한국항행학회 논문지 제15권 제4호 2011년 8월

온라인 게임 환경에서 인증 및 ID 기반 키 관리 프로토콜 분석 연구

A Study on the Analysis of Authentication and ID-based key Management Protocol in Online Game Environment

이양선*, 박상오**

Yang-Sun Lee*, Sang-Oh Park**

요 약

IT 기술의 발전과 네트워크의 비약적인 발전에 따라 온라인 게임 환경에서 유선 네트워크와 무선 네트워크의 경계가 사라지고 유무선 통합 서비스 환경이 도래되고 있다. 그러나 유무선 통합 서비스 환경에 적합한 보안 기술은 아직 미비한 실정이며, 유무선 통합 환경의 특성으로 인해 유선 네트워크에서의 보안 위협뿐만 아니라 무선 네트워크에서의 보안 위협까지 고려해야 한다. 따라서 유무선 통합 환경을 고려한 다양한 연구가 진행되어 왔으며, 그 중 유무선 환경을 고려한 경량화된 ID 기반 인증 및 키 관리 연구가 진행되었다. 최근 Moon 등[1]은 퍼베시브 환경에서 인증 및 ID 기반 키 관리 프로토콜을 제안하였다. 그러나, Moon 등의 방식은 ID 기반 공개키 방식을 사용하여 연산량을 줄였으나 Pairing 기법을 사용함으로써 기존 공개키 방식과 유사한 연산량을 나타내고 있다. 따라서 본 연구는 Moon 등의 방식에서의 보안 취약점을 분석한다.

Abstract

The development of IT technology and breakthrough of the network and the wired network, wireless network boundaries disappear and wired and wireless integrated service environment is the advent in online game environment. However, the wired and wireless integrated service environment appropriate security technology is still inactive, wired and wireless integration environment due to the characteristic as well as security threats wired network and security threats in wireless networks should be considered. Therefore, This wired and wireless integrated environment has been considering studied various, Among them wired and wireless environment considering the lightweight of ID-based authentication and key management has been in progress. In recent, Moon et al. pervasive environment in authentication and ID-based key management protocol is proposed. However, Moon et al.'s scheme is use the ID-based public-key approach to decreased the amount of computation. However, pairing by using a technique similar to the existing public key scheme can represent the amount of computation. Therefore, In this paper the way of Moon etc in security vulnerability analysis.

Key words : ID-Based, Authentication, Key Management

I. 서 론

최근 게임 산업에서는 컴퓨터 통신의 비약적인 발전과 디바이스의 다양화에 따른 서비스 확대와 유무

* 조선대학교 정보통신공학과(Dept. of Information Communication Eng., Chosun University)
** 중앙대학교 컴퓨터공학부(Dept. of Computer Eng., Chung-Ang University)(교신저자 : sj1st@cs.cau.ac.kr)
· 제1저자 (First Author) : 이양선
· 투고일자 : 2011년 8월 12일
· 심사(수정)일자 : 2011년 8월 12일 (수정일자 : 2011년 8월 26일)
· 게재일자 : 2011년 8월 30일

선 통합 서비스 환경이 나타나고 있다. 이러한 유·무선 통합 서비스 환경은 기존의 무선 네트워크 환경과 유선 네트워크 환경이 결합됨에 따라 기술간 융합의 문제점 및 서비스 융합의 문제점 등 다양한 문제점이 발생하고 있다.

이러한 환경이 도래됨에 따라 보안 기술 개발은 더욱 어려움을 나타내고 있으며 유·무선 통합 서비스 환경에 적합한 보안 기술은 매우 미비한 실정이다. 또한 유·무선 통합 환경의 특성으로 인해 유선 네트워크에서의 보안 위협뿐만 아니라 무선 네트워크에서의 보안 위협까지 고려하여 보안 기술을 개발해야 한다. 이로 인해 유·무선 통합 환경을 고려한 다양한 연구가 진행되어 왔으며, 그 중 유·무선 환경을 고려한 경량화된 ID 기반 인증 및 키 관리 연구가 활발히 진행되고 있다.

