액티브 네트워크 기술동향☆

이 원 구* 최 병 선* 이 성 현* 이 재 광**

◈ 목 차 ◈

1. 서 론

현재 인터넷을 이용하는 사용자의 수가 급격하게 증가하고, 이에 따른 네트워크에 대한 요구 또한 점차적으로 복잡해지고 있으며, 이러한 요구에 부응하고, 환경 변화에 대응하기 위한 여러 기술들에 대한 연구가 진행되고 있다. 하지만, 대부분의 연구 초점은 사용자 폭증에 따른 하부구조, 전달기술, QoS 지원기술, 주소문제 등 손쉽게 네트워크 서비스사용과 인터넷 자원 및 서비스의 효율성을 지원하기 위한 관리기능을 제공하여 인터넷 망의 광역화 및 고속화 목표를 갖고 차세대 인터넷을 구축하고자 하는데 있다.

그러나 근본적으로 차세대 인터넷 기술은 기존의 인터넷 인프라에 기반한 기술로서, 현재의 인터넷 인프라가 새로운 응용 서비스들을 신속하게 제공하거나 새로운 기능을 추가하기에는 적절하지 못하며, 사용자의 서비스 품질 요구수준의 기대치에 크게 미치지 못하고 있는 실정에 있기 때문에 차세대 인터넷 기술의 적용에 따른 한계성이 대두되고 있다. 따라서 차세대 네트워크를 구축하기 위해서는 네트워크의 성능을 저하시키지 않고 새로운 서비스를 도입하는데 용이하고, 서비스 및 네트워크의 품질 개선을 위해 네트워크의 제어와 관리를 동적으로 수행할 수 있는 새로운 네트워크 기술에 관한 접근과 연구가 요구되며, 이에 기존 네트워크의 근본적인 문제점과 한계점을 극복하기 위하여 새로운 대안으로 나타난 것이 액티브 네트워크이다.

따라서 본고에서는 현재 인터넷이 지닌 한계점을 해결하기 위한 액티브 네트워크의 최신기술에 대해 기존에 논의된 연구를 관리, 보안, 응용 및 미들웨어 관점으로 분류하여 기술하고 향후 전망을 제시한다.

* 한남대학교 공과대학 정보통신 · 멀티미디어공학부 컴퓨터공학전공 박사과정
** 한남대학교 공과대학 정보통신 · 멀티미디어공학부 컴퓨터공학전공 교수
☆ 본 연구는 산업자원부의 지역혁신 인력양성사업의 연구결과로 수행되었음.

2. 액티브 네트워크 관리

2.1 기존의 액티브 네트워크 관리동향

기존의 액티브 네트워크 관련 연구들은 액티브 네트워크의 구조를 정의하고 자신들이 정의한 구조 내에서 효율적인 액티브 네트워크 관리를 구현하기 위한 시스템 개념 정의 및 구축에 초점을 맞추고 있다.

이러한 액티브 네트워크를 관리 목적으로 하는 기존의 연구들은 네트워크 관리의 5가지 기본 목표인 장애, 구성, 계정, 성능, 보안, 관리들 중에서 지능적인 특성이 요구되는 구성, 장애, 성능, 보안, 과금 관리에 아래의 (표 1)과 같이 초점을 두고 있다.

그렇지만, 현재 액티브 네트워크 관리는 대부분 액티브 네트워크 기술을 이용한 기존의 망 관리에 초점

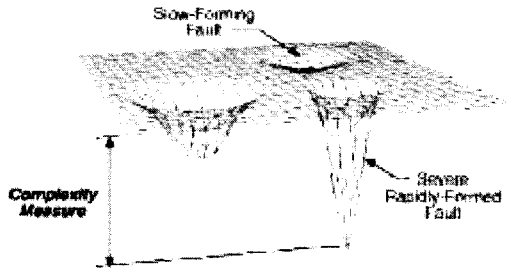
(표 1) 액티브 네트워크 관리 연구 현황[23]

분류	정의	연구동향
구성 관리	매니저의 개입 없이 액티브 노드의 구성을 자체적으로 설정할 수 있는 것으로 자가구성(self-configuration) 또는 자동구성 방식 등의 방향으로 연구가 진행 중임	ANCORS, FAIN, NETSTOR 등등
장애 관리	결함이 노드내에 탐지되면 그결함을 분석하여 원인을 파악하고 자동으로 복구하는 방식으로 연구가 진행 중임	AVNMP, FAIN, NESTOR 등등
성능 관리	네트워킹 성능을 향상시키고 자원을 효율적으로 관리하는 방식으로 연구가 진행 중임	AVNMP, FAIN 등등
보안 관리	자원의 접근 통제를 통해 제공하는 방향으로 연구가 진행 중임	ABLE,FAIN, PANTS, SENCOMM 등등

이 맞추어져 있고, FAIN에서만 액티브 네트워크 자체에 대한 관리를 언급하고 있다. 그리고 노드 내의 자동구성 및 복구, 자원의 접근제어 및 관리에 대한 연구는 있으나, 네트워크에서의 트래픽을 제어하고 성능을 향상시키는 부분에 대한 연구는 미흡한 실정이다. 게다가 향후 몇 년간 인터넷은 기존 네트워크와의 공존이 불가피하고, 표준화된 형태가 없기 때문에 다양한 액티브 네트워크가 함께 존재하게 된다. 그러므로 기존 네트워크 관리와의 연동 및 다른 액티브 네트워크 관리와의 연동문제가 대두되고 있다[23].

2.2 최근의 액티브 네트워크 관리동향

액티브 네트워크 관리 시스템의 경우 네트워크 관리기능의 분산화와 네트워크의 유연성이라는 액티브 네트워크의 장점을 십분 활용하기 위해 대개의 ANMS(Active Network Management System) 관련 프로젝트들은 장애관리와 성능관리 측면에서 네트워크 관리를 개선하는데 그 초점을 맞추고 있다. 이에 발맞추어 최근의 액티브 네트워크 관리와 관련된 연구는 네트워크 상에서 발생하는 트래픽을 모니터링하고 제어하여 오류가 발생 시 네트워크를 효율적으로 관리할 수 있도록 하는 쪽으로 방향이 잡혀가고 있다. 그 일



(그림 1) 복잡도-기반 관점에서의 네트워크 모니터링

례로서 본 절에서는 클러스터링(clustering)을 이용하여 네트워크의 오류 상황을 모니터링(monitoring)하는 기법과 액티브 모니터링을 이용하여 네트워크 모니터링을 수행하는 기법에 대해서 소개한다.

