성능을 고려한 이동 에이전트 보안 모델
(A Security Model of Mobile Agent Regarding Performance)

유 응 구 † 이 금 석 ††
(Eung-Gu You) (Keum-Suk Lee)

요 약 인터넷이 널리 사용되면서 이동 에이전트와 관련된 기술들은 지속적인 관심과 연구의 대상이 되고 있다. 이동 에이전트는 분산 정보 검색, 네트워크 시스템 관리, 분산 시스템 관리, 전자 상거래 분야에서 기존의 통신 패러다임보다 우수한 성능을 나타낸다. 이런 우수한 성능에도 불구하고 이동 에이전트가 상업적으로 널리 사용되지 않는 이유는 이동 에이전트가 갖는 보안 취약성 때문이다. 최근 이동 에이전트의 보안에 대한 연구가 활발히 진행되고 있지만 대부분 보안성을 높이기 위해 복잡한 연산이나 규약을 사용함으로써 성능 저하를 유발하였다.

따라서 본 논문에서는 상호 신뢰하는 이동 에이전트 시스템을 신뢰 도메인(Trusted Domain)으로 관리하고, 보안 서비스를 제공하며, 지역성을 고려한 여행을 안내하는 역할을 수행하는 TDGM(Trusted Domain & Guide Manager)을 이용한 이동 에이전트 보안 모델을 제안하고, 그 성능을 평가하였다. 제안한 모델은 이동 에이전트를 이용한 대규모 분산 검색 환경에서 높은 보안성을 제공하면서도 성능 저하를 최소화하는 것을 살펴볼 수 있다.

키워드 : 이동 에이전트, 보안, 신뢰 도메인

Abstract As the proliferation of Internet, mobile agent related technologies are examined for possible growth and evolution. In information retrieval, network and distributed system management, and electronic commerce, mobile agent is more flexible than the traditional communication paradigm. Despite the performance benefits, mobile agent is not used widely in the market because it is very vulnerable to a variety of attacks. In many studies related the security vulnerability for a mobile agent, the high security causes the performance to degrade.

In this paper, we propose and evaluate the efficient security model for mobile agent using TDGM(Trusted Domain & Guide Manager), which provides three kinds of services : the trusted domain management, the security service and the travel plan guide. The result clearly shows that this model provides high security and minimizes the performance degradation.

Key words : mobile agent, security, trusted domain, TDGM

1. 서 론

인터넷 사용이 크게 증가하면서 인터넷 정보 검색, 전자상거래, 네트워크 시스템 관리, 분산 시스템 관리 등 분산 응용을 위한 효율적인 통신 패러다임에 대한 연구가 진행되고 있다. 기존의 통신 패러다임으로는 RPC (Remote Procedure Call)를 기반으로 한 클라이언트-서버 모델이 사용되어 왔다. RPC 모델은 개념적으로 단순하고, 구현이 간단하기는 하지만 지속적인 연결과 많은 통신 부하로 분산 환경을 효율적으로 사용하는데 적합하지 않다. 이러한 문제를 해결하고자 분산 응용을 위한 통신 패러다임으로 이동 에이전트가 연구되어 왔다. 이동 에이전트는 분산되어 있는 호스트 사이를 이동하면서 사용자를 대신하여 작업을 수행하는 소프트웨어이다. 이동 에이전트는 자료가 있는 곳으로 이동하여 사용자를 대신하여 작업을 수행할 수 있기 때문에 대량의 자료 이동으로 인한 네트워크 부하를 줄일 수 있고, 비동기적 실행을 지원하기 때문에 지속적인 연결을 요구하지 않는다. 많은 연구에서 이동 에이전트를 이용한 방법은 기존의 방법보다 유연성과 우수한 성능을 나타내고 있다[1-4].

그럼에도 불구하고 상업적인 목적으로 개발된 분산 응용들 중에서 통신 패러다임으로 이동 에이전트를 사

† 학생회원 : 동국대학교 컴퓨터공학과
engus@dongguk.edu
†† 정 회 원 : 동국대학교 컴퓨터공학과 교수
kslee@dongguk.edu
논문접수 : 2003년 5월 16일
심사완료 : 2003년 8월 5일

용하는 예는 극히 드물다. 이것은 기존의 이동 에이전트 모델 대부분이 실제 분산 환경을 제대로 반영하지 못하는데 그 원인을 찾을 수 있다. 실제 분산 환경은 개방된 환경으로 다양한 보안 위협에 노출되어 있기 때문에 이러한 환경에서 안전하게 실행되기 위해서는 보안 위협으로부터 호스트, 이동 에이전트 시스템, 이동 에이전트를 보호하는 방법의 고려가 필수적이다[5-7]. 그러나 기존의 연구들은 보안을 고려하지 않았기 때문에 실제 분산 환경에 적용하기 어려웠다.

최근 지금까지 연구되어 왔던 이동 에이전트 성능 모델을 비교한 연구[8]과 보안을 고려한 이동 에이전트 성능에 대한 연구[9]가 발표되었고, 다양한 보안 모델이 연구되고 있다. 그러나 대부분의 연구들은 보안 수준을 높이기 위해 복잡한 연산이나 규약을 사용하기 때문에 이동 에이전트를 이용함으로써 얻을 수 있는 성능 향상을 기대하기 어렵다.

