Journal of The Korea Institute of Information Security & Cryptology(JKIISC) ISSN 1598-3986(Print)
VOL.23, NO.5, October 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.5.885

# LTE-Advanced에서의 Machine Type Communications을 위한 그룹 기반 보안 프로토콜

최 대 성,† 최 형 기‡
성균관대학교

# An Group-based Security Protocol for Machine Type Communications in LTE-Advanced

Dae-Sung Choi,† Hyoung-Kee Choi‡
SungKyunKwan University

## 요 약

사람이 개입할 필요 없이 기기 및 사물들을 셀룰러 망(cellular network)으로 연결하여 언제 어디서나 다양한 서비스를 제공하는 MTC(Machine Type Communications)는 차세대 통신의 주요 이슈로 고려되고 있다. 현재, 다수의 MTC 단말들이 동시적으로 망에 접속하려고 하면 각 MTC 단말들은 독립적인 접근 인증 절차를 수행해야 된다. 이로 인해 LTE-Advanced 네트워크에서 인증 시그널링(authentication signaling) 혼잡(congestion)과 부하(overload)의 문제가 야기된다. 본 논문은 그룹 기반의 인증 프로토콜과 키 관리 프로토콜을 제안한다. 그룹 단위로 MTC 단말들을 관리하기 위해 제안하는 프로토콜은 그룹 리더(leader)를 선출하고, 리더만이 코어 망(core network)과의 인증에 참여한다. 인증이 완료된 후, 그룹 리더는 이진트리(binary tree)를 구성하여 나머지 구성원(member)들과 MME(Mobility Management Entity)를 관리한다. 마지막으로 제안 프로토콜 분석은 제안하는 프로토콜이 MTC 단말들과 코어 망 사이에서 발생되는 인증 시그널링을 줄여줄 수 있을 뿐만 아니라 효율적으로 MTC 단말들을 관리할 수 있음도 보여준다.

## ABSTRACT

MTC(Machine Type Communications), providing a variety of services anytime and anywhere by connecting the cellular network to the machine and things without human intervention, is being considered as a major challenge of the next-generation communications. Currently, When a massive MTC devices simultaneously connect to the network, each MTC device needs an independent access authentication process. Because of this process, authentication signaling congestion and overload problems will cause in LTE-Advanced. In this paper, we propose a group-based authentication protocol and a key management protocol. For managing the MTC devices as group units, the proposed protocol elects a group leader and authentications only once with the core network. After the authentication is completed, a group leader manages the rest members and MME(Mobility Management Entity) by constructing a binary tree. Finally, the propose protocol analysis show that the proposed protocol not only can reduces the authentication signaling which generated in between the MTC devices and the core network but also can manages the MTC devices, efficiently.

**Keywords**: machine type communications (MTC), 3GPP authentication and key agreement (AKA), long term evolution-advanced (LTE-Advanced), group key management

접수일(2013년 3월 4일), 수정일(1차: 2013년 6월 10일, 2차: 2013년 7월 23일), 게재확정일(2013년 8월 8일)

† 주저자, ds.choi@skku.edu
‡ 교신저자, hkchoi@ece.skku.ac.kr(Corresponding author)

## I. 서 론

최근 들어 우리 주변의 모든 사물들을 네트워크를 통해 연결함으로써 언제 어디서나 필요한 정보를 얻고, 전달할 수 있는 M2M(Machine to Machine)이 통신 시장의 주요 이슈로 부각되고 있다. 사물의 이동성, 광범위한 서비스 지역, 네트워크의 유지보수 용이성, 데이터 전송의 신뢰성, 그리고 서비스의 품질 보장 등 다양한 장점을 가지고 있는 M2M에 대해 모바일 망(mobile network)을 사용하는 3GPP(Third Generation Partnership Project)는 MTC(Machine Type Communications)라고 정의하고 2008년부터 본격적인 표준화 작업을 진행하였다. 3GPP 망은 광역 커버리지(coverage), 신뢰할 수 있는 데이터 서비스의 고속 전송, 유연한 이동성, 그리고 내장된 보안 메커니즘(mechanism)을 가지고 [1], 다음과 같이 여러 응용 분야에 적용할 수 있다 [2]: (1) 보안(예, 침입 감시 시스템); (2) 추적(예, 학교 버스와 같은 특수 차량의 위치 추적, 제조 기업의 제품 공급 체인의 추적); (3) 원격 유지보수/제어(예, 고장에 대한 수리를 위해 공공 인프라 장치를 원격 제어); (4) 모니터링(예, 가전제품을 위한 스마트 미터링[3], 전자 의료 서비스[4][5]). 추가적으로, 3GPP는 다수의 MTC 단말들을 효율적으로 관리하기 위해 그룹 기반의 MTC 특징을 정의하였다. 하지만, MTC 그룹의 필요성과 정책(policing)에 대한 간단한 언급에 그칠 뿐 본격적인 논의는 이뤄지지 않고 있다.

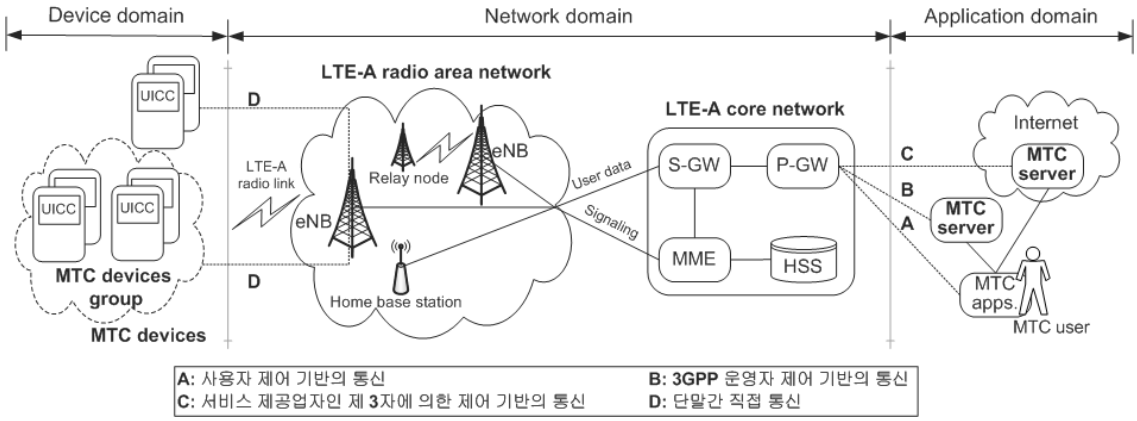
기존 3GPP의 보안 프로토콜은 H2H(Human to Human) 기반에 최적화하기 위해 설계되어 있다. 하지만, MTC는 다수의 단말들 존재, 독특한(unique) 트래픽 패턴, 낮은 이동성, 그리고 취약하거나 무인 장소에 MTC 단말들이 배치되는 것과 같이 H2H 환경과 다른 점 때문에 수많은 챌린지(challenge)가 발생한다. 특히, 공공 서비스들은 망 서비스 제공자(network service operator)에 의해 제공되기 때문에 다수의 단말들이 망 서비스 제공자와의 상호 인증을 위해 동시적으로 수많은 인증 시그널링(authentication signaling)을 발생시키면 코어 망(core network)에서 혼잡(congestion)과 부하(overload) 문제가 발생할 수 있고, 최악의 경우 코어 망에서 단말들의 접근을 거절하여 단말들은 서비스를 제공받지 못하는 문제가 발생한다[6]. 물론, 혼잡 제어(congestion control)에 대한 연구는 진행되었지만[7] 여전히 각 단말들 마다 발생시키는 인증 시그널링의 횟수는 똑같기 때문에 코어 망이 부담하는 인증 시그널링에 대한 혼잡과 부하를 줄여주지 못한다. 따라서, 존재하고 있는 인증 프로토콜은 다수의 MTC 단말들이 존재하는 환경에 직접적으로 적용할 수 없다.

