유.무선 네트워크 기반의 동기화 데이터 전송 시스템 설계

이근호°, 이송희, 김정범, 김태윤
고려대학교 컴퓨터학과
{root1004, pine, qston, tykim}@netlab.korea.ac.kr

A Design for Synchronization Data Transfer System on based Wire and Wireless Network

Keun-Ho Lee° Song-Hee Yi, Jeong-Beom Kim, Tai-Yun Kim
Dept. of Computer Science & Engineering, Korea University

요 약

정보통신 분야의 이동통신기술은 많은 부분에서 발전을 거듭하고 있다. 이동통신기술의 발전으로 인하여 무선인터넷과 유선인터넷 통합에 대한 관심과 연구가 활발히 진행되어 지고 있다. 본 연구에서는 유무선 인터넷의 통합화로 인한 데이터 동기화 과정을 소개하고, 동기화된 데이터의 관리와 전송을 위한 유.무선 데이터 관리 시스템들을 소개한다. 이에 본 논문에서는 이동 통신간 데이터의 동기화 과정과 동기화된 데이터를 안전하게 처리하여 전송할 수 있는 유.무선 데이터 동기화 전송 시스템을 설계한다.

1. 서 론

정보통신분야에서의 Mobile 통신 시스템은 빠르게 발전하고 있다. 기존의 유선 네트워크를 이용한 데이터 전송은 이동 통신의 발전으로 인하여 유.무선 시스템의 통합화가 이루어지고 있다. 기존의 무선환경의 단말기와 유선환경 시스템간의 원활한 데이터 전송을 위한 동기화 처리 기술이 활발히 연구되어 지고 있다. 무선 이동 통신 기술의 발전으로 무선 단말기(PDA, PocketPC, PDA 폰등)를 이용한 무선 데이터 전송 서비스가 활성화되어 가고 있으며, 사용자들은 특정 지역과 시간에 관계없이 데이터를 이용할 수 있는 이동 컴퓨팅 시대가 도래하였다. 이동 통신 사용자는 항상 네트워크에 연결되어 있지 않기 때문에 네트워크에 저장된 데이터를 항상 이용할 수 없다. 그래서 이동 통신 사용자는 네트워크로부터 원하는 데이터를 검색하고 그것을 이동 단말기에 저장한 후 그 데이터를 접근하여 처리하게 된다. 사용자는 정기적으로 네트워크에 재접속하여 이동 단말기에서 변경된 데이터를 네트워크 저장소에 전송하고 네트워크 저장소에 갱신된 데이터를 전송 받아 동기화 처리 후 일관성 있게 유지해야 한다. 공통된 데이터 동기화 기술은 터미널 사용의 성장을 발전시키고 사용자의 데이터 접근과 이동 데이터 서비스의 전달을 향상시킨다. 이러한 동기화 처리를 위한 데이터 동기화 표준이 SyncML이다. SyncML은 유.무선의 데이터 동기화에 최적화를 이룰 수 있다[8].

본 논문에서 제시하는 동기화 처리 부분은 SyncML을 이용하였다. 동기화 처리 후 데이터 전송을 위한 시스템은 WPKI(Wireless Public Key Infrastructure) 기반으로 구성하여 유.무선 동기화 데이터의 전송 시스템을 설계하였다.

2. 관련연구

유.무선 데이터 전송 시스템의 구조와 동기화 과정을 소개하고, 안전한 데이터 전송 시스템의 구조를 분석해 본다.

2.1 유.무선 데이터 전송 시스템

기존의 유선 데이터 전송 시스템은 XML을 기반으로 하여 설계되어진다. 전자 문서 또는 다른 표현 방법이라는 기존의 틀을 벗어나서 데이터와 메타데이터를 표현하는 수단뿐만 아니라 프로세스 제어와 통신 부분까지 XML 기반이 되어 가고 있다. 무선 데이터 전송에서 많은 부분이 WAP(Wireless Application Protocol)을 이용하고 있다.

- XML 기술 기반 구조

XML은 활용 대상이 단순한 전자 문서에서부터 무선 인터넷 컨텐츠 언어, 통신, 비즈니스 프로세스 및 워크플로우까지 너무나 많은 분야로 확산되고 있다. XML은 체계적으로 이해하기 위하여 7 Layers로 나누어 각 기능과 역할을 표현하고 있다. 그림 1과 같이 구분 할 수 있다[7].

