자료기지 보안 관리를 위한 이판 그래프 검증 기법

김남규, 손용락, 문송천
(ngkim@kgsm.kaist.ac.kr, syl@dbsun3.kaist.ac.kr, moon@kgsm.kaist.ac.kr)
한국과학기술원 테크노경영대학원

Double-Version Graph Validation Scheme for Security Management in Database Systems

Namgyu Kim, Yonglak Sohn and Songchun Moon
Graduate School of Management
Korea Advanced Institute of Science and Technology

요 약

다등급 보안 자료기지 관리체계는 하위 등급의 자료에 대한 쓰기 연산 및 상위 등급의 자료에 대한 읽기 연산을 불허하여, 상위 등급의 자료가 하위 등급의 거래에 노출되는 것을 방지한다. 하지만, 전통적인 다등급 보안 자료기지 관리체계는 서로 상이한 등급간 거래의 공모로 생성될 수 있는 비밀 경로는 차단할 수 없다. 이러한 비밀 경로의 생성을 막기 위한 여러 연구가 다중 버전의 환경 및 제한된 버전의 환경 하에서 수행되어 왔다. 하지만 다중 버전에 기반한 기법은 상위 등급의 거래가 지나치게 오래된 버전의 자료를 읽을 뿐 아니라 버전 관리를 위하여 추가적인 부담이 요구된다는 단점이 있고, 제한된 버전에 기반한 기법은 항상 상위 등급 거래의 지연 및 철회를 강요한다는 단점이 있다. 본 논문에서는 제한된 버전 하에서 직렬화 가능성 그래프 검사 기법을 사용하여, 각 보안 등급간의 형평성을 높일 수 있는 비밀 경로 생성 방지 기법을 제안한다.

1 배경

자료기지의 설계 및 관리 측면에서 고려되어야 할 가장 중요한 요소는 동시성 제어와 보안 기술이다. 비행기 예약이나 은행 업무 등과 같이 아주 짧은 실행시간 내에 처리 결과를 반환할 것을 요구하는 거래(transaction)를 수행하기 위해서는, 특정한 시점에 둘 이상의 거래를 동시에 수행할 수 있는 동시성 제어 기법이 요구된다. 많은 연구들을 통해 적법성이 검증되어 온 동시성 제어 기법의 원류로서 두 단계 잠금 기법[Eswa 76]과 시간표 순서화 기법[Reed 83]이 있다. 이러한 동시성 제어 기법은 항상 자료기지의 상태를 일관성 있게 유지하며, 항상 직렬화 가능한 실행 내력을 생성해 준다. 하지만 전통적인 동시성 제어 기법만을 사용하는 자료기지 관리체계(database management system: DBMS)에서는 거래 및 자료들에 대한 비밀 등급이 구분되어 있지 않기 때문에, 자료에 대해 비인가된 사용자들의 임의 접근을 막을 수 없다. 따라서 자료기지에 저장된 정보들을 인가되지 않은 사용자로부터 보호하기 위하여 동시성 제어 기법과 더불어 사용자와 정보에 대해 모두 적용되는 자료기지 보안 기술에 대한 연구가 진행되어 왔으며, 이들 대부분은 두 단계 잠금 기법에 근거한 보안 기법[McDe 93] 혹은 시간표 순서화 기법에 근거한 보안 기법[Amma 92b]을 채택한다.

자료에 대해 비인가된 사용자들의 임의 접근을 막기 위해서는 거래 및 자료들에 대해 다등급의 보안 등급을 부여하여, 그 보안 등급에 따라 허용된 연산만을 수행하도록 하는 다등급 보안 자료기지 관리체계(multilevel secure database management system: MLS/DBMS)[Keefe 90a]의 개념이 유용하게 쓰일 수 있다. MLS/DBMS는 거래들의 보안 등급을 확인하여, 자신의 등급과 같은 등급의 자료에만 쓰기 연산을, 자신의 등급과 같거나 낮은 등급의 자료에만 읽기 연산을 허가하는 제한된 B/L 모형[Bell 76]을 택한다. 이러한 정책을 택함으로 하여 상위 등급에서 하위 등급으로의 직접적인 정보의 흐름은 차단할 수 있다. 그러나 이 정책만으로는 상위 등급의 거래와

하위 등급의 거래가 공모하여 생성할 수 있는 비밀 경로(covert channel)는 차단할 수 없다.

