Journal of Korea Multimedia Society Vol. 7, No. 11, November 2004(pp. 1610-1619)

블루투스를 이용한 안전한 지불 시스템 모델에 관한 연구

서대희[†], 강서일[††], 이임영[†††], 박해룡[††††]

요 약

최근 근거리 무선 통신에 대한 연구가 활발히 진행되면서, 사용자 중심의 모바일 디바이스를 중심으로한 근거리 무선통신의 많은 응용 분야에 대한 연구가 진행중에 있다. 블루투스는 기존 근거리 통신이 갖고 있지 않는 여러 가지 장점들을 가지고 있다. 표준화와 관련하여 SIG와 IEEE에서 연구가 진행중 있으며, 다양한 환경의 응용 분야에 적용하기 위한 노력이 지속되고 있다. 따라서 본 논문에서는 블루투스의 여러 가지 응용 기술 중 블루투스를 이용한 지불 시스템을 제안한다. 제안방식은 사용자를 중심으로 안전한 피코넷을 형성하고 사용자가 자신의 승용차에 승차하여 자신의 모바일 디바이스 기기를 이용하여 주유소에서 자동차에 주유를 한 뒤 이를 결재하는 시나리오를 기반으로 한다. 또한 기존 블루투스가 가지는 보안적 취약점 뿐만 아니라 근거리 무선 통신을 이용한 지불에 필요한 여러 가지 보안적 요구사항을 만족할 수 있는 안전한 지불 시스템을 제안하였다.

A Secure on the Design Model of the Payment System on Bluetooth

Dae-Hee Seo[†], Se-Il Kang[††], Im-Yeong Leem[†††], Hea-Ryong Park[††††]

ABSTRACT

While researches and studies on short distance wireless communications have been actively carried out, studies on many applications of short distance wireless communications focusing on user-oriented Mobile device are also in progress. Since Bluetooth has several advantages that existing short distance communication does not have, studies on standardization have been carried out focusing on SIG, and IEEE has also jointly studied on this. Bluetooth is a short distance wireless communication technology that can be usefully applied to various kinds of applications. In this regard, this thesis presents payment system using Bluetooth, out of several application technologies of Bluetooth. This payment system is based on the scenario in which secure piconet is formed focusing on the user, the user gets in the car, fill up the gas at the gas station using his own Mobile device and pay. The secure payment system presented in this thesis is designed to complement the weakness of existing Bluetooth in terms of security and to secure several requirements of security required for payment using short distance wireless communication.

Key words: Mobile Commerce(모바일 상거래), Bluetooth Payment System(블루투스, 지불 시스템)

※ 교신저자(Corresponding Author) : 서대희, 주소 : 충남 아산시 신창면 읍내리 646(336-745), 전화 : 041)542 - 8819, FAX : 041)530-1494, E-mail : patima@sch.ac.kr
접수일 : 2004년 1월 12일, 완료일 : 2004년 5월 31일
[†] 준회원, 순천향대학교 대학원 전산학과 박사과정
[††] 준회원, 순천향대학교 대학원 전산학과 석사과정
(E-mail : kop98@sch.ac.kr)
[†††] 종신회원, 순천향대학교 정보기술공학부 부교수
(E-mail : imylee@sch.ac.kr)
[††††] 정회원, 한국정보보호진흥원
(E-mail : kcdsa@kisa.or.kr)

1. 서 론

동전과 지폐로 대별되던 화폐에 신용카드가 나오면서 화폐의 혁명이 시작되었다. 이른바 플라스틱 머니로 불리며 급속한 확산속도를 보이던 신용카드는 국민 1인당 1장 이상을 소유할 정도로 대중화된 화폐로 자리 잡고 있다. 최근에는 정보통신 및 컴퓨터 기술의 발달로 신용카드, 전자 자금 이체, 인터넷 뱅킹 등 현금대체 결제 수단이 보편화되고 있다[19,20].

한편 기술 발전과 인터넷에 대한 이용자의 폭발적인 증가에 힘입어 간단한 메시지 송·수신 단계에 머물던 무선 인터넷 서비스는 이제 기업 업무용으로까지 서비스 폭이 확대되고 있다. 따라서 무선 인터넷 시장에서 컨텐츠 유료화에 따른 수익 창출에 대한 기대가 모아지고 있는 가운데 근거리 무선 통신을 이용한 무선 전자상거래(M-Commerce)가 이슈로 부각되고 있다.

이처럼 인터넷 환경에서 유·무선 전자상거래가 활발하게 이루어지고 있지만 지불 수단의 미비로 인해 전자상거래 활성화를 저해하는 요인으로 지적되고 있다. 따라서 무선 전자상거래에서 안전하고 신뢰할 수 있는 전자화폐 시스템의 개발이 시급하다[5]. 국내외적으로 무선 전자 상거래 시스템에 신뢰할 수 있는 전자화폐 시스템 개발과 관련하여 사용자의 휴대 단말기를 기반으로 이루어지는 다양한 형태의 지불 시스템이 개발되고 있으나, 실제 블루투스 적용에 따른 안전성 보다는 적용성에 그 목적을 두어 연구되고 있어 사용자의 프라이버시 침해에 따른 안전성을 보장할 수 없는 문제점이 발생하고 있다[14,15].

따라서 본 논문에서는 무선 전자 상거래에서 요구되는 전자화폐 시스템 개발의 필요성에 의해 최근 근거리 무선 통신의 표준으로 자리 잡고 있는 블루투스를 이용하여 안전하고 신뢰할 수 있는 지불 시스템을 제안하였다.

