그룹 지정 암호화를 활용한 이동 에이전트 보호 메커니즘†

한 승 완, 임 형 석
전남대학교 전산학과
{hansw, hslim}@chonnam.chonnam.ac.kr

A Mechanism for the Protection of Mobile Agent Using a Group Cryptography

Seung-Wan Han, Hyeong-Seok Lim
Dept. of Computer Science, Chonnam National University

요약

본 논문에서는 이동 에이전트의 여정에 포함된 호스트들만이 이동 에이전트를 복호화하여 실행할 수 있도록 함으로써 이동 에이전트를 보호하는 메커니즘을 제안한다. 이를 위하여 본 논문에서는 기존의 그룹 지정 암호화 방법들을 비교 분석하고 그 중에서 이동 에이전트 환경에 가장 적합한 중국인의 나머지 정리에 기반한 그룹 지정 암호화 방법을 이동 에이전트 보호 메커니즘에 활용한다.

1. 서론

이동 에이전트는 이질적인 망(heterogeneous network)에서 자신의 제어로 호스트를 옮겨다니며 다른 호스트의 에이전트 서버나 에이전트와 상호 작용하면서 사용자의 작업을 수행하는 프로그램이다[4].

이동 에이전트의 특성은 이동성과 자율성이다. 이 두 가지 특성으로 인하여 이동 에이전트는 네트워크 부하를 줄일 수 있고 불안정한 통신 환경에서 클라이언트와 서버 사이의 지속적인 연결을 유지할 필요가 없으며, 또한 클라이언트의 요구가 다양하고 수시로 변하는 환경에서도 장점을 갖는다[4,6]. 이동 에이전트를 활용하면 장점을 갖는 분야로 정보 검색, 망 관리, 사건 모니터링, 이동 컴퓨팅 분야, 워크플로우 시스템, 전자상거래 등이 있다[4,6]. 이처럼 이동 에이전트는 분산 컴퓨팅 환경의 많은 분야에서 장점을 갖는다. 그러나, 이동 에이전트는 특성 중의 하나인 이동성에 의해서 야기되는 새로운 보안 취약점들 때문에 실제 응용에 적용하는데 제약을 갖는다[5]. 그러므로 이동 에이전트 기술을 실제 응용에 보다 널리 활용하기 위해서는 이동 에이전트 시스템의 보안에 관한 연구가 선행되어야 한다.

이동 에이전트 시스템의 보안은 크게 이동 에이전트의 보호와 호스트의 보호로 나눌 수 있다[5]. 이동 에이전트 시스템을 다양한 공격으로부터 보호하기 위해서는 이 두 범주의 보호가 동시에 제공되어야한다. 그러나 사용자 작업의 정확한 수행을 보장하기 위해서는 그 중에서도 이동 에이전트의 보호가 우선적으로 해결되어야 한다.

이동 에이전트의 보호는 공격이 시도되는 시점에 따라 이동 중인 에이전트 보호와 호스트 상에서 실행 중인 에이전트 보호로 나눌 수 있다. 그러나, 일반적으로 호스트는 실행 중인 이동 에이전트에 대해 절대적인 제어권을 갖기 때문에 호스트 상에서 실행 중인 이동 에이전트를 보호하기 위한 소프트웨어 기반의 현실적인 해결은 불가능한 것으로 알려져 있다[5]. 그러므로 본 논문에서는 소프트웨어적인 해결이 가능한 이동 중인 에이전트의 보호에 대해서 다룬다.

이동 에이전트가 개방된 분산 환경에서 호스트를 옮겨 다닐 때 악의를 가진 호스트에 의해 불법적으로 도청 또는 변경될 수 있다[5]. 그러나 정보 수집, 망관리, 사건 모니터링, 워크플로우 등과 같은 응용 환경처럼 이동 에이전트의 여정이 이동 에이전트가 생성될 때 미리 결정된다면 이동 에이전트 생성자는 여정에 포함된 호스트들만이 이동 에이전트를 수행할 수 있도록 제한할 수 있다. 이렇게 이동 에이전트를 수행할 수 있는 집합을 제한함으로써 여정에 포함되지 않은 잠재적인 악성 호스트가 이동 에이전트의 내용을 도청하거나 변경하는 공격으로부터 이동 에이전트를 보호할 수 있다.