MLS/DBMS는 하위 등급의 자료에 대한 쓰기 연산 및 상위 등급의 자료에 대한 읽기 연산을 허용하지않는 정책을 택하여 상위 등급의 자료가 하위 등급의 거래에 노출되는 것을 방지한다. 물론 MLS/DBMS에서도 자료기지의 일관성 유지를 위해서는 동시성 제어 기법이 적용되어야 한다. 이는 곧 임의의 거래에 대해 직렬화 가능한 실행 내력 생성에 위배되는 연산, 즉 다른 거래의 연산과 충돌을 일으키는 연산을 수행하지 못하도록 함을 의미한다. 그러나 이처럼 서로 충돌하는 연산을 제어하는 과정에서 성능 및 보안상의 결함이 발생할 수 있다.

이러한 결함 가운데 가장 치명적인 것은 비밀 경로가 생성되어서 자료기지의 보안성을 침해하는 경우이다. 즉, 상위 등급의 거래가 이미 읽기 연산을 수행하고 있는 하위 등급의 자료에 대해서, 하위 등급의 거래가 쓰기 연산을 수행하고자 하는 경우, 전통적인 동시성 제어 기법에서는 하위 등급의 거래를 철회시키거나 대기 상태로 변환시키는데, 이 과정에서 하위 등급의 거래가 상위 등급의 거래의 영향을 받기 때문에 비밀 경로가 생성될 수 있는 것이다. 보다 구체적으로, 상위 등급 거래의 읽기 연산 수행 여부에 따라서 하위 등급의 거래가 수행, 혹은 철회되므로 하위 등급의 거래는 상위 등급의 거래로부터 1 bit의 신호를 받을 수 있는 것이다. 이러한 1 bit 신호의 조합으로 상위 거래와 하위 거래간의 비밀 경로가 생성될 수 있으며, 자료기지의 일관성을 유지함은 물론 시스템의 성능과 신뢰성을 동시에 높이기 위해서는, 동시 수행되는 거래의 수를 높임과 동시에 비밀 경로의 생성 가능성을 차단할 수 있는 동시성 제어 기법이 반드시 필요하다

2 동기

비밀 경로는 여러 등급의 거래간의 공모로 생성되며, 각 거래가 동시성 제어기에 적법한 연산만을 요청하면서도 상위 거래에서 하위 거래로 정보를 유출시킬 수 있음을 의미한다.. 즉, 각각의 거래는 전통적인 동시성 제어 기법을 위반하지 않으면서도 비밀 경로를 생성시킬 수 있는 것이다. 이러한 비밀 경로는, 높은 수준의 보안이 요구되는 시스템의 경우 반드시 제거해야 할 보안 위험요소 중의 하나이다. 그러므로, 자료기지의 일관성을 항상 유지함은 물론, 시스템의 성능과 신뢰성을 동시에 높이기 위해서는, 동시 수행되는 거래의 수를 높임과 동시에 비밀 경로의 생성 가능성을 차단할 수 있는 동시성 제어 기법이 반드시 필요하다.

자료기지 관리의 동시성 제어 기법에서 비밀 경로의 문제점을 해결하기 위한 많은 연구들이 수행되어 왔다. 기존의 연구들은 그 접근 방식에 따라 크게 두 종류로 분류가 된다. 첫번째 접근 방식[Mosk 91, Hu 91]인 잡음삽입 방식은 거래에 대한 실행 내력이 형성될 때, 특정 연산을 수행토록 하여 거래의 철회 및 대기에 대한 잡음을 삽입하는 방식이다. 잡음 삽입 방식의 핵심 개념은 물리적으로, 혹은 논리적으로 하위 등급 거래의 실행 시간에 대한 지연 시간을 조작하여 하위 등급으로 하여금 상위 거래의 자료 접근에 의한 신호를 정확하게 파악하지 못하도록 하는 것이다. 이 방식은 항상 상위 등급의 거래가 철회되지는 않는다는 점에서 다른 방식의 기법보다 형평성을 높일 수 있다는 장점이 있으나, 상위 거래와 하위 거래가 공모가 여러 번 반복 시행으로 이루어지는 경우 비밀 경로의 생성 가능성을 완벽하게 제거한다고 확신할 수 없고, 지연 시간 조작에 대한 알고리즘이 악의를 가진 사용자에게 파악될 경우, 비밀 경로의 생성 가능성을 전혀 차단할 수 없다는 단점이 있다. 본 논문에서는 비밀 경로가 생성될 수 있는 아주 작은 가능성까지도 허용할 수 없는, 높은 보안 수준이 요구되는 시스템 환경을 가정하므로 이 접근 방식은 논외로 하고, 다음의 접근 방식만을 고려 대상으로 하여 논의를 진행하기로 한다.