본 논문의 2장에서는 최근 많은 연구가 진행중에 있는 블루투스와 무선 전자상거래를 위한 지불 시스템의 개요에 대하여 살펴본 뒤, 3장에서는 관련 연구로 기존 지불 시스템에 대한 취약성과 블루투스의 보안적인 취약점에 대해 분석하고 블루투스를 이용한 지불 시스템에서 요구되는 보안 요구사항에 대해 기술한다. 4장에서는 기존 시스템의 보안적 취약점을 보완하면서, 블루투스를 이용한 안전한 전자 지불 시스템을 제안하고, 5장에서는 3장에서 제시된 보안 요구사항을 기반으로 제안 방식을 분석한뒤 6장에서 결론을 맺고자 한다.

2. Technology Review

블루투스는 1994년 에릭슨의 이동통신그룹이 휴대폰과 주변기기 사이의 소비전력이 낮고, 가격이 싼 무선 인터페이스를 연구하기 시작하면서 비롯하였다. 그 후 에릭슨, 노키아, IBM, 도시바, 인텔, 모토로라, 마이크로 소프트, 루슨트 테크놀로지, 3COM 등이 설립한 SIG(Special Interest Group)를 중심으로 표준화를 추진중에 있다. SIG는 현재 2000여개 이상의 기업들이 회원으로 가입된 상태이며, 국내 참여 기업도 70여 곳에 이르고 있다[4].

블루투스 표준은 99년 버전 1.0을 발표한 이래로 2001년에 버전 2.0을 공개할 예정으로 있었으나, 현재까지 공개는 안되고 있는 실정이다.

현재까지 블루투스는 발전하는 단계에 있으며, 블루투스의 무한한 잠재력을 믿고 국내의 기업 뿐만 아니라, 세계의 우수 기업들이 연구를 지속하고 있다. 그러나 현재의 블루투스는 많은 부분의 보완을 필요로 하고 있다. 기존의 가전기기에 설치하여 사용하기 위해서는 단가를 낮추어야 하고 짧은 전송거리도 늘려야 한다. 또한 간단한 데이터 전송과 음성 전송만을 할 수 있지만, 화상회의 등 고속의 데이터 전송량을 필요로 하는 장소에서 사용하기 위해서 데이터 전송량을 늘릴 수 있는 방법도 개발되어야 한다. 블루투스를 이용한 통신에서 중요한 특징은 블루투스 네트워크 형성을 지적할 수 있다. 이러한 네트워크는 특별한 목적을 위하여 생성되는 네트워크로서 모든 장치들은 무선으로 서로 연결된다. 개인적인 디바이스들은 다른 장치들에 메시지들을 브로드 캐스팅할 때 장치들간에 직접적인 메시지를 받기 위해서는 장치들간에 거리가 문제시된다[5].

이는 모바일적인 특성을 가진 장치들이 다른 장치들간의 전달 범위의 안팎으로 움직일 때 유동성을 가진다. 블루투스 통신을 통한 네트워크 형성의 특성상 매우 특별한 목적을 위하여 형성된 네트워크이며, 공격에 취약한 구조를 가지고 있어 복잡한 보안이 필요하게 된다.

일반적인 무선 인터넷의 경우 공중망(PSTN : Public Switch Telephone Network) 혹은 인터넷망으로 접속한 후 보안 과정을 거치는 형태로 서비스가

이루어진다. 따라서 유선 인터넷 보다 더 많은 불법 해킹이나 개인정보 유출과 같은 문제가 발생할 수 있다. 국내에서 사용하는 무선 기술은 보안성이 뛰어난 코드분할다중접속(CDMA : Code Division Multiple Access)방식을 채택하고 있지만 사용자의 안전한 무선 인터넷 서비스 제공을 위해서는 현재의 보안 서비스보다 향상된 보안 모듈이나 솔루션이 필요하며, 무선 지불 분야도 무선 인터넷에서 해결해야 할 주요 과제 중 하나다. 디지털 정보뿐 아니라 쇼핑몰 등을 통해 물건을 사고 팔 때 결제 서비스가 제대로 지원되지 못하면 서비스 자체가 힘들기 때문이다. 지불 서비스 역시 기지국과 연동된 별도의 지불, 결제 게이트웨이나 시스템을 통해 가능하다. 물론 이를 위해서는 WAP와 같은 무선 프로토콜에 기반한 솔루션 개발이 뒤따라야하며, 유선 인터넷과 같이 사이버 공간에서 사용할 수 있는 전자화폐, 전자지갑 등 각종 전자화폐도 요구된다[3,19].

3. 기존 방식 분석 및 블루투스 지불 시스템의 보안 요구사항

3장에서는 블루투스를 이용한 안전한 전자 지불 서비스를 제안하기 위해 기존 무선 전자 지불 시스템에 대한 보안 분석과 블루투스에 대한 보안 취약성 분석을 수행한 뒤 블루투스를 이용한 전자 지불 시스템에서 요구되는 보안 요구사항을 제시하고자 한다.

3.1 기존 방식 분석

(1) Secure Wireless Payment Protocol (SWPP 방식)

Hong Wang외 1명이 제안한 논문으로써 WAP을 기반으로한 안전한 형태의 지불 서비스를 제안하였다. 제안된 방식은 기존 WTLS에서 End-to-End 보안 서비스를 제공하지 못해 발생 되는 보안 취약점을 해결한 제안방식이다[2]. 그러나 제안 방식의 경우 다음과 같은 보안 취약성을 지적할 수 있다.

