Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.1, Feb. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.1.75

개선된 위임 서명 방식을 이용해서 더 안전한 펨토셀 환경 구축

최 형 기,[1†] 한 찬 규,[2‡] 김 승 룡[1]
[1]성균관대학교, [2]삼성전자

Building More Secure Femtocell with Improved Proxy Signature

Hyoung-Kee Choi,[1†] Chan-Kyu Han,[2‡] Seung-Ryong Kim[1]
[1]Sungkyunkwan University, [2]Samsung Electronics

요 약

공공 장소에서 끊김없이 통신할 수 있도록 하기 위하여 펨토셀에 대한 요구가 엄청나게 증가하고 있다. 3GPP(3rd Generation Partnership Project)에서 새로 발표한 "Release 9"에서 Home eNode B는 HeNB(Home evolved Node B)로 언급된 펨토셀을 처리하기 위한 새로운 구조와 보안 요구사항을 정의했다. 따라서 본 논문에서는 HeNB의 보안에 대한 상호 인증, 접근 제어 및 안전한 키 동의 과정을 분석한다. 본 논문의 분석을 통하여 3GPP 기술 규격에 의해 정의된 보안 취약점 중에서 언급되지 않았거나 아직도 해결되지 않고 있는 보안 취약점들에 대해 설명한다. 이러한 보안 취약점으로는 도청, 중간자 공격, 가입자 접근 목록 손상, 그리고 유효한 HeNB로의 위장 등이 있다. 이 논문의 후반부에서는 HeNB에 대해 위임 서명된 위임 서명을 적용한 개선된 인증과 키 동의 메커니즘을 제안한다. 분석 결과 제안된 방법은 다양한 보안에 대한 위협을 막을 뿐만 아니라 사용자가 허용할 수 있는 범위의 최소 인증 지연 시간을 갖음을 알 수 있었다.

ABSTRACT

Demand for the femtocell is largely credited to the surge in a more always best connected communication conscious public. 3GPP defines new architecture and security requirement for Release 9 to deal with femtocell, Home eNode B referred as HeNB. In this paper, we analyze the HeNB security with respect to mutual authentication, access control, and secure key agreement. Our analysis pointed out that a number of security vulnerabilities have still not been addressed and solved by 3GPP technical specification. These include eavesdropping, man-in-the-middle attack, compromising subscriber access list, and masquerading as valid HeNB. To the best of our knowledge, any related research studying HeNB security was not published before. Towards this end, this paper proposes an improved authentication and key agreement mechanism for HeNB which adopts proxy-signature and proxy-signed proxy-signature. Through our elaborate analysis, we conclude that the proposed not only prevents the various security threats but also accomplishes minimum distance from use-tolerable authentication delay.

Keywords: long term evolution(LTE), home eNode B(HeNB), femtocell, mobile network security

접수일(2013년 6월 26일), 수정일(2013년 9월 24일), 게재확정일(2014년 1월 7일)

† 주저자, meosery@skku.edu
‡ 교신저자, ksryong0@nate.com (Corresponding author)

I. 서 론

펨토셀(femtocell)은 작은 셀룰러 통신을 할 수 있는 점 접근 기지국으로 알려져 있다. 일반적으로 가정용 펨토셀은 소규모 비즈니스 환경에 사용하기 위해 설계되었다. 최근에 4세대 네트워크에서 “always best connected”에 대한 수요가 증가하고 이에 대응함으로써 더 유명해지게 되었다. 3GPP는 HeNB를 펨토셀 [1][2][3]에서 구성된 아키텍처를 참고하여 정의한다. 2008년이 끝날 무렵에 3GPP 공식 표준화의 완성으로 통신망(예를 들면 GSM: Global System for Mobile communications, UMTS: Universal Mobile Telecommunication System, LTE: Long Term Evolution)들은 새로운 구조의 3GPP 펨토셀을 지원하기 위해 이동할 것이다.

펨토셀 HeNB는 다양한 실내 환경(예를 들면 가정집, 학교, 그리고 회사)에서 복잡하지 않게 설치될 것이다. 하지만 그 크기와 무게 때문에, 작은 크기의 HeNB는 엄격히 제한된 지역에만 설치될 것이다. 보통 HeNB의 유효 통신 범위는 가정에서 200미터 안쪽까지이고, HeNB의 특징 중 하나는 인터넷 프로토콜(IP: Internet Protocol)를 활용하여 플랫 기지국 구조와 연결하는 것이다. 또한 HeNB는 안전하지 않을지도 모르는 유선 광대역 연결을 통해 CN(Core Network)에 연결되어 있다. 이러한 연결을 backhaul이라고 한다.

3GPP는 위험, 요구사항 및 HeNB 보안 [1]의 해결책에 해당 되는 것을 명시한다. [1]에서 정의된 대부분의 보안 취약점은 두 가지 요소로부터 유래되었다. 첫 번째는, 사용자 장비와 HeNB 사이의 안전한 상호 인증의 부족과 특히 사용자 단말기가 확실하게 HeNB를 인증하는 능력의 부족. 두 번째는, backhaul으로 인한 HeNB와 core network 사이의 링크 불안전성이다. 전송 중에 데이터의 인터셉트(intercept)와 대화 중 도청하는 것이 쉽게 가능하기 때문에 무선 링크와 backhaul은 다양한 형태의 공격에 취약할 수 있다. 더욱이 본 논문의 분석은 현재 개정안이 여전히 도청, 중간자 공격, 가입자 접근 목록을 손상시키고 그리고 유효한 HeNB인 것처럼 가장하는 것과 같은 많은 위협과 요구사항에 대해 언급되지 않았다는 것을 가리킨다.

본 논문에서는 위임 서명을 적용함으로써 안전한 상호 인증과 접근 제어 메커니즘을 제안한다. HeNB operator와 core network operator는 서로 위임 서명을 발행함으로써 설치, 운영 및 HeNB의 관리에 대한 계약 관계를 가진다. HeNB operator (CN operator)는 그 자신의 위임 서명 기능을 HeNB에게 재위임 한다. 동시에, CN operator는 그 자신의 서명 기능을 사용자 단말기에 위임한다. 따라서, 사용자 단말(UE: User Equipment)은 HeNB의 operator뿐만 아니라 core network operator의 위임 서명된 공개 키를 통해 서명을 검증함으로써 HeNB를 인증한다. 동시에 HeNB는 core network의 공개 키를 통해 HeNB 에서 서명을 검증함으로써 사용자 단말을 인

