논문 2011-5-11

모바일용 스마트 메시지 서비스 플랫폼

Smart Message Service Platform for Mobile Environment

김남윤*

Namyun Kim

요 약 스마트폰의 급속한 보급으로 보안 공격에 안전하고 통합적인 메시지 서비스에 대한 요구가 증가하고 있다. 스마트폰은 3G/WiFi와 같은 데이터 네트워크를 이용하기 때문에 다양한 보안 정책을 통해 안전한 메시지 전송이 가능하고, 카메라와 GPS를 통해 수집된 다양한 정보를 포함할 수 있는 통합 메시지 서비스가 가능하다. 본 논문에서는 사용자 인증, 메시지에 대한 기밀성 및 무결성을 제공할 뿐만 아니라 위치, 사진, 문자 메시지를 통합하여 전송할 수 있는 메시지 서비스 플랫폼을 제시한다. 그리고 플랫폼의 기능성을 검증하기 위해 아이폰 앱과 메시지 전송 서버를 구축한 사례를 소개하고 구현 결과를 보인다.

Abstract With increasing use of smartphone, users require a new message service to prevent security attack and provide integrated messages. Since smartphone uses data services such as 3G cell network and WiFi, it can provide reliable message transfer through various security policies. In addition, it can transfer various data collected using built-in camera and GPS. This paper proposes a smart message service platform which can provide security services such as authentication, confidentiality and integrity as well as transfer the integrated message including location, picture and text. To verity the functionality of the platform, this paper implements an iPhone app and message transfer server, and then shows the implementation results.

Key Words : 스마트폰, 메시지 서비스 플랫폼, 메시지 보안, 통합 메시지, 메시지 전송 서버

Ⅰ. 서 론

아이폰(iPhone)의 등장은 “모바일 생태계”라는 새로운 시장 변화를 일으켰다[1,2]. 즉, 애플 앱스토어를 기반으로 “단말기-콘텐츠 개발자-소비자”를 유기적으로 연결함으로써 상승 효과를 유발하는 새로운 서비스 환경을 만들어내었다. 시장의 중심축이 이동 통신사에서 단말기 업체로 이동하였고 국내 스마트폰 가입자도 2011년 8월 현재 2,000 만명에 육박하고 있다. 그리고 앱스토어에는 수십만 개의 앱이 개발되어 유통되고 있다.

특히 문자 메시지 서비스는 간편함, 비동기성, 저비용으로 인해 시장이 급속히 성장하고 있다. 스마트폰의 메신저 서비스로는 “카카오톡”과 “whatsapp”이 있으며 카카오톡은 가입자가 1,500 만명을 넘어섰고 가입자당 하루에 평균 15회 이상 이용하고 있는 것으로 알려져 있다. 이러한 메신저 서비스의 주요 특징은 다음과 같다.

- 일반 휴대폰(feature phone)의 SMS와는 달리 메시지의 길이에 제한이 없다.
- WiFi와 3G의 데이터 통신망을 효율적으로 이용함으로써 고속, 저렴하게 서비스를 이용할 수 있다.
- Push 모델을 채택하고 있어 거의 실시간으로 사용자에게 전송이 가능하다.
- 이메일과 같이 “저장 및 전송(store and forward)” 방식을 이용하기 때문에 일시적으로 전송이 실패

*정회원, 한성대학교 정보시스템공학과
접수일자 2011.8.17, 수정일자 2011.9.23
게재확정일자 2011.10.14

한 메시지도 추후 전달이 가능하다.