본 논문은 그룹 기반의 최적화(optimization)를 통해 인증 시그널링을 줄일 수 있는 프로토콜을 제안한다. 제안하는 프로토콜은 인증 프로토콜과 키 관리 프로토콜로 나누어 구성되어 있다. 인증 프로토콜은 다수의 MTC 단말들을 하나의 그룹으로 묶어 코어 망과의 인증 과정을 진행하는 프로토콜이다. 키 관리 프로토콜은 인증이 완료된 이후, 코어 망과 MTC 단말들 사이의 세션 키 동의(session key agreement) 및 그룹 관리에 필요한 키(key)를 업데이트(update)하는 메커니즘(mechanism)을 제공한다. 키 관리 프로토콜은 [8]에서 제안된 프로토콜에 기초하고, 이 프로토콜은 안전한 스마트 그리드 통신을 위해 제안된 키 관리 프로토콜이다.

나머지 부분의 구성은 아래와 같다. 2장에서 제안한 프로토콜을 위한 관련된 연구에 대해서 알아본다. 3장은 MTC의 구조, 통신 시나리오, 그리고 MTC 환경의 취약점과 보안 요구사항에 대해서 설명한다. 제안하는 프로토콜을 소개하기 전 4장에서는 사전 지식에 대해서 설명한다. 5장은 제안하는 프로토콜을 자세하게 설명한다. 6장은 제안하는 프로토콜의 보안과 성능의 다양한 수치상의 분석을 제공한다. 마지막으로 7장에서는 결론에 대해 기술한다.

## II. 관련 연구

GPP 표준으로 정의된 EPS-AKA(Evolved Packet System-Authentication and Key Agreement)는 4세대 통신인 LTE(Long Term Evolution) 또는 LTE-Advanced에서 사용되는 인증 및 키 동의 프로토콜이다. 현재 EPS-AKA는 MTC 단말들이 존재하는 MTC 그룹에 직접적으로 적용할 수 없다. 그 이유는 다음과 같다. 첫 번째, EPS-AKA는 하나의 단말과 코어 망 사이의 일대일 인증을 위한 목적으로 설계되었기에 MTC 그룹의 구성원들이 동시적으로 발생시키는 인증 시그널링을 처리할 수 있는 메커니즘이 없기 때문이다. MTC 단말은 기존 H2H 환경의 단말들보다 1000배 이상의 단말들이 존재할 것으로 예상되므로[5] 동시적으로 발




〔그림 1〕 MTC 시스템 구조 및 4가지 유형의 통신 시나리오

생되는 인증 시그널링에 의한 혼잡 및 부하 문제의 발생 가능성은 상당히 높다. 두 번째, 하나의 MTC 그룹에 속하는 MTC 단말들은 그룹 구성원들과의 통신뿐만 아니라 다른 그룹 구성원들과의 통신을 할 수 있어야 하지만 EPS-AKA는 그룹 단위의 관리 및 통신을 지원할 수 있는 어떠한 메커니즘도 없기 때문이다. 따라서, LTE-Advanced에서 다수의 MTC 단말들로 인한 혼잡 및 부하를 줄일 수 있는 새로운 인증 프로토콜이 요구된다.

선행 연구된 그룹 기반의 인증 및 키 동의 프로토콜은 (1) 이종(heterogeneous) 도메인(domain) 사이에서의 로밍(roaming)시 인증을 위해 제안된 프로토콜; (2) 같은 도메인 사이에서의 인증을 위해 제안된 프로토콜로 분류할 수 있다. 이종 도메인 사이에서의 인증을 위한 프로토콜과 관련된 연구에서 Aboudagga 등은 공개 키 인프라상의 무선 네트워크에서 이종 도메인 사이의 로밍시 모바일 그룹 또는 개인 노드들을 인증하는 프로토콜인 mGAP(mobile Group Authentication Protocol)를 제안하였다〔9〕. 또한, Zhang 등은 홈(home) 도메인에서 방문(visited) 도메인으로 로밍하는 MTC 그룹들을 인증하는 프로토콜인 DGBAKA(Dynamic Group Based Authentication and Key Agreement)를 제안하였다〔10〕. 같은 도메인 사이에서의 인증을 위한 프로토콜과 관련된 연구에서 Ngo 등은 넓은 규모의 무선 네트워크에서 모바일 단말들의 자원을 고려한 인증 프로토콜을 제안하였다〔11〕. 또한, Chen 등은 3세대 통신 표준인 UMTS(Universal Mobile Telecommunication System) 상에서 단말 그룹들이 코어 망과의 인증 시그널링을 줄일 수 있는 프로토콜인 G-AKA(Group-based AKA)를 제안하였다〔12〕.

이전의 연구에서는 인증을 요청하는 처음 단말에 대해서만 정상 과정의 인증 절차를 수행하고, 나머지 단말들에 대해서는 처음 단말을 통해 얻은 그룹 정보를 이용하여 간소화된 인증 절차를 수행함으로써 인증 지연을 줄임을 보였다. 그러나 여전히 각 단말마다 인증 절차를 수행해야 되기 때문에 이 과정에서 발생되는 인증 시그널링은 줄이지 못한다.

## III. 시스템 모델

본 장에서는 MTC에 대한 소개로 시스템 구조, 통신 시나리오, 위험 요소 및 보안 요구사항에 대해서 설명한다.

### 3.1 MTC 시스템 구조

〔그림 1〕은 전형적인 MTC 시스템 구조를 묘사한 것이다. MTC 시스템 구조는 3개의 메인 도메인으로 구성되며 각각 단말 도메인(device domain), 망 도메인(network domain), 그리고 응용 도메인(application domain)으로 불린다. 단말 도메인은 수많은 MTC 단말들로 형성된다. MTC 단말들은 물리적 위치에 존재하는 기기(예, 가스 미터, 몸체 센서 등)에 부착되어, 해당 기기의 정보를 송신하거나 해당 기기에게 필요 정보를 전달한다. 추가적으로 MTC 단말은 제거할 수 있는 UICC(Universal Integrated Circuit Card)를 포함한다. UICC는 가입자 정보와 망에 접근하기 위한 몇몇의 암호학 키를 저

장한다. 망 도메인은 MTC 단말들과 무선 구간 망(radio area network) 사이를 제외한 나머지 모든 구간을 유선 망 환경으로 구성한다. 무선 구간 망은 MTC 단말들로부터 받은 데이터를 코어 망으로 릴레이(relay) 해준다. 코어 망에 존재하는 MME(Mobility Management entity)와 S-GW(Serving Gateway)는 각각 시그널링 트래픽(signaling traffic)과 사용자 데이터 트래픽(user data traffic)을 책임진다. MME가 보내는 시그널링은 HSS(Home Subscriber Server)로 전달된다. HSS는 MTC 단말들의 가입자 정보가 저장되어 있고, 암호학 함수를 통해 MTC 단말들을 인증하는데 필요한 값을 생성한다. S-GW는 사용자 데이터를 P-GW(Packet data network Gateway)로 전달하고, P-GW는 사용자 데이터를 외부 네트워크로 보낸다. 응용 도메인내의 MTC 서버(server)는 MTC 단말들로부터 전송된 데이터를 처리함으로써 MTC 사용자(user)들에게 서비스를 제공한다. 또한 MTC 사용자들(예, 일반 사용자, 제어 센터 등)은 MTC 단말들을 관리할 수 있는 데이터를 전송할 수 있다.

