《电子技术应用》 www.ChinaAET.com

移动自组网中多级安全事务的并发控制

雷向东，陈莉莉
（中南大学 信息科学与工程学院，湖南 长沙 410083）

摘 要：为满足移动自组网（MANETS）多级事务处理的安全性和并发性要求，将多版本两段锁协议运用到 MANETS 多级事务中。该协议有效地解决了由于竞争产生的错误的事务调度以及安全问题。模拟仿真结果表明，多版本两段锁协议在延迟截至时间率和重启动率方面比单一的多版本协议或者单一的两段锁协议都要低。

关键词：MANET；多级安全；并发控制；多级事务
中图分类号：TP393 **文献标识码**：A **文章编号**：1674-7720(2011)12-0054-04

Concurrency control for multilevel secure transactions in mobile Ad Hoc networks

Lei Xiangdong, Chen Lili
(School of Information Science and Engineering, Central South University, Changsha 410083, China)

Abstract: In order to fulfill the MANET multi-level transaction security and concurrency, we have applied multi-version of two phase locking protocol in the multi-level transaction of MANET. The protocol effectively solves incorrect transaction scheduling and security issue, which are arised by competition. THE simulation emulation results show that multi-version two-phase locking protocol in delay time rate and restart rate are superior to single multi-version protocol or single two-phase locking protocol.

Key words: MANET; multilevel secure; concurrency control; multilevel transaction

移动自组网 MANETS（Mobile Ad Hoc Networks）是由多个移动节点通过无线链路相连接，具有时变拓扑结构的一个多跳、临时性自治系统。MANETS 中的数据库系统是由许多移动主机组成的动态分布式数据库系统。通常分布式数据库中总是有若干个事务在运行，这些事务可能并发地存取相同的数据。当数据库中有多个事务并发运行时，系统必须对并发事务之间的相互作用加以控制，即通过并发控制机制来实现。然而，由于在 MANET 网络中节点到处移动导致网络拓扑结构频繁变化，使得很多有线网络中的并发技术在 MANET 网络中行不通。例如锁机制或时间戳机制，这些并发控制机制被应用到 MANET 的多级事务时，将会产生很多问题，如隐通道、高级事务被饿死和检索异常等[1]。因此解决 MANETS 中多级事务的并发控制具有重要的意义。

MANETS 中的数据库管理系统（DBMS）是一个由不同访问权限的用户共享的、包含多安全等级数据的安全系统。系统中的每一个数据项具有其安全等级，并且每一个用户被赋予不同的访问权限。由于这些特点，并发执行的事务可能导致不同的主体为了获取数据而产生竞争，进而竞争会导致安全问题，于是就要求 DBMS 对并发操作进行正确调度[2]，即允许非冲突的事务并行执行，而冲突的事务必须被串行化，即实现可串行化调度。

为保证 MANETS 中多级安全数据库的完整性和一致性，本文提出一种运用在 MANET 中的多版本两段锁并发控制协议。

1 多级事务

首先，看一个多级事务的例子：

T1：R(x,U,S) W(y,S,S)

这里 R（x,U,S）表示具有秘密密级的主体在具有公开安全级的对象 x 上的一个读操作；同样，W(y,S,S)表示具有秘密密级的主体在具有秘密安全级的对象 y 上的一个写操作。对于这类多级事务，定义被简化为如下形示：

T1(S)：R(x,U) W(y,S)

这个主体的分类级别与事务名有关联。

1.1 多级事务处理系统

目前多级安全事务处理系统有 4 种主要的体系结

《电子技术应用》 www.ChinaAET.com

构：基于完整性锁的体系结构、基于内核化的体系结构、基于数据复制的体系结构和基于可信主体的体系结构。这里以基于可信主体的体系结构为例，由 DBMS 自身实现强制访问控制。要求运行在多级安全局域网上，通过安全网络进行通信，所有对数据库的访问必须通过可信 DBMS，DBMS 在多个文件中存储多级数据库。在可信主体体系结构中实现多级安全的事务处理所遵循的机制如图 1 所示。