스마트폰용 메신저 서비스는 친구간의 대화에 초점을 맞추고 있기 때문에 불특정 다수, 즉, 기업과 고객 사이의 대규모 소통 수단으로는 부족한 단점이 있다. 이러한 소통의 개방성을 지원하기 위해서는 메시지의 보안성이 높아야하며 기존의 문자뿐만 아니라 위치, 사진과 같은 멀티미디어 데이터를 통합하여 전송할 수 있어야 한다. 본 논문에서는 스마트폰의 장점을 활용한 메시지 서비스 플랫폼(SMSP: Smart Message Service Platform)을 제시한다. 즉, 지인뿐만 아니라 타인과 기업에게 보낼 수 있는 개방성을 가지고 있으며 보안성이 뛰어난 통합 메시지 환경을 제공한다. 이러한 메시지 서비스 플랫폼은 독립된 형태로 메시지 앱으로 존재할 수도 있으며 다른 앱의 내부 솔루션으로 채택될 수 있는 장점을 가지고 있다.

일반적으로 개방형 메시지 서비스 플랫폼이 가져야 할 조건으로는 메시지의 보안성, 실시간 전송, 신뢰할 수 있고 효율적인 전송을 보장하여야 한다. 본 논문에서는 이러한 조건을 만족하기 위해 필요한 설계 사항을 제시하고 구현을 통해 결과를 보인다.

본 논문의 구성은 다음과 같다. 2절에서는 메시지 서비스 플랫폼이 가져야 할 요구 조건을 명시하고 시스템 구조에 대해 서술한다. 3절에서는 메시지 서비스 플랫폼의 세부적인 설계 내용과 4절에서는 구현 사항을 기술한다. 마지막으로 5절에서는 결론 및 향후 연구 과제에 대해 서술한다.

II. SMSP(Smart Message Service Platform) 모델

1. 요구 조건 분석

Zerfos[3]는 SMS(short message service) 문자 서비스에 대한 트레이스를 통해 사용자별 메시지 전송 개수와 메시지 서비스 시간에 대한 분포를 제시하였다. 3주간 실시한 실험의 주요 결과는 다음과 같다.

- 대부분의 사용자는 3주 동안 1,000개 이하의 메시지를 전송하지만 일부 사용자는 10,000개 이상의 메시지를 전송하는 경우가 있다. 즉, “person-to-pserson” 트래픽인 경우에는 전송 메시지 개수가 작지만 컨텐츠 제공자가 전송하는 “person-to-application” 트래픽의 경우에는 대규모의 메시지를 생성하는 것으로 알려져 있다. 이러한 트래픽은 주로 기업에서 뉴스, 주가, 통지 서비스로 사용되는 것으로 알려져 있다.
- 메시지 전송 성공 유무에 따른 분포를 보면, 성공한 메시지가 94.9%, 메시지 거부나 유효시간 경과로 인해 실패한 메시지가 각각 3.5%, 1.6%를 보이고 있다. 메시지 성공한 메시지에 대해 메시지 전송 시각과 메시지 수신 시각을 비교함으로써 메시지당 총 서비스 시간을 예측할 수 있는데, 10초 이내에 전달된 경우가 73.2%, 1분 이상 소요된 경우 17%, 1.5시간 이상 소요되는 경우가 5%인 것으로 나타났다.

이러한 연구 결과를 바탕으로 SMSP가 가져야할 조건을 다음과 같이 정의하였다.

- 보안 서비스: 개인 정보 및 메시지는 민감한 정보로서 안전한 서비스가 요구된다. 외부인이 이해할 수 없도록 암호화를 통한 기밀성(confidentiality), 메시지의 변조 유무를 탐지할 수 있는 무결성(integrity), 메시지의 재생을 통한 공격(replay attack) 방지, 개인 인증(authentication) 기능이 요구된다.
- 통합 메시지: 컨텐츠 제공자가 전송하는 “person-to-application” 트래픽은 문자뿐만 아니라 위치, 사진 등을 포함한 메시지 서비스를 요구한다.
- 신뢰성있는 메시지 전송: 모바일 환경하에서 3G 네트워크의 잦은 핸드오프, 약한 신호 세기, 혹은 인증되지 못한 WiFi 연결 등 네트워크 상황이 유선에 비해 현저히 열악하다고 볼 수 있다. 이러한 환경하에서는 메시지 전송 실패가 자주 발생한다. 따라서 네트워크 상황 변화에 대처할 수 있어야 하며 메시지의 실패시 사용자에게 알려줌으로써 재시도할 수 있도록 해야 한다.
- 실시간 메시지 전송: 메신저 서비스처럼 대화식으로 메시지를 전송하는 경우가 많기 때문에 실시간으로 메시지가 전송되어야 한다. 이를 위해서는 푸쉬(push)와 같은 알림 서비스와 UI(user interface)의 잠김 현상(locking)이 발생하지 않도록 멀티 스레딩 기술이 요구된다.
- 효율적인 메시지 전송: 회원 수가 증가할수록 전송되는 메시지 양은 급격히 증가하게 된다. 따라서 서버에서는 효율적인 메시지 전송을 통해 성능을 최대화하는 작

