情報保護學會論文誌
第20卷 第1號, 2010. 2

Binary CDMA 망을 위한 안전한 AKA 프로토콜*

김 용 희,[1†] 박 미 애,[1] 조 진 웅,[2] 이 현 석,[2] 이 장 연,[2] 이 옥 연[1‡]
[1]국민대학교, [2]한국전자부품연구원

Secure AKA(Authentication and Key Agreement) Protocol for Binary CDMA Network*

Yong-Hee Kim,[1†] Mi-Ae Park,[1] Jin-Woong Cho,[2] Hyeon-Seok Lee,[2]
Jang-Yeon Lee,[2] Okyeon Yi[1‡]
[1]KookMin University, [2]Korea Electronics Technology Institute

요 약

Koinonia 시스템은 무선 네트워크에서 QoS를 보장하는 Binary CDMA(Code Division Multiple Access)의 장점을 이용하여 설계되었다. 본 논문에서는 Koinonia 시스템을 기반으로 한 새로운 네트워크 구조인 BLAN(Binary CDMA LAN)을 제시하고, 이 구조에 적합한 안전하고 효율적인 AKA 프로토콜을 제안한다. 제안한 프로토콜을 이용한 BLAN은 강한 안전성과 높은 이동성을 지원할 수 있으며, 사용자 신원 모듈을 이용하여 보다 강한 사용자 인증을 제공하는 특징을 가진다. 우리는 이러한 연구가 특수한 환경의 공공망에도 적합하며 더 나아가 WLAN을 대체할 수 있는 새로운 네트워크 모델 제시에 도움이 될 수 있을 것으로 기대한다.

ABSTRACT

Koinonia system is designed to fully utilize the advantage of Binary CDMA so as to guarantee QoS in wireless networks. In this paper, we propose the new network structure based on this system and refer to it as BLAN(Binary CDMA LAN). Although BLAN is similar structure to IEEE 802.11 WLAN, it will ensure the fast handover and QoS. We also propose the AKA(Authentication and Key Agreement) protocol and Reauthentication protocol to be used for communication in BLAN. These protocols are securely and efficiently designed using the user identity module to support the more powerful authentication. Hence, BLAN, including the proposed protocols, will support the high mobility and security. In conclusion, we expect that BLAN can be applied to future infrastructure on special environment, and it can be helpful showing the new network model which alternate WLAN.

Keywords: Binary CDMA, Koinonia, AKA(Authentication and Key Agreement), Reauthentication

I. 서 론

Binary CDMA 기술은 WLAN이나 Bluetooth와 같은 다양한 무선 기술들의 혼재에 따른 주파수 배정 문제나 QoS(Quality of Service) 보장 문제를 해결하기 위해 제안된 무선 기술이다[1]. 또한, Binary CDMA 기술을 기반으로 한 Koinonia는 2009년 1월에 국제 표준화 기구 ISO/IEC JTC SC6에서 표준으로 채택된 시스템으로 기존의 여러 기술과의 상호 운영이 가능하고 잡음이 많은 무선 환경에서도 QoS를 보장하며 기존 통신 시스템에 간섭을 일으키지 않고 동시에 사용할 수 있는 특징을 가진다. 그리고 최근에는 Binary CDMA 기술에 기

접수일(2009년 9월 11일), 수정일(2009년 11월 12일), 게재확정일(2009년 12월 11일)
* 본 연구는 지식경제부 및 한국산업기술평가관리원의 IT산업원천기술개발 사업의 일환으로 수행하였음. (2009- S-039-01, u-City용 Binary CDMA 기반 무선 보안 기술 개발)
† 주저자, dragon-61@hanmail.net
‡ 교신저자, oyyi@kookmin.ac.kr

반하여 무선 암호화 기술을 적용한 Guardian 기술이 개발 중에 있다[2,12,13]. 따라서 이런 기술을 다양한 무선 통신에 활용하려는 연구도 활발히 진행되고 있다.

그러나 무선 상에서 다양한 보안 위협들이 날로 늘어가고, 이로 인해 개인 정보나 국가 기관의 중요한 정보가 유출 되거나 또는 장비의 심각한 손상을 초래하는 등 많은 피해가 발생하고 있다. 현재 널리 사용되고 있는 IEEE 802.11 WLAN의 경우, 보안이 강화된 IEEE 802.11i를 권고하고 있지만 실제 환경에서는 비용이나 관리상의 문제로 기대하는 만큼의 보안을 제공하지 못하는 것이 현실이다. 이런 이유로 공공망이나 일부 조직에서는 제한적인 내장 보안 기능을 사용하거나, 혹은 전면 금지하는 경우가 많아졌다. 또한 공공망 설계시 공공 기관에 도입되는 보안 제품에 탑재하는 것이 의무화된 암호 기술이 ARIA[3]이므로 AES를 사용한 802.11i WLAN이 안전성을 보장한다 하더라도 채택하기에는 어려움이 있다.

따라서 본 논문에서는 IEEE 802.11 WLAN[5]을 대체할 수 있는 새로운 공공망 모델로 Koinonia 시스템을 기반으로 하며, ARIA가 적용 가능한 새로운 유무선 네트워크 구조인 BLAN(Binary CDMA LAN)을 제시하고, 이 구조에 보안을 제공하기 위한 토대가 되는 인증과 키일치 프로토콜을 제안한다. 특히, 사용자의 빈번한 이동성을 예측하여, 이를 위한 핸드오버 시나리오를 제시하고 빠른 핸드오버를 제공하기 위한 재인증 프로토콜도 제안한다. BLAN은 RAP(Radio Access Point)를 이용한 네트워크 구조로 IEEE 802.11 WLAN과 유사한 형태이지만 물리적으로 취약한 RAP들을 관리하고, 빠른 핸드 오버를 지원하기 위해 새로운 서버를 추가한 것이 특징이고, 이 구조 안에서 안전한 통신을 위해 제안한 인증 프로토콜인 BLAN-AKA는 사용자 신원 모듈인 BSIM(Binary CDMA Subscriber Identity Module)을 기반으로 한 인증 프로토콜로써 기기 인증보다는 좀 더 사용자 인증에 가까운 인증을 가능하게 하였고, 사전에 홈 환경과 공유된 키를 사용한 상호 인증으로 사용자를 보호하기 위해 네트워크 인증을 우선하는 것이 특징이다.