① 전송 데이터에 대한 기밀성과 무결성 : 기존 WTLS v1.0에서 제시되고 있는 문제점 중 게이트웨이에서 발생할 수 있는 기밀성과 무결성의 문제성을 신뢰할 수 있는 은행 기반의 게이트웨이로 설정함으로써 End-to-End 서비스를 제공하고자 하였다. 따라서 은행에서는 개인의 프라이버시 정보 및 지불 정보에 대한 모든 내용을 획득할 수 있다. 이는 개인의 프라이버시를 침해하는 매우 중요한 취약점이다.

② PIN에 대한 인증의 문제점 : 제안된 방식의 경우 PIN에 근거한 서명값 생성으로 은행의 게이트웨이에서는 사용자의 PIN을 획득할 수 있을 뿐만 아니라 이를 기반으로 인가 메시지를 송신함으로써 공격자가 서명값을 획득하여 공격자의 서명값으로 변경하였을 경우 게이트웨이에서는 이를 확인할 수 없는 문제점이 발생한다.

(2) Sonera Mobile Payment (SMP 방식)

SMP 방식은 핀란드 통신그룹 Sonera에서 제안한 방식으로 모바일 전자 지불 시스템을 오프라인 형태로 제공하는 방식이다. SMP 방식의 경우 사용자의 휴대용 디바이스를 신뢰할 수 있는 기기로 가정하고 SMS(Short Message Service)를 이용한 모바일 지불 서비스를 제안하였다[18]. 그림 1은 전체의 흐름도 이다. 그러나 본 방식의 경우 다음과 같은 문제성을 지적할 수 있다.

① 사용자의 인증 : 본 방식의 경우 휴대용 디바이스에 대한 인증만을 수행한다. 따라서 휴대 단말기를 사용하는 사용자의 인증이 추가적으로 요구된다. 이는 모바일 통신 기술에서 매우 중요한 인증과정으로 제기되고 있다.

② 전송 데이터에 대한 기밀성과 무결성 : 제안된 방식의 경우 사용자의 프라이버시 메시지에 대한 기밀성과 무결성 서비스가 이루어지지 않는다. 이는 현재 휴대용 디바이스를 이용하고 있는 지불 시스템이 소액 지불을 위한 방식이기 때문이다. 따라서 휴대용 디바이스를 이용한 고액 지불을 위해서는 기밀성과 무결성이 추가적으로 요구되는 보안 요구사항이다.

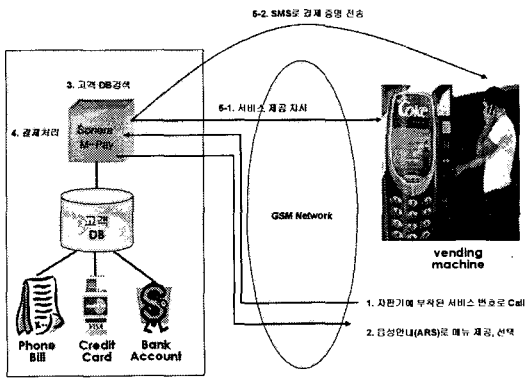

그림 1. SMP 방식 흐름도

3.2 블루투스 취약점 분석

블루투스가 가지는 취약점은 실제 블루투스를 적용하였을 때 나타나는 취약점과 기술내역서 자체가 가지는 취약점으로 구분하여 볼 수 있으며, 실제 적용시 예측되는 공격은 다음과 같다.(그림 2참조)

(1) 블루투스를 실제 적용시 예측되는 공격

블루투스를 실제 적용 하였을때 그림 2의 ①과 같은 공격이 이루어 질 수 있으며 이러한 공격 중 PIN에 대한 공격을 제기할 수 있다[16,17].

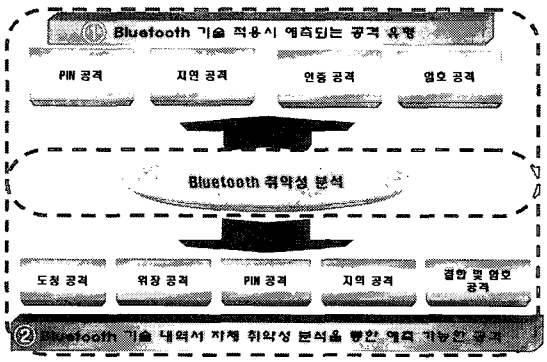

그림 2. 블루투스 적용시 예측되는 공격

- 암호화된 디바이스간의 통신을 도청과 PIN 공격

일반적으로 블루투스를 통해 당사자들이 중요한 통신을 하기 위해 상호간이 동의하에 암호화된 통신이 이루어진다. 블루투스의 적용시 예측되는 취약점은 디바이스들이 한 쌍이 되는 동안에 교환된 메시지들에 대한 도청을 할 수 있다는 것이다. 즉, 블루투스 계층에서 응용 프로그램 계층으로 암호화가 수행되지 않으면 공격자는 Man-in-the-middle-attack이 가능하다.

(2) 블루투스 기술 내역서 1.1의 취약성 분석

블루투스 기술 내역서에서 제공하고 있는 보안 서비스는 그림 2의 ②와 같은 5가지의 공격에 대한 보안 취약성을 가지고 있으며, 도청과 위장 공격 및 오프라인 PIN 공격에 매우 취약하다. 따라서 실제 피코넷이나 스캐터넷이 구성되었을 경우 보안 취약성이 발생할 수 있다[10,14,15].

- 도청과 위장 공격

근본적으로 키 생성 프로토콜이나 키 생성에 대한 프로토콜로서 블루투스의 키 생성 방식은 난수와 PIN 그리고 블루투스 디바이스 주소를 이용하여 계산된다. 만약에, PIN이 유효하지 않거나 유닛간에 전송이 안된다면 공격자는 이를 쉽게 알아낼 수 있다. 이러한 취약점은 PIN의 길이를 충분히 길게하여 보완할 수 있다.