### 3.2 통신 시나리오

3GPP는 일반적으로 망 도메인과 응용 도메인 사이에서 3가지 유형의 통신 시나리오를 지원한다. 3GPP 운영자 제어 기반의 통신([그림 1]의 B)의 경우 MTC 서버는 운영자 도메인에 위치하여 MTC 단말들과 통신한다. 서비스 제공업자인 제3자에 의한 제어 기반의 통신([그림 1]의 C)의 경우 MTC 서버는 운영자 도메인의 외부에 위치하여 MTC 단말들과 통신한다. 다양한 서비스들을 위해 많은 서비스 제공업자인 제3자를 수용할 경우 제3자에 대한 인증, 접근 제어 등과 같은 별도의 연동 프로토콜이 필요하다. 사용자 제어 기반의 통신([그림 1]의 A)의 경우 MTC 사용자는 어플리케이션을 통해 직접적으로 코어 망에 접근하여 MTC 단말들의 데이터를 얻을 수 있다. MTC 사용자가 직접 3GPP 코어 망에 접속하므로 보안 측면에서는 취약하지만, 기존의 3GPP 가입자라면 별다른 인터페이스(interface) 없이 자신의 모바일 단말로 직접 제어가 가능하다는 장점이 있다.

3GPP는 ad-hoc 통신을 지원하지 않는다[13]. 따라서, 비록 근/중거리내에 MTC 단말들이 존재하더라도 상호간에 직접적인 통신이 불가능하다. 이를 위해 3GPP는 코어 망을 이용하여 MTC 단말들간의 직접 통신([그림 1]의 D)을 지원한다. 코어 망을 이용하기 때문에 ZigBee나 Bluetooth와 같은 근/중거리내에서 발생할 수 있는 취약점들에 영향을 받지 않는다. 또한, 신뢰할 수 있는 제3자를 보장하므로 안전한 통신이 가능하다.

### 3.3 위험요소 및 보안 요구사항

본 절에서는 먼저, MTC의 보안 위험요소를 요약하여 설명한다. 주요 위험요소는 다음과 같다[14].

- 메시지의 불법적 변경(illegal modification of message): MTC 단말들과 코어 망의 AKA 과정 이후에, 코어 망은 무결성 보호와 암호화를 위한 보안 모드(security mode) 절차를 수행한다. 따라서, 공격자는 코어 망이 혼잡 제어을 위해 생성하는 접근 거절 메시지(access reject message)나 접근 우선순위 지표 메시지(access priority indicators message)를 위조하여 정상 MTC 단말들에게 전송할 수 있다. 이에 따라, 서비스 거부 공격(denial-of-service attack)이 일어나고 MTC 단말들의 서비스 이용이 거절된다.
- 가짜 망에 의한 위조된 메시지(forged message by false networks): MTC 단말들은 가짜 코어 망이나 MTC 서버로부터 자원 소모가 목적인 위조된 메시지를 받을 수 있다. 위조된 메시지는 H2H 통신보다 MTC에서 더욱 더 위험하다. 메시지를 판단할 수 있는 사람이 존재하는 H2H 통신과는 달리 MTC에서는 MTC 단말들이 자신이 받은 메시지가 정상인지 아닌지에 대해 판단할 수 없기 때문이다.
- 외부 인터페이스에 의해 노출된 메시지(exposed message by external interface): 코어 망과 MTC 서버 사이의 외부 인터페이스는 안전하지 않은 링크로 구성될 수 있다. 따라서, 외부 인터페이스를 통해 전달되는 모든 메시지들은 공격자에 의해 도청될 수 있다. 또한, 비인증된 MTC 서버 또는 제3자 서비스 제공업자에 의해 개인 식별자와 같은 개인정보가 남용될 수 있다.
- 그룹 최적화의 남용(misuse of group optimization): 그룹 내에 존재하는 MTC 단말이 다른 구성원들과 공모하여 서비스 거부 공격을 시행할 수 있다.

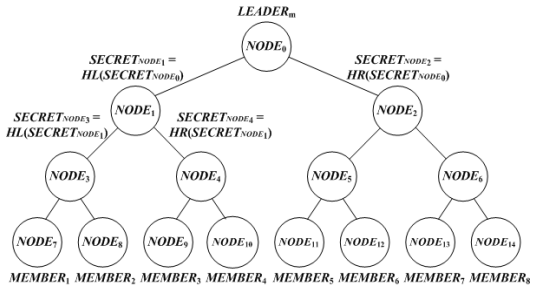
위에 언급된 보안 위험요소를 기반으로 MTC에서는 다음과 같은 보안 요구사항을 충족해야 한다.

- 상호 인증(mutual authentication): MTC 단말들과 망, 서버들은 서로간에 합법적이고 정상적인 개체(entity)인지 확인해야 한다. 특별히 운영자 도메인 외부에 위치하는 MTC 서버와 망과의 상호 인증은 필수적이다.
- 비밀성과 무결성(confidentiality and integrity): 3GPP 망을 통하여 연결된 MTC 서버가 MTC 단말들에게 보내는 메시지와 3GPP 망이 단말들에게 보내는 메시지는 비 인증된 개체들에 의한 노출 및 위조로부터 보호되어야 한다. 또한, 구성원들로 위장하거나 그룹 메시지를 위조하지 않도록 하기 위해 그룹 메시지의 암호화가 필요하다.

## IV. 사전 지식

본 장에서는 제안하는 프로토콜에서 사용하는 암호학 기법인 타원곡선을 이해하기 위한 사전 지식으로 다음 절에서 타원곡선시스템(elliptic curve cryptosystem)에 대해서 설명한다.

타원곡선시스템은 1985년 Miller와 Koblitz에 의해 제안된 공개키 암호 알고리즘이다. 타원곡선에 기반을 두고 있는 암호알고리즘의 기본 원리는 3차 방정식을 이용하여 유한순환군(finite cyclic group)을 만들 수 있다는 것이다. 이 유한순환군은 기존에 매우 큰 소수를 이용하여 만든 유한순환군을 대체할 수 있다. 따라서, 이산대수(discrete logarithm)에 기반을 두고 있는 기존 암호 알고리즘의 형태를 보존하면서 타원곡선 기반으로 쉽게 전환할 수 있다. 암호기술에서 타원곡선군은 다음과 같이 정의된다. $p$가 소수일 때, 유한체(finite field) $Fp$상에서의 $a,b \in Fp$의 조건을 만족하고, 방정식 $y^2 \bmod p = x^3 + ax + b \bmod p$에서 $x,y \in Fp$이며, $4a^3 + 27b \neq 0 (\bmod p)$의 조건을 만족하면 타원곡선 위의 점들로 구성된 $(x,y)$점들의 집합과 무한 원점(point at infinity) 이라고 불리는 점 $O$는 타원곡선을 이용하는 군의 원소들이 된다. 타원곡선군은 스칼라 곱(scalar multiplication) 연산을 수행함으로 덧셈군(additive group)을 생성할 수 있다. 이때, 기본 점(base point) $P_0$을 선정하여 임의의 값 $k$와의 연산을 수행했을 경우 무한 원점이 된다면 임의의 값 $k$는 위수(order)라고 불린다.