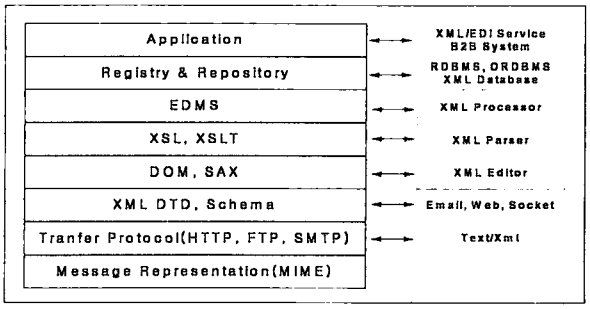

그림 1. XML 기술 기반 구조

- 무선 데이터 전송

무선 인터넷은 WAP 포럼의 WAP(Wireless Application Protocol), Microsoft사의 ME(Mobile Explorer)와 Stringer, OPENWAVE사의 UP(Unwired Planet) Browser, NTT DoCoMo사의 i-mode 그리고, Qualcomm사의 단말기 플랫폼인 BREW(Binary Runtime Environment for Wireless)등 다양한 방법이 있다. 대부분의 무선 인터넷에서는 WAP 방식이 사용되어 지고 있다[3].

현재 WAP2.0버전은 기존의 WAP1.2보다 보완된 기능을 많이 가지고 있다. WAP2.0에서는 XHTML(eXtended Hyper Text Markup Language)의 지원을 근간으로 하고 있다. WAP2.0을 WAP NG(Next Generation)라고도 하며, end-to-end security, MMS(Mobile Location Service) 및 PIM(Personal Information Management) 기능 강화 및 단말기 화면의 그래픽처리가 추가되었다[5][6].

2.2 동기화 과정

SyncML은 XML 기반의 데이터 동기화를 위한 표준 프로토콜이다. 이동 통신의 단말기와 같은 이동 가능 데이터 단말기를 이용하여 서버나 다른 단말기와 교환하는 데이터의 동기화 과정이다[9][11].

SyncML의 메시지 구성 요소는 메시지와 패키지, SyncML Header, SyncML Body, SyncML Command로 이루어져 있다[10].

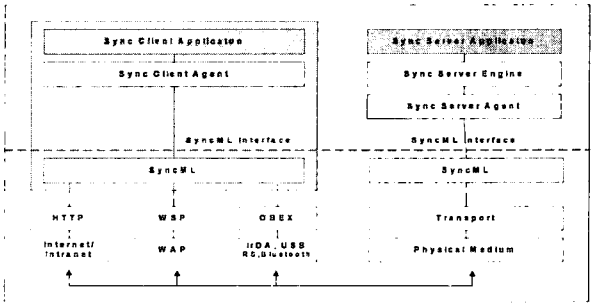

그림 2. SyncML Protocol Architecture

2.3 안전한 데이터 전송 시스템

- XKMS(Xml Key Management Specification)

XKMS는 차세대 인터넷언어인 XML에 기반을 두고 있으며, 기업이나 개발자들이 XML 웹서비스에 PKI 전자 서명과 암호화의 사용 효율성을 극대화할 수 있도록 지원하고 있다. XKMS는 개발자에게 전자상거래 응용 시스템에 적용할 전자서명과 데이터 암호화를 보다 용이하게 할 목적으로 개발되었다. XKMS는 개발자들이 전자 인증과 다른 온라인 보안 기능을 전자상거래 응용시스템에 쉽게 접목할 수 있게 한다. XKMS는 X-KISS(XML Key Information Service Specification)와 X-KRSS(XML Key Registration Service Specification)의 두 영역으로 구성되어 있다[1].

- WPKI(Wireless Public Key Infrastructure) 시스템

무선 인터넷이 안전한 전자상거래 서비스를 제공받기 위해서는 기밀성, 무결성, 인증, 부인봉쇄와 같은 서비스를 제공하기 위한 무선 PKI가 필요하다. 무선 PKI란 기존의 유선 PKI의 구성요소를 그대로 이용하여 무선환경에 적합하도록 기능을 최소한 변화시킨 것이다. 무선 PKI를 구축할 경우에는 유선과는 달리 클라이언트(무선 단말기)와 서버간의 제한된 대역폭, 클라이언트의 처리능력, 클라이언트의 제한된 메모리를 고려해야한다. 또한 기존 유선환경과는 달리 인증서 검증 매커니즘의 경량화가 필요하다[2].

3. 유무선 통합 시스템 설계

유.무선 인터넷의 동기화 데이터 전송 시스템을 설계하기 위해서 공개키 구조를 기반으로 하였다. XML시스템과 SyncML시스템을 연동하여 무선 PKI기반으로 시스템을 설계하였다.

