PDA에서 운용 가능한 보안 메시지 전송 프로토콜 설계 및 구현

이기영* · 이정균**

Design and Implementation of Protocol to Transfer Secure Messages for PDA

Ki Young Lee* · Jeong-kyoon Lee**

본 연구는 2002년도 인천대학교 학술연구조성비 지원에 의하여 수행되었음.

요 약

본 논문에서는 CDMA무선망을 이용한 PDA기반의 취약한 전송로 상에서도 안전하게 메시지를 전송할 수 있는 서비스 모델과 PDA 특성을 고려한 보안 메시지 전송 프로토콜 제안하고 구현하였다. 제안된 서비스는 유선 인터넷 망과 오프라인 상태의 클라이언트 단말기를 SMS(Short Message Service)를 이용하여 연결하였다. 단말기는 SMS 메시지 수신 후에 SMS의 데이터를 분석하여 RAS(Remote Access Service)를 통해 데이터 채널을 생성하고 서버 측의 데이터가 PUSH 되도록 구현되었다. 구현된 보안 프로토콜은 SMS와 데이터 채널을 가지는 2채널 방식을 이용하여 각 통신 부문에서 안전한 통신을 보장 할 뿐 아니라, 안전한 세션키 통신을 위한 비표(nonce table)키 방식을 사용하였기 때문에 세션키 전송 시 키 길이도 줄이면서 높은 비트의 암호화를 할 수 있는 효과를 보였다.

ABSTRACT

This paper proposes and implements a service model to transfer messages safely for PDA on CDMA wireless network and a secure massage transfer protocol which considers characteristics of PDA. Proposed service uses SMS(Short Message Service) connect to a off-line client device with the wired network for data communication. After receiving SMS message, client device processes the SMS message and creates a data channel through RAS(Remote Access Service), then the data of the server can be pushed to clients. The implemented security protocol can provide safe data transmission on each communication line through two way channels(SMS and data). Also, by using security nonce table, this protocol can reduce a number of transmissions for exchanging a safe session key, so intensity of encryption can be increased.

키워드

PUSH service, PDA Application, CDMA, SMS, Security Protocol

* 인천대학교 정보통신공학과 교수

** 인천대학교 정보통신공학과 박사과정

접수일자 : 2004. 11. 22

Ⅰ. 서 론

무선 네트워크를 이용하는 컴퓨팅이 활성화되는 요즘, 많은 이동 단말기들을 위한 인터넷 서비스들이 제안되고 있다. 원하는 정보만을 원하는 시간에 제공하는 맞춤형 서비스인 PUSH 서비스는 무선 인터넷의 특성에 잘 부합되는 형태이다. 그러므로 개인용 이동 단말기를 이용한 무선 인터넷에서 PUSH 서비스의 비중은 높아 질 것이라고 예상된다. 무선 서비스에서의 보안 문제는 서비스의 특성상 일정관리, 주소록, 증권정보 등 개인적인 데이터가 많기 때문에 필수 요소라 할 수 있다.

최근 활용도가 높아가고 있는 무선랜 에서의 정보 보호 취약점을 보완하고자 IEEE 802.11위원회에서 무선랜 에 암호화 기능과 인증기능을 제공하여 주는 WEP(Wired Equivalent Privacy)를 표준 권고안으로 발표[1] 하였으나 암호화 과정에서의 초기값 크기 및 재사용성에 대한 안전성 부족과 일방향 인증으로 인한 불법 인증 등의 문제에 대한 취약점을 여전히 가지고 있다[2][3]. 무선망의 보안성이 향상된다 하더라도 무선 서비스의 안전성을 보장하기엔 부족하다. 그래서 무선 서비스를 보다 안전하게 제공하기 위해서는 응용 프로그램 수준의 보안 솔루션이 필요하다.

본 논문에서는 이러한 무선 통신을 이용하는 개인 정보 전송 서비스에서 보다 안전하게 정보를 전달할 수 있도록 사용자의 인증과 메시지의 보안성을 고려한 메시지 보안 전송 시스템과 이 시스템에서 사용될 보안 프로토콜을 설계 하고 구현하였다. 보안에 취약한 무선 통신 환경에서 낮은 사양의 단말기도 안전성과 빠른 속도의 성능을 유지하며 정보전달을 할 수 있도록 하였다.

