m-CRM을 위한 무선인터넷단말기의 데이터무결성 모듈의 구현

박 현 철† · 김 동 규††

요 약

무선 인터넷 단말기 이용자들은 최근에 휴대폰이나 PDA와 같은 무선 인터넷 단말기를 이용한 고객 관계 관리로, 영업 사원들은 모바일 그룹웨어와 연동해 실시간으로 영업데이터와 고객정보를 알아내고 고객들은 무선으로 제품정보와 매입처 검색, 배송, 주문, 결제까지 편리하게 할 수 있다는 게 이점이다. 이에 본 논문에서는 사용자의 성향, 위치, 구매 정보를 이용해 실시간 맞춤 프로모션 정보를 모바일로 제공하는 서비스를 위해, 무선인터넷단말기의 안전한 데이터 전송을 위한 무선 인터넷 환경의 전환과 암호화 기술의 강조, 그리고 안전하고 신뢰할 수 있는 통신 환경 구축에 있어서 핵심적인 역할을 수행할 WTLS(Wireless Transport Layer Security) 기반의 무선인터넷단말기의 데이터 무결성 보장을 위한 보안 모듈 구현에 대한 방안을 제시한다.

Implementation of Data Integrity Module in Wireless Internet Terminal for Mobile Customer Relationship Management(m-CRM)

Hyun Cheol Park† · Dong Gyu Kim††

ABSTRACT

Recently, the wireless internet terminals like mobile phones or PDAs prevail in the management of customers. With such terminals, businessmen can get business data and information of customers in real time, in connection with mobile group wares. By the wireless terminals, customers can conveniently get information of goods, search purchase sites, and give orders and do settlement. This paper aims to present the safe data integrity modules of the wireless internet terminal, for service providing correct real-time promotion information, by using users' disposition, situation, purchase information. This study aims to suggest an implementation methodology of security module for data integrity of mobile internet terminal. This is based on the WTLS of WAP Protocol. This security module is expected to achieve central role in conversion of wireless internet environment and emphasis of encryption technology and safe and calculable wireless communication environment construction

키워드 : 이동형 고객관계관리(m-CRM), 데이타 무결성(Data Integrity), 무선인터넷(Wireless Internet)

1. 서 론

CRM(Customer Relationship Management)은 "고객관계관리"라는 뜻으로 현재의 고객과 잠재 고객에 대한 정보 자료를 정리, 분석해 마케팅 정보로 변환함으로써 고객의 구매 관련 행동을 지수화하고, 이를 바탕으로 마케팅 프로그램을 개발, 실현, 수정하는 고객 중심의 경영 기법을 의미한다. 즉 고객 관계 관리와 관련된 비즈니스 프로세스를 자동화하고 개선시키는데 초점을 두는 별도의 한 분야이자 따로 분리된 소프트웨어와 기술을 통합한 세트로서, 판매 주기와 판매 비용을 절감하고, 수입을 증가시키며, 확장시켜야 할 새로운 시장과 채널을 확인하고, 고객 가치, 만족, 수익성 및 고객 유치 증대를 목표로 한다.

CRM은 "기업의 요구 충족을 위해 웹 로그를 포함한 e-Business 관련 데이터 및 고객관련 각종 데이터를 통합, 분석하여 마케팅, 영업, 서비스 등에 전략적으로 활용하는 것을 지원하는 솔루션"을 말한다. 마케팅 관점에서 CRM의 중요성이 부각됨에 따라 기존의 ERP나 DW의 기능을 확장한 형태의 CRM 솔루션들이 등장하였다. 이후에 다양한 CRM 솔루션들이 등장하였으며, 전자상거래 및 포털 사이트의 급성장과 오프라인 기업들의 온라인 가속화 등으로 인터넷 기반이 점차적으로 확대됨으로 인하여 다양한 유형의 CRM이 등장하게 되었다.

CRM은 인터넷의 활성화에 힘입어 온라인 기반의 특화된 CRM인 e-CRM이 등장하게 되었으며, 무선인터넷이 IT 산업의 화두로 떠오르면서 m-CRM이 새로운 이슈로 떠오

† 정 회 원 : 대원과학대학 컴퓨터 정보통신과 교수
†† 정 회 원 : 아주대학교 컴퓨터공학과 교수
논문접수 : 2002년 12월 23일, 심사완료 : 2003년 11월 26일

르게 되었다. e-CRM과 m-CRM은 기존 CRM에서의 DB마케팅처럼 기업의 관점에서 기업내의 판매 프로세스를 지원하는 것이 아니라, 고객의 관점에서 고객의 구매 프로세스를 지원하는 기능을 더욱 강화하여야 한다. 이는 고객의 구매프로세스의 변화에 기인한다. 기존의 오프라인에서는 고객은 기업의 적극적인 판매활동에 대해 수동적인 구매자의 역할을 하였지만 온라인 거래에서 고객은 적극적인 구매활동을 펼치는 적극적 구매경향(Self Sales, Self Service경향)을 띄게 되었기 때문이다. 이러한 프로세스 주체의 전이가 CRM과 e-CRM, m-CRM을 구분짓는 기준이라 할 수 있겠다

CRM에 있어서 무선 인터넷의 가치는 위치성, 즉시성, 개인화 용이성이라는 세 가지 특성에서 기인한다고 말할 수 있다. 고객의 위치는 시시각각 변하며, 이에 따라 고객이 기대하는 것도 달라지게 마련이다. 또한 고객은 좀 더 빠른 시간내에 어떠한 서비스를 제공받기를 원하게 되며 기업들은 그러한 실시간 서비스에 대한 가능성을 가지게 되었다. 개인화 서비스에서도 기존의 pull 이외의 push 방식을 이용할 수 있게 되었을 뿐 아니라 기존 유선인터넷과 오프라인에서 제공하던 One-To-One marketing을 좀 더 적극적이고 강력하게 전개해 나갈 수 있게 되었다

최근에 휴대폰이나 PDA등 무선 인터넷 단말기를 이용한 고객 관계 관리로, 영업 사원들은 모바일 그룹웨어와 연동해 실시간으로 영업데이터와 고객정보를 알아내고 고객들은 무선으로 제품정보와 매입처 검색, 배송, 주문, 결제까지 편리하게 할 수 있다는 게 이점이다.