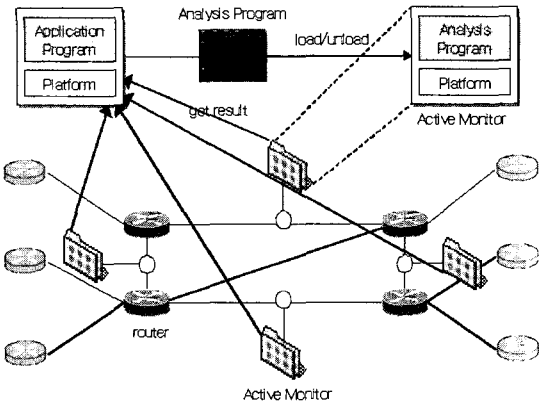
2.2.1 클러스터링을 이용한 트래픽 모니터링 기법

네트워크상의 한 노드에서 오류가 발생했을 경우, 그 노드와 연결된 노드들은 데이터 전송에 어려움을 겪게 된다. 이 경우 오류가 생긴 노드를 중심으로 네트워크에 문제가 발생하는 영역이 급격히 넓어져가게 된다.

(그림 1)은 클러스터링을 이용한 네트워크 오류 모니터링을 보여준다. 이 기법에서는 오류가 발생한 지역을 클러스터링 하여, 클러스터링의 크기가 정해진 기준을 초과하면 그 클러스터링은 네트워크상에서 문제가 있거나 문제를 일으킬 소지가 있다고 판단하여 네트워크 오류 관리를 해주게 된다. (그림 1)에서 아래로 깊게 패인 부분이 바로 네트워크상에서 오류관리를 해줘야 할 트래픽 발생 영역이다. 이때 액티브 네트워크의 장점을 이용하여 중앙에까지 이러한 정보를 전달해서 중앙의 처리를 기다릴 필요 없이, 장애가 발생한 노드가 바로 오류 처리를 해주는 작업이 가능하며, 이러한 네트워크 관리 방법을 이용하면 네트워크에서 심각한 문제를 일으킬 수 있는 트래픽이 발생하기 이전에 네트워크 자체에서 이런 상황을 모니터링 하여 처리해주는 일이 가능하게 된다[1,20].

2.2.2 액티브 모니터를 이용한 트래픽 모니터링 기법

기존의 네트워크 관리시스템은 중앙의 매니저에게



(그림 2) 액티브 모니터 네트워크

모든 관리 권한이 부여된 중앙 집중적인 구조이기 때문에 새로운 네트워크 모니터링을 적용하거나 네트워크 오류에 즉각적인 반응을 보이기가 매우 힘들었다. 이를 개선하기 위해 액티브 모니터 네트워크는 프로그래밍 가능한 트래픽 모니터(traffic monitor)와 매니저(manager)를 네트워크상에 가지고 있으며, 동적으로 네트워크 분석 프로그램을 로딩 할 수 있으므로 네트워크 모니터링을 유연하게 처리할 수 있게 된다. (그림 2)는 액티브 모니터가 포함된 액티브 모니터 네트워크를 나타낸다.

네트워크 분석 프로그램을 포함하고 실행시키는 액티브 모니터는 모니터링 된 애플리케이션 프로그램(application program)을 실행시키고 액티브 모니터를 제어하는 매니저와 통신을 주고받으며 액티브 네트워크 트래픽을 모니터링하고 제어하게 된다[2,20].

3. 액티브 네트워크 보안

3.1 기존의 액티브 네트워크 보안동향

액티브 네트워크가 지닌 보안상의 문제점들을 해결할 수 있어야만 기존 망과의 연동 또는 자체 네트워크로 생존할 수 있을 것이다. 따라서 효율적이고 신뢰할 수 있는 형태의 액티브 네트워크에 대한 연구가 지속적으로 요구된다. 더불어 액티브 네트워크 자체의 보안성 확보에 대한 연구뿐만 아니라 액티브 기술을 이용한 네트워크 보안에 대한 연구도 요구되며, 현재의 보안기술에 대한 동향분석을 통해 향후에 나아갈 방향을 제시한다[23].

3.1.1 IDIP

IDIP(Intrusion Detection and Isolation Protocol)는 침입자의 근원과 네트워크 기반 공격의 대응에 있어 네트워크 접근 수준 제한 정책을 동적으로 변화하게 한다. IDIP의 시스템 보안 정책 프로그램은 네트워크 기반 공격인 바이러스에 최선으로 대응하기 위한 메커니즘을 발전시키기 위해서 본래의 개념을 확장했다. 또한, 대응 메커니즘은 변화하는 위협 환경에 맞추어 동적으로 적응한다. 침입 프로그램에 대한 자동 대응은 다양한 접근 제어 통제와 침입 탐지, 그리고 침입 대응 시스템으로 네트워크 관리 구성요소들을 통합함으로써 본래의 개념을 향상시켰다. IDIP는 응용계층과 메시지계층으로 구성되며 이 계층은 OSI 프로토콜 계층 모델을 기반으로 구성되어 있다.

현재 IDIP 프로젝트는 그 수행 결과를 발전시켜 네트워크 보안에서의 각종 보안 정책을 추가한 CITRA (Cooperative Intrusion Traceback and Response Architecture)의 프로젝트로 발전해가고 있으며, 또한 프로토콜로 구현될 경우에 발생하는 기능 변경의 정적인 단점을 보완하여 보안 프레임워크 상에 유연성을 부여하기 위해 IDIP와 CITRA의 아이디어와 개념을 액티브 네트워크 플랫폼 상에서 구현하는 것을 목적으로 하는 AN-IDR 프로젝트가 수행 중에 있다. AN-IDR의 경우 단순히 공격자의 추적 및 고립화뿐만 아니라, 액티브 패킷을 이용하여 공격용 툴로써 설치된 에이전트 프로그램을 스캐닝하고 해당 에이전트의 실행을 중지시키는 것과 같이 침해된 시스템을 복구하는 기능도 포함하여 개발하고 있는 상태이다[19].