본 논문에서는 기존의 암호화 방법을 활용하여 이동 에이전트 생성자가 이동 에이전트 여정에 포함된 호스트들만이 이동 에이전트를 복호화하여 실행할 수 있도록 하는 이동 에이전트 보호 메커니즘을 제안한다.

2. 관련연구

가. 이동 에이전트 보호에 관한 연구

이동 에이전트 시스템 보안에 관한 연구는 크게 이동 에이전트 시스템 보안에 관한 일반적인 연구, 호스트 보호에 관한 연구, 이동 에이전트 보호에 관한 연구 등으로 나뉘어 진행되고 있다[5]. 그 중에서 이동 에이전트 보호에 관한 연구로는 제3의 신뢰기관을 통한 에이전트 보호, 부정 조작할 수 없는 하드웨어(tamper-proof hardware)를 통한 에이전트 보호, 소프트웨어적인 방법을 이용한 에이전트 보호 등이 있다. 이들 중에서 경제적 측면과 채택의 용의성 때문에 소프트웨어적인 방법을 이용한 에이전트 보호 방법이 더 활발하게 연구되고 있다[5].

소프트웨어적인 방법을 이용한 에이전트 보호 방법으로는 이동 암호화, 에이전트 코드 뒤섞기, 환경 키 생성, 암호학적 추적 기법, 상태 평가를 통한 보호, 부분 정보 보호 등이 있다[5].

나. 그룹 지정 암호화 방법

전체 n명 중에서 선택된 m명에게 안전하게 정보를 전송하기 위해서 그룹 소속원 m명의 공개키로 정보를 각각 암호화하는 방법[7,8], 회의 키잉 프로토콜(Conference Keying Protocol)[9], 다중키 공개키 암호시스템(Multi-key Public-key Cryptography)[1], (m, n) - 역치 방식(Threshold Scheme)의 비밀 분산(Secret Sharing)[2], 중국인의 나머지 정리(Chinese Remainder Theorem)[3,10] 등을 이용할 수 있다. 그러나 이동 에이전트의 장점을 유지하면서 이동 에이전트를 보호하기 위해서는 이동 에이전트 특성에 적합한 암호화 방법을 채택해야한다.

이동 에이전트는 통신 부하를 줄일 수 있고 서버와 클라이

† 본 논문은 한국과학재단의 특정기초연구(98-0102-11-01-3) 연구비 지원에 의한 것임.

언트 사이의 지속적인 연결을 요구하지 않기 때문에 낮은 대역폭을 갖거나 불안정한 통신 환경에 적합하다. 이러한 이동 에이전트의 장점을 살리면서 선택된 호스트들만 이동 에이전트를 복호화할 수 있도록 암호화하는 메커니즘은 통신 회수나 암·복호화 연산 비용이 적어야한다.

표 1은 전체 n중에서 m명의 그룹을 선택해서 암호화할 때, 각각의 방법에 대해서 사전 설정 단계 유무, 통신 회수, 암·복호화 연산수를 분석한 것을 나타낸다. 표 1에서 통신 회수 계산을 위해서 단일 방송(unicasting) 환경을 가정하였다. 그리고 암·복호화에 소요되는 연산수를 계산하기 위해서 각각의 알고리즘이 k비트인 정수를 사용함을 가정하였고 k비트의 곱셈과 나눗셈은 $O(k^2)$, 지수 법에 대해서는 $O(k^3)$를 사용하여 연산수를 계산하였다[7].

표 1 그룹 지정 암호화 방법의 비교

그룹 지정 암호화 방법	사전 설정 단계	통신 회수	암호화 연산수	복호화 연산수
m명 공개키 암호화 방식	없음	m번	$O(mk^3)$	$O(mk^3)$
중국인의 나머지 정리 방식	없음	m번	$O(mk^3)$	$O(k^3)$
회의 키잉 프로토콜 방식	있음	$2m(m-1)$ 번	$O(mk^3)$	$O(mk^3)$
다중키 공개키 암호시스템 방식	있음	$n+m$ 번	$O(k^3+(m+n)k^2)$	$O(2^{n-1}k^3)$
(m,n) 역치 방식 비밀 분산	있음	$n+m$ 번	$O(mk^3+m^2k^2)$	$O(mk^3+m^2k^2)$

표 1에서 나타난 것처럼 사전 설정 단계가 없고 전체적인 암·복호화 연산이 효율적인 중국인의 나머지 정리를 이용한 그룹 지정 암호화 방식이 이동 에이전트 환경에 적합하다. 이러한 분석에 근거하여 공개키 환경에서 동작하는 중국인의 나머지 정리에 기반한 그룹 지정 암호 방법을 본 논문에서 제안하는 에이전트 보호 메커니즘에 이용한다.

