Journal of Korea Multimedia Society Vol. 13, No. 11, November 2010(pp. 1687-1697)

개방형 스마트 폰 환경에 적합한 모바일 결제 시스템을 위한 안전한 AKA(Authentication Key Agreement) 모듈 설계

정은희†, 이병관††

요 약

스마트 폰 환경에서 모바일 결제 시스템을 수행하기 위해서는 USIM 기반의 AKA 인증 절차가 필수적인 이다. 본 논문에서는 개방형 스마트 폰 환경에 적합한 모바일 결제 시스템을 위한 결제 프로토콜과 AKA 모듈을 설계하였다. 결제 프로토콜은 모바일 결제 시스템의 구성요소들 간에 상호인증을 하도록 설계하여 신뢰성을 향상시켰고, 3GPP-AKA 프로토콜에 기반을 둔 모바일 결제 시스템의 AKA 모듈은 사전 등록을 통해 공유 비밀키(SSK)를 생성함으로써 IMSI 노출을 방지하고, 타임스탬프를 이용해 SQN(SeQuence Number) 동기문제를 해결하였다. 또한, SN과 인증기관 사이의 인증벡터 대신에 공유비밀키를 사용하도록 하여, 기존의 SN과 인증기관 사이의 대역폭이 (688 × N) × R bit에서 각각 320 × R bit, 368 × R bit로 감소시켰으며, MS와 SN간에는 일회용 공유비밀키인 OT-SSK를 사용해 메시지 암호화키인 CK와 IK를 생성하도록 하여 접속할 때마다 새로운 OT-SSK를 생성함으로써 데이터 재전송 공격을 방지하였다.

A Design of Safe AKA Module for Adapted Mobile Payment System on Openness SMART Phone Environment

Eun-Hee Jeong†, Byung-kwan Lee††

ABSTRACT

The USIM-based AKA authentication process is essential to a mobile payment system on smart phone environment. In this paper a payment protocol and an AKA module are designed for mobile payment system which is suitable for openness smart phone environment. The payment protocol designs the cross authentication among components of the mobile payment system to improve the reliability of the components. The AKA module of mobile payment system based on 3GPP-AKA protocol prevents the exposure of IMSI by creating the SSK(Shared Secure Key) through advance registration and solves the SQN(SeQuence Number) synchronization problem by using timestamp. Also, by using the SSK instead of authentication vector between SN and authentication center, the existing bandwidth (688×N)×R bit between them is reduced to 320×R bit or 368×R bit. It creates CK and IK which are message encryption key by using OT-SSK(One-Time SSK) between MS and SN. In addition, creating the new OT-SSK whenever MS is connected to SN, it prevents the data replay attack.

Key words: USIM, Mobile Payment System(모바일결제시스템), Mobile Payment Protocol(모바일결제 프로토콜)

※ 교신저자(Corresponding Author) : 정은희, 주소 : 강원도 삼척시 교동 중앙로 1. 강원대학교 삼척캠퍼스 인문사회과학관 308호(245-711), 전화 : 033)570-6646, FAX : 033)574-6640, E-mail : jeongeh@kangwon.ac.kr
접수일 : 2010년 10월 5일, 수정일 : 2010년 11월 1일
완료일 : 2010년 11월 26일
† 정회원, 강원대학교 삼척캠퍼스 지역경제학과 부교수
†† 정회원, 관동대학교 컴퓨터학과 교수
(E-mail : bklee@kwandong.ac.kr)

1. 서 론

최근에 각 산업을 망라해서 화두가 되고 있는 것 중의 하나가 컨버전스(Convergence)이다. 컨버전스는 디지털 기술을 매개로 하여 컴퓨터와 가전, 통신 등의 여러 가지 기기와 기반기술이 서로 유기적으로 융합되는 현상을 말한다. 이러한 컨버전스가 우리에게 의미가 있는 것은 바로 금융 산업 자체가 디지털화 되고, 정보산업으로 발전하고 있기 때문이다[1].

또한, 모바일 네트워크 고도화 및 단말기의 비약적인 발전으로 인해 사용자들의 다양한 요구를 충족시키는 스마트폰이 출현하게 되었으며, 3세대 이동 단말기부터 사용자 인증 모듈(Universal Subscriber Identity Module : USIM)이라 불리는 USIM 카드를 사용해 네트워크 인증과 부가 기능을 제공 한다. 즉, 스마트 폰은 다양한 인터페이스를 통하여 언제 어디서나 사용자가 원하는 모바일 서비스인 통신, 금융, 교통 등의 다양한 부가 서비스를 제공받게 되고, 그로 인하여 우리의 비즈니스 및 생활은 엄청난 기회를 갖게 되었다[2].

하지만, 무선 네트워크 환경에서 동작하는 모바일 서비스들은 불법적인 변조, 도청, 신분위장 등 다양한 보안 위협에 노출되기 쉬울 뿐만 아니라, 스마트 폰 환경은 기존의 이동통신의 폐쇄적인 서비스 환경과 달리 Openness 환경이므로 사용자는 다양한 콘텐츠를 다양한 경로로 단말기로 획득할 수 있으며, 불법적인 경로로 유입된 콘텐츠로 인해 사업자 영업방법의 피해 및 경제적 손실이 불가피 할 수 있으며, 바이러스에 감염된 콘텐트 설치로 모바일 바이러스로 인한 피해까지 발생할 수 있다.

현재 3GPP(3rd Generation Partnership Project)에서 3GPP-AKA(3GPP-Authentication Key Agreement) 표준을 제정해 모바일 환경에서 사용자 인증 및 암호화, 메시지 무결성을 제공하였지만, 3GPP-AKA 프로토콜은 SQN(SeQuence number)에 대한 동기문제와 False base station을 이용한 공격, 단말의 영구 식별자인 IMSI(International Mobile Subscriber Identity)의 평문 전송으로 인한 프라이버시 문제, 다수의 인증벡터 사용으로 인한 인증 데이터 오버헤드 등의 문제가 지적되었다[3,4,5].

