JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 17, No. 10 : 2337~2344, Oct. 2013

신뢰모델을 기반으로 한 이동 에이전트의 로드밸런싱과 에이전트 보호 기법

정창렬[1] · 이성근[2*]

A Load Balancing and Security Scheme of Mobile Agents based on the mobile Trust Model

Chang-ryul Jung[1] · Sung-keun Lee[2*]

[1] Department of Computer Engineering, Sunchon National University, Jeonnam 540-950, Korea
[2] Department of Multimedia Engineering, Sunchon National University, Jeonnam 540-950, Korea

요 약

이동 에이전트는 이동성이 있어 다양한 분야에서 응용되는 기술이다. 특히 오픈네트워크에서의 이동 에이전트 실행은 보안을 통한 안전한 실행이 보장되어야 한다. 또한 에이전트는 에이전트 실행을 위해 에이전트의 작업량 분배가 이루어져야 한다. 이를 위해 본 논문에서는 신뢰모델 기반의 에이전트 실행 보안 메커니즘을 제안하였다. 제안된 메커니즘은 에이전트의 안전한 실행 보장과 기존 연구에서 고려되지 않았던 합리적인 에이전트 작업량 분배를 위한 로드 밸런싱으로 처리율을 향상되도록 하였다. 제안된 신뢰기반 에이전트 보안 메커니즘에 대한 보안 분석을 통해 이동 에이전트의 안전한 실행을 증명하였다.

ABSTRACT

Mobile Agent is an autonomous mobility technology is being applied in various fields. In particular, mobile agents execution in the Internet environment through the safe execution of the security must be guaranteed. Also, agent to run the agent, the agent's workload should be distributed. In this paper, a trust model based on the security mechanism of the agent execution is proposed. Proposed mechanism to ensure safe execution of the agent was not considered in existing relative researches for rational agent workload distribution and load balancing to improve throughput was. The proposed trust-based security mechanisms for agents to go through security analysis proved safe execution of the agent.

키워드 : 에이전트 보안, 로드밸런싱, 신뢰모델, 이동 에이전트

Key word : Mobile Agent, Agents Security, Load Balancing, Trust Model

접수일자 : 2013. 08. 10 심사완료일자 : 2013. 10. 04 게재확정일자 : 2013. 10. 14

*** Corresponding Author** Sung-keunl Lee(E-mail:sklee@sunchon.ac.kr, Tel:+82-61-750-3831)
Department of Multimedia Engineering, Sunchon National University, Jeonam 540-950, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2013.17.10.2337 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

이동에이전트 기술은 이동성, 자율성, 그리고 지능적인 상호작용이 가능하여 다양한 분야에서 응용되고 있다. 그러나 이동 에이전트는 이동 여정에서 공격 위협에 항상 노출되어 있기 때문에 설계 시 보안에 대한 충분한 고려가 선행되어야 한다. [1]은 4개의 범주에서 공격위협을 고려하고 있다. 에이전트가 에이전트 플랫폼 공격으로부터 위협, 에이전트의 공격에 의한 에이전트 플랫폼의 위협, 에이전트 플랫폼 안에서 에이전트가 다른 에이전트 공격 위협, 마지막으로 에이전트가 다른 플랫폼에서 다른 에이전트의 공격 위협이다. 이들 위협은 플랫폼에서 통신 가용성에 대한 잠재적인 취약성 노출에 초점을 맞추고 있다[2]. 에이전트 플랫폼은 에이전트의 코드와 데이터가 안전하게 실행될 수 있도록 제어한다. 그러나 합법적인 실행 인증이 아닌 악의적인 코드를 이용하여 에이전트 상태 코드, 데이터, 여정 등을 공격하기도 한다[3]. 에이전트 여정은 미리 예측이 되지 않는 경로이지만 에이전트 보호 방법에서는 에이전트 코드, 상태, 데이터와 더불어 중요하다. 일반적으로 Free-roaming환경에서 에이전트는 실행하는 동안에 공모된 절단공격, 재실행 공격, 중간자 공격 등의 위협을 받고 있다. 이러한 공격에 대한 보호와 더불어 에이전트의 임무수행에 있어 중요한 것은 신뢰기반의 작업량의 할당이다. 이는 신뢰도가 높은 에이전트에게 수행 임무가 집중적으로 할당되기 때문에 발생되는 문제이다. 에이전트 작업량에 대한 밸런스의 조정은 보안의 가용성과 직결되는 중요한 부분이다. 따라서 본 논문에서는 에이전트의 가용성과 서비스 질 향상을 위해 에이전트의 로드 밸런싱이 이루어질 수 있는 신뢰모델 기반의 안전한 에이전트 실행 보장 메커니즘을 제시한다.

