이동에이전트 기반의 전자상거래를 위한 안전한 그룹통신 기법

조현진*, 김구수*, 엄영익*
*성균관대학교 컴퓨터공학과
e-mail : {hjcho, gusukim, yieom}@ece.skku..ac.kr

Secure Group Communication Scheme for e-Commerce Based on Mobile Agents

Hyun Jin Cho*, Gu Su Kim*, Young Ik Eom*
*Dept of Computer Engineering, SungKyunKwan University

요 약

이동 에이전트란 어떠한 동작을 수행하는 명령과 자신의 상태 정보를 포함하는 자율적인 소프트웨어 객체이다. 이동 에이전트는 자율적으로 이동할 수 있으며 복제와 증식이 가능하고 사용자의 업무를 대신해서 수행할 수 있다는 장점으로 인해 전자상거래에서 사용자를 대신하여 상품 검색 및 구매에 사용될 수 있다. 이 때 다수의 이동 에이전트가 하나의 그룹이 되어 서로 메시지를 주고받으며 사용자의 요구사항을 수행한다. 이동 에이전트간 전달되는 메시지는 상품의 정보뿐 아니라 사용자 또는 에이전트의 비밀정보가 될 수 있다. 악의를 가진 외부 개체로부터 그룹 멤버쉽이나 메시지가 변경된다면 이동 에이전트 그룹은 사용자가 의도하지 않는 동작을 수행할 수 있다. 본 논문에서는 이러한 공격을 방어하기 위해 그룹 멤버간 암호화 통신을 할 수 있는 그룹 세션키 생성 기법을 제안한다. 기존 기법과는 달리 본 논문에서는 중앙 키 분배 서버 없이 그룹에 참가하는 이동 에이전트 각자 그룹 세션키를 생성한다. 또한 키 갱신을 주기적으로 수행함으로써 외부 개체로부터 그룹 세션키의 습득을 어렵게 한다.

1. 서론

이동 에이전트란 계산수행 능력과 상태 정보를 포함하고 있는 능동적이고 자율적인 소프트웨어 객체이다. 이동 에이전트는 한 호스트에서 작업을 수행하다가 현재 상태를 저장해 다른 호스트로 이동하여 중단된 작업을 계속 수행할 수 있다. 그리고 이동 에이전트는 이동 코드 또는 이동 객체와는 달리 자율적으로 호스트를 이동할 수 있는 특징을 가진다. 이러한 특징으로 인하여 이동 에이전트는 대역폭이 적은 네트워크 환경 또는 네트워크가 단절된 상황에도 적절하게 대응할 수 있다. 그리고 스스로 복제할 수 있어 병렬처리를 쉽게 구현할 수도 있다[1].

위에서 열거한 여러 장점으로 인해 이동 에이전트는 네트워크 관리, 이동 컴퓨팅, 정보 관리, 웹 서비스, 원격 소프트웨어 관리, 전자상거래 등 여러 분야에 사용될 수 있다[2]. 특히 전자상거래의 경우 거래의 자동화를 위해 이동 에이전트를 도입하고 있다[3][4]. 전자상거래에 참여하는 사용자는 다수의 이동 에이전트를 생성하여 물품을 제공하는 서버로 이동시켜 자신이 원하는 거래를 수행하도록 한다[5]. 사용자가 생성한 에이전트들은 하나의 그룹을 구성하여 자신이 수집한 데이터를 주고받으며 업무를 수행해 나간다. 멤버간 통신은 인터넷의 개방된 네트워크 환경에서 이루어진다. 따라서 사용자의 목적을 올바르게 수행하기 위해서는 그룹의 멤버들이 안전하게 메시지를 교환할 수 있는 기법이 필요하다. 따라서 본 논문에서는 외부 개체로부터 멤버간 통신을 보호할 수 있는 그룹 통신 기법을 제시하고자 한다.

