http://dx.doi.org/10.3745/KIPSTC.2011.18C.4.237

3GPP LTE/SAE 네트워크에서의 핸드오버 키 최적 갱신주기에 관한 연구

한 찬 규[†] · 최 형 기[††]

요 약

LTE/SAE는 공격자의 키 획득 및 공격에 노출된 네트워크를 방지하기 위해 핸드오버 키 관리기법을 정의하고 있다. 본 논문에서는, 핸드오버 키 관리 기법이 비동기화 공격에 의해 전방향안전성이 보장되지 못 함을 보인다. 비동기화 공격을 방지하기 위해, 주기적인 루트키 갱신이 요구된다. 이에 본 논문에서는 시그널링 부하와, 공격에 노출되는 패킷의 양을 최소화 하는 최적 루트키 갱신 주기를 도출하고자 한다.

키워드 : 3GPP, LTE 보안, 핸드오버 보안, 최적화

Optimal Handover Key Refresh Interval in 3GPP LTE/SAE Network

Chan-Kyu Han[†] · Hyoung-Kee Choi[††]

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 so-called de-synchronization attacks, which is jeopardizing the forward secrecy of handover key management. We place an emphasis on periodic root key update to minimize the effect of the de-synchronization attacks. An optimal value for the root key update interval is suggested in order to minimize signaling load and ensure security of user traffic.

Keywords : 3GPP, LTE Security, Handover Security, Optimization

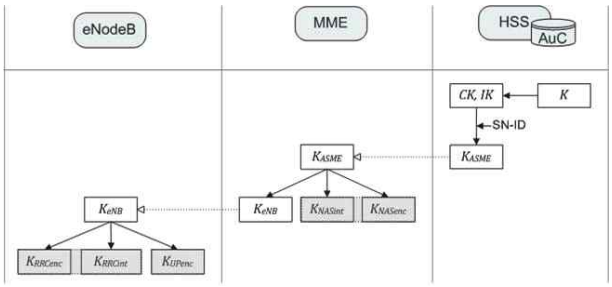
1. 서 론

Third Generation Partnership Project (3GPP) Long Term Evolution (LTE)/System Architecture Evolution (SAE)는 Evolved Packet System (EPS)에서 All-IP open-nature를 도입하고, 기존의 기지국 및 기지국 제어기를 evolved NodeB (eNodeB)로 통합하였다. 이러한 오픈된 환경에서는 악의적인 사용자들이 댁내기지국을 통해 위장기지국을 제작하거나, eNodeB를 손상시킬 가능성이 높아지고 있다. eNodeB에 관련된 공격을 방지하기 위해, EPS에서는 사용자가 eNodeB를 바꿀 때마다 무선구간 키를 갱신하는 핸드오버 키 관리기법을 정의하고 있다[1]. 핸드오버 키 관리기법에서는 특정 시점의 eNodeB가 이전 무선구간 키 또는 이후 무선구간 키를 획득할 수 없도록 후방향 및 전방향 안전성을 보장하고 있다. 본 논문에서는 EPS 핸드오버 키 관리기법의 취약점을 이용하여, 후방향 안전성을 보장하지 못 하게 하는 비동기화 공격을 제안한다. 비동기화 공격에서는 핸드오버 키 관리 동기계수의 비동기를 유도하여 이후 패킷에 대한 키를 획득할 수 있다. 비동기화 공격의 영향을 최소화하기 위해 루트키 갱신 주기를 최소치로 유지하면, 공격에 영향 받는 패킷의 양은 미미하다. 하지만 빈번한 루트키 갱신에 따른 코어네트워크에서의 시그널링의 부하가 증가하게 되므로, 이러한 상충관계를 조절하는 최적 키 갱신 주기가 요구된다. 본 논문에서는 시스템 관리자가 상황에 따라 유연하게 키 갱신 주기를 조절하는 알고리즘을 제안하고, 다양한 성능인자에 따른 결과를 시뮬레이션 및 수학적 모델을 통하여 분석하고자 한다.