3. 그룹 지정 암호화를 활용한 이동 에이전트 보호

이동 에이전트 생성자가 이동 에이전트의 여정 정보를 사전에 알 수 있다면, 생성자는 호스트 정보를 분석하여 호스트의 신뢰 정도를 결정할 수 있다. 이때, 이동 에이전트 생성자는 호스트들을 신뢰받는 호스트와 신뢰받지 못하는 호스트로 나눌 수 있다. 이런 환경에서 일반적으로 신뢰받지 못하는 호스트들은 잠재적인 악성 호스트로 구분될 수 있고 이동 에이전트 생성자는 이동 에이전트를 잠재적인 악성 호스트에게 노출되지 않게 함으로써 이동 에이전트를 보호할 수 있다.

본 논문에서는 이동 에이전트를 신뢰받는 호스트들만이 복호화하여 실행할 수 있도록 중국인의 나머지 정리에 기반한 그룹 지정 암호화와 RSA 공개키 암호시스템을 사용한다. 그리고 이 방법을 통하여 잠재적인 악성 호스트의 공격으로부터 이동 에이전트를 보호하는 메커니즘을 제안한다.

이동 에이전트 생성자 O는 초기 이동 에이전트 MA_0를 공통키 K로 암호화하여 $E_K(MA_0)$를 생성한다. 그리고 공통키 K를 이동 에이전트의 여정에 포함된 호스트들만이 복호화할 수 있도록 중국인의 나머지 정리에 기반을 둔 그룹 지정 암호화 방법을 사용하여 암호화한다. 이를 위하여, 이동 에이전트 생성자는 여정 정보로부터 이동 에이전트가 방문할 호스트들을 알아내고 그 정보를 이용하여 호스트들의 공개키 $((e_1,n_1),(e_2,n_2),\cdots,(e_m,n_m))$ 를 공개키 목록으로부터 획득한다. 그리고, RSA 암호시스템을 사용하여 공통키 K를 각각의 공개키로 암호화한다.

$$C_1 \equiv K^{e_1} \bmod n_1,\ C_2 \equiv K^{e_2} \bmod n_2,\ \cdots,\ C_m \equiv K^{e_m} \bmod n_m \quad (식\ 1)$$

일반적으로 사용자 $i\ (1 \le i \le m)$에게 할당된 공개키 (e_i,n_i) 중 n_i는 쌍마다 서로 소가 되도록 키분배 센터에 의해서 분배된다. 그러므로, 식 1의 $(C_1, C_2, \cdots, C_m)$ 에 대해서 중국인의 나머지 정리를 이용하여 암호화된 그룹키 C를 생성할 수 있다.

$$\begin{cases} x \equiv C_1 \bmod n_1 \\ x \equiv C_2 \bmod n_2 \\ \cdots\cdots \\ x \equiv C_m \bmod n_m \end{cases}, \quad x \equiv C \bmod n_1 n_2 \cdots n_m \quad (식\ 2)$$

이동 에이전트 생성자 O에 의해서 만들어진 이동 에이전트의 구조는 그림 1과 같다.