〔그림 2〕 비밀 키 관리를 위한 이진트리의 구성

## V. 제안 프로토콜

MTC 환경에서 다수의 MTC 단말들이 망과의 인증을 위해 발생시키는 인증 시그널링은 망의 부하를 증가시키고, 이로 인해 정상적인 통신을 지연시킨다. 본 장에서는 다수의 MTC 단말들이 발생시키는 인증 시그널링을 줄이기 위한 상호 인증 프로토콜과 키 관리 프로토콜을 제안한다.

### 5.1 그룹의 키 관리 단계

같은 MTC 사용자에 속해 있거나 같은 지역에 위치하는 MTC 단말들은 쉽게 관리 및 제어를 위해 그룹 단위로 묶을 수 있다[14]. LTE-Advanced 망 서비스를 제공하는 운영자는 서비스를 제공받기 원하는 $n$개의 MTC 단말들중 $m$개의 후보 그룹 리더(candidate group leader)를 지정한다. 후보 그룹 리더들 중 그룹을 대표할 수 있는 그룹 리더를 선출하기 위해 다음과 같은 작업을 수행한다. 본 논문은 후보 그룹 리더들간의 통신을 위해 WiFi가 지원된다고 가정한다.

1) 후보 그룹 리더들은 자신의 *LTE K*와 식별자 *IMSI*(International Mobile Subscriber Identity)를 해쉬함수를 통해 해쉬값을 생성하고, 서로 공유한다. 후보 그룹 리더간의 통신은 서로 공유된 비밀키인 그룹 리더 키 *GRK*에 의해 보호된 채널상에서 안전하게 이뤄진다.

2) 각 후보 그룹 리더는 공유된 해쉬값들과 자신의 해쉬값을 비교한다. 이때, 가장 높은 해쉬값을 생성한 후보 그룹 리더가 그룹을 대표하는 그룹 리더로 선출된다.

추가적으로 선출된 그룹 리더 및 나머지 후보 그룹 리더들은 운영자와 주기적으로 안전한 통신을 통해 그룹에 속한 나머지 구성원들의 정보를 얻을 수 있다고

가정한다.

가입자들의 정보가 저장된 데이터베이스 서버인 HSS(Home Subscriber Server)는 〔그림 2〕와 같이 그룹 리더들을 자식 노드로 구성하는 이진트리를 생성하여 그룹 리더들을 관리한다. 이때, HSS는 그룹 리더 및 나머지 후보 그룹 리더들에게 같은 비밀값 $SECRET_{NODE_n}$을 할당한다.

그룹 리더 및 나머지 후보 그룹 리더들도 자신이 속한 그룹의 구성원들을 자식 노드로 구성하는 이진트리를 생성한다. 그룹의 키 관리를 위해 자식 노드의 수는 하나의 그룹에 속하는 $n$개의 MTC 단말들보다 크거나 같아야 된다. 각 노드는 제한된 비밀 값 $RS$(Restricted Secret value)를 가지게 되는데, $RS$는 근원(root) 노드에서 자신이 위치한 경로 사이의 비밀 값 $SECRET_{NODE_n}$들을 제외한 모든 노드들의 비밀 값들의 집합으로 구성된다. 예를 들어 〔그림 2〕에서 보듯이 자식 노드내의 구성원 $MEMBER_5$의 $RS$는 $SECRET_{NODE_1}$, $SECRET_{NODE_6}$ 그리고 $SECRET_{NODE_{12}}$의 집합으로 구성된다. 각 노드의 비밀 값은 자신의 부모(parent) 비밀 값으로부터 왼쪽 노드에 대해서는 왼쪽 자식 해쉬함수 $HL(\cdot)$에 의해, 오른쪽 노드에 대해서는 오른쪽 자식 해쉬함수 $HR(\cdot)$에 의해 구해진다.

HSS는 자신이 생성한 이진트리내의 자식 노드로 구성된 그룹 리더들의 비밀 값을 이용하여 해당 그룹 리더의 이진트리에 속한 모든 구성원들의 $RS$를 생성한다. 그룹의 키 관리를 위해 LTE-Advanced 서비스에 가입하는 MTC 단말들의 UICC에는 자신의 그룹 식별자 $IMGI$(International Mobile Group Identity), 그룹 키 $GK$ 그리고 $RS$가 저장된다. 추가적으로 비밀 값 $SECRET_{NODE_n}$을 추출하기 위한 2개의 해쉬함수 $HL(\cdot), HR(\cdot)$와 그룹 키 갱신을 위한 1개의 해쉬함수 $H$도 UICC에 저장된다.

### 5.2 시스템 초기화 단계

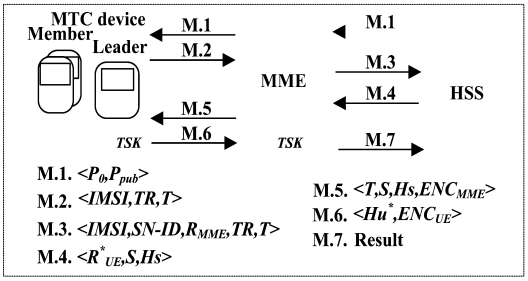
HSS는 그룹 리더와의 상호 인증을 하기 위해 다음과 같은 단계의 시스템 초기화 단계를 거치게 된다.

***Step 1***: HSS는 $i$-bit의 소수 $p$와 타원곡선그룹 $E_P(a,b)$로부터 위수 $a$와 기본 점 $P_0$를 선택한다.

***Step 2***: HSS는 〔1, $a$-1〕로부터 랜덤하게 비밀정보 $s_0$를 선택하고, 공개 키 $P_{pub}=s_0 \cdot P_0$를 계산한다.

***Step 3***: HSS는 다음과 같이 2개의 해쉬함수와 1개의 키 추출(derivation)함수를 생성한다.

- $H_1=\{0,1\}^* \rightarrow E_P(a,b)$
- $H_2=E_P(a,b)\times E_P(a,b)\rightarrow\{0,1\}^*$
- $KDF=\{0,1\}^* \times E_P(a,b)\rightarrow\{0,1\}^i$




〔그림 3〕 그룹 기반의 상호인증을 위한 7개 메시지와 임시적 세션 키 동의

***Step 4***: HSS는 각 MTC 단말들에게 다음과 같이 그룹에 맞는 고정적 공개 정보를 UICC에 저장시키고, 유동적 공개 정보를 MME에게 배포한다.

- 고정적 공개 정보 $\{p, E_P(a,b), a, H_1, H_2, KDF\}$
- 유동적 공개 정보 $\{P_0, P_{pub}\}$

추가적으로 $s_0$는 비공개로 보관된다.

### 5.3 상호 인증 단계

그룹 리더와 HSS는 〔그림 3〕과 같이 상호 인증을 한다. 이번 절에서 사용되는 변수들은 타원곡선상의 연산을 기반으로 계산된다.