※ 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No.2011-0005037).
† 준 회 원 : 성균관대학교 휴대폰학과 박사과정
†† 정 회 원 : 성균관대학교 정보통신공학부 부교수(교신저자)
논문접수 : 2011년 4월 28일
수 정 일 : 1차 2011년 6월 14일
심사완료 : 2011년 7월 1일

2. 관련 연구

Universal Mobile Telecommunications System (UMTS)에서는 우회공격을 통한 부당한 과금 및 보안세션 도청, 그



(그림 1) EPS 키 구조

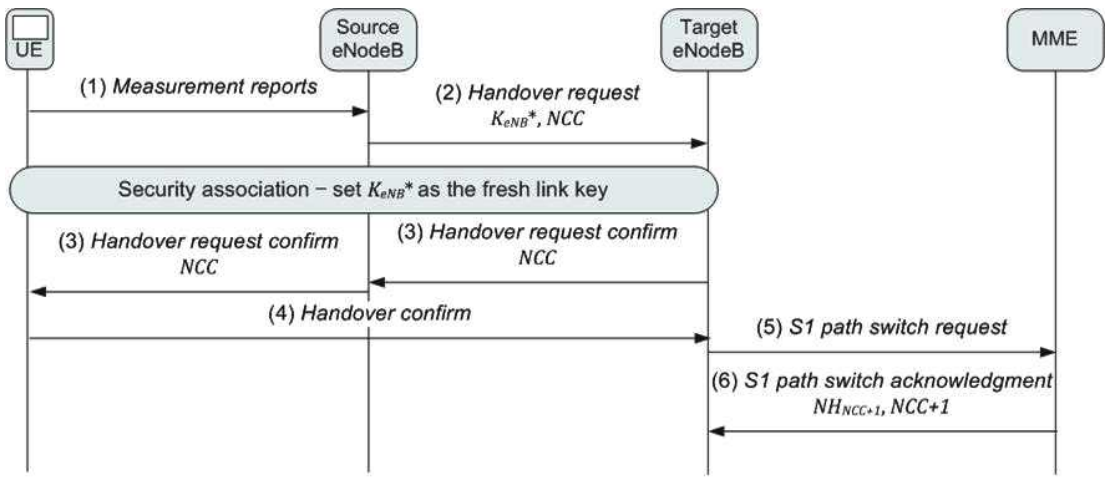
리고 인증벡터 재사용 공격이 연구되었다[2]. EPS에서의 위장기지국 공격은 아직 보고된 바가 없으나, 3GPP[3]에서 위장기지국 공격 가능성에 대하여 기술하고 있다. 해당 표준[3]에서는 악의적인 사용자들에 의해 제작된 기지국을 통해 사용자 추적, 사용자 데이터 도청 및 변조, 정상적인 기지국에 대한 물리적공격 (보안하드웨어 탈취 등) 및 서비스거부공격에 대한 가능성을 기술하고 있다. 이러한 공격을 막기 위해 안전한 핸드오버 키 관리기법을 대책으로 제시하고 있다. 핸드오버 키 관리에 관련된 조사연구[4]에서는 핸드오버 키 운영에 관한 정책을 기존 세션키 전달 방식과 비교하였다.

보안프로토콜의 핸드셰이크의 지연을 계산하여 보안프로토콜의 성능을 측정한 방법론이 제안되었다[5]. 해당 연구에서는 인증핸드셰이크를 구간별(무선 또는 유선)로 분리하여, 구간별 부하를 수학적으로 계산하여 보안프로토콜의 핸드셰이크를 비교하였다. UMTS 인증 및 키동의 과정을 확률모델로 표현한 연구결과 또한 발표되었다[6]. 이 연구결과는 포아송 분포를 따르는 인증 요청 랜덤 프로세스와, 지수 분포를 따르는 사용자 이동성 랜덤 프로세스를 이용하여 인증요청 회수를 최적화하여 시그널링 부하를 감소하는 알고리즘을 제안하였다. 이 연구[6]의 결과수식은 인증요청으로 인한 지연을 감소하기 위해, 사전에 인증요청을 미리 하는 기법[9]에 활용되어, 인증요청을 선처리 했을 때에 발생하는 시그널링 로드와 인증지연의 관계를 분석하였다. 인증파라미터를 네트워크에 저장하는 최적시간에 대한 연구[10]에서는 사용자 랜덤이동성모델을 이용하여, 사용자 핸드오버에 따른 인증지연과 네트워크에서의 저장공간소모 정도를 비교하였다. 네트워크 통계(가입자수, 셀넓이, 사용자 속도, 분포정도)를 이용한 UMTS의 분석결과[11]에서는 기존의 인증서버 방식의 기법을 지양하고, 단말에서 인증파라미터를 생성하는 방법을 제안하고 있다.

