디지털산업정보학회 논문지 제5권 제4호-2009년 12월

보안성을 갖는 1-사본 준직렬성을 위한 전역트랜잭션 스케줄링

정 현 철*

Global Transaction Scheduling for One-Copy Quasi-Serializability with Secure Properties

Jeong, Hyun Cheol

〈Abstract〉

In the security environments of heterogeneous multidatabase systems, not only the existing local autonomy but also the security autonomy as a new constraint are required. From global aspects, transactions maintain consistent data value when they assure serializability. Also, secure properties must protect these transactions and data values to prevent direct or indirect information effluence. This paper proposes scheduling algorithm for global transactions to ensure multilevel secure one-copy quasi-serializability (MLS/1QSR) in security environments of multidatabase systems with replicated data and proves its correctness. The proposed algorithm does not violate security autonomy and globally guarantees MLS/1QSR without indirect information effluence in multidatabase systems.

Key Words : Secure Properties, MLS/1QSR, Transaction, Autonomy, Scheduling.

Ⅰ. 서론

데이터의 보안성을 유지하기 위해 시스템에서 보안 정책의 지원은 필수적이다. 다단계 보안(MultiLevel Security, 이하 MLS) 시스템이나 보안 관리자는 사용자와 데이터에 보안등급을 할당한다. 그리고 접근 제어로써 트로이 목마 문제를 갖는 임의 접근 제어(Discretion- ary Access Control, 이하 DAC)보다는 이 문제가 방지될 수 있도록 강제적 접근 제어(Mandatory Access Control, 이하 MAC)를 대부분 채택한다. BLP모델[1-2]은 상위 보안등급(high-Security Level, 이하 h- SL)의 데이터가 하위 보안등급(low-Security Level, 이하 l-SL)의 사용자에게 불법적으로 직접 유출되지 않도록 보안성을 보장하므로 시스템의 보안 정책으로써 주로 사용된다. 데이터의 유용성을 높이는 효율적인 접근은 각 지역에 데이터를 중복시키는 것이며 중복 데이터에 대한 정확성 기준으로써 1-사본 직렬성(One-copy Serializable, 이하 1SR)[3]을 사용한다. 멀티데이터베이스 시스템(Multi-DataBase System, 이하 MDBS)에서는 MDBS가 구축되기 이전에 연관성이 없는 다른 은행의 데이터베이스가 어떤 고객에 대해 주소, 직업등과 같은 동일 정보를 갖을 수 있기 때문에 데이터 중

* 광주보건대학 병원전산관리과 부교수

복[4]이 발생할 수 있다. 지역 사용자가 원격지의 데이터를 쉽게 판독하므로써 검색 비용을 감소시키고 시스템의 결함이 발생하여도 데이터의 유용성을 증가시킬 수 있기 때문에 MDBS에서 데이터를 중복시키는 것은 바람직하다. [5]에서는 중복 데이터를 갖는 MDBS에서 1SR보다 제약이 약한 전역 트랜잭션(Global Transaction, 이하 GT)의 1-사본 준직렬성(One- copy Quasi-Serializability, 이하 1QSR)을 제안하였다. GT 사이의 상호작용은 GT를 스케쥴링하여 제어하고 지역 트랜잭션(Local Transaction, 이하 LT)사이의 상호작용은 지역간의 정보흐름을 제어함으로써 GT와 LT의 상호작용을 분리하기 때문에 준직렬성은 MDBS에서 적절하다. 준직렬성은 지역 자치성을 위반하지 않고 높은 동시성 제어를 제공하며 지역 수행간의 불일치로 GT를 철회하지 않는다[6]. 본 논문에서는 MDBS의 보안 환경 즉, 이질적이며 자치성을 갖는 다단계 보안 지역 데이터베이스 시스템(MLS/LDBS)을 통합한 다단계 보안 멀티데이터베이스 시스템(MLS/MDBS)에서 GT를 관리하기 위해 다단계 보안 1-사본 준직렬성(MultiLevel Secure One- Copy Quasi-Serializability, 이하 MLS/1QSR)[7]을 적용한다. 그리고 보안 관리자가 보안등급을 트랜잭션과 데이터에 할당할 때 GT가 MLS/1QSR을 보장할 수 있도록 하는 기법을 제안한다. 본 논문의 구성은 2장에서 관련 연구를 분석하고 3장에서는 전역적으로 GT를 제어하기 위한 환경인 MLS/MDBS의 시스템 모델을 서술하며 4장에서는 GT의 MLS/1QSR가 보장될 수 있도록 하는 제어 알고리즘을 제안하고 그 정확성을 증명한다. 5장에서는 결론과 향후 연구 방향을 기술한다.

Ⅱ. 관련연구

이 장에서는 부적절한 정보의 흐름과 갱신을 제어하는데 필요한 보안 모델과 이질형 데이터베이스 시스템 환경에서 중복 데이터에 대해 트랜잭션의 직렬성을 보장하는 방법을 살펴본다.