3.1.2 AN-IDR

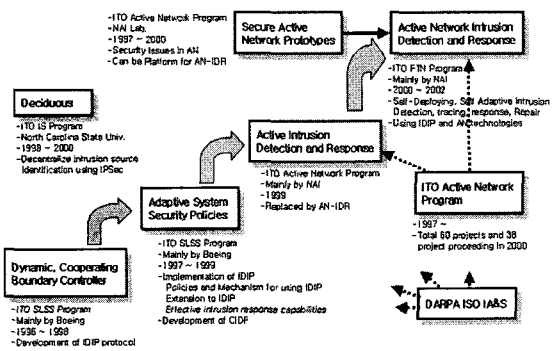
AN-IDR(Active Network Intrusion Detection and Response)은 IDIP가 정적인 특성으로 인한 유연성의 부족함과 특정 기능 수행 상에 있어서의 효율성 저하를 해결하기 위해 시작되었다. 이를 위해 IDIP 메커니즘과 액티브 네트워크 기술을 결합하여 상호 운용함으로써 기존의 정적인 IDIP에 이동성, 유연성, 확장성을

부여함으로써 좀더 발전된 침입자 참지 추적 기능을 수행하고자 하는 것이다. 따라서 침입자를 탐지 및 추적하여 공격자와 인접한 네트워크 노드에서 공격자의 네트워크에 대한 연결성을 단절함으로써 공격자에 대해 보다 강력한 대응을 하기 위한 목적으로 수행하고 있다.

다음 (그림 3)은 DARPA 내에서 AN-IDR과 관련한 프로젝트들을 보여준다. "Deciduous" 프로젝트는 AN-IDR과는 상관없지만 침입자를 탐지, 추적하기 위해 IP-Sec을 적용하는 방안을 연구 중인 프로젝트이다[1,22].

AN-IDR의 출발점은 1996년부터 시작된 "Dynamic, Cooperating Boundary Controller" 프로젝트이다. 이 프로젝트는 IDIP 프로토콜의 개발을 목적으로 시작되었으며, "Adaptive System Security Policies" 프로젝트로 이어져 IDIP 개발을 수행되었다. 이후 IDIP가 지니는 정적인 특성을 극복하기 위해 1999년에 NAI LAb과 Boeing사를 주축으로 하여 DARPA ITO 산하의 Active Network 프로그램 아래에서 수행되던 것이 FTN(Fault Tolerant Network) 프로그램으로 옮겨져서 2002년까지 기한으로 진행되었으며, 단독으로 수행되기보다는 Active Network 프로그램의 많은 프로젝트들의 결과를 이용하고 있다.

AN-IDR은 자체 프로젝트뿐만 아니라 DARPA에서 수행되는 "Active Network" 프로그램 프로젝트들의 결과를 많이 이용하고 있으며, 특히 NAI Lab.에서 수행하는 "Secure Active Network Prototype" 프로젝트의 결과는 AN-IDR의 기반 플랫폼으로 사용될 예정이다[19].



(그림 3) AN-IDR 개발현황

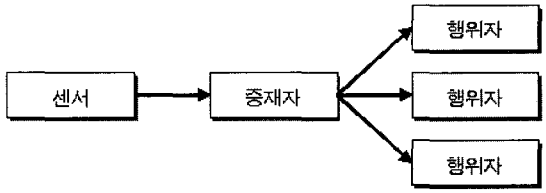
3.2 최근의 액티브 네트워크 보안동향

현재 많은 정보보안 업체에서 보안 문제를 해결하기 위해 침입차단시스템(firewall), 필터링 라우터(filtering router), 보호 장비(guards) 등과 같은 다양한 보안 장비들을 선보이고 있지만, 이들 장비들은 모두가 지엽적인 침입탐지와 이에 대한 개별적인 대응을 수행하고 있다. 설사 시스템 전반적인 협력을 통해 침입을 감지하고 대응하는 구조를 갖추려 해도 원격적인 공격자 차단 기능을 구현할 만한 표준 모델이 존재하지 않고 있다. 따라서 현재의 시스템적 대응 한계를 극복하기 위해 서로 다른 네트워크 시스템 간에 공격자 탐지 정보를 공유하고, 이를 통해 모든 시스템 환경에서 일정한 대응을 유도해내기 위한 인프라 구축과 관련된 많은 연구가 진행되고 있다[22].

3.2.1 NAI의 ActiveSecurity

NAI의 ActiveSecurity는 이동형 센서를 이용하여 신속하고 효율적인 대응을 제공하는 각 보안 장비간의 통합된 보안 솔루션(solution)이다. (그림 4)는 ActiveSecurity의 구성 요소들 간의 관계를 나타낸 것으로서, 센서는 네트워크 장치들을 감시하고 의심스러운 행위가 감지되면 중재자에게 보고한다. 중재자(arbitrator)는 센서로부터 받은 정보를 바탕으로 최적의 대응방안을 결정하고 행위자에게 취해야 할 대응방법을 전달한다. 행위자(behavior)는 중재자로부터 받은 대응을 대응 노드(corresponding node)에 행하는 역할을 가지고 있다. 위의 모든 동작은 보안 정책을 기반으로 이루어지고, 이 정책들도 상황에 맞게 동적으로 변화할 수 있다.

각 구성요소는 Gauntlet Firewall, Cyber Cop Scanner, Orchestrator 등이 있다. 여기서 중재자에 해당되는



(그림 4) NAI의 ActiveSecurity 구조

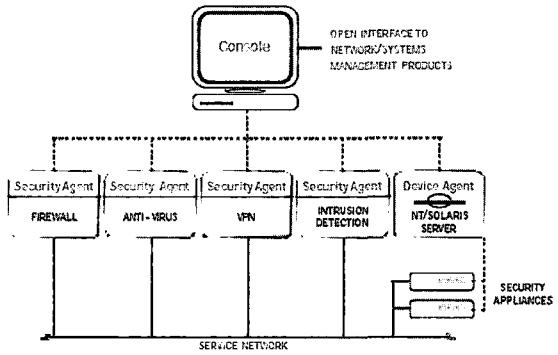
Event Orchestrator는 NAI 제품뿐만 아니라 다른 보안 제품들을 위한 이벤트 관리로써 네트워크 내의 보안 센서로부터 발생되는 이벤트를 중재하고 보안 정책을 관리하며, 이를 바탕으로 최적의 대응방안을 결정하여 행위자가 취해야 할 대응 방법을 결정한다.

NAI의 ActiveSecurity는 보안 환경에 유연하고 신속한 적응성을 지니는 보안 시스템 및 환경을 제공하는 것을 목적으로 하고 있으며, 모듈 접근방식을 토대로 구현되었기 때문에 자신이 필요로 하는 제품을 쉽게 통합할 수 있다[3,22].

