LTE-Advanced에서 그룹 기반의 단말 간 직접 통신을 위한 키 관리 기법

최대성, 홍성대, 김승룡, 최형기
성균관대학교
e-mail:{dschoi, sdhong, srkim, hkchoi}@hit.skku.edu

Key Management for Group-based Device-to-Device Communications in LTE-Advanced

Dae-Sung Choi, Sung-Dae Hong, Seung-Ryong Kim, Hyoung-Kee Choi
Sungkyunkwan University

요 약

사람이 개입할 필요 없이 기기 및 사물들을 셀룰러 망으로 연결하여 언제 어디서나 다양한 서비스를 제공하는 MTC(Machine Type Communications)는 차세대 통신의 주요 이슈로 고려되고 있다. 하지만 MTC 환경은 다수의 단말들이 존재하기 때문에 LTE-Advanced 네트워크에 상당한 혼잡과 부하 문제를 줄 수 있다. 이 문제를 해결하기 위해 단말 간 직접 통신 기술이 등장하였다. 본 논문에서는 단말 간 직접 통신에서 eNB와의 통신을 줄이고, 그룹 간의 안전한 통신이 가능한 그룹 키 관리 기법을 제안하고, 이에 따른 연산 및 통신 오버헤드를 분석한다.

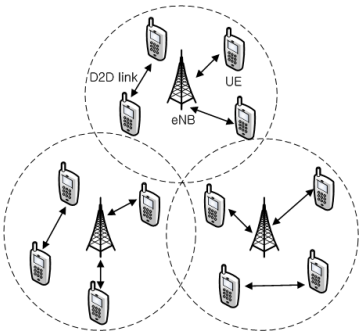
1. 서론

최근 들어 우리 주변의 모든 사물들을 네트워크로 연결함으로써 언제 어디서나 필요한 정보를 얻을 수 있고, 전달할 수 있는 M2M(Machine to Machine)이 통신 시장의 주요 이슈로 부각되고 있다. 이에 LTE-Advanced 네트워크를 사용하는 3GPP는 다수의 단말들이 인간의 개입 없이 서로간의 통신이 가능한 MTC(Machine Type Communications)를 정의하고 2008년부터 본격적인 표준화 작업을 진행하였다.

MTC 환경은 하나의 단말과 코어 망 사이에서의 트래픽을 처리할 수 있도록 최적화 되어 있는 H2H(Human to Human) 기반과 달리, 다수의 단말과 코어 망 사이에서의 트래픽을 감당해야 하므로 네트워크의 지연을 발생시킬 수 있다. 따라서, 이러한 문제를 해결하기 위한 기술로서, 기지국으로 전송되는 트래픽을 분산시킬 수 있는 인접 단말 간의 직접 통신이 등장하였다. 본 논문에서는 단말 간의 직접 통신에 대해 소개하고, 단말 간의 직접 통신 내에서 효율적으로 그룹을 관리할 수 있는 기법을 제안하고자 한다.

2. 관련 연구

Doppler 등은[1][2] 하나의 eNB 커버리지 내에서 인접하는 두 단말이 직접적으로 링크를 연결하여 eNB의 중계 없이 서로 간의 통신을 하는 것을 단말 간 직접 통신이라고 정의하였다. 이를 위해 단말 간에 하나의 eNB 커버리지 내에 존재하는 underlay 형태의 통신 링크를 연결함으로써 eNB와 동일한 주파수 자원을 이용하는 메커니즘을 제안하였다. 이와 비슷한 연구로 JANIS 등은[3] 셀룰러의 업 링크(uplink) 자원을 공유하는 단말 간의 통신을 위해 새로운 파워 제어 메커니즘을 제안하였다. Zulhasnine 등은[4] 단말 간의 통신 시 발생할 수 있는 간섭을 최소화할 수 있는 효율적인 자원 할당에 대한 방법을 제안하였다. 하지만 현재까지 단말 간의 직접 통신과 관련된 연구는 미비한 실정이고, 특히 표준에서의 단말 간 직접 통신은 필요성 및 가능성만 제기된 상태로서 활발한 연구는 이루어지지 않고 있다.