2.1 보안모델과 중복 데이터

BLP모델, BIBA모델, DION모델[1, 9]은 널리 알려진 보안정책이다. BLP모델은 다음의 두가지 성질을 이용하여 직접적인 정보 흐름을 방지한다. 첫째, 단순 성질에서 트랜잭션의 보안등급이 데이터 항목의 보안등급 보다 상위 등급이거나 같을 때 트랜잭션의 판독연산은 가능하다. 둘째, *-성질에서 기록하려는 데이터 항목의 보안등급이 판독연산을 시행한 데이터 항목의 보안등급 이상일 때 트랜잭션의 기록연산은 가능하다. BIBA모델은 트랜잭션이 데이터를 갱신하고자 할 때 무결성 등급이 적절하면 데이터를 기록할 수 있도록 허용해 주며 DION모델에서는 BLP모델의 보안성과 BIBA모델의 무결성을 결합시켰다. BLP모델의 *-성질[9]은 데이터 항목의 보안등급에 대해서 판독과 기록연산 사이에 종속성이 존재한다고 볼 수 있다. [10]에서는 *-성질에 있어서 고의적으로 혹은 실수로 데이터를 손상시키거나 파괴하여 무결성 문제를 발생시킬 수 있기 때문에 트랜잭션과 데이터 항목의 보안등급이 같을 때 기록연산을 하도록 *-성질을 제약하였다. 본 논문에서는 직접적으로 부적절한 정보의 흐름을 방지하고 데이터의 무결성 위배 문제를 제거하기 위하여 기록연산은 제약된 *-성질을 사용하며 판독연산에 있어서는 BLP모델의 단순 성질을 이용한다.

중복 데이터를 관리하기 위하여 MDBS에서는 지역 자치성을 위배하지 않고 제어하는 방법들이 [4, 5, 11]에서 제안되었다. [4]에서는 의족수 찬성 방법을 이용하여 트랜잭션의 직렬성을 보장하였다. 하나의 논리적 데이터가 전역 사본과 지역 사본으로 구분된다. GT는 전역 레벨에서 완료되고 지역 레벨에서 부트랜잭션의 철회가 허용된다. 전역 사본에서는 의족수 찬성 방법이 수행되고 실제적인 판독과 기록의 연산은 지역 사본에서 수행된다. 그러나 트랜잭션의 부분적 완료는 여러 차례의 보상 방법을 요구하게 된다. [5]에서 제안된 분산형 동시성 제어 알고리즘은 GT의 1QSR를 보장한다. 지역 서버들은 서로 조정되어 빠르거나 늦게 도착하는 부트랜잭션을 연기하

거나 무시함으로써 불일치한 값을 갖는 중복 데이터로의 접근을 막아 일치된 값을 유지시킨다. 또한, 중복 갱신 트랜잭션을 사용하여 각 지역에 물리적으로 존재하는 사본에 접근하여 일관된 값을 유지시킨다. 중복 데이터를 접근하는 트랜잭션을 제어하기 위하여 준직렬성(Quasi-Serializability, 이하 QSR)[6]를 1QSR로 확장하였다. 1QSR은 1SR에서 처럼 LT에 의한 지역 간접 충돌 문제를 고려하지 않으므로 중복 데이터에 대해 제약 사항을 완화시켜 GT의 직렬성을 유지시킨다. [11]의 전역적 확인 알고리즘은 사본의 일관성을 검증하므로써 트랜잭션의 1SR을 보장하였다. 전역적 제어를 받지 않는 트랜잭션의 1SR 위배를 방지하도록 전파 잠금 알고리즘을 사용하여 원본이 존재하는 지역에 전파 잠금을 사용하였다. 그러나 전파 잠금의 사용은 원본이 있는 지역으로 제출되는 LT를 연기시킨다. [2, 4, 12-13]은 동질적인 데이터베이스의 보안 환경, [14]은 이질적인 데이터베이스의 보안 환경에서 트랜잭션들이 보안 정책을 위반하지 않고 1SR을 보장할 수 있도록 하였다. [12]에서는 상위 등급의 데이터베이스에 하위 등급의 데이터를 모두 중복시켜 하위 등급의 데이터베이스에서 상위 등급의 데이터베이스로 정보가 흐르도록 하므로써 간접적으로 정보가 유출될 수 있는 비밀경로 문제를 제거하였다. 그러나 중복에 따른 비용이 과다하고 중복 데이터가 일관된 값을 갖도록 안전하게 전파하는 방법은 제시하지 않았다. [2, 13, 15]는 보안과 중복 구조 데이터베이스 모델의 표기를 [12]에서 채택해 사용했다. [13]은 다단계 보안 데이터베이스에 대한 새로운 트랜잭션 모델을 제안하고 제출 전에 충돌을 검사하여 갱신 프로잭션에 대한 제출 처리를 한번에 하나씩 하는 비관적 방법, 충돌 갱신 프로잭션에 대한 제출 순서를 유지하는 준낙관적 방법, 검사나 연기가 없는 낙관적 방법을 제안했다. [2, 15]는 동질적인 환경의 다단계 보안 데이터베이스에 대해 한 트랜잭션의 연산과 데이터 항목이 부분적으로 다른 보안등급을 갖는 다단계 트랜잭션을 정의하고 트랜잭션 처리에 대해 원자성의 개념을 도입하여 새로운 정확도의 개념으로 종속성이 있는 몇 개의 트랜잭션이 중첩되어진 다단계 트랜잭션에 대한 다단계 1-사본 직렬성(Multilevel 1SR)을 정의하여 알고리즘을 제시하고 증명하였다. [14]에서는 다단계 보안 연합 데이터베이스 시스템[16]에서 지역 자치성과 보안 요구사항을 고려하여 트랜잭션의 전역적 직렬성을 보장하도록 동시성 제어 알고리즘을 제안하였다. 각 지역의 보안 부분 순서 집합이 전체적으로 순서화 될 때 보안 검증 알고리즘은 타임스탬프 순서로 GT를 직렬화하고 부트랜잭션들이 지배하는 모든 티켓을 읽도록 요구하여 전역적으로 1-사본 직렬 가능한 히스토리를 유지하였다. 그러나 각 지역의 보안등급이 전체적으로 순서화 되어야 하고 각 보안등급마다 개별적으로 트랜잭션 관리자를 두고 있어 시스템 구축시 상당한 부담이 된다[7].