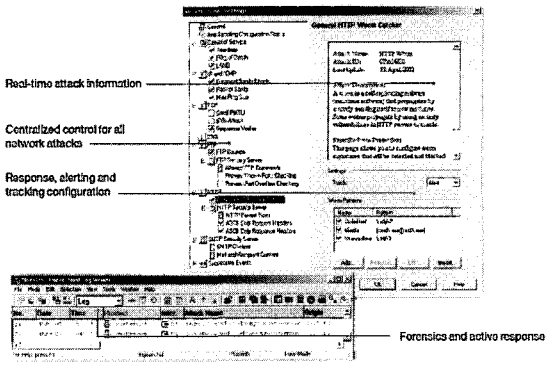
3.2.2 OpenService's SystemWatch

OpenService사의 SystemWatchsms 보안장비 및 응용으로부터 발생하는 이벤트를 분석하고 상호연동을 통해 시스템과 개인이 취해야 할 적절한 대응방법을 결정하며, 벤더(vendors)들의 보안 장비와 응용을 통합하여 하나의 콘솔로 관리함으로써 자동화된 보안 관리 솔루션을 제공한다. 또한 표준플랫폼을 사용함으로써 우연성을 제공하며, 보안 장비의 증가와 기업 조직 변화를 만족시키기 위한 적응성을 갖는다. 중요한 보안 응용프로그램과 제품들을 자동 관리하기 위한목적으로 다른 벤더들의 보안 제품들에게 공개 인터페이스를 제공한다.

(그림 5)는 SystemWatch 구조를 나타내는 것으로, SystemWatch Security Agent는 각 보안 장비에 상주하여 각 장비로부터의 데이터 및 상태 정보를 수집/분석하고, 보안 애플리케이션의 감시 및 관리를 수행한다. 각 에이전트로부터 실시간으로 수집된 이 정보는 SystemWatch의 상위 콘솔(Open Management Console, OMC)로 전달되고, OMC는 이를 웹 환경으로 보여준다. 이러한 계층적인 SystemWatch의 구조는 모든 보안 장비들이 하나의 콘솔로 통합관리를 가능하게 한다[4,22].



(그림 5) OpenService의 SystemWatc



(그림 6) CheckPoint의 SmartDefens

3.2.3 CheckPoint's SmartDefense

CheckPoint사는 차세대 보안 관리 솔루션으로 2002년 3분기에 능동형 보안 관리 시스템 부류의 첫 출시 솔루션으로 SmartDefense를 선보이기 시작하였으며, 주요 특징으로는 (그림 6)과 같다.

SmartDefense는 현재 알려진 모든 공격을 비롯하여 알려지지 않은 공격에 대해서도 침입에 대한 유형적인 구분에 따라 지능적인 보안 기술을 이용하여 대응한다. 탐지/차단/감사/경보에 대한 실시간 정보를 하나의 콘솔로 제공함으로써 중앙 집중적인 보안 관리 환경을 제공하며, DoS, IP 공격, 네트워크 프로빙, 웹과 응용들의 취약점 등을 포함한 공격 유형에 대처하고, 완전한 네트워크 방어를 위해 추가적으로 경보, 추적 감사 기능을 중앙에서 설정한다. 또한 새로운 공격 유형에 대한 보안 서비스를 온라인으로 업데이트하여 보안 관리 시스템의 확장성을 제공하며, 공격 방식에 대한 세부적인 설명과 특징을 포함한 인터페이스를 제공하며 보안매니저에게 네트워크 공격에 대한 이해와 적절한 대응 방법을 알려준다.

이는 기존의 장비간의 상호연동을 고려한 통합보다는 새로운 기술이나 기능 요구 변화와 보안 시장의 확장에 따라 더불어 진화하는 형태로의 발전을 기본으로 하고 있다[5,22].

4. 액티브 네트워크 응용

4.1 에이전트 기반 기술

많은 액티브 네트워크 구조들은 현재 코드 이동성 패러다임을 사용한다. 이동 코드 기술은 캡슐화, 전송, 안정성, 효율적인 실행 그리고 프로그램의 중재를 지원하다. 액티브 네트워크 기술과 이동 코드의 기술은 최근 네트워크 통제와 관리 시스템을 향상시킬 뿐만 아니라 분산 응용까지 현저하게 향상시킨다. 더욱이 고정된 기능과 프로토콜 엔진은 이동 에이전트를 통하여 기본 스테이션(station)과 종단 시스템, 라우터와 스위치에서 동적으로 개발된다. 또한, 액티브 네트워크의 전개와 유지, 서비스의 주문화, 그리고 프로토콜 캡슐화에 있어 코드의 이동성 적용은 더욱 더 적절하다. 이동 코드 기술은 이동 소프트웨어 에이전트 기술과 매우 밀접하다. 코드 이동성 패러다임은 이동 소프트웨어 에이전트 기술을 수행한다. 그러나 두 기술의 기본적인 차이로서, 액티브 네트워크 기술은 통신을 편리하게 하는 유연성을 제공하며 주문하는 네트워크를 동적으로 재구성하는 네트워크 계층 처리의 개념을 사용하며, 이동에이전트 기술은 다중 에이전트를 이용하여 사용자와의 친숙한 환경과 사용자의 구체적인 작업을 수행하기 위해 장소에서 장소로 이주하는 프로그램의 개체로서 응용계층에서 응용 프로그램으로서 실행이 가능하다. 잠재적으로 네트워크로부터 궁극적으로는 유비쿼터스(ubiquitous) 컴퓨팅 환경의 조성까지 일반적인 이동에이전트 기술은 에이전트 이주 컴퓨터작업(computation)을 지원하도록 설계되었다. 액티브 네트워크의 기본적인 기능이 이동 소프트웨어 에이전트의 응용으로 지원 가능하다. 이동 에이전트를 캡슐(액티브 패킷)의 특정형태처럼 볼 수 있기 때문이다.

국내에서는 이러한 에이전트 기반 기술을 이용하여 한국전자통신연구원(ETRI)에서 액티브 보안 관리 기술, 이동형 센서 기술 그리고 사이버 공격 역추적 기술을 이용하여 Esmart(ETRI Security Mechanism using Active Response Technology) 시스템을 개발하였다. Esmart 프레임워크는 다양한 유형의 사이버공격에 대한 신속한 대응 및 피해 국지화가 가능한 액티브 감지형 네트워크 보안 엔진 및 이동형 센서로 구성되어 있으며, DDoS 등과 같은 우회 루트 공격을 감행하는 사이버 테러 공격자의 위치 역추적을 통한 공격자의 근접점에서 공격적으로 대응이 가능하다. Esmart 시스템은 서비스 계층, 엔진 계층 그리고 NodeOS 계층으로 계층적으로 구조화되어 있다[6,21].