3. EPS 키 구조 및 핸드오버 키 관리 방법

(그림 1)은 EPS에서 정의된 계층적인 키 구조와 각 네트워크 노드 별로 유도되는 키를 도시한다. Home Subscriber Server / Authentication Center (HSS/AuC)에서는 인증 및 키동의 과정(EPS-AKA)의 결과로 사용자 비밀키(K)에 기반하여 암호화키(CK)와 무결성 검사 키 (IK)를 생성한다. UMTS에서는 {CK, IK}에 현재 단말 서비스 네트워크를 지정하지 않아서, 우회공격 취약점이 발견되었다[2]. 따라서 EPS에서는 서비스 네트워크의 식별자 (SN-ID)를 지정하는 중간레벨의 키인 K_{ASME}를 생성한다. K_{ASME}에 기반 하여 Mobile Management Entity (MME)는 Non-Access Stratum (NAS) 레벨 보안을 위한 K_{NASint}, K_{NASenc}를 생성하고, Access Stratum (AS) 레벨 보안을 위한 K_{eNB}를 생성하여 eNodeB에게 전달한다. K_{eNB}는 사용자평면 암호화를 위한 K_{UPenc}과 제어평면의 Radio Resource Control (RRC) 암호화 및 무결성을 위한 K_{RRCint}, K_{RRCenc}를 생성한다.

사용자가 eNodeB를 바꿀 때마다 핸드오버가 발생되는데, 이 때 K_{eNB}의 갱신이 요구된다. 1장에서 기술하였듯이 eNodeB는 공격자에 의해 노출될 위험이 크기 때문에, eNodeB 간에 키 갱신을 할 때 후방향 및 전방향 안정성 (backward 및 forward secrecy)을 지원해야 한다. (그림 2)는 핸드오버 시 eNodeB에서의 키 갱신 및 키 전달을 도시한 그림이다. 사용자 서비스를 K_{eNB}에 기반하여 지원하던 *이전* eNodeB (source eNodeB)는 새로운 키인 K_{eNB}^*를 계산하여, 동기계수인 Next-hop Chaining Counter (NCC)와 함



(그림 2) EPS 키 갱신 및 키 전달

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

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

께 사용자가 핸드오버 할 *다음* eNodeB (target eNodeB)로 전달한다. 이 때 새로운 키인 K_{eNB}^{*}는 식 (1) 또는 식 (2)을 통해 계산된다. 식 (1)은 수평 키 유도 (horizontal key derivation) 식 (2)는 수직 키 유도 (vertical key derivation) 과정이라 명명한다. Key Derivation Function (KDF)는 일방향 키 해쉬 함수를 의미한다.

수직 키 유도 과정에서 K_{eNB}^{*}는 NCC번째 Next Hop (NH) 키인 NH_{NCC}에서 유도되는데, NH 키는 이전 핸드오버에서 MME로부터 수신하였다고 가정한다. 메시지 (3)에서 보듯이, 다음 eNodeB는 NCC 값을 사용자에게 전달하고, 사용자는 NCC 값을 통해 핸드오버의 종류를 파악하여 (사용자가 보유하던 NCC값과 같으면 수평, 보유하던 NCC값보다 크면 수직 키 유도과정), 핸드오버 키 유도 과정을 진행한다. 메시지 (4)를 통해 핸드오버가 종료되고, 다음 eNodeB는 MME에게 핸드오버 종료를 메시지 (5)를 통해 보고한다. 이 때 MME는 다음 핸드오버를 위하여 NCC값을 1 증가시키고, {NCC+1, NH_{NCC+1}}를 다음 eNodeB에게 전달하여 이후 핸드오버에 사용하도록 한다. 만일 NCC 값이 현재 eNodeB에 저장된 NCC 값보다 적으면 수평 키 유도 과정을 진행하게 된다.

4. 공격자 모델 및 공격자 분석 모델

이 장에서는 NCC 값의 비동기화를 유도하여, 전방향 안전성을 보장하지 못 하게 하는 공격자 모델을 기술하고, 공격 효과를 수학적 모델을 도입하여 분석한다.