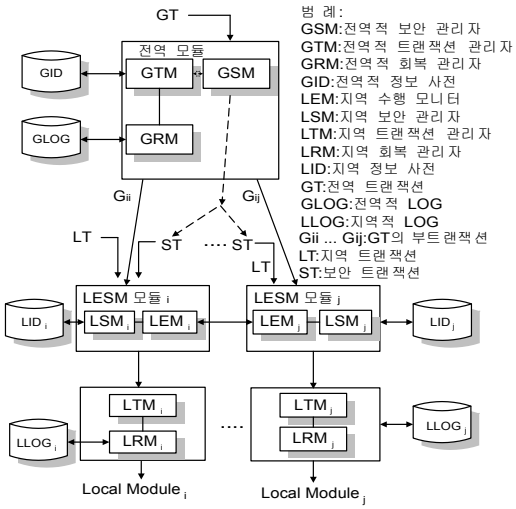
2.2 전역트랜잭션의 준직렬성

MDBS에서 GT의 전역적 제어를 위한 정확성 기준으로써 QSR[6]이 제시되었다. GT의 직렬화 순서를 LT와 관계없이 유지시키므로 QSR은 직렬성 보다는 제약이 약하며 보장하기가 쉽다. 전역적 트랜잭션 관리자(Global Transaction Manager, 이하 GTM)는 각 지역에서 수행되는 부트랜잭션을 제어한다. 다른 지역에서 수행되는 지역 트랜잭션(Local Transaction, 이하 LT)들은 서로 직접적인 선행관계는 없다. 수행 E_1: $GT_1 \rightarrow LT_1 \rightarrow GT_2$이고 수행 E_2: $GT_2 \rightarrow LT_2 \rightarrow GT_1$이다면 LT_1과 LT_2의 선행관계는 연관이 없다. GTM은 전역 순서대로 GT_1과 GT_2의 직렬화 순서를 제어하면 된다. 전체 순서가 $GT_1 \rightarrow GT_2$라면 수행 E_2에서 $LT_2 \rightarrow GT_1 \rightarrow GT_2$처럼 GT_2를 GT_1 다음으로 연기하면 된다. 1QSR[5]은 각 지역에 데이터의 사본을 갖는 MDBS에서 QSR를 확장시켜 전역적 동시성을 제어하는 정확성 기준으로 제시되었다. 각 지역에서의 수행은 직렬가능하고 전역 순서가 $T_i \rightarrow T_j$이면 각 지역에서 $^{\forall}op_i \rightarrow {}^{\forall}op_j$로 수행되어야 하며 판독관계와 마지막 기록연산이 동일해야 한다. MLS/1QSR[7-8]은 MDBS의 보안환경에서 1QSR에 보안성을 고려하여 GT의 전역적 동시성을 제어하기 위한