이와 같이 무선 데이터서비스에 대한 중요성이 강조되고 있는 가운데, 여러 가지 다양한 무선 인터넷 솔루션이 개발되고 있다. 이와 같은 무선 인터넷 솔루션은 크게 2가지 부류로 구분할 수 있다[2, 3, 18]. 첫째는 기존 유선 인터넷에서의 프로토콜인 HTTP에 기반해 무선 데이터 서비스를 제공하는 경우이며, 다른 하나는 무선 네트워크 환경에 적합한 새로운 프로토콜을 개발해 무선 데이터 서비스를 제공하는 방법이다. 현재 HTTP에 기반한 방식은 마이크로소프트사의 ME와 NTT 도코모의 i-mode 서비스가 대표적이며, 프로토콜을 새로 개발하는 방식은 WAP 포럼에서 개발을 주도하고 있는 WAP(Wireless Application Protocol)이 대표적이다.

WAP 포럼에서는 TCP/IP와는 별도의 무선 환경에 적합한 프로토콜을 정의하는 작업을 진행중인데, WTLS(Wireless Trnasport Layer Security)가 바로 그것이다. WTLS는 SSL과 TLS에 기반해 작성되었다. WTLS는 통신을 하는 두 응용 프로그램사이에 안전한 채널을 형성해 통신 내용의 보안을 보장하는 방법이다[2, 3, 18, 20].

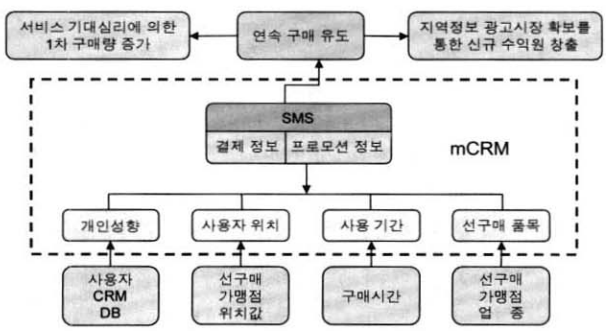
WTLS는 DES, IDEA 같은 관용 암호방식을 사용해 두 애플리케이션간의 기밀성 서비스를 제공하며, RSA와 같은 공개키 암호방식과 X.509 인증서를 사용해 클라이언트와 서버의 상호 인증을 제공하고, 내부적으로 누군가 데이터 전송을 방해할 수 없도록 하거나 재전송 공격에 이용할 수 없도록 데이터의 무결성을 제공하는 장점을 가진다[2, 3].

본 연구에서는 사용자의 성향, 위치, 구매 정보를 이용해 실시간 맞춤 프로모션 정보를 Mobile로 제공하는 서비스를 위해, 무선인터넷단말기의 안전한 데이터 무결성 모듈의 구현을 제시한다. 제 1장에서는 CRM의 개요와 유형, 그리고 m-CRM의 필요성에 대하여 설명하고. 제 2장에서는 m-CRM의 개요, 시스템 구성, 특성 및 효과, 그리고 서비스 시나리오에 대하여 설명하며, 제 3장에서는 m-CRM에서 무선인터넷단말기의 데이터 무결성 보장을 위해 WAP 프로토콜의 WTLS 보안 프로토콜에 추가하기 위해 고안된 무결성 모듈의 구현 부분에 대하여 논하고, 제4장에서 결론을 제시하였다.

2. m-CRM의 개요 및 시스템 구성

2.1 m-CRM의 개요

CRM에 있어 무선인터넷이라는 새로운 접점의 가치는 고객 채널 추가이상의 의미를 가질 수 있다. 무선인터넷 채널은 협업 CRM(Collaborative CRM), 운영 CRM(Operational CRM), 분석 CRM(Analysis CRM) 세가지 범주 모두에서 새로운 접근 방식과 새로운 분석 방식을 요구하는 것이다. 새로운 채널의 추가는 기업에게 있어 고객 만족 증대를 위한 새로운 기회일 뿐만 아니라 새로운 부담과 비용으로 작용될 수 있다. 고객은 무선이냐 유선이냐 오프라인이냐란 요소보다는 자신들이 원하는 서비스를 언제 어디서 받을 수 있는 지에만 관심이 있기 때문이다. M-CRM은 사용자의 성향, 위치, 구매 정보를 이용해 실시간(Real time) 맞춤 프로모션 정보를 모바일로 제공하는 서비스를 말하며, (그림 1)에 m-CRM의 모델로서의 위치를 나타내고 있다.



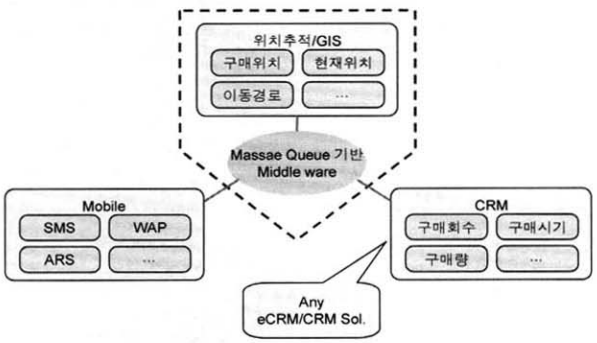
(그림 1) m-CRM의 모델

CRM에서의 무선인터넷의 활용은 분석 CRM, 운영 CRM, 협업 CRM의 세 가지 범주에서 살펴볼 수 있는데 먼저 분석 CRM 범주에서 살펴보면, 무선인터넷 채널을 통한 고객들의 이용 정보를 활용하여 Customer Segmentation 및 Cus-

tomer Action Analysis에 적용할 수 있다. 실시간성과 즉시성으로 인해 오프라인과의 연계가 용이한 무선인터넷이라는 새로운 접점에서의 고객 이용 정보는 고객의 성향을 파악하고 고객을 새로이 구분지을 수 있게 해줄 수 있다. 물론 이러한 추가적 정보에 대한 새로운 분석 방식이 충족되어야 할 것이다. 정보의 과다함이 반드시 정보의 정확성으로 이어지진 않기 때문에 적절한 분석의 적용이 반드시 필요하게 된다. 기존 유선인터넷에서 적용되던 웹로그 분석 및 페이지 방문이력만으로는 무선인터넷의 특성을 제대로 활용할 수 없으며 고객 성향에 관한 수많은 복선과 암시를 잃게 될 수 있을 것이다. 따라서 무선인터넷 고객에 대한 새로운 분석 범주가 적용되어야 할 것이다. 기존의 채널과 무선이라는 신채널과의 창의적인 통합(Channel Integration)이 요구된다. 다음으로 운영 CRM 범주에서 살펴보면, SFA (Sales Force Automation)는 영업과 관련된 프로세스를 자동화시키기 위한 CRM의 한 분야이다. 실시간 영업정보의 필요성은 무선인터넷의 이동성과 즉시성에 잘 부합하였으며, 이에 무선인터넷은 영업을 진행함에 있어 새로운 기회포착을 위한 도구로서, 영업 활동을 보고하고 상호 교환하기 위한 정보공유의 채널로서 많이 적용되어 왔다. 영업사원들은 PDA나 스마트 폰 등의 단말기를 이용하여 본사의 CRM 시스템에 접속하여 고객 이력 및 고객구매정보 등을 확인할 수 있다. 또한 영업결과를 곧바로 보고함으로써 최신의 고객영업정보를 효과적으로 유지할 수 있게 한다.