본 논문에서는 3GPP-AKA의 이러한 문제점들을 보안하고, 스마트 폰 환경의 Openness와 다양한 네트워크 인터페이스 및 연동 인프라에 대응할 수 있는 모바일 결제 시스템을 위한 안전한 AKA 모듈을 설계하여 사용자 또는 기기에 대한 네트워크 인증과 서비스 인증을 통해 안전하고 효율적인 서비스를 제공하고자 한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서 관련 연구를 살펴보고, 3장에선 본 논문에서 제안한 모바일 결제 시스템을 설명하고, 모바일 결제 시스템의 AKA 모듈의 안정성 평가 및 효율성 평가 결과를 4장에서 설명한다. 그리고 5장에서 결론을 맺는다.

2. 관련 연구

2.1 모바일 결제 시스템

모바일 지급결제(Mobile Payment)는 온라인과 오프라인 상에서 이루어지는 서비스와 재화 구매 시 대금을 이동통신망을 이용하여 지불하는 결제서비스로 정의된다. 즉, 모바일 지급결제는 현금이나 신용카드 등 기존 결제수단을 대신할 수 있는 새로운 지급결제의 유형으로, 이용자의 신원확인, 거래정보의 전달, 거래인증 등 결제과정이 이동통신망의 일부 또는 전부를 통해 이루어지는 것을 의미한다.

모바일 결제시스템은 그림 2와 같은 구조로 이루어지며, 모바일 결제 시스템의 프로토콜은 결제 거래 프로토콜과 세션키 생성 프로토콜로 구성된다[6,7].

그림 1의 결제 거래 프로토콜은 모바일폰과 발행은행 사이의 안전성을 위해 세션키를 생성하였지만 발행은행에 대한 신뢰할만한 검증 철자가 없으며, 발행은행은 USIM 카드 관리 역할을 수행하고 있으나 USIM 관리 시스템의 부재로 USIM 관리가 한계가 있다. 또한, USIM 카드가 장착된 모바일 폰에서 결제를 위한 별도의 Payment ID를 생성할 필요 없다. 따라서 본 논문에서는 신뢰할 수 있는 인증기관을 두어 별도로 USIM 카드를 관리 및 발행은행의 검증 및 사용자, 상점, Settlement center를 검증하고, Payment ID 대신에 USIM 카드의 IMSI를 이용하는 좀 더 안전한 모바일 결제 시스템을 제안한다.

2.2 USIM 인증

USIM은 소형 CPU와 메모리를 가지고 있어서 단말의 인증에 사용되는 암호 알고리즘과 프로세스를

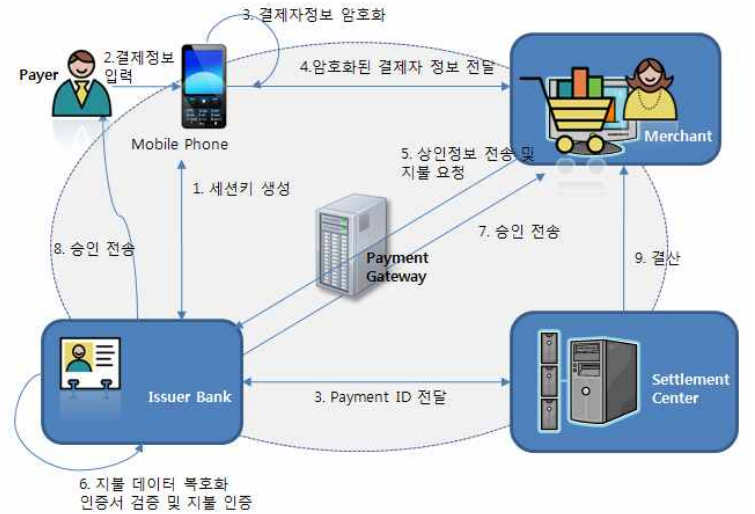

그림 1. 모바일 결제 시스템 및 결제 거래 프로토콜

동작하므로, 인증과 키 일치(Authentication and Key Agreement : AKA) 과정을 수행하고 이 과정에서 생성된 암호키를 이용해 단말기 사용자 데이터에 대한 암호 및 인증 서비스를 제공한다[8,9]

그림 2는 무선 인터넷 환경에서의 USIM 인증과정인 3GPP-AKA을 설명한 것으로 USIM/MS에서 IMSI(International Mobile Subscriber Identity) 혹은 TMSI(Temporary Mobile Subscriber Identity)의 정보를 SN(Serving Network)에 전송하여 자신을 알리면 SN은 인증 데이터 요구 메시지와 단말에서 수신한 IMSI/TMSI를 인증센터인 HN(Home Network)의 AuC(Authentication Center)에 전송한다. HN는 수신한 IMSI에 대한 인증벡터 AV(Authentication Vector)를 생성하여 인증 데이터 요구