3.3 블루투스 지불 시스템의 보안 요구사항

현재의 블루투스 기술은 사용자의 중심이 되는 모바일 디바이스간에 이루어지는 무선 통신 서비스이다.

따라서 블루투스를 무선 지불 시스템에 적용하기 위해서는 사용자의 프라이버시 보호를 위해 여러 가지 보안적인 요구사항이 필요하며, 이는 다음과 같다.

• 무결성 : 블루투스를 이용해 지불이 이루어질 경우 지불 정보 데이터에 대한 무결성이 보장되어야 한다. 그러나 블루투스 자체 제공 서비스에서는 무결성을 위한 보안 서비스를 제공하지 않는다.

• 기밀성 : 지불 데이터에 대해 기밀성이 보장이 이루어져야 한다. 그러나 블루투스 자체 제공 서비스에서 제공하는 기밀성 서비스는 보안 키에 의존하고 있으나 보안 키를 생성하는 PIN 번호에 대한 길이 및 보안 키 분배가 이루어질 때 Man-in-the-middle attack에 대한 보안 서비스가 반드시 요구된다.

• 부인봉쇄 : 블루투스를 이용하여 상호간 지불 사실에 대한 부인을 막을 수 있는 부인 봉쇄가 이루어져야 한다. 현재의 블루투스에서는 기기에 대한 인증은 이루어지나, 사용자에 대한 인증은 이루어지지 않는다.

• 상호인증 : 지불이 이루어지는 각 객체들간에 상호 인증을 통하여 안전한 지불 관계가 이루어지도록 해야 한다. 블루투스 기술 내역서에서는 객체들에 대한 인증이 이루어지지 않을 뿐 아니라 단지 조회 과정을 거쳐 블루투스 통신이 가능한지에 대한 과정만을 수행한다.

• 검증성 : 신뢰할 수 있는 제 3자에 의한 송수신 데이터에 대한 검증이 가능해야 한다.

4. 블루투스를 이용한 안전한 지불 방식 제안

본 논문에서는 초기 조회 과정을 거친 후 PIN 번호의 공유 및 유저의 PIN 번호 입력이 올바르게 이루어졌으며, 해당 모바일 디바이스는 PIN번호에 근거해 25시간마다 갱신되는 WPKI 인증서를 가지고 있

다는 가정을 기반으로 새로운 지불 시스템을 제안한다.

4.1 블루투스를 이용한 안전한 지불 시스템 구성 객체

제안 방식은 사용자의 모바일 디바이스간에 안전한 정보 교환을 통해 사용자를 중심으로 안전한 피코넷을 형성하여, 자신의 승용차에 주유 한 뒤 신용카드로 지불하기 위한 과정을 수행한다. 제안 방식의 구성 객체는 노트북, 모바일 폰, AP(Access Pointer), 은행(Bank)으로 구성되며, 다음과 같다.

- 노트북 : 사용자를 중심으로 형성된 피코넷의 마스터
- 모바일 폰 : 사용자를 중심으로 형성된 피코넷을 구성하는 슬레이브로써 모바일 전자지갑을 포함하고 있다.
- AP : 블루투스 통신을 위해 주유소에 설치된 Access Pointer
- 은행 : 블루투스 통신을 이용한 지불이 이루어질 때 사용자의 모바일 전자지갑을 발행하고 지불을 처리하는 객체

4.2 시스템 계수

블루투스를 이용한 안전한 피코넷 형성을 위한 시스템 계수는 다음과 같다.

*(N : 블루투스 마스터(NA : 마스터 A, NB : 마스터 B), C : 블루투스 슬레이브)

p_*, q_* : ECC 암호 알고리즘을 기반으로한 *의 공개키, 개인키쌍

g, n, G : 중앙 서버가 공개한 시스템 계수 (g : 유한체 F_m의 생성원(m은 소수), G : ECC의 Base Point, n : G의 위수)

r_* : 의사 랜덤수

T_* : *의 타임 스탬프

EC, E, H: 타원곡선 암호 알고리즘, 대칭키 암호 알고리즘, 안전한 해쉬 함수

S_j : 블루투스 슬레이브의 피코넷 그룹키 서명값

(p_{Ni}, q_{Ni}) : 블루투스 마스터에서 생성한 임의의 그룹키쌍

$Cert$: 공개키 인증서

ξ_* : 연접값

4.3 안전한 피코넷 프로토콜

4.3은 블루투스 피코넷 형성에 따른 마스터와 슬레이브의 상호 인증 및 그룹 키 설정 단계로써 다음과 같은 전제사항을 기반으로 수행된다.

<단계 1 : 마스터와 슬레이브간의 상호인증>

단계 1은 안전한 피코넷 형성을 위해 노트북(마스터)과 모바일 디바이스(슬레이브)와의 ECDH를 이용해 세션키를 설정하고 상호인증을 수행하는 과정이다.

