2001년 한국정보처리학회 춘계 학술발표논문집 제8권 제1호

ID기반의 다중서명을 이용한 이동 에이전트 시스템 보안에 관한 연구

탁동길*, 이옥빈**, 김성열*, 정일용*
*조선대학교 전자계산학과
**충북대학교 전자계산학과
e-mail:jasmine_tdk@hotmail.com

A Study on Secure Mobile Agent Systems employing the ID based Multi-Signature Scheme

Dong-Gil Tak*, Ok-Bin Lee**, Seong-Yeol Kim*, Il-Yong Chung*
*Dept of Computer Science, Chosun University
**Dept of Computer Engineering, Chungbuk University

요 약

본 논문은 이동 에이전트 시스템이 안고 있는 보안 문제를 해결하고자 하였다. 제안된 프로토콜은 이동 에이전트 및 에이전트 시스템 보안 위협에 대처하기 위하여 ID를 이용한 키 분배 기법과 Fiat-Shamir 디지털 서명 방식에 기초한 다중 서명 방법을 이용하여 에이전트와 에이전트 플랫폼의 양방향 인증, 실행 결과 데이터의 보호, 생명성 보장을 함께 처리하였으며 중간 검증이 가능하도록 제안되어 불필요한 오버헤드를 갖지 않도록 하였다. 제안된 이동 에이전트 보안 프로토콜을 적용하였을 때 얻을 수 있는 장점은 첫째, 이동에이전트의 생명성을 보장할 수 있으며 둘째, 에이전트의 실행 결과 데이터의 기밀성, 무결성을 보장할 수 있고, 세째, 에이전트 실행의 전 단계를 매 시스템마다 검증함으로써 변경, 삭제 등의 문제가 발생하는 즉시 발견할 수 있다.

I. 서론

이동 에이전트(mobile agent)는 기하급수적으로 증가하는 분산 처리 환경과 이동 컴퓨팅의 변화 때문에 주목받고 있는 기술이다. 그러나 이동 에이전트 시스템은 분산 어플리케이션의 구성에 유연한 환경을 제공하는 반면, 해결하여야할 보안 문제를 안고 있다. 이동 에이전트의 공격으로부터 호스트 컴퓨터를 보호하는 문제는 에이전트의 인증과 접근 제어로써 해결될 수 있지만 에이전트 서버의 공격으로부터 에이전트를 보호하는 문제는 일반화된 보호방법이 없어 현재 해결하기 어려운 문제로 남아 있다[1]. 또한 이동 에이전트 시스템의 보안 문제는 이동 에이전트의 실행 결과 데이터를 적절히 보호하는 방법과 이동 에이전트의 생명성을 보장하는 문제가 존재한다. 따라서 이동 에이전트 시스템 보안 문제는 이동 에이전트 시스템이 해결하여야 할 중요한 연구 과제로 부상하고 있다.

정적인 에이전트의 보안 문제는 전통적인 보안 대책으로 접근이 가능하지만, 이동 에이전트 시스템에 적용할 경우 이동 에이전트의 특징인 이동성을 파괴할 수 있다. 에이전트는 신뢰할 수 있는 영역(domain) 외부에서 자율적으로 운행되고 동작 할 수 있어야 하지만, 특정 플랫폼에 대한 정보가 잘 알려지지 않은 경우에 에이전트를 보호하기 어렵다. 즉 에이전트가 플랫폼 사이에서 이동할 때, 에이전트를 받아들이는 플랫폼은 유입된 에이전트에 의해 어떤 간섭이 발생할지 알 수 없으며, 이동 에이전트는 해당 플랫폼의 악성 여부를 결정할 수 없다. 따라서 이동 에이전트 시스템은 새로운 형태의 보안 메커니즘이 필요하다. 본 논문에서는 ID 기반의 디지털 다중 서명 기술을 이용하여 이동 에이전트의 실행 결과 데이터를 적절히 보호하는 방법과 이동 에이전트의 생명성을 보장하는 문제에 대한 효율적인 해결책을 제시하고자 한다. 이를 위하여 본 연구는 2장에서 이동 에이전트 시스템이 가질 수 있는 보안 위협 요소를 분석하고, 디지털 다중 서명(Digital Multi-signature)기법과 ID에 기반한 키(key) 분배 기법에 대하여 살펴본다. 3장에서 이동 에이전트 시스템의 보안 문제를 해결하기 위한 새로운 방법을 제안하고 4장에서 결론을 맺는다.