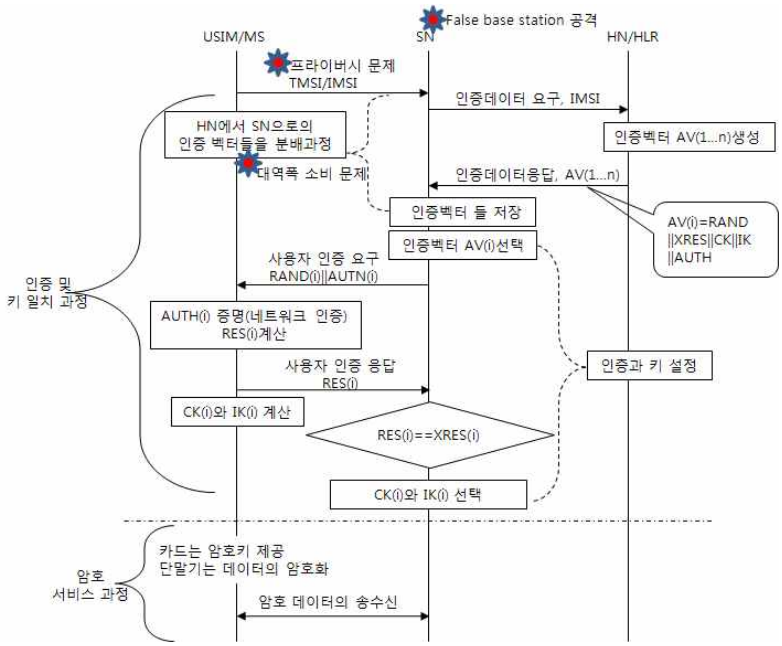

그림 2. 3GPP-AKA 상호 인증 흐름[10]

에 대한 응답으로 SN에 전송한다. SN은 AV 중 하나를 선택하고 랜덤수를 생성하여 AV내의 인증토큰(AUTN)을 추출하여 단말에서 사용자 인증 요구를 시도한다. 단말은 USIM의 네트워크 인증 알고리즘을 이용해 이 데이터에 대한 인증을 마치고 사용자 인증 응답을 SN에게 전송하는 한편 암호화 세션키 CK와 IK를 생성한다. SN은 수신한 RES와 자신이 저장하고 있던 XRES를 비교하여 단말과 사용자를 인증한 후 사용자 데이터 암호화에 이용될 세션키를 생성해 인증과 키 일치 과정은 완료된다[10,11,12].

하지만, 3GPP-AKA의 상호 인증은 SQN 비동기화로 인한 인증실패 현상인 SQN 동기화 문제, 단말기와 SN 사이의 통신에 개입하여 사용자가 의도하지 않는 다른 SN으로 redirect 하는 False base station 공격, SN과 HN사이의 대역폭 소비 문제, IMSI 평문 전송에 의한 프라이버시 등의 문제가 제기되고 있다.

3. 모바일 결제 시스템 설계

본 장에서는 모바일 결제 시스템의 전체적인 흐름을 설명하고, 모바일 결제 시스템의 각 구간별 인증 모듈에 대해 설계한다. 모바일 결제 시스템은 신뢰할 수 있는 인증기관, 발행은행, 결제센터, 상점 그리고 사용자로 구성되며, 각각의 구성원의 역할은 다음과 같다.

- 발행은행(Issuer Bank) : 신용카드를 발급한 은행이다. 발행은행은 USIM 카드 관리 역할을 수행하고 있으나 USIM 관리 시스템의 부재로 USIM 관리가 한계가 있으므로, 신뢰할 수 있는 인증기관을 두어 별도로 USIM 카드를 관리한다.
- 결제센터(Settlement Center) : 실질적인 모바일 결제 시스템의 지불 요청 및 응답을 관리하는 역할을 담당하며, 거래의 결과를 발행은행에 전달하여 사용자 계좌 정보를 갱신한다.
- 인증기관 : 신뢰할 수 있는 인증기관으로, USIM 카드를 관리하고, 발행은행, 상점, 결제센터를 등록하여 상호 인증을 수행한다.
- 상점 : 모바일 결제 시스템을 사용하는 온라인 및 오프라인 상점을 말한다.
- 사용자 : USIM 카드가 장착된 모바일 폰의 소유자로써 모바일 결제 시스템의 사용자를 말한다.

그림 3은 모바일 결제 시스템의 구성요소들 간의 전반적인 흐름을 설명한 것이다.

3.1 모바일 결제 프로토콜 설계

본 논문에서 설계한 모바일 결제 프로토콜은 상점에 모바일의 USIM 카드의 정보를 암호화하여 전송

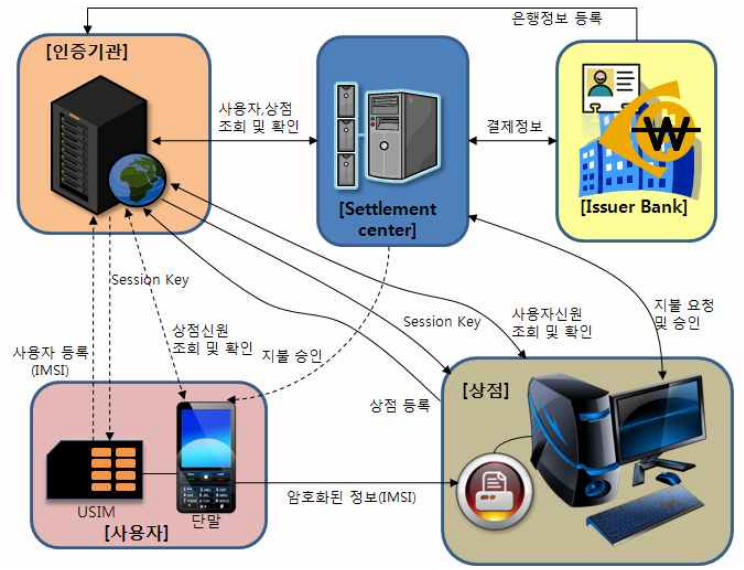

그림 3. 모바일 결제 시스템 흐름도

함으로써 사용자 인증 요청과 동시에 모바일 결제도 함께 요청을 하도록 설계 하였다. 이때, 사용자, 상점, 인증기관, 결제센터, 발행은행은 사전에 인증기관에 각자의 정보를 등록하면서 각자 공유 비밀키를 생성해 가지고 있으므로, 전송할 정보를 공유비밀키로 암호화해 전송한다.