정확성 기준으로써 정의된다. 보안 관리자는 트랜잭션과 데이터를 MLS/MDBS에서 표준화된 보안성 평가 기준에 따라 분류하여 등급을 할당한다. 각 지역 데이터베이스 시스템(Local Database System, 이하 LDBS)의 지역 보안 관리자(Local Security Manager, 이하 LSM)은 데이터와 트랜잭션에 합당한 보안등급을 할당하여 그 지역의 데이터가 안전하게 보호되고 정확한 값을 유지하도록 한다. 따라서, MLS/MDBS에서는 기존의 지역 자치성으로 알려진 통신, 설계, 그리고 수행 자치성 이외에 [17]에서 제시한 보안 자치성을 함께 고려한다. 즉, 각 LSM은 그 지역에 속하는 트랜잭션과 데이터에 대해서 독자적으로 보안등급을 할당하여 그 지역 데이터베이스를 보호할 자치적 권한을 갖는다. 기존의 직렬성에서 사용되는 판독관계는 MLS/MDBS의 보안 자치성에 대해서 적절하지 못하므로 보안성과 판독관계를 고려하여 보안 판독관계가 제시된다. 전역트랜잭션의 MLS/1QSR의 보장을 위해서 전역순서대로 수행되는 트랜잭션이 보안 판독관계를 만족시킴으로써 직접적인 정보 유출이 방지되도록 하였다. 또, 트랜잭션들의 공모로 연산 충돌시 형성되어 간접적으로 정보가 유출될 때 가장 최신 값을 보호하였다. 보안 판독관계에서 $T_i \rightarrow T_j$, $SL(T_j) =_H SL(T_i)$, $T_i, T_j \in \{\text{only GTs}\}$일 경우 $R^B_j[W^B_i(X^B)]$는 T_i와 T_j가 동일한 등급이므로 직접적인 정보 유출 문제는 발생하지 않지만 보안성이 고려되지 않은 기존의 판독관계처럼 간접적인 정보 유출이 발생할 수 있다. 또한, 보안등급 관계가 $B <_H A$ 인 경우 $R^A_j[W^B_i(X^B)]$는 전역순서 $T_i \rightarrow T_j$에 대해서 $SL(T_j) >_H SL(T_i)$일 때 $T^T_j:w^T_j(y^T)r^T_j(x^S)$, $T^S_i:w^S_i(x^S)$이고 E_1: $w^S_i(x^S)w^T_j(y^T)r^T_j(x^S)$이면 트랜잭션들이 전역순서대로 수행될 수 있도록 위반되지 않는 상하위 보안등급을 갖기 때문에 하위등급인 T_i가 먼저 수행되어 정보 유출은 발생하지 않는다. 그런데, 보안 판독관계가 위반되는 경우 즉, $SL(T_j) <_H SL(T_i)$일 때 $T^T_i:w^T_i(y^T)r^T_i(x^S)$, $T^S_j:w^S_j(x^S)$이고 E_2: $w^T_i(y^T)r^T_i(x^S)$ $w^S_j(x^S)$이면 전역순서대로 수행되지만 상하위 보안등급이 위반되기 때문에 간접적으로 정보가 유출될 수 있는 경로가 형성된다.

Ⅲ. 시스템 모델

GT의 전역적 제어를 위해 사용되는 환경인 MLS/MDBS의 모델은 기존의 MDBS 모델에 보안 모듈을 확장시켜 <그림 1>와 같이 세 단계의 주요 모듈 즉, 전역 모듈, 지역 수행 및 보안 관리 모듈, 그리고 지역 모듈로 구성된다. 전역 트랜잭션 관리자는 GT가 제출되면 물리적 연산을 하기 위해 부트랜잭션으로 분해하여 데이터를 접근할 수 있도록 부트랜잭션의 순서를 정하여 지역 수행 모니터(Local Execution Monitor, 이하 LEM)에게 부트랜잭션을 제출하고 원자적 완료 프로토콜에 따라 조정자 역할을 한다. 그러나 LT에 대한 정보를 직접 알지 못하며 LT를 제어 할 수 없다. 전역 보안 관리자(Global Security Manager, 이하 GSM)는 MLS/MDBS에서 표준화된 보안등급 평가 기준에 따라 GT의 보안등급을 관리한다. 그리고 한 데이터의 원본(Primary copy, 이하 Pc)에 기록연산이 수행될 때 각 지역에 있는 사본(Secondary copy, 이하 Sc) 값을 변경하는 보안 트랜잭션(Security Transaction, 이하 ST)을 지역 수행 및 보안 관리자 모듈(Local execution and Security Module, 이하 LESM)로 제출한다. ST는 GSM이 보안등급을 할당하고 사본을 단



<그림 1> MLS/MDBS 모델

순히 갱신하여 새로운 갱신 값을 만들도록 제출되며 보안성이 확실한 트랜잭션이다. GT가 데이터에 각 연산을 수행할 수 있도록 합당한 보안등급 관계가 형성될 때 ST는 각 지역에 중복되어 있는 사본에 갱신전 값(Before Value, 이하 BeV)과 갱신후 값(After Value, 이하 AeV)를 유지하므로 T∈{(GT)∪(ST)} 사이에서 가장 최신 데이터에 대한 간접적인 정보 유출을 방지할 수 있다.

Ⅳ. 전역적 스케쥴링

이 장에서는 MLS/MDBS 환경에서 GT이 MLS/1QSR을 보장하도록 전역적으로 제어되기 위한 알고리즘(Algorithms for Guaranteeing MLS/1QSR, 이하 AGM)을 제안하고 정확성을 증명한다.

4.1 알고리즘

AGM에서 사용되는 자료구조는 다음과 같다. 전역 큐(Global queue, 이하 Gq)는 각 데이터에 대해 연산을 수행한 트랜잭션을 제출 순서대로 유지시킨 전역 직렬화 순서(Global Serialization Order, 이하 GSO)를 갖는다. 갱신 큐(Updated queue, 이하 Uq)는 원본이 갱신되었지만 사본 갱신이 미확인된 ST의 직렬화 순서(Secure Transaction Serialization Order, 이하 STSO)를 유지한다. 지역 큐(Local queue, 이하 Lq)는 지역에서 수행되는 지역 직렬화 순서(Local Serialization Order, 이하 LSO)와 사본을 갱신한 마지막 트랜잭션을 갖는다. AGM은 GT가 제출될 때 전역 모듈, 원본 선택, LESM 모듈, 지역 모듈에 대한 알고리즘을 호출한다.