II. 기초연구

A. 기존 연구 분석

[2]는 네트워크 자원을 많이 사용하게 되어 많은 비용을 요구하고 실행 코드가 커진다는 단점이 있다. 또한 [3]은 실용적인 응용에는 적합하지 않은 것으로 평가된다. [4]는 [2],[3]에 나타난 문제를 해결하기 위하여 디지털 서명과 감사 도구를 이용하여 에이전트 여행 정보와 실행 상태 정보에 보안 시스템을 사용함으로써 에이전트를 보호하고 있다. 그러나 이 방식은 변경 행위를 즉각 발견하지 못함으로써 불필요한 오버헤드를 가질 수 있으며 서명 길이가 길어지는 단점이 있다.

이동 에이전트의 보호를 위해 제안된 방법으로는 [5], [6], [7] 등이 제안되었다. 또한 에이전트에 대한 서버의 위협은 무시하고 불법적인 에이전트로부터 서버를 위한 보안 프로토콜[8]이

제안되어 있으나 이러한 시스템들은 에이전트와 서버간의 상호 인증을 제공하지 않는다는 단점이 있다.

B. 이동 에이전트 시스템의 보안 위협

이동 에이전트 시스템의 보안 공격은 크게 정보 노출, 서비스 거부, 정보 손상으로 구분할 수 있다. 보안 공격을 고려하는데 에이전트와 에이전트 플랫폼이 주요한 요소가 되는데 에이전트 플랫폼은 호스트에 에이전트 서버가 탑재된 것으로 에이전트 실행 환경을 제공한다. 이동 에이전트 시스템의 공격은 에이전트의 에이전트 플랫폼 공격, 에이전트의 에이전트 공격, 에이전트 플랫폼의 에이전트 공격, 다른 요소의 에이전트 시스템 공격으로 나누어 볼 수 있다.

C. ID 기반 디지털 서명 방식

ID를 이용한 암호시스템에서는 키 발급 센터만이 비밀키를 생성할 수 있는 능력을 갖고 있으므로 키 발급 센터이외에는 누구도 ID를 변경할 수 없다[9].

1. Fiat-Shamir의 ID를 이용한 디지털 서명 방식

<표 1> Fiat-Shamir의 ID 서명 방식

1) 서명방식

① A는 t개의 랜덤한 수 $r_1, r_2, \ldots, r_t$ $(0<r_i<n)$을 생성하여 $x_i = r_i^2 \pmod n$을 계산한다.

② A는 $f(M, x_1, x_2, \cdots, x_t)$를 계산하여 상위 kt비트를 $e_{ij}(1 \le i \le t, 1 \le j \le k)$로 한다.

③ A는 $y_i = r_i \prod_{e_{ij}=1} S_j \pmod n$ $1 \le i \le t$ 을 계산하여 $ID_A, M, t \times k$ 행렬 $[e_{ij}], y_i (1 \le i \le t)$를 B에게 보낸다.

2) 검증방식

① B는 $I_j = f(ID_A, j)$ $(1 \le j \le k)$를 계산한다.

② B는 $Z_i = y_i^2 \prod_{e_{ij}=1} \pmod n$ $(1 \le i \le t)$를 계산한다.

③ B는 $f(M, Z_1, Z_2, \cdots, Z_t)$의 상위 kt비트가 e_{ij}와 같은가 확인한다.

A와 B가 이상과 같은 프로토콜을 수행한다면 B는 항상 $t \times k$ 행렬 e_{ij}와 y_i를 메시지 M의 서명됨을 확인할 수 있으며, A의 서명으로부터 A의 비밀키 $S_1, S_2, \cdots, S_k$에 대한 어떤 정보도 얻을 수 없다. 이 방식은 고속처리와 ID에 근거하기 때문에 RSA에 근거한 서명 방식보다 효율적이다.

2. 디지털 다중 서명 기법

한사람이 메시지에 전자적으로 서명하는 것으로써 단순 서명(single signature)이라 한다. 이와 같은 전자 서명 기술은 전자문서 교환을 위해 중요한 역할을 수행한다. 동일한 메시지에 대해 여러 사람이 전자적으로 서명하는 것을 '디지털 다중 서명'이라 한다.