본 논문의 구성은 제 2장에서 관련 연구로서 이동 에이전트와 관련한 주요 보안문제, 신뢰모델 그리고 로드 밸런싱을 기술한다. 제 3장에서는 에이전트의 로드밸런싱 알고리즘과 에이전트의 안전한 실행을 위해 신뢰모델 기반의 안전한 이동 에이전트 실행 보안 기법을 제안한다. 제 4장에서는 제안된 로드밸런싱과 신뢰모델 기반의 에이전트 실행에 대한 평가 및 보안 분석을 한다. 마지막으로 제5장에서 결론을 기술한다.

Ⅱ. 관련 연구

신뢰모델 연구들은 분산 환경에서 신뢰 형식화를 위한 프레임 구조를 중심으로 제안되었다. 몇 몇의 연구들에서는 보안을 위한 신뢰 통합에 초점을 두고 있지만 [4]와[5]에서는 검증서버에서 TTP(trust third parties)를 이용한 이동 에이전트 보안의 단일 신뢰모델이 제안되었다. 그러나 이 모델은 하드웨어적인 위조방지 장치인 Tamper-resistant가 필요함으로 시스템에 대한 기본 비용 부담과 TTP에 의존적 처리로 트래픽 발생 문제가 있다. [6]의 모바일 신뢰 관리 구조는 이동 에이전트 보안을 향상시키기 위해 신뢰 평가와 신뢰 값을 계산하여 결정하는 모델이다. 즉 신뢰 값에 의해 다양한 보안 관계들을 획득하는 모델이다. 그러나 이 모델은 신뢰에 대한 최적화와 규격화를 하기 위해서 지난 경험과 평판을 확인해야 하는 한계가 있다. [7]은 최근 신뢰정보, 과거의 신뢰 정보, 신뢰 예측 그리고 다른 에이전트들에 대한 신뢰 판단 등 에이전트의 신뢰 판단 방법을 제시하였다. 그러나 직접적인 연산에 트랜잭션 시간대별 상대 가중치를 할당하지 않고 단순평균함수 SAF (simple average function)을 이용하고 있다. 때문에 특정 간격의 평판정보에 따라 특정 에이전트에게 작업량이 집중되어 서비스의 질을 낮게 하는 문제점이 있다. [4]와[8]에서는 동적인 네트워크 환경에서 신뢰 값의 상호작용이 이루어지지 않으면 시간이 경과하면서 신뢰 값이 감쇠되도록 하고 있다. 여정경로가 길수록 악의적인 에이전트는 활동할 수 있는 기회가 많기 때문에 경로에 따른 가중치는 유동적이어야 한다.

신뢰모델의 보안관점에서 볼 때 연속적인 상호작용과 관계없이 이동 에이전트의 이동 여정이 길수록 짧은 경로에 비해 가중치를 더 적게 할당을 해야 한다. 그러나 그렇지 못하는 경우가 있어 문제가 있다. 그 외에도 [9]는 협력적 추천자 시스템에서 악의적인 에이전트들이 허위 트랜잭션을 생성 한 후 공모를 통해 악의적으로 신뢰 값을 조작하는 실링공격(shilling attack)을 분석하였다. 그러나 호스트에서 에이전트의 로드밸런싱이 이루지지 않아 특정 에이전트의 악의적인 활동 방지에는 한계가 있다. 본 논문에서는 이를 해결하기 위해 신뢰모델 기반의 에이전트 보안 메커니즘을 제시하고자 한다.

Ⅲ. 안전한 동적 모바일 신뢰모델, 로드밸런싱 알고리즘 그리고 보안메커니즘

3.1. 안전한 동적 모바일 신뢰모델

기존 이동에이전트 보안의 한계는 특정한 부분만을 보호하는 보안 메커니즘이다. 때문에 동적 모바일 신뢰을 기반으로 한 에이전트 보안 메커니즘이 설계되어야 한다. 신뢰모델에서는 수집 활동, 인터넷 응용 프로그램에 대한 신뢰 관계에 대한 평가와 보안, 그리고 증거 분석과 코드화가 이루어지기 때문에 신뢰 관리가 매우 효율적이다.