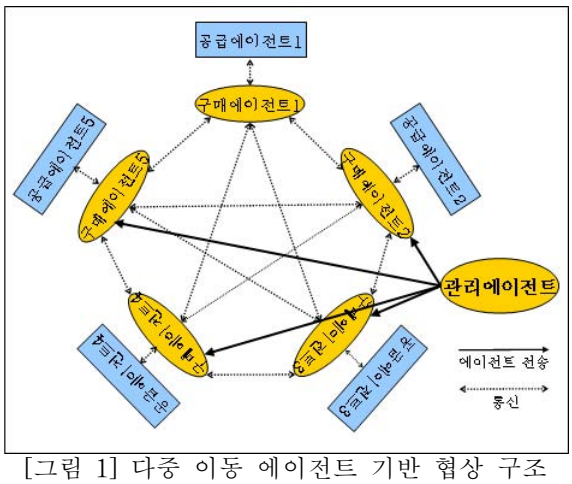
본 논문의 구성은 다음과 같다. 2장에서 이동 에이전트 기반의 전자상거래와 안전한 그룹 통신의 관련연구와 필요한 기술들에 대하여 기술하겠으며, 3장에서는 본 논문의 제안 기법을 기술한다. 마지막으로 4장에서는 이동 에이전트의 안전한 그룹 통신 기법의 결론과 향후 연구과제에 대해 설명한다.

2. 관련연구

2.1 이동 에이전트 기반 전자상거래 시스템

실제의 상거래는 소비자와 공급자간의 협상을 통해 이루어진다. 즉, 소비자는 다수의 공급자들의 제안 내용을 토대로 자신이 원하는 최적의 상품을 선택하게 된다. 전자 상거래 역시 구매자는 다수의 공급자들이 제안하는 내용을 비교하여 최후의 선택을 하게 된다. 사용자는 이동 에이전트가 복제를 통해 동일한 객체를 생성하고 이동성과 자율성을 가진다는 점을 고려하여 전자상거래를 위한 업무를 대신 수행하도록 지시 할 수 있다. 즉, 사용자는 하나가 아닌 다수의 구매 에이전트를 생성하고 공급처로 이동시켜 자신이 원하는 상

품을 검색하고 구매하도록 한다. 구매 에이전트는 공급 에이전트와 협상을 하고 구매 에이전트간 서로 정보를 공유하여 사용자가 원하는 거래를 수행한다[5]. 이러한 구조를 [그림 1]에서 보인다.



[그림 1] 다중 이동 에이전트 기반 협상 구조

2.2 안전한 이동 에이전트 그룹 통신

다수의 이동 에이전트가 데이터를 주고받으며 하나의 업무를 수행할 때, 각 에이전트는 나머지 멤버로부터 수신된 정보를 바탕으로 다음 수행할 행동을 결정한다. 전자상거래 같이 거래를 위한 통신 메시지에는 가격 정보뿐만 아니라 사용자 또는 에이전트의 비밀 정보가 담겨져 있다. 또한 금전정보 역시 전송될 수 있기 때문에 안전환 환경에서 통신이 이루어 져야 한다[6].

악의를 가진 에이전트는 자신이 그룹 멤버인 척 하거나 통신 메시지를 도청할 수 있다. 이러한 결과로 중요 정보 노출이나 사용자가 의도하지 않은 업무의 수행을 야기할 수 있다. 이러한 공격을 방어하기 위해서 그룹의 멤버는 그룹 내 다른 멤버들을 인증할 수 있어야 한다[7]. 또한 서로 주고받은 메시지를 외부 개체로부터 보호할 수 있어야 한다. 이러한 문제점들을 해결하기 위해 그룹 결성 전 멤버간 인증을 한다. 그리고 공동의 그룹 세션키를 생성하여 멤버간 전송하는 모든 메시지를 암호화 한다.

기존의 이동 에이전트를 위한 안전한 그룹통신에 대한 관련연구로 중앙 키 관리 서버를 이용하여 이동 에이전트 그룹 세션키를 생성하고 분배하는 기법이 있다[8].

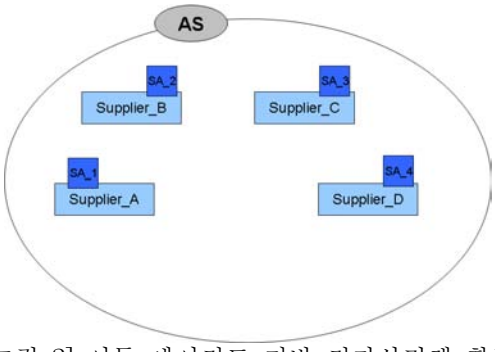
3. 제안 기법

기존에 제안한 기법은 Chairperson이라 불리는 중앙의 키 관리 서버가 존재하며, 키 생성과 분배를 담당한다[8]. 이러한 기법의 단점으로 첫 째, 키 분배 서버 자체의 동작 실패로 인해 키를 생성하지 못할 수 있다. 또한 네트워크의 단절로 인해 키 생성 후 또는 키 갱신시 모든 멤버가 동일한 시점에 새로운 키를 전송받지 못할 수 있다[9].