최근 Moon 등[1]은 퍼베시브 환경에서 인증 및 ID 기반 키 관리 프로토콜을 제안하였다. 그러나, Moon 등의 방식은 ID 기반 공개키 방식을 사용하여 연산량을 줄였으나 Pairing 기법을 사용함으로써 기존 공개키 방식과 유사한 연산량을 나타내고 있다. 따라서 본 연구는 Moon 등의 방식에서의 보안 취약점을 분석한다.

본 논문의 구성은 다음과 같다. 2장에서는 연구의 기반이 되는 ID 기반 방식에 대하여 알아보고 보안 요구사항을 도출하며, 3장에서는 Moon 등의 방식을 설명한다. 4장에서는 Moon 등의 방식의 안전성 및 효율성을 분석을 하고, 마지막으로 5장에서는 결론 및 향후 연구방향으로 마치도록 한다.

Ⅱ. 연구배경

본 장에서는 논문의 기반이 되는 ID 기반 방식에 대하여 설명하고, 인증 및 ID 기반 키 관리를 위한 보안 요구사항을 도출한다.

2-1 ID 기반 방식

ID 기반 암호시스템은 A. Shamir[2]에 의해 1984년 최초로 소개된 것으로 사용자가 이미 가지고 있고 잘 알려진 이메일 주소 등의 정보로부터 사용자의 공개키를 생성하는 방식이다. 기존의 PKI 기반 방식과 ID 기반 암호 방식의 가장 큰 차이점은 신뢰성을 가지는 제 3자로부터 발급 받은 인증서의 필요 우무이다. 기본의 PKI 기반 방식은 사용자의 공개키가 사용자와 관계없는 임의의 값이므로 사용자에게 할당된 공개키에 대한 인증서를 발급해줄 제 3의 신뢰기관과 인증서 관리를 위한 구조가 필요하다. 그러나 ID 기반 방식에서는 사용자의 ID 나 이메일 주소 등의 정보에서 그 사용자의 공개키를 유추해낼 수 있어 공개키를 배포하는데 인증서를 필요로 하지 않기 때문에 기존 공개키 기반 방식보다 효율적으로 시스템 적용할 수 있다. 이러한 ID 기반 기법은 ID 기반 암호화 기법의 개념이 정립되었고, 2001년 D. Boneh와 M. Franklin이 발표한 논문에서 제안한 pairing 기법으로 구현되었다[3].

표 1. PKI 기반 방식과 ID 기반 방식 비교
Table 1. Comparison of PKI based scheme and ID based scheme

	PKI 기반	ID 기반
공개키 생성	사용자 및 RA에 의해 생성	신원정보로부터 누구나 쉽게 생성
인증서 유무	공개키와 사용자를 연결짓기 위한 인증서가 반드시 필요	공개키로 인증이 되기 때문에 인증서 불필요
부인 방지	사용자가 개인키를 생성함으로써 부인방지 기능 제공	개인키를 신뢰기관에서 대신 생성해 주기 때문에 부인방지 기능 미비
철회 기능	CRL, OCSP	철회기능이 필요하나 아직까지는 제공하지 못함

2-2 보안 요구 사항

유·무선 통합 환경에서 인증 및 ID 기반 키 관리를 제공하기 위해서는 유선 네트워크 환경뿐만 아니라 무선 네트워크 환경까지 고려한 보안 요구 사항을 고려해야 하며, 요구 사항은 다음과 같다.

- 네트워크를 통해 전송되는 데이터는 악의적인 제

3자로부터 보호되어야 하며, 공격자가 메시지를 획득하더라도 원문의 메시지를 확인할 수 없는 기밀성을 제공해야 한다. 또한 무선 네트워크 환경의 대역폭 및 통신량을 고려하여 경량화를 제공하면서도 비도가 높은 기밀성을 제공해야 한다.