4.1 비동기화 공격 (Desynchronization attack)

공격 eNodeB는 이전 eNodeB를 위장하여 (그림 2) 메시지 (2)의 NCC 값을 허용최대치로 조정하여 다음 eNodeB에게 전송한다. 현재 정상 NCC 값을 α라 하고, 조작된 NCC 값을 β라 정의하자. 다음 eNodeB는 핸드오버의 결과로, MME로부터 $\alpha+1$을 전달받게 된다. 따라서 이 후 핸드오버 시에 $\alpha+1 \ll \beta$ 이기 때문에, 수평 키 유도 과정을 진행하게 된다. 이 경우 전방향 안전성을 보장하지 못 하기 때문에, 공격자는 지속적으로 사용자와 eNodeB 간 통신 키를 획득하게 된다. 다만, 비동기화 공격에서는 사용자를 지속적으로 추적하며, 정상 α값을 전송해야만, 사용자가 수직 키 유도 과정을 진행하는 것을 방지할 수 있다. 또한 공격자는 (그림 2)의 메시지 (6)을 변조하여 비동기화 공격을 유발할 수 있으나, MME와 eNodeB 간 통신은 IPSec에 의해 보호될 확률이 높다.

위의 공격을 방지하기 위해, 핸드오버 이전에 MME로부터 후방향 안전성을 보장받기 위한 값을 전달받는 암호학적인 보안대책을 고려할 수 있다. 하지만 3GPP 표준에서는 핸드오버 지연을 이유로 이를 지양하고 있다. 따라서 본 논문에서는 루트키(KASME)의 갱신을 통해 공격효과를 최소화 시키고자 하며, 갱신주기에 따른 파급효과를 분석하고자 한다.

4.2 공격자 분석 모델

〈표 1〉 공격자 분석 모델에 쓰이는 수식 설명

수식	설명
t_U	키 갱신 주기
t_R	MME 체류 주기
t_u	공격 발생 후 잔여 키 갱신 주기
t_r	공격 발생 후 잔여 MME 체류 주기
t_c	취약구간
$f_x(t)$	t_x에 대한 확률밀도함수 ($x \in \{U, R, u, r\}$)
$f_x^*(s)$	$f_x(t)$에 대한 라플라스 변환

<표 1>은 공격자 분석 모델에 쓰이는 수식을 요약한다. 공격 파급효과는 K_{ASME}가 K_{eNB}에 대한 안전성을 보장하기 때문에 K_{ASME}이 갱신되면 소멸된다. K_{ASME}은 수동 키 갱신 또는 MME 지역 이탈 시 EPS-AKA가 실행되면서 갱신될 수 있다. 따라서 공격이 임의의 시간에 발생한다고 했을 때, 공격 파급효과는 $min(t_u, t_r)$ [12]동안 지속된다. 공격에 취약한 구간(t_c)의 분포함수는 수식 (3)과 같이 계산된다. 수식 (3) $F_c(t)$의 양쪽을 미분하고, 라플라스 변환을 취하면 수식 (4)와 같이 확률밀도함수의 라플라스 변환인 $f_c^*(s)$을 계산할 수 있다.

본 논문에서는 키 갱신 주기(t_U)가 지수분포를 따른다고 가정하고, MME 체류 주기(t_R)는 감마분포를 따른다고 가정하였다. 단, 잔여 수명에서의 길이편향 효과[7]로 인해 잔여 키 갱신 주기(t_u)는 지수분포를 따르지만, 잔여 MME 체류 주기(t_r)은 감마분포를 따르지 않는다. 잔여 키 갱신 주기 및 잔여 MME 체류 주기의 확률분포의 라플라스 변환은 각각 식 (5), 식 (6)과 같이 계산된다. 단, MME 체류 주기(t_R)는 평균이 k/μ_r 이고, 분산이 k/μ_r^2 인 감마분포를 따른다고 가정한다. 또한 원래의 키 갱신 주기(t_U)는 평균이 μ_u인 지수분포를 따른다고 가정한다. 식 (5)에서 보듯이 잔여 키 갱신 주기는 원래의 키 갱신 주기와 같은 지수분포를 따른다.