본 논문에서는 이러한 점을 고려하여 그룹 멤버들간 비밀 정보를 생성하고 공유할 수 있는 기법[10]을 이용하여 중앙의 키 관리 서버 없이 그룹 세션키를 생성하는 기법을 제안하고자 한다.

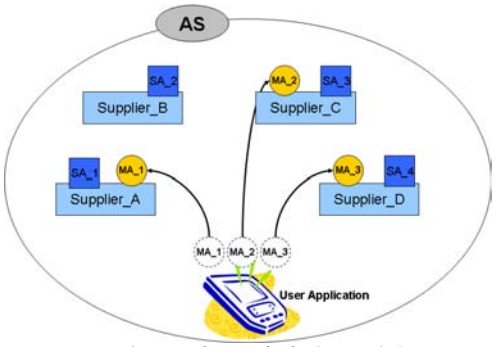
3.1 이동 에이전트 기반 전자상거래 환경

네트워크 내에 전자상거래를 위한 환경이 다음과 같이 구성되어 있다. 사용자에게 상품을 제공해 주는 세 개의 supplier(Supplier_A, B, C)와 그 위에 구매 에이전트와 통신 및 협상을 하는 supply agent(SA_1, 2, 3)가 존재한다. 또한 이동 에이전트간 인증을 위한 인증 서버(AS : Authentication Server)가 존재한다[그림 2].



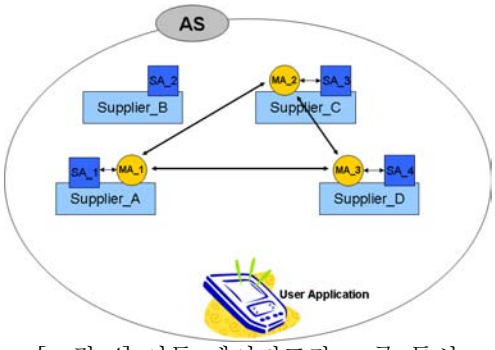
[그림 2] 이동 에이전트 기반 전자상거래 환경

사용자는 자신의 단말기를 이용하여 구매하고자 하는 물품의 가격을 조사하여 최저가로 공급하는 supplier를 찾고 싶다. 먼저 가격을 조사하는 이동 에이전트 3개를 생성한다. 이때 생성된 MA_1,2,3은 자동으로 멤버쉽이 구성되어 하나의 그룹을 형성하고 동일한 그룹 아이디(G_id)와 멤버 아이디 리스트(MA_1, 2, 3)를 할당받게 된다. 그 다음 사용자는 각 에이전트에게 supplier의 위치를 입력하여 이동 시킨다[그림 3].



[그림 3] 이동 에이전트 전송

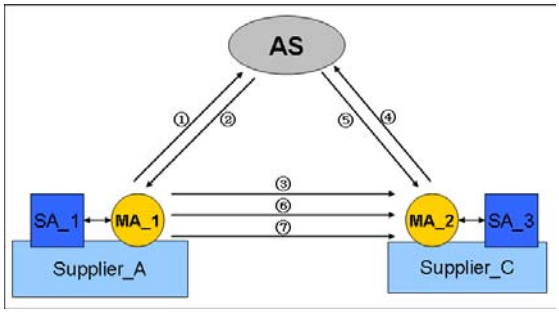
supplier로 이동한 사용자의 에이전트는 supply agent로 부터 상품 관련 정보(가격, 수량, 구매 조건 등)를 제공받는다. 각 사용자의 이동 에이전트는 자신이 알아낸 정보를 나머지 멤버와 공유하여 사용자가 원하는 요구사항에 최대한 가까운 제공자를 선택한다[그림 4].



[그림 4] 이동 에이전트간 그룹 통신

하지만 먼저 각 멤버는 통신하기 전 서로가 동일한 사용자에 의해 생성이 된 것인지 확인하기 위한 인증 절차가 필요하다. 인증 절차는 PKI기반의 Needham-Schroeder 프로토콜을 이용하며, 인증 절차의 예는 다음과 같다.