- 송신자가 전송한 메시지가 중간에 위조 및 변조되지 않은 것을 수신자는 즉시 확인 가능해야하며, 공격뿐만 아니라 네트워크 오류 등으로 인한 메시지 변형을 검출할 수 있어야 한다. 이와 같이 무결성을 보장하기 위해서 일반적으로 해쉬함수 및 오류 검증 코드를 사용한다.

- 인증은 송신자가 전송한 메시지가 정당한 사용자로부터 전송된 것인지 확인할 수 있어야 하며, 서비스 접근 시 정당한 권한을 보유한 사용자라는 것을 확인할 수 있는 보안 서비스이다. 유무선 통합 서비스 환경에서는 네트워크간 로밍을 고려하여 효율적인 인증이 제공되어야 한다.

- 이 외에 접근제어 및 부인 봉쇄 등 기본적인 요구사항을 고려하여 서비스를 제공해야 한다.

- 또한, 유무선 통합 환경은 서두에 언급한 것과 같이 다양한 보안 위협을 내재하고 있기 때문에 제3의 공격자에 대한 대응을 고려해야 한다. 일반적으로 도청, 위장, 재전송공격, MITM(Man-In-The Middle attack) 등과 같은 보안 위협으로부터 안전해야 한다.

Ⅲ. 인증 및 ID 기반 키 관리 프로토콜

인증 및 ID 기반 키 관리 방식은 다양한 환경 및 플랫폼을 기반으로 많은 연구가 진행되어 왔으며, 그 중 ID 기반 방식은 기술적 특징으로 인해 경량화 및 이기종 네트워크 융합 등 연산량 감소가 필요한 시스템을 중심으로 Jiang 등[4]과 Lee 등[5]의 제안과 같이 많은 연구가 진행되었다[6-12]. 최근 2009년 8월 Moon 등은 퍼베시브 환경에서 인증 및 ID 기반 키 관리 프로토콜을 제안하였다. 이에 본 장에서는 Moon 등의 방식을 분석하고 취약점을 도출한다.

Moon 등의 방식은 이기종 네트워크 환경에서 디바이스가 홈 인증 서버에게 자신이 결제할 금액과 결제를 위한 정보를 전송하여 인증을 요청하고 티켓을 발급 받으며, 디바이스는 이기종 네트워크로 로밍 시 홈 인증 서버로부터 발급받은 티켓을 제공하면 외부 인증 서버는 인증 요청 메시지에 신뢰 관계 인가 요청 메시지를 추가하여 전송한다. 홈 인증 서버는 티켓을 검증하고 이기종 네트워크에서 모바일 디바이스를 인증할 수 있도록 ID 기반 개인키 생성 값을 전송한다. 디바이스는 인증을 받고 서비스를 제공받을 수 있다. 이기종 네트워크에서 디바이스의 서비스 이용에 따라 티켓에 포함되어 있는 선불 금액 정보에서 이용한 금액만큼 차감을 하고 티켓을 재구성 하여 과금을 처리한다. 이후의 로밍 및 인증은 전과 동일한 단계를 거쳐 수행한다. 이로 인해 디바이스는 과금에 관한 정보 및 인증 요청을 매번 홈 인증 서버에게 전송하지 않아도 되며, 신뢰 관계를 유지하는 서버에서 처리할 수 있다. 또한 다른 이기종 네트워크로 이동하면, 이전 단계의 서버와 신뢰 관계를 구성하고 디바이스를 효율적으로 인증할 수 있다.

Moon 등의 방식은 총 3단계로 구성되며, 디바이스의 일련번호 및 패스워드와 대칭키는 등록 단계에서 분배되었다고 가정하며, 다음은 시스템 파라미터 이다.