그림 4는 모바일 결제 프로토콜의 전체적인 과정을 설명한 것으로 모바일 결제 프로토콜은 각 구성원들이 인증서버에 등록하는 등록단계, 실제 거래에서 상호인증을 수행하는 인증단계, 그리고 결제요청에 따른 결제 승인 및 결제 정보 정리단계로 구성된다.

3.1.1 등록단계

모바일 결제 시스템을 구성요소인 사용자, 상점, 발행은행, 결제센터가 인증기관에 각각의 마스터키를 등록하고 사용자, 상점, 발행은행, 결제센터가 인증기관과의 공유비밀키를 생성하는 단계이다.

공유비밀키는 EC-DH 알고리즘으로 생성되며, 이 공유비밀키는 상호인증시에 사용된다. 모바일 결제 시스템 구성 요소 중 인증기관과 상점의 공유비밀키 생성과정을 살펴보면 다음과 같다.

① 상인은 인증기관에 회원가입을 할 때, 상인의 정보를 등록한다.

② 인증기관은 상인에게 공유비밀키 생성에 필요한 초기점 P, E_P, 그리고 인증기관의 공개키인 $A_{SK}P$를 상인에게 전달한다.

③ 상인은 인증기관의 공개키로 공유비밀키 $M_{SK}(A_{SK}P)$를 생성한 후, 상인의 공개키인 $M_{SK}P$와 같이 인증기관에 전달한다.

④ 인증기관은 상인의 공개키로 공유비밀키 $A_{SK}(M_{SK}P)$를 생성한 후, 상인이 전달한 공유비밀키와 유효성을 검사한다.

⑤ 상인은 인증기관으로부터 전달받은 공유비밀키와 상인이 생성한 공유비밀키와 비교해 유효성을 검사한다.

⑥ 이때, 유효성 검사가 TRUE이면 상인과 인증기관의 공유비밀키로 사용한다.

3.1.2 인증단계

모바일결제시스템에서 사용자와 상점간의 상호인증, 상점과 결제센터와의 상호 인증, 결제센터와 발행은행간의 상호인증을 하는 단계를 말한다. 인증

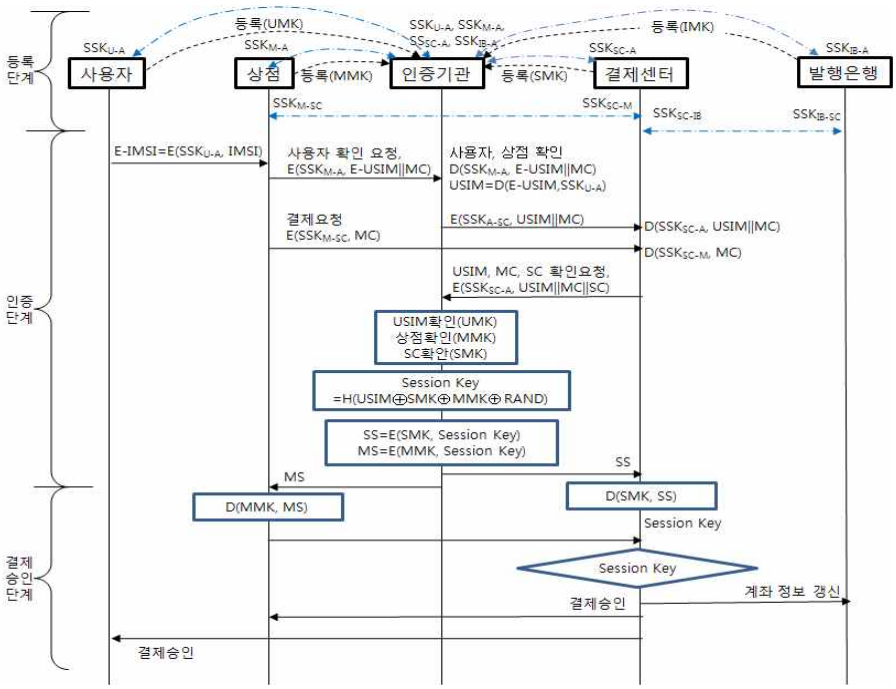

그림 4. 모바일 결제 프로토콜 흐름도

단계에서는 등록단계에서 생성한 공유비밀키로 각자의 정보를 암호화시켜 목적지에게 전송함으로서 각자의 정보를 보호한다. 특히, 이 단계에서 일회용 세션키를 생성해 결제승인 단계에서 사용함으로써 세션키 노출로 인한 개인 정보 및 계좌 노출을 방지한다.

① 사용자는 상점에 모바일 결제를 할 때, USIM 카드의 고유값 IMSI를 사용자와 인증 서버간의 공유비밀키인 SSK_{U-A}로 암호화한 값을 상점에 전달한다. 이때 상점은 암호화된 USIM 정보($E-USIM$)에 상점의 고유 코드인 MC를 연접해 SSK_{M-A}로 암호화해 인증서버에 사용자 신분 인증을 요청하는 동시에 결제센터에 전송하여 결제를 요청한다. 이때, 사용자 인증과 마찬가지로 상점은 상점의 코드인 MC를 상점과 결제센터간의 공유비밀키인 SSK_{M-SC}로 암호화시켜 결제센터에 전송한다.

