情報保護學會論文誌
第 22 卷 第 1 號, 2012. 2

3GPP LTE 네트워크에서의 핸드오버 키 관리 기법의 취약점 연구*

한 찬 규,† 최 형 기‡
성균관대학교

Security Weaknesses of Handover Key Management in 3GPP LTE Network*

Chan-Kyu Han,† , Hyoung-Kee Choi‡
[1]Sungkyunkwan University

요 약

LTE/SAE는 공격자의 키 획득 및 공격에 노출된 네트워크 노드를 고립시키기 위해 핸드오버 키 관리기법을 정의하고 있다. 본 논문에서는, 핸드오버 키 관리 기법이 비동기화 공격에 의해 전방향안전성이 보장되지 못 함을 보일 뿐만 아니라, 재전송 공격을 통해 안전한 핸드오버 키 전달을 저해하여, 핸드오버 지연을 유발할 수 있음을 보인다. 또한 상기의 공격들을 방지하기 위한 해결책을 제시하고, 해결책에 따른 연산 및 통신소모를 분석한다.

ABSTRACT

LTE/SAE has presented the handover key management to revoke the compromised keys and to isolate corrupted network devices. In this paper, we identify that the handover key management is vulnerable to de-synchronization attacks, which is jeopardizing the forward secrecy of handover key management. Also, an adversary could prevent the UE from creating the secure link with eNodeB, which is delaying the handover procedure. In this paper, we present a counrermeasure to prevent above attacks, and analyze the performance issues of the proposed protocol.

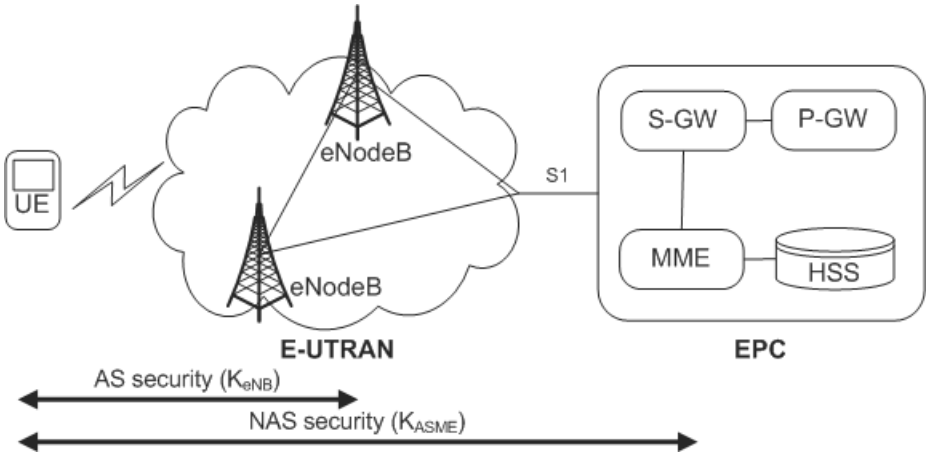
Keywords: LTE security, handover key management, 3GPP, mobile network

I. 서 론

3GPP Long Term Evolution (LTE)/System Architecture Evolution(SAE)는 Evolved Packet System (EPS)를 통하여 무선구간에서의 지연을 감소하고, All-Internet Protocol (IP) 망을 구현하는데 목표를 두고 있다. All-IP망이란 Internet Protocol (IP) 프로토콜을 기반으로 한 망 구조로, 유무선 통합 및 방송통신 융합서비스에 적합하다. 또한 네트워크 지연을 감소시키고, 플랫(flat) IP 구조를 지원하기 위해 기지국 및 기지국 제어기는 evolved NodeB (eNodeB)로 통합되었다. 악의적인 사용자들은 보다 손쉽게 eNodeB에 접근할 수 있으며, 코어망과의 구획이 단축됨에 있어 악성공격 또한 늘어나는 추세이다. 일례로 댁내기지국을 통한 위장기지국(rogue base station) 제작 위험성이 보고되었다[1][2]. 또한 eNodeB는 각기 다른 네트워크 관리자에 의해 운용될 수 있기 때문에, eNodeB 간 보안을 보장할 수 없는 실정이다.