업이 무엇보다 중요하다.

2. 시스템 구성도

본 논문에서 제안하는 SMSP의 구성요소는 그림 1과 같다.

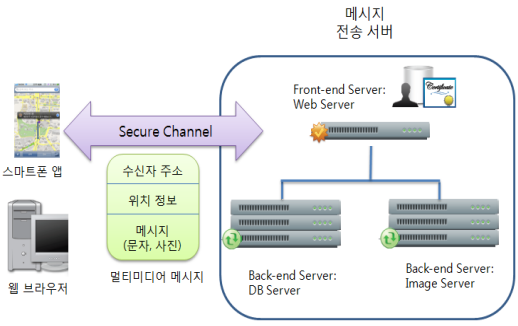


그림 1. SMSP 시스템 구성도
Fig. 1. System Architecture of SMSP

- 송신 단말기: 스마트폰이나 PC를 의미한다. 송신 단말기는 특정 네트워크 포트(Port, 80 혹은 443)를 이용하여 메시지를 "전송 서버"로 송신한다. 메시지는 수신자 정보(예: 전화번호)와 통합 데이터(문자, 사진, 위치 등)로 구성된다. 만약 네트워크 접속 실패로 인해 메시지가 제대로 전달되지 않을 경우에는 송신자가 인식하도록 한다. 위치 정보는 GPS 장치와 3G망, WPS(WiFi Positioning System)를 이용하여 획득된다. 본 서비스에서의 위치 정보는 사용자의 현재 위치뿐만 아니라 관심 지역을 포함하는 광의의 개념이므로 위치 정보를 측정할 수 없는 데스크탑에서도 서비스 이용이 가능하다.
- 메시지 전송 서버: 메시지를 임시 보관하는 서버로서 저장 및 전달(store and forward) 형식을 띠고 있다. 즉, 메시지를 임시로 보관한 후 수신자의 요청시 전달한다. 메시지 전송 서버는 웹 서버, 이미지 서버, 데이터 베이스 서버로 구성된다. 웹 서버는 사용자의 요청을 수신하며, 데이터베이스 서버는 사용자의 메시지를 저장한다. 이미지 서버는 사진과 같은 멀티미디어 데이터를 저장한다. 데이터베이스와 이미지 서버를 분리함으로써 네트워크 트래픽을 분산시킨다.
- 수신 단말기: 메시지 전송 서버는 애플의 APNS(Apple Push Notification Service)나 구글의 C2DM(Cloud to Device Messaging)에 푸쉬 전송을 요청함으로써 단말기에게 푸쉬를 전송할 수 있다. 사용자는 전송 서버에게 요청하여 저장된 메시지를 수신한다.

Ⅲ. SMSP 설계

1. 보안 서비스

본 논문에서는 SSL(Secure Socket Layer)[4]을 이용한 채널 보안과 AES[5]를 이용한 메시지 보안의 두 가지 방식을 채택하고 있다. 초기에 회원 가입과 대칭키 분배를 위해 SSL 기반 HTTPS를 사용한다. 그리고 메시지 송수신시에는 AES와 같은 대칭키 암호를 사용함으로써 효율성을 제고하고 있다.

