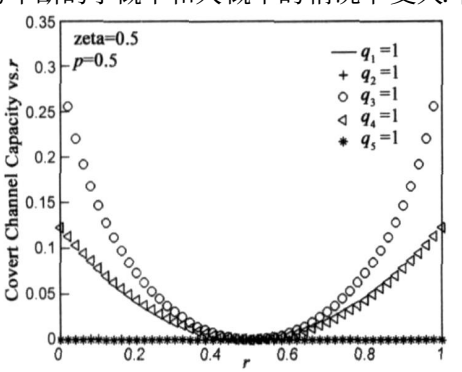

图7 噪声隐蔽通道带宽随 r 的变化(q 不同)

声事务 T_{noise} 选择在 $t+\Delta < t_{noise} < t+e_l$ 以及 $t+e_l < t_{noise} < t+\Delta+e_h$ 到达可以显著改变隐蔽通道的带宽. 当 r = 0.2, q_3= 1 时, 带宽为 0.07. 如果系统允许的带宽不超过 0.05, 则 T_{noise} 为恶意噪声事务.

在存在三种安全级别的 MLS/DBMS 中, 噪声事务 T_{noise} 的存在导致 T_s、T_c 以及 T_p 相关参数被(恶意)篡改, 根据式 4, 参数 p_1、p_2、ξ_1、ξ_2 的值被改变, 导致式 5~7 衍变成:

$$I[T_s, T_c, T_p] \sim p_1, \xi_1 \quad (8)$$

$$I[T_s, T_c, T_p] \sim p_2, \xi_2 \quad (9)$$

$$I[T_s, T_c, T_p] \sim 0 \quad (10)$$

式(8)~(10)反应了在噪声事务存在前提下, 同谋事务 T_s, T_c, T_p 之间的隐蔽通道不具有传递性, 进而可以得到以下结论:

推论 恶意噪声事务是打破不同安全级别隐蔽通道传递性的外在主体.

5 总结

在遭受外来攻击或者内部合法用户的滥用情况下, 检测入侵的恶意事务是维护 MLS/DBMS 可生存性的首要步骤. 本文分析了多级事务之间的基本隐蔽通道和带噪声的隐蔽通道, 并在此基础上提出了利用多级事务之间的隐蔽通道检测内部滥用权限用户和已渗透的恶意事务的方法. 通过参数模拟和实验分析, 给出同谋事务和恶意噪声事务检测的基本方法. 无论从可生存角度还是事务执行的并发控制角度, MLS/DBMS 中的隐蔽通道无法避免. 利用隐蔽通道检测恶意事务不仅可以增加系统安全性, 同时也为可生存性 MLS/DBMS 中的恶意事务进一步隔离以及受感染事务的恢复提供理论基础和分析依据.

参考文献:

[1] BERTINO E, SANDHU R. Database security: concepts, approaches, and challenges[J]. IEEE Trans on Dependable and Secure Computing, 2005, 2(1): 2-19.

[2] GEORGE B, HARITSA J. Secure transaction processing in real-time database systems[A]. Proc of ACM SIGMOD[C]. Tucson, USA: SIGMOD 1997, 462-473.

[3] BELL D E, LAPADULA L J. Secure computer systems: mathematical foundations[R]. Technical Report M74-244, Bedford MA: MITRE Corporation, 1973.

[4] CAHILL M J, ROHM U, FEKETE A D. Serializable isolation for snapshot databases[A]. Proc of ACM SIGMOD[C]. New York: ACM Press, 2008. 729-738.

[5] GEORGE B, HARITSA J. Secure buffering in firm real-time database systems[J]. VLDB J, 2000, 8(3-4): 178-198.

[6] AMMANN P, JAJODIA S, MCCOLLUM C D et al. Surviving

information warfare attacks on databases[A]. Proc of IEEE Symp on Security and Privacy[C]. Oakland, CA, USA: IEEE CS Press, 1997. 164- 174.

[7] SON S H, CHANEY C, THOMLINSON N. Partial security policies to support timeliness in secure real-time databases [A]. Proc of IEEE Symp. on Security and Privacy[C]. Oakland, CA, USA: IEEE CS Press, 1998. 136- 147.

[8] SON S H, MUKKAMALA R, DAVID R. Integrating security and real-time requirements using covert channel capacity[J]. IEEE Trans on Knowledge and Data Engineering, 2000, 12(6): 865- 879.

[9] AHMED Q N, VRBSKY S V. Maintaining security and timeless in real-time database system[J]. Journal of Systems and Software, 2002, 61(1): 15- 29.

[10] SHANNON C E, WEAVER W. The mathematical theory of communication[M]. Urbana, IL: University of Illinois Press, 1949.

[11] AMMANN P, JAJODIA S, LIU P. Recovery from malicious transactions[J]. IEEE Trans. on Knowledge and Data Engineering, 2002, 14(5): 1167- 1185.

[12] GOGUEN J A, MESEGUER J. Security policies and security models[A]. Proc. IEEE Symp on Security and Privacy[C]. 1982, 11- 20.

作者简介:

郑吉平　男, 1979 年生于安徽宣城, 现居住地为江苏省南京市, 博士, 助理研究员, 现为清华大学计算机科学与技术系博士后, 研究方向为场境感知数据管理、数据库安全.
E-mail: zhengjiping@tsinghua.edu.cn

秦小麟　男, 1953 年生于江苏南京, 现为南京航空航天大学信息科学与技术学院教授, 博士生导师, 研究方向为安全数据库、时空数据库、网格数据库等.
E-mail: qinxcs@nuaa.edu.cn

管致锦　男, 1962 年生于江苏连云港, 博士后, 研究方向为可逆计算.

孙　瑾　女, 1978 年生于河南洛阳, 博士, 讲师, 研究方向为计算机视觉, 图象处理与分析.