eNodeB에 관련된 공격을 방지하기 위해, EPS에

접수일(2011년 4월 14일), 수정일(2011년 7월 13일), 게재확정일(2011년 12월 12일)
* 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No.2011-0005037)
† 주저자, hedwig@ece.skku.ac.kr
‡ 교신저자, hkchoi@ece.skku.ac.kr



〔그림 1〕 EPS 네트워크 구조

서는 사용자가 eNodeB를 바꿀 때마다 무선구간 키를 갱신하는 핸드오버 키 관리기법을 정의하고 있다〔3〕. 핸드오버 키 관리기법에서는 특정 시점의 eNodeB가 이전 무선구간 키 또는 이후 무선구간 키를 획득할 수 없도록 후방향 및 전방향 안전성(backward/forward secrecy)을 보장하고 있다. 본 논문에서는 EPS 핸드오버 키 관리기법이 비동기화 공격에 취약하여 전방향 안전성을 보장하지 못 함을 보인다. 또한 재전송 공격을 통해, 핸드오버를 지연시킴을 보인다. 본 논문에서는 비동기화 공격, 재전송 공격이 성립함을 보이고, 이에 대한 보안 대책을 마련하고자 한다. 본 논문의 제안 기법은 새로운 성능 문제를 야기하지 않고, 기존 EPS-AKA가 가지는 보안속성〔6〕을 모두 만족한다.

II. 관련연구

위장기지국 공격〔1〕〔4〕은 3GPP 모바일 네트워크의 취약점으로 다수 연구되었다. 2세대 3GPP 모바일 네트워크(Global System for Mobile Communications: GSM)에서의 위장기지국 공격으로는 중간자공격을 통한 호 가로채기 (call stealing) 및 호 위장 (call spoofing) 등이 연구되었다〔4〕. 3세대 3GPP 모바일 네트워크(Universal Mobile Telecommunications System: UMTS)에서는 대표적으로 리다이렉트 공격 (redirect attack)을 통한 부당한 과금 및 보안세션 도청, 그리고 인증벡터 재사용 공격이 연구되었다〔1〕. 4세대 3GPP 모바일 네트워크인 EPS에서의 위장기지국 공격은 아직 보고된 바가 없으나, 3GPP 표준〔2〕에서 위장기지국 공격 가능성에 대하여 기술하고 있다. EPS에서의 보안연구는 주로 조사연구(survey)를 통해 이루어지고 있다. EPS 보안 관련 연구로는 EPS의 전반적인 보안 요구사항과 핸드오버의 종류에 관한 연구〔5〕가 대표적이다. 본 논문에서 대상으로 하는 핸드오버 키 관리에 관련된 연구〔6〕에서는 핸드오버 키 운영에 관한 정책을 기존 세션키 전달 방식과 비교하였다. EPS의 All-IP 특성으로 인한 공격으로는 IP 위조 및 서비스 거부공격, 웜 등이 연구되었다〔7〕. 하지만 실제로 LTE/SAE 상에서의 네트워크 및 보안 기법 특성을 활용한 공격에 대한 연구는 미비한 실정이다.