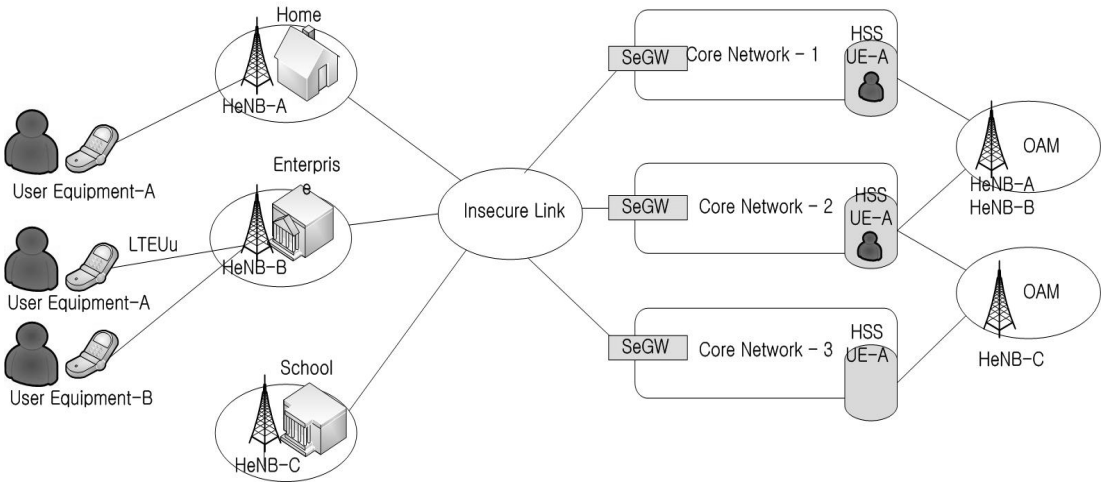

Fig.1. System Architecture of Femtocell

증한다.

이 논문의 주요한 기여는 네 부분으로 나눌 수 있다. (1) UE와 HeNB 사이에 안전한 상호 인증과 키 동의를 제공한다. (2) HeNB에서의 운영 모드에 관계없이 안전한 의사소통을 보장한다. (3) 프로토콜 공격들의 다양한 변종을 막는다(예를 들면 위장, 중간자 공격 및 DOS(Denial Of Service)공격, 등등). (4) 바람직하지 않은 HeNB들의 폐기 방법을 제시한다. 이러한 주제에 대해 본 논문에서는 분석과 실험을 통하여 계산 오버헤드를 조사한다. 그 결과 제안한 인증 메커니즘을 수행하는데 8.044μs가 걸렸다.

이 논문의 나머지 부분은 다음과 같이 구성되었다. 우리는 단원 2에서 HeNB 구조와 보안 요구사항을 명시한다. 단원 3에서는 HeNB의 보안상의 위협과 대책에 대해서 설명한다. 그리고 단원 4에서는 우리는 위임 서명을 사용하여 제안한 인증 메커니즘을 보여준다. 또한, 단원 5와 단원 6에서 제안된 메커니즘에 대한 성능과 보안 분석을 각각 제공한다. 마지막으로, 단원 7에서 추후 연구되어야 할 사항들과 함께 결론이 제시된다.

II. HeNB의 시스템 구조와 보안 요구사항

〔Figure. 1.〕은 HeNB의 시스템 구조와 사용되는 경우를 묘사한 것이다. UE와 HeNB 사이의 Air 인터페이스는 E-UTRAN(Evolved Universal Terrestrial Radio Access Network) 라고 불리는 LTE-Uu를 가지고 역호환 되어야 한다. HeNB와 보안 게이트웨이 (SeGW: Serving GateWay) 사이의 백홀(backhaul)은 안전하지 않을지도 모른다. 또한 SeGW은 HeNB와 상호 인증을 수행하는 operator들의 core network를 나타낸다. HeNB는 환경 설정이 필요하고 그리고 작동, 승인 및 관리시에 OAM(Operation, Administration and Maintenance)에 의해 권한을 부여 받아야 한다. 〔Figure. 1.〕에서 UE-A와 UE-B는 각각 LTE core network 1, 2에 속해 있다. UE-A는 각각 가정집과 회사에서 HeNB-A와 HeNB-B를 통해 그 자신의 core network에 접속한다. UE-B는 회사에서 HeHN-B를 통해 그의 core network에 접속한다. HeNB-A와 HeNB-B 모두 다 HeNB 작동을 관할하는 OAM 아래에 있다. 이러한 환경에서 세 가지 계약적 관계가 성립되어 있어야 하는데, 이는 ① HeNB 소유주(일반적으로 리드 사용자)와 OAM 사이, ② UE와 core network 사이, ③ UE의 core network와 OAM 사이이다.

TS 22.220는 HeNB의 지원을 위한 기본적인 기능에 대한 서비스 요구사항을 정의한다.〔2〕 폐쇄 가입자 그룹(CSG: Closed Subscriber Group)은 LTE의 하나의 셀 또는 여러 셀에 대한 접근이 허용될 수 있지만, CSG cell에 접근이 제한된 operator의 가입자(UEs)를 구분한다. 동일한 CSG identity를 공유하고 있는 CSG cell은 CSG 멤버에 의해 접근이 가능할 것이다. 따라서 접근이 가능하다면 UE는 가입자가 속한 CSG의 모든 CSG identity를 포함하는 USIM(Universal Subscriber Identity Module)안에 있는, white list를 유지 한다. 그러므로 다음 다섯 가지의 보안 특성이 만족되어야 한다.〔1〕

① HeNB 접근 보안(HeNB access security)은 HeNB와 SeGW 사이에 상호 인증과 보안 터널 설립을 포함한다. HeNB를 설치하거나, 공급하거나 환경 설정할 때 core network operator는 HeNB identity를 검증할 수 있게 하고 HeNB의 지리적 정보를 얻는다. 인증과 키 동의는 EAP-AKA(Extensible Authentication Protocol-Authentication and Key Agreement) 기반과 인증서 기반 방식으로 구축되게 된다.

② 네트워크 도메인 보안(network domain security)은 IPSec(Internet Protocol Security protocol)에 의해 보장된 SeGW와 core network 사이의 보안 통신을 포함한다.

③ HeNB 서비스 도메인 보안(HeNB service domain security)은 소프트웨어 및 구성 업데이트에 대해 core network에 위치한 OAM과 HeNB 사이의 보안 통신을 포함한다. HeNB는 네트워크 오퍼레이터가 원격의 HeNB의 환경을 설정하는 것을 허용하는 OAM 과정과, 소프트웨어 업그레이드와 일반적인 OAM 업무를 수행하는 것을 지원해야 한다.