$E-USIM = E(SSK_{U-A}, USIM)$ // USIM을 공유비밀키 SSK_{U-K}로 암호화

$E(SSK_{M-A}, E-USIM \| MC)$ // $E-USIM$과 MC를 연접해 SSK_{M-A}로 암호화

$E(SSK_{M-SC}, MC)$ // MC를 SSK_{M-SC}로 암호화

② 인증기관은 각각의 공유비밀키로 전달받은 암호문을 복호화 시켜 사용자의 신원과 상점의 신원을 확인한다. 그리고 사용자의 USIM과 상점의 MC를 결제센터간의 공유비밀키 SSK_{A-SC}로 암호화 결제센터에 전송한다.

$D(SSK_{U-A}, E(SSK_{U-A}, E-USIM)) = USIM$ // 암호문을 SSK_{U-A}로 복호화

$D(SSK_{M-A}, E(SSK_{M-A}, E(SSK_{U-A}, USIM) \| MC)) = E-USIM \| MC$

$\rightarrow MC$ 추출

$E(SSK_{A-SC}, USIM \| MC)$ // USIM과 MC를 연접해 SSK_{A-SC}로 암호화

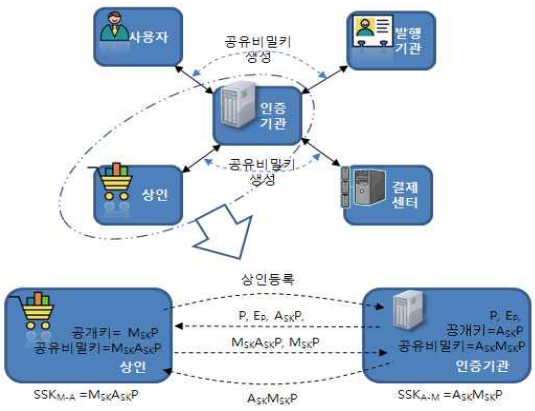

그림 5. 공유비밀키 생성(상인과 인증기관)

③ 결제센터는 상점으로부터 전송받은 지불 요청 메시지와 인증서버로 받은 사용자와 상점의 신원확인을 SSK_{A-SC}로 암호화하여 인증기관에 의뢰한다.

$D(SSK_{A-SC}, E(SSK_{A-SC}, USIM \| MC)) = USIM \| MC$ // 암호문을 SSK_{A-SC}로 복호화

$E(SSK_{A-SC}, USIM \| MC \| SC)$ // USIM, MC, SC를 연접해 SSK_{A-SC}로 암호화

④ 인증기관은 결제센터로부터 전송받은 메시지를 SSK_{A-SC}로 복호화 시킨 후, USIM, 상점, 결제센터 신원을 확인 한 후 DB에 저장되어 있던 각각의 마스터키를 찾는다.

⑤ 인증기관은 모바일 결제 승인에 필요한 USIM, 각각의 마스터키, 랜덤값을 XOR 연산한 후 해쉬하여 Session key를 생성한다.

$Session\ Key = H(USIM \oplus SMK \oplus MMK \oplus RAND)$

이때, session key는 각각의 마스터키를 이용해 암호화한 후 상점과 결제센터에 전달한다.

$SS = E(SMK, Session\ Key), MS = E(MMK, Session\ Key)$

3.1.3 결제요청 승인 단계

① 상점은 자신의 마스터키(MMK)로 복호호한 후 session key를 결제센터에 전송한다.

② 결제센터는 자신의 마스터키(SMK)로 복호화한 후 상점에서 전달받은 Session key와 비교하여 일치하면 결제 승인 메시지를 상점과 사용자에게 각각 전달함으로써 모바일 결제 처리가 종료된다.

이때, 인증 서버가 session key를 상점에 3분 이내에 전송하지 않거나, 사용자가 session key를 상점에 전송하지 않으면 거래는 취소된 것으로 처리한다.

③ 결제센터는 발행은행에 사용자의 정보를 암호화시켜 전송한다.

④ 발행은행은 사용자의 정보를 갱신한다.

3.2 USIM을 이용한 안전한 AKA(Authentication Key Agreement) 설계

모바일 결제 프로토콜은 모바일 폰의 특성상 고정된 장소에서만 결제가 이루어지는 것이 아니므로 USIM 카드를 이용한 사용자 인증에는 기존의 3GPP-AKA의 상호 인증을 프로토콜을 적용하였다. 그런데, 기존의 3GPP-AKA 상호인증의 SQN(Sequence Number) 동기화 문제, False base station 공격, SN(Servinig Network)과 인증기관 사이의 대역폭 소비 문제, IMSI 평문 전송에 의한 프라이버시 문제를 개선한 강력한 사용자 인증 모듈을 제안한다.

제안하는 사용자 인증 모듈은 MS가 자신이 속해 있는 SN의 ID를 알 수 있고, MS가 등록되어 있는 인증기관(HD)의 ID를 알고 있다고 가정한다. 그리고 SN과 인증기관(HD)은 신뢰할 수 있는 기관이고 SN과 인증기관(HD)의 통신채널이 안전하다고 가정하에 설계되었다.

그림 6은 USIM을 이용한 사용자 인증 절차를 설명한 것으로 각 단계에 대한 설명은 다음과 같다.

① 기존의 AKA에서 단말기의 IMSI 평문 전송에 의한 프라이버시 문제와 SQN의 동기화문제를 해결하기 위해 $IMSI$, T_{MS}(timestamp), 단말기 근처에 위치한 SN_{ID}를 연접해 함수 $f_K^1()$를 이용해 MS의 인증값을 생성한다. 또한, MS의 $IMSI_{MS}$를 HN와 MS간의 공유비밀키인 SSK_{MS-HN}로 암호화한 값인 $E-IMSI_{MS}$과 MAC_{MS}, HN_{ID}, T_{MS}를 MS의 근처에 있던 SN에 전송한다.

$$MAC_{MS} = f^1_{SSK_{MS-HN}}(IMSI_{MS} \| T_{MS} \| SN_{ID})$$

$$E-IMSI_{MS} = E(SSK_{MS-HN}, IMSI_{MS})$$

② SN은 전달받은 $E-IMSI_{MS}$, MAC_{MS}, T_{MS}를 해당 인증기관(HN)에 전달한다.