Step ① 마스터는 ID_N과 세션키 정보 Q_N을 생성하고 VN_C, ξ_1, T_N, $Cert_N$을 계산하여 이를 슬레이브에 전송한다.

$$Q_N = r_N \cdot G$$
$$\xi_1 = (Q_N \| ID_N)$$
$$h_N = H(\xi_1)$$
$$VN\_C = EC_{p_C}(\xi_1 \| h_N)$$

Step ② 슬레이브는 전송받은 VN_C를 확인하고 ID_C와 세션키 생성을 위한 Q_C를 계산하여 VC_N, ξ_2, T_C, $Cert_C$를 마스터에 전송한다.

$$Q_C = r_C \cdot G$$
$$\xi_2 = (Q_C \| ID_C)$$
$$h_C = H(\xi_2)$$
$$VC\_N = EC_{p_N}(\xi_2 \| h_C)$$

이상의 키 교환 과정을 거쳐 마스터와 슬레이브는 세션키 K를 생성하고 상호 인증 과정을 마친다.

$$K = G*r_N*r_C = G*r_C*r_N$$

- 블루투스 마스터는 피코넷 내의 모든 슬레이브 디바이스와 단계 1의 상호 인증 과정을 수행하며, 수행이 완료된 후 슬레이브들에게 할당할 임의의 키쌍 (p_{Ni}, q_{Ni})을 생성한다. (p_{Ni}, q_{Ni})는 블루투스 마스터가 임의로 생성하는 키 쌍이다.

<단계 2 : 그룹키를 적용한 안전한 피코넷 형성>

Step ① 피코넷의 마스터는 그룹키쌍에서 임의적으로 추출한 키쌍 (p_{Ni_1}, q_{Ni_1})과 안전한 해쉬값 h_N을 계산한 뒤 세션키 K로 암호화하여 VN_C, S_N, T_N를 블루투스 슬레이브에게 전송한다.

$\xi_3 = (p_{N_i}, q_{N_i})$

$h_N = H(\xi_3)$

$S_N = SIG_{q_N}(h_N || T_N)$

$VN\_C = E_K(\xi_3 || h_N)$

Step ② 피코넷 슬레이브는 전송받은 VN_C와 h_N으로 기밀성과 무결성을 검증하고, S_N을 이용해 전송 데이터에 대한 인증을 수행한 뒤, 블루투스 마스터부터 할당받은 임의의 그룹키 쌍 (p_{N_i}, q_{N_i})을 기반으로 서명값 S_j를 수행한 뒤 주변의 모바일 디바이스에 브로드캐스팅 한다. 브로드캐스팅 과정을 수행한 후 ξ_4, h_C를 피코넷 마스터에 전송한다.

$S_j = SIG_{q_{N_i}}(p_{N_i}, T_C)$

$\xi_4 = (S_j || T_C)$

$h_C = H(\xi_4)$

- S_j는 블루투스 피코넷 프로토콜에서 블루투스 슬레이브를 인증하기 위하여 사용된다.

- 그룹 객체의 검증 : 마스터는 $\zeta*(n_{N_i} = (p_{N_i}, q_{N_i}))$ 리스트를 신뢰할 수 있는 제 3의 검증자에게 제공하여 S_j를 검증할 수 있다. (ζ는 블루투스 피코넷의 슬레이브 개수)

Step ③ 블루투스 마스터는 블루투스 슬레이브가 브로드캐스팅한 S_j에 대한 서명 검증 과정을 수행하고 블루투스 슬레이브의 피코넷 공개키 p_{N_i}을 해당 피코넷에 브로드 캐스팅한 뒤 이벤트 종결 메시지를 블루투스 슬레이브에 전송한다.

이상의 프로토콜을 기반으로 마스터를 중심으로 안전한 피코넷이 그림 3과 같이 형성된다.

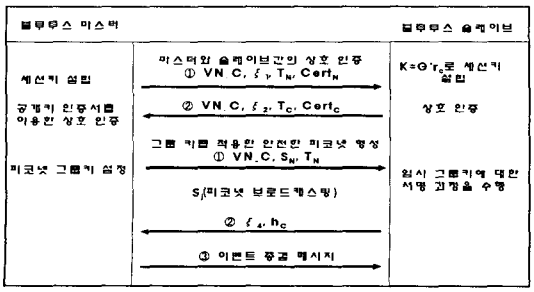

그림 3. 피코넷 객체간의 상호 인증 및 그룹 설정 단계

4.4 안전한 지불 프로토콜

안전한 피코넷 형성 이후 사용자는 자신의 승용차에 승차후 주유소에서 주유를 한 뒤 자신의 모바일 디바이스를 이용한 안전한 지불이 이루어지는 프로토콜이다.

가. 안전한 지불 프로토콜을 위한 시스템 계수

다음은 안전한 블루투스 지불 프로토콜을 위한 시스템 계수를 기술한다. 기술된 시스템 계수는 안전한 피코넷 프로토콜에서 추가된 사항만을 기술한다.

* (AP : A, 은행 : B)

TD_* : *의 트랜잭션 데이터

PI_* : *의 지불 정보

나. 초기 설정 단계

사용자가 블루투스 통신을 통해 지불 과정을 수행하기 위해 사용자 중심의 피코넷의 슬레이브를 은행에 등록하여 은행과 슬레이브간에 세션키를 공유하는 단계이다.

(사전단계 1) 블루투스 피코넷의 슬레이브인 모바일 폰은 다음을 계산하여 은행에 VC_B, ID_C, $Cert_C$를 전송한다.

$Q_{C_1} = r_{C_1} \times G$

$h_{C_1} = H(Q_{C_1} || ID_C)$

$VC\_B = EC_{p_B}(Q_{C_1} || PIN || h_{C_1} || T_C)$

(사전단계 2) 은행은 자신의 개인키로 VC_B를 복호화한 뒤 슬레이브의 정보인 Q_{C_1}과 PIN을 저장하고 VB_C, Q_B, ID_B, $Cert_B$를 슬레이브에게 전송한다.

$Q_B = r_B \times G$

$h_B = H(Q_B || ID_B)$

$VB\_C = EC_{p_N}(Q_B || h_B || T_B)$

블루투스 슬레이브인 모바일 폰과 은행은 다음과 같은 세션키 x를 계산하여 안전하게 사전 공유한다.