***Step 1***: MME는 HSS에게 받은 리더 식별자 요청 메시지 $\langle P_0, P_{pub}\rangle$(〔그림 3〕의 M.1)를 리더에게 보낸다.

***Step 2***: 리더는 〔1, $a$-1〕로부터 임의의 값 $RAND_{UE}$를 생성하고, 다음의 변수를 계산한다.

- $R_{UE}=RAND_{UE} \cdot P_0$
- $TID=H_1(IMGI \| GK)$
- $TR=RAND_{UE} \cdot P_{pub}$
- $T=R_{UE}+TID$

그리고 나서, 리더는 자신의 식별자 $IMSI$(International Mobile Subscriber Identity)를 포함하여 MME에게 리더 식별자 응답 메시지 $\langle IMSI, TR, T\rangle$(〔그림 3〕의 M.2)를 보낸다.

***Step 3***: MME는 〔1, $a$-1〕로부터 임의의 값 $RAND_{MME}$를 생성하고, 다음의 변수를 계산한다.

• $R_{MME} = RAND_{MME} \cdot P_0$

그리고 나서, MME는 자신의 식별자 $SN-ID$ (Serving Network Identity)와 함께 HSS에게 리더 인증을 위한 메시지인 리더 인증 요청 메시지 $\langle IMSI, SN-ID, R_{MME}, TR, T \rangle$([그림 3]의 M.3)를 보낸다.

***Step 4***: HSS는 처음에는 MME의 식별자 $SN-ID$를 통해 정상적인 MME인지를 확인한다. 정상적인 MME라면, 리더 인증 단계에 들어간다. HSS는 가입자 데이터베이스에서 리더의 식별자 $IMSI$를 통해 리더가 속해있는 그룹의 식별자 $IMGI$와 그룹 키 $GK$를 읽어 임시적(temporary) 그룹 식별자 $TID^{**} = H_1(IMGI \| GK)$를 추출한다. 그리고 나서, 다음의 변수를 계산한다.

• $R^*_{UE} = TR \cdot s_0^{-1}$

• $TID^* = T - R^*_{UE}$

만약 $TID^{**}$와 $TID^*$가 일치하지 않는다면 리더 거절 메시지를 보내게 된다. 일치할 경우 HSS는 리더를 인증하게 되고, 다음과 같이 변수를 계산하여 $R^*_{UE}$와 함께 MME에게 리더 인증 응답 메시지 $\langle R^*_{UE}, S, Hs \rangle$([그림 3]의 M.4)를 보낸다.

• $S = TID^* + R_{MME}$

• $Hs = H_2(R^*_{UE} \| TID^*)$

***Step 5***: MME는 임시적(temporary) 세션 키 $TSK = KDF(RAND_{MME} \cdot R^*_{UE})$를 생성하고, 리더가 올바른 $TSK$를 생성하는지 확인하기 위한 암호화 값 $ENC_{MME} = E_{TSK}(R^*_{UE})$를 계산한다. 추가적으로 $Hu = H_2(R^*_{UE} \| R_{MME})$를 계산한 후, 모든 그룹 구성원들에게 브로드캐스트(broadcast)로 HSS 인증 요청 메시지 $\langle T, S, Hs, ENC_{MME} \rangle$([그림 3]의 M.5)를 보낸다.

***Step 6***: 모든 그룹 구성원들은 동시에 다음과 같은 변수를 계산한다.

• $Hs^* = H_2(R_{UE} \| TID)$

• $Hu^* = H_2(R_{UE} \| R^*_{MME})$

• $R_{UE} = T - TID$

• $R^*_{MME} = S - TID$

만약 $Hs$와 $Hs^*$가 같다면 모든 그룹 구성원들은 HSS를 인증하게 된다. 그리고 나서, 리더는 임시적 세션 키 $TSK = KDF(RAND_{UE} \cdot R^*_{MME})$를 생성하고 암호화 값 $ENC_{MME}$를 복호화 한다. 만약, $R^*_{UE}$와 $R_{UE}$이 같다면 리더는 MME와 같은 임시적 세션 키 $TSK$를 생성했음을 확인할 수 있다. 추가적으로 MME가 리더로부터 올바른 임시적 세션 키 $TSK$가 생성되었는지 확인하기 위한 암호화 값 $ENC_{UE} = E_{TSK}(R^*_{MME})$를 계산한다. 이후, 리더는 MME에게 HSS 인증 응답 메시지 $\langle Hu^*, ENC_{UE} \rangle$([그림 3]의 M.6)를 보낸다.

***Step 7***: MME는 $Hu$와 $Hu^*$를 비교한다. 만약 둘의 값이 다르다면 그룹 구성원들에게 브로드캐스트로 리더 거절 메시지를 보낸 후, HSS에게 결과 메시지 $\langle Fail \rangle$([그림 3]의 M.7)를 보낸다. 한편, 둘 의 값이 같다면 암호화 값 $ENC_{UE}$를 복호화하여 $R^*_{MME}$와 $R_{MME}$를 비교한 후, 리더와 같은 임시적 세션 키 $TSK$를 가지고 있음이 확인되면 HSS에게 결과 메시지 $\langle Success \rangle$([그림 3]의 M.7)를 보낸다.

### 5.4 그룹 키 갱신 및 세션 키 동의 단계

리더와 HSS의 상호 인증이 성공적으로 완료되면, 리더는 그룹의 키 관리를 위해 MME를 이진트리의 자식 노드로 가입(join)시키기 위한 작업을 수행한다.

리더는 그룹 키 $GK$로 암호화된 가입 메시지 $< JOIN, MEMBER_n, \text{가입되는트리내의위치} >$를 코어 망으로 전송한다. 코어 망은 브로드캐스트를 통해 그룹 구성원들에게 가입 메시지를 보낸다. 그룹 구성원들은 암호화된 가입 메시지를 복호화한 이후, 2개의 해쉬함수 $HL(\cdot)$과 $HR(\cdot)$를 이용하여 가입하는 MME의 비밀값 $SECRET_{NODE_n}$을 추출한다. 그룹 구성원들은 기존 그룹 키 $GK$를 새로운 그룹 키 $GK$로 갱신하기 위하여 다음과 같은 수식을 이용한다.

$$GK' = H(GK \oplus SECRET_{NODE_n}) \quad (1)$$

이후, 리더는 MME에게 $\langle GK', RS \rangle$ 메시지를 보낸다. 이 메시지는 임시적 세션 키 $TSK$에 의해 보호된 채널상에서 안전하게 전달된다. 마지막으로 리더는 MME를 이진트리의 자식 노드로 가입시킨다.