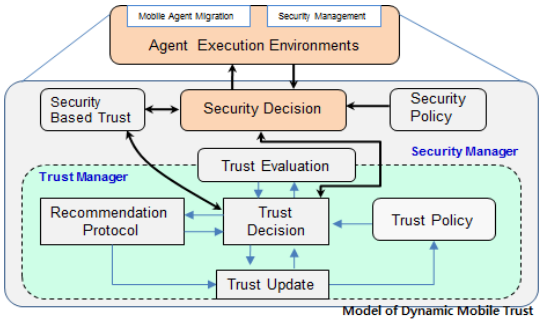

그림 1. 안전한 동적 모바일 신뢰 모델
Fig. 1 secure dynamic mobile trust model

또한 신뢰기반 모델은 개방적인 오픈 네트워크 환경에서 전통적인 서버-클라이언트 환경의 계층적 보안 정책 구조에 따라 안전한 보안 구조의 운영이 가능하다. 그러나 인터넷 환경에서는 정확한 신원확인을 위한 신뢰판단 메커니즘이 필요하다. 그리고 인터넷 환경의 네트워크에서 악의적인 행위자들이 정상적인 행위자로 위장하는 것을 방지하고 추적할 수 있도록 암호 기반이 필요하다. 이러한 문제점들을 해결할 수 있도록 신뢰모델의 각 구성들의 기능은 다음과 같다.

3.1.1. Recommendation Protocol

추천 프로토콜은 추천자로부터 신뢰관리를 위해 추천 요청을 보내고, 추천 개체들로부터 추천 응답을 받는 구조이다. 이는 신뢰결정 모듈과 상호작용을 한다.

3.1.2. Trust Decision

신뢰결정의 신뢰평가 값은 실시간으로 신뢰 관련 행동들을 관찰하고 다른 개체들로부터 추천된 신뢰와 신뢰 관계들의 초기 집합을 바탕으로 생성한다. 생성 후에는 신뢰 인터페이스 엔진 구동으로 최종 신뢰결정을 한다. 신뢰 정책들과 신뢰 값들을 저장소에 저장된 후 필요에 따라 이를 참조하여 리스크 분석과 새로운 신뢰 값을 결정한다. 그리고 오리지널 호스트는 최종 신뢰성을 산출하기 위해 다른 호스트들에서 평가된 신뢰 값을 교차하여 평가한다. 신뢰 값은 신뢰집합으로 구성하고, 신뢰집합은 신뢰결정과 보안결정의 요소가 된다. 따라서 기존의 방식에서의 나타난 에이전트 보안의 표면적이고 단편적인 보안 메커니즘의 한계를 극복할 수 있는 대안이다.

3.1.3. Trust Policy

신뢰정책은 신뢰결정자와 신뢰 대상자 사이에 수립된 신뢰 관계들로 구성되어 있다. 추천자에 의해 신뢰정책은 주기적인 업데이트가 이루어진다. 각 신뢰 대상 개체들에 대한 신뢰 정책들과 신뢰 값들이 DB화 되어 있다.

3.1.4. Trust Update

신뢰 업데이트는 기본적으로 통합되어 있는 신뢰와 추천자 프로토콜 자료를 포함하고 있는 신뢰자료(True Source)모듈에 의한 신뢰정보 업데이트가 이루어진다. 또한 업데이트 된 정보는 정책 반영을 위해 신뢰 결정자에게 적용된다. 이러한 피드백은 최적의 신뢰모델을 항상 유지한다. 또한 추천 프로토콜에 의해 추천된 에이전트는 평가자에게 정확도가 측정될 수 있도록 피드백 한다. 또한 악의적인 에이전트들에 의해 악의적으로 업데이트 되는 것을 방지하기 위해 암호화하여 전송하고 신뢰성을 유지를 위해 주기적으로 신뢰도를 평가를 한다.