4.2 액티브 무선기술

현재의 무선 네트워크는 신속한 핸드오버와 네트워크 토폴로지(topology)의 변화에 빠르게 적응하는 라우팅에 대한 어려움을 가지고 있다. 이러한 문제점을 액티브 기능을 이용함으로써 이동 네트워크에서 신속한 핸드오버(hand-over)가 가능하게 하며, 애드 혹(ad hoc) 네트워크에서 적응적인 라우팅이 가능하도록 한다.

이동 네트워크에서 이동 노드의 신속한 핸드오프(hand-off)를 지원하기 위해, 액티브 라우터는 홈 에이전트와 대응 노드로 가는 바인딩 갱신 메시지를 직접 처리하는 방식을 제안하며, 대표적인 연구로서 ADS (Active Delivery System)가 있다.

또한, 기지국이 존재하지 않는 동적인 ad hoc 네트워크에서 적응적인 라우팅을 지원하는 연구로는 ACIP (Active Cellular IP)가 있다. ACIP에서는 이동 노드가 MST(Minimum Spanning Tree)를 사용하여 자신의 위치를 알게 하고, 이를 위해 이동 노드는 이웃 발견 기능과 MST를 구축하는 액티브 기능을 탑재하고 있다[23].

4.3 멀티미디어 기술

대용량 및 다양한 종류의 멀티미디어 브로드캐스팅은 현재의 인터넷상에서 심각한 대역폭 및 컴퓨팅 자원을 요구한다. 현실적으로 대용량의 VBR(Variable Bit Rate) 멀티미디어 데이터 전송을 위한 대역폭 보장은 네트워크상에서 거의 불가능하므로, 전송 프로세스는 실제 가용한네트워크 대역폭에 실시간 적응이 가능하도록 구성하는 것이 필수조건이 될 것이며, 이때 허용 기준치 내의 품질을 유지하면서 멀티미디어 전송 및 트랜스코딩(transcoding)이 보다 효율적으로 이루어지

도록 지원하는 액티브 네트워크 기술이문제점 해결의 한 방안이 될 수 있다.

일반적으로 멀티미디어 전송 및 트랜스코딩을 효율적으로 하기 위한 액티브 라우터들은 전체 네트워크의 핵심적인 부분에 위치하며, 이들 라우터는 등록된 멀티미디어 서비스 제공자에게만 접근 허용이 가능하게 한다. 이러한 액티브 라우터는 효율적이면서도 안전하게 멀티미디어 브로드캐스팅(broadcasting)을 수행하는 적응 프로토콜을 다운로드 받아서 각 멀티미디어 스트림의 세그먼트에 기반한 적응적 품질 제어 및 트랜스코딩이 가능하게 한다.

실제 적응 기법은 MPEG/JPEG와 같은 비디오압축 기법에 맞추어 프레임별 종속성을 고려하거나 가용 자원 상태를 고려하여 Q-factor, 해상도, 전송 속도 등을 조절하도록 함으로써 각 액티브 라우터에서 실시간으로 지역적인 결정을 내려 처리하도록 구현하였다. 이들 적응 프로토콜을 액티브 라우터에 구현하기 위해서 PLAN이나 PLAN-P와 같은 언어를 구현하거나 커널레벨에서 C언어로 능동 네트워크 구조를 위한 서비스 모듈을 구현하였다. 또한, 비디오 트랜스코딩이나 패킷 드롭을 위해 적절한 휴리스틱(heuristic) 알고리즘을 사용하고 해시 테이블(hashing table)을 사용하여 프레임 타입 및 프레임 번호 등을 저장하여 두었다가 현재 가용 자원 상태를 고려한 적응 기법의 정보로 사용할 수 있다[7,23].

5. 액티브 네트워크 미들웨어

액티브 네트워크상에서 동작하는 프로그램을 작성하는 것 자체는 그다지 어려운 일이 아니지만, 많은 네트워크 사용자들이 범용적으로 사용할 수 있도록 상호 호환되면서, 안전한 프로그램을 작성한다는 것은 결코 쉬운 일이 아니다. 즉, 네트워크상에서는 예측불허의 상황들이 일어날 가능성이 항상 존재하기 때문에 이에 대한 처리가 미리 준비되어 있어야만 액티브 네트워크상에 적합한 프로그램이라 할 수 있으며, 이를 액티브 네트워크상에 적용 가능한 미들웨어라 말할 수 있다. 즉, 액티브 네트워크상에 적용 가능한 미들웨어는 애플리케이션의 기반을 제공하는 것으로 미들웨어 상에서 작성된 프로그램은 보다 쉽고 효과적으로 통신할 수 있는 기능을 갖게 되며, 관리 및 감시도 훨씬 수월하게 한다.

이러한 미들웨어는 그 구조에 따라 여러 가지로 분류될 수 있으며, 대표적인 형태로는 메시지 기반 미들웨어, RPC 기반 미들웨어, 객체 기반 미들웨어인 CORBA와 OLE/COM, 자바 RMI 기반의 미들웨어 등이 있다. 이들 기술에 따라 실제 제공되는 미들웨어 서비스의 내용이나 프로그래밍 언어와 플랫폼의 지원 등에 다소 차이가 있으며, 결론부터 말하자면 다른 유형의 미들웨어 기술이나 제품들 사이의 호환성은 아직 해결해야 할 향후 연구 분야이다. 본고에서는 응용적 미들웨어 부분만을 기술한다.

5.1 기존의 네트워크 미들웨어 동향

5.1.1 DB 미들웨어

DB 미들웨어는 애플리케이션과 데이터베이스(DB, DataBase) 간에 통신을 원활하게 하는 것을 목적으로 하는 미들웨어로, 다양한 형태로 구축된 데이터베이스 간의 통신이 가능하도록 해주는 제품을 말한다. DB 미들웨어는 다른 미들웨어와는 달리 2계층 클라이언트-서버(CS, Client-Server) 구조에서 사용된다는 특징을 지니고 있다. 따라서 업체들은 DB 미들웨어를 도입함으로써 하드웨어, 데이터베이스, 네트워크 프로토콜로 이루어진 복합 시스템 환경에서 생성된 다양한 DB를 클라이언트에서 보다 쉽게 조작 및 운영할 수 있게 된다. 일반적으로 프로그램 사용자가 100명 이하, 그리고 서버의 수가 1개 혹은 2개인 경우에 많이 사용되며, 대표적인 제품으로는 오라클 SQL 넷 등을 들 수 있다. DB 미들웨어의 경우 DB 업체마다 전용 기술을 채택하고 있어 호환 문제가 발생하는데 이를 해결하기 위해 나온 표준 기술이 개방형 DB 연결(ODBC)이다. DB 미들웨어는 2계층 CS 프로그램의 주류를 차지했지만, 최근 들어 컴퓨팅 환경이 3계층 구조로 전환됨에 따라 점차 밀려나는 추세에 있다[24].