이진트리내에 MME가 성공적으로 가입되면 MTC 단말들은 MME와 세션 키 동의를 진행한다. MTC 단말들과 MME는 서로 다른 $RS$내에서 공통된 비밀값 $SECRET_{NODE_n}$을 추출한다. 예를 들어, [그림 2]에서 하나의 구성원은 $MEMBER_3$이고 MME는 $MEMBER_8$이라고 하자. $MEMBER_3$과 $MEMBER_8$사이에 서로 공통된 비밀 값은 $SECRET_{NODE_3}$,

$SECRET_{NODE_5}$, $SECRET_{NODE_7}$, $SECRET_{NODE_8}$, $SECRET_{NODE_{10}}$, $SECRET_{NODE_{11}}$, $SECRET_{NODE_{12}}$그리고 $SECRET_{NODE_{13}}$이다. 최종적으로 둘 사이의 세션 키 $SK_{3,8}$는 다음과 같이 계산된다.

$$SK_{3,8} = H(SECRET_{NODE_3} \oplus SECRET_{NODE_6} \cdots \oplus SECRET_{NODE_{13}}) \quad (2)$$

만약 MTC 단말들이 핸드오버(handover)가 발생할 경우, 그룹 구성원이었던 오래된 MME는 이진트리에서 탈퇴될 수 있다. 핸드오버 절차를 수행하면서 그룹 리더는 새로운 MME를 이진트리내의 자식 노드로 가입시킨다. 이후, 그룹 리더는 오래된 MME를 이진트리의 자식 노드에서 탈퇴(leave) 시키기 위한 작업을 수행한다. 이후의 진행 사항은 가입 과정과 동일하다. 그룹 리더는 오래된 MME를 이진트리내의 자식 노드에서 탈퇴시키고, 새로운 MME가 포함된 코어 망으로 탈퇴 메시지 $\langle LEAVE, MEMBER_n, $트리내의탈퇴된노드위치$\rangle$를 전송한다. 코어 망은 브로드캐스트를 통해 그룹 구성원들에게 탈퇴 메시지를 보내고, 그룹 구성원들은 탈퇴한 MME의 비밀 값 $SECRET_{NODE_n}$을 추출한다. 이후, 그룹 구성원들은 (1)의 수식을 사용함으로써 기존 그룹 키 $GK$를 새로운 그룹 키 $GK'$로 갱신한다. 추가적으로 새로운 MME는 (2)의 수식을 사용함으로써 그룹 구성원들과 세션 키 $SK$를 동의한다.

### 5.5 그룹 리더 재 선출 단계

그룹 리더와 후보 그룹 리더간에는 주기적으로 컨트롤 신호를 통해 서로의 상태를 확인한다. 이를 통해, 후보 그룹 리더는 현재 그룹을 대표하는 그룹 리더의 정상 동작 여부를 판별할 수 있다. 하지만 그룹리더에게 다음과 같은 문제가 발생하게 되면 정상 동작을 할 수 없고, 그 결과 그룹 리더의 권한이 상실된다.

(1) 패킷 손실, 채널 간섭과 같은 네트워크 문제
(2) MTC 단말의 오류 발생과 같은 시스템 장애 문제
(3) 악의적 목적의 전원 종료, UICC의 불법적인 변경과 같은 공격자에 의한 물리적 공격 문제

그룹 리더의 권한 상실로 인해 후보 그룹 리더들 중에 그룹을 대표할 수 있는 그룹 리더를 재 선출한다. 재 선출 과정은 5장의 5.1절에서 설명했듯이 각 후보 그룹 리더는 해쉬함수를 통해 해쉬값을 생성하고, 다른 후보 그룹 리더들과의 해쉬값을 공유한다. 공유된 해쉬값들과 자신의 해쉬값을 비교하여 가장 높은 해쉬값을 생성한 후보 그룹 리더는 LTE-Advanced 망과의 인증을 거치게 된다. 이후, 성공적으로 인증을 완료하게 되면 새로운 그룹 리더로 재 선출된다.

## VI. 제안 프로토콜 분석

본 장에서는 보안성 분석 뿐만 아니라 인증 과정에서 메시지를 전달할 때의 통신 비용(cost)과 변수를 생성하고 암호적 연산을 수행할 때의 연산 오버헤드(overhead)와 관련하여 제안한 프로토콜의 성능(performance)을 분석한다.

### 6.1 보안성 분석(security analysis)

#### 6.1.1 상호 인증과 키 동의

그룹 리더와 HSS는 3-way 질의-응답 핸드쉐이크(handshake)를 이용하여 상호 인증을 함으로써 서로 간에 정상적인 개체(entity)임을 확신할 수 있다. 임시적 그룹 식별자 $TID$는 공개적으로 전송되지 않기 때문에 공격자가 $TID$를 알 수 없다. 추가적으로 $TID$는 그룹 식별자 $IMGI$와 그룹 키 $GK$를 이용하여 생성되는데 $IMGI$와 $GK$는 MTC 단말들이 LTE-Advanced 서비스에 가입하면서 UICC내에 저장되기 때문에 그룹 구성원과 HSS를 제외한 공격자는 알아낼 수 없다. 따라서, HSS는 〔그림 3〕의 M.3 메시지를 받은 후에 $TID^{**} ? = TID^{*}$를 확인함으로써 그룹 리더를 인증할 수 있다. 그룹 리더는 〔그림 3〕의 M.5 메시지를 받은 후에 $Hs ? = Hs^{*}$를 확인함으로써 HSS를 인증하게 된다. 그룹 구성원들도 $TID$를 통해 $Hs$를

〔표 1〕 제안한 프로토콜과 EPS-AKA에서 사용하는 변수들의 비트수

| 프로토콜 | 변수 | 비트수 |
|---|---|---|
| 제안한 프로토콜 | $SN-ID, Result$ | 48 |
| | $IMSI, IMGI$ | 128 |
| | $ECC\,group, RAND, ENC, GK, SECRET_{NODE_n}$ | 256 |
| EPS-AKA | $KSI_{ASME}$ | 32 |
| | $AK, SQN, SN-ID$ | 48 |
| | $MAC$ | 64 |
| | $K, RAND, CK, IK, AUTH, IMSI, RES, XRES$ | 128 |
| | $K_{ASME}$ | 256 |

〔표 2〕 제안한 상호 인증 프로토콜과 EPS-AKA와의 통신 비용 비교

| | 제안한 프로토콜 | EPS-AKA |
|---|---|---|
| M.1 | 512 | 0 |
| M.2 | 640 | 128 |
| M.3 | 944 | 304 |
| M.4 | 768 | 640 |
| M.5 | 1024 | 384 |
| M.6 | 512 | 128 |
| M.7 | 48 | - |
| 총 비트수 | 4448 | 1584 |

생성할 수 있기 때문에 HSS를 인증할 수 있다.

인증이 성공적으로 완료되면 MME는 그룹 구성원으로 포함된다. 그룹 구성원들과 MME는 어떠한 시그널링 없이 제한된 비밀 값 $RS$를 통해 세션 키를 동의할 수 있기 때문에 세션 키 동의는 도청과 같은 공격에 안전적으로 실행된다.

#### 6.1.2 재사용 공격(replay attack)

MTC 단말들과 MME사이는 무선구간이기 때문에 불안전한 링크로 연결된다. 따라서, 공격자는 〔그림 3〕의 M.2, M.3 그리고 M.6 메시지를 도청할 수 있다. 공격자가 〔그림 3〕의 오래된 M.2를 재사용한다고 가정하자. 만약 새로운 그룹 키 $GK'$로 갱신된 후에 재사용 되었다면, HSS는 $GK'$ 때문에 새로운 임시적 그룹 식별자 $TID$를 추출한다. 따라서, 오래된 메시지 M.2에서 추출한 $TID$와 새롭게 생성된 $TID$가 다르기 때문에 재사용 공격은 실패하게 된다.