디지털 다중 서명 방식이 갖추어야할 기본적인 조건들은 서명문 길이의 고정, 검증 가능성, 부정 조기 검출성, 비밀 유지성, 공통성 등이다[10]. 이러한 조건들을 만족하며 단순 서명 방법의 비효율적인 문제를 해결하기 위한 다중 서명 방법은 Itakura-Nakamura방법, Okamoto 방법, Brickell-Lee-Yacobi 방법, Fiat-Shamir방식에 근거하여 만들어진 Ohta-Oka -moto 방법 등이 있다[11].

Fiat-Shamir의 서명 방식에 근거한 디지털 다중 서명 방식은 RSA에 근거한 디지털 서명보다 서명 속도가 빠르고[11], ID에 근거한 방식이므로 공개 기록집이 불필요하다. 그리고 키 관리를 단순화할 수 있고 중간 서명자의 검증이 가능하도록 만들 수 있으며 서명을 위한 통신 회수가 적다는 장점을 가지고 있다.

III. 이동 에이전트 시스템 보안 프로토콜 설계

본 논문에서 제안하는 이동 에이전트 보안 프로토콜은 Fiat-Shamir의 ID 기반의 디지털 다중 서명법을 기초로 하여 에이전트가 경유하는 각각의 에이전트 플랫폼마다 서명을 수행하는 다중 서명 기능을 포함한다. 사용되는 표기법은 <표 2>와 같다.

<표 2> 제안된 프로토콜의 표기법

표기	설명
A	Mobile Agent Code
f	공개된 일방향 함수
h	공개된 해쉬 함수
AP_i	에이전트 플랫폼 i의 ID
AP_h	에이전트를 생성한 에이전트 플랫폼으로 홈
AP_{route}	홈이 선택하는 경로의 집합
ABS	Agent Base Server로 AP에게 키를 분배하는 기관이며 에이전트실행결과를 최종 점검한다.
$k_{n,m}$	n과 m의 공유키
$E_k(M)$	메시지 M이 키 k에 의하여 암호화됨
R_n	AP_n이 생성한 랜덤 수
$R_{n,m}$	AP_n이 AP_m에게 전송하기 위하여 생성한 수
$t1_n$	AP_n이 *status*를 생성한 시간의 timestamp
$t2_n$	AP_n이 AP_{n+1}, ABS와 통신 시 replay 공격에 대비한 timestamp

A. 이동 에이전트 시스템 보안 프로토콜

1. 에이전트 서버 등록 절차

서버 등록을 위해서 에이전트 플랫폼이 ABS에 등록을 요청하면 ABS는 서버 프로그램을 제공하기 전에 각각의 에이전트 플랫폼 고유의 키를 배포한다.

2. 에이전트 플랫폼 서비스 제공 프로세스

에이전트 플랫폼이 에이전트 실행을 위하여 제공하는 프로세스는 다음과 같은 절차로 수행된다.

[Step 1] AP_{i-1}으로부터 에이전트 실행 요청을 받아들여 세션 공유키 생성 절차를 수행한 후 AP_{i-1}와의 공유키 $k_{i,i-1}$를 생성한다.

[Step 2] AP_{i-1}로부터 실행할 에이전트를 수신한다.

$(A, AP_{route}, statustable, (e_{11}, \ldots, e_{1k}), \ldots, (e_{(i-1)1}, \ldots, e_{(i-1)k}), Y_{i-1}, t2_{i-1})$

[Step 3] 수신된 메시지에 대해 다음과 같이 검증한다.

① AP_i은 AP_1부터 AP_{i-1} 까지의 I_{nj}를 계산한다.

$I_{nj} = f(AP_n, j), \quad n = 1,2,\ldots,i-1, \; j = 1,2,\ldots,k$

$(e_{11}, \ldots, e_{1k}), \ldots, (e_{(i-1)1}, \ldots, e_{(i-1)k})$

② Y_{i-1}, 와 I_{nj}를 이용하여 Z_{i-1}을 계산한다.

$$Z_{i-1} = {Y_{i-1}}^2 \prod_{i=1}^{j=1} \prod_{e_{ij}=1} I_{nj} \bmod N, \quad j = 1,2,\ldots,k$$

③ 다음을 점검하여 일치하면 오류가 없음을 확인할 수 있다.

