정 보 보 호 학 회 지
제 30 권 제6호, 2020. 12

5G 보안에서의 허위 기지국 대응에 대한 주요 이슈 분석

박 훈 용*, 박 종 근**, 김 보 남*, 유 일 선*

요 약

2G에서부터 5G 이동 통신 시대까지 허위 기지국 공격의 위협은 이어져 왔다. 허위 기지국은 정상 기지국으로 위장하여 사용자의 정보를 수집하거나 서비스 거부 공격 등을 수행하는 기지국을 말한다. 바로 이전 세대인 LTE에서는 가짜 재난 문자, 멀웨어 전파, Device Bidding Down 공격 등의 사례가 발표 또는 보고되었다. 5G에서도 LTE의 공격 사례와 같은 공격들이 발생할 수 있어 이에 대한 보안 대책이 연구될 필요가 있다. 현재 3GPP TR 33.809 문서에서 5G에서의 허위 기지국 관련 주요 이슈와 솔루션들이 논의되고 있다. 본 논문에서는 TR 33.809 문서를 바탕으로 5G의 보안을 위한 허위 기지국 대응에 대한 주요 이슈들을 중심으로 분석한다.

Ⅰ. 서 론

2019년 4월, 국내에 5G 상용화 서비스가 시작되면서, 우리는 현재 5G 시대에 살고 있다. 5G 시대가 왔음에도 변하지 않은 것이 있다. 바로 허위 기지국을 이용한 공격 위협이다. 2G부터 3G, 4G를 거쳐 5G 시대에도 허위 기지국 공격으로부터의 위협은 존재한다[1].

허위 기지국은 이동 통신 네트워크의 정상 기지국으로 위장하여 사용자의 정보를 수집하거나 서비스 거부 공격을 수행하는 등 악의적인 행동을 하는 기지국을 말한다. 허위 기지국 공격은 RAN(Radio Access Network)를 통해 사용자에게 수동적으로 또는 능동적으로 공격하며 무선 액세스 네트워크의 보안 취약점과 UE(User Equipment)가 더 강한 무선 신호에 연결하려는 특성을 악용한다.

5G의 RRC(Radio Resource Control) 프로토콜을 다루는 3GPP TS 38.331에 따르면 일부 유니캐스트 메시지와, 브로드캐스트 메시지가 보호되지 않은 채로 전송되기 때문에 허위 기지국이 악용할 여지가 있어 대책에 대한 연구가 지속적으로 필요하다[2].

LTE에서는 다음과 같은 허위 기지국 공격 사례들이 존재한다.

- *가짜 재난 문자 공격*: 재난 문자 전송 표준 프로토콜은 신속히 내용을 전달하기 위해 브로드캐스트로 전송된다. 또한 인증 과정 없이 보내기 때문에 사용자는 조작된 재난 문자를 수신할 수밖에 없게 된다[3].
- *중간자 공격을 통한 멀웨어 전파*: 피싱 공격자들이 허위 기지국을 배포하여 이동통신사에서 보낸 것처럼 보이는 멀웨어 다운로드 링크가 포함된 SMS 메시지를 전송한 사례가 있음. 이 멀웨어는 안드로이드 SMS 앱을 자체 앱으로 교체하고 은행 토큰과 같은 SMS 기반의 2FA를 훔치고 피해자의 연락처를 통해 지인들에게 피싱 메시지를 보내어 2차 전파를 통해 멀웨어를 확산시킨다[4].
- *Device Bidding Down 공격*: 코어 네트워크는 UE가 연결하기 위해 등록할 때 UE의 무선 액세스 능력을 알기 위해 UE에게 UECapability를 요청한다. 허위 기지국은 중간자 공격을 통해 이를 가로채어 더 낮은 무선 액세스 능력으로 수정하여 정상 기지국으로 전달하여 UE는 자신이 받을 수 있는 서비스의 질보다 한참 떨어지게 받게 된다[5].

5G에서도 LTE의 공격 사례와 같은 공격들이 발생할 수 있어 3GPP TR 33.809에서 허위 기지국 대응에 대한 논의가 이루어지고 있다[6].