따라서 본 논문에서는 TDGM을 이용한 이동 에이전트 보안 모델을 제시하고, 성능을 평가하였다. TDGM은 신뢰 도메인을 관리 서비스를 제공하고, 인증 및 암호 모듈과 연동하여 보안 서비스를 제공하며, 도메인 지역적인 여행 계획을 안내하는 서비스를 제공하기 때문에 제안한 보안 모델은 높은 보안 수준을 제공하면서도 성능의 저하를 최소화할 수 있다.

본 논문의 구성은 2장에서 기존에 연구되어 왔던 이동 에이전트 보안 방법, 성능 모델 및 신뢰 도메인에 대하여 살펴본다. 3장에서는 제안한 이동 에이전트 보안 모델을 살펴본다. 4장에서는 제안한 모델의 성능을 알아보고, 5장에서는 실험을 통하여 평가해본다. 마지막 6장에서는 결론 및 향후 연구에 대하여 기술한다.

2. 관련연구

2.1 이동 에이전트 보안

이동 에이전트 보안은 크게 이동 에이전트 시스템 보안, 호스트 보안 및 이동 에이전트 자체에 대한 보안으로 분류된다.

이동 에이전트 시스템에 대한 보안은 이동 에이전트 보안 분야 중에서 가장 활발한 연구가 진행 중인 분야로 호스트나 이동 에이전트의 공격으로부터 에이전트 시스템을 보호하는 것으로 보안 관리자를 이용한 방법과 제한된 실행 환경을 제공하는 방법 등이 연구되어 왔다.

호스트 보안은 악의적인 이동 에이전트의 공격으로부터 호스트를 보호하는 것으로 표준 라이브러리나 서비스를 통해서 호스트 자원을 접근할 수 있도록 하는 방법이나 인증 및 접근 제어를 이용하는 방법이 연구되어 왔다.

이동 에이전트 보안은 악의적인 호스트나 다른 이동 에이전트의 공격으로부터 에이전트를 보호하는 것으로 비밀성을 높이기 위해 암호화 기법을 이용하는 방법[6], SSL과 같은 안전한 통신 채널을 이용하는 방법, 에이전트 재구성을 통해 중요 자원을 보호하는 방법[10] 등이 연구되어 왔다.

2.2 이동 에이전트 성능

이동 에이전트 성능은 분산 정보 검색, 네트워크 및 분산 시스템 관리 분야에서 활발히 연구되어 왔고, 많은 연구에서 RPC, REV(Remote Evaluation) 방법보다 우수한 성능을 제공하는 것으로 연구되었다[3,4,8]. 그러나 기존의 이동 에이전트 성능은 분산 컴퓨팅 환경을 제대로 반영하지 못하고 있어 실제 적용이 어려웠다.

최근 보안 서비스를 고려한 이동 에이전트 성능에 대한 연구가 발표되었다[9]. [9]에서는 중앙에 안전한 키 분배 센터를 통하여 인증 서비스를 제공하고, 암호화와 서명을 이용하여 비밀성과 무결성을 제공하는 이동 에이전트 모델을 제안하였다.

2.3 신뢰 도메인(Trusted Domain)

대부분의 이동 에이전트 보안은 인증과 비밀성, 무결성을 제공하기 위해 키분배, 암호화, 복호화 같은 복잡한 보안 연산을 수행한다. 이런 보안 연산은 이동 에이전트 시스템을 복잡하게 만들고, 이동 에이전트의 성능을 저하시킨다.

최근 도메인을 이용한 보안 모델이 연구되고 있고[11,12], 이동 에이전트 시스템들 간의 상호 신뢰를 이용한 보안 모델이 연구되고 있다[13,14]. 이런 보안 모델은 이동 에이전트 시스템의 복잡도를 낮추고, 보안 정책의 관리가 용이하며, 도메인 내의 보안 연산을 줄임으로써 향상된 성능을 제공한다.

3. TDGM을 이용한 보안 모델

[9]에서 제안한 모델은 중앙의 키 분배 센터를 이용하여 인증 서비스를 제공하고, 암호화를 이용하여 비밀성을 제공하며, 서명을 이용하여 무결성을 제공하면서도 Secure RPC보다 우수한 성능을 나타내고 있다. 그림 1은 [9]에서 제안한 중앙 집중형 보안 서비스 모델의 구성도를 나타낸다.

그러나 그림 1의 중앙 집중형 보안 서비스 모델에서는 키 분배 센터가 키 분배와 인증을 하기 때문에 대규모 분산 환경에 적용하기 어렵고, 이동 에이전트가 이동할 때마다 고비용의 보안 연산이 발생하기 때문에 전체 작업 시간이 증가하는 단점이 있다.