③ 인증기관(HN)은 $E-IMSI_{MS}$을 MS와 HN 간의 공유비밀키 SSK_{MS-HN}로 복호화 시켜 MS의 IMSI 값을 복원한 후, 인증기관(HN)의 데이터베이스에 MS의 IMSI가 있는지 검사한다. 또한, 인증기관(HN)이 복원한 $IMSI_{MS}$와 전달받은 T_{MS}를 이용해 $XMAC_{MS}$를 계산해 전달받은 MAC_{MS}와 비교하여 메시지 무결성을 검사한다.

$$E-IMSI_{MS} = D(SSK_{MS-HN}, IMSI_{MS}) = IMSI_{MS}$$

$$XMAC_{MS} = f^1_K(IMSI_{MS} \| T_{MS} \| SN_{ID})$$

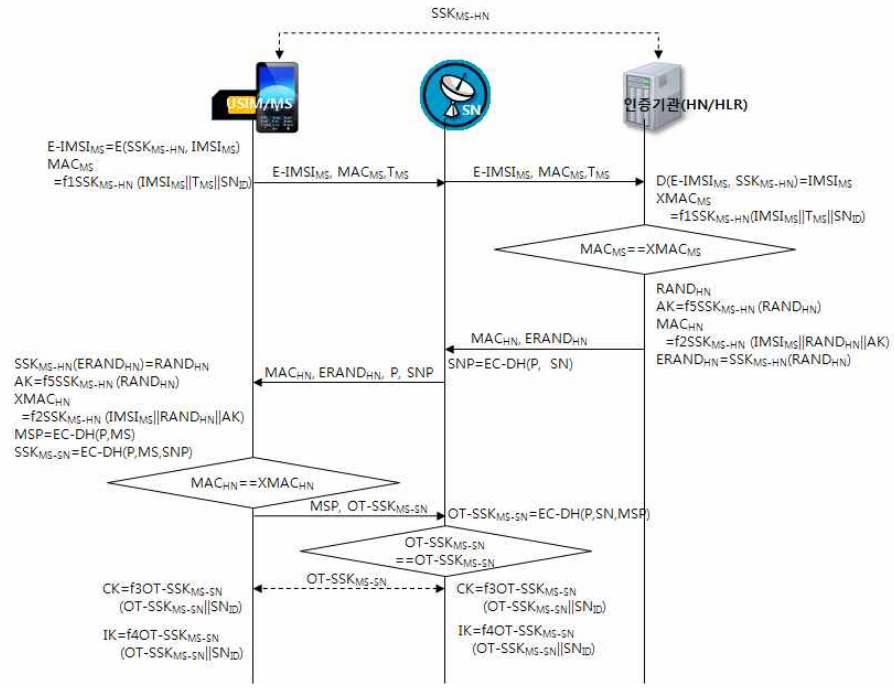

그림 6. 안전한 AKA 절차

④ MS의 신분을 확인한 인증기관(HN)은 인증기관(HN)의 신분을 확인할 MAC_{HN}, E_$RAND_{HN}$를 생성해 SN에 전달한다. 이때, 인증기관(HN)은 임의로 선택한 랜덤 값인 $RAND_{HN}$을 이용하고 MS의 $IMSI_{MS}$로 XOR 연산을 한 값을 SN에 전송한다.

$$AK = f^5_{SSK_{MS-HN}}(RAND_{HN})$$

$$MAC_{HN} = f^2_{SSK_{MS-HN}}(IMSI_{MS} \| RAND_{HN} \| AK)$$

$$ERAND_{HN} = IMSI_{MS} \oplus RAND_{HN}$$

⑤ SN은 인증기관(HN)으로부터 전달받은 MAC_{HN}, $ERAND_{HN}$를 MS에 전달한다. 이때, SN은 MS가 SN의 신분을 확인할 수 있도록 일회용 SSK인 $OT-SSK_{MS-SN}$을 생성하기 위한 초기점과 SN의 공개키인 P, SNP을 MS에 전송한다.

$$SNP = EC-DH(P, SN)$$

⑥ MS는 전달받은 $ERAND_{HN}$를 공유비밀키인 SSK_{MS-HN}을 이용해 복호화하여 인증기관(HN)의 랜덤값인 $RAND_{HN}$을 추출한다. 이 값을 이용해 $XMAC_{HN}$을 계산하여 전달받은 MAC_{HN}을 비교해 인증기관(HN)의 신분을 확인한다. 이때, MS는 SN으로부터 전달받은 공개키에 자신의 비밀키로 $OT-SSK_{MS-SN}$를 생성한다. 그리고 SN에 자신의 공개키인 MSP와 일회용 공유비밀키인 $OT-SSK_{MS-SN}$를 전송한다.

$$E(SSK_{MS-HN,} ERAND_{HN}) = RAND_{HN}$$

$$XMAC_{HN} = f^2_{SSK_{MS-HN}}(IMSI_{MS} \| RAND_{HN})$$

$$OT-SSK_{MS-SN} = EC-DH(P, MS, SNP)$$

⑦ MS와 인증기관(HN)의 상호 인증이 완료되었으므로, 안전한 정보 전송을 위해 MS와 SN의 간의 상호인증을 한다. SN은 MS로부터 전달받은 MS의 공개키인 MSP를 이용해 일회용 공유비밀키인 $OT-SSK_{MS-SN}$를 생성해, MS로부터 전달받은 $OT-SSK_{MS-SN}$와 일치하는지를 검사하여 MS의 신분을 확인을 상호 인증한다.