3.1.5. Security-based Trust

기존의 보안 메커니즘은 기능적인 보안에 치중 되어 있어 보안 강화를 위해서는 항상 시스템 오버헤드를 고려해야만 했다. 본 논문의 보안 기반의 신뢰는 신뢰 결정을 위한 보안요소로만 작용하기 때문에 시스템의 오버헤드에 직접적인 영향은 없다. 또한 보안요소의 특징은 기존의 모형과 보안요소의 구조를 기반으로 하고 있기 때문에 구체적으로 묘사하지는 않는다.

3.2. 로드밸런싱

로드밸런싱은 에이전트 실행 처리율 향상과 양질의 서비스 보장을 위한 안전한 신뢰모델 기반의 에이전트 작업량 분배이다. 본 논문에서는 휴리스틱(heuristic) 값을 부여하여 로드밸런싱 작업량 값을 계산 후 적은 값을 가진 에이전트들 중에서 트랜젝션 요청이 발생되면 에이전트가 실행된다. 이때 에이전트 공급자의 작업량 휴리스틱 값이 신뢰 값 임계치(threshold)에 도달하면 공급자의 신뢰 에이전트를 선택한다. 그러나 휴리스틱 값이 임계치에 하나도 도달하지 못 할 경우 기존의 시퀀스 방법에 따라 에이전트를 실행한다. 이를 위해 작업량의 휴리스틱(heuristic) 값 계산과 가장 적은 로드를 가진 에이전트를 선택하기 위해 연산된 에이전트 신뢰 값을 바탕으로 식(1)을 이용하여 근사로드 연산을 한다.

$$Nod^t(p,q) = I^t(p,q) + \sum_{w-\{p\}} Fedb_i^n(p,x) \times I^t(x,q) \quad (1)$$

식(1)에서의 p와 q는 에이전트, x는 임의의 에이전트, 그리고 I는 에이전트의 상호작용 수치이다. w는 $w = TS(q)$로 에이전트 q와 상호작용한 경험이 있는 에이전트들의 집합을 나타낸다. $Fedb_i^n(p,x)$는 신뢰 업데이트를 위해 최신 신뢰도를 평가한다. 이때 유사성의 최소 허용치 $\theta = 0.01$로 한다. 이로써 $Nod^t(p,q)$는 t시간대에서 에이전트 q가 연산에서 에이전트 p에 의해서 직·간접적으로 상호작용하는 총 수치를 나타낸다. 이에 따라 근사로드 값의 증가 순으로 서비스가 제공되기 위해 에이전트를 정렬한 후 트랜잭션 요청에 부합한 서비스 제공 가능한 가장 적은 작업량을 가진 에이전트를 선택한다.

$$\mathrm{Prob}(p,q) = \begin{cases} \dfrac{Trust_i^n}{\sum_{x \in unknownAgt}}, \text{if} \sum_{x \in unknownAgt} Trust_i^n(p,x) \neq 0, \\ randomly\ select\ any\ agent, \\ else. \end{cases} \quad (2)$$

그러나 초기 트랜잭션이 발생되지 않은 단계에서 알려지지 않은 서비스 제공 에이전트로 분류될 수 있다. 이 경우, 식(2)와 같이 개연성 척도를 바탕으로 에이전트를 선택한다. 알려지지 않는 에이전트($unknown\,Agt$)에서 하나의 에이전트가 선택되어질 때 에이전트가 실행 가능하도록 신뢰 값을 높여준다. 이로써 알려지지 않은 에이전트가 실행을 위해 무한 대기나 신뢰 값에 따라 특정 에이전트에게 작업량 집중되는 것을 방지 할 수 있다.

```
select : service Agt(p,S)
evaluate : Agt(p), set of Agents
respond : service request S, Agt q, t
if x∈S
compute Trust(p,x)
if Trust(p,x) > threshold
know_Agt ← know_Agt ∪ {x}
elseendi
unknow_Agt ←unknow_Agt ∪ {x}
if know_Agt ≠ 0 then
compute Nod^t(p,x)
sort know_Agt ← load Agt
select Agt q ← smallest laad Agt
else
Total_Trust ←0
 for x∈unknow_Agt do
  Total_Trust = Total_Trust + Total_Trust(p,x)
 end for
if Total_Trust > 0 then
 for Total_Trust x ∈ unknow_Agt do
    compute Prob(p,x)
  end for
    return Agt q ← probability Prob(p,q)
 else Agt q ← Agt q randomly
end if
```