④ UE 접근 제어 도메인 보안(UE access control domain security)은 오직 legacy UE에만 적용한다. Rel-8에 따르면 UE에 대한 접근 제어는 CSG 목록이 허락하는 것에 기반을 둔다. CSG는 PLMN(Public Land Mobile Network)의 하나 또는 여러 셀에 접근하는 것이 허용

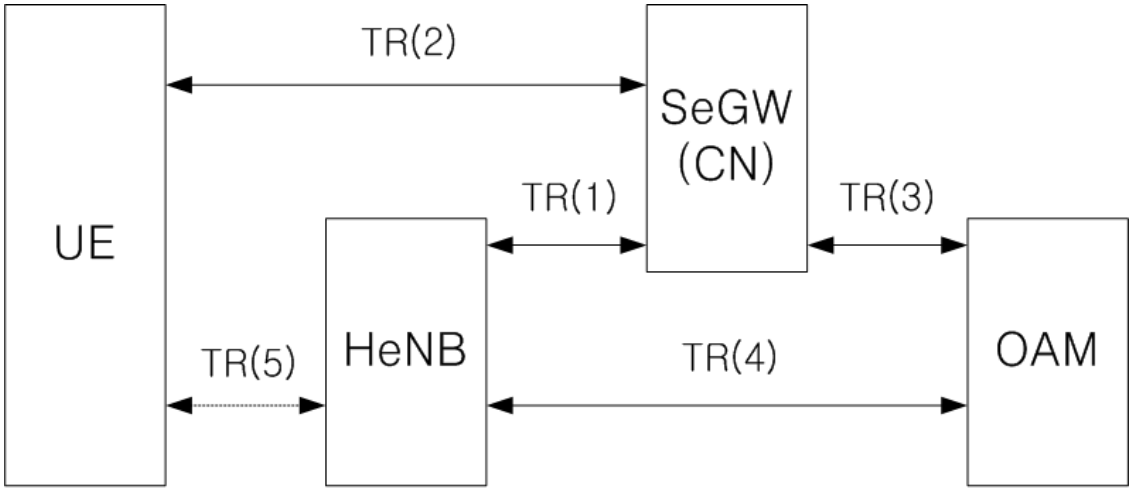

Fig.2. The TR(Trust Relations) in HeNB Security Architecture

되지만 CSG 셀들에 접근이 제한되는 operator의 UE를 구분한다.

⑤ UE 접근 보안(UE access security)은 UE에게 모바일 통신 시스템에 대한 안전한 접근을 제공한다. 이러한 특성은 모바일 통신 시스템의 명세서에 정의된 보안 특성과 같다.[4]

III. HeNB의 보안 분석

이 단원에서는 HeNB에서 발생할 수 있는 위협과 대응 대책에 대해서 논의할 것이다. 다음 목록은 HeNB에서 발생할 수 있는 보안 취약점과 그로 인해 발생할 수 있는 일들에 대해 요약하였다. 각 위협의 세부적인 내용은 다른 자산들에 대한 각각의 위협에 대한 영향과 그들이 속해 있는 위험 수준에 대해 [1]에서 주어졌다. 우리는 네트워크 보안 범위에서의 위협은 제외한다. (예를 들면. 물리적 공격, 무선 자원과 관리에 대한 공격)

① HeNB 인증 토큰의 손상 (compromise of HeNB authentication token): 공격자는 HeNB의 유선으로부터 인증 증명서를 읽고 그것을 복사한다. 복제된 토큰은 HeNB를 UE로 위장하는데 사용될 수 있고 이는 UE에 대한 추가적인 공격을 낳는다.

② 사용자 HeNB 인증 토큰 클로닝 (user cloning the HeNB authentication token): 공격자는 정당한 HeNB의 인증 자격을 복제하고 다른 HeNB에 그 인증서를 설치한다. 이러한 공격은 공격자들이 도청하거나 다른 UE로 도용할 수 있으므로 위협①보다 더 심각한 영향을 끼친다.

③ 가짜 소프트웨어 업데이트/ 구성 변경 (fraud software update/configuration change): HeNB는 명백한 core network에서의 OAM으로부터 소프트웨어 업데이트를 수락해야 한다. 만약 소프트웨어 유통 센터(OAM)가 위험에 노출 되면 대다수의 HeNB가 악의적인 소프트웨어를 받아 설치할 수도 있다.

④ 잘못된 설정과 ACL(Access Control List)의 위험노출 (mis-configuration and compromise of ACL): 공격자가 CSG 목록을 수정함으로써 UE는 네트워크에 접근할 수 없게 된다. 또한 공격자들은 접근해야하는 UE들을 제거할 수도 있다.

⑤ HeNB 첫 번째 네트워크 접근 상의 중간자 공격(man-in-the-middle attack on HeNB first network access): 인터넷 상에서 공격자는

HeNB로부터의 모든 트래픽을 가로챌 수 있고 모든 사적인 정보에 대해 접근할 수 있다. 이와 같은 공격은 HeNB와 core network 사이에 통과하는 모든 데이터를 도청할 수 있다. 또한, 당사자를 대신하여 데이터를 전송할 수 있다.

⑥ OAM과 OAM상의 트래픽에 대한 공격 (attack on OAM and its traffic): 침입자가 OAM과 HeNB 사이의 통신 링크에 대한 접근을 가질 수 있을 때, 트래픽 도청, 중간자 공격, HeNB의 잘못된 구성, 가짜 소프트웨어 업데이트와 같은 다른 공격들을 수행할 수 있다.

⑦ HeNB 네트워크 접근의 위협 (threat of HeNB network access): 만약 HeNB SeGW에 있는 HeNB에 HeNB에 대한 접근 권리를 확인하기 위한 서비스 도메인의 접근 제어 정보 같은 것이 없다면, 불법 HeNB는 네트워크 접근을 얻을 수 있다. 공격자는 엿듣거나 HeNB에 있는 다른 UE로 도용할 수 있다.

⑧ 기록 없이 HeNB 위치 변경 (changing of the HeNB location without reporting): HeNB 소유주는 HeNB를 재배치하고 부당한 위치 정보를 제공할 수도 있다.

⑨ 다른 사용자의 E-UTRAN 사용자 데이터 도청(eavesdropping of the other user's E-UTRAN user data): 공격자는 HeNB를 소유하고, 그것을 설치하고, 그리고 개방 접근 모드로 환경 설정한다. 데이터는 보호되지 않은 air 인터페이스이거나 IP 인터페이스 보안을 가지지 않았다면 쉽게 읽을 수 있다. 따라서 피해자는 이러한 HeNB에 대한 지식 없이 일반적인 air 인터페이스를 사용하여 머물게 된다.

⑩ 다른 사용자로 위장 (masquerade as other users): ⑨위협과의 차이점은 ⑨위협의 공격자는 수동적인 공격자들 같이 오직 듣기만 하지만, 반면에 위협⑩의 공격자들은 또한 위조한 트래픽을 넣어 추가적인 공격을 할 수 있다.