$$OT-SSK_{MS-SN} = EC-DH(P, SN, MSP)$$

⑧ 마지막으로 안전한 정보전송을 위한 CK, IK를 생성하는데, 본 논문에서는 EC-DH의 알고리즘을 이용한 $OT-SSK_{MS-SN}$를 CK, IK 생성에 활용한다.

$$CK = f^3_{OT-SSK_{MS-SN}}(OT-SSK_{MS-SN} \| SN_{ID})$$

$$IK = f^4_{OT-SSK_{MS-SN}}(OT-SSK_{MS-SN} \| SN_{ID})$$

4. 분 석

본 논문에서는 개방형 스마트 폰 환경에 적합한 모바일 결제 시스템을 위한 안전한 AKA(Authentication Key Agreement) 모듈 설계하였다. 본 논문에서 설계한 AKA 모듈은 기존의 3GPP-AKA 인증 방식을 사용하였으나, 기존의 3GPP-AKA에서 발생 가능한 문제점을 분석하고, 그 문제점을 개선하였다.

4.1 안전성 분석

4.1.1 상호 인증

① MS와 인증기관의 상호 인증

본 논문에서 제안한 AKA 모듈은 상호 인증을 위해 MS와 인증기관(HN)간에 EC-DH 알고리즘 기반 공유 비밀키인 SSK_{MS-HN}을 사용한다. 이때 사용되는 공유 비밀키인 SSK_{MS-HN}는 USIM 카드를 처음 등록할 때, USIM카드와 인증기관에 등록되어 있던 초기점과 비밀키를 이용해 생성된 것으로 MAC_{MS}, $XMAC_{MS}$를 생성해 상호 인증을 한다.

② MS와 SN의 상호 인증

본 논문에서 제안한 AKA 모듈은 MS와 SN간의 상호 인증을 위해선 초기점에 따라 다르게 설정되는 일회용 공유 비밀키로 EC-DH에 기반을 $OT-SSK_{MS-SN}$를 사용한다. 이 일회용 공유 비밀키인 $OT-SSK_{MS-SN}$를 이용해 MS와 SN간의 상호 인증을 한다.

③ 상점과 결제센터 인증

본 논문에서 제안한 모바일 결제 프로토콜의 상점, 결제센터에도 일회용 공유비밀키를 생성해 각각의 마스터키를 이용한 새로운 session key를 생성해 상호 인증을 한다.

4.1.2 프라이버시 보호 강화

본 논문에서 제안한 AKA 모듈은 SSK_{MS-HN}로 IMSI를 암호화 시켜 인증기관에 전달함으로써 IMSI 평문 전송에 의한 프라이버시 문제를 해결하였다.

본 논문에서 제안한 모바일 결제 프로토콜에서도 OT_SSK를 이용해 상점고유코드(MC)와 결제센터의 고유코드(SC)를 암호화시켜 인증기관에 전달하

므로 상점과 결제센터의 정보 또한 보호하였다고 볼 수 있다.

4.1.3 재전송 공격

본 논문에서 제안한 AKA 모듈은 MS와 인증기관이 상호인증을 요청할 때마다 타임스탬프를 사용하고, 새로운 인증키를 생성하는 OT-SSK 방식을 사용하고 있으므로 공격자의 재전송 공격에도 안전하다.

4.1.4 완전 전방향 안전성 만족

본 논문에서 제안한 모바일 결제 프로토콜과 AKA 모듈은 EC_DH 기반의 SSK와 OT-SSK를 사용하므로, 초기점 P와 공개키가 공개되어도 각자의 비밀키를 모르기 때문에 SSK와 OT-SSK를 산출할 수 없으며, 완전한 전방향 안정성을 만족한다.

4.2 효율성 분석

표 1은 기존의 3GPP-AKA과 본 논문에서 제안한 AKA 모듈의 성능을 비교한 것이다[13].

4.2.1 대역폭 감소

표 1의 인증데이터 메모리 량에서 알 수 있듯이 본 논문에서 제안한 AKA 모듈은 인증벡터를 사용하지 않으므로 기존의 3GPP-AKA와 같이 n개의 인증벡터를 생성해 SN와 인증기관 사이에서 전송하지 않는다. 따라서 기존의 SN과 인증기관 사이의 대역폭이 (688 × N) × R bit에서 각각 320 × R bit, 368 × R bit로 감소되었다.

4.2.2 SN의 저장데이터 감소

본 논문에서 제안한 AKA 모듈은 인증벡터 AV를 사용하지 않으므로, SN이 인증기관(HN)으로부터 전송받은 인증벡터 AV를 별도로 저장할 필요가 없으므로 SN의 저장 데이터가 (688 × N) × R bit에서 각각 320 × R bit으로 감소되었다고 볼 수 있다.

5. 결 론

통신의 급속한 발전과 인터넷의 범용적인 사용으로 많은 사람들이 분산된 컴퓨팅 환경에서 원격 서버에 접속하는 일이 빈번해지고 있지만, 인증된 보호 시스템 없이 안전하지 않는 채널을 통한 데이터 전송은 재생공격이나 오프라인 패스워드 공격 및 가장 공격 등과 같은 문제점들이 많이 노출되고 있다. 이에 본 논문에서는 이런 문제점들을 해결할 수 있는 개방형 스마트 폰 환경에 적합한 모바일 결제 시스템을 위한 안전한 AKA(Authentication Key Agreement) 모듈을 설계하였다.