또 다른 접근 방식인 불간섭 방식[Keef 90b, Sohn 99, Amma 92a, Manc 96, McDe 93, Amma 92b]은 어떤 일이 있어도 상위 등급의 거래에 의해 하위 등급의 거래가 간섭받지 않을 것을 보장하여주는 실행 내력을 구성하는 방식이다. 이 불간섭 방식의 기본 개념은, 둘 이상의 거래에서 충돌이 발생했을 경우, 항상 충돌을 야기한 거래들 가운데 가장 높은 보안 등급을 갖는 거래를 철회, 혹은 대기시킴으로써, 상위 등급의 거래에 의해 하위 등급의 거래가 영향을 받을 가능성을 완전히 제거한다는 것이다. 불간섭 방식을 따르는 연구를 보다 부적으로 분류하면, 자원의 제한성 여부에 따라, 자료의 버전을 무제한으로 허용하는 다중버전 접근방식[Keef 90b, Sohn 99]과 두버전 접근방식[Amma 92a, Manc 96], 그리고 단일버전 접근방식[McDe 93, Amma 92b]으로 나눌 수 있다. 또한 이 각각은 사용하는 동시성 제어 기법에 따라 잠금 기법에 근거한 연구와 시간표 순서화 기법에 근거한 연구로 분류될 수 있다. 다중버전 접근방식은 거래간 충돌로 인한 철회의 수를 감소시키기 위해 제안된 것으로, 동일한 자료에 대해 여러 개의 버전을 관리하여 동시성을 유지하는 방식이다. 그런데 이 기법은 동일한 자료의 복사본을 여러 곳에 저장하므로 공간의 낭비가 있을 뿐 아니라, 주기적으로 버전을 관리하는 것에 필요한 자원이 소모될 수 있다. 따라서 다중버전 접근방식은 거래의 수에 비해 자료의 양이 많은 경우에는 적합한 방식이라고 할 수 없다. 이 방식은 본 논문에서 제안하는 기법과 상이되는 환경이 상이하므로 역시 논의에서 제외하기로 한다.

불간섭 방식을 따르는 연구 중 단일버전 자료기지에

용되는 대표적인 것으로 잠금 기법에 근거한 Orange Locking 기법(약칭 *OL*)[McDe 93]과 시간표 순서화 기법에 근거한 보안 시간표 순서화 기법(약칭 *TOSSMO*)[Amma 92b]이 있다. 이 두 가지 기법은, 이전부터 널리 사용되어온 동시성 제어 기법인 두 단계 잠금 기법과 시간표 순서화 기법에 다등급 보안 모형의 개념을 적용한 기법이다. 따라서, 이 기법은 기존에 사용하던 동시성 제어 기법의 변형을 통해 쉽게 구현할 수 있다는 장점과, 여러 연구에 의해 검증된 직렬화 가능한 실행 내력을 생성해줄 수 있다는 장점이 있다. 하지만 두 기법 모두, 서로 다른 등급을 갖는 거래의 충돌시 항상 상위 등급의 거래를 철회시키므로, 등급간의 형평성을 유지하지 못한다는 단점이 있다. 또한 실제로 철회되지 않아도 되는 거래를 철회시킴으로써, 시스템의 성능을 저하시키는 단점을 포함하고 있다.

불간섭 방식을 따르는 연구 중 이중버전 자료기지에 적용되는 대표적인 것으로는 Two-Snapshot 동시성 제어 기법(약칭 *2SCC*)[Amma 92a]과 Certify Lock(*CL*) 기법[Manc 96]이 있다. 2SCC는 시간표 순서화 기법에 근거한 연구이며, CL은 두 단계 잠금 기법에 근거한 연구이다. 두 연구는 공통적으로 모든 자료에 대해서 committed version(CV)과 new version(NV)를 동시에 관리한다. 즉, 모든 거래에 대해서 읽기 연산을 수행할 때에는 CV에서 그 값을 읽도록 하고, 쓰기 연산을 수행할 때에는 NV에 그 값을 쓰도록 한다는 것이다. 따라서 쓰기 연산이 읽기 연산의 영향을 받지 않으므로, 비밀 경로의 생성 가능성이 없어지게 된다. 이 두 기법은 이중버전으로 자원이 한정되어 있는 조건 하에서 비밀 경로 문제를 해결할 수 있는 방안을 제안하였다는 점에서 의미가 있다. 그러나, 두 연구 모두 상위 거래가 지나치게 오래된 버전의 자료를 읽는 경우가 빈번하다는 단점이 있다. 또한 연산을 마친 거래가 commit 하는 시점에서 NV를 CV에 기록할 때 자료기지의 일관성을 법은 자체적으로 직렬화 가능성을 보장하지 못하 고, 일관성 유지를 위한 부담을 응용 프로그램 차원에서 해결한다는 치명적인 문제점을 내포하고 있다. 본 논문에서는 단일버전과 이중버전에 근거한 연구 가운데 대표적인 OL과 2SCC를 선택하여 분석하고, 본 논문에서 새로 제안하는 기법과 그 성능을 비교하기로 한다.