Table 1. Security Threats and its Countermeasure

Threat group	Number	Security threats	Countermeasure
Compromise HeNB credentials	1	Compromise HeNB authentication token	Authentication credentials of the H(e)NB shall be stored inside TPM(trusted platform module) or a UICC
	2	User cloning the HeNB authentication token	The users could be required to obviously confirm their acceptance before being joined to HeNB
Configuration attacks on HeNB	3	Fraud software update/Configuration changes	All software and configuration changes shall be cryptographically signed by OAM
	4	Mis-configuration and compromise of CSG	Security means is required for generation, maintenance, and store of CSG
Protocol attacks on HeNB	5	MitM attacks on HeNB first network access	Credentials of HeNB should be recognized on the core network operator's side
	6	Attack on OAM and its traffic	Communication between HeNB and OAM should be secured
	7	Threat on HeNB network access	SeGW in core network should have the related profile information of HeNB to check whether a HeNB can access the network
	8	HeNB location change without reporting	Location locking mechanism should be designed and implemented
User data and identity privacy attack	9	Other user's eavesdrop E-UTRAN user data	When the UE camps on a closed or open type HeNB, the user should be notified
	10	Masquerading as other users	Same as number 9
	11	Masquerading as a valid HeNB	CSG configuration and setting should be hidden

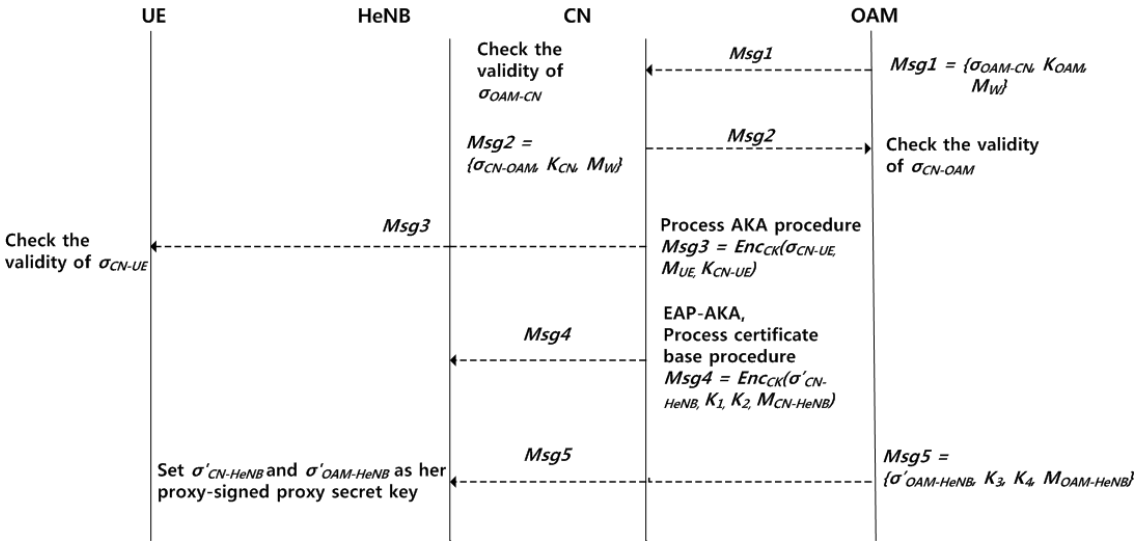

Fig.3. Registration Phase

⑪ 유효한 HeNB로 위장 (masquerade as a valid HeNB): 공격자는 HeNB를 사서 정당한 UE를 유혹하기 위하여 목표 HeNB의 CSG와 비슷하게 환경설정을 한다. 관련 정보를 가지게 되면 공격자들은 HeNB에서 암호화를 하지 않거나 무결성 수준을 변경할 수 있고 또는 HeNB에서 사용자 키로 접근할 수 있다.

〔Table 1〕은 보안 위협과 대책이 나열된 행렬(Matrix)을 보여준다. 〔1〕에 따르면 이전의 위협, 보안 요구사항이 포함하는 것을 완화하기 위해서는 (1)SeGW와 HeNB 사이에 상호인증과 보안 터널 설립, (2)신뢰성 있는 환경, (3)접근 제어 메커니즘, (4)위치 잠금 메커니즘, (5)OAM에 대한 보안 메커니즘, (6)사용자 인증 메커니즘 등이 만족되어야 한다.

〔Figure. 2.〕는 HeNB 보안 구조에서 신뢰 관계에 대해서 묘사한다. 굵은 화살표는 표면적인(물리적인) 상호 신뢰 관계를 표시한다. 반면, 점선은 내부적인 신뢰 관계를 표시하는데 이것은 통신 경로에 대해 보안 규칙을 만들기 위하여 생성되어야 한다. 많은 사람들은 core network와 OAM이 독립적으로 인증한다면, HeNB가 충분히 신뢰할 수 있다고 믿는다. 그러나 이러한 믿음은 완전히 틀렸다.

본 논문에서는 〔1〕에서 언급 되었던 보안 요구사항이 보안 위협을 완전하게 막을 수 없다는 것을 발견했다. UE와 HeNB 사이의 안전한 상호 인증 없이는 중간자 공격, 유효한 HeNB로 위장 및 OAM에서 core network와 UE 전부 위장한 상황에서 발생된 공격 등 다양한 프로토콜 공격을 막을 수 없었다. 그러므로 core network와 OAM은 HeNB가 IP 기반 네트워크에서 유효하지 않기 때문에 서로 협력적으로 HeNB를 인증해야 한다.

요약하면, UE는 그것이 HeNB에 탑재되었을 때, UE의 core network와 유효한 OAM에 의해 HeNB가 검증되었다는 어떠한 실마리도 가지지 않는다. 한편, 공격자에 의해 위험에 노출될 수 있고 위조될 수 있는 CSG는 HeNB에 대해 UE를 인증하기에 불충분하다.

IV. 제안된 방법

본 논문에서는 (1)UE와 core network 사이, (2)HeNB와 OAM 사이, 마지막으로 (3)UE와 HeNB 사이에 강한 상호 인증과 키 동의 프로토콜을 제시한다. 〔Figure. 1.〕에서 보는 것과 같이 시스템 구조 내에서 다양한 core network와 OAM이 그물망처럼 연결되어 있다. core network는 제한된 수의 OAM과 계약적 관계를 가진다. 이러한 상황에서 UE는 UE의 core network operator를 가지는 OAM과 계약된 것 중 하나에 속하는 HeNB와 연결되었는지 아닌지 확인해야 한다. UE-A는 그의 core network(CN-1)을 통해 HeNB-C와 연결할 수 없다. 왜냐하면 CN-1은 HeNB-C OAM과 서로 계약되어 있지 않기 때문이

다. 반면에 UE-B의 경우에는 HeNB-C와 연결되어 있으므로 가능하다. OAM은 상응하는 core network에 있는 HeNB를 인증하기 위해 UE를 확인해야 한다. 위임 서명 방법은 각 객체 사이에 검증하는 것과 위임하는 것에 대한 효과적인 방법을 제공한다. 본 논문에서 OAM은 HeNB에게 core network를 대신하여 위임 서명을 발급한다. 또한 코어네트워크는 HeNB에게 OAM을 대신하여 위임 서명을 발급한다. 그리고 자신의 서명을 UE에 발급한다. 그렇게 되면 UE (또는 HeNB)는 core network와 OAM을 대신하여 위임 서명을 가지고 HeNB(또는 UE)와 신뢰 관계를 형성한다.