식 (5), (6)를 식 (4)에 대입하여 확장할 수 있다. 본 논문에서는 공격에 취약한 구간(t_c) 동안에 영향 받는 패킷볼륨, $E[N]$을 식 (7)과 같이 계산한다. 또한 키 갱신에 따른 시그널링 부하, $E[S]$를 식 (7)과 같이 계산한다. 이 때 λ_p, ρ 는 각각 평균 RRC 및 user data 패킷 도착간격과 EPS-AKA 시에 소요되는 인증 시그널링이다.

$$F_c(t) \equiv \Pr(t_r \le t) + \Pr(t_u \le t) - \Pr(t_r \le t) \cdot \Pr(t_u \le t) \tag{3}$$

$$f_c^*(s) = \int_0^\infty f_r(t)\left[\int_t^{T_R} f_u(\tau)d\tau\right] \cdot e^{-st}dt + \int_0^\infty f_u(t)\left[\int_t^\infty f_r(\tau)d\tau\right] \cdot e^{-st}dt \tag{4}$$

$$f_u^*(s) = \frac{1 - f_U^*(s)}{s \cdot \int_0^\infty t \cdot f_U(t)dt} = \frac{\mu_u}{s + \mu_u} \tag{5}$$

$$f_r^*(s) = \frac{1 - f_R^*(s)}{s \cdot \int_0^\infty t \cdot f_R(t)dt} = \frac{\mu_r}{s \cdot k}\left\{1 - \left(\frac{\mu_r}{s + \mu_r}\right)^k\right\} \tag{6}$$

$$E[N] = \lambda_p \cdot -\frac{d}{ds} f_c^*(s)|_{s=0},\ E[S] = \frac{\rho}{-\frac{d}{ds} f_U^*(s) \cdot f_R^*(s)|_{s=0}} \tag{7}$$

4.3 키 갱신의 중요성

비동기화 공격 방지를 위해서는 수식 (1)과 (2)에서 K_{eNB}^*를 계산할 때 NCC값을 포함해야 하며, 이를 통해 사용자는 K_{eNB}^*가 비동기화 공격하에 있음을 탐지할 수 있다. 이는 비동기화 공격하에서는 사용자와 정상적인 eNodeB가 소유하는 NCC값이 다르다는 것에 착안한 것이다.

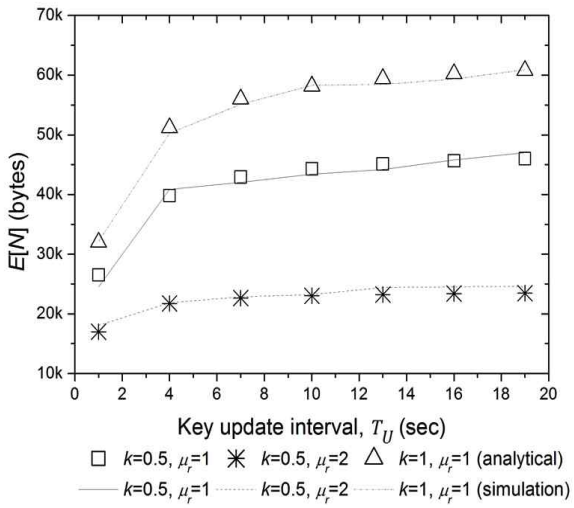
하지만 LTE 환경에서는 다양한 IP 기반 공격이 발생할 수 있고, 이를 사전에 예방하는 것은 현실적으로 난해하다. 따라서 발생 가능한 공격(사용자의 패킷변조와 관련)의 효과를 최소화하기 위해서는 루트키 갱신이 가장 현실적이다. 따라서 본 논문에서는 루트키 갱신의 중요성을 역설하고, 최적화된 갱신주기를 제안하고자 한다. 키 갱신주기는 보안을 최대한 보장하면서, 시그널링 부하를 최소화하는 효율적인 방향으로 결정된다.

5. 시뮬레이션 결과

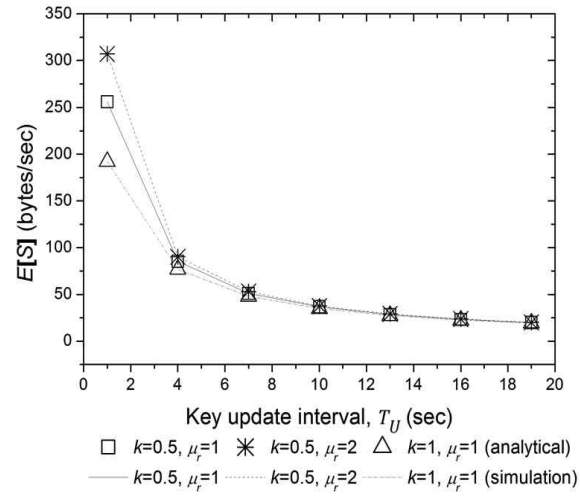
본 논문에서는 네트워크 시뮬레이터 (ns-2)에 EPS 보안 프로토콜을 구현하였다. KDF 함수로는 HMAC-SHA-256을 채택 하였으며, 키 및 시그널링 패킷의 기본 단위로는 256bit로 정의하였다.