신뢰 도메인만을 이용한 모델은 상호 신뢰하는 에이전트 시스템을 신뢰 도메인으로 구성하고, 도메인 관리자가 도메인 등록 관리, 보안 정책 관리, 도메인 간 인

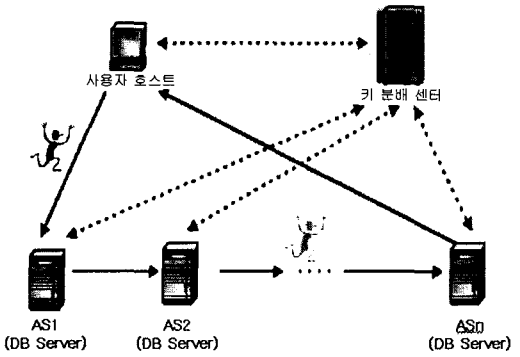

그림 1 중앙 집중형 보안 서비스 모델

증 서비스를 제공하므로써 쉬운 보안 정책 관리 기능과 도메인 내의 보안 연산을 줄이는 장점을 제공한다 [13,14]. 그러나 신뢰 도메인만을 이용한 모델은 이동 에이전트의 여행 계획에 따라 그 성능이 크게 좌우된다. 즉 빈번한 도메인 간 이동을 유발하는 경우 도메인 간의 보안 연산이 크게 증가하여 전체 작업 시간이 급격하게 증가하기 때문에 대규모 분산 환경에서 안정된 성능을 제공하기 어렵다.

따라서 본 논문에서는 고비용의 보안 연산 발생으로 인한 성능 감소와 불안정한 성능 문제를 보완하기 위하여 대규모 분산 환경에 적합한 TDGM(Trusted Domain & Guide Manager)을 이용한 보안 모델을 제안한다. 그림 2는 TDGM을 이용한 보안 모델의 시스템 구성도를 나타낸다.

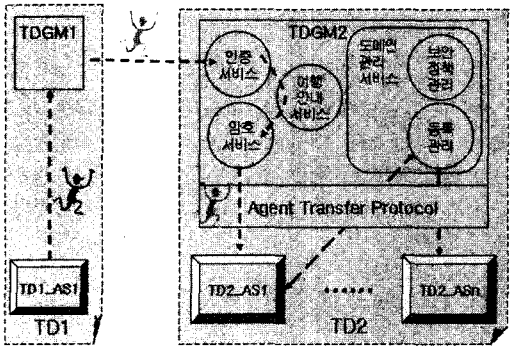

그림 2 TDGM을 이용한 보안 모델의 시스템 구성도

그림 2의 TD1과 TD2는 신뢰 도메인으로 PKI를 이용하여 상호 인증된 에이전트 시스템들과 TDGM으로 구성된다. 이동 에이전트는 신뢰 도메인 안에서 이동할 때 최소의 보안 확인 과정을 거친다[13]. TD1_AS1의 이동 에이전트가 TD2의 TD2_AS1로 이동할 경우, 먼저 TDGM1로 이동하고, TDGM1로부터 보안 검증을 받는다. TDGM1과 TDGM2는 상호 인증을 하고, TDGM2는 보안 확인 후 에이전트를 수락한다. 수락된 이동 에이전트는 TDGM2를 거쳐 TD2_AS1로 이동하고, 할당된 작업을 수행한다.

3.1 TDGM의 구성 및 기능

TDGM은 신뢰 도메인 관리자와 마찬가지로 이동 에이전트 시스템의 도메인 등록과 도메인 보안 정책 관리 등 도메인 관리 서비스를 제공하고, 인증 및 암호 서비스를 제공하면서도 다른 도메인으로부터 들어온 이동 에이전트에 여행 계획을 질의하여 도메인 지역적인 여행 계획으로 재조정하는 여행 안내 서비스를 제공한다. 여행 안내 서비스는 새로 도착한 이동 에이전트를 복호화하고 인증을 해야하므로 인증 및 암호 서비스와 연동하고, 허가된 이동 에이전트에게 신뢰 도메인에 등록된 에이전트 시스템 리스트를 이용하여 도메인 지역적인 여행 계획을 제공한다. 이동 에이전트 인증은 전자 서명의 특성을 가질 수 있도록 인증서 기반의 인증을 수행한다.

3.2 TDGM의 특징 및 장점

TDGM을 이용한 모델은 도메인 단위로 보안 연산을 수행하기 때문에 중앙 집중형 모델에서 발생하는 고비용의 보안 연산의 발생을 최소화할 수 있고, 여행 안내 서비스를 통하여 도메인 간의 이동을 최소화하기 때문에 신뢰 도메인만을 이용한 모델보다 안정적이고, 향상된 성능을 나타낼 수 있다.

4. 새로 제안한 보안 모델의 성능

이 장에서는 [9]에서 제시한 모델과 신뢰 도메인만을 이용한 모델 및 새로 제안한 보안 모델의 성능 모델을 제시한다. 상호 인증은 세션키를 생성하지 않고도 수행할 수 있고, 세션키를 사용함으로 보안성을 향상시킬 수 있지만 본 논문에서는 각 TDGM은 안전한 구성 요소이고, 상호 인증은 TDGM간에만 발생하기 때문에 보안 연산을 줄이기 위해 세션키를 생성하지 않고 인증 요청을 처리하도록 하였다. 표 1은 성능 모델을 분석하기 위하여 고려된 매개변수로 [4]와 [9]에서 실험 및 구현을 통하여 구해진 값이다.