한편, $GK'$로 갱신되기 전에 재사용 되었다면 오래된 메시지 M.2에서 추출한 $TID$와 HSS가 생성한 $TID$가 같기 때문에 HSS는 공격자를 정상적인 사용자로 인증하게 된다. 하지만, MME에 의해 새로운 $R_{MME'}$가 생성되기 때문에 오래된 메시지 M.6에 포함된 $Hu^*$와 새롭게 생성된 $Hu$가 다르다. 따라서, MME는 공격자가 보내는 오래된 메시지 M.6을 잘못된 메시지로 판단한다. 그러므로 제안한 프로토콜은 재사용 공격에 대해 안전하다.

#### 6.1.3 알려진 세션 관련 공격

그룹 리더와 MME는 각자 임시적 세션 키 $TSK$를 생성한다. 인증이 완료되면, 그룹 리더와 MME간의 메시지는 $TSK$에 의해 보호된 안전한 채널상에서 전달된다. 그룹 리더가 생성한 임의의 값 $RAND_{UE}$와 MME가 생성한 임의의 값 $RAND_{MME}$는 공개되지 않기 때문에 공격자는 $TSK$를 생성할 수 없다. 만약 $RAND_{UE}$를 그룹 구성원들도 알게 되면, 그룹 리더가 MME에게 보내는 제한된 비밀 값 $RS$를 도청할 수 있기 때문에 이진트리내 근원 노드와 자신이 위치한 자식노드 경로 사이의 모든 비밀 값 $SECRET_{NODE_n}$을 알게 되는 문제가 생긴다.

〔표 3〕 제안한 키 관리 프로토콜과 EPS-AKA의 세션 키 동의 과정의 복잡성 비교

| | 제안한 프로토콜 | EPS-AKA |
|---|---|---|
| MTC 단말들 | $O(1)$ | $O(n)$ |
| MME | | |

#### 6.1.4 전방향 보안 및 후방향 보안(forward secrecy and backward secrecy)

키 관리 프로토콜에서 제한된 비밀 값 $RS$를 통해 얻을 수 있는 비밀 값 $SECRET_{NODE_n}$을 XOR과 해쉬 함수 연산을 통해 전방향 보안 및 후방향 보안을 보장할 수 있다. 기존 노드가 그룹 구성원에서 탈퇴되었다고 가정하자. 모든 그룹 구성원들은 기존 그룹 키 $GK$를 새로운 그룹 키 $GK'$로 갱신한다. 이때, XOR된 값에 해쉬함수를 사용했기 때문에 탈퇴되는 노드는 새로운 그룹 키 $GK'$를 알지 못한다. 따라서, 탈퇴된 그룹 구성원에 대해서 후방향 보안이 보장된다.

한편, 새로운 그룹 구성원으로 가입되는 노드에 대한 절차는 기존 그룹 구성원들이 새로운 그룹 키 $GK'$로 갱신된 이후에 진행된다. 가입되는 노드는 이미 새로운 그룹 키 $GK'$가 UICC내에 저장되고 이후, 이진트리로 추가되기 때문에 이전의 그룹 키 $GK$를 알 수 없다. 따라서, 가입하는 그룹 구성원에 대해 전방향 보안이 보장된다.

### 6.2 성능 분석(performance analysis)

#### 6.2.1 통신 비용(communication cost)

〔표 1〕은 제안한 프로토콜과 EPS-AKA에서 사용되는 변수들의 비트수를 보여준다. 제안한 상호 인증 프로토콜은 256 비트의 타원곡선 변수들로 구성되고, EPS-AKA에서 사용되었던 기존 변수들은 〔15〕의 기준에 따른다. 제안한 프로토콜과 EPS-AKA에서 분석된 통신 비용을 각 메시지마다 열거하여 〔표 2〕에

〔표 4〕 제안한 프로토콜과 EPS-AKA의 암호적 연산과 〔표 2〕를 참고하여 측정한 연산 오버헤드의 총합

| 프로토콜 | | 암호적 연산 | 연산 오버헤드 총합 |
|---|---|---|---|
| 제안한 프로토콜 | 시스템 초기화 단계 | 1ECSM | 1020.121 μs |
| | 상호 인증 단계 | 6ECSM+5ECA/ECS+8H+2E+2D | 6844.587 μs |
| | 그룹 키 갱신 단계 | 1H+1X | 20.737 μs |
| EPS-AKA | | 12H | 241.680 μs |

ECSM(elliptic curve point scalar multiplication): 타원곡선 스칼라 곱, ECA/ECS(elliptic curve point additive/subtraction): 타원곡선 덧셈/곱셈, H(hash function): 해쉬함수, E(encryption): 암호화, D(decryption): 복호화, X(XOR operation): XOR 연산

〔표 5〕 암호적 연산의 경과 시간

| 암호적 연산 | 평균 시간 (μs) | 중간 시간 (μs) | 최대, 최소 시간의 차 (μs) |
|---|---|---|---|
| 타원곡선 스칼라 곱 | 1020.121 | 1020.201 | 0.910 |
| 타원곡선 덧셈/곱셈 | 2.521 | 2.563 | 0.310 |
| 해쉬함수(HMAC-SHA-256) | 20.140 | 20.187 | 0.616 |
| 암호화(AES-256) | 156.448 | 156.442 | 1.002 |
| 복호화(AES-256) | 118.620 | 118.607 | 0.716 |
| XOR 연산 | 0.597 | 0.595 | 0.002 |

구성하였고, 각각 4448 비트와 1584 비트의 통신 비용이 나온다. MTC 단말 1대를 인증할 경우 제안한 프로토콜의 통신 비용은 EPS-AKA보다 높다. 하지만, $n$대의 MTC 단말들을 고려해보자. EPS-AKA의 경우 $1584n$ 비트의 통신 비용이 걸리지만 제안한 프로토콜은 그룹 리더와 구성원들이 신뢰 관계에 있기 때문에 그룹 리더를 제외한 다른 구성원들의 인증을 위한 통신 비용은 0이 된다. 〔표 3〕은 MTC 단말들과 MME간 세션 키 동의 과정의 복잡성(complexity)을 보여준다. EPS-AKA의 경우 $n$대의 MTC 단말들이 존재하면 $n$번의 세션 키 동의 과정을 거치기 때문에 $O(n)$의 복잡성이 나온다. 하지만, 제안한 프로토콜은 그룹 리더와 MME 사이에서의 메시지 전달외에는 그룹 구성원들이 전송하는 메시지가 없기 때문에 $O(1)$의 복잡성이 나온다.