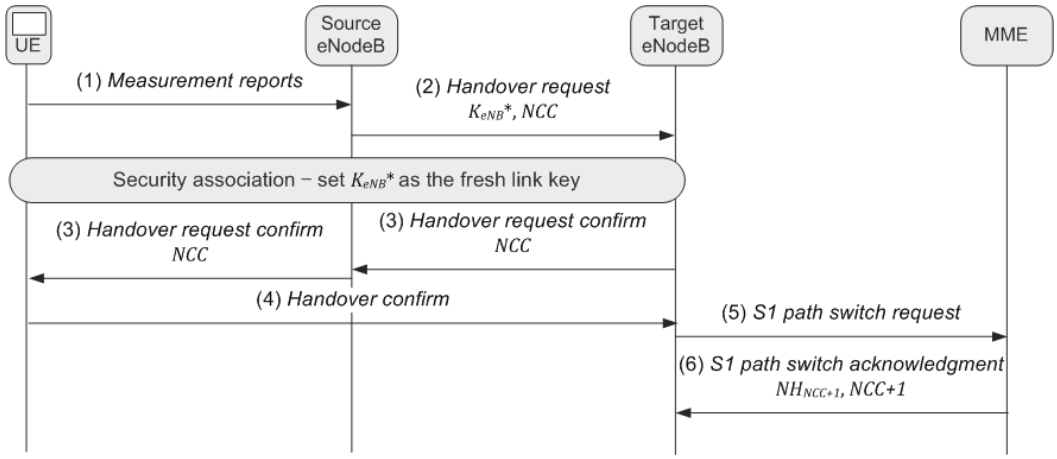
III. EPS 네트워크 구조 및 핸드오버 키 관리 방법

3.1 EPS 네트워크 구조 및 계층 별 보안

EPS 네트워크는 코어망인 Evolved UMTS Terrestrial Radio Access Network (E-UTRAN)과 액세스 망인 Evolved Packet Core (EPC)로 구성된다. 〔그림 1〕에 간략한 EPS 네트워크 아키텍처를 도시하였다. E-UTRAN에서는 지연을 줄이기 위하여 네트워크 노드를 eNodeB로 단일화하고, IP 스택을 추가하였다. 또한 〔그림 1〕에서 보듯이 관리를 용이하게 하고, 빠른 핸드오버를 보장하기 위해서 eNodeB 간 링크를 허용하였다. 따라서 액세스망에서의 eNodeB 접근성이 높아졌으며, 이는 보안위협으로의 발전가능성을 내포하고 있다. 이에 3GPP는

$$K_{eNB}^{*} = KDF(K_{eNB}, PCI, EARFCN-DL) \quad (1)$$

$$K_{eNB}^{*} = KDF(NH_{NCC}, PCI, EARFCN-DL),\ NH_{NCC} = KDF(K_{ASME}, NH_{NCC-1}) \quad (2)$$



〔그림 2〕 EPS 키 갱신 및 키 전달

EPS 인증 및 키 동의 (EPS Authentication and Key Agreement: EPS-AKA)과정을 정의하고 있다. EPS-AKA는 인증서버 (Home Subscriber Server :HSS) 로부터 인증정보를 받아 Mobile Management Entity (MME)와 사용자 (User Equipment: UE) 간의 인증 절차를 진행한다. EPS-AKA를 통해서 사용자와 MME 간에는 비밀키 K_{ASME}를 공유하고, 비밀키는 Non-Access Stratum (NAS) 구간 암호화 및 무결성을 위해 사용 된다. Access Stratum (AS) 레벨 (사용자와 eNodeB 간)을 보호하기 위한 세션키는 K_{eNB}로 정의되고, K_{eNB}는 사용자의 핸드오버에 따라 eNodeB를 변경할 때마다 갱신된다. NAS 구간은 사용자와 MME 구간을 통하는 시그널링 트래픽만을 보호하며, Serving Gateway (S-GW)와 Packet data network Gateway (P-GW)를 통하는 데이터 트래픽은 오직 AS 구간에서만 보호된다.

3.2 EPS 핸드오버 키 관리

MME가 K_{eNB}를 직접 갱신하는 방법은 네트워크 지연을 발생시킬 수 있기 때문에, EPS는 eNodeB 간 직접적인 키 갱신을 지원하고 있다. 1장에서 기술하였듯이 eNodeB는 공격자에 의해 노출될 위험이 크기 때문에, eNodeB 간에 키 갱신을 할 때 후방향 및 전방향 안정성 (backward/forward secrecy)을 보장해야 한다.