- 개체: (MD: 디바이스, AAAH: 홈 인증서버, HN_domainID: 외부 인증서버)
- ID: 식별자, PW: 패스워드, h(): 해쉬함수
- PIN: 디바이스 시리얼 번호
- AT: 인증 시간 값
- OTP: 일회용 패스워드
- e: $G1 \times G1 \rightarrow G2$ Bilinear Map
- α, β, χ, γ, υ, ω: 인증을 위한 값
- MAC: 메시지 인증 코드
- KGV: ID 기반 키 생성 값
- E[ ]: 암호화, Sign: 서명
- KU/KR: ID 기반 공개키쌍

- KUCert/KUCert: 인증서 기반 공개키쌍
- KS: 사전 공유키
- Account_info: 과금 정보
- Balance_info: 잔액 정보
- Balance_inf orenewal: 갱신된 잔액 정보

인증 및 티켓 발행 과정은 디바이스가 홈 인증 서버에게 결제할 금액 정보와 인증 요청을 하며, 홈 인증 서버는 정당한 사용자라고 판명되면 티켓을 생성하고 발급한다. 본 단계는 내부 네트워크에서의 디바이스와 홈 인증 서버간의 상호 인증 단계이다. 암호키는 ID 기반 공개키/개인키 쌍을 생성하여 사용함으로써 기밀성을 제공하며 pairing 기반의 암호화 방식을 사용한다(그림 1 참조).

과금 정보 갱신 과정은 디바이스가 홈 네트워크에서 이기종 네트워크로 로밍 시 이기종 네트워크를 관리하는 인증 서버에게 홈 인증 서버로부터 발급받은 티켓을 이용하여 인증을 받는다. 인증이 완료되면, 서비스를 이용하고 이용에 따른 금액을 티켓의 과금 정보에서 차감하고 티켓을 갱신하여 과금한다. 이 과정 역시 이기종 네트워크 인증 서버와 ID 기반 공개키 방식을 이용하여 안전성을 제공한다(그림 2 참조).

계층적 신뢰 관계를 이용한 과금 정보 갱신 과정은 디바이스가 이전에 이동한 이기종 네트워크에서 또 다른 이기종 네트워크로 이동하였을 때, 이전 인증 서버가 갱신한 티켓을 이용하여 인증을 받고 과금 정보 갱신 과정과 동일한 프로토콜을 거친다. 이와 같은 방식은 기존에 연구된 로밍 인증 방식과는 다르게 홈 인증 서버로 인증 및 티켓 갱신을 요청하지 않고 이기종 네트워크에서 모든 프로세스가 처리됨으로써, 홈 인증 서버의 로드를 감소시킬 수 있다(그림 3 참조).

Ⅳ. 인증 및 ID 기반 키 관리 프로토콜 분석

Moon 등의 방식의 전체 프로토콜은 그림 1, 2, 3과 같으며 ID 기반 공개키 방식을 사용하여 연산량을 줄였으나 Pairing 기법을 사용함으로써 기존 공개키 방식과 유사한 연산량을 나타내고 있으며, 여전히 인증서 기반 공개키를 사용함으로써 연산량이 증가하는 문제점을 가지고 있다. 본 장에서는 Moon 등의 방식을 안전성 및 효율성에 중심으로 분석한다.

인증 및 티켓 발행 프로토콜에서 디바이스는 ID 기반의 공개키를 생성하는데 공개되어있는 밑수 g에 ID를 지수승 연산하여 생성하기 때문에 공격자는 디바이스의 공개키를 쉽게 생성 가능하여 위장 및 서비스 거부 공격에 위험하다. 아래와 같이 공격자가 임의이 공개키를 생성하여도 공개키를 확인하는 과정이 없기 때문에 공격에 노출되기 쉽다.

디바이스의 공개키 생성 : $KU_{MD} = g^{ID_{MD}}$

공격자의 임의의 공개키 생성 : $KU_{MD}{}' = g^{ID_{MD}'}$

- 또한 개인키를 생성할 때 입력되는 파라미터인 ID 기반 키 생성 값은 사전에 공유되는 대칭키를 이용한 메시지 인증 코드로 생성한다. 이는 대칭키를 이용한 ID 기반 개인키를 생성하는 것으로써, 대칭키를 빈번하게 갱신해 주어야한다.