본 논문에서는 3GPP TR 33.809 문서에서 논의되고

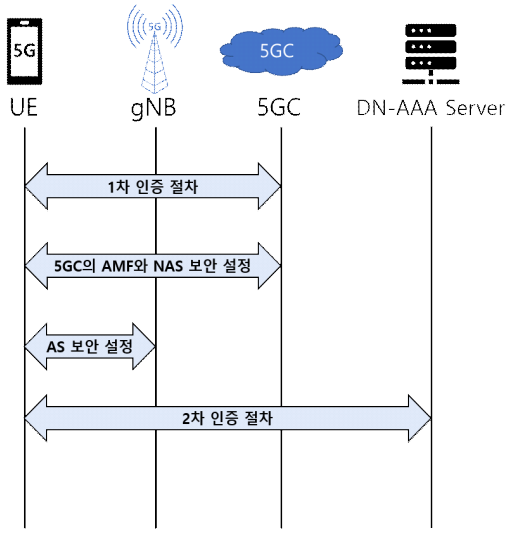
본 연구는 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2020-0-00952, 5G+ 서비스 안정성 보장을 위한 엣지 시큐리티 기술 개발)
* 순천향대학교 정보보호학과 (hoon456@sch.ac.kr, 대학원생, kimbona@sch.ac.kr, isyou@sch.ac.kr, 교수)
** 한국전자통신연구원 지능화융합연구소 정보보호연구본부 (책임연구원, queue@etri.re.kr)

있는 주요 이슈들을 분석하고 정리한다.

Ⅱ. 5G의 보안과 허위 기지국

[그림 1]과 같이 5G 보안의 가장 기본인 인증 및 키 교환은 5GC(5G Core) 네트워크에 대한 1차 인증과 응용 서비스에 대한 2차 인증 그리고 UE와 코어 네트워크의 AMF(Access and Mobility Management Function) 사이에서 교환 되는 메시지의 무결성 보호와 암호화를 위한 NAS(Non Access Stratum) 보안 설정과 UE와 gNB(Next Generation Node Base Station) 사이의 RRC 시그널링 메시지와 사용자 평면의 데이터의 무결성 보호와 암호화를 위한 AS(Access Stratum) 보안 설정으로 구성된다[7].

하지만 허위 기지국은 RRC 시그널링 메시지를 보호하기 위한 AS 보안 설정이 완료되기 전에 전송되는 일부 유니캐스트 메시지들, gNB에서 브로드캐스트 되는 시스템 정보와 같은 메시지 또는 보안 설정 이후에도 보호되지 않는 메시지들을 최대한 악용한다. 특히 브로드캐스트 메시지의 경우, 특성상 보안을 추가하는 경우, 기지국과 UE들에게 많은 연산 부담을 줄 수 있어 메시지들을 보호하는데 많은 어려움이 있다. 따라서 5G 보안을 위한 많은 노력에도 허위 기지국이 악용할 수 있는 취약점들이 존재한다.



〔그림 1〕 5G의 인증 및 키교환 구조

Ⅲ. 5G에서의 허위 기지국 대응 주요 이슈

이 장에서는 3GPP TR 33.809에서 논의되고 있는 주요 이슈들을 분석하고 정리한다. [표 1]은 3GPP TR 33.809에서 논의되는 주요 이슈들을 정리한 것이다.

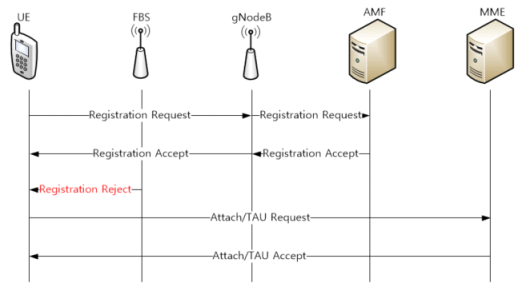
〔표 1〕 5G 허위 기지국 대응 주요 이슈 정리

번호	주요 이슈
1	보호되지 않는 유니캐스트 메시지의 보안
2	시스템 정보의 보안
3	네트워크의 허위 기지국 탐지
4	SON 오염 시도에 대한 보호
5	인증 릴레이 공격에 대한 대응
6	전파 교란에 대한 방어
7	허위 기지국의 중간자 공격에 대한 보호

3.1. 보호되지 않는 유니캐스트 메시지의 보안

첫 번째 이슈는 보호되지 않고 전송되는 Uplink와 Downlink Unicast 메시지에 대한 이슈이다.