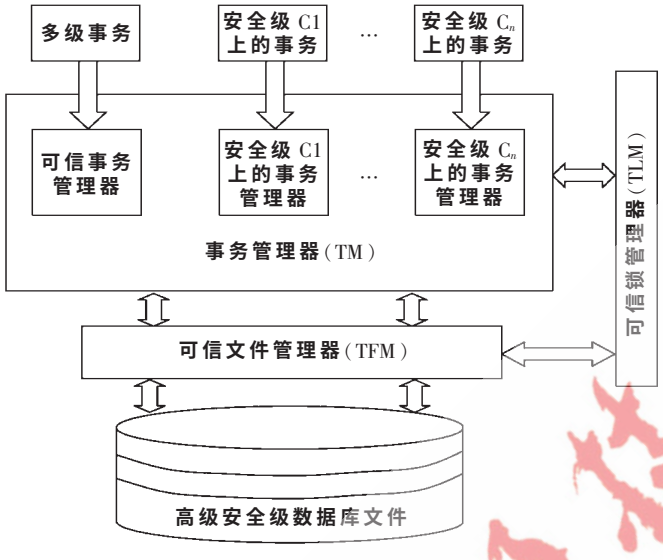

图 1 系统结构

图中事务管理器 TM(Transaction Manager)由可信事务管理器和各安全级上的不可信事务管理器组成。事务管理器负责管理所有事务的执行，事务的每一个操作都需要事务管理器的调解。对于单级事务，系统将它发送给该安全级上的不可信事务管理器进行处理。对于多级事务，事务管理器用单级事务的处理机制来实现多级事务的处理。系统首先将多级事务发送给可信事务管理器，然后可信事务管理器将多级事务划分为单安全级的子事务，将这些子事务分别发送给相应安全级的不可信事务管理器。可信锁管理器负责安全锁协议的实现，它的主要功能是提供对数据项的加锁和解锁操作。可信文件管理器管理对数据项的物理访问。

1.2 一种安全调度框架

要实现一个多级事务调度的安全性能需实现以下两方面安全性：

(1)调度协议的安全性；

(2)执行的安全性。

本文只关注第一部分，通过分析协议，可以估计一个调度的内在的安全性。无需考虑调度的执行就可以评估调度。不安全的调度协议能够在执行之前被发现。如果调度协议是安全的，则可以考虑对执行问题做分析；否则，很可能将对协议的分析简化为对执行情况的分析。

1.3 多版本调度

在数据库中，多版本调度允许一个元素有多个版本。这种特征降低了对一个元素的争夺。一个多版本调度产生的调度表称为一个完整的调度时间表，表示为(s，V)。其中 s 代表输出操作，V 代表版本类型。它映射了输出操作 s 与被访问元素版本 V 之间的关系。其中版本 V 有 3 种类型：(1)到写版本的先前操作的参考；(2)到新版本的参考，即写操作创建一个新版本；(3)到空版本的参考，即一个元素的写操作会被丢弃。当操作到达时，调度程序会做出 3 个基本决定：(1)操作是否可以立即执行；(2)读操作或写操作的实体是什么版本；(3)调度是否可以继续。而调度程序会根据本身的间隔状态做出决定。

现在，定义一种调度程序，把这个程序之前的输出操作定义为调度状态，这里只讨论调度程序的输出操作，不考虑为读或写操作分配版本。

定义 1 一个调度程序是输出状态等价，当且仅当任意两个状态 st_1、st_2 有各自的输出 (s_1,V_1)、(s_2,V_2)，如果 s_1 等于 s_2，则 s_1 对一个即将被调度的程序的操作决策与 s_2 对该程序做出的操作决策是相同的。换言之，一个输出状态等价调度，如果两个不同状态调度的输出操作是相同的，则这两个状态是等价的。这意味着到达的操作即将被调度，但发生了延迟，不过不影响调度程序所做的决定。

现在定义一个输出状态等价的弱版本。在这种情况下，输出操作仅决定带有决策的调度行为。

定义 2 一个调度程序是输出调度冲突，当且仅当任意两个状态 st_1、st_2 有各自的输出 (s_1,V_1)、(s_2,V_2)。如果 s_1 等于 s_2，则 s_1 对一个即将被调度的程序的操作决策与 s_2 对该程序做出的操作决策是相同的。

如图 2 所示的简单调度模型中，操作从左边输入，右边输出。如果一个操作不能被立即调度，它将被排在队列中。调度问题主要关注事务操作的顺序，以便保持正确性，并允许同一时间的并发性。如果两个事务之间出现冲突，就将事务串行化。