5.1.2 트랜잭션 처리 모니터

트랜잭션 처리(TP, Transaction Processing) 모니터는

통신부하 양이 많은 클라이언트와 서버 사이에 위치하여 서버 애플리케이션 및 자원을 효율적으로 관리할 뿐만 아니라 통신부하를 효과적으로 분배(load balancing)함으로써 클라이언트와 서버 사이의 통신이 원활하게 이루어질 수 있도록 해주는 역할을 하며, 분산 환경의 핵심 기술인 분산 트랜잭션을 처리하기 위해 없어서는 안 되는 미들웨어이다. 주로 사용자가 많고 안정적이면서도 즉각적인 처리가 필요한 업무 프로그램의 개발에 많이 사용된다. 주로 은행의 창구업무 프로그램 작성에 많이 사용된다. 메인 프레임 영역에서 IBM의 CICS나 IMS 및 UNIX 계열의 BEA의 턱시도(Tuxido)와 톱엔드(Top-end) 등의 제품 등이 있다[24].

5.1.3 레거시웨어와 비즈니스웨어

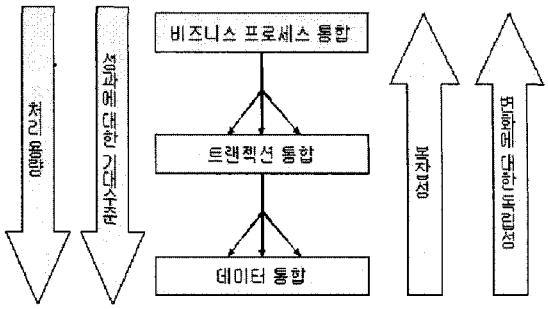
레거시웨어(Legacyware)는 기존의 애플리케이션이나 DB 기반에 새로운 업데이트 기능을 덧붙이고자 할 때 사용되는 미들웨어이다. 최근에 기존의 기업 DB와 애플리케이션들을 웹 환경에 적합하도록 변형하고자 하는 요구가 늘어나면서 꾸준히 시장이 성장하고 있는 분야이다. 대표적인 벤더로는 Fugitsu, 컴퓨터 협업(Computer Associates), 시걸 소프트웨어(Seagull Software), 자카드(Jacade) 등이 있다.

비즈니스웨어(Businessware Management System)는 기업의 다양한 애플리케이션을 통합하기 위해 사용되는 미들웨어로, 대개 기존 미들웨어의 기능 위에 비즈니스 프로세스 자동화와 실시간 애플리케이션 통합, 데이터 통합, 지능형 라우팅(intelligent routing), GUI(Graphic User Interface) 등의 기능을 덧붙인 것이다. 전자 상거래의 등장과 함께 가장 높은 성장을 할 것으로 예상되는 분야이며, 기존의 미들웨어들은 하나의 인터페이스로 통합하면서 발전할 것으로 기대되고 있는 분야이다. 대표적인 벤더로는 TIBCO Soft의 TIB/ActiveEnterprises, Vitra Businessware, web Method 등이 있다[19].

5.2 최근 액티브 네트워크 미들웨어 동향

5.2.1 EAI기반 액티브 네트워킹

EAI(Enterprise Application Integration)는 비즈니스 프로세스(BP, Business Process)를 중심으로 기업 내 각종 애플리케이션 간의 상호연동이 가능하도록 통합하는 솔루션이나 방법론을 의미한다. 즉 EAI 솔루션은 ERP, CRM 등의 애플리케이션들을 통합하여, 동일한 플랫폼을 통해 서로 커뮤니케이션 하도록 하는 것을 목적으로 한다. 이처럼 EAI는 기존 애플리케이션의 변화 없이 이들 간의 통신이 가능하게 한다는 점에서 미들웨어의 하나로 분류될 수 있다. 다만 전통적인 미들웨어가 P2P(Point to Point)로 애플리케이션을 연결하는데 사용된 반면, EAI는 기업이 비즈니스 프로세스를 중심으로 여러 애플리케이션간의 네트워크를 통합적으로 관리한다는 점에서 기존의 순수 미들웨어와 구별된다.

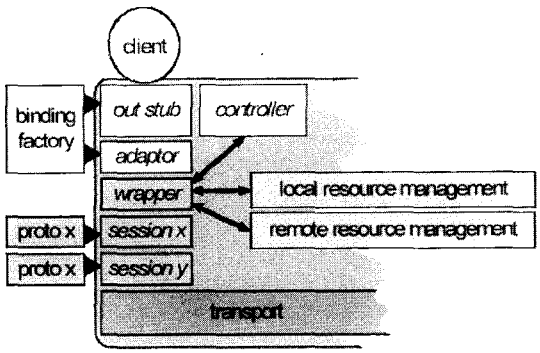


(그림 7) NAI 통합기술 단계간의 관계

현재 대부분의 EAI 솔루션들은 기존의 미들웨어 솔루션에서 출발하여, 비즈니스 프로세스 통합과 보안 기능 등을 통합하여 개발된 것들이다. 여기에 최근 기업 간 통합의 중요성이 더해지면서 XML 기능 등을 추가해 가고 있다. 따라서 대부분의 웹 애플리케이션 서버나 미들웨어들이 EAI 솔루션으로도 소개되고 있으며, 대부분의 미들웨어 업체들은 자신들의 기존 솔루션을 업그레이드하면서 EAI 시장에 진출하고 있다. 이에 따라 EAI 솔루션들은 각기 초점을 맞추고 있는 통합 분야와 강점이 다를 수 있으며, 아직 몇몇 제품들은 기존의 포인트 간 통합 수준에 머물러 있는 것으로 파악된다[19].