2장에서 PDA를 활용한 문자 정보에 대한 PUSH 서비스모델을 제시하고 3장에서는 이와 같은 서비스 모델에 적합한 암호화 알고리즘을 적용한 보안프로토콜을 제안하였고 4장에서는 제안된 시스템의 성능 및 결과에 대한 분석을 하였다. 마지막으로 5장에서는 제안된 시스템이 가지는 의미와 향후과제에 대하여 논함으로써 결론을 맺는다.

Ⅱ. PUSH 서비스 설계와 구현

2.1. PDA 단말기의 PUSH서비스 특징

PDA 단말기는 일반 유선망처럼 항시 온라인 상태가 아니다. 그 이유는 기본적인 음성 통신을 위한 기능을 기본으로 하기 때문이다. 항시 데이터 회선으로 열어놓을 경우 음성통신을 위한 대기 시간을 가질 수 없기 때문에 유선망과는 오프라인 상태라 할 수 있다.

이러한 특징을 가지는 PDA 단말기에서 유선망으로의 접속을 위해 사용자의 요구에 따라 접속하는 것이 아니라 원하는 정보를 위한 이벤트가 발생하였을 때 접속하는 것이 첫 번째 특징이다. 본 논문에서는 PUSH 서비스를 위해 SMS 채널 과 데이터 채널을 동시에 운용함으로써 모바일 단말기의 PUSH 서비스를 구현하였다.

SMS는 모바일 단말기가 가지는 일반적인 특성일 뿐 아니라 SMS 데이터도 모바일 단말기에서 처리가능하기 때문에 이는 적절한 연결방식이 될 수 있다.

2.2. PUSH 서비스 설계

본 논문에서는 PUSH서비스 설계를 아래와 같이 하였다. 일반 음성통신의 특성을 가지는 모바일 단말기에 부가적인 기능인 SMS와 RAS로의 데이터 연결을 통한 두 개의 채널을 적절히 혼합하여 설계 하였다.

그림 1에서 ①은 원하는 PUSH 서비스의 형태와 자신 단말기 번호와 같은 개인 정보를 등록하는 단계이다. ②는 PUSH 데이터 생성 단계이다. 이는 정해진 시간이 아니기 때문에 이벤트라는 명칭으로 했다. ③은 오프라인상태의 단말기를 호출하는 단계이다. 이때 서버 쪽의 어떠한 메시지가 도착했을 지와 서버의 주소를 알려주고 이를 받기 위한 준비를 하는 과정이다. ④는 SMS로 온 데이터를 기준으로 접속을 시도하여 데이터 채널을 만든다. ⑤의 단계에서 사용자에게 원하는 데이터를 PUSH 해 준다.

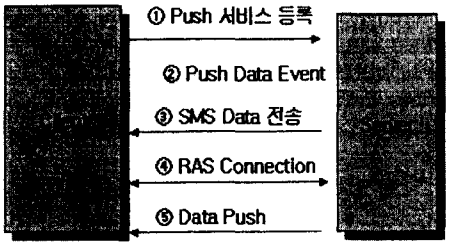


그림 1. PUSH 서비스 설계
Fig.1 Design of PUSH service

①의 단계는 서비스를 받기위해 한번만 시행 할

뿐이고 실제 PUSH 서비스의 중심이 되는 통신은 ③④⑤의 단계이다. 3번의 통신횟수를 거쳐야 하는 이유는 오프라인의 PDA 단말기를 온라인으로 만들어야 하기 때문에 ③④의 과정이 필요하기 때문이다.

2.3 PUSH 서비스 구현

본 논문에서 PUSH 서비스의 구현은 PDA 단말기를 윈도우즈 CE 3.0 OS를 가지는 iPAQ을 이용하였으며 PUSH 서버와 SMS 서버, 콘텐츠 서버는 윈도우 2000으로 구동되는 Pentium III-1G Hz CPU급의 PC로 구현하였다. 그 외에 SMS를 위한 셀룰러 단말기도 사용하였다. 실제 SMS 데이터와 데이터 연결도 실제 RAS서비스를 통해 구현하였다.