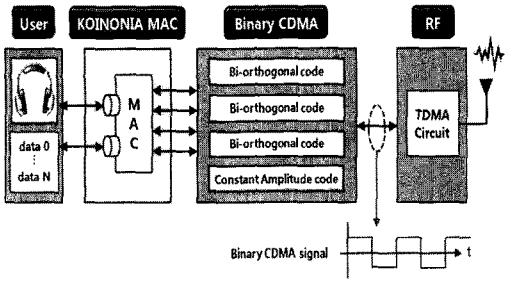
본 논문의 구성은 다음과 같다. 2장에서는 BLAN의 기반이 되는 Koinonia 시스템에 대해 소개하고, 새로운 유무선 네트워크인 BLAN의 구조와 각 개체에 대해 정의한다. 또한 인증 프로토콜 설계에 고려해야 할 보안 위협과 이에 관련된 보안 요구 사항을 정리하고, 이동성을 설명하기 위해 핸드오버를 정의한다. 3장은 BLAN에서 사용될 키 체계와 인증 프로토콜인 BLAN-AKA, 이동성 지원을 위한 재인증 프로토콜을 제안한다. 4장은 제안한 프로토콜의 특성과 안전성을 분석하였으며, 마지막 5장은 결론이다.

II. Background

2.1 Koinonia 시스템

Koinonia는 국내 독자 기술로 2009년 1월 국제 표준화 기구인 ISO/IEC JTC SC 6에서 표준으로 채택된 근거리 디지털 무선 통신 기술이다[2]. 이 시스템은 크게 물리 계층과 데이터 링크 계층으로 나뉘고, 데이터 링크 계층은 매체 접근(MAC) 부계층과 Adaptation 부계층으로 나뉜다. 매체 접근 부계층은 물리 계층인 Binary CDMA의 특성(즉, 기존의 다중코드 CDMA 방식에 발생되는 다양한 레벨의 변조 신호를 이진화하여 외형적으로 TDMA 신호 파형으로 전송하는 구조로 잡음이 강한 CDMA 특성과 전력 소비량이 적으면서도 초고속 전송을 가능하게 한 TDMA(Time Division Multiple Access) 장점을 동시에 가진)을 살려 코드와 시간 슬롯의 조합을 통해 매체접근을 하는 HMA(Hybrid Multiple Access) 방식을 사용한다. Adaptation 부계층은 하위 프로토콜 스택과 상위의 다른 무선 표준의 프로토콜 스택을 호환해주는 역할을 한다. 그림 1은 Koinonia 시스템을 보여준다.

Koinonia 시스템은 잡음이 많은 무선 환경에서도 QoS를 보장하고, 다양한 디지털 기기들을 하나의 네트워크(Koinonia 네트워크)에 묶어 상호 운영을 가능하게 하며, 기존 통신 시스템에 간섭을 일으키지 않고 동시에 사용할 수 있는 특성을 가진다. 특히, 혼잡 운영지역에서의 간섭과 소비 전력 문제를 해결하여 북



[그림 1] Koinonia 시스템

〔표 1〕 근거리 무선 통신 기술 비교

구 분	Koinonia v1.0	Bluetooth v1.2	802.11b	UWB
서비스 범위	10~100m	10~100m	10~100m	1~10m
QoS	○	△	×	△
모 듈	Binary CDMA	FHSS: GFSK	DSSS: QPSK/CCK	CDMA:PSK DFDM:QPSK
원천기술 보유	○	×	×	×
네트워크 토폴로지	Ad-hoc/인프라	Ad-hoc	Ad-hoc/인프라	Ad-hoc/인프라
국제표준 주체	한 국	유 럽	미 국	미 국

미나 유럽이 주도하는 Bluetooth, 802.11b 등 기존 근거리 무선 통신 기술이 가지는 한계점을 극복하였다. 표 1은 근거리 무선 통신 기술을 비교한 것이다.

또한 Koinonia 시스템은 Binary CDMA 무선 구간의 암호화 서비스를 위해 ARIA와 AES를 모두 사용할 수 있도록 개발되고 있으므로 국내 기간망 및 공공기관에 사용할 수 있다. 이러한 Koinonia 시스템은 근거리 무선 네트워크 기기 표준화 기술 개발, 시스템 개발과 수요의 창출을 통하여 국내 업체의 경쟁력을 갖출 수 있고, 또한 관련 산업의 핵심 기술로 발전하여 가전 산업의 무선 디지털 가전기기와 통신 산업의 WPAN용 휴대 단말기 및 WLAN 접속기와 반도체 산업의 저전력 주문형 반도체와 전자 산업의 무선 PostPC 등에서 핵심기술로써 통합, 발전될 전망이다[4].

2.2 BLAN(Binary CDMA LAN) 구조

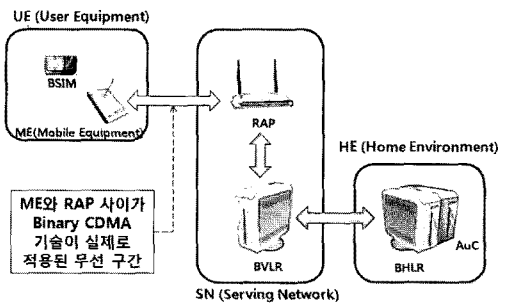
BLAN은 그림 2처럼 유무선으로 이루어진 구조로 UE(User Equipment), SN(Serving Network), HE(Home Environment)로 구성 된다. UE와 SN 사이는 무선 구간이고, SN과 HE 사이는 유선 구간이다.

2.2.1 UE (User Equipment)

UE는 BLAN의 사용자 영역으로, BSIM(Binary CDMA Subscriber Identity Module)과 ME(Mobile Equipment)로 구성된다. BSIM은 각 사용자가 개별적으로 소유한, 가입자를 식별하고 인증하는데 사용되는 장치이다. 즉, BSIM은 사용자 인증에 필요한 암호 알고리즘과 가입자의 서비스 프로파일을 저장하고 있으며, 따라서 기능적으로 3G의 USIM(Universal Subscriber Identity Module)[6]과 유사하게 고려될 수 있다. ME는 실제 무선 구간에서 모든 물리적인 연결을 책임지는 인터페이스와 BSIM과의 상호작용을 위한 인터페이스를 제공하는 장치이다.