- 세션키 $\chi = r_{C_1} \times Q_B = r_{C_1} \times r_B \times G = r_B \times Q_{C_1} = r_B \times r_{C_1} \times G$

다. 안전한 블루투스 지불 프로토콜

초기 인증과정을 거친 후 모바일 폰은 전자지갑을

기동하고 지불정보 수신대기를 위한 활성 모드로 전환하며, AP는 특정 폰 접속을 위한 지불 내역을 전송하게 된다. 활성 모드의 전환은 블루투스의 전력 상태중 슬립(Sleep)상태로 전력을 최소한으로 유지한 상태에서 데이터 전송 및 활동 상태로의 전환을 위한 전력 모드의 전력 모드 변환 메시지이다.

전송된 지불 정보는 피코넷 마스터의 인증된 모바일 폰을 통하여 은행에게 전송된 후 은행의 승인 과정을 통하여 AP와 피코넷 슬레이브인 모바일 폰에게 지불에 대한 결과를 전송하게 된다. 이상의 프로토콜 과정을 통하여 안전한 블루투스 지불이 이루어진다. 그림 4는 프로토콜의 전체 과정을 보여준다.

Step ① 주유소에 설치된 AP는 모바일 폰에 지불정보 수신을 위한 활성 모드로의 전력 전환을 위한 지불정보 대기요청 메시지를 전송한다.

Step ② 지불정보 대기요청을 보낸 AP는 지불 정보를 자신의 ID와 함께 다음을 모바일 폰에 전송한다.

$(ID_A \| TD_A \| PI_A)$

Step ③ 지불정보를 전송받은 모바일 폰은 사용자의 PIN번호 입력을 요구한 뒤 다음을 계산한 뒤 g^{PIN}, X_C, S_C', h_C'를 AP에게 전송한다.

사용자의 PIN 번호 입력 → g^{PIN}

$h_C' = H(g^{PIN} \| ID_C)$

$\alpha = E_\chi(ID_C \| h_C' \| TD_A \| PI_A \| g^{PIN})$

$S_C' = SIG_{q_C}((\alpha \| ID_C), T_C)$

$X_C = (H(\alpha \| S_C') \oplus H(h_C' \| T_C)) \bmod n$

Step ④ AP는 전송된 g^{PIN}, X_C, S_C', h_C'를 다음과 같이 검증한다.

- S_C'를 모바일 폰의 공개키로 서명을 검증하여 α, ID_C, T_C를 확인한다.

- $h_C'' = H(g^{PIN} \| ID_C)$, $h_C' \stackrel{?}{=} h_C''$를 검증한다.

- $X_C' = (H(\alpha \| S_C') \oplus H(h_C'' \| T_C')) \bmod n$,

  $X_C' \stackrel{?}{=} X_C$를 검증한다.

- 모바일 폰에서 전송된 값이 검증이 올바른 경우 다음을 계산한 뒤 S_A, h_A, $Cert_A$를 은행에게 전송한다.

$S_A = SIG_{q_A}(ID_A \| \alpha \| T_A)$

$h_A = H(S_A \| ID_A)$

Step ⑤ 은행은 AP로부터 전송된 S_A, h_A, $Cert_A$를 다음과 같은 검증과정을 실시한다.

- S_a를 AP의 공개키로 공개키 서명을 확인한 뒤 ID_A, α, T_A를 저장한다.

- $h_A'' = H(S_A' \| ID_A')$, $h_A'' \stackrel{?}{=} h_A'$이면 α를 사전단계에서 모바일 폰과 공유했던 세션키 χ를 이용하여 복호화한 뒤 $ID_C, TD_A, PI_A, g^{PIN}$을 확인한다.

- 사전 과정에서 등록된 IIN을 이용해 $g^{IIN'} \stackrel{?}{=} g^{IIN''}$을 검증한다.

은행은 이상의 과정이 모두 올바르다면 TD_A, PI_A를 지불 처리한 뒤 영수증 값 $TD_{B_{res}}$, $PI_{B_{res}}$를 작성한 뒤 다음을 계산하여 AP에 β, h_B', S_B, X_B를 전송한다.

$\beta = E_\chi(ID_B \| TD_{B_{res}} \| PI_{B_{res}})$

$X_B = (H(\beta \| ID_B) \oplus H(g^{PIN} \| T_{B_{res}})) \bmod n$

$h_B' = H(\beta \| X_B)$

$S_B = SIG_{q_B}(ID_B \| h_B' \| T_B)$

Step ⑥ AP는 전송된 은행으로부터 전송된 β, h_B', S_B, X_B를 다음과 같은 검증과정을 수행한다.

- 은행으로부터 전송된 S_B를 은행의 공개키로 서명값을 검증하여 ID_B, h_B', T_B를 확인한뒤 β, X_B의 무결성을 검증한다.

$h_B'' = H(\beta \| X_B)$, $h_B'' \stackrel{?}{=} h_B'$

AP는 이상의 과정이 올바르다면 다음을 계산하여 모바일 폰에 β, X_B, S_{A_1}을 전송한다.

$h_{A_1} = H(ID_A \| \beta \| X_B)$

$S_{A_1} = SIG_{q_A}(h_{A_1} \| ID_A \| T_{B_{res}})$

Step ⑦ 모바일 폰은 AP로부터 전송된 β, X_B, S_{A_1}을 다음과 같은 과정을 거쳐 지불 데이터에 대한

영수증 값을 확인하고 저장한다.