3.1 XML 시스템

XML파서는 DTD에 따른 유효성 검증 기능과 문서의 처리기능 및 다음 단계의 XSLT 프로세서 기능까지 포함한다. 전자서명은 비대칭 암호화 방식과 해싱 함수를 활용하여 구현되어 진다. XML Signature을 통해서 필요한 모든 정보들과 수신자측에 보내야할 정보들을 XML 형식으로 표현한다.

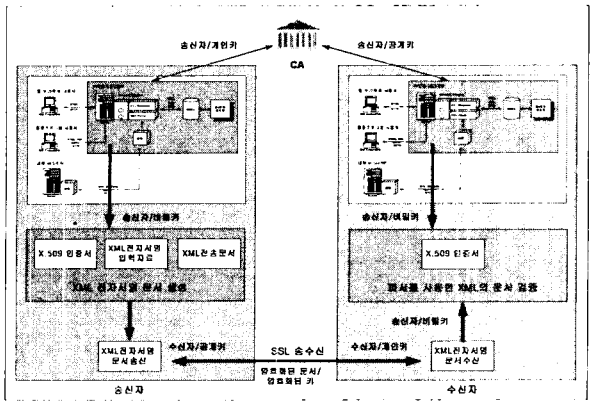

그림 3. XML 데이터의 문서생성 및 전송 과정

3.2 SyncML 시스템

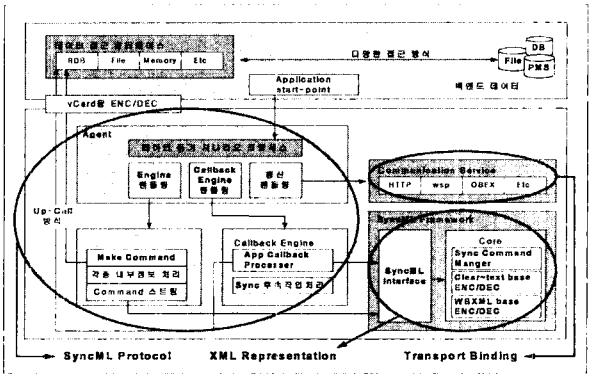

그림 4. SyncML의 상호 운영 시스템

데이터 동기화 표준을 위해서 데이터 동기화에 필요한

정보를 담는 메시지 구조체, 메시지의 핸들링에 필요한 프로토콜, 구성된 메시지의 네트워크 송수신을 위한 트랜스포트 바인딩에 대한 표준이 있어야 한다. 트랜스포트 바인딩에서는 WAP의 WSP를 이용한다.

3.3 WPKI 시스템

무선 PKI모델의 특징은 기본적으로 X.509인증서를 사용하지만, 무선 CA 서버는 단말기 검증능력을 고려하여 Short-lived인증서인 WTLS인증서를 사용하며, 단말기의 경우 저장공간의 문제로 인증서를 발급 받을 경우 인증서의 URL을 이용한다. 단말기에서 무선용 X.509 서버 인증서를 검증 메커니즘으로 CRL이나 OCSP를 사용하도록 한다. 또한 무선에서는 CRL를 잘게 쪼개서 최근 CRL를 가져와서 검증 할 수 있는 메커니즘인 Delta CRL이 옵션으로 사용된다. 무선 단말에서 RSA를 사용하여 키 생성이 용이하지 않아 ECDSA를 사용하여 키를 생성할 수 있는 기능이 무선에서 추가되었으며, 서명 알고리즘으로는 RSA ECDSA가 사용되며, 키 분배용으로는 RSA, ECDH가 사용된다. 무선에서는 WAP에 기반한 SignText()함수를 사용하여 무선 환경에 맞는 인증서 요청 및 관리를 프로토콜 규격을 정의하여 사용한다.