암호화된 그룹키	공통키에 의해 암호화된 이동 에이전트	두 필드에 대한 서명
C	$E_K(MA_0)$	$S_O(C,E_K(MA_0))$

그림 1 그룹 지정 암호화 결과 생성된 이동 에이전트의 구조

이동 에이전트 생성자 O는 그림 1과 같은 구조를 갖은 이동 에이전트를 여정 정보를 참고하여 첫 번째 수신자 R_1에게 전달한다. 수신자 R_1는 먼저 세 번째 필드의 서명값에 대한 검증을 수행함으로써 첫 두 필드에 대한 무결성과 메시지를 생성한 사람을 확인한다. 그 결과 전송 중 오류나 공격에 의한 변경이 없는 것이 확인되었다면, 암호화된 그룹키인 C에 대해 수신자 R_1의 법 n_1을 적용하여 자신의 공개키로 암호화된 공통키를 얻는다.

$$C_1 = K^{e_1} \equiv C \bmod n_1 \quad (식\ 3)$$

수신자 R_1은 식 3에 자신의 비밀키 d_1를 적용함으로써 공통키 K를 획득할 수 있다.

$$C_1^{d_1} = K^{e_1 d_1} \equiv K \bmod n_1 \quad (식\ 4)$$

수신자 R_1은 식 4의 결과로 얻은 공통키 K를 사용하여 두 번째 필드 $E_K(MA_0)$로부터 이동 에이전트 MA_0로 복호화한다.

$$D_K(E_K(MA_0)) = MA_0 \quad (식\ 5)$$

수신자 R_1은 이동 에이전트 MA_0을 복호화한 후 에이전트를 수행하여 새로운 상태의 이동 에이전트 MA_1을 얻고 그것을 공통키 K로 암호화하여 $E_K(MA_1)$을 생성한다. 그런 다음, 암호화된 그룹키 C와 $E_K(MA_1)$에 대해서 전자 서명하여 서명문 $S_{R_1}(C,E_K(MA_0))$를 생성한다. 그림 2는 수신자 R_1이 이동 에이전트의 수행을 마친 후 이동 에이전트의 상태를 나타낸다.

수신자 R_1은 그림 2의 이동 에이전트를 여정 정보를 참고

하여 다음 수신자 R_2에게 전달한다. 수신자들의 중계를 통하여 이동 에이전트가 마지막 수신자까지 전달되도록 이러한 과정을 반복함으로써 그룹으로 선택되지 않은 호스트의 공격으로부터 이동 에이전트를 보호하는 메커니즘을 수행한다.

암호화된 그룹키	공통키에 의해 암호화된 이동 에이전트	두 필드에 대한 서명
C	$E_K(MA_1)$	$S_{R_1}(C,E_K(MA_1))$

그림 2 수신자 R_1이 수행 후 이동 에이전트 상태

그림 3은 본 논문에서 제안된 이동 에이전트 보호 메커니즘에 대한 요약을 나타낸다.

[단계 1] (이동 에이전트 생성자 O) 이동 에이전트를 그룹 지정 암호화 방법으로 암호화

① 이동 에이전트 MA_0을 공통키 K로 암호화한다.
$E_K(MA_0)$

② 이동 에이전트 여정에 포함된 호스트들의 공개키 $((e_1,n_1),(e_2,n_2),\cdots,(e_m,n_m))$ 를 사용하여 공통키 K를 암호화한다.
$C_1 \equiv K^{e_1} \bmod n_1,\ C_2 = K^{e_2} \bmod n_2,\ \cdots,\ C_m = K^{e_m} \bmod n_m$

③ $(C_1, C_2, \cdots, C_m)$ 에 대해서 중국인의 나머지 정리를 이용하여 암호화된 그룹키 C를 생성한다.

$$\begin{cases} x \equiv C_1 \bmod n_1 \\ x \equiv C_2 \bmod n_2 \\ \cdots\cdots \\ x \equiv C_m \bmod n_m \end{cases}, \quad x \equiv C \bmod n_1 n_2 \cdots n_m$$

[단계 2] (이동 에이전트 생성자 O) 암호화된 이동 에이전트 서명 및 전송

④ 암호화된 이동 에이전트에 대해 전자 서명한다.
$S_O(C,E_K(MA_0))$

⑤ 암호화된 이동 에이전트를 전송한다.
$C,\ E_K(MA_0),\ S_O(C,E_K(MA_0))$

[단계 3] (이동 에이전트 수신자 $R_i\ (1 \le i \le m)$) 암호화된 이동 에이전트의 전자 서명 확인 후 복호화

⑥ 암호화된 이동 에이전트의 전자 서명을 확인한다. 이때, R_0은 이동 에이전트 생성자 O을 나타낸다.
$[C,\ E_K(MA_{i-1})]\ ?=\ V_{R_{i-1}}(S_{R_{i-1}}(C,E_K(MA_{i-1})))$