4.1 위임 서명

Mambo, Usuda 및 Okamoto에 의해 소개된 위임 서명 방법 [5]에서 원래의 서명자가 그의 서명하는 권한을 다른 서명자에게 위임하는 것을 위임 서명이라고 한다. 그러면 검증하는 사람은 처음의 서명자 공개 값을 사용하여 서명을 검증할 것이다. 이런 방법은 실제 상황에서 사람들이 다른 사람에게 자신의 도장을 위임하는 것과 비슷하다. 일단 q|(p-1) 같은 두 개의 큰 소수 p와 q를, 위수 q로 $g \in Z_p^*$를 생성한다. 그리고 일방향 해쉬 함수 h(•) 가 공개적으로 사용된다. 처음 서명자는 그의 개인 키 $s \in Z_p$를 가지고 있고 공개 키 v 는 $v = g^s mod\ p$으로 만들어 낸다. 위임 서명 방법은 세 가지 단계로 구성된다.

(생성) 원래 서명자는 랜덤한 수 k를 선택한다. $k = Z_p$, 그러면 $K = g^k\ mod\ p$를 계산하게 한다. 나중에 이 k 값으로 위임 서명 $\sigma = s + kK\ mod\ p$를 계산해야 한다.

(전달) 원래의 서명자는 (σ, K)쌍을 위임 서명자에게 안전한 방법으로 전해준다.

(검증) 위임 서명자는 다음과 같은 식을 사용해서 일치하는지 확인한다. $g^{\sigma} \equiv vK^K\ mod\ p$. 만약 (σ, K)쌍이 이것을 통과하면 그는 원래의 서명자에 의해 확인된 유효한 위임 서명으로 받아들인다.

위임 서명자가 원래의 서명자를 대신하여 문서에 서명할 때, 그는 그의 비밀 키의 대안으로 σ를 사용한다. 그리고 이산 대수 문제(DLP: Discrete Logarithm Problem)를 기반으로 일반적인 서명 작업을 수행한다. 위임 서명의 검증은 원래의 서명 방법과 동일한 검사 일치 작업에 의해 수행 된다. 다만 새로운 공개 값 $v'(\equiv vK^K\ mod\ p)$의 계산이 유일한 예외이다.

이러한 위임 서명의 기초적인 개념에 더해져서 다음의 요구사항이 HeNB 보안에 위임 서명을 적용하는 것에 대해 만족된다: (1)해당하는 객체의 식별코드에 보증서는 그의 유효기간을 서술하고, 그들의 관계가 고려되어야 한다. (2)원래의 서명자는 위임 서명자의 권리를 침해하지 않아야 한다. 그리고 (3)서명자는 그의 서명을 일의 우선순위에 따라 위임할 것이다. 실제 상황에서도 어떤 사람이 도장을 한 개만 소유할 수 있지만, 여러 개의 다른 도장들을 동시에 소유할 수도 있는 것과 같다.

Kim et al.은 "partial delegation with warrant"[6] 이라 불리는 디지털 위임 서명의 새로운 타입을 나타낸다. 다중 위임 서명 방식(multi-proxy signature scheme) [7]에서 원래의 서명자는 다수의 위임 서명자에게 서명 권한을 위임한다. 이와 반대 개념으로, 위임 다중 서명 방식(a proxy multi-signature scheme) [8]에서 위임된 위임 서명자는 원래의 서명자의 그룹을 대신하여 서명을 생성할 수 있다. 우리는 Kim et al.방식이 첫 번째 요구사항과 두 번째 요구사항을 만족시킬 수 있는 방안으로 생각했다. 다중 위임 서명과 위임 다중 서명은 해결책이 될 수 없다. 왜냐하면 전체 그룹 멤버는 두 방식 전부다 참여해야 하기 때문이다. 그러므로 우리는 세 번째를 포함하여 위의 요구사항을 만족하는 새로운 위임 서명 방식을 제안한다.

4.2 등록(Registration)

[Figure. 3.]은 제안된 메커니즘에서 등록 절차의 메시지 흐름을 설명한다. 다섯 가지 메시지는 (msg1에서 msg5까지) 이전 인증 방식에 피기백(piggyback) 될 것이다. (예를 들면 msg4는 [4]에서 정의된 사용자 인증 반응 메시지로 피기백 된다.) 논문에서 사용된 σ_{X-Y} 에서 X 는 그의 서명 권한을 Y로 위임했다는 것을 의미한다. 각각, s_x, v_x($\equiv g^{sx}$ mod p) 그리고 ID_X는 X의 개인키, X의 공개 키 그리고 X의 식별자(identity) 이다. 등록 절차는 다음과 같다.

Msg(Message)1 : 동의하는 과정에서 OAM은 보증서 $M_W(\sigma_{OAM-CN},\ K_{OAM},\ M_W)$을 가지고 대응하

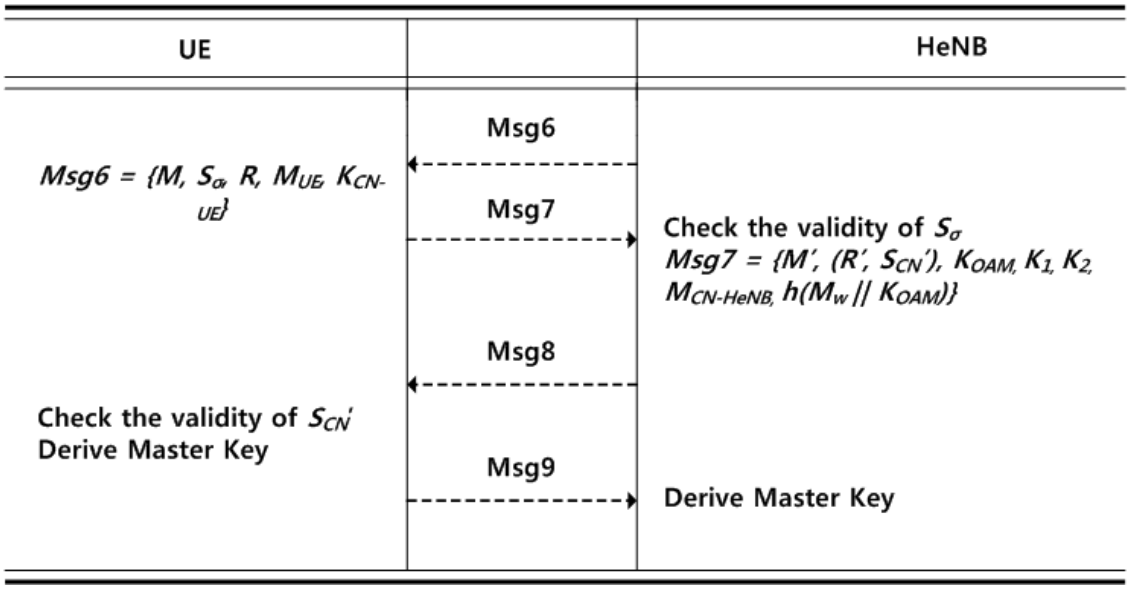

Fig.4. Authentication and Access Control Phase

는 core network에 위임 서명을 발급한다. 보증서를 가지고 하는 위임 서명의 생성은 방정식 (1)에서 보여주는 것처럼 [6]과 비슷하다. M_W은 $(ID_{OAM} \,||\, ID_{CN} \,||\, t_{agreement})$로 구성된다.

$$e = h(M_W \| K_{OAM})$$
$$\sigma_{OAM-CN} = e \cdot s_{OAM} + K_{OAM} \bmod p \quad (1)$$

core network는 Msg1을 받은 후에 방정식(2)를 계산함으로써 그것의 유효성을 검사한다.

$$g^{\sigma_{OAM-CN}} \equiv v_{OAM}^{e} K_{OAM} \bmod p \quad (2)$$

Msg2: core network는 위임 서명 $(\sigma_{CN-OAM}, K_{CN}, M_W)$을 생성하고, 이것을 다시 OAM로 보낸다. 다시 첫 번째 과정과 동일한 검증 방식을 사용하여 OAM은 유효성을 검사한다. 만약 동일하다면 OAM은 σ_{CN-OAM}를 위임 서명으로써 받아들인다.