- AP의 공개키로 S_{A_1}에서 $h_{A_1}, ID_A, T_{B_{res}}$를 확인한다.

$$h_{A_1}' = H(ID_A \| \beta' \| X_B'), \quad h_{A_1}' \stackrel{?}{=} h_{A_1}$$

- β를 은행과 사전에 공유했던 세션키 χ를 이용하여 복호화한 뒤 지불 데이터에 대한 영수증 값을 저장한다.

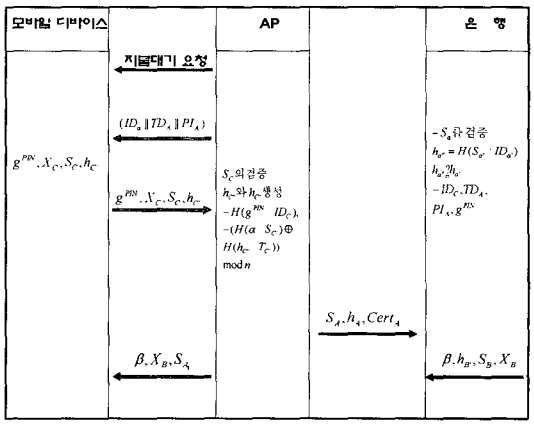

그림 4. 블루투스를 이용한 안전한 지불 시스템

5. 제안 방식 고찰

본 논문에서 제안된 지불 프로토콜은 다음과 같은 보안적 특징을 가지고 있다.

• 무결성 : 안전한 해쉬 함수 H와 타임 스탬프 T를 이용한 데이터의 무결성을 유지할 수 있다. 이는 세션키 설정 뿐만 아니라 지불 데이터와 영수 내역 전달 단계에서 사전에 공유된 g^{PIN}과 안전한 해쉬 함수 $H()$를 이용한 $X_B(X_B = (H(\beta \| ID_B) \oplus H(g^{PIN} \| T_{B_{res}})) \bmod n)$의 생성을 통해 전송 데이터에 대한 무결성을 제공하였다.

• 기밀성 : 공개키 암호 방식을 사용하여 기밀성을 유지하고자 하였으며 계산 능력을 고려하여 타원곡선 암호 알고리즘을 이용한 방식을 이용하였다. 제안방식의 경우 공개된 G를 공격자가 인지한다 할지라도 송신자와 수신자가 생성하는 의사난수 r값에 의해 안전한 세션키 설립($\chi = r_{C_1} \times Q_B = r_{C_1} \times r_B \times G = r_B \times Q_C = r_B \times r_{C_1} \times G$)을 제안하였다. 또한 사용자의 PIN에 대한 기밀성 서비스도 안전한 사전 등록과정을 통한 기밀성 서비스를 제공하였다.

• 부인봉쇄 : 각 객체간의 부인 봉쇄를 위하여 공개키 서명 방식과 더불어 블루투스 디바이스에 해당될 경우 ID가 48Bit 고유 주소로 결정되지만, 블루투스 디바이스 이외의 객체들의 경우 객체의 공개 ID를 적용할 수 있도록 제안하였다. 따라서 블루투스 디바이스의 경우 하드웨어적 주소를 이용한 인증 과정을 통한 부인봉쇄 서비스를 제시하였으며, 공개 ID를 사용하는 객체의 경우 안전한 공개키 암호 알고리즘의 서명값과 타임스탬프(T)를 통한 부인봉쇄 서비스를 가능하게 하였다.

• 상호인증 : 초기 피코넷 형성에서의 그룹 키를 이용한 피코넷 구성 객체들과의 안전한 상호 인증뿐만 아니라 은행과의 초기 상호 인증 단계을 통하여 안전한 지불 프로토콜이 진행되기 위한 과정을 제안하였다. 초기 피코넷의 경우 블루투스 마스터로부터 할당된 임시 그룹키를 기반으로 상호 인증과정을 수행하여 안전한 피코넷 설립이 되도록 하였으며, 지불 과정에서는 안전한 해쉬함수와 세션키 설립시에 전송되는 정보를 기반으로 상호인증이 가능하도록 하였다.

• 검증성 : 피코넷의 슬레이브의 그룹키를 검증함으로써 피코넷 마스터인 노트북은 슬레이브를 피코넷 디바이스로 검증이 가능할 뿐만 아니라 초기 블루투스 마스터가 저장하고 있는 피코넷 슬레이브의 공개키, 개인키쌍에서 개인키 쌍을 현재 슬레이브에 배포된 개수와 함께 신뢰된 제 3의 기관에 전송하여 검증할 수 있도록 하였다. (마스터는 $\zeta^*(p_{N_i}, q_{N_i})$ 리스트를 검증자에게 제공하여 검증자는 S_i를 검증할 수 있다.)

제안방식의 경우 기존 무선 지불 시스템을 3장에서 제시된 보안 요구사항을 기반으로 비교 분석하였을 경우 표 1과 같이 정리할 수 있다.

또한 기존의 블루투스에서 제시되고 있는 피코넷 구성과 제안방식에서 구성된 블루투스 피코넷을 3장에서 제시된 블루투스의 보안 취약성을 기반으로 분석하였을 경우 표 2와 같이 비교 분석할 수 있다.