RRC와 NAS 계층의 Reject 메시지는 암호화되지 않고 전송된다. UE가 RRC_INACTIVE 상태인 경우와 AS 보안 설정 후 보안 문맥(Context)을 유지하는 동안에도 RRC Reject 메시지는 보호되지 않는다. [그림 2와 같이 공격자는 NAS REJECT 메시지를 위조하여 CIoT(Cellular Internet of Things) UE에 전송하여 UE가 5GC에서 LTE 네트워크로 강제로 다운 그레이드 되도록 할 수 있다[8]. 이로 인해 SUPI(SUbscription Permanent Identifier) 보호, 초기 NAS 보호 등과 같은 5G 보안 강화 기능을 사용할 수 없어 UE의 프라이버시가 노출될 수 있다.

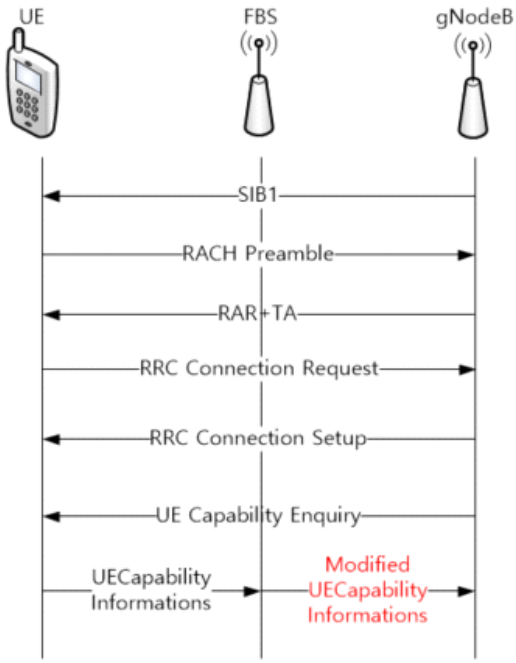


〔그림 2〕 5G에서 LTE로 다운그레이드 공격

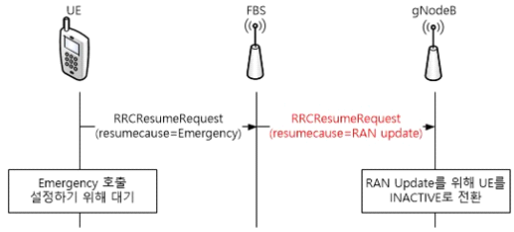
현재 3GPP Release 16에서는 AS 보안 설정을 위한 무선 액세스 기능 정보를 요청하기 위한 유니캐스트 메시지인 RRC UE Capability Enquiry 및 RRC UE Capability Informations 메시지를 AS 보안 활성화 전에 보호되지 않고 전송되도록 설계되었다. 따라서 [그림 3]과 같이 허위 기지국은 중간자 공격을 통해 무선 상에서 UECapabilityInformation을 캡처하고 이 메시지의 값을 더 낮은 무선 기능 수준으로 수정하고 이를 실제 gNB로 전달하여 UE가 제한된 무선 능력 수준으로만 작동하도록 하는 Device Bidding Down 공격을 할 수 있다.

RRCResumeRequest 메시지의 resumecause 필드는 재개 사유를 나타낸다. 이 필드는 메시지의 무결성 보호를 위한 ResumeMAC-I 값 연산을 위한 입력값에 포함되지 않아 허위 기지국에 의한 중간자 공격이 가능하다. [그림 4]처럼 공격자가 resumecause 필드를 “emergency”에서 “ran update”로 변조할 경우 UE가 Emergency 호출을 설정하기 위해 대기하는 동안 네트워크는 RAN Update를 위해 UE를 INACTIVE 상태로 전환하게 된다.

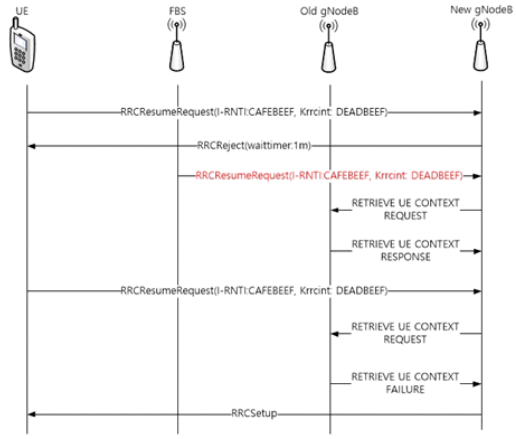
[그림 5]와 같이 UE가 RRC Resume 절차를 시작할 때 새로운 gNB에게 보내는 경우, UE는 이전에 AS보안 설정으로 생성한 KRRCint로 연산한 ResumeMAC-I와