⑦ 암호화된 그룹키 C에 수신자의 법 n_i을 적용하여 C_i를 얻는다.
$C_i = K^{e_i} \equiv C \bmod n_i$

⑧ C_i와 수신자의 비밀키 d_i을 적용하여 공통키 K를 복호화한다.
$C_i^{d_i} = K^{e_i d_i} \equiv K \bmod n_i$

⑨ 공통키 K를 사용하여 암호화된 이동 에이전트를 복호화한다.
$D_K(E_K(MA_{i-1})) = MA_{i-1}$

[단계 4] (이동 에이전트 수신자 $R_i\ (1 \le i \le m)$) 이동 에이전트 수행 및 변경된 이동 에이전트 암호화

⑩ $Data_i$을 사용하여 이동 에이전트를 수행한다.
$(MA_{i-1}, Data_i) \Rightarrow MA_i$

⑪ 변경된 이동 에이전트를 공통키 K로 암호화한다.
$E_K(MA_i)$

[단계 5] (이동 에이전트 수신자 $R_i\ (1 \le i \le m)$) 암호화된 이동 에이전트 서명 및 전송

⑫ 암호화된 이동 에이전트에 대해 전자 서명한다.
$S_{R_i}(C,E_K(MA_i))$

⑬ 암호화된 이동 에이전트를 전송한다.
$C,\ E_K(MA_i),\ S_{R_i}(C,E_K(MA_i))$

그림 3 그룹 지정 암호화를 활용한 이동 에이전트 보호

4. 결론

개방된 분산 환경에서 호스트를 옮겨 다니며 사용자의 작업을 수행하는 이동 에이전트는 악의를 가진 호스트에 의해 불법적으로 도청 또는 변경될 수 있다.

본 논문에서는 정보 수집, 망관리, 사건 모니터링, 워크플로우 등과 같은 응용 환경처럼 이동 에이전트의 여정을 이동 에이전트가 생성될 때 미리 알 수 있는 경우에 이동 에이전트를 수행할 수 있는 집합을 여정에 포함된 호스트로 제한함으로써, 악성 호스트가 이동 에이전트의 내용을 도청하거나 변경하는 공격으로부터 이동 에이전트를 보호하는 메커니즘을 제안하였다. 본 논문에서는 이를 위하여 중국인의 나머지 정리에 기반한 그룹 지정 암호 방법을 활용하였다.

향후 연구로는 이동 에이전트 환경에서 보다 더 효율적인 그룹 지정 암호 방법의 개발과 이동 에이전트의 여정 정보가 알려지지 않은 환경에서 이동 에이전트를 보호하는 소프트웨어 기반의 실현 가능한 기법에 대한 연구가 필요하다.

참고문헌

[1] C. Boyd, "Some Applications of Multiple Key Ciphers," Advances in Cryptology-EUROCRYPT '88 Proceesings, Springer-Verlag, pp. 455-467, 1991.

[2] S. Berkovits, "How to Broadcast a Secret," Advances in Cryptology-EUROCRYPT '91 Proceedings, Springer-Verlag, pp. 535-541, 1991.

[3] G. H. Chiou and W. T. Chen, "Secure Broadcasting Using the Secure Lock," IEEE Transaction on Software Engineering, Vol. 15, No. 8, pp. 929-934, August 1982.

[4] C. G. Harrison, D. M. Chess, and A. Kershenbaum, "Mobile Agents : Are they a good idea?," Research Report, IBM Research Division T. J. Watson Research Center, March 1995.

[5] W. Jansen and T. Karygiannis, "Mobile Agent Security," NIST Special Publication 800-19, 1999.

[6] D. B. Lange and M. Oshima, "Seven Good Reasons for Mobile Agents," Communications of the ACM, Vol. 42, No. 3, pp. 88-89, March 1999.

[7] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997.

[8] B. Schneier, Applied Cryptography, Second Edition, John Wiley & Sons, Inc., 1996.

[9] D. T. Tang and C. K. Wong, "A Conference Key Distribution System," IEEE Transaction on Information Theory, Vol. IT-28, No. 5, pp. 714-720, September 1982.

[10] 김응대 외 1인, 정수론, 경문사, 1997.