분산객체 환경에서의 이동객체 보안

홍성표* · 송기범* · 이철승* · 이 준**

*조선대학교 대학원 컴퓨터공학과
**조선대학교 전자정보공과대학 컴퓨터공학부

Mobile Object Security in Distributed Object Environment

Seong-pyo Hong* · Gi-beom Song* · Chiol-seong Lee* · Joon Lee**
*Dept. of Computer Engineering, Graduate School, Chosun University
***School of Computer Engineering, Chosun University

요 약

분산시스템 환경에 있어서 적합한 개선안으로 믿어지고 있으며, 전자상거래, 이동 컴퓨팅, 원격통신시스템, 정보관리, 정보검색 등의 분야에서 응용이 확산되고 있는 이동에이전트와 분산객체 환경 표준인 CORBA와의 통합은 분산시스템에서 일어나고 있는 여러 가지 문제점들을 효율적으로 개선시킬 수 있다. 그러나, 대단위 분산객체 기술과의 결합은 이동에이전트 시스템을 확장시키고, 다른 에이전트 플랫폼과의 호환성을 보장하지만 그에 대한 역효과로 여러 가지 보안상의 문제점들이 나타나고 있다.

본 논문에서 제안한 이동에이전트 시스템은 기존의 시스템과는 달리 이동에이전트 표준인 MASIF를 기반으로 하고, MASIF에서 제시한 보안 요구들을 CORBA 보안서비스 명세를 이용하여 구현함으로써 다른 에이전트 플랫폼과의 호환성을 보장할 수 있도록 하여, 추후 전자상거래를 비롯한 다양한 인터넷 서비스들의 대규모 개방형 분산시스템으로의 확장이 가능할 것이다.

ABSTRACT

Integration with CORBA and mobile agent is improving various kinds problems that are happening in distributed system. This technology is guarantee the interoperability to other agent platforms and extend the mobile agent system but appears various kinds problems of security.

In this paper, we propose the mobile agent security system that is based on CORBA security service specification and MASIF. Since proposed system is based on CORBA and MASIF, it is extend the large scale of distributed system and interoperable with other agent platforms.

키워드
Distributed object environment, Mobile agent Security, CORBA

I. 서 론

현재 이동에이전트 기술은 분산시스템 환경에 있어서 적합한 개선안으로 믿어지고 있으며 분산환경을 위한 여러 가지 이동에이전트 시스템들이 개발되어지고 있다. 이동에이전트는 기존의 클라이언트/서버 구조의 여러 가지 비효율적인 문제점들을 감소시켜 주기 때문에, 전자상거래, 이동 컴퓨팅, 원격통신시스템, 정보관리, 정보검색 등의 분야에서 응용이 확산되고 있는 추세이다.[1]

분산객체 시스템의 표준으로 자리잡아가고 있는 CORBA를 제안한 OMG(Object Management Group)에서는 새로운 패러다임인 이동에이전트 플랫폼간의 상호운용성 지원을 위해 CORBA를 기반으로 하는 MASIF(Mobile Agent System Interoperability)를 추가하였다. MASIF는 특정 플랫폼에 의존하지 않는 중

립적인 구조를 지향하고 있으며, 시스템 차원에서 에이전트 상호 운영성을 제공하고자하는 목표를 가지고 있다.[2]

분산객체시스템의 표준인 CORBA와 분산시스템 환경에 적합한 개선안으로 믿어지고 있는 이동에이전트와의 통합은 분산시스템에서 일어나고 있는 여러 가지 문제점들을 효율적으로 개선시킬 수 있다. 그러나, 대단위 분산객체 기술과의 결합은 이동에이전트 시스템을 확장시키고, 다른 에이전트 플랫폼과의 호환성을 보장하지만 그에 대한 역효과로 여러 가지 보안상의 문제점들이 나타나고 있다.

이러한 대단위 분산 이동에이전트 환경에서 안전한 컴퓨팅환경이 구현되기 위해서는 공유 자원의 노출이나 변경, 불법적인 사용자들의 위협 등에 대처하며 분산환경의 이질화된 시스템들과 다양한 암호학적 알고리즘에 대해 중립적인 통합 메커니즘이 요구된다.[3]

본 논문에서는 CORBA와 이동에이전트를 통합함으로써 나타나는 여러 가지 보안 문제점들 중에서 각종 자원과 데이터에 대한 무결성과 가용성에 영향을 끼칠 수 있는 보안 위협에 대한 보안 기능을 가진 에이전트 시스템의 모델을 설계하였다. 제안한 시스템은 기존의 이동에이전트 시스템과는 달리 이동에이전트 표준인 MASIF를 기반으로 하기 때문에 분산 이동 컴퓨팅 환경에 적용이 가능하다. 또한, MASIF에서 제시한 보안 요구들을 CORBA 보안서비스 명세를 이용하여 구현함으로써 다른 에이전트 플랫폼과의 호환성을 보장할 수 있도록 하여 추후 전자상거래를 비롯한 다양한 인터넷 서비스들의 대규모 개방형 분산시스템으로의 확장이 가능할 것이다.