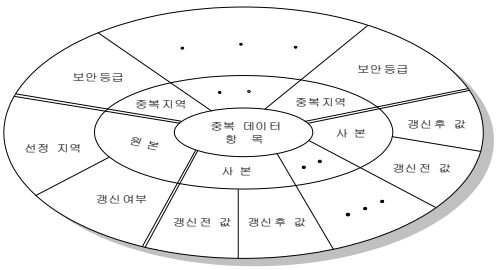
전역적 수행이 MLS/1QSR을 유지할 수 있도록 하기 위해 간접적인 정보 유출 방지와 보안 자치성을 고려하여 집합 {(GT)∪(ST)}의 전역순서가 보장되도록 한다. 간접적인 정보 유출의 경로가 설정될 경우 GT의 전역순서를 유지하면서 데이터에 대한 최상의 h-SL의 값이 보호되도록 한다. 따라서 BeV와 AeV에 대한 GT의 접근이 전역순서를 위반하지 않도록 제어된다. GSM은 보안성을 신뢰할 수 있는 트랜잭션인 ST를 LESM으로 제출한다.

Algorithm **GlobalModule(GTM, GSM for GTs)**:

1. If Gq is Front = Rear
   Then Execution Exit.
2. If Gq is Front ≠ Rear /*직렬화된 전역트랜잭션 존재*/
   Then {
   1) Insert GT into Gq
   /*GT보안등급*/ Assign SL(GT)∈{T, S, C, U} by GSM
   2) Decompose GT into SubTs
   /*각 연산목록 생성*/3) Make readlist, writelist for SubTs
   4) Search GID(IW) for replicated data
   /*기록연산*/ 5) If SubTs ∈ { write_set }
   /*원본선택 호출*/ Then Call **PrimaryCopySelection**
   6) Submit SubTs into each LESM
   /*원본지역에 ST 제출*/ 7) Issue ST into LESM_Site(D^P)
   }
3. If GT Commit or Abort
   Then Delete it in Gq/*연산종료된 트랜잭션 제거*/
4. Repeat 1. to 3.

각 지역에 중복되어 있는 데이터에 대해 원본을 결정하기 위하여 먼저, GTM이 GT를 각 지역에 부트랜잭션으로 제출하고 GSM이 GT에 보안등급을 할당할 때 GT의 구성연산을 알 수 있으므로 제출된 GT의 판독연산 집합과 기록연산 집합을 구한다. 그런 다음, 중복 데이터의 일관성과 보안성 유지를 위하여 데이터 갱신은 신중히 이뤄져야 하므로 기록집합의 각 원소에 대해 여러 지역에 중복된 데이터 중에서 최상 보안등급을 갖는 데이터를 원본으로 정한다. 판독집합의 원소인 경우는 상위등급의 정보를 보호하기 위하여 GT의 보안등급과 동일한 데이터를 원본으로 정한다. GSM은 전역 정보 사전(Global Information Dictionary, 이하 GID)에 있는 <그림 2>의 정

보 윈도우(Information Window, 이하 IW)를 참조하여 전역적으로 원본이 존재하는 지역을 결정한다. 따라서, 중복 데이터의 원본 결정은 지역 자치성을 위배하지 않는다.

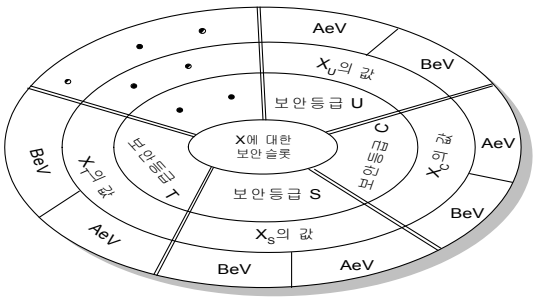


<그림 2> 전역 정보 사전의 정보 윈도우

Alogorithm **PrimaryCopySelection(Replicated_Data)**:

1. If Operation ∈ { write_set }/*기록연산*/
Then Reference GID(IW) by GSM/*전역정보사전참조*/
2. If highest $SL(RD)_{RD \in write\_set}$}/*최상위보안등급*/
in each replicated $D \in^{\forall}$(site)
Then Select a Site(D^{P})/*기록연산 원본*/
for write_op as primary copy
3. If Operation ∉ { write_set }/*판독연산*/
Then Select Same_SL($D \in^{\exists}(site_i)$)/*판독연산 원본*/
for read_op as primary copy
4. Return SelectPrimaryCopy_msg /*메세지 반환*/
to GlobalModule(GSM)