- 인증 및 티켓 발행 프로토콜에서는 이기종 네트워크와 홈 네트워크간 통신에서 PKI 기반 공개키 방식을 사용하기 때문에 효율성이 떨어진다.

- 무결성 검증을 위해 해쉬 함수와 메시지 인증 코드를 사용하나 해쉬 함수는 디바이스 일련번호만 해쉬하며 메시지 인증 코드는 바로 검증 되는 것이 아니라 일회용 패스워드를 확인한 이후에 검증하기 때문에 무결성을 바로 제공하기 어렵다. 이로 인해 서비스 거부 공격을 받더라도 사전에 차단할 수 있는 방안이 마련되어 있지 않다.

- 재전송 공격을 방어하기 위해 인증 시간 값 및 일회용 패스워드와 티켓의 유효시간을 사용하나 인증 시간 값은 디바이스와 홈 인증 서버가 동기화된 시간을 사용하는 것이 아닌 각각의 시간을 사용하기 때문에 동기화 문제가 발생한다. 또한 일회용 패스워드는 매 세션 변경되어야 하나 로밍 및 티켓 갱신에도 기존에 사용하는 일회용 패스워드가 입력 값으로 들어가게 되어 실질적인

freshness를 제공하지 못한다.

- 신뢰 관계 서버를 이용한 빠른 로밍 인증은 티켓의 유효시간에 따라 갱신 횟수 및 갱신 여부가 결정된다. 그러나 티켓의 갱신이 과금에 따라 갱신되기 때문에 너무 빈번하게 발생하여 오히려 홈 인증 서버로 접근하여 갱신되는 시나리오 보다 더 많은 오버헤드가 발생할 가능성이 있다.

- 디바이스가 서비스를 이용할 때 과금 처리 부분은 디바이스 중심으로 이루어진다. 그러나 이는 디바이스의 과금 정보를 신뢰할 수 없고 불확실하기 때문에 네트워크 에이전트를 통한 과금 처리가 필요하다.

- 오버헤드 분석을 보면 이기종 네트워크에서의 일반적인 인증 방식과 비교하였으나 일반적인 인증 방식에 대한 설명이 전혀 되어 있지 않으며, 또한 인증 방식 분석에 대한 검증도 되어 있지 않아 효율성을 검증할 수 없다.

- 결과적으로 퍼베시브 환경을 위해 제안한 방식이 오히려 안전성 및 효율성 저하를 가져오며, 퍼베시브 환경을 고려한 경량화된 프로토콜이 필요하다. 계층적 신뢰 관계 서버를 이용하여 홈 인증 서버로드 로드는 감소 시킬 수 있으나, 이 역시 디바이스의 연산량 증가 때문에 전체적인 측면에서 효율성이 저하된다고 볼 수 있다.

V. 결 론

본 논문은 온라인 게임 환경에 필요한 인증 및 ID 기반 키 관리 분석을 위해 2009년 Moon 등이 제안한 기법을 안전성 및 효율성 측면에서 분석하였다. Moon 등의 방식은 퍼베시브 환경을 고려하여 ID 기반 공개키 방식, 일회용 패스워드, 티켓 방식, pairig 기반 암호 방식 등을 사용하였다.

그러나, 홈 인증 서버와 이기종 인증 서버와의 통신에서 PKI 기반 공개키 방식을 사용하며, ID 기반 공개키 방식에서 아이덴티티의 검증 과정이 없어 서비스 거부 공격 및 위장 공격에 노출 되며, 티켓의 갱신 문제, 디바이스 중심의 과금 처리 등의 문제점이 발견되었다.

향후 온라인 게임 환경만의 보안 요구사항을 도출하여 안전성 및 효율성을 제공할 수 있는 방안에 대하여 제시할 것이며, Moon 등의 방식과의 비교 분석을 통해 효율성을 제공할 것이다.