최초 이동 에이전트의 데이타 크기, D_{Init}는 이동 에이전트 코드와 초기 상태 정보로 다음과 같다.

$$D_{Init} = D_{Code} + D_{State} \quad (1)$$

이동 에이전트 시스템 간을 이동할 때 이동 에이전트의 크기, D_{Mig}는 이동 에이전트 코드와 상태 정보뿐만 아니라 정보 검색 작업의 수행 결과를 포함한다. 이때 정보 검색 결과의 크기는 정보 검색 결과의 크기를 줄

표 1 성능 모델에서 사용되는 매개변수의 값

이름	의미	값
N	참여 에이전트 시스템의 수	50
D_{Code}	이동 에이전트의 코드 크기	39KBytes
D_{State}	이동 에이전트의 상태 크기	4KBytes
D_{Data}	이동 에이전트의 데이타 크기	512Kbytes
R_{Se}	정보 검색 처리율	4 회/s
R_{Rf}	정보 가공 처리율	4 회/s
R_{Th}	네트워크 처리율	1000kbps
R_E	암호화 처리율	1.6MByte/s
R_D	복호화 처리율	1.6MByte/s
R_S	서명 처리율	4.36MByte/s
R_V	서명 검증 처리율	2.03MByte/s
T_{ReqPK}	공개키 요청 시간	0.0000625 sec
T_{ResPK}	공개키 전송 시간	0.2500297 sec
$T_{ReqAuth}$	인증 요청에 소요되는 시간	2.3663329 sec
$T_{ResAuth}$	인증 요청을 처리하고 응답하는 시간	2.3661502 sec
$T_{EndAuth}$	상호 인증이 완료되는데 소요되는 시간	4.76837E-06 sec

일 수 있는 능력을 나타내는 에이전트 선택도, σ에 의해 좌우된다[3]. 따라서 이동중인 이동 에이전트의 데이타 크기는 다음과 같다.

$$D_{Mig} = D_{Code} + D_{State} + D_{Data} * (1 - \sigma) \quad (2)$$

4.1 중앙 집중형 보안 서비스 모델

[9]에서 제시한 모델의 총 수행시간, T_{SMA}은 정보 검색 작업 수행 시간, T_{MATh}와 상호 인증에 소요된 시간, T_{MAAuth} 및 비밀성과 무결성 서비스에 소요된 시간, T_{MASec}으로 구성된다.

T_{Mig}는 이동 에이전트가 하나의 에이전트 시스템을 방문해서 정보 검색하고, 가공하는데 소요되는 시간으로 동일한 시스템에서 연속적으로 검색 작업을 수행할 확률, p를 고려하고 있다.

$$T_{Mig} = \left\{ \left(\frac{1}{R_{Se}} + \frac{1}{R_{Rf}}\right)\left(\frac{1}{1-p}\right) + \frac{D_{Mig}}{R_{Th}} \right\} \quad (0 \le p < 1) \quad (3)$$

이동 에이전트가 처음 이동할 때에는 이동 에이전트의 코드와 상태 정보, D_{Init}만을 전송하고, 마지막 방문 시스템에서의 작업을 마치면 이동 에이전트의 코드와 상태 정보는 전송할 필요가 없기 때문에 검색 작업의 결과로 생성된 데이타, D_{Data}만 전송하므로 T_{MATh}는 다음과 같다[9].

$$T_{MATh} = \frac{D_{Init}}{R_{Th}} + \frac{D_{Data}}{R_{Th}} + (N-1) * T_{Mig} \quad (4)$$

두 시스템이 상호 인증을 하기 위해서는 중앙의 키 분배 센터에 공개키를 요구하고, 전송을 받아야 한다. 또한 목적 시스템에 인증을 요청해야 하고, 목적 시스템으로부터 인증을 받아야 하기 때문에 T_{MAAuth}는 다음과 같다[9].

$$T_{MAAuth} = 2T_{ReqPK} + 2T_{ResPK} + T_{ReqAuth} + T_{ResAuth} + T_{EndAuth} \quad (5)$$

T_{SData}는 이동 에이전트가 상태 정보와 정보 검색 작업을 수행함으로써 발생한 데이타를 암호화, 복호화, 서명 및 서명 검증에 소요된 시간을 나타낸다.

$$T_{SData} = (D_{State} + D_{Data}) * \left\{ \frac{1}{R_S} + \frac{1}{R_E} + \frac{1}{R_D} + \frac{1}{R_V} \right\} \quad (6)$$

무결성과 비밀성 제공하기 위해 이동 에이전트의 초기값에 대해서는 암호화, 복호화, 서명 작업이 수행되어야 하고, 코드에 대한 서명 검증 작업이 수행되어야 한다. 그리고 이동 중에는 코드에 대한 서명 검증이 필요하고, 상태 정보와 생성된 데이타에 대한 암호화, 복호화, 서명, 서명 검증이 수행된다. 마지막 방문 시스템에서의 작업을 완료하면 생성된 데이타에 대하여 암호화, 복호화, 서명, 서명 검증 작업을 수행해야 한다. 따라서 T_{MASec}는 식 (7)과 같다.