#### 6.2.2 연산 오버헤드(computation overhead)

인증 프로토콜은 크기가 256 비트인 다음과 같은 소수 $p$를 기반으로 타원곡선이 생성된다.

$$p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1 \quad (3)$$

타원곡선군을 생성하는 방정식은 다음과 같다.

$$y^2 = x^3 - 3x + b \quad (4)$$

〔표 4〕는 제안한 프로토콜의 암호적 연산을 보여주고, 〔표 5〕는 〔표 4〕에서 정의된 암호적 연산의 경과 시간을 측정하여 보여준다. 암호적 연산의 경과 시간은 Intel Core Duo 1.86GHz와 2GB의 랜덤 액세스 메모리(random-access memory)안에 설치된 Ubuntu 11.10에 의해 측정되었다. 또한, JavaTM 3.0.4 SDK, Classic Edition을 사용한 Java Card 에뮬레이터(emulator)〔16〕상에서 수행되었다. 추가적으로 〔표 4〕에서는 〔표 5〕를 참고하여 연산 오버헤드의 총합을 보여준다. 〔표 4〕에서 보듯이 시스템 초기화, 상호 인증 그리고 가입 및 탈퇴 노드를 위한 그룹 키 갱신 단계의 연산 오버헤드는 각각 1020,121, 6844.587 그리고 20.737 μs가 된다. 제안한 프로토콜의 연산 오버헤드는 EPS-AKA의 연산 오버헤드보다 상당히 높다. 하지만, 다수의 단말들이 존재하는 MTC 환경 (예, 환자들의 몸에 센서들을 부착하여 지속적으로 상태를 확인할 수 있는 헬스케어 분야)을 고려해보자. 바디센서 50개를 하나의 그룹으로 간주했을 때, EPS-AKA의 연산 오버헤드는 50개 단말 전체에 대해 연산을 수행하므로 12084 μs가 되는 반면 제안한 프로토콜은 그룹 리더의 단말에 대해서만 연산을 수행하면 되므로 6844.587 μs의 연산 오버헤드가 나온다. 결국, 제안한 프로토콜은 EPS-AKA보다 적은 연산 오버헤드를 가지게 된다.

〔표 5〕는 〔표 4〕의 연산 오버헤드의 총합을 측정하기 위한 기준이 되는 암호적 연산을 6개로 분류하였고, 각 연산마다 100번씩 측정하여 결과를 산출하였다. 타원곡선 스칼라 곱(elliptic curve point scalar multiplication)과 타원곡선 덧셈/덧셈

(elliptic curve point additive/subtraction)에 소비되는 평균 경과 시간은 각각 1020.121와 2.521 μs이다. 한편, HMAC-SHA-256과 AES-256의 평균 경과 시간 20.140, 156.448(암호화 시간) 그리고 118.620(복호화 시간) μs가 된다. 추가적으로 XOR 연산은 0.597 μs의 평균 시간이 측정되었다.

## VII. 결론

3GPP의 궁극적인 목표는 4세대 모바일통신인 LTE-Advanced에서 MTC를 위해 최적화된 망을 구축하는 것이다. MTC에서 MTC 단말들의 인증을 위한 프로토콜로 EPS-AKA를 사용하기에는 상당한 복잡성을 요구하므로, 본 논문에서는 그룹 기반의 인증 프로토콜과 키 관리 프로토콜을 제안하였다. 제안한 프로토콜은 (1) 그룹 리더만이 인증만이 인증에 참여하고, MME와의 세션 키 동의에 관여하므로 복잡성을 $O(n)$에서 $O(1)$로 줄였고, (2) 그룹 키를 사용함으로써 효율적으로 그룹을 관리할 수 있다. 그러므로, 제안하는 프로토콜은 MTC 단말들을 그룹 기반으로 관리하고 그룹 구성원들 사이의 안전한 통신을 위한 효율적인 보안 프로토콜이다.

## 참고문헌


[1] S. Lien, K. Chen and Y. Lin, "Toward Ubiquitous Massive Accesses in 3GPP Machine-to-Machine Communications," IEEE Communications Magazine, vol. 49, no. 4, pp. 66-74, Apr. 2011.

[2] Third Generation Partnership Project; Technical Specification Group Services and System Aspects; "Study on Facilitating Machine to Machine Communications in 3GPP Systems (Release 8)," 3GPP TR 22.868 ver.8.0.0, May 2007.

[3] D. Niyato, L. Xiao and P. Wang, "Machine-to-Machine Communications for Home Energy Management System in Smart Grid," IEEE Communications Magazine, vol. 49, no. 4, pp. 53-59, Apr. 2011.

[4] G. Wu, S. Talwar, K. Johnsson, N. Himayat and K. D. Johnson, "M2M: From Mobile to Embedded Internet," IEEE Communications Magazine, vol. 49, no. 4, pp. 36-43, Apr. 2011.

[5] Z.Md. Fadlullah, M.M. Fouda, N. Kato, A. Takeuchi, N. lwasaki and Y. Nozaki, "Toward Intelligent Machine-to-Machine Communications in Smart Grid," IEEE Communications Magazine, vol. 49, no. 4, pp. 60-65, Apr. 2011.

[6] Third Generation Partnership Project; Technical Specification Group Services and System Aspects; "Service requirements for Machine-Type Communications (Release 11)," 3GPP TS 22.368 ver.11.5.0, June 2012.

[7] T. Taleb and A. Kunz, "Machine Type Communications in 3GPP Networks: Potential, Challenges, and Solutions," IEEE Communications Magazine, vol. 50, no. 3, pp. 178-184, Mar. 2012.

[8] J. Kim and H. Choi, "An Efficient and Versatile Key Management Protocol for Secure Smart Grid Communications," Wireless Communications and Networking Conference(WCNC), pp. 1823-1828, Apr. 2012.

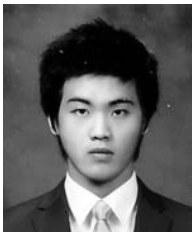
[9] N. Aboudagga, J. Quisquater and M. Eltoweissy, "Group Authentication Protocol for Mobile Networks," Wireless and Mobile Computing, Networking and Communications, 2007. WiMOB 2007. Third IEEE International Conference on, pp. 28-36, Oct. 2007.

[10] Y. Zhang, J. Chen, H. Li, W. Zhang, J. Cao and C. Lai, "Dynamic Group based Authentication Protocol for Machine Type Communications," Intelligent Networking and Collaborative Systems (INCoS), 2012 4th International Conference on, pp. 334-341, Sep. 2012.

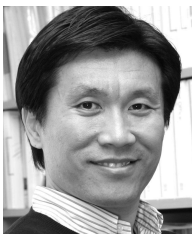
[11] H.H. Ngo, X. Wu, P.D. Le and B. Srinivasan, "An Individual and Group Authentication Model for Wireless Network Services," Journal of Convert-

gence Information Technology, vol. 5, no. 1, pp. 82-94, Feb. 2010.
〔12〕 Y. Chen, J. Wang, K. Chi and C. Tseng, "Group-Based Authentication and Key Agreement," Springer Wireless Personal Communications, vol. 62, no. 4, pp. 965-979, Feb. 2012.
〔13〕 Third Generation Partnership Project; Technical Specification Group Services and System Aspects; "System Improvements for Machine-Type Communications (Release 11)," 3GPP TR 23.888 ver.1.6.1, Feb. 2012.
〔14〕 Third Generation Partnership Project; Technical Specification Group Services and System Aspects; "Security aspects of Machine-Type Communications (Release 11)," 3GPP TR 33.868 ver.0.8.0, May 2012.
〔15〕 Third Generation Partnership Project; Technical Specification Group Services and System Aspects; "3GPP System Architecture Evolution (SAE); Security architecture (Release 11)," 3GPP TS 33.401 ver.11.5.0, Sep. 2012.
〔16〕 Sun Microsystems, Java Card 3,0,4 Platform, Sep. 2011. http://www.oracle.com/technetwork/java/javame/javacard/download/devkit/index.html

## 〈저자소개〉



최 대 성 (Dae-Sung Choi) 학생회원
2012년 2월: 광운대학교 컴퓨터공학과 학사졸업
2012년 3월~현재: 성균관대학교 IT융합학과 석사과정
〈관심분야〉 3GPP 이동통신 보안



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