2.2.2 SN (Serving Network)

SN은 사용자에게 여러 가지 서비스를 제공하기 위한 주체로 RAP(Radio Access Point)와 BVLR (BLAN Visitor Location Register)로 구성된다. RAP는 사용자와 네트워크를 연결하는 접근 장치가 되며, ME와의 사이에 Binary CDMA 기술을 이용한 무선 인터페이스를 제공한다. BVLR은 자신의 영역 내에 있는 RAP들을 관리하고, HE(Home Environment)와의 상호작용을 통해 사용자에게 인증 서비스를 제공하는 개체이다. BVLR은 상대적으로 물리적인 보안 위협이 가장 큰 RAP가 직접 인증을 수행하지 않도록 함으로써, 사용자 정보나 인증 정보 등의 중요한 비밀의 직접적인 노출을 최소화하여 전체 네트워크의 안전성을 높일 수 있다. 또한 BVLR이 실제 인증의 주체로 작동하기 때문에 3.3절의 핸드오버와 관련된 재인증 프로토콜을 가능하게 함으로써, 동일 BVLR내의 RAP 사이에서의 핸드오버를 효율



〔그림 2〕 BLAN(Binary CDMA LAN) 구조

적으로 관리하여 높은 이동성을 제공할 수 있는 토대를 제공한다. 마지막으로 BVLR은 부분적인 소규모 네트워크 추가를 용이하게 한다. 단일 BVLR과 필요한 수의 RAP로 구성된 네트워크를 특정 지역에 추가하는 것이 용이하며, 이를 기존의 전체 네트워크와 다른 보안 등급으로 관리하는 것도 가능하다. 또한 여전히 높은 이동성을 제공할 수 있으므로, 공사 현장이나 프로젝트를 위한 임시 공간 등에 네트워크를 구축해야 하는 경우에 효과적이다.

2.2.3 HE(Home Environment)

HE는 사용자의 개인 정보 및 권한 정보를 저장하며, BLAN-AKA 메커니즘을 지원한다. HE는 BHLR(BLAN Home Location Register)과 인증서버(AuC)로 구성된다. BHLR은 사용자를 관리하기 위한 DB(database)로 가입자 신원과 이와 관련된 정보, BVLR에 관한 정보를 저장한다. 이에 반해, AuC는 각 사용자의 인증과 암호화, 무결성 등에 필요한 데이터를 가지며, 각 사용자에 대해 사전에 공유한 마스터키 MK와 필요한 다른 키를 생성하기 위한 함수를 저장하고, 또한 사용자의 인증 요청시 인증에 필요한 데이터를 생성한다. 비록 BHLR과 AuC가 논리적으로 서로 다른 개체이지만, 실제로는 물리적으로 동일하게 구현될 수 있다.

2.3 BLAN 인증 프로토콜의 보안 요구사항

2.2절에서 살펴본 바와 같이 BLAN은 유무선이 혼재하는 네트워크이다. 그러나 이 새로운 네트워크에 대한 보안을 고려할 때, 핵심이 되는 부분은 무선 구간을 포함하는 UE와 SN 구간이다. 보안 관점에서 SN과 HE 사이는 기존의 여러 유선 네트워크와 크게 다르지 않으며, 또한 SN내의 RAP와 BVLR 사이도 이 구간을 확장한 것으로 고려될 수 있다. 따라서 우리는 BLAN의 유선 구간, 즉 RAP↔BVLR과 BVLR↔BHLR 사이에는 안전한 채널이 형성되어 있어서, 각 개체 사이의 상호 인증 및 모든 통신의 안전성이 보장된다고 가정할 것이다. 예를 들어 VPN 등을 이용하여 이러한 가정을 쉽게 충족시킬 수 있기 때문에, 이 가정은 프로토콜의 특징과 안전성에 대한 분석을 한정하기 위한 매우 합리적인 가정이다. 따라서 이러한 가정 하에, 이 절에서는 먼저 무선 인터페이스에서 발생할 수 있는 다양한 보안 위협[7,8]에 기반하여, 본 논문의 주제인 인증과 키일치에 관련된 여러 가지 보안 요구사항을 정의한다.

2.3.1 인증

본 논문에서 고려하는 상호인증 대상은 사용자의 UE와 HE로부터 인증을 위임받은 SN이 된다. 즉, UE와 SN 사이가 상호인증의 대상이다. 이러한 과정은 사용자와 네트워크 사이에 메시지 교환으로 진행되며, 이 과정 후에 사용자는 연결된 네트워크가 자신의 HE에서 제공되고 신뢰되었다는 것을 확신할 것이고, 네트워크는 주장하는 사용자의 신원이 사실이라는 것을 확인하게 될 것이다.

2.3.2 기밀성

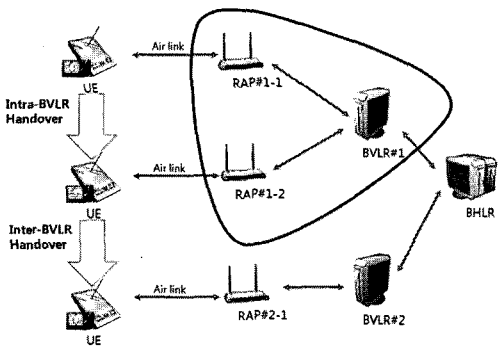
기밀성은 2가지로 구분될 수 있는데, 사용자 기밀성과 사용자 데이터 기밀성이 그것이다. 사용자 기밀성은 사용자의 신원을 사용하는 대신에 임시 신원을 사용하여 사용자의 위치 정보나 그 밖의 사용자에 관련된 개인 정보를 보호하는데 목적이 있다. 사용자 데이터 기밀성은 UE와 RAP 사이의 실제 데이터를 보호하기 위해 인증 프로토콜이 성공적으로 완료된 이후에, ARIA와 같은 블록 암호 알고리즘을 사용하여 수행된다.