가. SSL을 통한 개인정보 보호

네트워크 상에서 안전하게 메시지를 전송하기 위해 개인 정보를 포함한 데이터 통신은 국제 표준 보안 프로토콜인 SSL을 이용한다. SSL 프로토콜은 서버 인증, 암호화를 통한 기밀성 제공, 메시지 인증 코드를 통한 무결성 제공의 기능을 가진다. SSL은 서버뿐만 아니라 다양한 단말기에서 지원이 되는데, 예를 들어 iPhone은 SSL v3을 지원하고 있다. 그림 2는 SSL 프로토콜의 단순한 형태를 보여주고 있다. 클라이언트와 서버간의 암호 알고리즘 협상이 종료된 후, 세션 키 Ks를 이용하여 암호화된 데이터를 송수신한다. 이 과정에서 개인 정보, 대칭키(Kcs), 클라이언트 인증을 위한 TUK(Temporary User Key)가 교환된다. 대칭키는 추후 메시지 보안에 사용되며 TUK는 사용자의 신분증 역할을 하는데 로그인시에 서버에 전달된다.

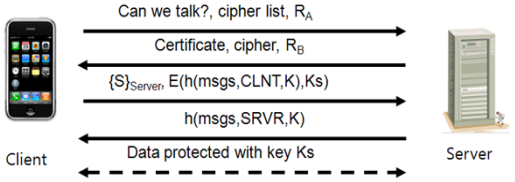


그림 2. SSL 프로토콜의 동작 과정
Fig. 2. Operation Flow of SSL Protocol

나. 메시지 보안

SSL 프로토콜은 채널 암호화를 위해 다소 복잡한 핸드세이크 과정을 거친다. 따라서 작은 메시지 전송을 위

해 매번 SSL 채널을 생성하기에는 많은 오버헤드가 발생한다. 따라서 본 연구에서는 메시지 전송은 AES 128 비트를 이용한 대칭키 암호 알고리즘을 사용한다.

클라이언트에서 메시지 전송시 전달하는 데이터는 그림 3과 같다. TUK를 통한 개인 인증, {메시지, 타임스탬프}의 대칭키(Kcs) 암호화를 통한 기밀성, 그리고 {메시지, 타임스탬프}의 해쉬값을 통한 무결성을 제공한다. 한편, 타임 스탬프는 재생 공격 방지를 위해 사용되는데, 서버에서는 현재 시각과 타임 스탬프 값의 차이가 임계치를 넘는 경우, 메시지를 무시한다.

Kcs: 클라이언트와 서버간의 공유되는 대칭키
TUK: 클라이언트 신분증, 서버의 마스터 키로 암호화되어 있음.

그림 3. 메시지 보안 서비스
Fig. 3. Message Security Service

2. 메시지 전송 서비스

그림 4는 사용자가 메시지를 전송하였을 경우 전체적인 흐름을 보여주고 있다.

1) 메시지 전송 요청: HTTP의 몸체(body)에 메시지를 AES로 암호화하여 저장한 후, get 혹은 post 메소드를 이용하여 서버에 전송 요청한다.
2) 메시지 저장: 웹 서버를 통해 전송 요청을 수신한 후 DB에 메시지를 저장한다. 만약 사진과 같은 멀티미디어 데이터는 이미지 서버에 분리하여 저장한다. SMSP는 기본적으로 “store-and-forward” 방식으로 동작하기 때문에 사용자의 요청이 있을 경우 메시지를 전달한다.
3) 푸쉬 요청: 애플의 APNS[6]나 구글의 C2DM[7]을 이용하여 사용자에게 푸쉬 알림을 요청한다. 애플이나 구글 서버는 사용자에게 푸쉬를 보내게 된다. 이 때 주의할 점은 순간적으로 너무 많은 푸쉬 요청을 애플이나 구글에 요청하지 않도록 해야 한다.
4) 메시지 수신: 푸쉬를 받은 클라이언트는 전송 서버로부터 메시지를 수신하게 된다. 전송과 마찬가지로 HTTP 프로토콜을 이용하여 메시지를 수신한다. 암호화된 메시지는 복호화된 후, 화면에 출력된다.