마지막으로 협업 CRM 범주에서 살펴보면, 고객은 무선인터넷 단말기라는 새로운 채널을 소유하게 되었다. 철저한 고객중심의 접근을 통해야만 효과를 발휘할 수 있는 CRM에 있어서 무선인터넷 단말기는 매우 훌륭한 접점이 될 수 있다. 개인별로 차별화 된 1 : 1 마케팅을 실시하면서 고객과의 지속적인 관계를 유지해 충성스런 고객으로 확보해 나가기 위한 새로운 기회를 준다. 더 이상 고객이 자신의 사이트로 접속하기를 기다릴 필요가 없다. 자신의 사이트를 떠난 고객을 새로이 유혹할 수 있는 접점이 생긴 것이다 (물론 이러한 접점이 고객에게는 스팸으로 다가올 수 있다는 사실을 염두에 두어야 할 것이다). 일방적인 관계(Pull)에서 쌍방적인 관계(Pull-Push)로의 전환으로 인해 기업은 고객관계를 관리함에 있어 새로운 전기를 맞이 하게 되는 것이다. 무선 인터넷이라는 새로운 미디어의 특성에 가장 잘 부합될 수 있는 분야가 협업 CRM일 것으로 생각하고 CRM 전문 기업들에 의해서 지속적인 발전 또한 이루어지리라 본다.

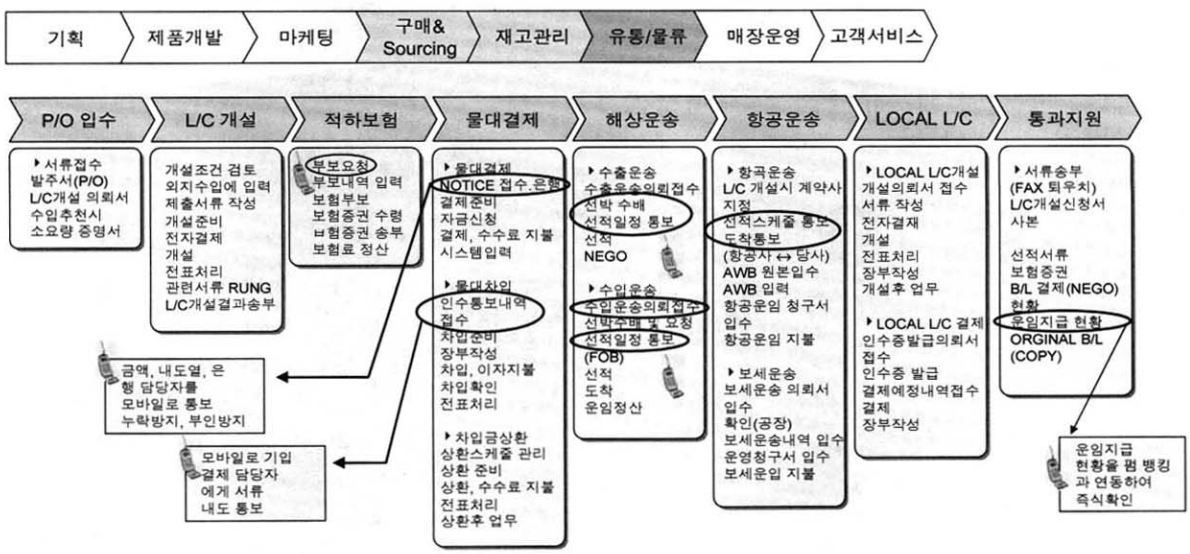
2.2 m-CRM의 시스템 구성



(그림 2) m-CRM의 시스템 구성

2.3 특성 및 효과

모바일의 급속한 확산은 기업에게 모바일 애플리케이션에 대한 신규 수요와 더불어 기존 시스템과 모바일 솔루션



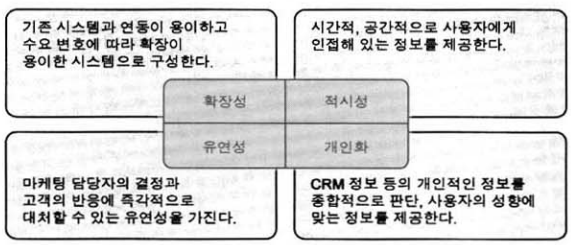
(그림 3) 모바일 적용가능 영역의 예시

간의 새로운 시스템 통합 문제가 제기될 것이다. (그림 3)과 같이 한 기업의 기능별 기간계 시스템을 그려 놓고 기능별 영역을 그려 놓은 것이다. 생산관리 시스템, 영업 관리 시스템, 경영관리 시스템, 그룹웨어 등 기업 내 기간시스템에서 모바일을 적용할 수 있는 가능성이 있는 구간을 표시하였다.

이러한 환경변화에 따른 m-CRM을 도입시 확장성, 적시성, 유연성, 개인화라는 특성을 가지게 되며, 이를 요약하여 정리하면 (그림 4)와 같다. 또한 이에 따른 효과는 <표 1>과 같다.

〈표 1〉 m-CRM의 효과

1대 1 마케팅 실현	사용자가 광고가 올 것을 인지하고 기다리는 시점에 이동 가능한 장소의 광고를 Real-Time으로 사용자의 성향을 고려해 보내준다.
연속적 구매 유도	실시간 프로 모션 정보를 통해 연속 구매를 동일한 카드로 유도, 카드 사용량의 증가를 가져온다
그 카드만 쓰게 된다	단순히 결제정보가 아닌 실속 맞춤 정보를 제공해 주는 서비스로 양질의 정보를 위해 다음 1차 구매 시에도 동일 카드 사용을 유도한다
위치 기반 마케팅 실현	최초의 본격적 위치 기반 마케팅의 실현이며 이에 따라 획득된 정보는 차기 위치기반 마케팅의 중요한 기초 정보가 된다.