5.1 키 갱신 주기에 따른 E[N]과 E[S] 분석

(그림 3)과 (그림 4)는 각각 키 갱신 주기에 따른 $E[N]$ 및 $E[S]$의 평균값을 도시한 그림이다 (단, t_U=1/T_U). 사용자는 Random waypoint 모델을 따르고, 이에 따른 MME 체류시간은 감마함수 임을 확인하였다. 키 갱신 시간 (T_U)가 증가함에 따라 공격에 노출되는 패킷볼륨은 증가하지만, 키 갱신에 따른 시그널링 부하는 감소한다. 또한 감마함수의 μ_r가 증가함에 따라, 사용자의 MME 체류시간이 감소하면서 공격에 노출되는 패킷볼륨은 감소하고, 키 갱신에 따른 시그널링 부하는 증가한다.



(그림 3) 키 갱신 주기에 따른 평균 노출 패킷 볼륨

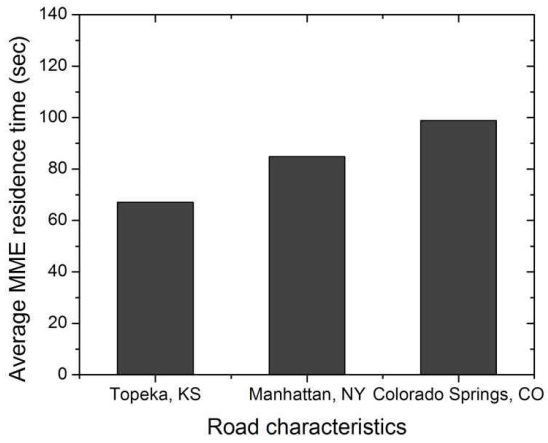


(그림 4) 키 갱신 주기에 따른 평균 시그널링 부하

5.2 키 갱신 주기 최적화 분석

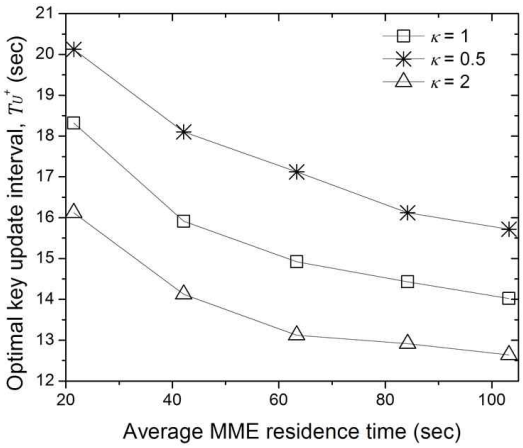
사용자의 MME 체류시간은 키 갱신 주기를 결정하는 중요한 지표이다. 실험결과 eNodeB 간 거리가 증가하고 사용자의 이동속도가 감소함에 따라, 사용자의 MME 체류시간은, 증가하였다. (그림 5)는 도로특성에 따른 평균 MME 체류시간을 도시한다. 본 논문에서는 TIGER[8]에서 제공하는 미국 전역의 도로정보를 ns-2에서 사용할 수 있도록 수정하였다. 이에 따른 결과로는 거주지역 (예. Colorado Spring, CO)의 경우 도로 및 이동특성 상 MME 체류시간이 가장 길었고, 전원지역 (예. Topeka, KS)의 경우 고속도로로 인하여 MME 체류시간이 가장 짧았다. MME 체류시간은 공격에 노출되는 패킷볼륨 ($E[N]$) 및 키 갱신을 위한 시그널링 부하 ($E[S]$)를 조정하여, 키 갱신 주기를 결정한다. 본 논문에서 제안하는 최적 키 갱신 주기 알고리즘의 의사코드는 다음과 같다.