Msg3: 우리는 UE가 core network에서 모바일 관리 객체를 대신하여 eNB(evolved Node B)를 통하여 [4]에서의 인증과 키 동의 과정을 수행하였다고 가정했다. AKA(Authentication and Key Agreement) 후에, 비밀 키는 UE와 MME(Mobility Management Entity)에 의해 계산될 수 있다. AKA의 마지막 메시지에서 위임 서명 $(\sigma_{CN-UE}, M_{UE}, K_{CN-UE})$은 CK(Cipher Key)를 가지고 암호화되고 UE로 보내진다. M_{UE}는 $(I_{DUE} \,||\, ID_{CN} \,||\, AV_n)$ 으로 구성되고, 여기서 AV_n는 남겨진 인증 벡터의 수이다.

Msg4: 이 단계에서는 core network는 다시 그의 위임 서명 권한(σ_{OAM-CN})을 HeNB에게 위임한다. 첫 번째로 core network는 위임 서명 개인키 (s'_{CN})로 그의 위임 서명 권한(σ_{OAM-CN})을 설정하고 대응하는 공개 키 (v'_{CN})를 계산한다. core network는 랜덤한 수 $k_1, k_2 \in Z_p$를 선택하고 $K_1 = g^{k1} mod\ p$, $K_2 = g^{k2} mod\ p$ 를 계산한다. 그리고 core network는 방정식 (3)을 따라서 그의 일시적인 위임 서명된 위임 능력(proxy-signed proxy capability)을 계산한다. σ'_{X-Y} 는 x가 그의 위임 서명 권한을 누군가로부터 y까지 다시 위임하는 것을 의미한다. 다시 말해, 위임 서명된 위임 서명 (proxy-signed proxy signature) 이다.

$$\sigma'_{CN-HeNB} = k_1 + (\sigma_{OAM-CN} + k_2) \cdot h(M_{CN-HeNB}) \bmod q \quad (3)$$

그러면, core network는 $\sigma'_{CN-HeNB}$, k_1, k_2, $M_{CN-HeNB}$를 EAP-AKA 또는 증명서 기반 장치 인증으로 안전하게 마지막 메시지에 게시한다. $M_{CN-HeNB}$는 CSG cell이나 ID_{CN}가 속하는 대응되

는 HeNB 객체를 의미한다. $M_{CN\text{-}HeNB} = (ID_{HeNB} \,||\, ID_{CSGcell} \,||\, ID_{CN})$

Msg5: OAM은 core network가 Msg4에서 작동한 것과 동일하게 작동한다. OAM은 전송할 때 $\sigma'_{OAM\text{-}HeNB}$, K_3, K_4, $M_{OAM\text{-}HeNB}$를 끼워 넣었다.

$$\sigma'_{OAM-HeNB} = k_3 + (\sigma_{CN-OAM} + k_4) \cdot h(M_{OAM-HeNB}) \bmod q \quad (4)$$

같은 보안 정책을 가졌거나 같은 CSG 객체(white-list)를 가진 HeNB 그룹은 같은 $\sigma'_{OAM\text{-}HeNB}$나 $\sigma'_{CN\text{-}HeNB}$를 가질지도 모른다. OAM이나 CN이 그의 서명 능력을 직접적으로 HeNB에게 위임하는 것은 바람직하지 않다. 왜냐하면 core network는 OAM이 core network와 서로 동의된 보증서를 가지고 일치하면, 그 보증서를 가지고 환경설정되고 작동되었다는 사실을 통지받아야 하기 때문이다. 반대로도 같은 메커니즘을 가진다. 덧붙여 말하자면, HeNB가 실패의 한 점이 되어 공격자들에게 쉽게 노출될 수 있다.

4.3 인증 및 접근 제어 (Authentication and Access Control)

등록 절차 이후, 인증과 접근 제어 절차는 [Figure. 4.]와 같이 동작된다.

Msg6: 이 단계에서 HeNB가 UE의 identity를 향해 요청을 보내 상호 인증 절차가 시작된다.

Msg7: UE는 Msg3$(\sigma_{CN\text{-}UE}, M_{UE}, K_{CN\text{-}UE})$에게서 받은 위임 서명을 사용함으로써 HeNB에 대한 인증을 증명한다. UE는 Msg3$(r = Z_q, R \equiv g^r \bmod p)$을 사인한다. Nuberg Rieppel 서명 방식[9]이 사용된다고 가정한다. 그러면 UE 는 S_σ, R, M_{UE} 그리고 $K_{CN\text{-}UE}$ 와 메시지 $M = (ID_{UE} || ID_{CN} || r_{UE})$를 가지고 HeNB에게 전송한다.

$$S_\sigma \equiv r - R\sigma_{CN-UE} \cdot h(M) \bmod q \quad (5)$$

Msg8: Msg7을 받게 되면 HeNB는 다음과 같은 방정식(6)을 사용하여 검증할 것이다. 여기서 v_{CN}은 core network의 공개 키이다. 만약 방정식(6)이 맞다면 HeNB는 UE를 인증한다.

$$v \equiv v_{CN}^{h(M_{UE} || K_{CN-UE})} K_{CN-UE} \bmod p$$
$$R \equiv g^{S_\sigma} v^{R \cdot h(ID_{UE} || ID_{CN} || r_{UE})} \bmod p \bmod q \quad (6)$$

HeNB는 임시로 위임 서명된 위임 서명 $\sigma'_{CN\text{-}HeNB}$ ($\sigma_{OAM\text{-}CN}$에 의해 위임된)를 가질 것이다. HeNB는 임의로 r'을 선택하여 방정식 (7)을 이용하여 계산한다. HeNB는 $\{M', (R', S_{CN}'), K_{OAM}, K_1, K_2, M_{CN_HeNB}, h(M_W || K_{OAM})\}$을 보낸다. 여기서 R'과 M'은 다음과 같다. $R' \equiv g^{r'} \bmod p$ 그리고 $M' = (ID_{HENB} \,||\, ID_{CSG} \,||\, ID_{OAM} \,||\, ID_{CN} \,||\, r_{HeNB})$.