〔그림 2〕는 핸드오버 시 eNodeB에서의 키 갱신 및 키 전달을 도식화 한 그림이다. 이전 eNodeB (source eNodeB)는 새로운 키인 K_{eNB}^{*}를 계산하여, 동기계수인 NCC (Next-hop Chaining Counter)와 함께 사용자가 핸드오버 할 목표 eNodeB (target eNodeB)로 전달한다. 이 때 새로운 키인 K_{eNB}^{*}는 식 (1) 또는 식 (2)를 통해 계산된다. PCI와 EARFCN-DL은 각각 셀 레벨 식별자와 하향 주파수를 의미한다. 식 (1)은 수평 핸드오버 키 유도 (horizontal handover key derivation), 식 (2)는 수직 핸드오버 키 유도 (vertical handover key derivation) 과정이라 명명한다. Key Derivation Function (KDF)는 일방향 해쉬 함수를 의미한다.

수평 핸드오버 키 유도 과정에서는 이전 eNodeB가 사용하였던 K_{eNB}에서 직접 유도하기 때문에, 전방향 안전성이 보장되지 않는다. 한편, 수직 핸드오버 키 유도 과정에서 K_{eNB}^{*}는 NCC번째 Next Hop (NH) 키인 NH_{NCC}키에서 유도되는데, NH 키는 이전 핸드오버에서 MME로부터 수신한 값이다. NH는 동기계수인 NCC로 색인하고, 핸드오버가 발생될 때마다 업데이트 된다. 〔그림 2〕의 메시지 (2)를 받은 목표 eNodeB는 자신과 사용자 간의 세션키를 K_{eNB}^{*}로 설정하고 이에 기반해 보안 통신을 시작한다. 〔그

림 2]의 메시지 (3)에서 보듯이, 목표 eNodeB는 NCC 값을 사용자에게 전달하고, 사용자는 NCC 값을 통해 핸드오버의 종류를 파악하여 (사용자가 보유하던 NCC값과 같거나 작으면 수평, 보유하던 NCC 값보다 크면 수직 핸드오버 키 유도과정이라 판단), 수직 또는 수평 핸드오버 키 유도 과정을 진행한다. [그림 2]에서 메시지 (4)를 통해 핸드오버가 종료되고, 목표 eNodeB는 MME에게 핸드오버 종료를 메시지 (5)를 통해 보고한다. 이 때 MME는 다음 핸드오버를 위하여 NCC값을 1 증가시키고, NCC+1 값과, NH_{NCC+1}키를 목표 eNodeB에게 전달한다.

IV. EPS 핸드오버 키 관리 기법의 취약점 분석

4.1 비동기화 공격 (De-synchronization attack)

본 논문에서는 비동기화 공격을 시도하기 위해, 공격자는 위장 eNodeB을 소유한다고 가정한다. 또는 보안취약점을 이용하여 eNodeB를 손상시킬 수 있다고 가정한다. 공격 eNodeB는 이전 eNodeB를 위장하여 [그림 2] 메시지 (2)의 NCC 값을 기존 NCC 값보다 큰 값으로 변조하여 목표 eNodeB에게 전송한다. 또는, eNodeB 간 통신이 IP 패킷에 기반 하기 때문에, 공격자가 위장 eNodeB를 소유하지 않고서도 메시지를 변조할 수 있다. 현재 정상 NCC 값을 α라 하고, 조작된 NCC 값을 β라 정의하자 ($\alpha \ll \beta$). 목표 eNodeB는 변조된 NCC 값을 탐지하지 못 하고 핸드오버를 진행하고, 핸드오버의 결과로 메시지 (6)을 통해 MME로부터 $\alpha+1$을 전달받게 된다. 따라서 다음 핸드오버 시에 eNodeB는 최신 NCC값을 유지하고 있지 않다고 판단되기 때문에 ($\alpha+1 \ll \beta$), 수평 핸드오버 키 유도 과정을 진행하게 된다. 이 경우 전방향 안전성을 보장하지 못 하기 때문에, 공격자는 사용자가 핸드오버를 한 이후에도 지속적으로 사용자와 정상적인 eNodeB들간 통신 키 K_{eNB}^*를 획득하게 된다.