$$T_{MASec} = \frac{D_{Init}}{R_S} + \frac{D_{Init}}{R_E} + \frac{D_{Init}}{R_D} + N * \frac{D_{Code}}{R_V} + \frac{D_{Data}}{R_S} + \frac{D_{Data}}{R_E} + \frac{D_{Data}}{R_D} + \frac{D_{Data}}{R_V} + (N-1) * T_{SData} \quad (7)$$

중앙의 키 분배 센터를 이용한 모델에서는 에이전트가 이동할 때마다 상호 인증 작업을 수행해야 하기 때문에 방문 시스템의 수가 N인 경우 N+1회의 상호인증이 필요하다. 따라서 총 수행시간, T_{SMA}는 식 (8)과 같다.

$$T_{SMA} = T_{MATh} + (N+1)T_{MAAuth} + T_{MASec} \quad (8)$$

4.2 신뢰 도메인을 이용한 모델

신뢰 도메인만을 이용한 모델의 총 수행시간, T_{TD}는 정보 검색 작업 수행 시간, T_{TDTh}와 도메인 관리자 상호 인증에 소요된 시간, T_{TDAuth} 및 무결성과 비밀성 서비스에 소요된 시간, T_{TDSec}로 구성된다.

신뢰 도메인만을 이용한 모델에서 이동 에이전트는 도메인 관리 노드를 방문하고, 도메인에서의 작업이 완료된 경우 다시 도메인 관리 노드를 거쳐 다른 도메인으로 이동한다. 즉, 도메인을 방문할 때마다 부가적으로 2번의 관리 노드 방문이 발생한다. 따라서 정보 검색 작업은 방문하는 신뢰 도메인 수, C_{TD}의 2배만큼을 더 이동해야 하기 때문에 정보 검색에 소요되는 시간은 [9]에서 제안한 모델의 정보 검색 시간보다 $2 * C_{TD} * \frac{D_{Mig}}{R_{Th}}$가 더 길어지고, 여행 계획이 도메인 지역적이지 않은 경우 4.1절에서 제안한 모델의 정보 검색 시간보다 $2 * (N-1) * \frac{D_{Mig}}{R_{Th}}$가 더 길어진다.

$$T_{MATh} + 2 * C_{TD} * \frac{D_{Mig}}{R_{Th}} \leq T_{TDTh} \leq T_{MATh} + 2*(N-1)*\frac{D_{Mig}}{R_{Th}} \quad (9)$$

도메인 관리자 상호 인증에 소요되는 시간은 여행 계획이 지역적인 경우 도메인 개수만큼만 상호 인증을 하면 되고, 여행 계획이 지역적이지 않은 경우 최대 $(N-1)$번 상호 인증을 해야하기 때문에 다음과 같다.

$$C_{TD} * T_{MAAuth} \leq T_{TDAuth} \leq (N-1) * T_{MAAuth} \quad (10)$$

여행 계획이 지역적인 경우 무결성과 비밀성을 제공하기 위해 소요되는 시간은 4.1절에서 제안한 모델보다 에이전트 코드에 대한 서명 검증과 상태 정보 및 데이타에 대한 암호화, 복호화, 서명, 서명 검증에 소요되는 시간이 도메인 개수의 2배만큼 증가하지만, 여행 계획이 지역적이지 않은 경우 $2*(N-1)$배가 증가하여 급격한 성능 저하를 유발한다.

$$T_{MASec} + 2 * C_{TD} * \left\{ \frac{D_{Code}}{R_V} + T_{SData} \right\} \leq T_{TDSec} \leq T_{MASec} + 2*(N-1)*\left\{ \frac{D_{Code}}{R_V} + T_{SData} \right\} \quad (11)$$

신뢰 도메인을 이용한 모델은 지역성을 고려한 여행을 하는 경우 다음과 같은 성능을 나타내다.

$$T_{MATh} + 2 * C_{TD} * \frac{D_{Mig}}{R_{Th}} + C_{TD} * T_{MAAuth} + T_{MASec} + 2 * C_{TD} * \left\{ \frac{D_{Code}}{R_V} + T_{SData} \right\} \leq T_{TD} \quad (12)$$

신뢰 도메인만을 이용한 모델은 도메인 간 여행이 빈번한 경우 식 (13)과 같은 성능을 나타내고, 대규모 분산 정보검색 환경에서 T_{SMA}와 비교하여 급격하게 성능이 저하된다.

$$T_{TD} \leq T_{MATh} + (N-1) * T_{MAAuth} + T_{MASec} + 2*(N-1)*\frac{D_{Mig}}{R_{Th}} + 2*(N-1)*\left\{ \frac{D_{Code}}{R_V} + T_{SData} \right\} \quad (13)$$

4.3 TDGM을 이용한 모델

그림 3은 본 논문에서 제안한 TDGM 모델에서 이동 에이전트의 이동을 나타낸다.

TDGM을 이용한 모델의 총 수행시간, T_{TDGM}은 정보검색 작업 수행 시간, T_{TDGTh}와 TDGM간의 상호 인증에 소요된 시간, $T_{TDGAuth}$과 여행 안내 서비스에 소요되는 시간, T_{Guide} 및 무결성과 비밀성 서비스에 소요된 시간, T_{TDGSec}으로 구성된다.