5.2.2 ORB 기반 액티브 네트워킹(15)

독일의 GMD-KOKUS 연구소의 Thomas Becker등은 분산 애플리케이션의 실행에 있어 서비스 품질(QoS,



(그림 8) GMD-FOKUS의 ORB기반 바이딩 구조(클라이언트 측)

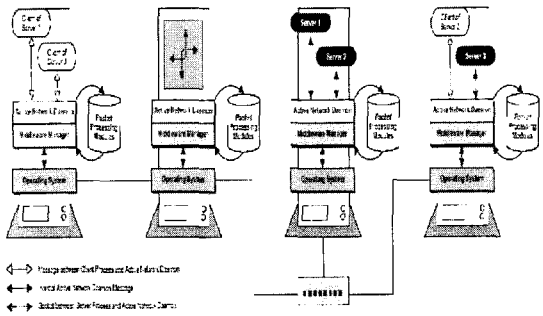
Quality of Service) 개선을 위해 ORB(Object Request Broker) 기반의 미들웨어 브리지를 사용하여 end-to-end QoS를 지원하는 액티브 미들웨어 프레임워크를 제안했다. 이들은 기존의 CORBA와 같은 미들웨어 프레임워크들이 QoS 구조와의 결합이 어려우며, QoS를 지원하는 미들웨어 솔루션들이 특정 네트워크 방식에 결합되어 있어 액티브 네트워킹에 적합하지 않음을 지적하며, 다양한 범주의 분산 애플리케이션을 위해 최종 사용자들에 대한 QoS 지원을 위한 미들웨어 프레임워크를 개발했다[15,19].

5.2.3 ComAN 기반 미들웨어

뉴질랜드 Canterbury 대학의 Carl Cook 등은 액티브 네트워크에서 모든 시스템 작업을 용이하게 하기 위해 미들웨어의 서비스를 활용한 ComAN 구조를 제안하였다. 기존 미들웨어의 장점을 활용하여 ComAN은 언어 독립적인 구조와 cross-platform 상호운영성과 같은 이점을 얻을 수 있다. 기존의 IP-기반 라우터는 이용 가능한 정보가 패킷 헤더내의 필드에 의해 제한되는데 이는 곧 기능성과 네트워크 성능에 대한 제한으로 이어진다.

ComAN은 어떠한 토폴로지의 네트워크를 통해서도 쉽게 설치될 수 있고, 유연한 패킷 처리, 차세대 서비스와 애플리케이션을 위한 라우팅을 제공하는 실제적인 desktop-to-desktop 액티브 네트워크 구조로 설계되고 구현되었다.

또한, 이전 액티브 네트워크 구조와 달리 명백한



(그림 9) ComAN의 구조

구성과 사용자 데이터의 주문 정렬을 위한 추가적인 메커니즘을 요구하지 않고, 이들 기능은 내부적으로 실행된다. 액티브 네트워크 서비스가 설치될 수 없는 경우에, ComAN은 노드를 가로질러 IP 패킷 전송으로 자동적으로 복귀하게 된다. 패킷 전송에 있어서도 운영체제 라우팅 테이블과 관련되어 있는데 시스템이 기초적인 라우팅 테이블에 대한 변화에 순응하도록 한다. ComAN은 사용자-정의 라우팅이 요구되지 않는 한 패킷을 라우팅 할 때 기존의 IP 전송 로직을 사용한다. 추가적으로 ComAN은 라우터 모듈의 호출을 기술하기 위한 특별한 메커니즘과 더불어, 데이터의 전송을 위한 BSD 소켓 루틴(socket routine)을 대리 실행하는 간단한 API를 제공한다. 보안에 대한 ComAN의 구조적 특징은 DCOM 서비스와 마찬가지로 모든 액티브 네트워크 컴포넌트의 인증이 운영체제에 의해 유지된다는 것이다. 이를 통해 ComAN에 연결하고, 등록하고, 적재하고, 호출하는 사용자를 제한하는 것이 가능하다.

ComAN은 사용자 모드에서 독립적으로 실행되기 때문에 악의 있는 라우터 모듈이 네트워크 내부에서 실행되더라도 단지 로컬 ComAN 서비스의 주소 공간 내에 있는 데이터만이 손상된다. ComAN 구조는 분리된 프로세스 경계에 각 클라이언트가 위치함으로써 클라이언트 메모리에 대한 인증되지 않은 접근을 예방하고, 다른 클라이언트와 ComAN 서비스로부터의 클라이언트 충돌을 예방한다. 구조적 특징 중 마지막으로 접근성을 들 수 있다. DCOM 바인딩이 C언어, C++, JAVA, VB 등에 존재하기 때문에 ComAN 액티브 네트워크의 클라이언트에 대한 다중-언어 접근을

허용한다. 다른 미들웨어-기반 액티브 네트워크는 미들웨어 바인딩이 DCOM, CORBA, JAVA 사이에 존재하고 있기 때문에 ComAN과 직접적으로 통신할 수 있는 잠재성을 가지고 있다[19].

6. 결 론

액티브 네트워크 기술은 현재의 인터넷 확장과 앞으로의 차세대 인터넷 구축 시에 in-service 상태에서 새로운 서비스의 적용을 용이하게 하고, 네트워크 성능을 저하시킴 없이 트래픽 제어 및 관리를 동적으로 수행하게 하는 새로운 기술이다. 또한, 액티브 네트워크는 프로그래밍이 가능한 네트워크로 현재의 네트워크 문제를 해결하기 위한 네트워크의 새로운 패러다임이다. 본고에서는 이러한 액티브 네트워크를 관리, 보안, 응용 및 미들웨어 관점으로 분류하여 기술 현황을 분석하였다.

우선, 차세대 네트워크 구조인 액티브 네트워크는 프로그램 코드를 네트워크 내에서 실행가능하게 지원함으로써 기존의 네트워크 관리 시스템이 제공하지 못했던 유연성과 중앙 집중화 되어 있던 기존 네트워크 시스템의 분산화라는 장점을 네트워크에 제공해 줄 수 있다. 이러한 유연성으로 인하여 사용자가 원하는 프로그램을 수행하거나 혹은 새로운 기술에 대한 표준화 속도가 빨라질 수 있다는 점과 네트워크의 관리를 보다 능동적으로 대처할 수 있는 점 등 매우 많은 장점을 산출할 수 있는 패러다임임에 분명하다. 그러나 액티브 네트워크가 실제로 사용되거나 사용자에게 확산되기 위해서는 아직 해결해야 할 문제점들이 많이 존재한다. 따라서 향후의 새로운 구조 혹은 연구결과는 이런 문제에 대해 적절한 해결책을 제시하여야 할 것이다.