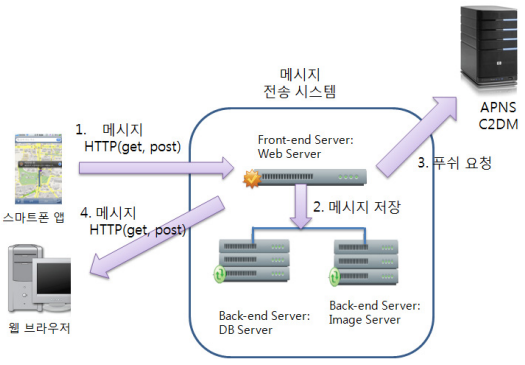


그림 4. 메시지 전송 과정
Fig. 4. Sequence of Message Transfer

메시지 전송 소프트웨어의 구조는 그림 5와 같다. UI를 담당하는 메인 스레드는 기본적으로 “run loop”혹은 “event loop”를 돌면서 사건을 처리한다. 사용자가 전송 버튼을 선택하였을 경우 내부적으로 네트워크 오퍼레이션을 구성한 후, 큐에 삽입을 한다. 이 때 시스템 내부적으로 "worker thread pool"에 있는 스레드가 깨어나서 오퍼레이션을 처리한다. 실제로 모바일 네트워크를 통한 메시지 전송은 유선 네트워크에 비해 비신뢰적이므로 UI 스레드가 네트워크 오퍼레이션이 끝날 때까지 기다린다면 응답 시간이 매우 길어지게 된다. 따라서 UI 스레드와 네트워크 스레드를 분리함으로써 UI 잠김 현상(locking)을 막는 효과를 줄일 수 있다.

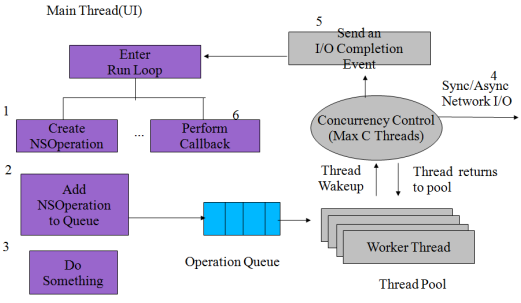


그림 5. 메시지 전송 소프트웨어의 구조
Fig. 5. Architecture of Message Transfer Software

한편 네트워크 스레드는 동기 혹은 비동기식으로 동

작을 하며 처리 결과가 왔을 때 메인 스레드에게 통지를 한다. 이 때 메인 스레드는 콜백 함수를 처리하며 메시지의 성공 유무를 사용자에게 알린다. 결국, 이러한 구조를 통해 UI 잠김 현상을 줄일 수 있고 "worker thread pool"을 사용함으로써 thread의 개수의 급격한 증가로 인한 시스템 자원 낭비를 줄일 수 있는 장점이 존재한다.

2.1절에서 제시한 바와 같이 모바일 사용자의 위치 파악이 되지 않거나 일시적으로 서비스가 불가능할 경우, 그리고 사용자가 메시지 조회를 미루었을 경우 서버는 메시지를 저장하고 있다. 이 때 각각 메시지를 하나씩 보내는 경우보다는 이를 묶어 전송함으로써 서버는 효율적으로 메시지를 전송할 수 있다. 본 논문에서는 메시지의 크기가 임계치를 초과할 경우에는 다수의 메시지를 묶어 전송하고 있다. 또한 사진을 포함한 멀티미디어 메시지인 경우, 요약 이미지를 나타내는 섬네일(thumbnail)을 표시해주고 사용자의 요청이 있을 경우에 전달하는 방식을 통해 트래픽을 분산시키고 있다.

Ⅳ. 구현 결과

1. 스마트폰 앱

본 논문에서 제시한 SMSP는 애플의 아이폰(iPhone)에서 구현하였다. 아이폰의 iOS 4.3에서 제공하는 Foundation, UIKit, MapView, CoreAnimation[8]과 같은 다양한 프레임워크를 활용함으로써 소프트웨어의 생산성을 높일 수 있다. 스마트폰 앱은 멀티스레드로 동작하며 기본적인 구조는 그림 6과 같다.