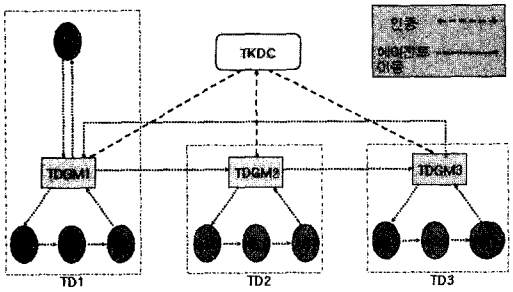

그림 3 제안한 모델에서 이동 에이전트 이동

TDGM을 이용한 모델의 여행 계획은 도메인 지역적이다. 이를 위해 신뢰 도메인의 수, C_{TD}만큼 여행 안내 서비스를 받아야하므로 $C_{TD} * T_{Guide}$만큼의 여행 안내 서비스 시간이 추가적으로 소요된다.

TDGM을 이용한 모델의 정보 검색 작업 수행 시간은 신뢰 도메인을 이용한 모델과 같이 신뢰 도메인 수의 2배만큼의 부가적인 이동을 발생하기 때문에 [9]에서 제안한 모델보다 $2 * C_{TD} * \frac{D_{Mig}}{R_{Th}}$만큼 증가한다.

$$T_{TDGTh} \leq T_{MATh} + 2 * C_{TD} * \frac{D_{Mig}}{R_{Th}} \quad (14)$$

TDGM간의 상호 인증은 신뢰 도메인 수만큼 발생하기 때문에 소요되는 시간은 다음과 같다.

$$T_{TDGAuth} = C_{TD} * T_{MAAuth} \quad (15)$$

이동에이전트의 코드에 대한 서명 검증과 상태 정보 및 데이타에 대한 암호화, 복호화, 서명, 서명 검증이 도메인 개수의 2배만큼 발생하기 때문에 무결성과 비밀성 서비스에 소요된 시간은 다음과 같다.

$$T_{TDGSec} \leq T_{MASec} + 2 * C_{TD} * \left\{ \frac{D_{Code}}{R_V} + T_{SData} \right\} \quad (16)$$

따라서 제안한 모델은 신뢰 도메인만을 이용한 모델에서 여행 계획이 도메인 지역적인 경우보다 $C_{TD} * T_{Guide}$만큼의 시간이 더 소요된다.

$$T_{TDGM} \leq T_{TDGTh} + T_{TDGAuth} + C_{TD} * T_{Guide} + T_{TDGSec} \quad (17)$$

5. 실험 및 평가

본 논문의 실험 환경으로는 윈도우즈 NT 4.0기반 펜티엄III 450Mhz PC, 윈도우즈 2000 기반 펜티엄III 800Mhz PC에 이동 에이전트 시스템으로 Aglet2.0.2를 사용하였고, 실험 모델은 이동 에이전트 시스템들이 신뢰 도메인으로 구축되어 있고, 도메인 간의 이동은 TDGM을 통하여 이동하는 것으로 한다. Agelt2.0.2에서는 여행 계획이 Java의 벡터로 구현되어 있기 때문에 T_{Guide}는 TDGM이 이동해 온 에이전트에 자신이 관리하는 에이전트 시스템의 정보를 질의하여 벡터에 저장된 여행 계획을 조정하는데 소요된 시간으로 실험을 통하여 얻은 평균값을 사용하였고, 데이타 크기, 처리율 및 보안에 관련된 매개변수는 [4]와 [9]에서 사용한 수치를 참조하였다.

TGDM을 이용한 모델이 [9]에서 제시한 중앙 집중형

보안 서비스 모델보다 우수한 성능을 나타내기 위해서는 $T_{SMA} \geq T_{TDGM}$이 성립해야 한다. 부등식을 N과 C_{TD}에 대하여 전개하면 다음과 같다.

$$T_{MATh} + (N+1)T_{MAAuth} + T_{MASec} \geq T_{TDGTh} + T_{TDGAuth} + C_{TD} * T_{Guide} + T_{TDGSec} \quad (18)$$

$$(N+1)T_{MAAuth} \geq \left\{2 * \frac{D_{Mig}}{R_{Th}} + T_{MAAuth} + T_{Guide} + 2 * \left\{\frac{D_{Code}}{R_V} + T_{SData}\right\}\right\} * C_{TD} \quad (19)$$

위 식에서 C_{TD}는 신뢰 도메인의 수를 의미하고, N은 참여 에이전트 시스템의 수를 의미한다. N이 50인 경우 여행 안내 서비스 시간, T_{Guide}은 실험값으로 0.068sec을 나타낸다. 식 (20)은 식 (19)에 표 1의 매개변수 값과 T_{Guide}를 적용한 결과를 나타낸다.

$$(N+1) \geq 3.0090 * C_{TD} \quad (20)$$

$\frac{N}{C_{TD}}$는 신뢰 도메인 당 방문한 평균 에이전트 시스템의 수를 의미하고, 그 값이 3.0090개보다 크다는 것은 방문하는 신뢰 도메인의 수가 적어, 도메인 지역적인 여행을 하는 경우 도메인 간의 이동 횟수를 줄일 수 있다는 것을 의미한다. 제안한 모델은 도메인 지역적인 여행을 하기 때문에 신뢰 도메인의 수가 $\frac{(N+1)}{3.0090}$보다 적은 경우 [9]에서 제시한 모델보다 우수한 성능을 나타낸다. 즉 대규모 분산 정보 검색과 같은 환경에서 다수의 에이전트 시스템들이 신뢰 도메인을 구성하는 경우 제안한 모델은 높은 보안성과 우수한 성능을 제공한다.