그림2의 단계 ①은 PUSH 서비스를 위한 등록 단계이다. 자신의 PDA 단말기의 번호($ID_{[A]}$)를 서버 쪽에 등록한다. 이 단계는 최초 서비스를 위한 등록단계이므로 전체 서비스에서 1회 실행된다. 또한 유선 인터넷 서비스를 통해서 등록하거나 또는 PDA 단말기에서 직접 등록할 수 있다. 통신 방법은 데이터 채널을 이용한다. 단계 ②는 등록된 단말기의 번호($ID_{[A]}$)를 DB에 삽입한다. 단계 ③은 PUSH 데이터 생성단계로 수시로 발생하는 PUSH 데이터($PUSH\_Data_{[A]}$)를 원하는 서비스 사용자의 단말기 번호($ID_{[A]}$)와 함께 콘텐츠 DB에 저장한다. 단계 ④에서 콘텐츠 DB의 삽입과 동시에 같은 트랜잭션으로 트리거 명령을 통해 SMS DB에 PUSH 데이터의 번호($ID\_PUSH\_Data_{[A]}$)와 단말기 번호($ID_{[A]}$)를 삽입한다. 단계 ⑤는 이 데이터를 SMS 서버에 전송한다. 단계 ⑥은 SMS 서버가 SMS 채널을 통해 단말기 번호($ID_{[A]}$)를 참조하여 콘텐츠 서버의 주소($ID_{[content\_server]}$)와 PUSH 데이터의 번호($ID\_PUSH\_Data_{[A]}$)를 함께 전송한다.

단계 ⑦은 단계 ⑥에서 받은 SMS 데이터를 처리한 후 콘텐츠 서버의 주소($ID_{[content\_server]}$)를 참조하여 RAS 연결을 생성한다. 이로써 데이터 채널이 생성된다. 단계 ⑧을 생성된 데이터 채널을 통해 콘텐츠 DB에서 단말기 번호($ID_{[A]}$)에 해당하는 PUSH 데이터 ($PUSH\_Data_{[A]}$)를 콘텐츠 서버에서 준비한다. 단계 ⑨를 통해 사용자 단말기($ID_{[A]}$)에 PUSH 데이터를 전송함으로써 PUSH 데이터를 전송하고 데이터 채널의 연결을 끊는다.

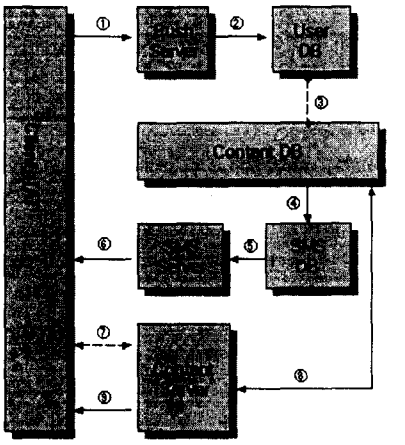


그림 2. PUSH 서비스 구현
Fig.2 Implementation of PUSH service

III. 보안 프로토콜 설계 및 구현

3.1 PDA PUSH 서비스를 위한 보안 프로토콜

PDA 단말기에서 많은 데이터 흐름을 가지게 될 PUSH 서비스는 특성상 개인적인 성향의 정보를 많이 가지게 될 것이다. 그러나 모바일 단말기 PUSH 서비스는 다음과 같은 문제를 가지고 있다 [7].

첫째, PDA 단말기가 가지는 저 용량성과 저 처리능력이다. 이는 안전한 보안 방식을 사용하기에는 너무도 많은 작업시간과 작업공간을 필요로 한다. 둘째, 공중망 통신을 이용하기 때문에 도청이 쉽다. 이는 공중망 특성으로 인한 어디서나 도청이 가능하다는 관점뿐 아니라 PUSH 서비스가 가지는 개인적인 정보의 남용으로 이어 질 수 있다. 셋째, 위장에 의한 접근이 가능하다. 제 3자가 SMS 메시지를 받은 것처럼 위장하여 콘텐츠 서버에 접근하여 PUSH 정보를 받아갈 수가 있다.