$(e_{(n-1)1},\ldots,e_{(n-1)k}) = h\,(A, AP_{route}, statustable, Z_{n-1})$

[Step 4] 검증 결과 오류가 있으면 이를 ABS에 보고하고 서비스 요청 대기 상태로 돌아간다.

[Step 5] ABS와 세션 공유키 세션 절차를 수행하여 ABS와의 공유키 $k_{i,ABS}$를 생성한다.

[Step 6] AP_{route}에 근거하여 다음에 에이전트를 실행할 AP_{i+1}와 세션 공유키 세션 절차를 수행하여 AP_{i+1}와의 공유키 $k_{i,i+1}$를 생성한다.

[Step 7] 에이전트를 실행하여 실행 결과 데이터인 $status$을 작성한 다음, ABS와의 공유키로 암호화하여 $statustable$에 저장한다.

$$\log_i = E_{k_{i,ABS}}(status, t1_i)$$

$$statustable = \log_{i-1} \| \log_i$$

이 절차에 의하여 에이전트 실행 결과 데이터는 다른 에이전트 플랫폼으로부터 보호될 수 있다.

[Step 8] 에이전트 및 실행 결과에 대해 서명한다.

$R_i \in Z_N \qquad Z_N(: \{0,1,\ldots,N-1\})$

$X_i = {R_i}^2 Z_{i-1} \bmod N$

$(e_{i1},\ldots,e_{ik}) = h\,(A, AP_{route}, statustable, X_i)$

$$Y_i = Y_{i-1} R_i \prod_{e_{ij}=1} S_{ij} \bmod N, \quad j=1,2,\ldots,k$$

[Step 9] AP_i는 AP_{route}에 근거하여 AP_{i+1}에게 다음과 같이 에이전트와 [Step 8]의 서명정보를 전송한다. 전송되는 정보에는 재전송 공격을 방지하기 위하여 timestamp가 포함된다.

$AP_i \rightarrow AP_{i+1}$:

$E_{k_{i,i+1}}(A, AP_{route}, statetable, (e_{11},\ldots,e_{1k}),\ldots,(e_{i1},\ldots,e_{ik}), Y_i, t2_i)$

[Step10] 서비스 요청 대기 상태로 돌아간다.

3. 에이전트 홈 서비스 제공 절차

사용자가 에이전트를 생성하고자 하는 경우 에이전트 플랫폼은 에이전트 홈 서비스를 제공하기 위한 프로세스를 다음과 같이 수행한다.

[Step 1] AP는 에이전트 서비스 요청을 받으면 에이전트 홈으로서의 서비스를 수행하기 위해 다음과 같이 에이전트 이동 경로를 생성한다.

$$AP_{route} = AP_1 \| AP_2 \| \ldots \| AP_m \| AP_{m+1}$$

[Step 2] ABS와 세션 공유키 세션 절차를 수행하여 ABS와의 공유키 $k_{h,ABS}$를 생성한다.

[Step 3] 최초로 에이전트를 실행할 AP_1와 공유키 세션절차를 수행하여 AP_1와의 공유키 $k_{h,1}$를 생성한다.

[Step 4] 다음과 같이 에이전트 코드와 경로 정보를 ABS에 전송한다.

$$AP_h \rightarrow ABS: E_{k_{h,ABS}}(A, AP_{route}, t2_h)$$

[Step 5] 다음과 같이 서명한다.

① 랜덤 수 $R_h \in Z_N$을 선택한다.

여기서 Z_N은 $\{0,1,\ldots,N-1\}$을 나타낸다.

② 다음을 계산하여 서명 메시지 Y_h를 생성한다.

$X_h = {R_h}^2 \bmod N$

$(e_{h1},\ldots,e_{hk}) = h\,(A, AP_{route}, statustable, X_h)$

$$Y_h = R_h \prod_{e_{hj}=1} S_{hj} \bmod N, \quad j=1,2,\ldots,k$$

[Step 6] AP_h는 최초로 에이전트를 실행할 AP_1에게 다음을 전송한다.