ID_{CSG}는 HeNB의 위치정보를 포함할 수 있다.

$$S_{CN}' = r' + \sigma'_{CN-HeNB} \, h(M') \bmod q \quad (7)$$

Msg9: 검증자 UE는 위임 서명된 공개 키 v_p ($v_p \equiv g^{\sigma_{CN-HeNB}} \bmod p$)를 다음과 같은 방정식(8)을 사용하여 복구한다.($v_{CN}' \equiv v_{OAM}^e K_{OAM} \bmod p$)

$$v_p = K_1 \cdot (v_{CN}' \cdot K_2)^{h(M_{CN-HeNB})} \bmod p \quad (8)$$

그러면 UE는 다음 방정식(9)의 타당성을 검사한다. 만약 같다면 검증자 UE는 유효한 위임 서명된 위임 서명으로써 (r', S_{CN}')를 수락한다. 그리고 HeNB 를 인증한다.

$$g^{S_{CN}'} \equiv r' v_p^{h(m')} \bmod p \quad (9)$$

$\sigma'_{OAM\text{-}CN}$의 경우 따로 설명할 필요가 없다. 우리는 공간의 제약 때문에 프로토콜의 정확성 이외에 어떠한 도움을 줄 수가 없다. 성공적인 인증 후에, 두 키 CK, IK(Integrity Key)는 암호화와 사용자 데이터의 메시지를 인증하는데 사용할 수 있다. CK와 IK는 다음 방정식 (10)과 같이 Diffie-Hellman 키 동의에 의해 파생된다.

$$CK \| IK \equiv g^{r_{UE} r_{HeNB}} \bmod p \quad (10)$$

V. 보안 분석

본 논문에서 제안한 메커니즘은 다음과 같은 위임 서명의 특징을 만족한다.

비가역성(unforgeability): 오직 위임된 UE만이 CN의 대신으로 σ_{CN-UE}를 사용하여 위임 서명을 생성할 수 있다. 또한 HeNB는 OAM(σ_{OAM-CN})의 승인을 가지고 CN을 대신해서 $\sigma'_{CN-HeNB}$을 사용하여 위임 서명된 위임 서명을 생성할 수 있고, 반대로도 마찬가지이다. 이산 대수 문제는 공격자가 비록 공개 값*((R', S_{CN}'), v_P, K_{OAM}, K_1, K_2, $M_{CN-HeNB}$)*와 M_{CN-UE}을 가지더라도 $\sigma'_{CN-HeNB}$와 σ_{CN-UE}를 수학적으로 계산하기 어렵게 만든다.

부인 방지(undeniability): 위임 서명된 서명 *($M', (R', S_{CN}')$, K_{OAM}, K_1, K_2, $M_{CN-HeNB}$))*이 검증되면, 그 보증서 $M_{CN-HeNB}$가 검사되고 서명자의 위임 공개 키 v_{CN}'과 원래 서명자의 공개 키 v_{OAM}가 사용된다. 서명자 CN이 HeNB에게 보내지는 서명을 부인 할 수 없게 된다. 그러므로 제안된 방식은 부인 방지 특성을 만족한다. OAM의 경우에도 따로 설명할 필요가 없다. UE 또한 서명을 부인할 수 없다.

식별성(identifiability): 원래 서명자 OAM은 서명 S_{CN}'($\sigma'_{CN-HeNB}$에 의해 서명된)으로부터 위임 서명과 일치하는 CN을 식별한다, 반대로도 마찬가지이다. 더구나 원래 서명자 CN은 S_0(σ_{CN-UE}에 의해 서명된)을 조사함으로써 UE를 식별할 수 있다.

구별성(distinguishability): UE 인증의 경우 위임 서명*(σ_{CN-UE}, M_{UE}, K_{CN-UE})*이 사용될 때 누구나 일반적인 서명으로부터 위임 서명을 구분할 수 있다. 그리고 HeNB의 인증의 경우 위임 서명된 서명 공개 키 v_P가 위임 서명된 위임 서명을 검증하기 위해 사용되고 반면에 v_{CN}'은 v_{OAM}의 위임 서명을 검증하는데 사용할 것이다. 그러므로 어떤 사용자들도 일반적인 서명으로부터 구분할 수 있을 것이다.

다음 목록은 본 제안이 향상시킨 것을 보안 측면에서 요약한 것이다.

UE와 HeNB 사이의 상호 인증(mutual authentication between UE and HeNB): 상호인증의 향상은 UE와 HeNB사이 상호 인증을 CN과 OAM이 협력적으로 보장한다는 사실에서부터 나왔다. HeNB는 UE의 메시지로부터 CN의 서명이 맞는지 아닌지를 검사한다. 또한, UE는 HeNB의 메시지로부터 정확하게 CN과 OAM에 의해 위임 서명되었는지 검사한다.

키 동의(Key agreement): 키 유도 방식의 강점은 인증 객체가 키 생성에 기여할 수 있다는 것이다. 제안된 방식이 키 파생 방식의 좋은 예이다. 각 객체는 그것들의 난수에 기여한다. (r_{UE}, r_{HeNB})

프로토콜 공격들에 대한 내성(withstanding protocol attacks): 기본적으로 우리의 키 동의 방식은 Diffie-Hellman 키 동의와 같다. 그러나 OAM과 CN은 위임 서명을 가지고 OAM과 CN을 확인하기 때문에 중간자 공격이 방지된다. 합법적인 HeNB를 가지는 악의 있는 OAM은 CN을 속일 수 없게 된다. 왜냐하면 HeNB와 UE가 통신할 때 σ_{CN-OAM}가 필요하기 때문이다. 정확하게 CN이나 OAM은 둘 다 스스로 작동하지 않는다. 공격자는 CN으로부터 위임 서명을 소유하지 않고서는 유효한 HeNB로 위장할 수 없게 된다.

취소할 수 있는 위임 서명(revocable proxy-signature): 만약 OAM(CN)이 특정한 (그룹) HeNB에서 빠지게 된다면, 간단하게 $\sigma'_{OAM-HeNB}$ *($\sigma'_{CN-HeNB}$)* 그리고 공개 값을 취소한다. 비록 위임 서명된 위임 서명이 취소될 지라도 σ_{CN-OAM}*과* σ_{OAM-CN}이 가지는 위임 서명에 관해서는 CN과 OAM 사이에서의 동의는 여전히 유효하다. 그러므로, 단일 점에 의한 영향은 최소화 된다.

일시적인 유저 인증(temporary user authentication): 일시적인 멤버에 대해서는 CSG의 멤버로 간주되는 가입자의 시간 기간을 제한할 수 있다.

Table 2. Authentication Delay in Terms of Operational Cost

Message	UE	HeNB
Msg6	-	-
Msg7	2TM + TH + 1TA	3TE + 3TM + 2TH
Msg8	3TE + 3TM + 2TH +1TA	1TM + 1TH + 1TA
Msg9	1TE	1TE

우리가 제안한 방식에서는 UE는 그의 위임 서명된 권한 σ_{CN-UE}를 임시적인 멤버에게 재 서명할 수 있다. 이러한 위임 서명된 위임 서명의 생성과 검증은 Msg4 (5)와 동일하다.