참 고 문 헌

[1] Jong Sik Moon, Deok Gyu Lee, Jong Hyuk Park, Im Yeong Lee, "Authentication and ID-Based Key Management Protocol in Pervasive Environment," *WIRELESS PERSONAL COMMUNICATIONS, 2009.08.* (Online Pullished)

[2] A. Shamir, “Identity-based cryptosystems and signature schemes,” *CRYPTO’84,* pp. 47–53, 1984.

[3] 김경신, “효율적인 ID기반 강한 검증자 지정 서명 기법,” *고려대학교 정보경영공학전문대학원 석사졸업논문* 2010.

[4] Jiang, J., He, C., and Jiang, L. G., "On the Design of Provably Secure Identity-Based Authentication and Key Exchange Protocol for Heterogeneous Wireless Access," *ICCNMC,* pp. 972-981, 2005.

[5] 이원진, 김은주, 전일수, “스마트카드를 이용한 ID 기반의 사용자 인증 프로토콜,” *한국컴퓨터종합학술대회,* Vol. 32, No. 1, pp. 166-168, 2005.

[6] Wang, H., Yao, G., and Jiang, Q., "An identity-based group key agreement protocol from pairing," The 2008 Third International Conference on Availability, *Reliability, Security (ARES),* pp. 532-537, 2008.

[7] Wang, S., Cao, Z., Choo, K.-K. R., and Wang, L. "An improved identity-based key agreement protocol and its security proof," *ISCI, 179(3)*, pp. 307-318, 2009.

[8] M.Scott, "Cryptanalysis of an ID-based Password Authentication Scheme using Smart Cards and Fingerprints," *IACR e-print archive,* 2004.

[9] J.P. Jeong, M. Y. Chung and H.S. Choo, "Integrated

OTP-Based User Authentication Scheme Using Smart Cards in Home Networks," *HICSS,* pp. 294, 2008.
[10] H.J. Bae, H.S. Kim, K.Y. Yoo, "ID-based key exchange protocol using smart cards," *Korea Computer Congress 30(1),* pp.l 491-493, 2003.
[11] S.U. Lee, "ID-based Wireless LAN Authentication Technique Between Terminals," *Kyungpook National University Graduate School,* 2004.
[12] H.S. Kim, S.W. Lee, K.Y. Yoo, "ID-based password authentication scheme using smart cards and fingerprints," *ACM Operating Systems Review 37(4),* pp. 32-41, 2003.
[13] J.K. Lee, S.R. Ryu, K.Y. Yoo, "Fingerprint-based remote user authentication scheme using smart cards," *Electronics Letters 38(12),* pp. 554-555, 2002.

이 양 선 (李洋先)

2001년 동신대학교 전기전자공학과 졸업(공학사)
2003년 동신대학교 대학원 전기전자공학과 졸업(공학석사)
2007년 목원대학교 대학원 IT 공학과 졸업(공학박사)
2007년 2월~2009년 9월 : (주)휴메이트 기술연구소 기획팀장
2009년 10월~현 재 : 조선대학교 정보통신공학과 연구교수
관심분야 : 멀티미디어통신, 유비쿼터스, UWB통신, 무선통신시스템

박 상 오 (朴像吾)

2005년 중앙대학교 컴퓨터공학과 졸업(공학사)
2007년 중앙대학교 컴퓨터공학과 졸업(공학석사)
2010년 중앙대학교 컴퓨터공학과 졸업(공학박사)
2010년 9월~현 재 : 중앙대학교 문화콘텐츠기술연구원 전임연구원
관심분야 : 내장형시스템, 사이버물리시스템, NAND 플래시 메모리 파일시스템, 저전력 시스템, 유비쿼터스 컴퓨팅