둘째로 액티브 보안 기술은 보안 기반구조에 유연성을 부여함으로써 다음과 같이 네트워크 보안 분야에서 보안 신뢰도를 한 차원 향상시킬 것으로 보인다. 향후 국내 각 기관들의 보안 정책과 의지를 반영하고, 액티브 보안 기술을 적용 및 실행을 위해서 국내에서 운용중인 여러 네트워크 플랫폼에 공통적으로 적용될 수 있도록 각 장비별 플랫폼에 이식이 가능한 프레임워크 작업이 이루어져야 할 것이다. 이를 바탕으로 액티브 보안을 위한 시스템들 간의 통신 프로토콜 정의 및 구현, 공격 및 대응의 동작 양식을 기술할 수 있는 언어, 액티브 보안 메커니즘 실행을 위한 각 플랫폼별 실행환경, 시스템들 간의 인증, 암호화 기술들에 대한 연구가 신속히 이루어져야 할 것이다.

또한, 끝으로 액티브 네트워크에서 미들웨어는 다양한 기능을 갖고 발전해 가고 있으며, 현재의 구현은 대체로 객체 기반 미들웨어 기술에 가까운 형태로 진행되고 있다. 그러나 여러 액티브 미들웨어 모델들이 난립하고 있는데, 이는 액티브 네트워크 기술 자체가 여러 방향으로 발전하고 있는데 기인하는 것으로 생각되며, 액티브 네트워크 구조들이 정립되면 액티브 미들웨어들도 함께 정리될 수 있을 것이다.

이제, 향후의 액티브 네트워크 기술들은 차세대 네트워크에서 풀 수 없었던 여러 가지 서비스 및 응용을 적용할 때 나타나는 난제들을 해결하는 효과적인 방안을 제시할 것이며, 향후의 인터넷과 같은 망에서의 시험을 통해 안정성과 보안성을 확보한 후, 차세대 네트워크에 적용할 수 있을 것으로 예측된다.

참 고 문 헌

[1] Amit B. Kulkarni and Stephen F. Bush, GE Co. R&D, "Active Network Management and Kolmogorov Complexity," IEEE Openarch'01, 2001

[2] Toru Hasegawa et. al., "Programmable Remote Traffic Monitoring Method Using Active Network Approach," IWAN'01 Conference, 2001

[3] Gerhard Escelbeck, "Active Security : A proactive Approach for Computer Security System,"Journal of Network and Computer Application, Vol.23, 2000

[4] OpenService Inc,. "A Flexible Architecture for Internet Security Management", White Report, 2000

[5] CheckPoint, "SmartDefense ; An Active Defense Solutioin," http://www.checkpoint.com/products/downloads/smartdefense_datasheet.pdf

[6] Chin-Lin hu and Wen-Shyen E. Chen, "A mobile Agent-Based Active Network Architecture,' Depart-

ment of Electrical Engineering National Taiwan University, IEEE 0-7695-0568-6/00, 2000

[7] Floyd. S. Boulder, "Adaptive Web Caching," Cache Workshop, http://ww-nrg.ee.lbl.gov/floyd/web.html

[8] J. Murphy, "Are you ready for active networking?," http://techupdate.zdnet.com, 2002

[9] Danny Raz. Yuval Shavitt, "Active networks for Efficient Distributed Network Management,"IEEE Communications Magazine, 2000

[10] Stephen F. Bush, Admit B. Kul-Karmi, "Active Networks and Active Network Management A Proactive Management Framework," Kluwer Academic/Plenum Publishers, 2001

[11] Celestin Brou, "Future Active IP Network," WP4-GMD-011-D3-pub, 2001

[12] Amila Fernando, et. al., "A New Dynamic Architecture for and Active Network," IEEE OPENARCH, 2000

[13] Alex Galis, et. al., "A Flexible IP Active Networks Architecture", IWAN'00 Conference, 2000

[14] Thomas Becker, Hui Guo, Stamatis Karnouskos, "Enable QoS Distributed Object Application by ORB-Based Active Networking, "IWAN'00, 2000

[15] Jessica Kornblumn, D. Raz, Y. Shavitt, "The Active Process Interaction with Its Environment," IWAN'00, 2000

[16] Liquid Software: A New Paradigm or Networked System, http://www.cs.arizona.edu/liquid/

[17] T. Wolf, D. Decasper, C. Tschudin, "Tags for High Performance Active Networks," IEEE OPENARCH'00, 2000

[18] ETRI 네트워크보안구조연구팀, "액티브 네트워크 기술 분석", 2002

[19] 이재광, "액티브 네트워크 보안 프로토콜에 관한 기반연구", 2004

[20] 채기준 외 2인, "액티브 네트워크 관리 방안", 한국통신학회지, 제20권 제8호, 2003

[21] 전용희 외 3인, "에이전트 기반 액티브 네트워킹 기술", 한국통신학회지, 제20권 제8호, 2003

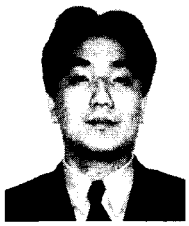
[22] 박치항 외 3인, "액티브 보안 기술", 한국통신학회지, 제19권 제8호, 2002

[23] 박치항 외 3인, "액티브 네트워크 기술의 현황 및 전망", 제19권 제8호, 2002

◐ 저 자 소 개 ◑

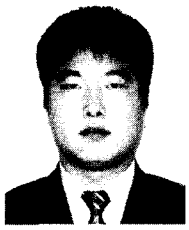
이 원 구

2000년 : 한남대학교 전자계산공학과 졸업(학사)
2002년 : 한남대학교 대학원 컴퓨터공학과 졸업(석사)
2002년~현재 : 한남대학교 공과대학 컴퓨터공학과 박사과정
관심분야 : 모바일 보안, 유비쿼터스 보안



최 병 선

2002년 : 한남대학교 전자계산공학과 졸업(학사)
2004년 : 한남대학교 대학원 컴퓨터공학과 졸업(석사)
2004년~현재 : 한남대학교 공과대학 컴퓨터공학과 박사과정
관심분야 : 네트워크 보안, 시스템 보안



이 성 현

2001년 : 한남대학교 전자계산공학과 졸업(학사)
2003년 : 한남대학교 대학원 컴퓨터공학과 졸업(석사)
2003년~현재 : 한남대학교 공과대학 컴퓨터공학과 박사과정
관심분야 : 그리드 보안, PKI

이 재 광

광운대학교 전자계산학과(학사)
광운대학교 대학원 전자계산학과(석사)
광운대학교 대학원 전자계산학과(박사)
군산전문대학 전자계산학과 부교수
University of Alabama 객원교수
한남대학교 공과대학 컴퓨터공학과 교수
관심분야 : 정보통신, 정보보호