그림3은 본 논문의 서비스를 위한 보안 알고리즘이다. 단계는 다음과 같다. 클라이언트는 RSA 알고리즘을 이용하여 개인키($KR_{[C]}$)와 공개키($KU_{[C]}$)를 생성한다. 생성된 공개키($KU_{[C]}$)를 서버에 등록하고 서버로부터 서버의 공개키($KU_{[S]}$)를 얻어온다. 임의의 수($ID_{[RANDOM]}$)를 생성하여 서버 쪽으로 보낸다. 이때 자신의 개인키($KR_{[C]}$)와 서버의 공개키($KU_{[S]}$)로 암호화하여 보낸다. 서버와 클라이언트는 정의된 Round Hash 함수를 통해 비표(Nonce Table)를 생성한다. 이후 PUSH 메시지가 발생 할 때 마다 서버는 SMS 채널을 통해 비표번호를 기존 정보와 같이

전송하고 데이터 채널이 생성되면 SEED 암호화를 통하여 비표 번호에 근거한 세션 키로 통신한다[5]. 비표를 생성하기위한 임의의 수($ID_{[RANDOM]}$)는 데이터가 전달되는 동안 사용자가 원할 때나 시간적 주기를 두고 가동적으로 생성시키어 비표를 변경하면서 사용할 수 있다.

본 연구에서 구현한 보안 프로토콜은 초기등록단계, 비표생성단계, PUSH 서비스 단계 로 동작한다. 그림3은 구현된 보안프로토콜을 나타낸다.

초기등록단계는 PUSH 서비스를 받기 위한 서비스 등록 단계로 다음과 같이 진행된다.

클라이언트에서는 RSA알고리즘에 의해서 공개키($KU_{[C]}$) $Client_{[n,e]}$와 개인키($KR_{[C]}$)가 생성된다. 역시 서버 쪽도 같은 방식으로 공개키($KU_{[S]}$) $Server_{[n,e]}$와 개인키($KU_{[S]}$)를 준비한다. 첫 등록단계에서 클라이언트는 서버 쪽에 공개키($KU_{[C]}$) $Client_{[n,e]}$를 전송하고 서버 쪽에서는 클라이언트에게 공개키($KU_{[S]}$) $Server_{[n,e]}$를 전송한다.

비표 생성단계는 안전한 세션키를 생성하기 위한 비표 생성단계로 64개의 비표를 만든다. 비표를 생성하기 위한 첫 ID값은 클라이언트로부터 임의로 만들어진 수를 받는다. 하지만 이 단계의 정보가 중요한 만큼 RSA의 암호화와 복호화를 이용한다. 클라이언트는 임의의 수($ID_{[RANDOM]}$)를 생성한다. 생성한 임의의 수는 클라이언트의 개인키($KR_{[C]}$) $Client_{[n,d]}$로 암호화 한다.

$$KR_{[C]}(ID_{[RANDOM]})=ID_{[RANDOM]}{}^{d} \bmod n \equiv ID_{[KR\_C]}$$

다음 단계는 서버의 공개키($KU_{[S]}$) $Server_{[n,e]}$로 암호화 한다.

$$KU_{[S]}(ID_{[KR\_C]})=ID_{[KR\_C]}{}^{e} \bmod n \equiv ID_{[KR\_C||KU\_S]}$$

이와 같은 과정으로 도착한 메시지를 서버 쪽에서는 자신의 개인키로 복호화하고 다시 클라이언트의 공개키로 복호화 함으로써 원래의 임의 수($ID_{[RANDOM]}$)를 알 수 있다.

마지막으로 PUSH 서비스 단계는 PUSH메시지를 전송하는 단계에서 이루어진다. PUSH 서비스의 속도를 향상시키기 위해 준비된 비표를 사용한다. 또한 보다 안전한 통신을 위해 비표의 번호는 SMS 채널을 이용하고 PUSH 데이터는 데이터 채널을 이용한다.

SMS 채널로 온 데이터에는 서버 쪽의 콘텐츠 서버의 주소와 PUSH 메시지의 번호가 들어있고 또한 보안을 위한 비표 번호가 들어있다. 이에 클라이언트는 해당 서버에 접속하여 서버로부터 온 데이터를 받는다.

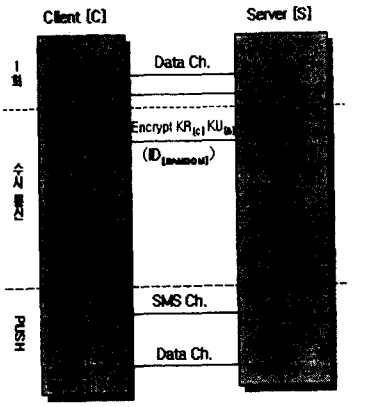


그림 3. 모바일 PUSH 서비스를 위한 보안 프로토콜
Fig.3 Secure protocol for mobile PUSH service

받은 데이터는 SEED로 암호화 되어있지만 서버와 같이 약속된 비표 번호에 해당하는 비표파일의 인덱스 번호에 해당하는 비표내용이 받은 데이터의 SEED암호의 키가 된다[5].