그림 2. 에이전트 실행 로드밸런싱 알고리즘
Fig. 2 agent execution load balancing algorithm

그러나 모든 에이전트가 $(unknow\,Agt = 0)$인 경우는 에이전트 선택을 위한 어떠한 예측지원도 하지 않아 에이전트를 선택 할 수 없다. 이 경우, 선택의 효율성이 보장되지 않기 때문에 기존 시퀀스 처리 방법이나 에이전트를 랜덤 선택할 수밖에 없다. 그러나 에이전트 서버에서 처음 서비스가 이루어질 때 외에는 발생되지 않는 경우이다. 로드 밸런싱 알고리즘은 그림 2와 같다. 이처럼 이동에이전트의 신뢰모델과 로드밸런싱을 통해 에이전트의 안전한 실행과 작업 분배가 이루어진다. 이는 신뢰모델 기반의 에이전트 보호 메커니즘을 통해 이루어진다.

3.3. 이동에이전트 보호 메커니즘

이동에이전트는 실행되는 동안 많은 위협에 노출되기 때문에 에이전트의 결과 신뢰는 안전한 실행이 보장이 답보되었을 때 얻을 수 있다. 그림 3은 신뢰모델을 기반의 이동에이전트 보호 메커니즘이다. 에이전트가 실행하는 동안에 신뢰가치 평가는 기존 평판과 함께 고려해야 하고, 에이전트 노드밸런싱으로 에이전트 처리율을 향상시켜야 한다.

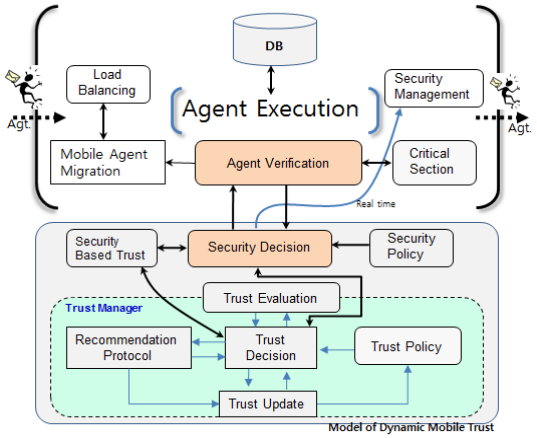

그림 3. 신뢰기반 모델 기반의 이동 에이전트 보호 메커니즘
Fig. 3 Mobile Agent security Mechanism based on trust Model

이로써 악의적인 에이전트에 집중되는 문제를 해소하고, 에이전트 실행 시 트래픽 발생 최소화가 이루어진다. 이를 위해 본 논문에서는 신뢰모델을 기반으로 한 에이전트의 작업량 분배와 안전한 실행 보장을 위해 신뢰모델에서는 에이전트의 실행을 위해 신뢰 평가를 한다. 신뢰 기준이 충족되면 에이전트를 암호화하여 에이전트 실행 서버로 보내어 신뢰 검증을 한다. 에이전트 신뢰 검증 처리는 DMTM (Dynamical Mobile Trust Model)에서 이루어진다. 신뢰검증 시퀀스는 그림 4와 같다. 신뢰모델의 신뢰관리(TM)와 보안관리(SM)간의 에이전트 신뢰 검증은 암호화된 시퀀스를 통해 이루어진다. 신뢰관리는 보안결정을 위해 에이전트 소유자 키(ENC^{Pub}_{owner}), 신뢰 값($tValue()$), 에이전트의 상태 정보(S_A), 그리고 신뢰관리의 인증서($Cert^{TM}_{DMTM}$)을 보안 관리에 전송한다. 또한 보안 관리는 신뢰 정보에 대한 보안결정과 함께 수락여부(Acc)를 송신한다.

$$
\begin{aligned}
&//Runing\ of\ Trust\ Value\ verfication\\
&//TM:\ Trust\ Manager,\ SM:\ Security\ Manager\\
&TM > SM: Request\{Agt_i\},\\
&ENC^{Pub}_{AS_i}\{ENC_{TM}\{ENC_{AS_i}, ENC^{Pub}_{owner}, tValue()\},\\
&\qquad\qquad S_A(code, Cert_{DTMT}, T(code_{DMTM}), Cert^{TM}_{DMTM}\}\\
&SM > TM: Response\{Result\{Agt_i\}\},\\
&ENC^{Pub}_{AS_i}\{Cert^{SM}_{DMTM}, tValue(),\ T(code_{DMTM}), Acc\}
\end{aligned}
$$