〔그림 3〕 5G에서의 Device Bidding Down 공격



〔그림 4〕 resumecause 변조를 통한 중간자 공격



〔그림 5〕 RRCResumeRequest 메시지 재전송 공격

I-RNTI를 포함하는 RRCReusumeRequest 메시지를 새로운 gNB에게 전송한다. 새로운 gNB의 부하가 많은 경우, 일반적으로 wait timer와 함께 RRCReject 메시지를 전송한다. UE가 RRCReject 메시지를 수신하면 다시 INACTIVE 상태로 돌아가 wait timer가 만료된 후에 다시 시도한다. 이때, UE는 이전에 보낸 메시지와 동일한 I-RNTI와 KRRCint를 사용해야하므로 두 번째 RRCResumeRequest 메시지는 처음 보낸 메시지와 동일하다. 따라서 첫 번째 메시지를 포착할 수 있는 허위 기지국은 UE wait timer가 만료되기 전에 새 gNB로 메시지를 보낼 수 있으며, 이전 gNB는 ResumeMAC-I를 검증하여 유효한 것으로 판단하여 새로운 gNB에게 UE 문맥을 전송한다. UE가 다시 Resume 절차를 시도하면 새 gNB가 UE 문맥을 할당하지 못하므로 실패하게 되어 초기 RRC 설정 절차를 다시 진행하게 된다.

3.2. 시스템 정보의 보안

기지국은 주기적으로 동기화 신호와 시스템 정보를

셀 내에 브로드캐스트 한다. IDLE 또는 INACTIVE 상태인 UE는 셀의 시스템 정보를 모니터링하고 연결하기 적합한 셀을 선택한다. 시스템 정보에는 셀 (재)선택 매개 변수, 인접한 셀의 정보, 주파수 우선 순위, 블랙리스트 셀, 공통 채널 설정 정보, NAS 공통 정보 및 공공 경보 시스템 메시지와 같은 정보가 포함된다.

허위 기지국이 악성 시스템 정보 메시지를 브로드캐스트 하거나 다른 정상 기지국의 시스템 정보를 그대로 전송하는 것에 대해 새로운 보호 메커니즘을 도입할 수 있는지가 두 번째 이슈이다. 시스템 정보 메시지는 모든 UE에게 전송되는 브로드캐스트 메시지이기 때문에 무결성과 재전송에 대한 보호가 엄격히 적용될 필요는 없지만 보호된 시스템 메시지는 허위 기지국이 이후에 시스템 정보를 브로드캐스트 하는 것을 어렵게 만들 수 있다.

브로드캐스트 메시지에 보안을 추가하는 것은 앞서 서술한 것처럼 기지국과 UE에게 많은 연산 부담을 주게 되는 문제가 있어 새로운 보호 체계에 대한 연구가 필요하다.

3.3. 네트워크의 허위 기지국 탐지

3GPP 측정 절차는 주로 핸드오버와 SON(Self-Organizing Networks) 기능을 사용하기 위해 설계되었지만 보안 목적으로 허위 기지국 탐지에도 유용하게 활용할 수 있다[9]. UE가 네트워크로 보내는 측정 보고에는 주변 무선 환경 상태에 대한 다양한 정보가 포함된다.

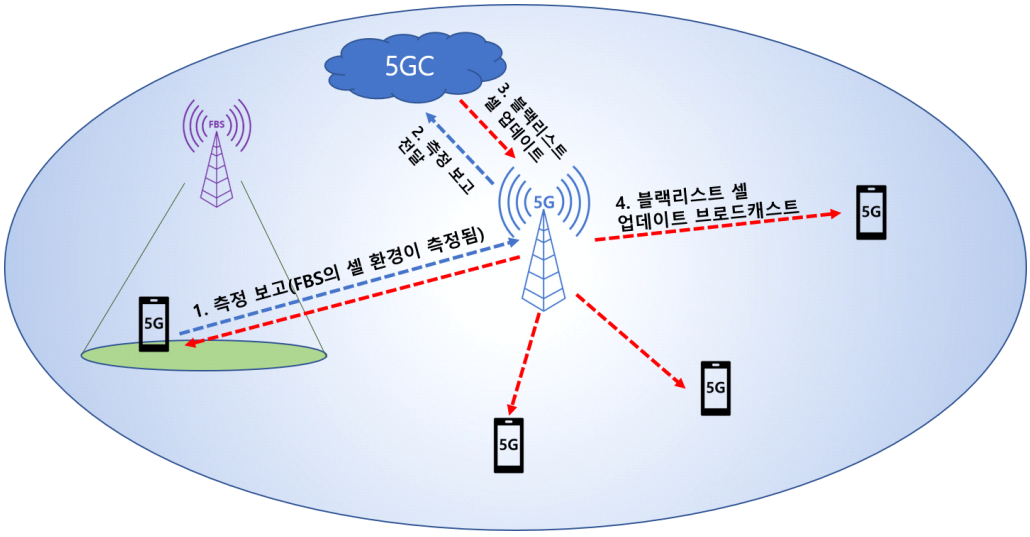
이 측정 보고에 더 유용한 정보를 추가하여 허위 기지국 탐지에 효과적으로 사용할 수 있다. 허위 기지국 탐지를 위해 어떤 정보들을 추가할지에 대한 연구 필요성을 제기한 것이 세 번째 이슈이다. [그림 6]처럼 특정 기지국이 허위로 판정되면 네트워크는 허위 기지국을 격리하기 위해 UE들에게 정보를 주어 연결을 방지할 수 있다.