2.3.3 무결성

메시지의 출처나 내용을 검증하기 위한 보안 성질이다. 메시지에 의도되지 않은 변경이나 고의적인 훼손이 없었는지를 확인하기 위하여, 일반적으로 MAC (Message Authentication Code) 알고리즘을 사용하여 구현된다.

2.4 핸드오버

무선망에서 서비스의 연속성을 위한 핸드오버는 필수 서비스 중 하나이다. BLAN 환경에서는 UE가 한 RAP에서 다른 RAP로 연결을 전환할 때가 핸드오버가 될 것이고, 이럴 경우에 기존의 어떠한 무선망보다도 매우 빈번한 핸드오버가 발생할 것으로 예측된다. 따라서 빠른 핸드오버를 지원하기 위한 인증 프로토콜이 별도로 필요하며, 이를 AKA 프로토콜과 구별하기 위해서 재인증 프로토콜로 정의한다. 그러나 모든 핸



〔그림 3〕 핸드오버의 2가지 종류의 예

드오버에 동일한 재인증 프로토콜을 적용하는 것이 비효율적일 수 있으므로, 먼저 핸드오버를 그 성격에 따라 다음과 같은 2가지로 구분한다.

2.4.1 Intra-BVLR 핸드오버

Intra-BVLR 핸드오버는 단일 BVLR 내에서의 핸드오버를 뜻한다. 즉, 동일한 BVLR에 연결된 서로 다른 RAP 사이를 UE가 이동할 때 발생하는 핸드오버이다. 이때는 UE와 BVLR로 다전에 인증을 성공적으로 수행했내에서의 핸드의미하므로, 이를 이용한 재인증 프로토콜로 더 효율적인 인증 방법로 이동할 때 그림 3의 경우에는 UE가 동일한 BVLR#1에 연결된 RAP#1-1에서 RAP#1-2로 (혹은 그 반대 방향으로) 이동할 때, 이러한 Intra-BVLR 핸드오버가 발생한다.

〔표 2〕 2가지 핸드오버의 비교

		Intra-BVLR 핸드오버	Inter-BVLR 핸드오버
정 의		동일 BVLR 내의 상이한 RAP 사이의 이동	다른 BVLR에 각각 연결된 RAP 사이의 이동
인증 특징		기존 BVLR과의 인증결과 이용 가능	새로운 BVLR에 대한 인증이 요구됨
발생 가능성		높 음	낮 음
인증 프로토콜		재인증 프로토콜	BLAN-AKA
Key update	TK	불필요	필 요
	SK	필 요	필 요

2.4.2 Inter-BVLR 핸드오버

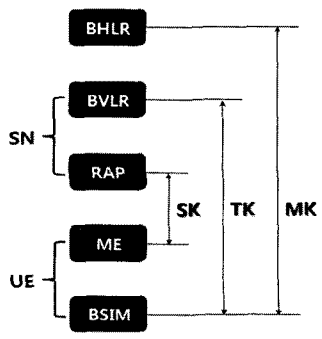
상이한 BVLR에 각각 연결된 RAP 사이에서의 핸드오버를 의미한다. 이러한 경우에는 새로운 BVLR에 대한 인증이 반드시 필요하다. 따라서 기존 BVLR로부터 이러한 인증에 필요한 정보를 획득하거나 또는 BHLR을 이용한 새로운 AKA 과정이 요구된다. 전자의 경우 BVLR 사이에 새로운 secure 채널을 요구한다. 이 채널은 핸드오버의 경우를 제외하면 사용성이 그다지 크지 않을 것이므로, 따라서 전체 네트워크의 효율성을 고려하면 이미 존재하는 각 BVLR과 BHLR 사이의 채널을 이용하는 후자의 인증 방법이 더 바람직할 것이다. 즉, BVLR이 바뀌는 핸드오버의 경우에는 재인증이 아니라 AKA 과정을 다시 수행하는 것이 오히려 더 효율적이다. 그림 3은 Intra-BVLR 핸드오버와 Inter-BVLR 핸드오버의 예를 보여주며, 표 2는 각 핸드오버의 차이점을 정리한 표이다.

III. BLAN-AKA 및 재인증 프로토콜

이 장에서는 먼저, 사용되는 키들에 대한 체계를 구축하고, BLAN 환경에 적합하고 안전한 AKA 프로토콜과, 효율적인 핸드오버를 지원하기 위한 재인증 프로토콜을 제안한다.

3.1 키 체계

제안한 인증 프로토콜에 사용되는 키는 MK, TK, SK 총 3개이다. MK(Master Key)는 BHLR과 BSIM이 사전에 공유한 비밀키로, 사용자와 네트워크의 상호인증을 위한 비밀 값이다. 이 값은 중간 개체, 즉 BVLR, RAP, ME에게 노출되지 않는다.



〔그림 4〕 제안한 프로토콜의 키 체계

TK(Temporary Key)는 MK로부터 유도된 임시키로, 주로 핸드오버 등의 재인증에 사용된다. BHLR에 의해 생성되지만 AKA 과정에서 BVLR에 전달되어, BSIM과 BVLR 사이에 공유되는 비밀키이다. 재인증시에는 TK가 AKA 과정의 MK 역할을 수행한다. 마지막으로 SK(Session Key)는 성공적인 인증의 결과물로써, 이후의 실제 Binary CDMA가 적용된 무선 구간의 모든 트래픽을 보호하기 위해 사용되는 키다. 그림 4는 각 개체와 공유된 키들을 나타낸다.