그림 4. DMTM에서 에이전트 신뢰 검증 시퀀스
Fig. 4 agent trust-verification sequence in DMTM

$$
\begin{aligned}
&//Migration\ to\ Agent\ Server\ of\ Agt_i\\
&verification: Cert_{DMTM}\\
&agent\ code\ chacking: ENC_{owner}(c)\\
&//Agent\ Certification\ and\ verification\\
&//Agent\ load\ Balancing\\
&\text{if } Nod^t(p,q) \neq 0\\
&\ Agt\ Authentication\\
&\ ENC^{Pub}_{DMTM}(Cert^{Pub}_{DMTM}(), Ret_{Psi})\\
&else\ \text{if}\\
&\ \text{Prob}(p,q) = 0\\
&\ randomly\ select\ any\ agent\\
&\ //Agent\ Execution\\
&Request: Agt \rightarrow DMTM\\
&\ ENC^{Pub}_{DMTM}(Cert^{Pub}_{AS_i}(), code(), Time-stamp_{AS_i})\\
&Response: DMTM(Agt) \rightarrow AS_i\\
&ENC^{Pub}_{AS_i}(Cert_{SM}, tValue(), Time-stamp,\\
&\qquad T(code_{DMTM}), Acc)\\
&\text{if } Acc = accept\\
&\quad Agt\ execute\\
&else\ \text{if} = reject\\
&\ Agt\ refusal\\
&\ record\ time-out(Agt)\\
&appending\ reject\ list\\
&protocol\ eceution\ termination\\
&\text{or } waiting\ other\ agent
\end{aligned}
$$

그림 5. 에이전트 서버 실행 알고리즘
Fig. 5 agent server execution algorithm

이때 에이전트 실행에 대한 추적이 가능하도록 ($T(code_{DMTM})$)을 함께 보내 재전송 문제를 해결한다. 이로써 신뢰모델 기반 에이전트 서버는 에이전트의 안전한 실행 보장과 악의적인 에이전트나 호스트의 부정한 행위 방지가 이루어진다. 이러한 신뢰모델 기반 에이전

트 서버는 신뢰정보를 바탕으로 에이전트의 로드밸런싱에 따라 에이전트를 실행한다. 그림 5는 에이전트 서버에서 에이전트 실행 알고리즘을 나타내고 있다.

Ⅳ. 평가 및 보안 분석

다양한 네트워크 환경에서 에이전트는 안전한 실행 보장이 우선시 되어야 한다. 이를 위해 본 논문에서 제안된 메커니즘의 에이전트 처리 요구량을 분석을 통해 안정적인 처리가 이루어짐을 평가하였다. 또한 다양한 공격으로부터 신뢰모델 기반의 에이전트 보호 메커니즘에 대한 안전성을 분석 하였다.

4.1. 에이전트 실행 처리요구량 평가 분석

네트워크 대여폭 10MBbps, 에이전트사이즈 2M, 에이전트 처리율 100/s, 인증서사이즈 10M, 처리 시간 60min, 인증서 취소율 10%, 악의적인 에이전트 비율 40%, threshold 0.25, 신뢰가중치0.5, 에이전트 개수 100으로 하여 시뮬레이션 toolkit SimJava를 이용하여 시뮬레이션 하였다. 보안 메커니즘에서 에이전트 처리는 요구량에 비해 안정적인 처리가 이루어짐을 알 수 있다.

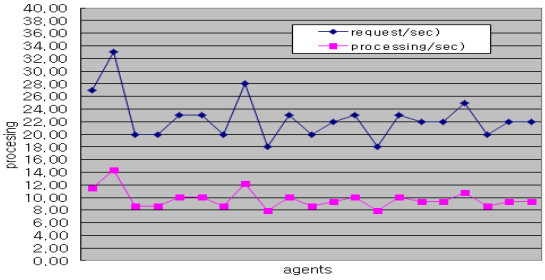

그림 6. 에이전트 실행처리 요구량 평가
Fig. 6 agent execution process request rate evaluation

그림 6의 결과는 에이전트 서비스 요구들에 대해 에이전트 노드밸런싱으로 에이전트 작업량이 분배되어 처리되는 것을 보여주고 있다.