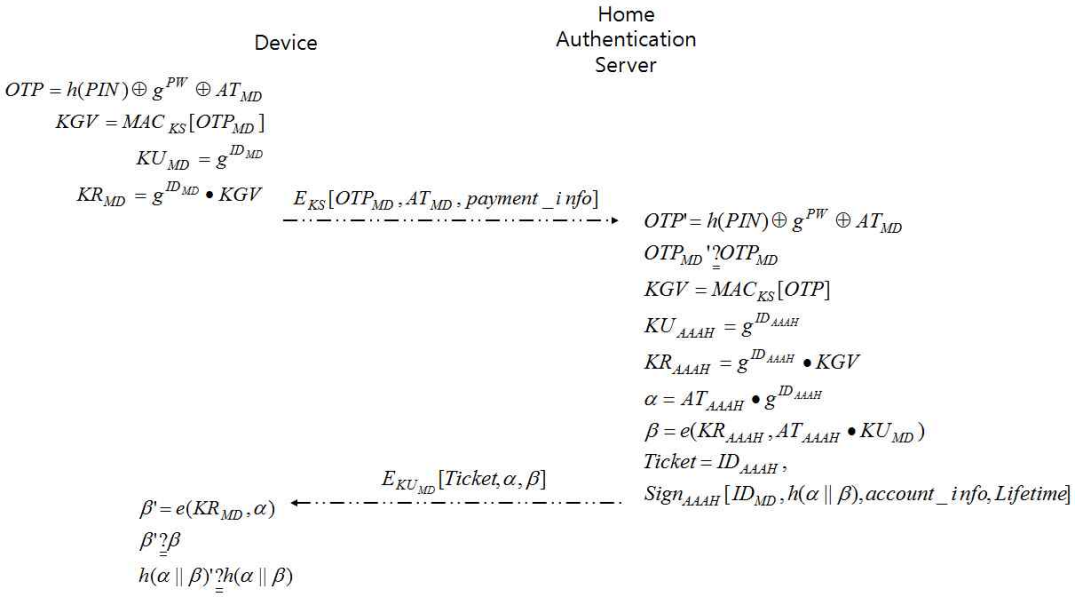

그림 1. 인증 및 티켓 발행 프로토콜
Fig. 1 Protocol of authentication and ticket issue

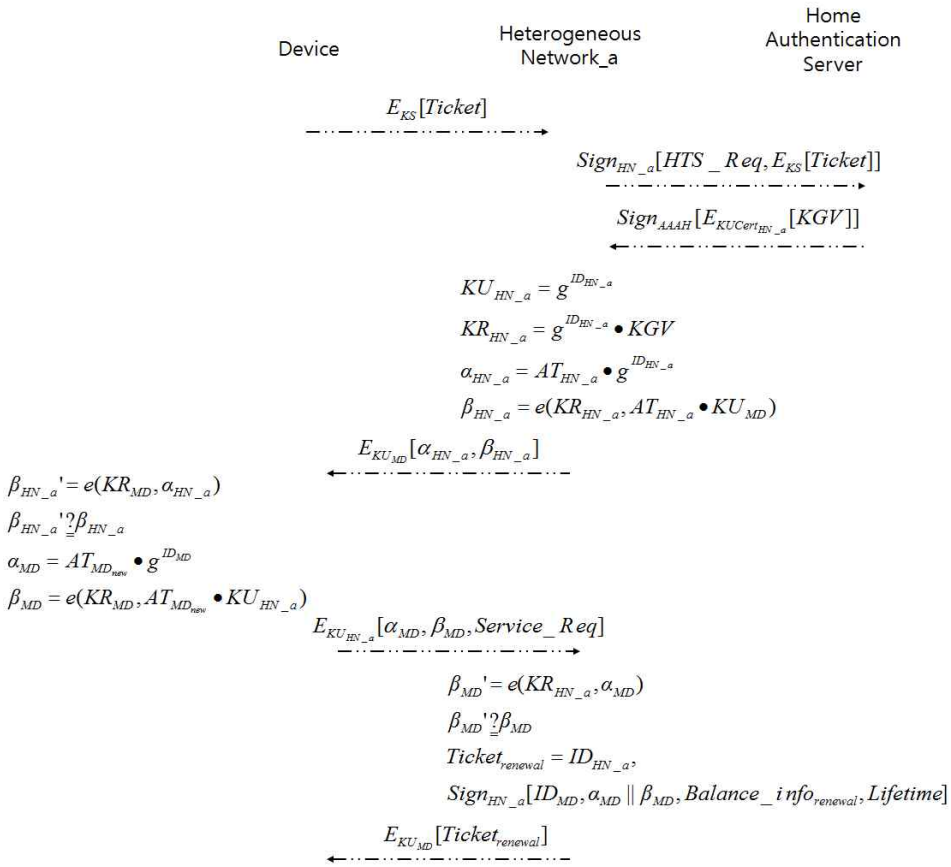

그림 2. 과금 정보 갱신 프로토콜