3.4. SON 오염 시도에 대한 보호

3GPP에 의해 표준화된 SON의 기능은 다음과 같이 세 가지 범주에 속한다.

- 자가 구성/재구성
- 자가 최적화
- 자가 회복

SON 기능은 UE로부터 수신된 측정 보고를 바탕으로 처리를 한다. UE에서 모뎀, 베이스밴드와 같은 측정 보고를 다루는 부분은 일반적으로 멀웨어와 사용자 어플리케이션으로부터 보호되고 있기 때문에 UE에서 수신되는 측정 보고는 신뢰할 수 있고 손상되지 않았다고 간주된다. 하지만 UE는 보호되지 않은 상태로 전송되는 동기화 신호와 MIB(Master Information Block)을



〔그림 6〕 측정 보고를 통한 허위 기지국 탐지 및 차단

전달하는 SSB(Synchronization Signal Block)을 기반으로 인접한 셀의 신호 강도를 측정한다[10].

UE는 SSB 신호를 검증할 수 없기 때문에 허위 기지국에 의해 생성된 SSB를 기반으로 측정할 수 있다. 만약 허위 기지국 C가 정상 기지국 B로 위장하고 무선 환경을 구축한 다음 UE가 이 환경을 토대로 측정하여 서빙 기지국 A로 측정 보고를 하게 되면 A는 C의 무선 환경을 B에서 측정된 것으로 추정하게 된다. 추가적으로 공격자가 자체 구축한 SDR(Software Define Radio)를 사용하는 UE로 악의적으로 생성한 측정 보고를 기지국으로 전송할 수 있다.

허위 기지국은 인접한 정상 기지국들의 Cell ID를 수집하여 그 중 하나로 위장할 수 있다. UE는 기지국으로부터 오는 시스템 정보를 검증할 수 없기 때문에 UE는 기지국이 허위인지 아닌지 구별할 수 없다. 그 결과 UE는 허위 기지국으로부터 수신된 정보를 바탕으로 측정 보고를 수행하여 서빙 기지국으로 전송하게 된다.

앞선 사례들이 성공하더라도 매우 소규모이기에 영향이 적고 대규모로 공격하는 것은 상당힌 비용이 요구되기 때문에 비실용적이다. 중요한 것은 네트워크가 UE의 측정 보고를 맹목적으로 신뢰하는 경우에만 SON 오염 시도가 성공한다는 사실이다. 안전하게 구현된 SON은 측정 보고가 위조된 정보일 가능성을 고려하고 복원 기능을 가지고 있기 때문에 오염 시도가 완전히 영향이 없거나 거의 영향을 받지 않을 수 있다.

