JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 26 No. 10, pp. 93-100, October 2021
https://doi.org/10.9708/jksci.2021.26.10.093

Analysis of Incarceration Attacks with RRCReject and RRCRelease in 5G Standalone Non-Public Network

Keewon Kim*, Jong-Geun Park**, Tae-Keun Park***

*Professor, Dept. of Computer Engineering, Mokpo National Maritime University, Mokpo, Korea
**Principal Researcher, Information Security Research Division, ETRI, Daejeon, Korea
***Professor, Dept. of Computer Engineering, Dankook University, Yongin, Korea

[Abstract]

In this paper, the possibility of a UE (User Equipment) incarceration attack using RRCRejecet and RRCRelease in 5G SNPN (Standalone Non-Public Network) is analyzed based on the 3GPP standard document. First, the cell selection and reselection procedures of the UE are analyzed, and then the processing process of the false base station and the UE before and after transmission of RRCReject and RRCRelease is analyzed. As a result of the analysis, it is possible that the false base station that transmits a strong signal causes the victim UE to establish an RRC connection to the false base station itself. In addition, if the false base station transmits an RRCReject message without integrity protection in response to the victim UE's attempt to establish an RRC connection, it is determined that the victim UE can continue to stay in the RRC connection attempt process. On the other hand, it is determined that it is impossible to incarcerate the victim UE by inducing an attempt to establish an RRC connection to another false base station using RRCRelease.

▸ **Key words**: 5G, Standalone Non-Public Network, RRC, 3GPP Standard, Incarceration Attack

[요 약]

본 논문에서는 5G SNPN (Standalone Non-Public Networ)에서 RRCRejecet와 RRCRelease를 이용한 UE (User Equipment) 감금 (Incarceration) 공격의 가능성을 3GPP 표준 문서를 기반으로 분석한다. 먼저 UE의 셀 선택과 재선택 절차를 분석하고, RRCReject와 RRCRelease의 전송 전/후의 허위 기지국과 UE의 처리 과정 분석한다. 분석 결과, 강한 신호를 송출하는 허위 기지국은 피해자 UE가 허위 기지국 자신에게 RRC 연결 설정을 하도록 하는 것이 가능하다. 또한, 피해자 UE의 RRC 연결 설정 시도에 대한 응답으로 허위 기지국은 무결성 보호가 되지 않는 RRCReject 메시지를 전송하면, 피해자 UE가 RRC 연결 시도 과정에 계속 머무르게 할 수 있을 것으로 판단된다. 반면, RRCRelease를 이용하여 다른 허위 기지국으로 RRC 연결 설정 시도를 유도함으로써 피해자 UE를 감금하는 것은 불가능한 것으로 판단된다.

▸ **주제어**: 5G, Standalone Non-Public Network, RRC, 3GPP 표준, 감금 공격

• First Author: Keewon Kim, Corresponding Author: Tae-Keun Park
*Keewon Kim (kwkim@mmu.ac.kr), Dept. of Computer Engineering, Mokpo National Maritime University
**Jong-Geun Park (queue@etri.re.kr), Information Security Research Division, ETRI
***Tae-Keun Park (tkpark@dankook.ac.kr), Dept. of Computer Engineering, Dankook University
• Received: 2021. 09. 29, Revised: 2021. 10. 14, Accepted: 2021. 10. 18.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

5G 이동통신 네트워크는 우리 삶의 거의 모든 것에 영향을 미치는 다양한 새로운 서비스 및 사용 사례를 가능하게 한다. 그러나 이러한 5G 이동통신 네트워크의 잠재력이 실현되기 위해서는 5G 이동통신 네트워크 지원 애플리케이션을 안전하게 제공해야 하며, 네트워크와 고객을 모두 보호하기 위해 다양한 보안 이슈는 처음부터 네트워크 기반에서 해결되어야 한다 [1]-[4].

5G 이동통신 네트워크에서의 안전한 응용을 위해서 다양한 보안 연구가 진행되었다 [3]-[9]. 등[8]은 5G 이동통신 네트워크의 RRC (Radio Resource Control)와 NAS (Non-Access Stratum) 계층의 프로토콜에 대한 정형적인 모델 (Formal Model)을 구성하여 5GReasoner라는 프레임워크를 제안하였다. 이를 이용한 보안 검증을 통해서 5G 이동통신 네트워크의 보안 설계 취약점을 도출하였다.

5G NPN (Non-Public Network)은 맞춤형 5G 이동통신 네트워크로서 공장이나 캠퍼스와 같은 특정 지역의 범위 내에서 특정 사용자에게 이동통신 서비스를 제공하기 위해 도입된다 [10,11]. 5G-ACIA (Alliance for Connected Industries and Automation)는 산업 도메인에 5G 이동통신 네트워크 적용하기 위해서 네 가지 5G NPN (Non-Public Network) 구축 모델을 제시하였다 [10]. 최근 Kim 등[9]은 Hussain 등[8]이 5GReasoner를 이용하여 발견한 “Cutting off the Device” 공격에 대해 3GPP 표준 문서를 기반으로 분석하여, 5G Standalone NPN 시스템이 3GPP 표준을 충실히 준수하여 구현된 경우 해당 공격이 불가능한 것을 보였다. 본 논문에서는 5G-ACIA가 제시한 네 가지 구축 모델 중 하나인 5G Standalone NPN의 환경에 초점을 맞추고 있다.