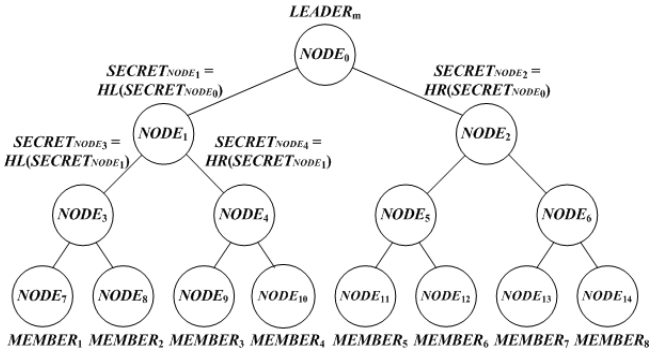


(그림 1) 단말 간 직접 통신의 예

3. 단말 간 직접 통신

초기에 단말들은 서로 간의 통신을 위해 eNB로 접속한다. eNB를 포함한 LTE-Advanced 네트워크에서는 단

말 간에 LTE 전용 주파수 대역을 사용하는 링크를 연결한다. (그림 1)에 간략한 단말 간 직접 통신의 예를 도시하였다. (그림 1)과 같이 eNB는 단말과 제어 신호를 지속적으로 주고 받으면서 통신에 대한 상태를 확인하고, 분석한 상태 정보를 기반으로 단말 간의 통신 상태를 제어한다. 하지만 underlay 형태의 통신 링크를 연결하기 때문에



(그림 2) 그룹 키 관리를 위한 이진트리 구성

다른 단말들과의 간섭이 발생할 수 있는 문제점이 존재한다. 따라서, 단말들 마다 발생시키는 시그널링의 최소화를 위한 단말들의 그룹화 방법은 주요 이슈 중에 하나이다. 한 예로 차량 통신(Vehicle Ad-hoc Network: VANET)에서 같은 지역 내에 속하는 차량들을 그룹 단위로 묶어 리더를 선정한 뒤, 리더만이 기지국에게 시그널링을 보내는 방식을 말할 수 있다. 본 연구에서는 LTE-Advanced 환경에서 단말들을 효율적으로 그룹화 할 수 있는 그룹 키 관리 기법에 대해 제안한다.

4. 제안기법

같은 eNB 커버리지 내에 위치하는 단말들은 하나의 그룹 단위로 묶을 수 있고, 그룹원들 간에만 안전한 통신을 위해 그룹 키 GK 를 가진다. 본 논문에서는 그룹원들 간에 이미 인증이 완료되었기 때문에 서로 신뢰관계에 있다고 가정하고, 그룹 키 관리 기법은 [5]에서 제안한 기법에 기초한다.

4.1 초기화 단계

LTE-Advanced 서비스 제공업자는 임의로 리더를 선정한다. 리더는 이미 인증을 성공적으로 완료했기 때문에 LTE-Advanced 코어 망과의 안전한 채널을 통해 통신할 수 있다. 코어 망은 안전한 채널을 통해 리더에게 현재 eNB 커버리지 내에 존재하는 단말들의 정보를 전달한다. 단말들의 정보를 받은 리더는 (그림 2)와 같이 자신을 제외한 단말들을 자식 노드로 관리하는 이진트리를 구성한다. 각 노드는 제한된 비밀 값 RS를 가지게 되는데, RS는 루트 노드에서 자신이 위치한 노드 사이의 경로에 위치한 비밀 값 $SECRET_{NODE_n}$을 제외한 모든 비밀 값들의 집합이다. 예를 들어, $MEMBER_8$의 RS값은 $SECRET_{NODE_1}$, $SECRET_{NODE_5}$, $SECRET_{NODE_{13}}$으로 구성된 집합이 되고. 2개의 해쉬 함수 $HL(\cdot)$, $HR(\cdot)$를 통해 자신의 경로를 제외한 모든 경로의 비밀 값들을 유도할 수 있다.

4.2 가입 단계

eNB가 자신의 커버리지 내에 새로운 단말을 감지하면 리더는 새로운 노드를 자식 노드로 가입시키기 위한 작업을 수행한다.

리더는 그룹 키 GK로 암호화된 가입 메시지 $< JOIN, MEMBER_n,$트리내의 위치$>$를 그룹 구성원들에게 보낸다. 그룹 구성원들은 메시지를 복호화 뒤, 2개의 해쉬 함수를 통해 가입되는 노드의 비밀 키를 알아낸다. 구성원들은 기존 그룹 키 GK를 새 그룹 키 GK'로 갱신하기 위해 다음과 같은 수식을 이용한다.

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

이후, 리더는 코어 망과의 안전한 채널을 통해 현재 갱신된 새 그룹 키를 알리고, 가입되는 노드는 코어망을 통해 새 그룹 키를 부여 받은 뒤, 리더에 의해 RS를 부여받고 그룹에 속하게 된다.

4.3 탈퇴 단계

eNB는 자신이 관리하고 있던 단말이 커버리지 내에서 감지하지 못한다면 리더는 그 단말을 탈퇴시키기 위한 작업을 수행한다.