II. 개방형 분산환경을 위한 보안 서비스

2.1 DCE(distributed computing environment)

OSF/DCE(open system foundation/distributed computing environment) 보안 서비스는 kerberos 5.0을 기반으로 권한 부여 및 접근 제어 기능을 추가하여 이질적 분산환경에 대한 사용자 인증과 데이터의 무결성, 비밀성을 지원한다. OSF/DCE의 서비스는 등록 서비스, 인증 서비스, 권한 부여 및 접근 제어 서비스로 구성된다.

● 등록 서비스는 이름, 식별자, 비밀키 등의 보안 주체에 대한 정보들을 데이터베이스에 유지, 관리한다.

● 인증 서비스는 사용자의 로그인 절차를 통해 사용자의 실체에 대한 인증을 수행하며, 이 때 유효기간이 설정된 TGT(ticket-granting ticket)을 부여받아 다른 사용자의 도용을 방지한다.

● 권한 부여 및 접근 제어 서비스는 임의의 사용자들에 대한 접근 여부를 선별하도록 한다.

DCE는 원격 프로시저 호출(RPC)을 사용하며 GSS-API(Generic Security Service Application Program Interface)를 지원한다. 따라서, DCE 서버 응용프로그램은 클라이언트와 전송되는 데이터에 대하여 인증할 수 있다. RPC-GSS_API는 비보호, 인증, 데이터 무결성, 비밀성을 제공한다.

클라이언트/서버 구조에 대한 비보호란 클라이언트와 서버 사이의 통신상에 DCE 보안 서비스가 포함되지 않기 때문에 클라이언트의 사용자는 모두 서버에게 인증되어야 한다. 데이터의 무결성을 제공하기 위해 서버에 전송되는 데이터에 체크썸(Checksum)을 포함한다. 이것으로 서버에 수신된 데이터와 클라이언트의 데이터의 일관성을 보장하도록 한다.

DCE는 DES(Data Encryption Standard)와 MD5 알고리즘을 추가하여 RPC-GSS_API를 통해 사용자 데이터의 무결성을 보장한다. DCE에서는 비밀키와 세션 키가 사용된다. 비밀키는 로컬 머신과 DCE 보안 서버와 공유하여 각기 데이터베이스에 저장된다. 세션 키는 응용 클라이언트와 응용서버, DCE 보안 서버 사이에서 데이터와 체크썸을 암호화하며 난수로 생성되어 한번 사용되고 버려진다.[4][5]

2.2 SESAME

SESAME(Secure European System for Application in a Multivendor Environment)는 안전한 개방형 분산 시스템을 구축하기 위하여 OSI 7계층 모델의 응용계층에 중점을 둔 보안 시스템으로 인증, 권한 부여, 데이터 무결성 및 비밀성, 부인 봉쇄 등을 지원한다.

SESAME는 보안 서비스 제공에 대해 암호화 알고리즘의 사용을 최소화하였다. 즉, 클라이언트와 서버 사이에 전달되는 보안 관련 제어 데이터에 대해서만 암호화하였으며, 사용자 데이터에 대해서는 필요에 따라 선택적으로 암호화하도록 하였다.

SESAME에서는 데이터를 보호하기 위해 Kerberos 키 분배 규약을 이용하였으며 공개 키 암호 기법을 이용할 수 있도록 하였다. 또한, X.509 디렉토리 사용자 신임장을 지원한다. 따라서, 이 구조는 SSO(Single Sign On) 방식으로 Kerberos의 정의에 기반한 인증 기법과 공개 키 암호화를 사용한 인증을 수행한다. 따라서, SESAME는 kerberos 5.0의 특징에 이질성과 보다 정교한 접근 제어 및 공개키 기법을 추가한 확장형태라 할 수 있다. 그리고, 분산 환경에 대한 확장된

접근 제어는 GSS-API를 사용한다. 온라인 서버와 오프라인 서버로 구성하여 관리의 효율성을 추구한다.