3.2 시스템 구성

본 연구에서 제안한 시스템은 PUSH 서버와 클라이언트로 나눌 수 있다

PUSH 서버는 두 개의 시스템으로 구성 되어있다. 콘텐츠DB, SMSDB, UserDB를 갖춘 윈도우 2000 서버 컴퓨터와 SMS 셋톱박스가 연결되어 SMS전송을 담당한다. SMS데이터는 SMS DB와 연동되어 발송하게 되며 콘텐츠DB는 유선망 접속으로 데이터를 전송 할 수 있다.

PUSH 클라이언트는 SMS 데이터를 받을 수 있도록 무선 모뎀이 장착되어 있어야 하며 이 응답을 처리 할 수 있도록 모뎀과의 연결 포트에 대한 처리가 되어 있다. 본 논문에서는 iPAQ을 모델로 SKT의 nate 모듈, 019 i-kit 모듈이 구현되어 있다. 또한 PDA의 특성인 절전모드로 인한 시스템 슬립 타임에도 SMS 메시지를 받으면 슬립 타임에서 깨어 날 수 있도록 wake up 구현 하였다. 본 연구에서 제안한 서버와 클라이언트에 탑재한 보안 모듈은 각각 RSA키 생성모듈, Round Hash 모듈, SEED 파일단위 처리 모듈로 구성되어 있다.

IV. 성능 분석 및 평가

본 논문에서 제안한 알고리즘에 사용된 암호 방

식은 3가지로서 PUSH 채널을 개시하기 위한 세션 키로서의 RSA 알고리즘과 데이터 송수신시 보안을 위한 SEED 알고리즘, 그리고 비표를 생성하기 위하여 MD5 함수를 사용하였다. 이 메커니즘들이 제안된 보안 프로토콜의 수행과정에서 각 각 담당하는 부문의 역할 및 의의를 밝힘으로써 프로토콜이 가지는 보안요소측면의 분석을 하였다. 그리고 제안된 프로토콜을 이용하여 수 Kbyte부터 10Mb의 데이터 전송 시 클라이언트 단말인 PDA에서 암호화, 복호화에 걸리는 시간측정을 통하여 제안된 보안프로토콜의 동작 특성을 평가 하였다.

4.1. 암호화 프로토콜 분석 및 평가

RSA 알고리즘의 역할은 처음 가입자가 자신의 클라이언트에서 생성한 공개키와 비밀키를 생성하고 서버측도 공개키와 비밀키를 생성한다는 것이다. 이를 이용하여 PUSH 서비스를 개시하기위한 데이터 채널을 사용 한다. 이는 공개키 기반 구조 형식을 취하므로 부인 방지의 역할을 할 수 있을 뿐 아니라 보내고자 하는 객체는 자신의 비밀키와 상대방의 공개키를 이용함으로써 인증의 역할을 동시에 수행할 수 있다. 차후 이 방식을 이용해 자신만의 디지털 서명도 보낼 수 있는 좋은 방법이 될 수 있다.

SEED 알고리즘을 세션 통신에 사용한 이유는 타 알고리즘에 비해 속도가 빠르다는 장점과 블록 형태의 알고리즘이므로 데이터 통신용으로 적합하다고 판단하였기 때문이다. 또한 SEED는 국내 표준으로 지정되어 있기 때문에 차후 다른 서비스와 혼용되어 질 때 본 알고리즘을 그대로 적용시킴으로써 호환성을 유도했다.

MD5 알고리즘은 메시지를 간소화하거나 인증코드 등의 목적으로 사용한 것이 아니라 임시비표를 생성함에 있어 보다 분포가 다양한 형태의 암호키를 생성하기 위해 사용하였다. 제3자의 공격 형태에 세션 키 공격을 감안한 형태로 임의의 값들과 동시에 생성된 비표는 전혀 중복되는 키가 나타나지 않는다.

4.2. 프로토콜 분석 및 평가

논문에서 제안한 시스템이 공격 당할 수 있는 몇가지 공격 형태에 대해 대처능력을 유형별로 분석해 보았다.