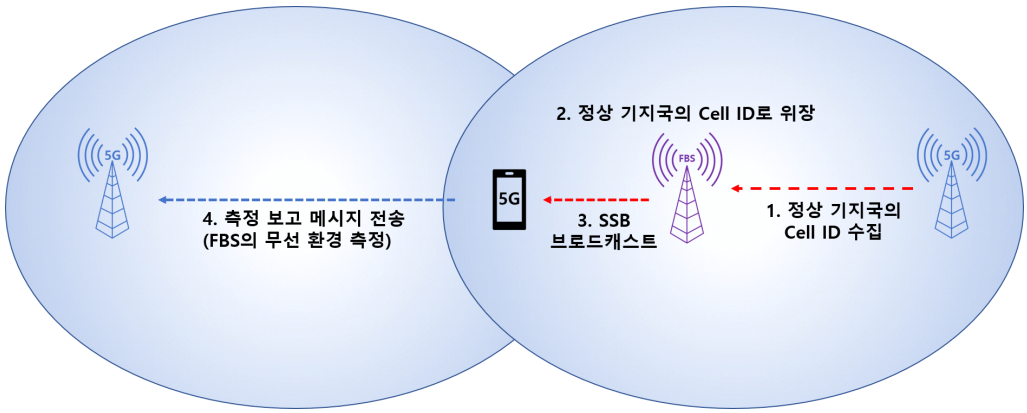
하지만, 부실하게 SON을 구현한다면 네트워크가 Signalling flood 상태가 되거나 셀이 중단되는 상황이 발생할 수 있다. 따라서 표준화된 솔루션을 명세하여 SON 구현을 개선하는데 도움이 되는 가이드라인에 대한 연구가 필요하다.

3.5. 인증 릴레이 공격에 대한 대응

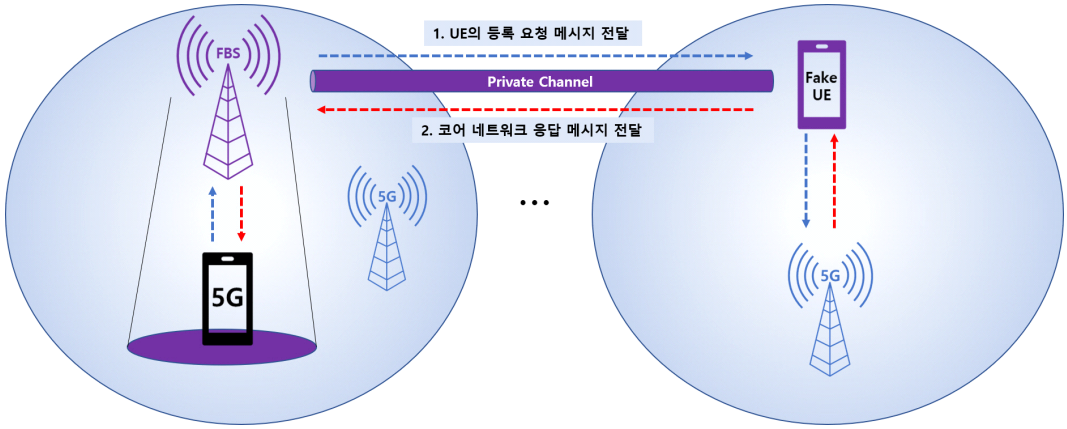
허위 기지국이 정상 기지국보다 더 강한 무선 신호를 보내게 되면 UE는 허위 기지국으로 연결될 수 있다. 그렇게 된다면 허위 기지국은 악성 UE와 사설 채널을 통해 통신하며 인증 릴레이 공격을 수행할 수 있게 된다. 허위 기지국과 악성 UE는 물리적으로 떨어져 있고, LAN 또는 WAN으로 연결되어 두 개의 PLMN(Public Land Mobile Network)를 통해 네트워크를 형성할 수 있다. 허위 기지국은 피해자 UE의 등록 요청 메시지를 악성 UE로 전달하고, 악성 UE는 이를 피해자 UE와 멀리 떨어진 정상 기지국을 통해 코어 네트워크로 전달한다. 다시 역순으로 허위 기지국과 악성 UE는 코어 네트워크가 보낸 응답 메시지를 피해자 UE에게 전달하여 인증을 완료한다. 이러한 방식으로 코어 네트워크가 인식하는 사용자의 위치와 실제 위치가 일치하지 않아 거짓 알리바이를 만들거나 허위 증거로 범죄 수사를 방해할 수 있다. 또한, 공격자가 정상 UE를 로밍 네트워크에 접속한 것처럼 조작하여 많은 과금을 유도할 수 있다. [그림 8]은 위 과정을 도식화 한 것이다.

인증 릴레이 공격을 통해 발생할 수 있는 위협에 아래의 사항들이 포함된다.