접근 제어 정책은 사용자의 조직적 역할 또는 업무에 기본을 둔 권한 서비스를 제공한다. 또한 분산 시스템 환경에 있어서 권한 정보들이 위임되는 경우 권한 정보의 원래 소유자 범위를 초과할 때 권한 정보의 속성과 타당한 원격지를 제약할 수 없도록 고려하였다.

SESAME는 대칭/비대칭형 암호화 알고리즘과 단방향 암호화 알고리즘을 사용하였다. 대칭형 알고리즘은 무결성과 기밀성을 위하여 필요한 교환 데이터를 암호화하는데 이용되며, 비대칭형 암호화 알고리즘은 데이터 발신지의 인증과 PAC(Privilege Attribute Certificate) 정보의 무결성과 비대칭 키를 전달받는 PVF(PAC Validation Facility)의 키 분배 및 다른 보호 영역 사이에서의 키 분배, 디렉토리 신임장을 서명하거나 요구할 때에 이용된다. 또한, 사용자 데이터의 무결성을 보호하기 위하여 단방향 알고리즘을 사용하였다.

클라이언트와 서버의 데이터 교환은 임시적 기본키와 대화키를 사용한다. 기본 키는 클라이언트와 서버의 PVF 사이에 설정된 임시 키이며, 대화키는 SACM(Secure Association Context Manager)을 통한 클라이언트 응용과 서버 응용사이에 설정된 임시 키이다. 또한, 키 분배 기법은 KDS(Key Distribution Server)에 기본 키와 X.509 디렉토리 신임장에 기반하여 해당 사용자의 키를 등록하도록 한다.

암호화를 사용하여 이용자 또는 원격 응용간에 정보를 교환하며, 서로 다른 정보보호 정책을 가진 다수의 도메인 운영이 가능하다. 공개 키 기술을 이용하여 대규모 네트웍으로 확장이 가능하며, 국제 표준의 준수, GSS-AP를 적용, 메커니즘에 독립적인 서비스와 인터페이스 제공 및 정보보호 기반 요소들의 집합체적 구성으로 구조적 유연성을 제공한다.[6][7]

III. CORBA 기반 보안 서비스와 이동에이전트 시스템

3.1 CORBA 기반 보안 서비스

개방형 분산 객체환경은 서브 클래스나 상속 개념으로 대규모 시스템으로 확장되며, 소프트웨어 요소간 캡슐화에 의한 상호 작용이 증가하여 사용자의 신뢰 범위가 복잡해진다. OMA(Object Management Architecture)를 기반으로 하는 CORBA 시스템은 단일 시스템에 비해 다양한 경로로 정보 접근이 가능하여 그들간의 일관성이나 신뢰성에 대한 문제의 가능성이 발생한다. OMG는 CORBA 응용들에 대해서 핵심적인 보안 기능들과 인터페이스를 정의하여 인터넷을 비롯하여 ISDN, 이동 통신망, 위성 통신망, 각종 LAN 등 다양한 이질 시스템의 연동에 따른 보안 문제의 해결책을 제공하고 있다.

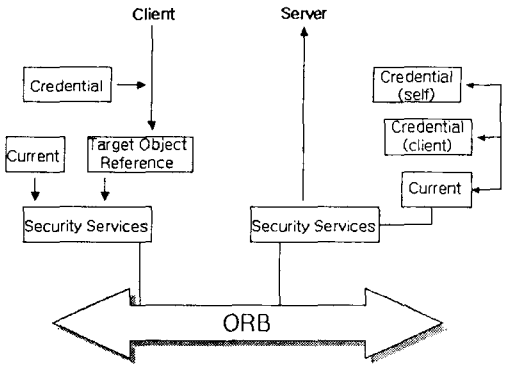

그림 1. CORBA 보안 서비스

CORBA 보안 서비스는 전체 OMA 및 서비스들 사이에서 비밀성, 무결성, 책임성, 유용성 등을 만족시킨다. 또한, 기능적으로 접근제어, 감사, 인증을 수행 할 수 있다. CORBA의 객체 보안 서비스는 사용자뿐 아니라 운용되는 모든 객체들에 대해서 적용될 수 있다. 즉, 사용자의 접근만을 제어하는 대신 객체들의 접근을 줄여 객체 단위의 추가적인 보안 기능에 대한 영향을 최소화하여야 한다.