3 목적

본 논문에서는 거래의 보안 등급별로 철회 비율의 형평성을 제공하는 비밀 경로 방지 기법을 제안한다. 본 논문 접근 방식의 기본적인 철학은 다음의 크게 다음의 두 가지로 요약될 수 있다. 한 가지는 서로 다른 보안 등급 거래간의 충돌시 항상 상위 거래가 철회 혹은 대기하여야 하는 비형평성을 없애는 것이다. 또다른 한 가지는 철회되어야 할 거래는 추가 연산을 수행하지 않고 바로 철회시킴으로써, 연속 철회의 횟수를 줄임과 동시에 시스템의 성능을 향상시키는 것이다. 이를 위해 전통적인 직렬화 가능성 그래프 검사 기법(약칭 *SGT*)[Bern 87]을 확장하여 동일 등급 거래간의 우선순위와 상이 등급 거래간의 우선순위를 자별적으로 관리하는 규식을 정의하고, 자료의 버전을 3가지로 관리하여 자료기지의 일관성을 유지하는 기법을 제안한다. 또한 본 논문에서 제안되는 동시성 제어 기법의 성능 평가를 위한 모의 실험을 수행하고, 이 결과를 단일버전 기반의 OL 기법 및 이중버전 기반의 2SCC 기법에 근거한 결과와 비교 평가하고자 한다.

4 참고문헌

[Amma 92a] P. Ammann, F. Jaeckle and S. Jajodia, " A Two Snapshot Algorithm For Concurrency Control In Multi-Level Secure Databases," *Proc. IEEE Computer Society Symp. Research in Security and Privacy*, Oakland, California, U.S.A., pp. 204-215, May 1992.

[Amma 92b] P. Amma and S. Jajodia, " A Timestamp Ordering Algorithm for Secure, Single-Version, Multi-Level Databases," *Proc. IFIP WG11.3 Working Group on Database Security*, West Virginia, U.S.A, pp. 191-202, Nov. 1991.

[Bell 76] D. E. Bell and L. J. LaPadula, " Secure Computer Systems: Mathematical Foundations and Model," *Technical Report M74-244, MITRE Corp.*, Bedford, Massachusetts, May 1973.

[Bern 87] P. A. Bernstein, V. Hadzilacos and N. Goodman, *Concurrency Control and Recovery in Database Systems*, Addison-Wesley, Chap. 4, 1987.

[Eswa 76] K. P. Eswaran, J. N. Gray, R. A. Lorie and I. L. Traiger, " The Notions of Consistency and Predicate Locks in a Database System," *Comm.* ACM 19(11): 624-633, November, 1976.

[Keef 90a] T. F. Keefe, W. T. Tsai and J. Srivastava, " Multilevel Secure Database Concurrency Control," Proc. Sixth International Conference on Data Engineering, Los Angeles, California, U.S.A., 1990.

[Keef 90b] T. F. Keefe and W. T. Tsai, " Multiversion Concurrency Control for Multilevel Secure Database Systems," *Proc. IEEE Computer Society Symp., Research in Security and Privacy*, Oakland, California, U.S.A., pp. 69-383, May 1990.

[Manc 96] L. V. Mancini and Indrajit Ray, " Secure Concurrency Control in MLS Databases with Two Versions of Data," *Proc. European Symp. Research in Computer Security*, Rome, Italy, pp. 204-225, Sept. 1996.

[McDe 93] J. McDermott and S. Jajodia, " Orange Locking: Channel-Free Database Concurrency Control Via Locking," *Proc. IFIP WG11.3 Working Group on Database Security*, B. M. Thuraisingham and C. E. Landwehr, eds. North-Holland, 1992, pp. 267-284.

[Reed 83] D. Reed, " Implementing Atomic Actions on Decentralized Data," *ACM Transactions on Computer Systems*, Volume 1, Number 1, 1983.

[Sohn 99] Y. L. Sohn and S. C. Moon, " Verified Order-based Secure Concurrency Controller in Multilevel Secure Database Management Systems," *IEICE Transactions on Information and Systems*, 1999.