- 기만: 공격자는 피해자 UE 코어 네트워크에 연결되어 있다고 속인다.
- 위치 기록 오염: 악성 UE는 서로 다른 TA(Tracking Area)에서 이 공격을 지속적으로 수행하여 피해자 UE의 위치 기록을 오염시킬 수 있다. 결과적으로 한



〔그림 7〕 정상 기지국으로 위장한 허위 기지국의 무선 환경 측정 보고



〔그림 8〕 인증 릴레이 공격 절차

위치에 숨어있는 범죄자는 코어 네트워크를 속여 다른 위치에서 접속했다고 속일 수 있다.

- 서비스 거부 공격: 악성 UE와 허위 기지국은 피해자 UE의 전화/SMS/데이터 전송을 모두 또는 선택하여 거부할 수 있다.
- SON에 대한 공격: 물리적으로 멀리 떨어진 기지국을 중계함으로써 공격자는 UE가 잘못된 기지국 신호 강도 및 무선 환경 신호 강도 측정값을 허위 기지국에 보고하기 때문에 네트워크 SON 구성에 혼란을 줄 수 있다.

3.6. 전파 교란에 대한 방어

전파 교란(재밍)은 불법 무선 장치를 사용하여 정상 발신자와 수신자 간의 무선 통신을 방해하는 것이다. 5G 시스템에는 전파 교란 공격을 어렵게 만드는 빔 포밍과 같은 기능이 존재하고 전파 교란의 특성상 공격의 존재를 쉽게 인식할 수 있다. 게다가, 공격자가 공격을 정지하면 시스템이 자체 복구하므로 지속적인 공격 효과를 보기에도 많은 어려움이 있다.

그럼에도 불구하고, 3GPP가 무선 전파 교란에 대한 내성을 어떻게 향상시킬 수 있을지에 대한 연구는 지속적으로 필요하다는 것이 여섯 번째 이슈이다. 예를 들어 탐지 솔루션으로 공격자의 위치 같은 정보가 노출되는 경우, 탐지될 확률이 높을 때 공격자가 공격하는 것을 억제하는 효과가 있다. 이처럼 효과적으로 전파 교란 공격을 막는 것에 대한 연구가 필요하다.

3.7. 허위 기지국 중간자 공격에 대한 보호

전형적인 허위 기지국 공격은 UE에 대한 서비스 거부를 야기하지만 결과적으로 UE 또는 사용자는 서비스 이용이 불가하기 때문에 쉽게 공격을 유추하고 그에 맞는 조치를 취할 수 있다. 그러나 정교한 공격자는 허위 기지국을 사용하여 은밀하게 다양한 유형의 공격을 시도할 수 있다.

MitM(Man in the Middle) 허위 기지국은 UE와 네트워크 간의 메시지를 전달한다. 보안된 메시지는 그대로 전달하지만 사전 인증 트래픽, MAC/RLC 계층 메시지 헤더 등과 같이 보호되지 않은 메시지는 삭제, 변경 및 삽입할 수 있다.

일부 상황에서 MitM 공격은 주로 메시지를 재전송하여 수행된다. 이 경우 UE와 네트워크 중간에서 허위 기지국은 오랫동안 아무 작업도 하지 않거나 특정 상황에서만 메시지를 변조한다면 탐지하기가 매우 까다롭다. 따라서 MitM 공격에 대응하기 위한 기본적인 요구사항으로 재전송에 대한 보호가 있다.

허위 기지국이 무선 환경 구성과 관련하여 위장한 기지국을 얼마나 모방하는지는 알려지지 않았다. 개념 증명 수준으로 실제 네트워크에서 수행된 공격은 위장한 gNB를 모방하는 기능 포함하지 않고 진행되었다[11,12]. 그러나 공격자가 UE 및 네트워크가 허위 기지국을 탐지하기 위한 조치를 할 수 있다는 점을 고려한다면 실제 공격에서는 gNB를 모방하여 동작할 수 있을 것이다.

모든 트래픽을 변조하지 않고 단순히 전달만 하는 중

계기는 7번 이슈에서 허위 기지국으로 간주하지 않는다. 예를 들어, 전파 범위 확장기와 같은 장치에 대한 합법적인 사용은 공격으로 보지 않는다.

Ⅳ. 결 론

허위 기지국 공격은 이동 통신 네트워크가 오랫동안 발전하면서 함께한 위협이다. 이 위협들이 몇 세대에 거쳐 이어진 것은 보안 설정 전에 전송되는 메시지들을 변조하는 것으로 치명적인 피해를 끼치기 어려운 것과 시스템 정보 브로드캐스트 메시지 같이 가용성과 보안성의 트레이드오프로 보호할 수 없는 문제들이 있기 때문이다.