CORBA 보안 서비스는 인증 서비스, 권한 부여 서비스, 키 분배, 감사, 접근 제어 서비스로 제시되어 있다. 시스템과 시스템의 정보에 대한 위협 요소들은 각 시스템과 취급 정보의 특성에 따라 다양하다. 이에 대해 구조적 모델과 객체 모델을 기반으로 보안 구조를 제시하였으며, 보안 구조들은 객체 단위로 교체가 가능하여 외부 보안 서비스를 응용 인터페이스로 제공할 수 있다. CORBA는 객체 중심 모델을 기반으로 미들웨어 형태의 보안 서비스를 제공하는 참조 모델을 제시한다.

CORBA 보안 서비스의 구조적 모델은 응용 요소, 보안 서비스 요소, 보안 기술 요소, 기본적인 보호 및 통신 요소 등 4개의 계층으로 구성된다.

● 응용 요소는 객체 호출 시 ORB에 의해 제공되는 보안 서비스에만 의존하며 어떤 응용들은 자체적인 보안 정책을 가지고 보안 서비스를 직접 호출한다.

● 보안 서비스 요소는 특정 보안 기술에 독립적인 ORB 보안 서비스, 관리 객체 등의 요소들로 구성된다. ORB 보안 서비스는 ORB Core를 기반으로 보안에 관련된 호출과 접근을 제어하는 ORB 서비스중의 하나

이다. ORB 보안서비스와 응용들은 인증, 접근, 제어, 감사, 부인 봉쇄 및 안전한 호출을 위해 보안 서비스 객체를 이용한다. 이들 보안서비스 객체는 보안 기술에 종속적인 처리를 위해 다시 외부 보안 서비스들을 호출하기도 한다. 보안 관리 객체는 호출 접근 정책, 호출 감사 정책, 안전 호출 정책, 호출 위임 정책, 응용 접근 정책, 응용 감사 정책, 부인 봉쇄 정책, 구성 정책들과 그 영역을 관리하는 영역 관리 객체를 선택한다. 새로운 객체가 생성되면 ORB는 적어도 1개 이상의 보안 영역과의 관계를 내부적으로 설정한다. 각 영역에는 여러 가지 유형의 정책 객체가 존재하며, 이들은 영역내의 모든 객체들에 의해 공유된다.

● 보안 기술 요소는 안전한 연계 설정을 위한 키 생성 및 관리와 데이터의 기밀성 또는 무결성을 위한 메시지 보호 알고리즘을 처리하는 계층으로서 구현 시 채택하는 보안 메커니즘이나 알고리즘에 종속적인 부분이다. 기본적인 보호 및 통신 요소에서의 보호 영역은 동일한 영역 내에 있는 객체간에는 상호 신뢰하고, 그 영역 내에서는 별도의 보안 서비스를 받지 않아도 안전한 상호 작용이 가능한 환경이 제공된다.

CORBA 보안 서비스는 암호화 알고리즘의 사용을 최소화하여 보안 관련 제어 데이터에 대해서만 암호화하며, 일반 데이터는 필요에 따라 선택적으로 암호화하도록 함으로써 특정 메커니즘이나 알고리즘에 중립적 특성으로 대규모 시스템 구성에 대한 범용성을 제공한다.[8][9]

3.2 CORBA 기반 이동에이전트 시스템

OMG에서는 새로운 패러다임인 이동에이전트 플랫폼간의 상호운용성 지원을 위해 CORBA를 기반으로 MASIF(mobile agent system interoperability facility)를 추가하였다. MASIF는 특정 플랫폼에 의존하지 않는 중립적인 구조를 지향하고 있으며, 시스템 차원에서 에이전트 상호 운용성을 제공하고자하는 목표를 가지고 있다. MASIF는 IIOP를 전송 프로토콜로 이용하고 있고, 기존의 CORBA 서비스의 개념을 대폭 수용하고 있다. CORBA 환경에서 이동에이전트는 주로 CORBA 객체로 구현되며, 코드와 수행상태를 ORB를 통해 이동시킨다. MASIF와 CORBA의 관계는 그림 2와 같다. MASIF는 이동에이전트 시스템들간의 상호연동을 위해 MAFAgentSystem 인터페이스와 MAFFinder 인터페이스를 정의하고 있다. 전자는 에이전트 수신, 생성, 중지, 종료 등과 같은 에이전트 관리를 위한 기본적인 인터페이스를 정의하며, 후자는 에이전트의 등록, 등록 해제, 위치 확인 등과 같은 명명(Naming) 서비스를 위한 인터페이스를 제공한다.[10][11][12]