(그림 4) m-CRM의 특성

2.4 서비스 시나리오

m-CRM은 사용자의 성향, 위치, 구매 정보를 이용해 실시간(Real time) 맞춤 프로모션 정보를 모바일로 제공하는 서비스의 형태를 갖추어야 하므로, 이를 만족하기 위한 m-CRM의 서비스 시나리오의 예를 들면 (그림 5)와 같다.

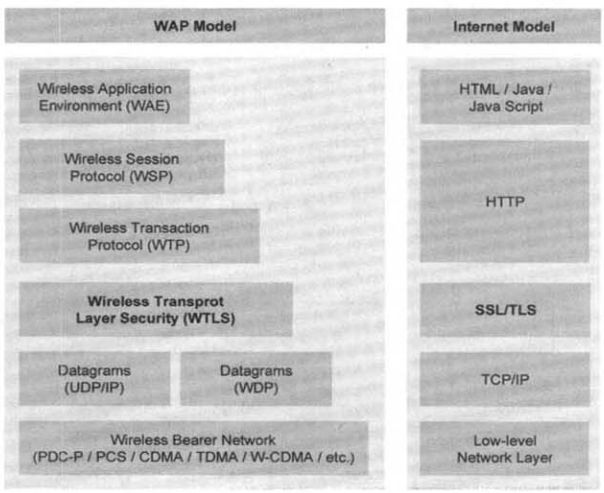
(그림 5) m-CRM의 서비스 시나리오

3. m-CRM을 위한 무선단말기의 보안모듈 구현

3.1 관련 연구

기존의 유선 인터넷에서는 많은 양의 데이터를 빠른 시간에 전송할 수 있지만, 무선 환경에서는 이러한 서비스가 어렵다. 특히 이미지나 동영상과 같은 경우에는 상당히 많은 양의 데이터 처리가 필요한데, 무선 환경에서는 이러한 대량의 데이터 위주의 서비스를 제공하는데 무리가 있다[1, 3]. WAP은 이와 같이 기존의 인터넷 프로토콜을 사용할 경우에 발생하는 문제들을 해결하고, 기존 인터넷 중심의 데이터 서비스를 무선 환경에서 효율적으로 처리하기 위해 제안된 프로토콜이다. 국제적으로 WAP 정의를 위해 표준화 기구인 WAP 포럼이 설립되어 표준화 작업이 진행되어, 1997년에 Nokia, Motorola, Ericsson, Phone.com 등 4개의 단말기 업체를 중심으로 구성되었으며, 현재 약 200여개의 업체가 참여중이다.

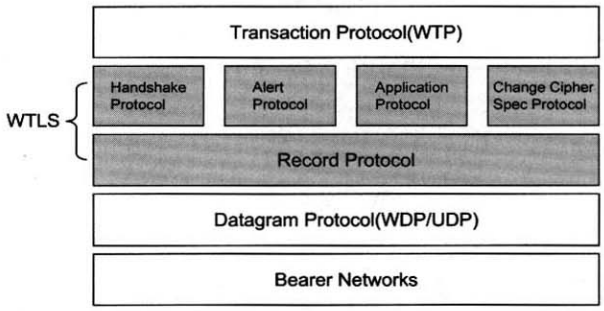
WAP 포럼에서는 (그림 6)과 같이 기존 TCP/IP와는 별도의 무선 환경에 적합한 프로토콜을 정의하는 작업을 진행중인데, 이 가운데 무선 환경의 보안 프로토콜이 WTLS이다. WTLS의 역할은 인터넷에서의 SSL/TLS와 동일하며, SSL/TLS를 기반으로 해서 설계되었다.



(그림 6) WAP 프로토콜 스택

WTLS의 구조는 (그림 7)과 같은데, 이 가운데 핸드쉐이크 프로토콜(Handshake Protocol), 얼라트 프로토콜(Alert Protocol), 사이퍼 스펙 프로토콜(Cipher Spec Protocol)은 WTLS의 동작에 대한 관리를 위해 사용되며, 실질적인 보안서비스는 레코드 프로토콜(Record Protocol)에서 제공된다[2, 3]. 무선인터넷단말기와 서버가 WTLS를 통해 연결할 경우, 먼저 핸드쉐이크 프로토콜을 수행해 한 세션동안 보안 서비스 제공에 사용되는 세션키, 암호 알로리즘, 인증서 등과 같은 암호 매개변수를 서로 공유하게 된다. 여기서 생

성된 세션 정보는 레코드 프로토콜에서 보안 서비스를 제공하는 이용된다. WTLS 얼라트 프로토콜은 핸드쉐이크 프로토콜, 체인지 사이퍼 스펙 프로토콜, 레코드 프로토콜이 수행중일 때 발생하는 모든 오류 메시지를 처리하는 프로토콜이다.



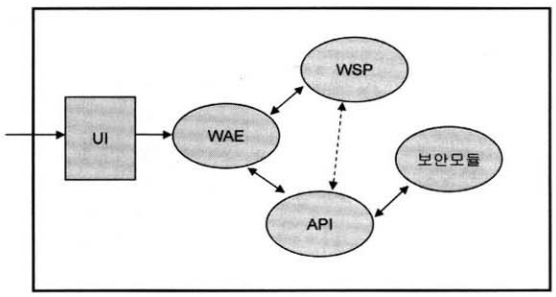
(그림 7) WAP의 보안프로토콜 WTLS

핸드쉐이크 프로토콜은 Handshake Protocol, Alert Protocol, Change Cipher Spec Protocol 등 3개의 하위 프로토콜로 구성되며, Record Protocol에서 사용될 보안 파라미터 결정, 클라이언트와 서버 인증, 오류 처리 등에 이용된다. 레코드 프로토콜은 데이터를 압축하고, 해쉬 및 암호화를 수행하여 전송하거나, 수신한 데이터를 복호화 및 검사하는 역할을 한다. 이때 데이터 압축, 해쉬 계산, 암호화 등에 사용되는 매개변수들은 핸드쉐이크 과정에서 결정된다.

3.2 보안 블록 다이어그램

현재 인터넷에서 전자상거래의 주류는 사이버 쇼핑몰을 통한 거래이다. 즉 구매자는 인터넷을 통해 사이버 쇼핑몰을 방문하여 물품 검색 등을 통해 구매하고자 하는 물품을 선택하며, 물품 구매후 지불은 신용카드를 이용하는 방법이 가장 많이 사용되고 있다. 그러나 이와 같은 형태는 네트워크, 디스플레이 장치, CPU 및 메모리의 한계 등으로 인해 무선통신 환경에서는 적합하지 않은 실정이다. 따라서 무선인터넷 환경에서는 비교적 간단한 형태의 전자상거래 솔루션이 주류를 이룰 것으로 예상되며, 이를 위한 데이터 보안 솔루션이 제공되어야 할 것이다.