안전한 소프트웨어/환경설정 업데이트(secure software/configuration update): 모든 소프트웨어의 업데이트와 환경설정 변경은 암호학적으로 v_{OAM}을 통해서 서명될 것이고 대칭 암호화 방식으로 $\sigma'_{OAM-HeNB}$를 가지고 암호화된다.

VI. 서비스 분석

〔Table. 2.〕는 제안된 방식을 동작시켰을 때의 값을 보여준다. T_E, T_M, T_H 그리고 T_A는 각각 모듈러 지수형, 곱셈, 해쉬 그리고 산술연산적 운영상 값이다. 우리는 Msg1부터 Msg4까지의 운영상의 값은 포함하지 않는다. 그 이유는 Msg1과 Msg2는 CN과 OAM 사이에서 계약적인 동의와 관련될 때 서로 교환될 수 있기 때문이다. 또한 Msg5는 HeNB가 생성되었을 때 삽입될 것이다. Msg3과 Msg4는 일반적인 인증 절차를 할 동안 미리 계산될 것이다. 따라서 총 운영상의 값은 four-way handshake를 완수하기 위해 $8T_E + 9T_M + 6T_H + 2T_A$ 정도 걸릴 것이다 (Msg6부터 Msg9까지).

본 논문에서는 T_M, T_E, T_H 및 T_A의 연산속도를 xyssl〔10〕를 이용하여 측정했다. xyssl은 c언어로 제작된 공개 소스 암호 라이브러리이다. 이 라이브러리는 현재 대칭형 암호, 해시 함수, RSA, X.509 읽기 지원 기능 등등 여러 가지 특징을 가지고 있다. 또한, 모바일 컴퓨팅 환경에서 시뮬레이션하기 위해 팬티엄3 500GHz 프로세스에서 테스트를 수행했다. 그 결과로써 1024비트에 대해 모바일 지수는 0.98 microsecond 걸리고 곱셈, 해시 그리고 산술연산은 각각 0.00758, 0.0202 그리고 0.00743 microsecond 걸렸다. 이러한 결과를 토대로 총 인증 지연은 약 8.044 microsecond가 걸리고 이것은 UE가 거의 인식하지 못한다. RSA 1024 암호화가 약 8.921 microsecond가 걸린다는 것에 주의해야 한다.

VII. 결론

본 논문에서 우리는 HeNB 구조를 분석했고 그리고 HeNB가 제공하는 보안성에 대해서 조사했다. 비록 3GPP HeNB에서 UE와 HeNB에 대한 접근 제어를 소개했지만 이것은 여전히 다양한 악의적인 공격에 취약하다(예를 들면 위장하는 것). 이러한 취약성은 악의 있는 공격자가 사용자 트래픽의 방향을 바꿔 사용자를 악의적인 HeNB에 접근하도록 유도한다. 따라서 이런 보안 문제점들을 해결하기 위하여 본 논문에서는 새로운 인증과 키 동의 메커니즘을 제시했다. 제안된 메커니즘은 인증 성능을 3가지 방법으로 개선했다. (1) UE와 HeNB 사이의 상호인증이 강화되었다. (2) 악성 HeNB 공격과 그 변종을 방지한다. (3) 신호 부하와 계산 지연을 줄인다. 그리고 공개키 연산은 USIM에서 구현할 수는 있지만, 편의성 때문에 현재 USIM에서 공개키 연산을 사용하지는 않는다. 즉, 상용화되어 있지 않기 때문에 불가능한 것은 아니지만 구현에 다소 어려움이 있다. 앞으로의 통신 기술 발전에 따라 펨토셀은 더 많이 필요하게 되고 이슈화될 것이다. 펨토셀 환경에서 보안 측면과 퍼포먼스 측면에서 더 향상된 프로토콜이라고 할 수 있다.

References

〔1〕 3GPP 3GPP, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security of H(e)NB (Release 8), 3GPP TR 33.820 v8.3.0, December 2009.

〔2〕 3GPP, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service requirements for Home NodeBs and Home eNodeBs (Release 11), 3GPP TS 22.220 v11.6.0, September 2012.

〔3〕 3GPP, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture aspects of Home NodeB and Home eNodeB (Release 9), 3GPP TS 23.830 v9.0.0, October 2009.

〔4〕 3GPP, 3rd Generation Partnership

〔5〕 Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security Architecture (Release 12), 3GPP TS 33.401 v12.8.1, July 2013.
〔6〕 Masahiro Mambo, Keisuke Usuda, and Eiji Okamoto, "Proxy signatures: Delegation of the power to sign messages," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, pp.1338-1354, Vol.E79-A, No.9, 1996.
〔7〕 S. Kim, S. Park and D. Won, "Proxy signatures, Revisited," Proceedings of the First International Conference on Information and Communication Security, Lecture Notes In Computer Science, Vol. 1334, pp.223-232, 1997.
〔8〕 S.-J. Hwang and C.-H. Shi, "A Simple Multi- Proxy Signature Scheme," Proceedings of the 10th National Conference on Information Security, pp. 134-138, 2000.
〔9〕 Lijang Yi, Guoqiang Bai and Guozhen Xiao, "Proxy multi-signature scheme: A new type of proxy signature scheme," IEEE Electronics Letters, pp.527-528, Vol.36, No.6, 2000.
〔10〕 Kaisa Nyberg, Rainer A. Rueppel, "A new signature scheme based on the DSA giving message recovery," Proceedings of the first ACM Conference on Computer and Communications Security, pp. 58-61, 1993.
〔11〕 xyssl (PolarSSL), available at http://polarssl.org/

〈저 자 소 개〉

최 형 기 (Hyoung-Kee Choi) 정회원
1992년 2월: 성균관대학교 전자공학과 학사졸업
1996년 2월: Polytechnic University in Brooklyn, NY 석사졸업
2001년 2월: Georgia Institute of Technology in Atlanta, GA 박사졸업
2001년~2004년: Lancope 근무
2004년 3월~현재: 성균관대학교 정보통신대학 부교수
〈관심분야〉 네트워크보안, Traffic characterization and modeling

한 찬 규 (Chan-Kyu Han) 학생회원
2006년 8월: 성균관대학교 컴퓨터공학전공 학사졸업
2008년 2월: 성균관대학교 전자전기컴퓨터공학과 석사졸업
2012년 2월: 성균관대학교 휴대폰학과 박사졸업
2013년 3월~현재: 삼성전자 근무
〈관심분야〉 네트워크보안

김 승 룡 (Seung-Ryong Kim) 학생회원
2012년 8월: 광운대학교 전자통신공학과 학사졸업
2012년 9월~현재: 성균관대학교 전자전기컴퓨터공학과 석사과정
〈관심분야〉 네트워크보안