3.2 BLAN-AKA

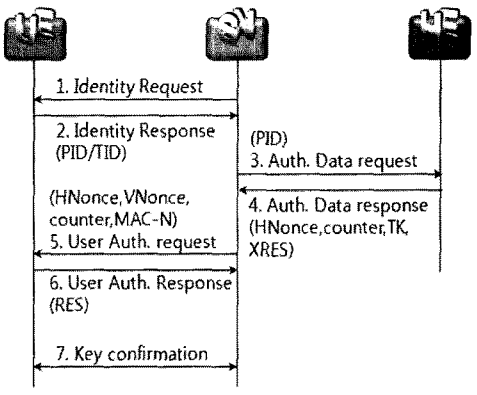
AKA는 사용자와 네트워크 사이의 상호인증과 키 일치를 통해, 이후의 트래픽에 대한 무결성과 기밀성 보호와 같은 보안 특징을 제공하기 위해 선행되어야 하는 과정이다. 그림 5는 BLAN-AKA 과정을 간단히 표현하며, 각 단계에 전송되는 데이터 및 구성 개체들이 처리해야 하는 과정은 다음과 같다.

1. SN이 UE에게 Identity Request를 전송함으로써 AKA 과정이 시작된다. 이후, RAP는 세션키 SK를 BVLR로부터 수신할 때까지, UE와 BVLR 사이의 통신을 단지 중계만 한다.
2. Identity Request를 수신한 UE는 Identity Response로 영구 사용자 신원인 PID(Permanent ID)나 임시 사용자 신원인 TID(Temporary ID)를 전송한다. PID는 BSIM이 HE에 등록한 사용자의 영구 신원이며, TID는 이전의 AKA 과정을 통해 상호인증 된 SN, 특히 BVLR로부터 수신한 임시 신원이다. TID는 PID을 숨김으로써 사용자의 위치 기밀성을 보장하는데 이용된다.
3. BVLR은 AKA를 위해 필요한 사용자의 데이터를 얻기 위해, UE로부터 수신한 PID를 BHLR로 전송한다. 만일 TID를 수신했다면, 이에 대응하는 PID를 찾아 BHLR로 전송한다. 수신한 TID와 대응하는 적절한 PID를 찾을 수 없다면, UE에게 PID를 전송할 것을 요청하고 단계 2부터 다시 시작한다. PID를 수신한 BHLR은 HNonce를 생성하고, 사전에 BSIM과 공유한 마스터 키 MK를 이용하여, KDF(Key Derivation Function)로 임시키 TK를, MAC(Message Authentication Code)으로 사용자 인증을 위한 XRES를 계산한다. 그 후, HNonce, TK, XRES, counter를 BVLR로 전송한다. counter는 3GPP의 SQN[9]과 유사한 개념으로, 프로토콜에 freshness를 보장하기 위해 사용되는 변수이며, BSIM과 BHLR이 각각 update 한다.

   $TK = KDF(MK, HNonce, counter)$

   $XRES = MAC(MK, HNonce, counter)$
4. 필요한 데이터를 단계 3에서 수신한 BVLR은 이것을 이용하여, 사용자를 인증한다. 즉 제안한 BLAN-AKA 프로토콜에서 사용자를 인증하는 개체는 BHLR로부터 이 권한을 위임받은 BVLR이 된다. 사용자 인증을 위해, BVLR은 우선 VNonce를 생성하고 이것과 TK를 이용하여 MAC-N을 계산한다. MAC-N은 사용자가 네트워크 즉, SN과 HE를 인증하는데 사용된다. BVLR은 HNonce, VNonce, MAC-N, counter를 AKA Request로 UE에게 전송한다.

   $MAC\_N = MAC(TK, VNonce, counter)$
5. UE는 MAC-N을 확인해서 네트워크를 인증한다. 인증에 실패하면, 인증 거부를 통보하고 연결을 종료한다. 인증에 성공한다면, 수신한 counter가 허용 범위 내에 있는지를 확인한다. 수신한 counter 검증에 실패하면, counter 재동기를 위한 재동기 요청을 BVLR로 전송하고, BVLR은 이를 BHLR에 통보한다. 이때 BHLR은 이 메시지를 검증하여 counter를 update하고 새로운 AKA 과정을 시작할 수 있다. counter 검증에 성공한다면 BSIM은 자신의 counter를 update한다. 이후, VNonce를 이



[그림 5] BLAN-AKA 프로토콜

용하여 세션키 SK를 생성한다. 그리고 자신의 인증을 위한 RES를 계산하여, 이를 AKA Response로 BVLR에 전달한다.

$SK = KDF(TK, VNonce, counter)$

$RES = MAC(MK, HNonce, counter)$

6. BVLR은 XRES와 RES가 동일한지 확인하여 사용자를 인증한다. 인증에 성공하면, VNonce와 TK를 이용하여 SK를 생성하여, 이를 RAP에 전달한다. 또한 키일치 과정에 사용될 ANonce도 SK와 함께 전달한다. ANonce는 재인증 과정에서도 사용되므로, RAP가 생성하는 것보다는 BVLR이 생성하여 RAP에게 전달하는 것이 효율적이다. UE 쪽에서는 BSIM이 ME에게 SK를 전송한다.
7. UE와 RAP는 각자 수신한 SK가 서로 동일한지를 확인하기 위한 키일치(key confirmation) 과정을 수행한다. 이 과정은 이후의 실제 트래픽을 보호하기 위해 사용되는 보안 알고리즘을 이용하여 진행되는 것이 일반적이다. 이는 키일치와 더불어 알고리즘에 대한 일치도 확인할 수 있기 때문이다. 따라서 키일치 과정에 사용되는 MAC 알고리즘은 단계 6까지의 인증 과정에 사용되었던 MAC 알고리즘과 다를 수 있다. (구분을 위하여 수식에서는 소문자로 표현하였다) 키일치 과정은 그림 6과 같다.

$MAC1 = mac(SK, ANonce)$

$MAC2 = mac(SK, ANonce + 1)$

BLAN-AKA가 성공적으로 완료되면, BVLR과 UE는 AKA 과정에서 공유한 데이터 중에서 TK와 ANonce를 이후의 재인증에 대비해 각자 저장하고, BVLR은 AKA가 성공적으로 완료되었음을 BHLR에 통보하여, BHLR이 counter를 update할 수 있도록 한다.