본 논문에서 제시하는 무선인터넷단말기의 데이터 무결성 보장을 위한 종단간(End-to-End)보안모듈의 블록 다이어그램은 (그림 8)과 같다. API를 call하는 위치는 무선인터넷단말기 개발자의 편의에 따라 WAE 또는 WSP에 위치할 수 있으며, WAP 서버에서 무선인터넷단말기의 종단간 보안을 처리하기 위해 "Application/vnd.wap.ter_wap_sec_wml"과 같은 콘텐츠 타입을 정의해야 한다. 또한, 무선인터넷단말기의 보안 모듈을 실행시킬때에는 WSP layer에서는 Connection Oriented로 세션을 연결시켜야 한다. 이때 무선인터넷단말기에서 사용하는 관용 보안 알고리즘은 Message Authentication Code(SHA-1 : Secure Hash Algorithm), Symmetric Cryptography Algorithm(SEED), Asymmetric Cryptography Algorithm(RSA : Rivest Shamir Adeleman), Random-DES 등이다.



(그림 8) 무선인터넷단말기의 보안 블록 다이어그램

3.3 무결성 모듈의 구현

3.3.1 레코드 정의

무선인터넷단말기의 데이터 무결성 보장을 위한 보안 모듈에서 사용되는 레코드를 <표 2>와 같이 정의한다. 레코드는 레코드 헤더(Record header)와 단편(Fragment)으로 구성되며, 레코드 헤더는 레코드 타입(1 바이트)과 순서(2 바이트), 그리고 레코드 크기(2 바이트)를 포함한다. 또한, 단편은 n 바이트의 크기를 가지며, 데이터와 해쉬 값을 포함하고 있다.

<표 2> 레코드 정의

의미	Record Header			Fragment
	Record Type	Sequence #	Record Size	
길이	1 바이트	2 바이트	2 바이트	n 바이트
값	• 상위 4비트 : 암호화여부 0010 : 암호화된 레코드 0000 : 비암호화 레코드	연속된 레코드를 전송할 경우 사용 (레코드순번)	Fragment의 크기(n)	• 일반 record : data + hash 값
	• 하위 4비트 : Record Type 0001 : alert 0010 : handshake 0011 : application data			• 암호화된 record : 암호화 data + hash 값

① Client Hello Record

본 레코드는 무선인터넷단말기에서 서버로 송신하기 위한 레코드로서 난수발생기에 의해 "Client Random#1"을 발생시키고, <표 3>과 같은 레코드를 서버로 송신한다.

<표 3> "Client Hello" Record

Rec type	Seq#	Size	Type	Data Size	Ver.	Mode	Client Random#	User_id	Hash 값
1바이트	2	2	1	2	1	1	16	n	m
00000010	0		1(Client Hello)		1	1/2			

② Server Hello Record

본 레코드는 서버에서 무선인터넷단말기로 송신하기 위한 레코드로서 서버에서 버전을 체크하고 "Client Random#와 Mode정보"를 서버에 저장하여 난수 발생기에 의해 "Server Random#"를 발생시킨 뒤, <표 4>와 같은 레코드를 무선인터넷단말기로 송신한다.

〈표 4〉 "Server Hello" Record

Rec type	Seq#	Size	Type	Data Size	Ver.	Random#	Public Key	Hash 값
1바이트	2	2	1	2	1	16	128	m
00000010	0		2(Server Hello)		1			

③ Xfer Key Info Record

본 레코드는 패스워드와 무선인터넷단말기의 난수 생성 정보를 암호화하여 서버로 전송하는 레코드로서 무선인터넷단말기의 버전 검사, "Server Random#2"를 단말기에 저장, "Client Random#2" 생성, password와 Client Random#2 해쉬 처리, 그리고 서버의 Public Key로 정보를 암호화한 후, <표 5>와 같은 레코드를 서버로 송신한다.

〈표 5〉 "Xfer Key Info : Ep(Password+Client Random#2)" Record

Rec type	Seq#	Size	Type	Data Size	Data (Ep(…)	Hash값
1바이트	2	2	1	2	n	m
00000010	1		3(Xfer Key Info)			

④ Verification Record

본 레코드는 미리 정의된 데이터를 암호화하고 검사하여 서버로 전송하는 레코드로서 서버의 Private Key로 복호화를 수행하고 "Client Random#1, Client Random#2 + Password, Server Random#"로 Key Block을 생성하여 미리 정의된 데이터를 암호화한 후, <표 6>과 같은 레코드를 서버로 송신한다.

〈표 6〉 "Verification Ep(Predefined data)" Record

Rec type	Seq#	Size	암호화된 Rocord Body			
			Type	Data Size	Data(Ep(…)	Hash값
1바이트	2	2	1	2	n	m
00000010	2		4(Verification)			

⑤ Required Sign Key

본 레코드는 사용자의 Sign Key를 서버에 가지고 있지 않을 경우 서버에서 무선인터넷단말기로 Sign Key를 요청하는 레코드로서 <표 7>과 같은 레코드를 단말기로 송신한다.

〈표 7〉 "Required Sign Key" Record

Rec type	Seq#	Size	Type	Data Size	Data	MAC값
1바이트	2	2	1	2	1	m
00000010	2		5(Required Sign Key)	1	1	

⑥ Exchange Sign Key Record

본 레코드는 무선인터넷단말기가 "Required Sign Key" 레코드를 서버로부터 수신한 뒤, 단말기에서 Sign Key를 생성하여 서버로 송신하는 레코드로서 <표 8>과 같은 레코드를 서버로 송신한다.

〈표 8〉 "Exchange Sign Key Eks(Sign Key)" Record

Rec type	Seq#	Size	Eks {Record Body}				MAC값
			Type	Data Size	단말기#	Public Key	
1바이트	2	2	1	2	11	n	m
00100010	2		6(Verification)				

⑦ Finished Record

본 레코드는 서버에서 암호화된 데이터를 복호화하여 미리 정의된 데이터와 비교한 뒤, 두 데이터가 같으면 무선인터넷단말기로 송신하는 레코드로서 <표 9>와 같은 레코드를 무선인터넷단말기로 송신한다.