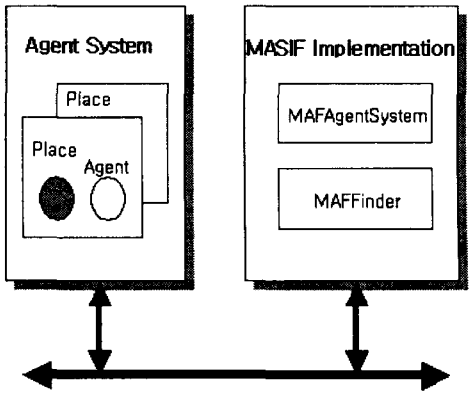

그림 2. MASIF와 CORBA의 관계

IV. 에이전트 보안 모델

이동에이전트에 관련된 보안 위협에 대응하기 위해 제안하는 보안 기능을 갖는 이동에이전트 시스템은 Agent Name Manager Server, Agent Server, Security Manager Server, Mobile Agent로 구성되며, 일정 영역 외부의 보안 관리를 담당하는 도메인 보안 서비스 DSS(Domain Security Server)와 통신할 수 있는 기능을 가진다. 제안한 시스템의 구성은 그림 3과 같다.

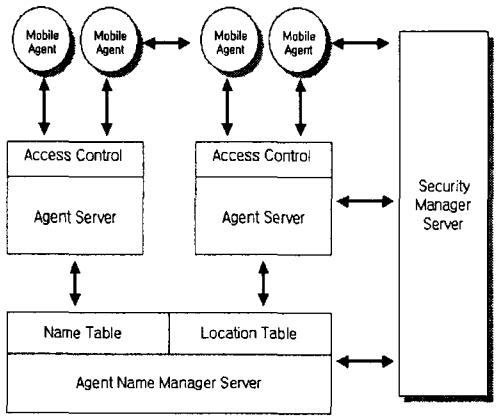

그림 3. 이동에이전트 보안 모델

이 시스템의 동작은 다음과 같다.

1) 인증:

인증 서비스는 에이전트 서버에 의한 이동에이전트 사용자 인증과 이동에이전트에 의한 이동에이전트 수행 환경 또는 에이전트 서버의 인증으로 나누어 수행

된다. 에이전트 시스템은 인증 서비스를 지원하기 위하여 에이전트가 생성될 때, 에이전트의 식별자, 작업을 의뢰한 사용자, 에이전트를 생성한 시스템의 식별자, IP를 이동에이전트에 부여하고 SMS(Security Manager Server)로 전송하여 저장한다. 식별자는 시스템 내부에서 중복되지 않게 부여된다. 이 정보들은 외부의 도메인 보안 서버의 요청에 의하여 외부 영역의 에이전트 인증이나 외부 서버의 인증에 사용된다.

- 에이전트 서버에 의한 이동에이전트 사용자 인증

이동에이전트가 에이전트 서버에 수신될 때 SMS는 에이전트가 보유하고 있는 에이전트 식별자, 사용자, 에이전트를 생성한 시스템 식별자를 검증하여 에이전트의 인증과정을 수행한다. 이동에이전트가 외부의 도메인 서버 식별자를 가질 경우, SMS는 DSS 서버를 통하여 인증 과정을 거치게 된다.

- 이동에이전트에 의한 에이전트 수행환경과 서버의 인증

이동에이전트의 서버에 대한 인증과정은 해당 서버의 악성여부를 판단하기 위해서 필요하다. 에이전트 서버의 인증과정은 다음과 같다.

에이전트 이동시 에이전트 서버는 수신 측 에이전트 서버의 신뢰성 여부를 SMS에게 요청하면 SMS는 해당 서버의 식별자 인증과정을 거친 후, 에이전트 서버로 결과를 전송하고, 에이전트 서버는 에이전트를 해당 서버로 전송한다.

2) 권한 검사:

SMS는 보안 요구사항을 처리하기 위해 데이터와 응용 프로그램의 권한을 영역별, 등급별로 저장하고, 필요시에 에이전트 서버가 요구하는 권한을 검사한다. 권한 등급은 그룹과 계층의 수평적, 수직적 구조를 가지며, 에이전트 서버의 위치 정보와 역할, 응용 프로그램에 관한 정보에 기초하여 분류되어 저장된다.