GT들간의 연산충돌이 빠르게 탐지될 수 있도록 먼저 원본이 갱신된 후 사본이 변경된다. 각 사본은 사본의 값이 변경될 때 Sc_{BeV}와 Sc_{AeV}를 갖는다. ST는 갱신된 원본의 값에 대하여 여러 지역의 사본을 전역적으로 기록연산만을 수행하여 갱신하므로 LT와 성격이 다르며, 전역적으로 합의되어 암호화된 특별한 트랜잭션이다. 각 지역에 제출되는 ST는 갱신연산, 갱신될 사본의 지역과 보안등급, 그리고 원본의 갱신 후의 값으로 구성된다. ST의 보안등급은 GSM이 GID의 IW를 참조하여 보안 함수(Security Function, 이하 SF)에 따라 결정한다. SF는 ST가 각 사본을 접근할 수 있도록 ST에게 모든 사본에 대해 제약된 *-성질을 만족하는 보안등급을 매핑한다. 지역 수행 모듈(Local Execution Module, 이하 LEM)은 GT에 대해 원자적 완료 프로토콜의 참가자 역할을 하고 GTM이 제출한 부트랜잭션을 받아 지역 데이터베이스 시스템(Local Database System, 이하 LDBS)으로 제출하며 LDBS의 결과를 GTM에게 반환한다. 다른 지역의 LEM과 서로 통신하여 GT의 직렬성을 유지하기 위한 정보를 제공한다. 지역 보안 관리자(Local Security Manager, 이하 LSM)는 그 지역의 LT와 데이터에 대해 MLS/MDBS에서 표준화된 보안등급 평가 기준에 따라 독자적으로 보안등급을 할당하며 지역에 필요한 정보를 지역 정보 사전(Local Information Dictionary, 이하 LID)에 유지한다. LID는 <그림 3>와 같다.



<그림 3> 지역 정보 사전에 있는 데이터 X의 보안슬롯

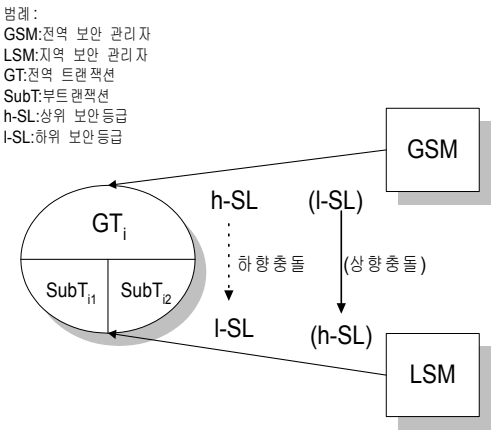
Algorithm **LESMModule(LEM, LSM for SubTs, STs, LTs)**:

1. If SubTs are SecurityLevelConflict
Then Call **SolveSLConflict**/*보안등급충돌 해결호출*/
2. If SubTs are operation_conflict
Then { According to GSO,
1) Case(read):/*판독연산*/
/*모든 사본의 갱신완료*/If $Sc(^{\forall}site)$ = Update_OK
/*사본의 갱신후 값 판독*/ Then Read Sc_{AeV}
/*사본의 갱신전 값 판독*/ Else Read Sc_{BeV}

2) Case(write):/*기록연산*/
/*원본 확인*/ Confirm Pc($^{\forall}$site)
/*모든 사본에 ST제출*/ Issue ST into Sc($^{\forall}$site)
}
3. If Uq is Front = Rear /*원본 갱신이 없음*/
Then ST is Finish
Else {
1) Contain $W^{S}(Pc_{Aev}:S_i)$ for STs
/*보안함수에 따른 ST를 사본 지역에 제출*/
2) SF: {SL (D) $=_H$ SL(write_op.)} → SL(ST))
for Sc(D) $\in^{\forall}$(site)
3) Update Sc($^{\forall}$site) /* 모든 사본 갱신 */
4) Maintain Uq to STSO
/*메세지 반환*/5) Return ScUpdate_msg to GID(IW)
}
4. If LT is submitted /*지역 트랜잭션 제출*/
Then Send LocalModule
5. Repeat 1. to 4. for each Transaction

GSM이 할당한 보안등급은 각 지역의 보안 자치성으로 인하여 LSM이 GSM과 다른 보안등급을 GT의 부트랜잭션에게 할당하는 경우가 발생한다. 즉, GSM이 GT에 보안등급을 할당하고 GT의 부트랜잭션들이 각 해당 지역으로 제출되면 LSM이 그 부트랜잭션에게 다른 보안등급을 할당한다. GSM이 할당한 보안등급보다 LSM이 높게 보안등급을 할당할 경우 상향 등급 충돌, 낮게 보안등급을 할당할 경우 하향 등급 충돌이라 한다.

Algorithm **SolveSLConflict(GSM, LSM)**:
1. If GSM(SL) $=_H$ LSM(SL) /*보안충돌 없음*/
Then Execution Exit
2. If GSM(SL) $_H>$ LSM(SL) /*하향등급 충돌*/
Then {
1) If Operation is read_op/*판독연산*/
/*보안슬롯의 갱신후 값 판독*/Then Read SecureSlot(AeV)



<그림 4> 보안등급 충돌

SS: 2) If Operation is write_op /*기록연산*/
/*보안슬롯의 갱신후 값 생성*/
Then Create each SecureSlot(AeV)
in LID(IW) }
3. If GSM(SL) $<_H$ LSM(SL) /*상향등급 충돌*/
Then {
1) If Operation is read_op/*판독연산*/
Then Read each SecureSlot(BeV)
/*각 보안슬롯의 갱신전 값 판독*/ in LID(IW)
2) If Operation is write_op
Then Go to SS
}
4. Return SolveSLConflict_msg /*결과 메세지 반환*/
to GlobalModule(GSM)

각 지역으로 제출된 트랜잭션인 LT의 지역적 순서 제어는 지역 트랜잭션 관리자(Local Transaction Manager, 이하 LTM)가 스케줄링한다.