본 논문에서 제안한 AKA 모듈은 사용자 인증은 MS와 인증기관(HN)간에 공유비밀키를 생성해 USIM의 IMSI 값을 암호화하여 전송함으로써 IMSI 노출을 방지하고, MS와 SN간에는 일회용 공유비밀키인 OT-SSK를 사용해 메시지 암호화 키인 CK와 IK를 생성하도록 하여 접속할 때마다 새로운 OT-

표 1. 제안 기법 성능 비교

비교항목		3GPP-AKA	제안기법
Sequence Problem		Yes	No
인증 데이터 메모리 용량	MS	560bit	496bit
	SN	(688 × N) × R bit	320 × R bit
	HN	(688 × N) × R bit	368 × R bit
저장되어야 할 인증 파라미터	MS	RAND, CK, IK, SQN, AK, AMF, MAC	MAC, AK, XMAC, CK, IK, SSK, T
	SN	RAND, CK, IK, SQN, AK, AMF, MAC, XRES	CK, IK, SSK
	HN	RAND, CK, IK, SQN, AK, AMF, MAC, XRES	RAND, MAC, XMAC, AK, SSK
인증데이터별 저장공간	RAND : 128bit, XRES:128bit, CK:128bit, IK:128bit, SQN:48bit, AK:48bit, AMF:16bit, MAC:64bit, SSK:64bit N : 인증 벡터 수, R : MS 수		

SSK를 생성함으로써 데이터 재생 공격을 방지하였다. 또한 본 논문에서 제안한 AKA 모듈은 인증벡터와 SQN을 사용하지 않으므로 SN과 인증기관(HN)의 대역폭을 감소시키고, SQN대신에 공유비밀키 SSK를 사용해 현재 접속 중인 MS를 체크함으로써 SQN 동기문제를 해결하였다.

본 논문에서 제안한 모바일 결제 프로토콜의 사용자 인증은 상점에서 인증서버로 USIM을 각각의 공유비밀키로 암호화 시켜 전송함으로써 USIM이 노출될 가능성을 배제하였으며, 사용자, 상점, 결제센터의 신원을 확인할 때마다 USIM, Random 값, 사용자의 마스터키, 상점의 마스터키, 그리고 결제센터의 마스터키를 이용해 Session key를 새로 생성하도록 하여 이전의 Session key의 노출로 인해 악의의 사용자가 모바일 결제를 시도할 수 없도록 하였다. 또한, 신원을 확인할 때마다 새로운 Session key를 생성함으로써 데이터 재전송 공격을 방지하고 인증단계를 2단계로 처리하여 좀 더 안전한 거래가 될 수 있도록 설계하였다.

참 고 문 헌

[1] 이용희, "제3세대 이동통신과 모바일 금융서비스의 발전방향," 금융, 통권 제637호, pp. 20-29, 2007. 4.

[2] 김기영, 강동호, "개방형 모바일 환경에서 스마트폰 보안기술," 정보보호학회지, 제19권 제5호, pp. 21-28, 2009.10.

[3] W. Juang and J. Wu, "Efficient 3GPP authentication and key agreement with robust user privacy protect," Proceedings of the 2007 IEEE on Wireless Communications and Networking Conference, pp. 2720-2725, 2007.

[4] M. Zhang, Y. Fang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," *IEEE Transactions on Wireless Communications*, Vol. 4, No. 2, pp. 734-742, 2005.

[5] C. Huang, J. Li, "Authentication and key agreement protocol for UMTS with low bandwidth consumption," Proceedings of the 19th International Conference on Advanced Information Networking and Application 2005. pp. 392-397, 2005.

[6] Li Xi, Hu Han-Ping, "A secure mobile payment system," *Computer Technology and Application*, ISSN1934-7332, Vol. 1, No. 1, June 2007.

[7] 성순화, "안전한 모바일 결제 프로토콜을 위한 위임기관을 사용한 인증과 키 동의," 정보과학회논문지, 정보통신 제 37권 제2호, pp. 135-141, 2010.

[8] GPP TS 33.102 : "3G Security : Security Architecture," V3.10.0. Dec. 2001.

[9] 김신효, 정병호, "스마트카드 기반 휴대단말 보안기술 동향," 전자통신동향분석 제17권제3호, pp. 15-22, 2002. 8.

[10] 김춘수, "무선 네트워크 연동을 위한 USIM 보안 모듈 설계 및 구현," 정보보호학회논문지, 제17권 제2호, pp. 41-49, 2007.

[11] 송유진, 이재용, "무선 인터넷 환경의 USIM 인증 취약성과 보안메커니즘," 한국인터넷정보학회지, 제9권 제3호, pp. 32-37, 2008

[12] 원동규, 조은성, 양형규, 김승주, 원동호 "SIM/USIM의 표준화 동향에 관한 연구," 정보보호학회지 15권 3호, pp. 48-60, 2005

[13] 김두환, 정수환 "3GPP 네트워크에서 효율적인 인증 데이터 관리를 위한 개선된 AKA프로토콜," 정보보호학회논문지, 제19권 제2호, pp. 93-103, 2009.

정 은 희

1991년 2월 강릉대학교 통계학과 이학사
1998년 2월 관동대학교 전자계산공학과 석사
2003년 2월 관동대학교 전자계산공학과 박사

2003년 9월~현재 강원대학교 삼척캠퍼스 지역 경제학과 부교수
관심분야 : 네트워크 보안, 전자상거래, 웹 프로그래밍, 멀티미디어

이 병 관

1975년 2월 부산대학교 기계설계학과 졸업
1986년 2월 중앙대학교 전자계산공학과 석사
1990년 2월 중앙대학교 전자계산공학과 박사

1988년 3월~현재 관동대학교 컴퓨터학과 교수
관심분야 : 네트워크 보안, 컴퓨터 네트워크, 전자상거래