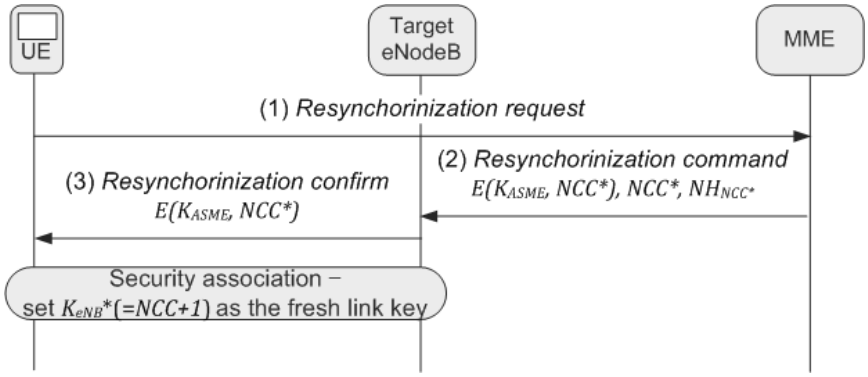
또한 공격자는 [그림 2]의 메시지 (6)의 NCC값을 변조하여 비동기화 공격을 유발할 수 있으나, MME와 eNodeB 간 통신은 IPSec에 의해 보호될 확률이 높다. 하지만 메시지 (6)에 대한 서비스거부공격을 통해 수평 핸드오버 키 유도 과정을 조장할 수 있다. 서비스거부공격으로는 메시지 (6) 손실, 또는 리소스 잠식 등이 있다.

4.2 재전송 공격 (Replay attack)

만약 eNodeB 간 통신링크가 IPSec에 의해 보호된다면, eNodeB 간 전달되는 NCC 값을 변조하기 어렵기 때문에 비동기화 공격을 수행하기 어렵다. 하지만 EPS 키 전달 과정은 재전송 공격에 취약하다. 재전송 공격은 세션키 탈취가 목적이 아닌, 단순 보안통신 링크 생성 방해의 목적을 가지고 사용자와 eNodeB 간 핸드오버 과정을 조작한다. 공격자는 사용자와 정상 eNodeB 간 핸드오버 메시지를 도청하여, [그림 2]의 메시지 (3)을 획득 한다 (메시지(3)은 암호화 되어 있음). 그 후 사용자가 핸드오버를 할 때마다, 정상적인 메시지 (3) 대신에, 획득한 메시지 (3)을 전송한다. 사용자는 메시지 (3)에 있는 NCC 값과 자신이 현재 소유한 NCC 값을 비교하는데, 이 때 재전송 공격을 위해 패킷을 수집한 시간이 과거이기 때문에 사용자가 현재 소유한 NCC 값이 재전송 공격 당시 수집된 메시지 (3)의 NCC 값보다 항상 크거나 같게 된다. 따라서 사용자는 수평 키 핸드오버 유도기법에 기반하여 K_{eNB}^*를 유도하게 된다. 하지만 정상적인 eNodeB는 NCC 값을 새롭게 업데이트 하였으므로 수직 키 핸드오버 유도 기법에 기반하여 K_{eNB}^*를 계산하게 된다. 따라서 메시지 (4)를 통한 보안통신 링크가 성립되지 않게 된다. 하지만 현재 표준에서는 이러한 공격기법에 대한 대책이 없어, 핸드오버 키 과정을 초기화하여 메시지 (1)부터 다시 시작하게 된다.

V. 제안기법

핸드오버 이전에 MME로부터 후방향 안전성을 보장받기 위한 값을 전달받거나, 목표 eNodeB와 사용자 간에 키교환 기법을 통해 비동기화 공격을 방지할 수 있다. 하지만 표준에서는 핸드오버 지연을 이유로, 이러한 기법을 지양하고 있다. 보다 근본적인 해결방법은 핸드오버가 일어날 때마다 EPS-AKA를 통해서 K_{ASME}와 K_{eNB}를 갱신하는 방법이 있을 수 있겠으나, 이는 플랫 All-IP 구조에서 eNodeB 간 링크를 활용하여 통신 지연을 최소화하고자 하는 LTE의 기본 원칙[3]에 위배된다. 따라서 본 논문에서는 불필요한 지연을 최소화하고자 [그림 3]과 같은 재동기화 과정을 제안한다. 제안하는 스킴에서는 비동기화 또는 재전송 공격이 발생했음을 감지했을 때에 한정되어, 재동기화 과정을 통해 핸드오버 키를 다시 설정할 수 있다.