사용자 에이전트 MA_1과 MA_2는 통신하기 전 서로에 대한 신원을 확인하고자 한다. MA_1과 MA_2는 AS와 통신하여 자신의 공개키를 전송받는다. 그러고 나서 MA_1이 인증하려는 MA_2의 공개키를 AS에게 요청한다. MA_2의 공개키를 전송받은 MA_1은 $nonce_{MA_1}$ 생성한 후 자신의 ID와 함께 MA_2의 공개키로 암호화 하여 MA_2에게 전송한다. MA_2역시 AS와 통신하여 MA_1의 공개키를 전송받는다. 그리고 이 전에 MA_1이 전송한 $nonce_{MA_1}$와 자신의 ID, 그리고 $nonce_{MA_2}$를 생성하여 MA_1의 공개키로 암호화한 후 MA_1에게 전송한다. MA_2로부터 $nonce_{MA_2}$를 수신한 MA_1은 MA_2의 공개키로 암호화하여 MA_2에게 전송한다. 이 과정을 통해 MA_1과 MA_2는 서로를 신뢰할 수 있게 된다[그림 5]. 나머지 멤버 역시 이 과정을 통해 서로에 대한 인증을 수행한다.



① $MA_1 \rightarrow AS: MA_1 \| MA_2$
② $AS \rightarrow MA_1: E_{KR_S}\{KU_{MA_2}, MA_2\}$
③ $MA_1 \rightarrow MA_2: E_{KU_{MA_2}}\{nonce_{MA_1}, MA_1\}$
④ $MA_2 \rightarrow AS: MA_2 \| MA_1$
⑤ $AS \rightarrow MA_2: E_{KR_S}\{KU_{MA_1}, MA_1\}$
⑥ $MA_2 \rightarrow MA_1: E_{KU_{MA_1}}\{MA_2, nonce_{MA_1}, nonce_{MA_2}\}$
⑦ $MA_1 \rightarrow MA_2: E_{MA_2}\{nonce_{MA_2}\}$

[그림 5] 이동 에이전트간 인증 절차

3.2 그룹 세션키 생성

그룹 세션키 생성과정은 다음과 같다.

가. 멤버간 인증 후 MA_1이 각 멤버에게 데이터를 전송해야 할 상황이 발생하였다. MA_1은 임의의 변수 a와 G_id를 자신의 비밀키로 서명하여 MA_2와 MA_3에게 전송한다.

① $MA_1 \rightarrow MA_{2,3}: E_{KR_{MA1}}(a, G\_id, MA\_1,2,3)$

나. MA_2,3은 이 정보를 MA_1의 공개키로 확인하고 전송받은 데이터 a를 자신의 비밀키와 XOR 연산하여 그룹 세션키를 생성할 정보(Y_{MAi})를 생성한다. 이 후 자신의 비밀키로 서명하여 나머지 멤버에게 전송한다.

① $MA_{2,3}$: $D_{KU_{MA1}}(E_{KR_{MA1}}(a, G\_id, MA\_1,2,3))$
② MA_i: $Y_{MAi} = KR_i \oplus a$
③ MA_i: $E_{KR_{MAi}}(Y_{MAi})$
④각 멤버는 나머지 멤버에게 다음의 메시지 전송 : $E_{KR_{MAi}}(Y_{MAi})$

다. 이제 모든 멤버는 다른 멤버의 Y_{MAi} 를 갖게 되었다. 이 정보를 이용하여 그룹 세션키(KG_{id})를 생성한다. 그룹 세션키를 생성하는 과정은 다음과 같다.

① 그룹 내에 멤버 MA_1, MA_2, MA_3 이 있다.
② 멤버 MA_1은 다음과 같이 그룹 세션키를 생성한다.

$$KG_{MA1} = KR_{MA1} \oplus Y_{MA2} \oplus Y_{MA3}$$

이것을 다음과 같이 쓸 수 있다.

$$KG_{MA1} = KR_{MA1} \oplus KR_{MA2} \oplus a \oplus KR_{MA3} \oplus a$$

③ 멤버 MA_2는 다음과 같이 그룹 키를 생성한다.

$$KG_{MA2} = Y_{MA1} \oplus KR_{MA2} \oplus Y_{MA3}$$

이것을 다음과 같이 쓸 수도 있다.

$$KG_{MA2} = KR_{MA1} \oplus a \oplus KR_{MA2} \oplus KR_{MA3} \oplus a$$

④ 멤버 MA_3은 다음과 같이 그룹 키를 생성한다.

$$KG_{MA3} = Y_{MA1} \oplus Y_{MA2} \oplus KR_{MA3}$$

이것을 다음과 같이 쓸 수도 있다.