〈표 9〉 "Finished" Record

Rec type	Seq#	Size	Type	Data Size	Data	Hash값
1바이트	2	2	1	2	1	m
00000010	0		14(Finished)			

⑧ Alert Record

본 레코드는 무선인터넷단말기에서 서버로 보낸 데이터인 User ID와 Password가 일치하지 않는 경우 사용하는 레코드로서, <표 10>과 같은 레코드를 무선인터넷단말기로 송신한다.

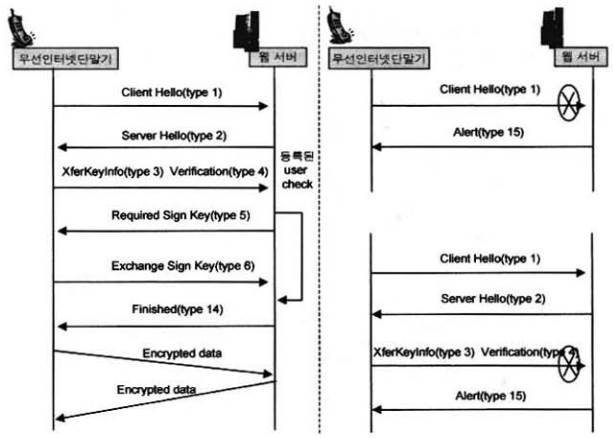
〈표 10〉 "Alert" Record

Rec type	Seq#	Size	Type	Data Size	Data	Hash값
1바이트	2	2	1	2	1	m
00000010	0		15(alert)			

※ Data : User ID Mismatched 0x01
Password Mismatched 0x02

위에서 정의한 레코드를 이용하여 무선인터넷단말기의 데이터 무결성 보장을 위한 보안모듈의 처리 흐름을 (그림 9)와 같이 도식화할 수 있으며, (그림 9)(a)는 정상적인 처리 흐름을 나타내고 (그림 9)(b)는 비 정상적인 처리 흐름

을 나타내고 있다.



(a) 정상적인 Flow (b) alert Flow

(그림 9) 무결성 모듈의 처리 흐름도

3.3.2 API 함수

① WAP Gateway에서 Bypass시키기 위해 콘텐츠타입을 미리 정의된 보안 타입으로 변경하는 함수

```
void devGetContentType (U8*Ctype, U8*Ctype2)
    {
      memcpy (Ctype1, "sec_wml", 7) ;
      memcpy (Ctype2, "sec_wmls", 8) ;
    }
```

* input : First ContentType, Second ContentType

② 종단간 보안 핸드쉐이크 시작 함수

```
void devSecurityStart (U8 mode, UserID, U8 UserIDLength, U8*Pwd,
                       U8 PwdLength, U8*Returndata, U8*rdataLength,
                       U8*Rstatus, U8*ErrorType)
    {
      secClientStart (U8 mode, UserID, U8 UserIDLength, U8*Pwd,
                      U8 PwdLength, U8*Returndata, U8*rdataLength,
                      U8*Rstatus, U8*ErrorType) ;
    } ;
      mode          : mode/sign mode
      UserID        : USER_ID
      UserIDLength  : USER_ID length
      Pwd           : User Password
      PwdLength     : Password Length
      Returndata    : record to be sent to server
      rdataLength   : Return data size
      Rstatus       : Record type
      ErrorType     : the state of received record
```

③ 서버로부터 데이터를 받았을 때 이를 파싱(parsing)시키는 함수

```
void devParseRecord (U8*data, UNIT16 dtataLength, U8*Returndata,
                     UNIT16*rdataLength, U8*Rstatus, U8*ErrorType)
    {
      secParseRecord (U8*data, UNIT16 dtataLength, U8*Returndata,
                      UNIT16*rdataLength, U8*Rstatus, U8*ErrorType) ;
    } ;
    data          : received data from server
    dataLength    : received data length
    Returndata    : record to be sent to server
    rdataLength   : Return data
    Rstatus       : Record type
    Error Type    : the state of received record
```

④ 무선인터넷단말기에서 서버로 데이터를 보내는 함수

```
void devSendRecord (U8*data, UNIT16 dtataLength, U8*Returndata,
                    UNIT16*rdataLength, U8*Rstatus, U8*ErrorType)
    {
     secSendRecord (U8*data, UNIT16 dtataLength, U8*Returndata,
                    UNIT16*rdataLength, U8*Rstatus, U8*ErrorType) ;
    } ;
    data          : sending data from server
    dataLength    : data length
    Returndata    : record to be sent to server
    rdataLength   : Return data
    Rstatus       : Record type
    Error Type    : the state of received record
```

⑤ 종단간 보안 mode 종료 함수

```
void devSecurityClose()
    {
        secSecurityClose(void) ;
    }
```

⑥ Error 처리 함수

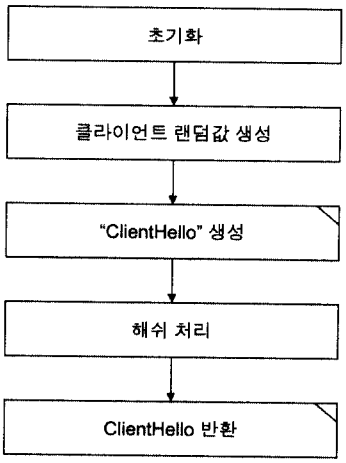
```
if (ErrorType & Fatal_Error)
{
    if ((ErrorType &0xF0) == sec_USERIDMISMATCHED ||
      (ErrorType &0xF0) == sec_HASHCODENOTCORRECT)
        {
          display error message ("잘못된 ID입니다. 다시 입력하세요")
          display both UserID input and Password input card
        }
    else if((ErrorType &0xF0) == sec_PWDMISMATCHED)
        {
          display error message ("패스워드가 올바르지 않습니다")
          display both UserID input and Password input card
        }
}
```

3.3.3 보안 모듈 함수의 처리 흐름도

① dev_clientStart 함수

무선인터넷 단말기단에서 데이터 무결성 보장을 위한 통신을 시작하기위해 "Client Hello"시 최초로 호출하는 함수(dev_clientStart)의 내부 흐름도이다. 클라이언트 앤덤값을 생성한 후, 해쉬처리를 하여 Client 레코드 타입을 무선 인

터넷 단말기단으로 반환한다.



(그림 10) ClientHello 초기 호출 함수

(그림 10)에서 클라이언트 랜덤값을 생성하기 위해서 다음과 같은 함수형을 사용하였다.

```
void EN_GenerateRandom_DES (uint8 *out, uint32 bytes)
```

함수에서 입력인자 "bytes"는 발생시킬 난수의 바이트 수이며, 출력인자 "out"은 생성된 난수를 저장할 데이터를 의미한다.