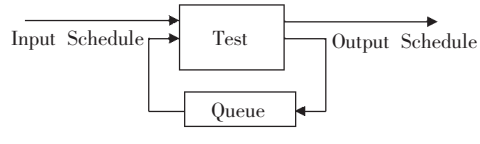

图 2 调度模型

2 多版本两段锁协议

参考文献[3]提出了一种使用多版本数据的安全的并发控制机制。当 T_i 试图写一个数据对象 x 时发现 T_s 已经在 x 上请求了一个读锁，T_i 就创建了 x 的一个新的版本。因为通过给每一个多级事务一个不同的版本已经解决了冲突，所以就避免了隐通道的创建。然而，这样做带来了新的问题，即高级事务的读操作读到的可能是不一致的版本，即所谓的检索异常。但是在两段锁协议中，一个事务应当在确定其不再需要其他加锁的情况后才释放所持有的锁。于是下面提到的多版本两阶段封锁协议可以解决检索异常问题。

《电子技术应用》 www.ChinaAET.com

2.1 多版本两段锁协议概述

每一个只读事务 T_i 发出读数据项 Q 时，返回值是小于 $T_s(T_i)$ 时间戳的最大版本 Q_k 的内容。这是因为一个事务应读取在它之前的最近版本。更新事务执行两段锁协议，在提交之前不释放任何锁，事务可以按其提交的顺序串行化，更新事务 T_i。读取数据项 Q 时，T_i 在获得数据项 Q 上的共享锁后读取 Q 最新版本的值。更新事务 T_i。想写数据项 Q 时，T_i 首先要获得数据项 Q 上的排它锁，然后为 Q 创建一个新版本，写操作在新版本上进行。新版本的时间戳初值为 ∞，它大于任何可能的时间戳值。在创建此版本的事务 T_i 完成之前，阻止其他只读事务对此版本进行读操作。当更新事务 T_i 完成后，T_i 将它创建的每一个版本的时间戳设为 Counter+1。然后 T_i 将 Counter 增加 1。在 Counter 增加之前启动的只读事务将看到被 T_i 更新之前的值。无论是哪种情况，只读事务均不必等待加锁[4]。

2.2 多版本两段锁调度算法

多版本调度允许同一实体有多个版本，通过限制访问一个实体的竞争加强并发性。这种竞争会引起不安全调度或者不安全恢复。这里考虑到的调度之一是冲突集调度。这个调度的输出是有序冲突调度的集合。有序冲突的定义如下：

定义 3 一个调度是有序冲突的，当且仅当它能通过一系列 0 次或者多次转换变成一个有序调度。在这些转换中，任何一对来自不同事务的相邻步骤可以互换，除非它们相冲突。即两个事务冲突，如果它们访问相同实体并且这两个实体中至少有一个正在执行写操作。接下来定义一种调度属性——安全级别有序。

定义 4 一个调度是安全级别有序的，当且仅当调度中所有的事务对 p 和 q 共享一个单一主题的分类等级，且在一个序列顺序中 p 紧跟 q 或 q 紧跟 p。

根据上述描述，设计多版本两段锁并发控制调度算法，其算法描述如下：

(1)在冲突集 $C_i(Q)$ 上搜索在数据项 Q 的持锁事务 T_i 和优先级最高事务 T_j；

(2) 如果 T_j 估计运行时间+系统时间≤T_j 截止时间并且 T_i 截止时间<T_j 截止时间，则进行下一步骤；反之结束；

(3)判断 T_j 在数据项 Q 上是否持有排他锁，若没有则转到步骤(7)；

(4)判断 T_i 是否申请共享锁，若没有，则转到步骤(6)；

(5)在冲突集 $C_i(Q)$ 上，每个申请共享锁的事务获准共享锁，执行步骤(9)；

(6)获准 T_i 排它锁，执行步骤(9)；

(7)判断 T_j 在数据项 Q 上是否持共享锁，若没有，则转到步骤(9)；

(8)T_i 获得排他锁，T_j 重启动；

(9)算法结束。

本算法中只读事务不必等待任何锁。更新事务在对数据项加锁发生冲突时，若持锁的事务优先级低，而重启动不会延误截止时间，则持锁的事务重启动。在该协议中，一次只允许一个更新事务提交。

3 模拟仿真和性能分析

仿真的目的是研究新提出的并发控制协议在 MANETS 中的性能。为了对比，选用多版本协议和两段锁协议作为基准协议。主要的性能指标为延误截止时间率和重启动率。仿真模型由移动主机和广播磁盘组成。广播磁盘传输数据项和控制信息，数据项所有版本放在同一个磁盘上，每个数据项所有版本将相继广播，热数据的老版本位于最新版本之后，都放在快速磁盘上。冷数据所有版本则位于慢速磁盘上。一个数据项所有版本以相同的频率广播[5-6]。仿真参数如表 1 所示，一旦事务截止时间到，事务立即结束。