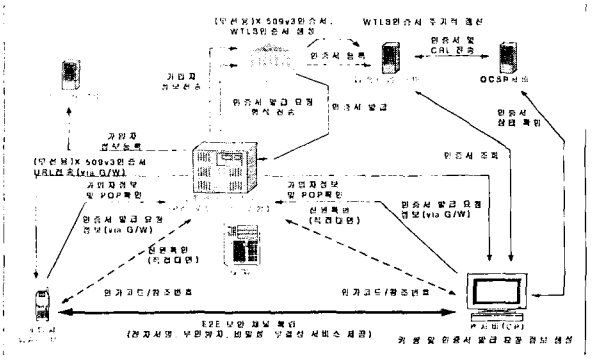

그림 5. 무선 PKI 구조

3.4 유.무선 동기화 데이터의 전송 시스템

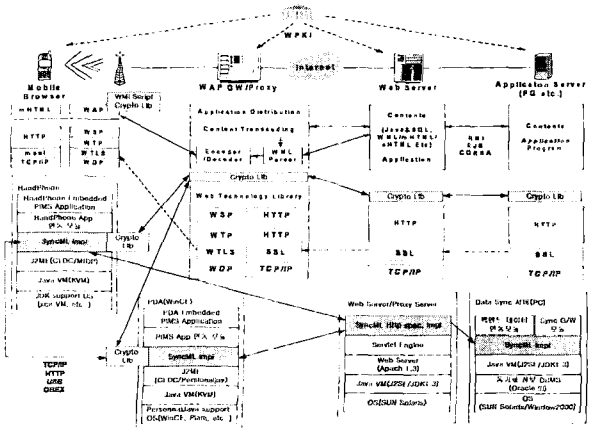

그림 6. 유.무선 동기화 데이터의 안전한 전송 시스템

제안된 시스템은 데이터 동기화 표준인 SyncML과 유.무선 데이터 전송 시스템의 전체적인 모듈을 제안한 시스템이다. 유.무선의 모든 데이터 자료에 대하여 동기화 처리 후 데이터를 안전하게 전송 하기 위하여 무선 PKI의 구조를 적용시켰다. 기존의 데이터 처리 시스템까지도 고려하여 유연성, 확장성, 동시성, 안전성등을 지원하도록 설계하였다. 본 논문의 제안 시스템은 M-Commerce 분야에서도 활용할 수 있다. WAP의 전송 계층에서 제공하지 못하는 부인방지를 위한 전자서명 기능은 WMLScript Crypto Library를 이용한다. SyncML은 Authentication Handler의 기능을 이용하여 표준 인증타입에 의한 처리와 다른 인증타입도 지원할 수 있다.

4. 결론 및 향후과제

본 논문에서는 유.무선 네트워크의 동기화 데이터 전송을 위한 시스템을 설계하였다. 동기화 과정 처리를 위해서 SycnML을 이용하여 유.무선 데이터를 동기화 하였다. 또한 WAP을 이용하여 유.무선 데이터의 전송과정을 명시하였고, 이러한 시스템 설계 과정을 위한 데이터 표현을 위해서 XML 기반의 데이터 처리 시스템을 설계하였다. 유.무선에서의 안전한 데이터 전송을 위해서 공개키 기반으로 시스템을 설계하였다. 향후 연구로는 안전성 검증과 관련된 프로토콜 모델을 설계할 것이다.

참 고 문 헌

[1] XML Key Mangement Specification(XKMS). http://www.w3.org/TR/xkms/

[2] "차세대 인터넷 보안 무선 PKI", 정보보호뉴스, 한국정보보호진흥원, Vol.47, 2001. 8

[3] 김현욱, 김연규, 이성범, 이명성, " IMT-2000 이동통신의 원리", 진한도서

[4] Miyazawa, T., Kushida, T.,"An advanced Internet XML/EDI model based on secure XML documents" Parallel and Distributed Systems:Workshops, Seventh Internation Conference on, 2000, page : 295-300

[5] WAP specifications. http://www.wapforum.org/what/technical.htm

[6] WAP 2.0 Technical White Paper http://www.wapforum.org/what/WAPWhite_Paper1.pdf

[7] Extensible Markup Laguage(XML), http://www.w3.org/xml

[8] "동기화 표준 SyncML의 표준화 동향", ITFIND, 주간기술 동향, 통권 1031호, 2002.01.30, ETRI IT 정보센터

[9] SyncML, http://www.syncml.org

[10] 하인숙, 조재혁, 양지현, "데이터 동기화의 표준 SyncML 기초 다지기, 마이크로 소프트웨어, 2001.5월, page:330-340

[11] 이지연, 조진현, 최훈, "SyncML 데이터 동기를 위한 데이터베이스 설계 및 구현", 정보처리학회 추계 학술대회, 제 8권, 제 2호, page : 1343-1346

[12] 김세영외 5명, "XML 전자서명 시스템의 설계 및 구현", 정보처리학회 추계 학술대회, 제 8권, 제 2호, page: 891-894

[13] 박남제, 송유진, "모바일 서비스 플랫폼 기반의 무선 전자상거래 보안 가술", 정보보호학회지, 제 11권 제 4호, 2001.8, page : 9-28