그리고 (그림 10)에서 해쉬 처리를 위해서 다음과 같은 함수형을 사용하였다.

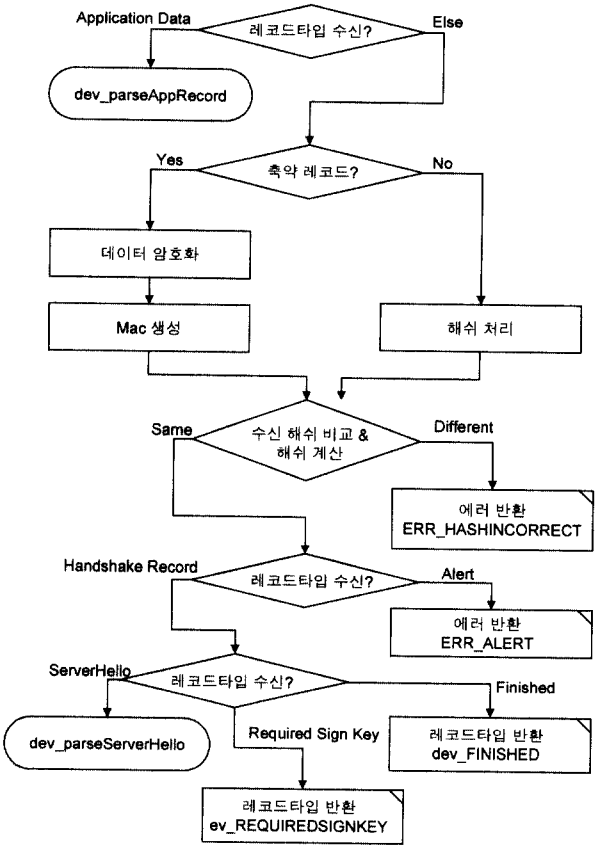
```
void E_SHA1(U8* out, U8* in, U32 bytes)
```

함수에서 입력인자 "in"은 축약할 데이터, "bytes"는 축약할 데이터의 바이트 수이며, 출력인자 "out"은 축약된 160(20byte) 비트의 데이터를 의미한다.

② dev_parse 함수

"dev_parse"로 시작되는 API들은 무선인터넷 단말기단에서 데이터 무결성 보장을 위한 통신과정에서 WAP 서버로부터 수신한 데이터의 복호화를 수행하여 단말기단으로 반환하는 함수이다. 이 함수들은 dev_parseRecord와 부함수로서 암호화된 데이터를 수신하여 복호화하는 dev_parseAppRecord, 통신과정시 WAP 서버로부터 수신한 데이터를 복호화하여 단말기단으로 반환하는 dev_parseServerHello들로 구분된다.

(그림 11)에서 무선인터넷 단말기단에서 데이터 무결성 보장을 위한 통신과정 중에 암/복호화 함수, 키 생성 함수를 호출하여 암/복호화 및 세션키를 생성한 후, 각 단계별로 정의된 레코드타입의 데이터를 송/수신한다. 이때 암/복호화 및 키블록 생성에 사용되는 함수는 다음과 같다.



(그림 11) dev_parseRecord 함수

ⓐ 암호화 함수

```
Void E_SEED_Encrypt(U32 *data, SEED_KEY *key, long bytes,
U8 *iv)
```

함수에서 입력인자 "data"는 암호화할 128비트 평문, "key"는 라운드 키를 저장하고 있는 SEED_KEY 구조체, "iv"는 라운드 키를 갖는 벡터 테이블 값이며, 출력인자 "data"는 암호화된 128비트 암호문을 의미한다.

ⓑ 복호화 함수

```
Void E_SEED_Decrypt(U32 *data, SEED_KEY *key, long bytes,
U8 *iv)
```

함수에서 입력인자 "data"는 복호화할 128비트 암호문, "key"는 라운드 키를 저장하고 있는 SEED_KEY 구조체, "iv"는 라운드 키를 갖는 벡터 테이블 값이며, 출력인자 "data"는 복호화된 128비트 평문을 의미한다.

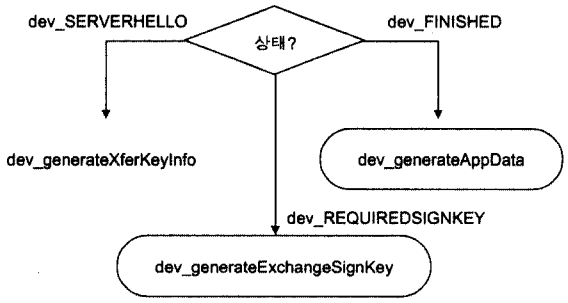
ⓒ MAC 처리 함수

```
Void E_SHA1_MAC_Update(SHA1_CTX* ctx, U8* data,
U32 bytes, U8* add)
```

함수에서 입력인자 "ctx"는 SHA1_CTX 구조를 가진 컨텍스트, "data"는 축약할 데이터, "bytes"는 축약할 데이터의 바이트 수, "add"는 덧붙여진 입력 데이터이며, 출력인자 "ctx"는 SHA1_CTX 구조를 가진 컨텍스트를 의미한다.

③ dev_sendRecord 함수

이 함수는 무선인터넷 단말기단에서 데이터 무결성 보장을 위한 통신과정에서 WAP 서버로 데이터를 보낼 때 호출하는 함수이다. 상태 정보를 입력받고 그 상태에 따라 "dev_SERVERHELLO"시에서는 "dev_generateXferKeyInfo" 부함수를 호출하고 "dev_FINISHED"이면 "dev_generateAppData"라는 부함수를 호출하며, 마지막으로 상태 정보가 "dev_REQUIREDSIGNKEY"이면 "dev_generateExchangeSignKey" 부함수를 호출하여 처리한다.



(그림 12) dev_sendRecord 함수

4. 결 론

이동통신 사용자는 국내에서만 이미 2천만 명을 넘어서고 있으며, 전 세계적으로는 2002년까지 7억 이상의 사용자를 확보할 것으로 예상되고 있다. 이러한 가운데 무선통신을 통한 데이터 서비스의 제공이 필수적인 요소로 받아들여지고 있으며, 이에 따라 무선통신과 기존 인터넷과의 결합은 향후 정보통신 산업의 중추적인 역할을 할 것으로 기대된다. 이에 대비하여 이미 Mobile IP, IMT2000, WAP 등 무선 인터넷을 겨냥한 다양한 메카니즘이 연구·개발되고 있다.

www의 등장과 함께 혁명적인 전환을 맞았던 인터넷은 이제 무선 인터넷이라는 또 다른 전환기를 맞고 있다. 이와 함께 무선통신 기술에 안전성 및 신뢰성을 보장할 수 있는 정보보호 서비스에 대한 비중 또한 점차 높아지고 있다.