Fig. 2 Protocol of accounting information renewal

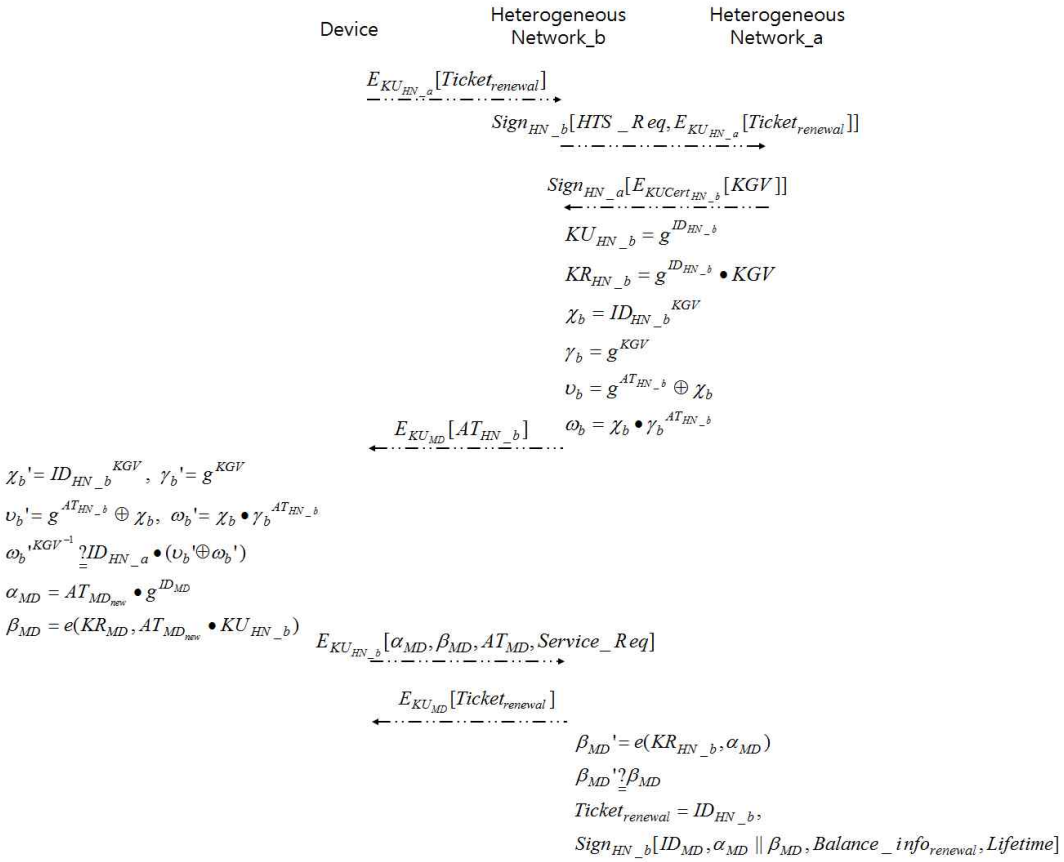

그림 3. 계층적 신뢰 관계를 이용한 과금 정보 갱신 프로토콜
Fig. 3 Protocol of accounting information renewal using hierarchal trust relation