리더는 그룹 키 GK로 암호화된 탈퇴 메시지 $< LEAVE, MEMBER_n,$트리내의 위치$>$를 그룹 구성원들에게 보낸다. 이후의 과정은 가입 단계의 과정과 동일하다.

5. 제안기법 분석

5.1 보안성 분석(security analysis)

본 장에서는 제안한 이진트리를 이용한 제한된 비밀 값RS를 통해 전방향 보안과 후방향 보안을 보장할 수 있다. 기존 노드가 그룹 구성원에서 탈퇴 되었다고 가정하자. 모든 그룹 구성원들은 기존 그룹 키 GK를 새 그룹 키 GK'로 갱신한다. 이때, 그룹 구성원들은 자신이 가지고 있는 RS의 값에서 탈퇴하는 노드의 비밀 키를 유도 후, XOR된 값에 해쉬함수를 사용하였기에 탈퇴 하는 노드는 새 그룹 키를 알지 못한다. 따라서, 후방향 보안이 보장된다.

추가적으로 새로운 노드가 그룹원으로 가입된다고 가정하자. 리더가 새로운 노드를 그룹원으로 가입시키기 전에 이미 그룹 내 모든 노드들의 그룹 키는 새 그룹 키로 갱신되었다. 이후, 새로운 노드는 새 그룹 키를 받기 때문에 전방향 보안이 보장된다.

5.2 성능 분석(performance analysis)

본 논문은 단말 간의 직접 통신을 위해 단말들을 그룹 단위로 관리하는 그룹 키를 제안하였다. 이를 통해 그룹 간에 안전한 통신이 가능함을 보였다. 따라서 우리는 그룹 키 생성에 필요한 연산 오버헤드를 먼저 측정하고, 기존 LTE-Advanced에서의 단말 간 직접 통신과 비교하여 통신 오버헤드를 분석하도록 한다.

본 논문에서는 Intel Core Duo 1.86GHz와 2GB의 랜덤 액세스 메모리(random-access memory) 안에 설치된 Ubuntu 11.10상의 Crypto++ 5.6.1 라이브러리[6]를 이용하여 AES-256(E), HMAC-SHA-256(H)의 연산 오버헤드를 측정하였다. XOR 연산은 충분히 작기 때문에 무시하도록 한다. 우리가 측정한 연산 오버헤드는 각각 0.118ms, 0.020ms이다. 우리가 제안한 그룹 키 생성 및 갱신에 필요한 연산 오버헤드는 2E+1H로 총 0.256ms가 소요된다. 통신 오버헤드의 경우 기존 단말 간 직접 통신은 단말들이 필요시 eNB와의 직접 통신을 진행하였다. 이로 인해 $O(n)$의 복잡성을 가진 통신 오버헤드가 발생한다. 하지만 제안하는 기법의 경우 각 단말은 리더와의 통신을 진행하기 때문에 eNB와의 직접 통신은 리더만이 진행한다. 따라서, 제안하는 기법은 $O(1)$의 복잡성을 가진 통신 오버헤드만 발생한다.

6. 결론

본 논문에서는 LTE-Advanced 상에서의 그룹 기반의 단말 간 직접 통신에 관한 그룹 키 관리 기법에 대해 제안하였다. 그룹 키를 사용함으로써 그룹 내의 단말들은 서로 간에 안전한 통신을 할 수 있고, eNB로의 시그널링은 리더만이 진행하기 때문에 시그널링으로 인한 혼잡 및 부하의 문제를 줄일 수 있다.

참고문헌

[1] K. Doppler and M. Xiao, “Innovative Concepts in Peer-to-Peer and Network Coding,” Celtic WINNER+, Deliverable 1.3, Jan. 2009.

[2] K. Doppler, *et al.*, “Device-to-Device Communication as an Underlay to LTE-Advanced Networks,” IEEE Commun. Mag., vol. 47, no. 12, Dec. 2009, pp. 42-49.

[3] P. JANIS, *et al.*, “Device-to-Device Communication Underlaying Cellular Communications Systems,” Int. J. Communications, Network and System Sciences, vol. 2, no. 3, June 2009, pp. 169-178.

[4] M. Zulhasnine, *et al.*, “Efficient Resource Allocation for Device-to-Device Communication Underlaying LTE Network,” IEEE WiMob, Oct. 2010, pp. 368-375.

[5] J. Kim and H. Choi, “An Efficient and Versatile Key Management Protocol for Secure Smart Grid Communications,” WCNC, Apr. 2012, pp. 1823-1828.

[6] Crypto++, http://www.cryptopp.com/