그림 4는 N이 50이고, 에이전트의 선택도, σ의 값이 0.1이며, 동일한 에이전트 시스템에서 연속적으로 작업을 수행할 확률, p의 값이 0.1인 경우 신뢰 도메인 당 방문한 에이전트 시스템의 수에 따른 두 패러다임의 작업 수행 시간의 변화를 보여준다.

그림 4를 보면 신뢰 도메인 당 방문한 이동 에이전트 시스템의 수가 1인 경우, T_{TDGM}은 신뢰 도메인 안에 있는 시스템을 방문하기 위해 TDGM으로 이동해야 하고, 여행안내를 받아야 하며, 다음 TDGM과 상호 인증을 해야 한다. 즉, 4.1절의 모델과 비교하여 인증에 소요되는 시간은 감소하지 않고 부가적으로 소요되는 시간이 크게 증가하기 때문에 T_{SMA}와 비교하여 매우 낮은 성능을 나타낸다. 신뢰 도메인 당 방문한 이동 에이전트 시스템의 수가 4이상인 경우, 신뢰 도메인 안에 있는 4개의 시스템을 방문하기 위해서는 5번의 이동을 해야 하고, (N+1)/4만큼의 여행안내를 받으며, 다른 TDGM과 상호 인증을 한다. 이동 에이전트의 이동과 여행안내에 소요되는 시간은 증가하지만 인증에 소요되는 시간은 크게 감소하기 때문에 T_{TDGM}은 T_{SMA}와 비교하여

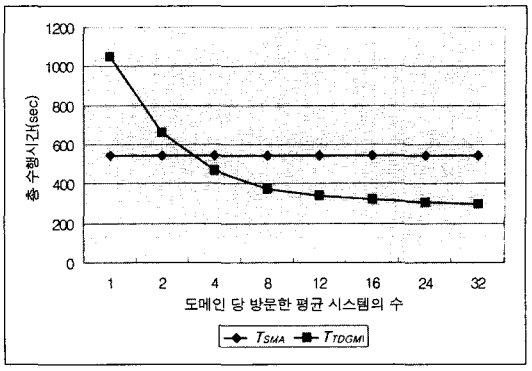

그림 4 N=50인 경우, 신뢰 도메인 당 평균 방문 시스템의 수에 따른 총 수행 시간

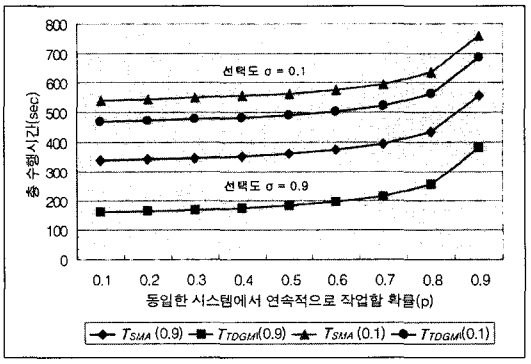

그림 5 N=50인 경우, 동일한 시스템에서 연속적으로 작업할 확률에 따른 총 수행시간

성능이 향상된다.

그림 5는 N이 50이고, σ의 값이 0.1 또는 0.9이며, 신뢰 도메인 당 방문한 에이전트 시스템의 수가 4인 경우 p의 값에 따른 두 패러다임의 작업 수행 시간의 변화를 보여준다.

그림 5를 보면 p의 값이 작고, σ의 값이 큰 경우 제안한 모델의 성능이 4.1절의 모델보다 크게 향상되는 것을 알 수 있다. 제안한 모델의 경우 보안 연산에 소요되는 시간을 줄이기 위해 TDGM을 사용함으로써 이동 에이전트가 방문하는 시스템의 수가 증가한다. 따라서 이동하는 에이전트의 크기와 상태 및 데이타의 크기가 작을수록 성능이 크게 향상된다. 제안한 모델의 총 수행 시간, T_{TDGM}은 4.1절의 모델보다 σ의 값이 0.1이고 p가 0.1인 경우 15%, p가 0.9인 경우 10%의 성능 향상을 나타내고, σ의 값이 0.9이고 p가 0.1인 경우 53%, p가 0.9인 경우 32%가 향상되었다.

대규모 분산 정보 수집 및 검색과 같은 응용은 참여 시스템의 수가 많고, 다수의 시스템들이 도메인으로 구

성될 수 있기 때문에 신뢰 도메인의 수, C_{TD}가 식 (19)를 만족할 수 있고, 그 경우 제안한 모델은 [9]에서 제시한 모델보다 우수한 성능을 제공한다.