$$KG_{MA3} = KR_{MA1} \oplus a \oplus KR_{MA2} \oplus a \oplus KR_{MA3}$$

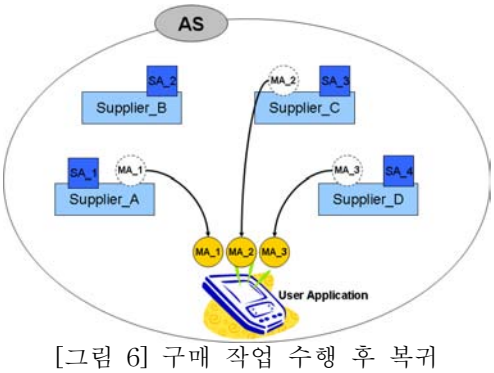
⑤ XOR 연산은 결합법칙과 교환법칙이 성립한다. 따라서 모든 멤버가 알고 있는 a값의 위치를 변경함으로써 각 멤버는 동일한 그룹 키를 생성할 수 있다.
이 때 각 멤버는 키 생성 순서를 알아야 하는데 그룹 세션키 생성을 요청하는 첫 번째 메시지에 포함되어 있다.

$E_{KR_{MA1}}(a, G\_id,$ MA_1,2,3)

⑥ 이제 A, B, C 세 멤버 모두 동일한 그룹 키를 가지게 되었다.

($KG_{id} = G_{MA1} = G_{MA2} = G_{MA3}$)

그룹 세션키가 생성되면 이후의 통신은 암호화된 메시지를 이용한다. 구매 에이전트는 업무를 모두 종료한 뒤 사용자의 단말기로 복귀하여 수행한 작업의 내용을 출력한다.



[그림 6] 구매 작업 수행 후 복귀

3.3 그룹 세션키 갱신

그룹 세션키는 멤버쉽의 변화에 관계없이 주기적으로 갱신된다. 이는 각 멤버가 이미 동일한 사용자에 의해서 생성된 객체이기 때문이다. 따라서 그룹 세션키를 forward_secrecy나 backward_secrecy를 만족할 필요없이 외부의 개체에 대해 보호만 하면 된다.

키 갱신을 요청하는 멤버는 리스트의 순서에 따른다 (MA_1 → MA_1+i → MA_i+2 → ... → MA_1). 각 멤버는 자신의 순서가 되면 임의의 변수 a와 다음 그

룹 세션키 갱신 시간을 생성하고 처음 이전의 그룹 세션키로 서명하여 각 멤버에게 전송한다. 각 멤버는 이 정보를 확인하여 새로운 그룹 세션키를 생성하게 된다. 키 갱신 과정은 다음과 같다.

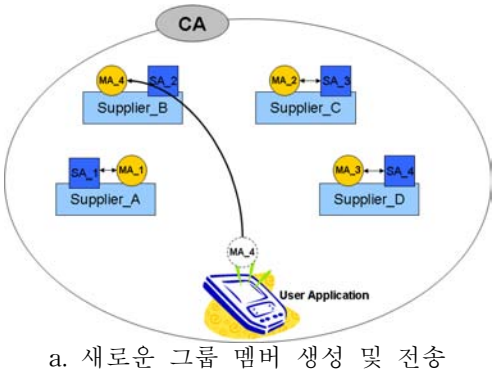
① 그룹 내에 멤버 MA_1, MA_2, MA_3 이 있고, 그룹 세션키를 갱신해야 하는 멤버는 MA_2가 되었다.
② MA_2는 새로운 변수 a′와 다음 그룹 세션키 갱신 시간을 생성한다. 그러고 나서 이 전의 그룹 세션키로 서명 하여 각 멤버에게 전송한다.

$$\{a', G\_id, MA\_1,2,3, time, ((a' PVERG\_id PVERMA1,2,3 PVERtime) \oplus E_{KG,si})\}$$

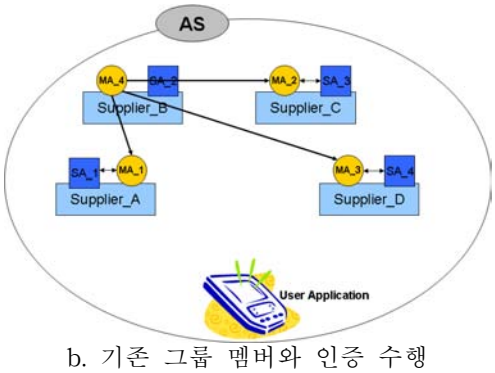
③ 이 후, 각 멤버는 전송받은 정보의 서명을 확인하고 새로운 키 생성을 시작한다.(동일한 키 생성 과정)