$AP_h \rightarrow AP_1: E_{k_{h,1}}(A, AP_{route}, statustable, (e_{h1},\ldots,e_{hk}), Y_h, t2_h)$

[Step 7] ABS로부터 결과를 획득한다.

4. 세션(session) 공유키 생성 절차

AP가 다른 여러 AP와 연관되어 이동 에이전트 서비스를 수행함에 신뢰성 있는 암호 통신 방법이 필요하다. 이를 위해 두 AP간에 세션 공유키를 생성하는 절차를 거친다.

[R_i 생성] AP_i는 랜덤 수 $R_i \in Z_N$(Z_N: $\{0,1,\ldots,N-1\}$)을 선택한다.

[C_{AP_i}] AP_i는 다음을 계산하여 AP_{i+1}에 전송한다.

$$C_i = S_i \cdot g^{R_i} \bmod N$$

[$C_{AP_{i+1}}$] AP_{i+1}는 랜덤 수 R_{i+1}를 선택한 후 다음을 계산하여 AP_i에게 전송한다.

$$C_{i+1} = S_{i+1} \cdot g^{R_{i+1}} \bmod N$$

[키 생성 k_i] R_{i+1}와의 공유키 k_i를 계산한다.

$$k_i = (C_{i+1}{}^e / AP_{i+1})^{R_i} \bmod N$$

$$= g^{e \cdot R_i \cdot R_{i+1}} \bmod N$$

[키 생성 k_{i+1}] R_{i+1}는 다음과 같이 AP_i와의 공유키 k_{i+1}를 계산한다.

$$k_{i+1} = g^{e \cdot R_i \cdot R_{i+1}} = k_i$$

5. 실행 결과의 제공

ABS는 에이전트가 정상적으로 수행되었음을 확인하고 각 AP_i들과 설정하였던 세션(session) 공유키 테이블을 참조하여 실행 결과를 획득한다.

<표 3> ABS의 세션 공유키 테이블

에이전트 서버의 ID	세션 공유키
AP_1	$g^{e \cdot R_1 \cdot R_{ABS}}$
AP_2	$g^{e \cdot R_2 \cdot R_{ABS}}$
⋮	⋮
AP_{m-1}	$g^{e \cdot R_{m-1} \cdot R_{ABS}}$
AP_m	$g^{e \cdot R_m \cdot R_{ABS}}$

$statustable$는 $statustable = \log_1 \| \ldots \| \log_n$과 같이 구성되어 있고 $\log_i$는 $\log_i = E_{k_{i,ABS}}(status, t1_i)$와 같이 구성되므로 각 서버에서 t시간에의 실행 결과를 복호화하여 얻을 수 있다. 이를 홈에 암호화하여 전달함으로써 이동 에이전트의 실행을 마치게 된다.

B. 제안된 프로토콜의 보안 서비스 분석

제안된 보안 프로토콜은 Fiat-Shamir의 ID 기반 디지털 다중 서명법을 기초로 설계되었다. Fiat-Shamir의 ID기반의 디지털 서명은 이산 대수 문제에 근거하여 암호학적인 안전성이 있으며 이산 대수 문제는 암호, 인증 방식을 구성하기 위한 대표적인 문제이다. 제안된 디지털 서명을 이용한 보안 프로토콜의 안전성은 Fiat-Shamir의 방식과 동일하다. 제안된 프로토콜은 이동 에이전트 보안 측면에서 에이전트 서버의 인증, 에이전트 코드와 데이터의 기밀성, 에이전트 코드와 데이터의 무결성, 실행 결과 데이터의 보호, 에이전트의 생명성 보장, 에이전트 전송의 부인 방지, 이동 에이전트 실행 감사 수행 등을 만족하고 있다, 또한, 에이전트 플랫폼 보안 측면에서는 에이전트의 인증, 에이전트의 호스트 컴퓨터에 대한 리소스 접근 제어 기능을 만족하고 있다.

제안된 프로토콜은 암호화 기술을 기반으로 하는 보안 기술을 이용하여 제안된 프로토콜로써, 다중 서명 기법을 이용하여 Back 방식의 서명 길이가 길어진다는 단점을 해결하였으며, 양방향 인증, 기밀성, 무결성, 부인 방지를 만족시키고 있다. 또한 에이전트에 대한 불법적인 조작이 발생한 경우에 대한 조치를 수행하는 fault-tolerance가 고려되었고, 실행 결과 데이터를 에이전트 플랫폼들에게 공개되지 않도록 하는 기능을 가지고 있다. 이는 다른 시스템들에서 지원하지 못하고 있는 fault-tolerance, 실행 결과 데이터 보호 등의 문제 해결책을 제안함으로써 이동 에이전트 시스템의 실제 응용에 사용될 수 있도록 하였다.