- 메인 스레드는 UI를 담당하며 사용자의 요청에 따라 다른 스레드를 조정하는 역할을 담당한다.
- 네트워크 워커(worker) 스레드는 메시지 전송 서버와의 통신을 통해 메시지의 송수신 기능을 담당한다.
- 사용자의 연락처와 송수신한 메시지를 데이터 베이스에 저장하기 위해 스토리지 스레드가 존재한다. 이 스레드는 SQLite를 이용하여 DB 입출력을 담당한다.
- 내부 스레드: iOS에서 내부적으로 생성하는 스레드로서 지도를 가져오기 위한 MapView, 위도/경도를 기반으로 실제 주소(예:서울시 성북구)를 가지고 오는 Reverse Geocoding 스레드가 존재한다. 또한 현재 위치를 수정하기 위한 Location Update, 그래픽 애니메이션 처리를 위한 Animation 스레드가 존재한다.

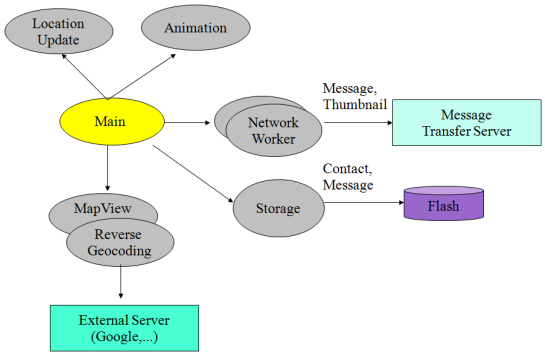


그림 6. 스마트폰 앱의 스레드 구조
Fig. 6. Thread Architecture of Smartphone App

2. 전송 서버

메시지 전송 서버는 메시지 전송 요청을 수신하는 "Message Delivery Server", 회원 정보를 관리하는 "Account Server", 사진과 같은 컨텐츠를 관리하는 "Content Server", 주기적인 메시지 처리 작업 및 푸쉬 요청을 위한 "Batch Server", 회원 정보와 메시지를 저장하는 MySQL 데이터베이스로 구성되어 있다.

한편 서버의 내부 Action은 자바 웹 프레임워크[9]로 구현된다. 자바 웹 프레임워크는 Open Source로서 계층화되어 있어 유연한 웹 애플리케이션 개발이 가능하다. WebWork, iBatis, Quartz 등으로 구성되어 있다.

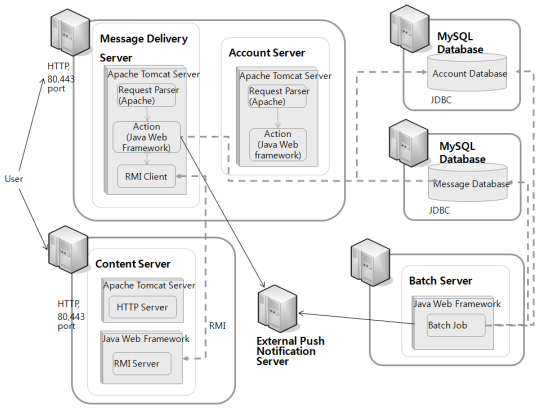
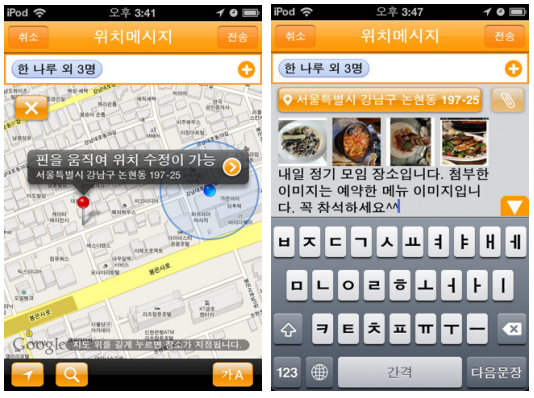