Algorithm **LocalModule(LTM)**:
1. IF Lq is Front = Rear
Then Execution Exit.

2. If Lq is Front ≠ Rear /*직렬화된 지역 트랜잭션 존재*/
   Then {
      1) Submit LTs into LTM
      2) According to LSO /*지역 직렬화 순서*/
         Execute LTs, SubTs/*대로 구별없이 수행*/
            without distinguish
   }
3. If LT Commit or Abort
   Then Delete it in Lq /*연산 종료된 트랜잭션 제거*/
4. Return LT'sExecutionResult_msg to LESM
5. Repeat 1. to 4.

4.2 정확성 증명

이 절에서는 다음의 (정리 4.1)을 통하여 AGM의 정확성을 증명한다.

【정리 4.1】 다단계 보안 1-사본 준직렬성
AGM은 전역트랜잭션들 사이에서 전역적으로 다단계 보안 1-사본 준직렬성을 보장한다. □

증명) $S_i \in ST$, $T_j \in \{(GT) \cup (ST)\}$이고 각 지역에서 트랜잭션들 사이에 선행 관계를 경우 1과 경우 2를 통하여 살펴보기로 하자.

경우 1: (지역 $_i$)에서 $T_j \rightarrow S_i$이고 (지역 $_j$)에서 $S_i \rightarrow T_j$
(지역 $_i$)에서 T_j가 S_i를 선행하고 (지역 $_j$)에서는 S_i가 T_j를 선행할 때 (지역 $_j$)에서 S_i가 제출되기 전에 (지역 $_i$)에서 T_j가 도착했으므로 $T_j \rightarrow S_i$가 된다. (지역 $_j$)는 전역모듈로부터 이 순서를 통보받고 이를 시행하기 위하여 (지역 $_j$)에서는 T_j가 선행할 수 있도록 즉, $T_j \rightarrow S_i$되도록 S_i를 연기시키게 된다.

경우 2: (지역 $_i$)에서는 $T_j \rightarrow S_i$ 이고 (지역 $_j$)에서는 $S_i \rightarrow T_j$, $T_j \in$ GT 혹은 ST

(지역 $_i$)에서 S_i가 T_j를 선행하고 (지역 $_j$)에서는 T_j가 S_i를 선행하며 $T_j \in$ GT 혹은 ST 일 때, S_i의 보안등급이 T_j의 보안등급 보다 높거나 같고 T_j의 보안등급은 데이터 x의 보안등급과 같다고 하자. (지역 $_j$)에서 $T_j \in$ GT 일 때, GSO가 $S_i \rightarrow GT_j$라면 S_i가 시행되기 전에 T_j가 갱신을 한다. 이들 간에는 보안 성질이 $SL(T_j) =_H SL(x)$이고 $SL(T_i) \geq_H SL(T_j)$ 인 것을 고려한 판독 관계인 $r_i(w_j(x))$의 관계가 성립한다. $T_j \in$ ST 일 때 (지역 $_j$)에서 늦게 도착하는 S_i는 토머스 기록 규칙인 TWR에 따라서 무시하고 수행 완료 메세지를 반환한다. 따라서 두 지역에서 동일하게 보안 판독 관계가 성립한다. 경우 1과 경우 2는 모든 지역에서 수행은 직접 혹은 간접적인 정보 유출없이 직렬 가능하다. 그리고 $T_i, T_j \in \{(GT) \cup (ST)\}$의 전역적 직렬 순서가 $T_i \rightarrow T_j$일 경우 각 지역에서 수행되는 트랜잭션의 모든 지역의 연산은 $^{\forall}op_i \rightarrow {}^{\forall}op_j$이다. 또, $T_i, T_j \in \{(GT) \cup (ST)\}$에 대해서 T_i가 데이터를 갱신한 마지막 연산이고 보안 판독관계라면 T_j는 마지막 갱신 후 값인 AeV을 판독한다. 간접적인 정보 유출이 있는 경우 보안 판독관계라면 $T_i \rightarrow T_j$대로 수행하고 T_j는 갱신 전 값인 BeV을 판독한다. 1-사본 준직렬성과 유사하게 모든 지역 수행에서 ST를 포함한 GT의 전역적 직렬 순서가 동일하다. ST는 각 지역의 사본을 갱신하도록 기록연산을 수행하므로 데이터의 일관성을 유지 하도록 ST와 GT 사이의 전역적 직렬 순서가 보장된다. 간접적인 정보 유출 없이 마지막 기록연산과 보안 판독관계가 각 지역 수행에서 동일하다. 그러므로, GT들의 전역적 수행은 다단계 보안 1-사본 준직렬성을 보장하게 된다.