3) 접근 통제:

에이전트 서버는 이동에이전트 수행에 필요한 자원을 할당하기 위하여 이동에이전트를 수신하기 전에 에이전트의 식별자, 작업을 의뢰한 사용자, 에이전트를 생성한 시스템의 식별자를 요구하여 에이전트의 권한을 검사한다. 이동에이전트의 수행이 시작되면, 에이전트 서버는 접근 통제 메커니즘을 행하여 에이전트의 상태를 불법적으로 변경하지 못하도록 한다.

V. 결론 및 향후 연구 과제

이동에이전트 기술은 분산시스템 환경에 있어서 적합한 개선안으로 믿어지고 있으며 분산환경을 위한 여러 가지 이동에이전트 시스템들이 개발되어지고 있다.

이에 따라서, CORBA를 제안한 OMG(Object Management Group)에서는 새로운 패러다임인 이동에이전트 플랫폼간의 상호운용성 지원을 위해 CORBA를 기반으로 하는 MASIF(Mobile Agent System Interoperability)를 추가하였다. MASIF는 특정 플랫폼에 의존하지 않는 중립적인 구조를 지향하고 있으며, 시스템 차원에서 에이전트 상호 운용성을 제공하고자하는 목표를 가지고 있다.

분산객체시스템의 표준인 CORBA와 분산시스템 환경에 적합한 개선 안으로 믿어지고 있는 이동에이전트와의 통합은 분산시스템에서 일어나고 있는 여러 가지 문제점들을 효율적으로 개선시킬 수 있다. 그러나, 대단위 분산객체 기술과의 결합은 이동에이전트 시스템을 확장시키고, 다른 에이전트 플랫폼과의 호환성을 보장하지만 그에 대한 역효과로 여러 가지 보안상의 문제점들을 나타나고 있다.

본 논문에서 제안한 시스템은 기존의 이동에이전트 시스템과는 달리 이동에이전트 표준인 MASIF를 기반으로 하기 때문에 분산 이동 컴퓨팅 환경에 적용이 가능하다. 또한, MASIF에서 제시한 보안 요구들을 CORBA 보안서비스 명세를 이용하여 구현함으로써 다른 에이전트 플랫폼과의 호환성을 보장할 수 있도록 하여 추후 전자상거래를 비롯한 다양한 인터넷 서비스들의 대규모 개방형 분산시스템으로의 확장이 가능할 것이다.

제안한 모델에서는 각 이동에이전트나 에이전트 시스템, DSS 서버간의 통신 부하를 줄이는 방법은 고려되지 않았기 때문에 통신 부하를 줄이는 기법의 연구와 자료 전송시에 자료의 무결성을 보장할 수 있는 암호화 기법에 대한 연구가 필요하다.

참고문헌

[1] Kassab, Lora L. Voas, Jeffrey. "Agent Trustworthiness, in: Proceedings of the ECOOP Workshop on Distributed Object Security and 4th Workshop on Mobile Object Systems: Secure Internet Mobile Computations: pp. 121-133, INRIA, France, 1998.

[2] Gray, Robert. "Mobile Agent Security in: Proceedings of the ECOOP Workshop on

Distributed Object Security and 4th Workshop on Mobile Object Systems: Secure Internet Mobile Computations, pp. 79-80, INRIA, France, 1998.

[3] Joint submission OMG TC Doc. "Mobile Agent System Interoperability Facility Specification" Nov.1997

[4] OMG, Mobile Agent System Interoperability Facilities Specification, November, 1997.

[5] OMG, CORBA Service: Common Object Services Specification, 1998.

[6] M. Wooldridge and N.R jennings. "Intelligent Agent: Theory and practice. The Knowledge Engineering Review" 10(2) pp. 115-152, 1995

[7] J. E. White "Telescript Technology : Mobile Agent General Magic White paper, White paper, 1996.

[8] Hohl, Fritz. "A Model of Attacks of Malicious Hosts Against Mobile Agents, in : Proceedings of the ECOOP Workshop on Distributed Object Security and 4th Workshop on Mobile Object Systems: Secure Internet Mobile Computations:, pp. 105-120, INRIA, France, 1998

[9] W. M. Farmer, J. D. Guttman, and V. Swarup, "Security for Mobile Agents: Issues and Requirements", 19th National Information Systems Security Conference (NISSC 96), 1996.

[10] William Stallings, "Cryptography and Network Security: Principles and Practice:, 2nd Edition, 1998.

[11] Edward G. Amoroso, Fundamentals of Computer Secutity Technology, AT&T Bell Laboratories. 1994.

[12] Alper Gaglyan, Colin Harrison, "Agent Source Book", John Wiley & Sons, 1997.