4.2. 기밀성/ 무결성 보장

에이전트는 긴 여정 중에 발생하는 공격위협으로부터 안전한 실행을 위해서는 기밀성과 에이전트 상태정보그리고 데이터의 정보에 대한 무결성이 보장되어야 한다.

본 논문에서는 에이전트 소유자의 공개키 ENC_{Owner}^{Pub}로 암호화하여 기밀성을 보장받고, 신뢰모델의 인증서 $Cert_{DMTM}^{TM}$ 을 이용하여 에이전트 신뢰 무결성을 보장한다. 또한 에이전트 추적이 가능하도록 신뢰모델의 보안관리에 의해 생성된 추적코드 $T(Code_{DMTM})$를 삽입한다. 향후 악의적인 요소의 에이전트를 추적하여 사후관리와 에이전트 평가 단계를 낮추어 실행 제한을 할 수 있기 때문에 에이전트의 안전한 실행이 보장된다. 제안된 신뢰모델기반 기밀성과 무결성이 TM과 SM에서 다음과 같이 이루어진다.

$TM > SM$:

$$ENC_{AS_i}^{Pub}\begin{Bmatrix} ENC_{TM}\{ENC_{AS_i}, ENC_{owner}^{Pub}, tValue()\}, \\ S_A(code, Cert_{DTMT}, T(code_{DMTM}), Cert_{DMTM}^{TM}) \end{Bmatrix}$$

$SM > TM$:

$$ENC_{AS_i}^{Pub}\begin{Bmatrix} Cert_{DMTM}^{SM}, tValue(), T(code_{DMTM}), \\ Acc \end{Bmatrix}$$

4.3. 공모에 의한 공격 위협 방지

기존 신뢰모델에서는 신뢰성이 낮거나 신뢰성이 없는 에이전트들의 실행을 거절할 수 없었다. 그러나 본 논문의 제안 메커니즘에서는 실행거절이 가능하다. 뿐만 아니라 에이전트 기반 전자상거래에서 발생할 수 있는 실링공격을 방지하였다. 기존 모델들에서는 전자거래의 판매자를 평가할 때 기준이 판매자가 가지고 있는 신뢰 값에 의해 이루어지고, 에이전트의 신뢰 값에 의한 평가는 제한적이었다. 즉 실링공격과 같은 악의적인 요소들 간에 공모를 통해 에이전트 신뢰 값을 상승시켜 악의적인 에이전트가 높아진 평판과 신뢰 값으로 에이전트 실행 우선권을 갖는다. 본 논문에서는 이러한 공모를 방지하기 위해 에이전트 서버와 신뢰모델 간의 메시지 송신이 이루어진다. 이 경우 공모가 이루어지기 위해서는 신뢰모델의 보안 관리가 먼저 공모에 참여하거나 협력해야 한다. 그러나 이러한 경우는 그림 5와 같이 에이전트 서버에서 암호화된 처리가 이루어짐으로 공모가 이루어지지 못한다. 또는 보안 관리는 신뢰관리와 사전 공모가 이루어져야 한다. 만약에 공모가 발생하여도 에이전트 서버와 보안 관리는 상호작용 과정에서 에이전트 서버 인증서 $Cert_{AS_i}^{Pub}$와 신뢰모델의 인증서

$Cert_{DMTM}^{Pub}$가 송수신과정에서 검증된다. 이로써 협력적 공모는 이루어질 수 없기 때문에 안전하다.

4.4. 에이전트 실행 로드밸런싱과 보안 문제 해결

에이전트의 신뢰 값 우선순위에 의해 에이전트 임무를 분배하는 로드 밸런싱을 통해 에이전트의 작업량 과 에이전트의 처리율이 향상시켰다. 또한 제안된 로드밸런싱 알고리즘은 신뢰기반 보안 메커니즘에서 동작함으로 기존의 에이전트 기반 시스템에서 발행되는 무임승차 문제도 해결할 수 있다. 무인승차문제(free riding problem)는 P2P의 경우 에이전트가 서비스 소비만 하고, 서비스나 피드백 제공을 하지 않는 경우 발생한다. 이를 해결하기 위해 에이전트 로드밸런싱 실행 과정에서 에이전트 서버는 에이전트 서버의 공개키(ENC_{AS}^{Pub})로 암호화된 모듈을 수신하고, 다음과 같이 수락정보(Acc)가 포함된 검증정보를 전송함으로서 무임승차 문제를 해결 한다.

$$ENC_{AS_i}^{Pub}(Cert_{SM}, tValue(), Time-stamp, T(code_{DMTM}), Acc)$$

또한 동일 서비스 요구나 트랜잭션 발생을 감지하여 실행을 제한함으로써 해결할 수 있다.