표 1. 제안방식 비교 분석 - I

보안 요구사항	SWPP 방식	SMP 방식	제안방식
무결성	×	×	O
기밀성	×	×	O
부인봉쇄	△	△	O
상호인증	△	×	O
검증성	O	△	O

[× : 취약, △ : 보통, O : 안전]

표 2. 제안방식 비교 분석 -II

보안 취약성	블루투스 표준 v1.1	제안 방식
PIN 공격	×	O
지연 공격	×	△
인증 공격	△	O
암호 공격	△	O
도청 공격	×	O
위장 공격	×	O
결합 및 암호 공격	△	△

[× : 취약, △ : 보통, O : 안전]

6. 결 론

본 논문에서는 최근 근거리 무선통신의 표준으로 자리잡고 있는 블루투스를 이용한 여러 가지 응용 방법 중에서 전자상거래에 적극 활용이 가능한 지불 프로토콜을 제안하였다. 현재 무선 환경에서 제공되고 있는 여러 가지 응용 서비스들은 유선에 비해 취약한 보안적 문제점들이 지적하고 있어 실제 전자상거래 환경에 적용하기엔 많은 문제점이 있다.

특히 제안방식은 기존의 블루투스 표준의 취약성으로 제시되고 있는 여러 가지 공격 방법 중에서 다양한 보안 취약성에 대해 안전한 보안 서비스를 제공하고 있다. 그러나 지연 공격과 결합 및 암호 공격에는 여전히 높은 안전성 부분에서는 여전히 문제점을 내포하고 있다. 또한 기존 방식과 비교하여 볼때 보안적은 측면에서 안전성을 높이기 위해 계산량과 각 개체간의 교환 메시지 수와 같은 측면에서는 많은 문제점을 내포하고 있다.

따라서 본 논문에서 제안하는 지불 프로토콜은 안전성 및 실제 적용이 가능한 프로토콜로서 사용자에게 안전한 무선 전자상거래를 제공하기 위한 하나의 방법으로 활용할 수 있으리라 사료되며, 향후 본 논문의 고려사항에서 보안적인 요구사항을 좀 더 확대해 안전성 뿐만 아니라 안전성 증가에 따른 효율성(교환 메시지 수 및 계산량)을 고루 갖춘 지불 프로토콜에 대한 계속적인 연구가 필요하다.

참 고 문 헌

[1] J.Camenisch, U Maurer, and M. Stadler. "Digital Payment Systems with Passive Anonymity- Revoking Trustees." Computer Security -ESORICS 1996.

[2] J.Hall, S.Killbank, M.Barbeau, E. Kranakis, WPP : A Secure Payment Protocol for Supporting Credit and Debit-Card Transactions of ICT 2001(International Conference on Telecommunication), Romania, Bycharest, June 4-7, 2001

[3] X.Song, "Mobile Payment and Security," 2001, http://www.tml.hut.fi/Studies/T-110.501/2001/papers/xing.song.pdf

[4] General information on bluetooth http://www.mobileinfo.com/bluetooth/

[5] Thomas Muller, Bluetooth WHITE PAPER : Bluetooth Security Architecture, Version 1.0, 15July 1999.

[6] Annikka Aalto, Bluetooth http://www.tml.hut.fi/Studies/Tik110.300/1999/Essays/bluetooth.html

[7] Bluetooth information, http://www.bluetoothcentral.com/

[8] Oraskari, Jyrki. Bluetooth 2000. http://www.hut.fi/~joraskur/bluetooth.html

[9] How Stuff works, information on BT http://www.howstuffworks.com/bluetooth3.htm

[10] Information on Bluetooth (Official Homepage) http://www.bluetooth.com/

[11] Bluetooth Baseband http://www.infotooth.com/tutorial/BASEBAMD.htm

[12] Bluetooth - an inferior LAN concept? http://www.infotooth.com/knowbase/othernetworks

/71.htm
[13] Bluetooth Glossary. http://www.infottooth.com/glossary.htm#authentication
[14] Authentication process in Bluetooth. http://www.infotooth.com/knowbase/security/66.htm
[15] Authentication in Bluetooth. http://www.infotooth.com/knowbase/security/80.htm
[16] Bluetooth specification : profiles : http://www.bluetooth.com/developer/specification/profiles.asp
[17] Dan Chalmers and Morris Sloman, A Survey of Quality of Service in Mobile Computing Environments, IEEE Communications surveys 1999, online: http://www.comsoc.org/pubs/surveys/2q99issue/sloman.html
[18] http://www.sonera.com
[19] 장석철, "분할성 및 익명성 제어를 갖는 네트워크형 전자화폐 시스템에 관한 연구", 순천향대학교 석사학위 논문, 2001.
[20] 이임영 "전자상거래와 보안 입문", 생능출판사, 2001.
[21] Alfred J Menezes, Paul C, Oorschot, and Scott A. "HANDBOOK of APPLIED CRYPTOGRAPHY", CRC, 1996.

서 대 희

2003년 2월 순천향대학교 전산학 전공 석사
2004년 6월~현재 순천향대학교 전산학과 박사과정

관심분야 : 암호이론, 정보이론, 컴퓨터 보안

강 서 일

2003년 2월 순천향대학교 정보기술 공학부 졸업
2004년 6월~현재 순천향대학교 전산학과 석사과정

관심분야 : 정보보호, 암호 기술, 전자 화폐, 전자 상거래

이 임 영

1981년 8월 홍익대학교 전자공학과 졸업
1986년 3월 오사카대학 통신공학 전공 석사
1989년 3월 오사카대학 통신공학 전공 박사
1989년 1월~1994년 2월 한국전자통신연구원 선임연구원
1994년 3월~현재 순천향대학교 정보기술공학부 부교수
관심분야 : 암호이론, 정보이론, 컴퓨터 보안

박 해 룡

1998년 2월 전남대학교 수학과 이학사
2001년 2월 서울대학교 대학원 수학과 이학석사
2000년 12월~현재 한국정보보호진흥원 암호인증기술팀 연구원
관심분야 : 암호프로토콜, 전자화폐, DRM 등