특히 유선 인터넷과 마찬가지로 인터넷과 연동되는 무선망 뱅킹, 증권거래, 전자상거래 서비스 등에서 처리되는 데이터의 내용은 노출이나 불법 도용에 매우 민감함으로 더욱더 보안의 중요성은 대두된다. 이렇게 대두되는 정보보호의 필요성에 대해 유선망 환경의 인터넷에서는 다양한 정보보호 기술이 발전되어졌다. 특히 네트워크 보안을 위한 방법으로 SSL(Secure Socket Layer)/TLS(Transport Layer Security) 및 S/MIME, S-HTTP 등의 기술이 개발되어 사용되었으며 현재는 공개키 기반 구조를 활용한 인증서 기반의 보안 인프라가 각광을 받고 있다.

그러나 무선 인터넷망에서는 보안에 대한 연구가 부족한 실정이므로, 본 연구는 이러한 보안 인프라를 무선망에서 효율적으로 적용할 수 있도록 핸드쉐이크 프로토콜을 구현하고 네트워크 정보보호 서비스를 제공하기 위하여 RSA 공개키 알고리즘 및 SEED 대칭키 알고리즘, SHA-1 해쉬 알고리즘을 적용하여 단 대 단(End to End) 보안을 유지하여 데이터 무결성을 보장하기 위한 보안모듈을 구현하였다.

또한, 본 연구는 이러한 무선 인터넷 환경의 전환과 암호화 기술의 강조, 그리고 안전하고 신뢰할 수 있는 통신 환경 구축에 있어서 핵심적인 역할을 수행할 WTLS 기반의 무선인터넷단말기의 데이터 무결성 보장을 위한 모듈 구현에 대한 방안을 제시하였다.

앞으로 무선 인터넷의 계속적인 발전은 유·무선 통합 환경의 등장으로 이어질 것으로 예상된다. 유·무선 통합 환경에서는 기존의 인터넷이나 무선 통신에서의 정보보호 서비스와는 다른 새로운 패러다임이 적용될 것이며, 지금부터 이에 대한 연구 및 개발이 시작되어야 할 것이다.

참 고 문 헌

[1] 김춘길, "전자상거래의 개념과 발전방향", 정보과학회지, 제16권 제5호, May, 1998.

[2] 김현욱, 김영결, 조원득, 김연규, 이성범, "Wireless Application Protocol 서비스 개요", SK Telecom Technical Journal, Vol.6, No.4, Oct., 1999.

[3] 주해종, "Mobile EC-통신프로토콜과 보안문제", 한국상무학회, Dec., 2000.

[4] 김재문, "E-비지니스 모델에 맞는 e-CRM 구축실행 가이드", 거름출판사, 2001.

[5] 허경희, "CRM-신경영 패러다임", 정보과학회지, 2001.

[6] Elsenpeter, R. C. and Velte, T. J., "e-Business A Beginner's Guide", McGraw-Hill, Berkeley, 2001.

[7] 최정환, "CRM을 위한 데이터베이스마케팅", 다산출판사, 2001.

[8] 폴 티머스 저 이석주 옮김, "B2B 전략과 모델", 물푸레 출판사, 2001.

[9] Pieter Adriaans & Dolf Zantinge 저 용환승 역, "데이터 마이닝", 그린출판사, 1998.

[10] 김재경, 송희석 "Mining the Time-dependent Behavior of Interet Shopping Mall Customers", 한국경영과학회/대한산업공학회, 춘계공동학술대회 발표 논문, 2001.

[11] 2001년 산.학.연 컨소시엄 센터 보고서 "2001년도 산.학.연 공동기술개발 컨소시엄 결과보고서", 대원과학대학, 2001.

[12] S. C. Hui, G. jha, "Data mining for customer service support," Information & Management, 2000.

[13] Jiawei Han, Micheline Kamber and Anthony K. H. Tung, Spatial Clustering Methods in Data Mining : A Survey,

2000.
[14] Fayyad, U. M., et al., "Advances in Knowledge Discovery and Data Mining," AAAI Press/The MIT Press, 1966.
[15] 조민관, 정정우, 이영해, "e-Marketplace와 SCM의 통합을 위한 개념적 모델에 관한 연구", 한국경영과학회/대한산업공학회 춘계공동학술대회, 2001.
[16] 이 준, 이종태, "신경망을 이용한 군집화 기법의 개선과 데이터마이닝의 기능 향상에 관한 연구", 한국경영과학회/대한산업공학회 춘계공동학술대회, 2001.
[17] 윤병운, 백재호, 박용태, "데이타 마이닝을 이용한 특허 인용 분석", 한국경영과학회/대한산업공학회 춘계공동학술대회, 2001.
[18] WAP Forum, "Wireless Transport Layer Security," Nov., 1999.
[19] Dierks T., Allen C., "The TLS Protocol," IETF RFC2246, Jan., 1999.
[20] http://www.wapforum.org.
[21] http://www.zionwap.net.
[22] 무선 WTLS 인증서 프로파일 규격서, http://www.rootca.or.kr.
[23] 무선 WTLS 인증서 DN 규격, http://www.rootca.or.kr.
[24] 신뢰성 있는 멀티캐스트 전송 표준의 개발, http://www.sunlimited.co.kr.

박 현 철

e-mail : park@daewon.ac.kr
1983년 호서대학교 전자계산학과 학사
1991년 아주대학교 컴퓨터공학과 석사
1996년 아주대학교 컴퓨터공학과 박사수료
1983년~1991년 해태유업 전산실 재직
1991년~1993년 비전테크날리지 대표
1996년~현재 대원과학대학 컴퓨터 정보통신과 교수
관심분야 : 컴퓨터네트워크, EC, e-CRM, Data Mining

김 동 규

e-mail : dkkim@madang.ajou.ac.kr
서울대학교 공과대학(학사)
서울대학교 자연과학대학원(석사)
미국 Kansas 주립대 대학원(Ph.D. 전산학 박사, 정보통신 전공)
미국 Kansas 주립대 전산학과 교수
1979년~현재 아주대학교 컴퓨터공학과 교수
관심분야 : 컴퓨터 네트워크, 정보통신 프로토콜 엔지니어링, 정보통신 Security, 분산처리 시스템