V. 결 론

본 논문에서는 신뢰모델을 기반으로 에이전트 작업량의 분배와 에이전트의 기밀성과 무결성을 보장하여 에이전트의 안전한 실행을 보장하는 메커니즘을 제안하였다. 또한 멀티 에이전트시스템의 신뢰모델로서 기존의 단편적인 보안구조를 개선하여 특정 어플리케이션의 요건 충족이 아닌 에이전트가 실행하는 동안 발생할 수 있는 공격을 보호할 수 있는 메커니즘이다. 이를 통해 에이전트의 기밀성과 무결성 보장, 그리고 에이전트 신뢰 값을 상승시키기 위해서 협력적 공모를 통한 공격으로부터 에이전트의 안전한 실행을 보장하였다. 마지막으로 에이전트 실행 작업량의 효율적인 배분 알고리즘을 통해 에이전트의 처리율을 향상시켰고, 기존 모델에서 발생된 무임승차 문제를 공개키 암호모듈을 사용하여 개선하였다. 또한 보안 분석을 통해 보안의 안전성을 제시하였다.

REFERENCES

[1] M. V. Prem, S. Swamynathan, “Securing Mobile Agent and its Platform from Passive Attack of Malicious Mobile Agents,” *Proc. International Conference on Advances in Engineering, Science and Management(ICAESM-2012)*, pp.605-609, 2012.

[2] Zhidong Shen, Xiaoping Wu, “A Trusted Computing Technology Enabled Mobile Agent System,” *Proc. International Conference on Computer Science and Software Engineering*, pp.567-570, 2008.

[3] F. T. Ibharalu, A. B. Sofoluwe, A. T. Akinwale, “A reliable protection architecture for mobile agents in open network system,” *International Journal of Computer Applications*, Vol.17, Issue 7, pp.6-14, 2011.

[4] P. Dadhich, K. Dutta and M. C. Govil, “On the Approach of Combining Trust and Security for Securing Mobile Agents: Trust Enhanced Security,” *Proc. IEEE 2011 2nd International Conference on Computer and Communication Technology (ICCCT)*, pp. 379-384, 2011.

[5] H. K. Tan, L. Moreau, “Trust relationships in a mobile agent system,” *proc. 5th IEEE International Conference on mobile Agents*, Vol. LNCS2240, Atlanta, Georgia, December, 2001.

[6] U. K. Tupakula, V. Varadharajan, “Detecting Security Attacks in Trusted Virtual Domains,” *proc. 2010 IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC)*, pp.529-535, 2010.

[7] B. Li, M. Xing, J. Zhu, and T. Che, “A Dynamic Trust Model for the Multi-Agent Systems,” *Proc. IEEE Int’l Symp. Information Processing (ISIP ’08)*, pp. 500-504, 2008.

[8] L. Wen, P. Lingdi, L. Kuijin, and C. Xiaoping, “Trust Model of Users’ Behavior in Trustworthy Internet,” *Proc. IEEE WASE Int’l Conf. Information Eng. (ICIE ’09)*, pp. 403-406, 2009.

[9] Z. Fuguo, “A Survey of Shilling Attacks in Collaborative Filtering Recommender Systems,” *Proc. International Conference on Computational Intelligence and Software Engineering (CiSE 2009)*, pp.1-4, 2009.

정창렬(Chang-Ryul Jung)

1999년 순천대학교 컴퓨터교육 석사
2005년 순천대학교 컴퓨터과학과 박사
※관심분야 : 보안, 에이전트 보안, RFID/USN 보안, 네트워크 보안

이성근(Sung-Keun Lee)

1987년 고려대학교 전자공학과 공학석사
1995년 고려대학교 전자공학과 공학박사
현 재 순천대학교 멀티미디어 공학과 교수
※관심분야 : USN, 멀티미디어 통신, 인터넷 QoS