(1) Initialize T_U=1
(2) while
(3) {
(4) do $T_U = T_U + 1$
(5) calculate $E[N]' = E[N]/\eta$
(6) calculate $E[S]' = E[S]/\delta$
(7) if($E[S]'/E[N]' \geq \kappa$)
(8) then return T_U
(9) }



(그림 5) 도로특성에 따른 평균 MME 체류시간

(그림 6)은 평균 MME 체류 시간에 따른 최적 키 갱신주기의 변화를 κ에 따라 나타낸 것이다. 평균 MME 체류 시간이 길어질 수록, 공격에 노출되는 시간이 길어지기 때문에 키 갱신을 자주 해야 할 필요성이 있다. κ은 시스템관리자가 해당 모바일네트워크의 $E[N]$을 감소하고자 함을 지칭한다. 따라서 κ가 증가할 수록, 최적 키 갱신주기는 감소하게 된다.본 논문에서는 정규화인자인 η 및 δ를 정의하고 있다. η 및 δ은 $E[N]$ 또는 $E[S]$의 상대적인 중요도를 결정할 수 있다. 따라서 본 논문에서 제안하는 알고리즘은 상황



(그림 6) MME 체류 시간에 따른 최적 키 갱신 주기의 변화 (η=10Kbytes δ=128bytes/sec)

(context)에 따라 시스템 관리자가 유연하게 최적 키 갱신주기를 조정할 수 있다.

6. 결 론

본 논문에서는 3GPP EPS 상에서의 핸드오버 키 관리에 관한 취약점을 발견하고, 공격 파급효과를 분석하였다. 공격 파급효과를 최소화하기 위한 루트키 갱신을 제안하였고, 루트키 갱신에 따라 공격에 노출되는 패킷볼륨과 키 갱신을 위한 시그널링 부하의 상충관계를 분석하였다.

참 고 문 헌

[1] 3GPP TS 33.401, "Security architecture," Dec., 2009.
[2] M. Zhang, *et al.*, "Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol," *IEEE Trans. Wireless Commun.*, Mar., 2005.
[3] 3GPP TR 33.821, "Rationale and track of security decisions in Long Term Evolved (LTE) RAN / 3GPP System Architecture Evolution (SAE)," Jun., 2009.
[4] D. Forsberg, "LTE Key Management Analysis with Session Keys Context," *ELSEVIER Comput. Commun.*, Oct., 2010.
[5] Y.-B. Lin, *et al.*, "One-pass GPRS and IMS Authentication Procedure for UMTS," *IEEE J. Sel. Areas Commun.*, Jun., 2005.
[6] Y.-B. Lin, *et al.*, "Reducing Authentication Signaling Traffic in Third-Generation Mobile Network," *IEEE Trans. Wireless Commun.*, May, 2003.
[7] 이호우, "대기행렬이론: 확률과정론적 분석", 시그마프레스 1996.
[8] U.S. Census Bureau TIGER. http://www.census.gov/geo/www/tiger/

[9] Y. Zhang *et al.*, "An Improvement for Authentication Protocol in Third-Generation Wireless Networks," *IEEE Trans. Wireless Commun*, Vol.5, No.9, Sep., 2006.
[10] L.-Y. Wu, *et al.*, "Authentication Vector Management for UMTS," *IEEE Trans. Wireless Commun.*, Vol.6, No.11, Nov., 2007.
[11] J.-A. Saraireh, *et al.*, "A New Authentication Protocol for UMTS Mobile Networks," *EURASIP Wireless Commun. and Networking.*, Oct., 2010.
[12] S. Pack, *et al.*, "Optimal Binding-Management-Key Refresh Interval in Mobile IPv6 Networks," *IEEE Transactions on Vehicular Technology*, Vol.58, No.7, Sep., 2009.

한 찬 규

e-mail : hedwig@ece.skku.ac.kr
2006년 성균관대학교 컴퓨터공학전공(학사)
2008년 성균관대학교 전자전기컴퓨터공학과 (석사)
현 재 성균관대학교 휴대폰학과 박사과정
관심분야 : 3GPP 이동통신 보안

최 형 기

e-mail : hkchoi@ece.skku.ac.kr
1992년 성균관대학교 전자공학과(학사)
1996년 Polytechnic University 전기전자 (석사)
2001년 Georgia Institute of Technology 전기전자(박사)
2001년~2004년 Lancope Inc. 연구원
현 재 성균관대학교 정보통신공학부 부교수, ACM Transactions on Internet Technology 편집위원(Associate Editor)
관심분야 : 네트워크보안, 트래픽모델링