V. 결론

정보를 보호하기 위하여 보안 문제가 중요시 고려된다. 기존의 시스템에서 트랜잭션들 사이의 직렬성만 유지되던 트랜잭션들은 보안성도 고려하여야 한다. 보안 환경에서 중복 데이터들의 일관성이 유지되도록 GT들은

다단계 보안 1-사본 준직렬성이 보장되도록 스케줄링 되어야 하며 불법적인 데이터 접근 방지를 위해서는 보안 정책인 단순 성질과 *-성질이 요구된다. 본 논문에서는 다단계 보안 환경을 기반으로 하여 중복된 데이터를 갖는 이질형 시스템에서 기존의 1-사본 준직렬성을 다단계 보안 1-사본 준직렬성으로 확장하여 전역트랜잭션들이 각 지역의 보안 자치성을 위배하지 않고 전역적으로 다단계 보안 1-사본 준직렬성을 보장할 수 있는 AGM을 제안하였다. AGM은 모든 지역에서 각 보안등급마다 여러 개의 트랜잭션 관리자를 두어 1-사본 직렬성을 유지하는 기존 방법과는 다르게 전역과 각 지역에 트랜잭션 관리자와 보안 관리자를 두면서 중복 데이터들의 전역적 일관성을 유지 시키고 각 지역의 보안 자치성을 보장하도록 한다. 또한, 보안 자치성에 따른 보안등급 충돌을 효율적으로 해결한다. 향후 연구로는 전역트랜잭션의 전역적 일관성이 유지되면서 각 지역에서의 효율적인 스케줄링 기법과 각 지역의 보안정책에 따른 시스템의 오버헤드를 경감시켜 성능을 개선하는 부분이 고려되어야 한다.

참고문헌

[1] S. Castano, *DatabaseSecurity*, Addison-Wesley, 1994, pp. 82-96.

[2] O. Costich, “Transaction Processing Using an Untrusted Scheduler in a Multilevel Database with Replicated Architecture,” Database Security V: Status and Prospects, C. E. Landwehr and S. Jajodia(Editors), Elsevier Science Publishers B. V. (North-Holland) IFIP, 1992, pp. 173-189.

[3] Bernstein, *Concurrency Control & Recovery in Database Systems*, Addison-Wesl ey, 1987.

[4] J. Tang, “Managing Replicated Data in Heterogeneous Database Systems,” Proceedings, 11th Symposium on Reliable Distributed Systems, 1992, pp. 12-19.

[5] W. Du, et al, “Supporting Consistent Updates in Replicated Multidatabase Systems,” VLDB, Journal No. 2, 1993, pp. 215-241.

[6] W. Du, Elmagarmid A., “Maintaining Quasi Serializability in Multidatabase Systems," Proceedings, 7th International Conference on Data Engineering, 1991, pp. 360- 367.

[7] H. C. Jeong, “Transaction Serializability with Security in Heterogeneous Medical Database Systems,” Journal Korean Society of Medical Informatics, 1999, pp. 73-86.

[8] H. C. Jeong, “Global Transaction Control with Multilevel Security Environments,” LNCS 4223, 2006, pp. 660-663.

[9] C. P. Pfleeger, *Security in Computing*, Prentice Hall, 1989, pp. 249-250.

[10] R. Sandhu, “Lattice-Based Access Control Models,” IEEE Computer, 1993, pp. 9-19.

[11] J. Jing, Du W., Elmagarmid A., Bukhres O., “Maintaining Consistency of Replicated Data in Multidatabase Systems,” IEEE, 1994, pp. 552-559.

[12] S. Jajodia, B. Kogan, “Transaction Processing in Multilevel-Secure Databases Using Replicated Architecture,” Proceedings, Symposium on Security and Privacy, 1990, pp. 360-368.

[13] M. H. Kang, O. Costich and J. N. Froscher, “A Practical Transaction Model and Untrusteded Transaction Manager for a Multilevel-Secure Database System,” Database Security VI: Status and Prospects (A-21), B. M. Thuraising- ham and C. E. Landwehr (Editors), Elsevier Science Publishers B. V. (North-Holland) IFIP, 1993, pp. 285-300.

[14] I. E. Kang, T. F. Keefe, "Concurrency Control for Federated Multilevel Secure Database Systems," 8th IEEE Computer Security Foundations Workshop, 1995, pp. 118 -135.

[15] O. Costich, "Maintaining Multilevel Transaction Atomicity in MLS Database Systems with Replicated Architecture," Database Security, VII (A-47), T. F. Keefe and C. E. Landwehr (Editors), Elsevier Science B. V. (North-Holland) IFIP, 1994, pp. 329-355.

[16] B. Thuraisingham, "Security issues for Federated Database systems," Computer & Security, 1994, pp. 509-525.

[17] H. C. Jeong, "Managing of Replicated Data in MLS/DMDBS," Proceedings, 1st KIPS Spring Conference, Korea Information Processing Society, 1995, pp. 203-206.

■ 저자소개 ■

정 현 철
Jeong, Hyun Cheol

1998년 3월~현재
광주보건대학 병원전산관리과 교수
1997년 8월 전남대학교 전산학과(이학박사)
1989년 2월 중앙대학교 전산학과(이학석사)
1987년 2월 조선대학교 전산통계학과(이학사)

관심분야 : 정보보안, 의료정보, 유비쿼터스
E-mail : hcjeong@ghc.ac.kr

논문접수일 : 2009년 10월 19일
수 정 일 : 2009년 11월 10일
게재확정일 : 2009년 11월 17일