3.3 재인증 과정

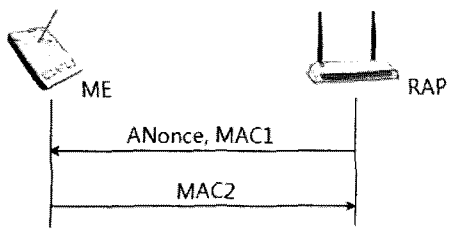


그림 6. BLAN-AKA의 키 일치 과정

빈번한 핸드오버가 발생할 시, 재인증을 제공하는 것은 오버헤드를 줄여 빠른 핸드오버를 가능하게 한다. 이러한 인증은, 이전의 전체 AKA 과정을 통해 BSIM과 BVLR이 공유한 비밀값을 이용하여 수행될 수 있다. 제안된 BLAN-AKA 프로토콜에서는 TK가 이러한 비밀값이 된다. 즉, TK는 AKA 과정을 통해서 update되고, 동일 BVLR 내의 RAP 사이에서의 핸드오버는 이 TK를 이용한 인증을 수행하는 것이다. 핸드오버에 대한 내용은 2.4절에 있다.

그림 7은 RAP#1-1과 RAP#1-2가 동일한 BVLR#1과 연결을 유지할 때, UE가 RAP#1-1에서 RAP#1-2로 이동한 경우인, intra-BVLR 핸드오버 재인증 과정을 보여준다.

1. Intra-BVLR 핸드오버가 발생하면, UE는 재인증을 위해 임시 사용자 신원인 TID를 BVLR에 전송한다.
2. BVLR은 이 TID와 대응하는 PID를 찾고, AKA 과정에서 저장해 두었던 TK와 ANonce를 이용하여 새로운 세션키 SK′을 생성하고, 새로 생성한 ANonce′을 UE에게 전송한다. AKA 과정과 비교할 때, MAC-S는 키일치 과정에서 사용한 MAC1과 유사하다. 단지 SK와 ANonce 대신 SK′과 ANonce′이 사용되었을 뿐이다.

$SK' = KDF(TK, ANonce)$

$MAC\text{-}S = MAC(SK', ANonce')$

3. UE는 BVLR과 마찬가지로, 이전 AKA 과정에서 저장해 두었던 TK와 ANonce, BVLR로

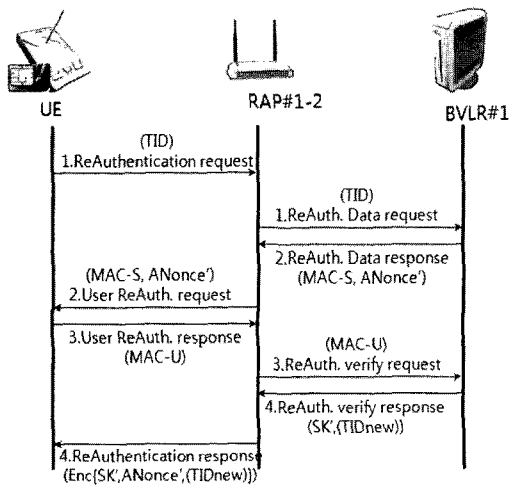


그림 7. 재인증 프로토콜

부터 새로 수신한 ANonce′을 이용하여, SK′을 생성하고, MAC-S를 검증한다. 검증에 성공하면, 이에 대한 응답으로 MAC-U를 계산해서 이를 BVLR에게 전송한다.

$MAC\_U = MAC(SK', ANonce'+1)$

4. BVLR이 수신한 MAC-U의 검증에 성공하면, ANonce′을 SK′으로 암호화한 값을 UE에게 전송한다. 만약 TID의 재할당이 필요하다면, 새로운 TID 값인 TIDnew를 함께 암호화하여 전송한다.

재인증 과정을 AKA 과정과 비교해보면, AKA에서는 다음과 같고,

$SK = KDF(TK, VNonce, counter)$
$MAC1 = mac(SK, ANonce)$
$MAC2 = mac(SK, ANonce+1)$

재인증 과정에서는 아래와 같다.

$SK' = KDF(TK, ANonce)$
$MAC\_S = MAC(SK', ANonce')$
$MAC\_U = MAC(SK', ANonce'+1)$

즉, 재인증에서는 VNonce 대신에 ANonce가, ANonce 대신에 ANonce′이 사용되었다는 것을 확인할 수 있다. 정리하면, 이전 AKA의 키일치 과정에 사용되었던 nonce를 다음 재인증의 키 유도에 사용한다는 것이다. 이와 같은 방법으로의 재인증이 완료된 후, 차후의 재인증에서는 ANonce′이 새로운 세션키를 생성하기 위해 사용될 것이다. 이를 위해 재인증이 완료된 후, UE와 BVLR은 각자 ANonce를 ANonce′으로 update해야 한다.

제안된 재인증 프로토콜은 BLAN-AKA와 비교할 때 표3과 같은 장점을 가진다. 메시지 전송 횟수는 UE가 PID 혹은 TID를 전송하는 것을 시작으로 카운트 하였으며, BLAN-AKA에서는 인증이 완료된 후 BHLR에게 통보하는 과정이 별도로 진행되어야 하기 때문에 총 12회가 되었다. 또한 표에 나타난 알고리즘 연산 횟수는 각 개체의 생성과 검증을 구별하여 계산하였다. 따라서 XRES/RES를 제외한 나머지 각 parameter들은 2회의 연산 횟수를 가진다. 재인증 프로토콜에서 나타나는 메시지 전송 횟수 및 연산 횟수에서 현저한 감소는 BLAN-AKA 과정에는 참여하는 BHLR의 참여 배제와 인증과 키 교환을 동시에 수행하는 재인증 프로토콜의 특성 때문이다. 재인증 프로토콜에서는 세션키 SK′이 인증을 통해 검증되기 때문에, 별도의 키 일치 과정을 수행할 필요가 없다.