〔그림 3〕 제안하는 스킴의 재동기화(resynchronization) 과정

먼저, 수평 혹은 수직 키 핸드오버 키 유도 과정에서 K_{eNB}^* 생성 시 현재 세션키 동기계수인 NCC를 포함하는 기법을 제안한다. 사용자가 NCC를 수신하였을 때 (〔그림 2〕의 메시지 (3)) NCC의 비동기화를 감지할 수 있다. 재전송 감지 후 〔그림 3〕에서 보듯이 사용자는 재동기화 요청 메시지를 MME에게 전송한다. MME는 사용자의 NCC값을 확인하고, NCC값을 갱신한 NCC*(=NCC+1)을 eNodeB를 통해 전달한다. 이 때 사용자에게 전달할 NCC* 값은 K_{ASME}를 통해 대칭키 암호화되고, eNodeB에게 전달하는 NCC*, NH_{NCC}*값은 평문으로 전송한다 (단, MME와 목표 eNodeB간 링크는 IPsec에 의해 보호된다고 가정). 사용자와 eNodeB는 새로운 NCC*값을 설정하고, 이에 기반한 수직 핸드오버 키 유도 과정을 진행하여 새로운 세션키 K_{eNB}^*를 생성한다.

5.1 보안분석

본 장에서는 제안한 K_{eNB}^* 생성 시 NCC 값 포함 및 재동기화 과정을 통해 비동기화 공격 및 재전송 공격을 막을 수 있음을 보인다. 비동기화 공격으로 인해 목표 eNodeB는 현재의 K_{eNB}의 NCC값을 β로 착각하게 된다. 따라서 다음 핸드오버를 위한 K_{eNB}^* 생성 시, 수평 키 핸드오버 과정을 진행하지만 본 논문에서 제안한 기법에 따라 KeNB*는 NCC(=β)값을 포함하여 생성하게 된다. 하지만 사용자의 NCC 값은 α로 유지되므로, 동일하게 수평 키 핸드오버 과정을 진행하지만, 서로 세션키가 다르게 된다. 따라서 이 때 사용자는 비동기화 공격을 감지하고, 〔그림 3〕에서 제안한 재동기화 과정을 유도한다.

5.2 성능분석

핸드오버 과정에서는 K_{eNB}^*시 NCC값만을 추가하였기 때문에, 공격이 일어나지 않았을 때의 연산 및 통신오버헤드는 기존의 EPS 키 핸드오버 관리 기법과 차이가 없다. 따라서 재동기화 과정의 연산오버헤드 〔표 1〕 및 통신오버헤드 〔표 2〕만을 측정하였다. MME와, 사용자가 각각 새로운 NCC*를 암호화하고, 복호화하는 데 각각 대칭키 암호화방식 (AES 가정) 1회가 소모된다. 또한 사용자와 eNodeB는 재동기화된 NCC*에 기반하여, 새로운 세션키 K_{eNB}^*를 생성하는데 일방향 해쉬함수를 각 1회씩 소모한다. 따라서 핸드오버 지연은 2H+2E로 결정된다. 본 논문에서는 PolarSSL〔8〕을 통해 펜티엄 IV 3.0GHz (2GB 램)에서 테스트하여 SHA-256 (H) 및 AES-128 (E)의 연산지연을 각각 0.0061ms, 0.0058ms로 측정하였다. 따라서 총 비동기화 공격 및 재전송 공격이 발생했을 때의 핸드오버 지연은 0.0238ms이다. 추가적인 통신오버헤드는 K_{ASME}이 256bits, NCC, NH가 128bits로 계산했을 때 총