6. 결론 및 향후 연구

분산 환경에 이동 에이전트를 적용하기 위해서는 보안에 대한 고려가 필수적이다. 그러나 기존의 연구에서 대부분의 이동 에이전트 성능 모델은 보안을 고려하지 않았고, 보안 모델은 성능을 고려하지 않았기 때문에 이동 에이전트를 이용함으로써 발생하는 장점을 기대하기 어려웠다.

따라서 본 논문에서는 TDGM을 이용하여 신뢰 도메인을 구성하고, 이동 에이전트의 여행을 안내하며, 보안 정책을 관리하도록 하였다. 제안한 모델은 대규모 분산 정보검색 환경에서 도메인 내의 보안 연산을 크게 줄이고, 도메인 간의 이동을 최소화함으로써 기존의 보안을 고려한 이동 에이전트 모델보다 우수한 성능을 나타낸다.

향후 연구 과제로는 TDGM을 이용한 보안 모델을 구현해보고, 침입 탐지 기능을 추가함으로써 통합 보안 기능을 제공하도록 한다.

참 고 문 헌

[1] M.Strasser., et al., "Communication Concepts for Mobile Agent," Proceedings for the 1st International Workshop on Mobile Agents, Berlin(D), Lecture Notes in Computer Science, No. 1219, Springer-Verlag(D), pp.123-135, April 1997.

[2] R. Gray, D. Kotz, S. Nog, D. Rus and G .Cybenko, "Mobile agents for mobile computing," Technical Report PCS-TR96-285, Department of computer Science, Dartmouth College, Hanover, 1996.

[3] M. Strasser and M. Schwehm, "A Performance Model for Mobile Agent System," Proceedings of the International Conference Parallel and Distributed Processing Techniques and Applications PDPTA97, 1997.

[4] A. Puliafito, S. Riccobene and M. Scarpa, "An analytical comparison of the client-server, remote evaluation and mobile agents paradigms," the First International Symposium on Agent Systems and Applications/Mobile Agents, Palm Springs, California(USA), October 1999.

[5] R.S. Gray, D. Kotz, G. Cybenko and D. Rus, "D'Agents:Security in a Multiple-language, Mobile-agent System," Mobile Agent and Security, LNCS 1419, Springer-Veralg, pp.154-186, 1998.

[6] T. Sander and C.R. Tschundin, "Protecting Mobile Agents Against Malicious Hosts," Mobile Agent and Security, LNCS 1419, Springer-Veralg, 1998.

[7] N.Karnik and A. Tripathi, "Security in the Ajanta Mobile Agent System," Software-Practice and Experience, 2001.

[8] L. Tang and B. Pagurek, "A Comparative Evaluation of Mobile Agent Performance for Network Management," Proceedings for the 9th IEEE International Workshop on the Engineering of Computer-Based Systems, April 8-11, 2002.

[9] Seung-Wan Han, Ki-Moon Jeong, Seung-Bae Park and Hyeong-Seok Lim, "A Performance Comparison of the Mobile Agent Model with the Client-Server Model under Security Conditions," 정보과학회논문지:정보통신, 제29권 제3호, Jun 2002.

[10] Jae-Kyoung Park and Yoo-Hun Won, "Design and Implementation of Secure Mobile Agent Gateway," 정보과학회논문지:컴퓨팅의 실제, 제8권 제2호, April 2002.

[11] A. Puliafito and O. Tomarchio, "Security mechanisms for the MAP agent system," the 8th Euromicro Workshop on Parallel and Distributed Processing(PDP2000), Rhodos (Greece), January 2000.

[12] A. Puliafito and O. Tomarchio, "Design and development of a practical security model for a mobile agent system," In IEEE Symposium on Computer Communications(ISCC2002), Taormina (Italy), July 2002.

[13] G. Noordende, F. Brazier and A. Tanenbaum, "A Security Framework for a Mobile Agent System," the second Internatinal Workshop on Security of Mobile Multiagent System(SeMAS 2002), July 2002.

[14] N. Motrovic and U.A. Arribalzaga, "Mobile Agent security using Proxy-agents and Trusted domains," the second Internatinal Workshop on Security of Mobile Multiagent System(SeMAS 2002), July 2002.

유 응 구

1997년 동국대학교 공과대학 전자계산학과 졸업(공학사). 1999년 동국대학교 일반대학원 컴퓨터공학과 졸업(공학석사) 1999년~현재 동국대학교 컴퓨터공학과 박사과정. 관심분야는 이동 에이전트, 보안, 분산시스템 관리 등

이 금 석

1971년 서울대학교 공과대학 응용수학과 졸업(학사). 1973년 한국과학기술연구소 전산개발센터 전산기술과 근무. 1978년 한국과학기술원 전산학과 졸업(이학석사) 1981년~현재 동국대학교 컴퓨터공학과 교수. 2001년 건국대학교 컴퓨터공학과 졸업(공학박사). 관심분야는 운영체제론, 컴퓨터 성능평가, 소프트웨어 품질 공학등