表 1 仿真测试参数

参数	值
CPU 数	4
磁盘数	4
CPU 计算时间/ms	10
磁盘访问时间/ms	20
每个事务的页面数	8~15
事务到达率/(事务数/s)	5~25
页面命中率/%	85

从图 3、图 4 可以看出，在 MANETS 网络中多版本两阶段封锁协议的性能优于多版本协议和两段锁协议，且事务到达率越高效果就越明显。前者的延误截止时间率、重启动率都比较低。这是由于多版本机制消除了只读事务和更新事务的冲突，降低了只读事务的响应时间，又通过多版本动态调整串行次序，而两阶段锁协议保证了并发操作调度的正确性，避免了一切不必要的事务重启动。又因为移动事务在移动主机上进行了部分有效性确认，从而及早地检测了数据冲突，进而减少了移动事务延误截止时间率。此外，多版本机制消除了移动只读事务和移动更新事务之间冲突，读请求从不失败且不必等待。

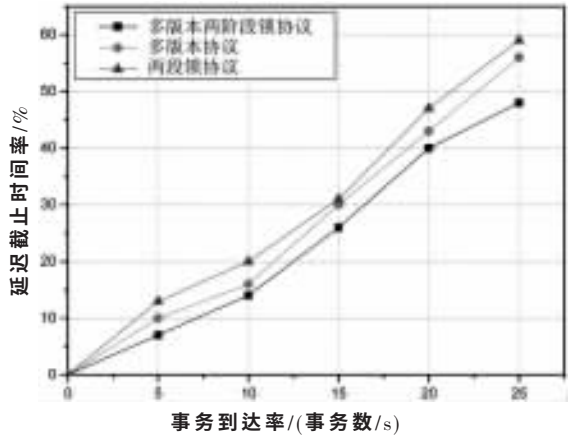

图 3 延误截止时间率-事务到达率

《电子技术应用》 www.ChinaAET.com

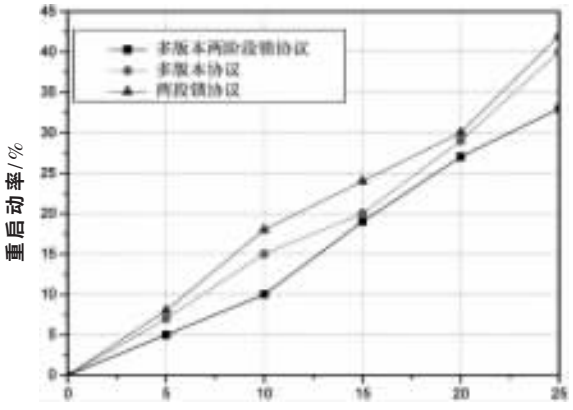

图 4 重启动率-事务到达率

该文提出了在 MANETS 中处理多级安全事务要采用的多版本两段锁并发控制协议。该协议结合了多版本和两段锁协议的优点，在 MANETS 中提高了事务的并发度，读请求从不失败且不必等待，事务间冲突通过等待解决而不是通过回滚解决。

该协议与两段锁协议、多版本协议相比，在多级事务的处理上能更好地保证数据的完整性和一致性。仿真结果表明，在正常负载下其延误截止时间率和重启动率都要低得多，性能较好。

参考文献

[1] KIM H W, PARK D S. Advanced transaction scheduling protocol for multilevel secure database in wireless mobile network environment[C]. Joint 4th IEEE International Conference on ATM(ICATM 2001) and High Speed Intelligent Internet Symposium, 2001.

[2] 曲立平. 基于多版本的多级安全并发控制机制的研究[J]. 信息技术, 2005, 52(6): 14-16.

[3] 李丽萍, 何守才. 数据库多级安全模型的研究[J]. 上海第二工业大学学报, 2006, 23(3): 218-222.

[4] 雷向东, 袁晓莉. 并行实时数据库系统多版本两阶段封锁并发控制协议[J]. 中南工业大学学报, 2003, 34(3): 298-301.

[5] 雷向东, 袁晓莉. 多版本两阶段封锁并发控制协议性能研究[J]. 计算机工程与科学, 2003, 25(04): 46-49.

[6] RAHBAR A.A new data communication protocol for distributed mobile datbases in mobile Ad Hoc networks[C]. Sixth International Conference on Information Technology, 2009.

(收稿日期: 2010-12-21)

作者简介:

雷向东, 男, 1964 年生, 副教授, 主要研究方向: 移动数据库。