그림 7. 메시지 전송 서버의 구조
Fig. 7. Architecture of Message Transfer Server

3. 실행 화면

SMSP에서 단말기 앱은 아이폰에서 구현되었으며 실행 화면은 그림 8과 같다. 그림 8(a)는 구글 지도를 사용하여 현재 위치를 나타내고 있다. 사용자는 위치를 검색하여 관심 지역을 지정할 수도 있다. 그리고 위도/경도 정보를 이용하여 실생활 주소로 변환하는 "reverse geocoding"을 통해 애노테이션에 표현하고 있다. 그림 8 (b)에서는 위치뿐만 아니라 문자와 사진을 작성하고 있는 화면을 보여주고 있다. 따라서 SMSP는 다양한 데이터를 통합해서 전달이 가능하고 수신자는 지인뿐만 아니라 전화번호를 직접 입력하여 외부인에게 전송하는 것이 가능하다. 그림 8 (c)는 대화 목록을 보여주고 있다.



(c)

그림 8. 스마트폰 앱 실행 화면
Fig. 8. Screen Shot of Smartphone App

V. 결 론

스마트폰의 보급으로 개인간의 소통 수단인 메시지 서비스가 급속히 성장하고 있다. 본 논문에서는 지인뿐만 아니라 개인과 기업간의 통신을 지원하는 개방형 플랫폼을 지원하기 위해 보안성과 통합 메시지 환경을 제공하는 SMSP를 설계 및 구현한 내용을 제시하였다. 즉, 개인 인증과 메시지에 대한 기밀성/무결성을 제공하고 다양한 정보가 통합된 메시지 플랫폼의 성능 개선 방안을 제시하였다. 그리고 실제 아이폰 앱 및 서버를 구축하여 수행 결과를 제시하였다.

향후에는 메시지 전송 요청을 효율적으로 분배하는 부하 분배 기업에 대해 연구할 예정이다. 사용자가 증가함에 따라 수십~수백 대의 서버가 부하를 담당해야 하기 때문에 대규모 메시지 플랫폼에서는 핵심적인 연구주제라고 할 수 있다.

참 고 문 헌

[1] Tomi T Ahonen, Alan Moore, *Communities Dominate Brands,* FutureText Ltd., March 2005.

[2] Nagarjuna Venna, "The Evolving Nature of Competition in the Wireless Ecosystem: Emergent Opportunities and Threats," Massachusetts Institute of Technology, June 2009.

[3] P. Zerfos, X. Meng, S. H.Y. Wong, V. Samanta and S. Lu, "A study of the Short Message Service of a nationwide cellular network," IMC 2006

[4] A.O.Freier, P.Karlton, and P.C.Kocher, The SSL Protocol Version 3.0, Internet Draft, March 1996.

[5] J. Daemen and V. Rijmen, *The Design of Rijndael, the Advanced Encryption Standard,* Springer-Verlag, 2003.

[6] Alasdair Allan, *Learning iPhone Programming,* O'Reilly, 2010.

[7] Android Cloud to Device Messaging Framework, http://code.google.com/intl/ko-KR/android/c2dm/index.html

[8] 유동근, *iPhone & iPod Programming,* 한빛미디어, 2009.

[9] Craig Walls, *Spring in Action,* Manning, 2011.

※ 본 연구는 한성대학교 교내 연구비 지원과제입니다.

저자 소개

김 남 윤(정회원)

- 1992년 2월 서울대학교 컴퓨터공학과 학사
- 1994년 2월 서울대학교 컴퓨터공학과 석사
- 2000년 2월 서울대학교 컴퓨터공학과 박사
- 1999년 9월 ~ 2002년 2월 삼성전자 무선사업부 책임연구원
- 2002년 ~현재 한성대학교 정보시스템공학과 부교수

<주관심분야 : 멀티미디어 통신, 모바일 통신 및 응용>