〔표 1〕 연산 오버헤드

		AES 암복호화 (E)	일방향 해쉬함수 (H)
EPS-AKA 제안기법(공격 미발생)	단말	0	1
	eNodeB	0	1
	MME	0	1
합계		0	3
제안기법 (재동기화 과정)	단말	1	1
	eNodeB	0	1
	MME	1	0
합계		2	2

〔표 2〕 통신 오버헤드

		통신오버헤드 (송신 bits)
EPS-AKA 제안기법 (공격 미발생)	단말과 eNodeB 간 링크	128
	eNodeB 간 링크	384
	eNodeB와 MME 간 링크	256
합계		768
제안기법 (재동기화 과정)	단말과 eNodeB 간 링크	384
	eNodeB와 MME 간 링크	640
합계		1024

1024bits를 소모하게 된다. 하지만 이러한 통신오버헤드는 비동기화 공격이 일어났을 때의 사용자 데이터 손실 bits에 비해 극히 적은 오버헤드이다. 또한 재전송 공격이 지속적으로 발생했을 때는, 핸드오버 지연이 무한대 발산하므로 이러한 오버헤드는 감내할만하다고 할 수 있다.

VI. 결 론

본 논문에서는 3GPP EPS 상에서의 핸드오버 키 관리에 관한 취약점을 발견하고, 공격 파급효과를 분석하였다. 비동기화 및 재전송 공격을 막기 위해, 재동기화 과정을 통한 핸드오버 개선책을 제안하였다. 제안하는 기법은 기존 EPS 핸드오버 키 관리 기법에 존재했던 취약점을 가지고 있지 않으며, 공격 발생 시 가벼운 연산을 통해 재동기를 수행할 수 있도록 설계되었다.

참고문헌

〔1〕 M. Zhang, et al., "Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol," IEEE Trans. Wireless Commun., vol. 4, no. 2, pp.734-742 , Mar. 2005

〔2〕 3GPP, "Rationale and Track of Security Decisions in Long Term Evolution (LTE) RAN / 3GPP System Architecture Evolution (SAE) (Release 9)," TS 33.821, Jun. 2009.

〔3〕 3GPP, "3GPP System Architecture Evolution (SAE); Security Architecture (Release 9)," TS 33.401, Dec. 2009.

〔4〕 C. Michell, "The Security of the GSM Air Interface Protocol," Univ. of London, Royal Holloway, Technical Report, RHUL-MA-2001-3, Aug. 2001.

〔5〕 C.B. Sankaran, "Network Access Security in Next-Generation 3GPP Systems: A Tutorial," IEEE Commun. Mag., vol. 47, no. 2, pp. 84-91 , Feb. 2009.

〔6〕 D. Forsberg, "LTE Key Management Analysis with Session Keys Context," ELSEVIER Comput. Commun., vol. 33, no. 16, pp.1907-1915, Oct. 2010.

〔7〕 Y. Park, et al., "A Survey of Security Threats on 4G Networks," IEEE GLOBECOM Workshop on Security and Privacy in 4G Networks, pp. 1-6, Nov. 2007.

〔8〕 PolarSSL: Open Source embedded SSL/TLS cryptographic library, http://polarssl.org/

〈著者紹介〉

한 찬 규 (Chan-Kyu Han) 학생회원
2006년 8월: 성균관대학교 컴퓨터공학전공 학사졸업
2008년 2월: 성균관대학교 전자전기컴퓨터공학과 석사졸업
2008년 3월~현재: 성균관대학교 휴대폰학과 박사과정
〈관심분야〉 네트워크 보안

최 형 기 (Hyoung-Kee Choi) 정회원
1992년 2월: 성균관대학교 전자공학과 학사졸업
1996년 2월: Polytechnic University 전자전기 석사졸업
2001년 2월: Georgia institute of Technology 전기전자 박사졸업
2004년 3월~현재: 성균관대학교 정보통신공학부
현재 성균관대학교 정보통신공학부 부교수
〈관심분야〉 네트워크 보안, 트래픽 모델링