Unknown Key share 공격 : 사용자들 간의 동일한 공개키가 존재할 경우 발생할 수 있는 공격 형태로 본 논문에서 제안한 방식에서는 사용자간에 실제 동일한 공개키가 존재하더라도 비표생성을 위한 아이디 생성부분과 비표에서 서로 다른 키 값을 나타내므로 동일한 공개키에 의한 공격에 대해 대처할 수 있다.

세션 키 공격 : 세션 키를 사용자가 임의로 추론하여 공격하는 방식이다. 본 논문에서 세션 키의 설정은 128bit 출력을 기반으로 한 임시비표에서 임의로 선택되기 때문에 2128개의 세션 키를 가진다. 이는 공격을 시도의 횟수와 이를 해독하는데 정보를 보호할 만큼 많은 시간을 소요하게 된다.

키 전송단계에서의 공격 : 키의 전송을 비대칭 방식인 RSA 알고리즘을 사용하여 안전 할 뿐 아니라 데이터 채널과 SMS 채널을 동시에 이용하므로 공격자의 데이터 채널 공격만으로는 원하는 키를 얻을 수 없다.

위장 공격 : 가입자가 아닌 제3의 공격자가 자신을 정당한 가입자로 속여 공격하는 방법이다. 하지만 서버 측에서 클라이언트의 공개키와 클라이언트 쪽에서 가지는 자신만의 비밀 키를 소유함으로써 제 3자는 확인이 안 되는 객체가 되어 버리므로 위장 공격에 대처할 수 있다. 다시 말해 본 논문에서 제안한 프로토콜은 인증의 역할도 동시에 할 수 있다.

부인방지 : 이동 단말기의 부하를 최소화 하기위한 방법으로 프로토콜상의 암호 메커니즘에 의한 부인 방지 대책이 고려되진 않았다. 그러나 사용자가 PUSH서비스를 받은 메시지를 안 받았다고 부인할 경우 이는 SMS의 데이터 전송 기록과 사용자가 받아간 콘텐츠 DB 안의 2가지 정보가 동시에 유지되므로 이를 알 수 있을 뿐 아니라 해당 비표를 가지지 않은 사람은 데이터를 받더라도 쓸모없는 정보가 된다.

4.3. 성능분석

본 논문에서 제안한 방식이 실제 PDA 단말기에서 구동되는 시간을 측정해 보았다.

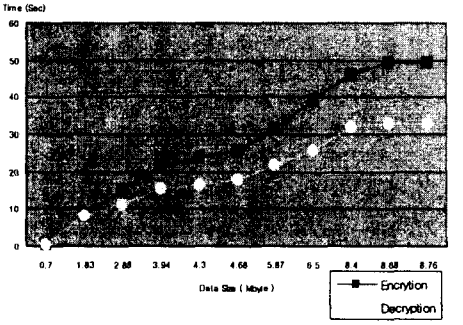


그림 4. PDA의 데이터 암호화 복호화 시간
Fig.4 Data processing time of PDA

그림 4는 데이터 량에 따른 PDA에서의 암호화 시간과 복호화 시간을 측정한 결과이다. 데이터가 7 kbyte 이하에서는 0.5초 이하로 측정되었으며 1.83Mbyte 이상이 되면 8초 정도로 사용자가 기다리기에는 적지 않은 시간이 된다.

모바일 단말기의 암호화 시간과 복호화 시간은 데이터 량이 1M 이하일 경우 1초 정도의 소요 시간이 걸리며 이는 사용자가 수용할 수 있는 시간이다. 모바일단말기에서 서비스되는 데이터가 대부분 문서나 그림과 같은 작은 사이즈의 데이터임을 감안할 때 충분히 사용자가 사용하기에는 적절한 시간이 될 수 있다.

또한 복호화 하는 시간이 암호화하는 시간보다 빠르다는 것을 확인 할 수 있다. 이는 모바일 단말기에서 PUSH서비스를 위한 좋은 장점이 될 수 있다. 하지만 구현된 PDA 단말기만으로 측정하였기 때문에 좀 더 다양한 단말기에서의 실험이 필요하겠다.

V. 결론 및 향후과제

본 논문은 모바일 푸시 서비스를 기준으로 하여 작성하였으며 이에 적절한 보안 요소를 위해 상용 알고리즘 중 안전한 형식을 따르는 비대칭 형식의 RSA와 데이터 통신의 고속화를 위한 SEED 방식을 취함으로써 저 사양 저속 모바일 환경에서 안전하면서 빠른 속도의 성능을 발휘하는데 초점을 맞추었다. SEED방식에서 데이터의 암호화 및 복호화에 사용될 비표를 양단에서 일정 주기 마다 생성하여 등록 시켜 놓고 데이터 전송 시 비표의 인덱스만을 전송에 이용함으로써 양단에서의 데이터 송수신 량을 줄이는 효과를 얻었다.