3.4 그룹 멤버쉽 관리

가. 멤버 참가
사용자는 새로운 이동 에이전트를 생성하여 그룹에 참가시킬 수 있다. 이 때 기존의 멤버와 새롭게 그룹에 참가하는 멤버는 서로의 신원을 확인해야 한다. 사용자는 MA_4를 생성하여 다른 공급자에게 전송한다. MA_4는 자신의 존재를 기존의 멤버에게 알리고 나머지 멤버와 상호 인증을 수행한다[그림 7].



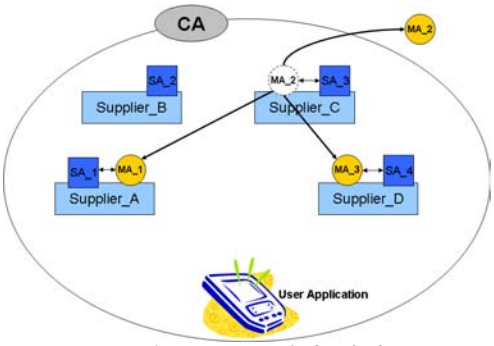
a. 새로운 그룹 멤버 생성 및 전송



b. 기존 그룹 멤버와 인증 수행

[그림 7] 새로운 그룹 멤버 생성 및 인증 수행

나. 멤버 탈퇴
그룹 내 멤버는 여러 가지 이유로 인해 그룹을 벗어날 수도 있다(사용자의 호출, 다른 업무 수행, 뜻하지 않은 종료 등). MA_2는 그룹 탈퇴 시 기존의 모든 멤버에게 자신의 탈퇴를 전달한다[그림 8].



[그림 8] 그룹 멤버 탈퇴

4. 결론 및 향후과제

본 논문에서는 이동 에이전트 기반의 안전한 그룹 통신을 위한 키 생성 기법을 제안하였다. 기존의 중앙 키 관리 서버가 있는 모델은 중앙 키 관리 서버의 병목 현상이 있을 수 있다. 또한 네트워크의 단절로 인한 키 전달의 실패 가능성도 있다[9]. 따라서 본 논문에서는 기존의 기법과는 달리 그룹에 참여하는 멤버 각자가 그룹 세션키를 생성하는 기법을 제안한다.

향후 연구 과제로는 중앙 키 관리 기법과의 성능 비교와 대 규모의 멤버가 참가하는 그룹 내 인증 및 그룹 세션키 생성 기법을 연구할 예정이다.

참고문헌

[1] Aneiba, A., Rees, J. S., "Mobile Agent Technology and Mobility," Proceeding of the 5th Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting, June 2004
[2] Danny B. L., Mitsuru O., "Seven good reasons for mobile agents," Communications of the ACM, pp 88-99, March 1999
[3] Dasgupta, P., Narasimhan, N., Moser, L. E.,; Melliar-Smith, P. M., "MAgNET: mobile agents for networked electronic trading," IEEE transactions on knowledge and data engineering, 1999
[4] Huai, Q., Sandholm, T., "Nomad: Mobile Agent System for an Internet-Based Auction House," IEEE internet computing, 2000
[5] Lin, F. C., Kuo, C. N., "Cooperative multi-agent negotiation for electronic commerce based on mobile agents," IEEE International Conference, 2002
[6] Novak, P., Rollo, M., Hodik, J., Vlcek, T., "Communication Security in Multi-agent Systems," Lecture notes in computer science, no. 2691, 2003
[7] John P., Arkady Z., Maria I., "A Buddy Model of Security for Mobile Agent Communities Operating in Pervasive Scenarios," Australasian Information Security Workshop, 2004
[8] Mazlan, M. A., Samsudin, A., Budiarto, R., "Secure groups communication for mobile agents based on public key infrastructure, " The 9th Asia-Pacific Conference, 2003
[9] Moyer, M. J., Rao, J. R., Rohatgi, P., "A survey of security issues in multicast communications," IEEE network, 1999
[10] Saxena, A., Soh, B., "A new paradigm for group cryptosystems using quick keys," The 11th IEEE International Conference, 2003