특히 재난 문자의 경우 사회 공학적으로 악용될 수 있기 때문에, 허위 기지국 공격을 이용한 가짜 재난 문자 공격 가능성이 LTE에서도 보고가 되고 5G 또한 공공 경보 시스템 메시지가 포함된 MIB가 보호되지 않아 이를 악용한 공격 가능성이 있기 때문에 5G에서는 이러한 문제들이 해결되어 이후의 이동 통신 세대에서는 발생하지 않도록 해야 한다.

본 논문에서는 3GPP TR 33.809의 주요 이슈들에 대해 논의된 솔루션은 다루지 않았지만 AS 보안 설정 이전에 교환되는 유니캐스트 메시지는 보안 설정 후에 다시 요청하여 대응하는 기법들이 제안되고 있다.

이처럼, 허위 기지국에 대한 공격이 가능한 취약점들을 해결 할 수 있는 보안 기술을 연구 및 개발하고 표준에 반영하는 것이 지속되어야 한다.

참 고 문 헌

[1] T. Wan, “False Base Station or IMSI Catcher: What You Need to Know”, CableLabs, Oct 2019.

[2] 3GPP, “NR; Radio Resource Control (RRC); Protocol specification”, 3GPP TS 38.331, Sep 2020.

[3] S. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, “LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE”, Network and Distributed System Security (NDSS) Symposium 2018, Feb 2018.

[4] Richard Chirgwin, “Fake mobile base stations spreading malware in China”, The Register, Mar 2017.

[5] A. Shaik, R. Borgaonkar, S. Park, J. Seifert, “New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities”, Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, pp. 221-231, May 2019.

[6] 3GPP, “Study on 5G Security Enhancement against False Base Stations”, 3GPP TR 33.809, Oct 2020.

[7] 3GPP, “Security architecture and procedures for 5G system”, 3GPP TS 33.501, Sep 2020.

[8] 3GPP, “Study on evolution of Cellular Internet of Things (CIoT) security for the 5G System”, 3GPP TR 33.861, Sep 2020.

[9] 3GPP, “Study on the Self-Organizing Networks (SON) for 5G networks”, 3GPP TR 28.861, Dec 2020.

[10] A. Shaik, R. Borgaonkar, S. Park, and J. Seifert. “On the Impact of Rogue Base Stations in 4G/LTE Self Organizing Networks”. *In Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec '18).* pp. 75-86, 2018.

[11] R. David, K. Katharina, H. Thorsten, and P. Christina. “IMP4GT: IMPersonation Attacks in 4G NeTworks”. https://imp4gt-attacks.net/media/imp4gt_camera_ready.pdf (2020)

[12] R. David, K. Katharina, H. Thorsten, and P. Christina, “Breaking LTE on Layer Two”. 1121-1136. Available online at https://alter-attack.net/media/breaking_lte_on_layer_two.pdf (2019)

〈저 자 소 개〉

박 훈 용 (Hoon Yong Park)

학생회원

2019년 2월 : 순천향대학교 정보보호학과 졸업

2019년 3월~현재 : 순천향대학교 정보보호학과 석·박사 통합 과정 중

<관심분야> 정보보호, 이동통신보안, 정형화 보안 검증

박 종 근 (Jong-Geun Park)

정회원

1997년 2월 : 성균관대학교 산업공학과 학사

1999년 2월 : 성균관대학교 산업공학과 석사

2013년 2월 : 충남대학교 컴퓨터공학과 박사

1999년 3월~2001년 4월 : 국방과학연구소 연구원

2001년 5월 ~ 현재 : 한국전자통신연구원 책임연구원

<관심분야> 이동통신보안, SDN/NFV, 클라우드보안

김 보 남 (Bo Nam Kim)

정회원

2003년 8월 : Auburn University Computer Science & Software Engineering 석사 졸업

2006년 8월 : Auburn University Computer Science & Software Engineering 박사 졸업

2020년 9월~현재 : 순천향대학교 정보보호학과 연구교수

<관심분야> 무선네트워크, IoT, 이동통신보안

유 일 선 (Ilsun You)

종신회원

2002년 2월 : 단국대학교 전산통계학과 박사 졸업

2005년 3월 ~2015년 8월 : 한국성서대학교 정보과학부 부교수

2015년 9월~현재 : 순천향대학교 정보보호학과 교수

<관심분야> 인증 및 접근통제, 이동통신보안, 인터넷 보안, 정형화 보안 검증