PDA PUSH 서비스는 주로 작은 크기의 그림이나 텍스트 기반의 소량의 정보 전달이 주가 되며 본 연구에서 1 Mbyte 이하의 데이터 처리 시간을 측정해 본 결과 1초미만의 결과를 얻었다. 이 결과는 사용자가 충분히 수용할 수 있는 정도이며 실제 사용이 가능하다는 것을 보여준다.

본 연구에서는 최초 연결 생성 시 서버와 클라이언트의 공개키를 분배하여 주는 키 분배 센터를 이용하지 않았다. 이 부분은 상용화 될 경우 공인된 인증기관을 통해 해결해야 하는 부분이라 여겨진다. 그리고 PDA 단말기를 위한 특성화된 PUSH 서비스만을 기준으로 작성한 보안프로토콜로서 좀 더 확장된 형식의 보안 서비스를 위해서는 상호 통신을 위한 보안 요소도 구비되어야 할 것이다.

본 논문에서 PDA 단말기를 Pocket PC로 한정했지만 다른 플랫폼에서도 원활히 동작하도록 이에 적절히 변형되어야 하는 것도 또 하나의 향후 과제로 남는다.

참고문헌

[1] LAN MAN Standards Committee of IEEE Computer Society, Wireless LAN Medium access control(MAC)and physical layer(PHY) specification, IEEE Standard 802.11, 1999 edition, 1999.

[2] William A. Arbaugh, N. Shankar, and Y.C. Justin Wan, "Your 802.11 Wireless Network has No Clothes", In Proceedings of the first IEEE International Conference on Wireless LANs and Home Networks, December 2001.

[3] KISA, 128-bit Symmetric Block Chiper (SEED), TTAS.KO-12.0004, 28, sep. 1999.

[4] RFC 2437, B. Kaliski, J. Staddon, "RSA Cryptography Specifications Version 2.0", October 1998.

[5] TTA.KO-12.0004 "128비트 블록암호알고리즘 표준", 한국정보통신기술협회, 1999년 9월.

[6] 우원택, "전자상거래에서의 RSA 알고리듬의 분석과 구현", 한국정보시스템학회, 2000년도 춘계학술대회 발표논문집, 2000.

[7] 김성열, 정일용, 오명옥, 배용근, "효율적인 그룹키 분배 및 갱신을 위한 보안 프로토콜의 설계", 한국정보처리학회논문지, 2002.

[8] 최용락, 소우영, 이재광, 이임영 역, ",컴퓨터 통신 보안", 도서출판 그린, 2002.

[9] William Stallings, "Cryptography and Network Security Principles and Practice 2ed", 1999.

[10] 이정배, 이두원, "임베디드 시스템 연구 동향", 정보처리 학회지 특집 제9권 1호, 2002. 1.

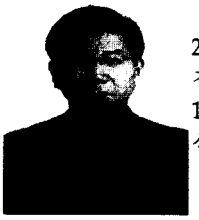
[11] 김기천, "모바일 서비스 기술 동향", 정보처리 학회지 특집 제9권 2호, 2002. 3.

[12] 이은주, "RSA 암호의 구현", 고려대학교 교육대학원, 2001. 11.

[13] Douglas Boling, "Programming Windows CE 2nd ed.", 정보문화사, 2002. 1.

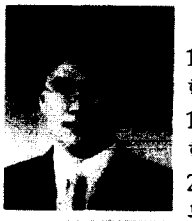
[14] 고재관, "Mobile PDA Programming", 삼각형프레스, 2001. 8.

저자소개



이기영 (Ki Young Lee)

2004년 한국해양정보통신학회 논문집 제 8권 8호 참조
1994년3월-현재 인천대학교 정보통신공학과 교수



이정균(Jeong Kyoon Lee)

1993-1997 수원대학교 전기공학과 학사
1998-2001 인천대학교 정보통신대학원 정보통신공학 석사
2001-현재 인천대학교 대학원 정보통신공학과 박사과정
1997-2001 신화전자 주식회사 부설연구소 연구원
2003-현재 TNFE 대표이사