〔표 3〕 BLAN-AKA와 재인증 프로토콜의 비교

구 분		BLAN-AKA	재인증 프로토콜
메시지 전송 횟수		12회 (무선구간 5회)	8회 (무선구간 4회)
알고리즘 연산 횟수	MAC /mac	8회 (RES/XRES, MAC-N, MAC1,MAC2)	4회 (MAC-S, MAC-U)
	KDF	4회 (TK, SK)	2회 (SK′)
기 타			암/복호화 2회 (그림7의 과정4 참조)

IV. 제안 프로토콜 분석

2.3절에서 언급했던 기본적인 보안 요구사항인 상호인증, 기밀성 및 무결성, freshness 등을 보이는 것은 3장의 프로토콜 소개와 부분적으로 언급된 보안 사항을 참조하면 어려운 일이 아니므로, 이 장에서는 BLAN의 구조와 비교될 수 있는 WLAN등과의 보안 특징을 비교 분석할 것이다. 비교 결과는 표4로 나타나며, 이 장의 각 절은 표의 각 항목에 대해 부연 설명한다. 먼저 분석의 범위를 한정하기 위해, 2.3절에서 언급했던 것처럼 BLAN의 유선 구간, BHLR↔BVLR과 BVLR↔RAP 사이에는 안전한 채널이 형성되어 있다고 가정한다.

4.1 사용자 인증

단말 인증을 수행하는 WLAN과 달리[11], BLAN은 USIM과 유사한 BSIM을 이용함으로써 사용자 인증에 근접한 인증을 수행한다. 이는 단말 이용의 효율성을 향상시키고, 개인 프라이버시를 더 강력하게 보호할 수 있음을 의미한다. 또한 BSIM의 성능 향상 및 USIM과의 호환성 연구를 통해, BLAN 시스템과 3G 혹은 4G 시스템과의 연동 가능성을 기대할 수 있게 한다.

4.2 이동성 보장

〔표 4〕 BLAN과 여타 무선망과의 보안 특징 비교

구 분	BLAN	WLAN	WiBro	3GPP
사용자 인증	○	△	○	○
이동성 보장	○	△	○	○
재동기 여부	△	×	×	○

핸드오버의 포인트가 비교적 넓은 영역을 다루는 3G의 RNC(Radio Network Controller)나 WiBro의 RAS(Radio Access Station)/ACR (Access Control Router)에 비해, WLAN이나 BLAN은 핸드오버의 포인트가 상대적으로 좁은 영역을 다루는 AP 혹은 RAP이다. 이는 사용자의 활동성을 동일하게 가정했을 경우, WLAN이나 BLAN의 핸드오버가 상대적으로 빈번하다는 것을 의미한다. 따라서 WLAN이나 BLAN에서 이동성 보장은 중요한 이슈 중의 하나이다. 보안 관점에서 WLAN의 이동성 지원을 고려해보면, AAA 프로토콜의 결과로 공유되는 정보인 MSK(Master Session Key, AAA-Key)가 AP로 직접 전송됨으로써, 만약 AP가 훼손된다면 MSK를 이용한 재인증 프로토콜은 이 AP를 경유한 모든 station에게 영향을 줄 수 있다. AP가 상대적으로 취약한 장비이므로 이러한 가정은 간과할 수 없는 위협이다. 따라서 WLAN에서의 재인증 프로토콜은 MSK를 이용보다는, IAPP(Inter-Access Point Protocol)같은 AP간의 새로운 프로토콜을 이용해야 한다. 그러나 빈번한 핸드오버를 가정한다면 AP간의 새로운 프로토콜은 과도한 트래픽을 유발할 뿐만 아니라, 이전 MSK를 이용하지 않으면서, 전체 인증 프로토콜을 수행하는 것보다 빠른 새로운 핸드오버 프로토콜의 안전성을 보장하는 것도 쉬운 문제는 아니다. 이에 반해 BLAN은 WiBro의 ACR과 기능적으로 유사한 핸드오버를 위한 BVLR을 이용하여, 이러한 문제를 해결한다. 인증의 결과로 생성되는 TK를 RAP에 전달하지 않고 BVLR이 유지함으로써, 재인증에서 UE는 BVLR과의 간단한 인증만으로 안전성을 보장할 수 있다. 보안상 상대적으로 취약한 RAP가 TK를 저장하지 않기 때문에, 단일 RAP의 훼손이 WLAN에서처럼 핸드오버 전체의 안전성에 영향을 주지는 않는다. 더구나 3.3절에서 언급된 것처럼 제안한 BLAN 재인증 프로토콜에서는 다음번 재인증에 사용될 세션키 SK'을 이전 인증에서 사용되었던 ANonce와 TK를 이용하여 BSIM과 BVLR이 각각 미리 생성할 수 있으므로 좀 더 빠른 인증을 지원할 수 있다. 따라서 빈번한 핸드오버가 발생하더라도 제안한 프로토콜을 이용하는 BLAN은 이를 효율적으로 처리할 수 있다.

4.3 재동기 여부

M.Zhang 등은 3GPP-AKA의 SQN 동기화의 어려움을 지적하고, 이를 해결하기 위해 AP-AKA 프로토콜을 제안하였다[10]. 3GPP-AKA에서 이러한 재동기의 어려움은 3G가 글로벌 통신 시스템이라는 점 이외에도 HLR(Home Location Register)이 n개의 AV를 생성하고, 이를 VLR(Visitor Location Register)에 한 번에 전달하는데 그 원인이 있다. 즉, 단일 사용자에 대해 비교적 원거리에 위치한 다수의 VLR에 분배된 AV들이 이러한 재동기의 어려움을 유발하는 것이다. 그러나 제안된 BLAN-AKA에서는 비교적 근거리의 BVLR들의 요청에 의해, BHLR이 단 한 개의 인증 데이터 묶음만을 전송하고 또한 성공적인 BLAN-AKA 과정 완료 후에만 BSIM과 BHLR이 각각 update할 수 있기 때문에, 재동기가 발생할 가능성은 매우 희박하다. 따라서 제안된 인증 프로토콜에는 재동기 요청이 발생할 시, 이를 보안 정책상 무조건 공격이 있었던 것으로 가정하거나, 혹은 효율성을 고려하지 않은 강력한 재동기 프로토콜을 적용하는 것이 가능하다. 이러한 이유로 제안한 프로토콜에서의 재동기 여부는 3GPP-AKA에서와는 달리 보안상 중요한 문제는 아니다.