IV. 결론

본 논문은 이동 에이전트 시스템이 안고 있는 보안 문제를 해결하고자 하였다. 제안된 프로토콜은 이동 에이전트 및 에이전트 시스템 보안 위협에 대처하기 위하여 ID를 이용한 키 분배 기법과 Fiat-Shamir 디지털 서명 방식에 기초한 다중 서명 방법을 이용하여 에이전트와 에이전트 플랫폼의 양방향 인증, 실행 결과 데이터의 보호, 생명성 보장을 함께 처리하였으며 중간 검증이 가능하도록 제안되어 불필요한 오버헤드를 갖지 않도록 하였다. ID 기반의 암호화 방식은 키 분배, 디지털 서명 등에 적용될 수 있으며 키 관리의 단순화라는 장점이 있으며 공개키 방식에 비하여 서명 처리 속도가 빠르다는 장점을 가지고 있다. 제안된 이동에이전트 보안 프로토콜의 특징을 요약하면 첫째, 키 관리를 단순화시킨 구조이며 둘째, 기밀성, 무결성, 부인 방지, 재전송 방지를 보장하고 셋째, 에이전트의 생명성을 보장하는 기능이 있으며 넷째, 실행 결과 데이터를 보호하고 다섯째, 인증 기능을 갖추고 있다는 것이다.

제안된 이동 에이전트 보안 모델은 현재 컴퓨팅 기술에서 이슈가 되고 있는 이동 에이전트 시스템의 보안 문제 해결에 대한 가능성을 디지털 다중 서명 기법을 통해 제시하였으며 실제 이동 에이전트 시스템의 구성에 적용될 수 있다. 향후는 이동 에이전트 서버들의 디렉토리 서비스를 위한 연구가 수행되어져야 할 것이다.

[참고문헌]

[1]Wayne Jansen, Tom Karygiannis, "Mobile Agent Security," NIST Special Publication 800-19, 1998.

[2]Giovanni Vigna,"Protecting Mobile Agents throu- gh Tracing," the Mobile Object Systems ECOOP Workshop, 1997.

[3]Bennet S.Yee., "A Sanctuary for Mobile Agents," the DARPA Workshop on Foundations for Secure Mobile Code Workshop, pp.26-28, 1997

[4]백주성, 이동익 , 디지털 서명과 감사 도구(Audit trail)를 이용한 이동 에이전트의 보호, 한국정보과학회 학술발표논문집, 제24권 2호, 1997.

[5]Fritz Hohl, "An Approach to Solve the Problem of *Malicious Hosts in Mobile Agnet Systems*," Universitat Stuttart, Fakultat Infomatik, Fakultatsbericht Nr. 1997.

[6]Wilhelm, Uwe, G. and Staamann, Sebastian, "Protecting the Itinerary of Mobile Agents," in Proceedings of the ECOOP Workshop on Distributed Object Security and 4th Workshop on Mobile Object Systems: Secure Internet Mobile Computations, pp. 135-145, INRIA, France, 1998.

[7]James Riordan and Bruce Schneier, "Environmental Key Generation towards Clueless Agents," in Giovanni Bigna(Ed.), Mobile Agents and Secrity, pp15-24, Springer-Verlag, 1998.

[8]Ordille, Joann, "When agents roam, who can you trust?" In Proc. of the First Conference on Emerging Technologies and Applications in Communications, Porland, May 1996.

[9]A.Shamir, "Identity-based cryptosystem and signature scheme,"Advances in cryptology:Proc. of CRYPTO 84, Springer-Verlag, pp.47-57, 1985.

[10]김승주, 원동호, "특수 디지틀 서명방식에 대한 고찰," 통신정보보호학회지, 제6권, pp.30-31, 1996.

[11]강창구. 「디지탈 다중서명 방식과 응용에 관한 연구」,충남대학교: 공학박사학위논문, 1993.