V. 결 론

본 논문에서는 ARIA 적용이 가능함으로써 공공망 무선 시스템에 적합하고, BVLR을 이용하여 높은 이동성을 제공할 수 있는, Koinonia를 기반으로 하는 네트워크 구조인 BLAN에서 사용될 수 있는 안전하고 효율적인 인증 프로토콜인 BLAN-AKA와 이동성 지원을 위한 재인증 프로토콜을 제안하였다. 제안한 인증 프로토콜은 BSIM을 이용한 사용자 인증과 높은 이동성 지원을 위한 BVLR의 이용, 재인증 프로토콜을 제공한다는 특징을 가진다. 여타의 무선 기술과는 다른 뚜렷한 특징을 갖는 Koinonia 시스템을 이용한 이러한 BLAN의 특성과 이에 적합한 BLAN-AKA/재인증 프로토콜은 Binary CDMA 기술의 보급과 기존 무선 기술로 해결할 수 없었던 공공망 등의 다양한 분야에 폭넓게 활용될 수 있을 것으로 기대된다.

참 고 문 헌

[1] 안호성, 류승문, 나성웅, "Binay CDMA 소개," JCCI 2002, VI-A.1, Apr. 2002.

[2] KETI, "Koinonia 표준규격서, 물리 계층과 데이터링크 계층 규격 버전 1.0," 2003년 5월.

[3] 산업자원부 기술표준원, "128비트 블록 암호 알고리즘 ARIA," KS X 1213:2004, 2004년 12월.
[4] 강성진, 홍대기, 주민철, 조진웅, "Binary CDMA를 이용한 홈 네트워크," 정보통신설비학회논문지, 3(1), pp. 56-74, 2004년 3월.
[5] IEEE 802.11 standard, "Wireless Lan medium Access Control (MAC) and Physical layer(PHY) specification," June 2007.
[6] 3rd Generation Partnership Project, "Technical Specification Group Core Network and Terminals; USIM and IC card requirements (Release 8)," 3GPP 21.111 V8.2.0, June 2008.
[7] 3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; 3G Security; Security Threats and Requirements (Release 4)," 3GPP TS 21.133 V4.1.0, Jan. 2002.
[8] C. Boyd and A. Mathuria, Protocols for Authentication and Key Establishment, Springer, Sep. 2003.
[9] 3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 8)," 3GPP TS 33.102 V8.1.0, Dec. 2008.
[10] M. Zhang and Y. Fang, "Security Analysis and Enhancements of 3GPP AKA protocol," IEEE Transactions on Wireless Communication, vol. 4, no. 2, pp. 734-742, Mar. 2005.
[11] 윤종호, 무선 LAN 보안 프로토콜, 교학사, 2004년 10월.
[12] 임순빈, 정쌍봉, 이태진, 전선도, 이현석, 권대길, 조진웅, "Koinonia 고속 WPAN에서 보안을 위한 대칭/비대칭 비밀 키 교환 방법," 한국통신학회논문지, 31(6B), pp. 551-560, 2006년 6월.
[13] 강성진, 홍대기, 이현석, 조진웅, "Design methodology : Binary CDMA를 기반으로 하는 Koinonia 시스템의 모뎀 설계," IT SOC magazine, 통권 제15호, pp. 44-50, 2006년 11월.
[14] 김두환, 정수환, "3GPP 네트워크에서 효율적인 인증 데이터 관리를 위한 개선된 AKA 프로토콜," 정보보호학회논문지, 19(2), pp. 93-103, 2009년 4월.
[15] 김대영, 최용강, 김상진, 오희국, "프라이버시와 완전한 전방향 안전성을 제공하는 UMTS 키 동의 프로토콜," 정보보호학회논문지, 17(3), pp. 81-90, 2007년 6월.
[16] L. Chen, "Recommendation for key derivation using Pseudorandom Functions," NIST SP800-108, Nov. 2008.

〈著者紹介〉

김 용 희 (Yong-Hee Kim) 학생회원
2001년 2월: 광운대학교 수학과 졸업
2003년 8월: 광운대학교 수학과 석사
2003년 8월~현재: 국민대학교 수학과 박사과정
〈관심분야〉 정보보안, 이동통신 암호 프로토콜

박 미 애 (Mi-Ae Park) 정회원
1992년 2월: 국민대학교 수학과 석사
2007년 2월: 국민대학교 수학과 박사
2009년 3월~현재 : 국민대학교 정보보안연구소 연구원
〈관심분야〉 보안 프로토콜, 이동통신, 무선통신

조 진 웅 (Jin-Woong Cho) 정회원
2001년 2월: 광운대학교 전자통신공학과 박사
1999년 1월~1999년 12월: (일본)Electrotechnical Lab. STA fellow 초빙연구원
1993년 7월~현재: 전자부품연구원 통신네트워크 센터장
2004년~현재: 산업표준심의회 JTC/SC6 표준전문가(산자부)
2006년~현재: 신기술인증 및 IR52 장영실상 심의의원
〈관심분야〉 Binary CDMA, 무선 PAN 통신 시스템, 통신 SoC

이 현 석 (Hyeon-Seok Lee) 정회원
2000년 2월: 한양대학교 전자,전자통신,전파공학과 학사
2002년 2월: 한양대학교 전자통신,전파공학과 석사
2002년 1월~2003년 2월: 삼성전기 주임연구원
2003년 2월~현재: 전자부품연구원 선임연구원
〈관심분야〉 무선통신 시스템 (MAC, Network Layer)

이 장 연 (Jang-Yeon Lee) 정회원
1996년 2월: 한양대학교 전자통신공학 학사
2002년 2월: 한양대학교 전자통신전파공학 석사
1996년 2월~2000년 3월: 삼성전자 주임연구원
2002년 1월~현재: 전자부품연구원 선임연구원
〈관심분야〉 무선통신(WPAN,WLAN), H/W 보드설계

이 옥 연 (Okyeon Yi) 종신회원
1990년 2월: 고려대학교 수학과 이학석사
1996년 8월: University of Kentucky 이학박사
1999년 7월~2001년 8월: 한국전자통신연구원 선임연구원(팀장)
2001년 9월~현재: 국민대학교 자연과학대학 수학과 부교수
2009년 3월~현재: 국민대학교 정보보안연구소 소장
〈관심분야〉 정보보안, 이동통신 보안, 스마트그리드 보안