본 논문에서는 5G 이동통신 네트워크에서 Hussain 등[8]이 제안한 RRCReject와 RRCRelease를 사용한 UE 감금 (Incarceration) 공격의 가능 여부를 3GPP 표준 문서에 근거하여 분석한다.

II. Incarceration Attack with RRCReject and RRCRelease

본 장에서는 Hussain 등 [8]이 제안한 5G 이동통신 네트워크에서 RRCReject와 RRCRelease를 이용한 UE 감금 공격에 대하여 소개한다. 공격자가 이미 UE의 C-RNTI 또는 TMSI를 알고 있고, 두 개의 허위 기지국을 설정할 수 있다고 가정한다.

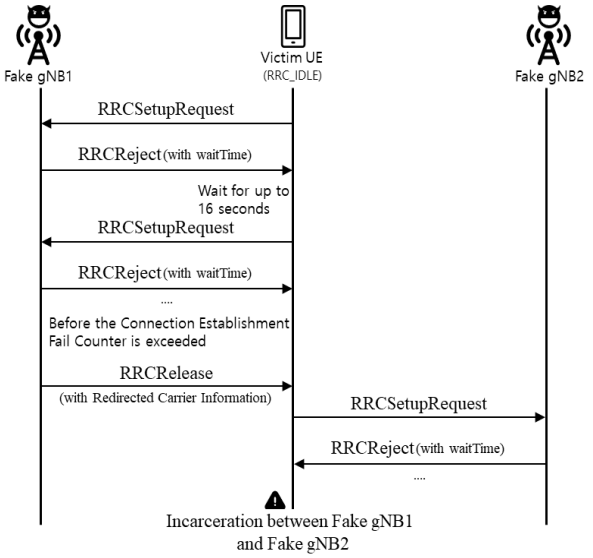


Fig. 1. Incarceration Attack with RRCReject and RRCRelease

공격 절차는 Fig. 1과 같으며 간략히 기술하면 다음과 같다. 먼저 허위 기지국 중 하나가 UE를 유인하여, UE가 RRCSetupRequest 메시지를 전송하도록 한다. 해당 허위 기지국은 이에 대한 응답으로 무결성 보호가 되지 않는 RRCReject 메시지를 전송한다. UE는 RRC_IDLE 상태에 있기 때문에, 허위 기지국이 전송한 무결성이 보호가 되지 않는 RRCReject 메시지를 수락한다. 만약 허위 기지국이 RRCReject 메시지에 이동성 백 오프 타이머 (Mobility Backoff Timer)를 설정하면, 사용자는 최대 16초 동안 RRC_IDLE 상태에서 대기한 후에 재연결을 시도한다. 그런 다음 허위 기지국은 RRCReject 메시지를 반복해서 전송함으로써 UE가 연결 설정 루프에 머물도록 강제할 수 있다. 그러나 UE는 동일한 셀에서 연결 설정 실패 카운터 (Connection Establishment Fail Counter)를 유지하고 있을 경우에, 해당 카운터가 한계에 도달하면 (예: 4회 시행) 셀 선택 기준을 변경한다. 카운터가 동일한 셀의 최대 제한에 도달하는 것을 방지하기 위해서, 허위 기지국은 RRCReject 메시지와 인터리빙하여 RRCRelease 메시지를 보낸다. 공격자는 RRCRelease 메시지안에 리다이렉트된 캐리어 정보 (Redirected Carrier Information)를 포함하여 사용자가 리다이렉트된 주파수 (Redirected Frequency)에서 작동하는 두 번째 허위 기지국과 연결하도록 유도한다. 허위 기지국을 한 번에 하나씩 켜고 끄면, 공격자는 가능한 한 오랫동안 UE를 연결 설정 루프에 감금할 수 있다.

III. Analysis of the Incarceration Attack with RRCReject and RRCRelease

이 장에서는, 5G SNPN 환경에서 Hussain 등 [8]이 제안한 RRCReject와 RRCRelease를 이용한 감금 공격의 실현 가능성을 3GPP 표준에 기반하여 분석한다.

1. Analysis of cell selection and reselection of UE

허위 기지국이 강한 신호를 사용하여 UE를 유인할 경우에 UE의 셀 선택 (Cell Selection)과 재선택 (Reselection) 절차를 분석한다.

3GPP TS 38.304 [12]에는 RRC_IDLE 모드와 RRC_INACTIVE의 상태인 UE의 필요한 절차들을 서술하고 있으며, Table 1에서 RRC_IDLE과 RRC_INACTIVE 상태에서 셀 선택과 재선택 과정이 기술되어 있다. UE AS (Access Stratum)의 셀 선택과 재선택만 발췌하여 정리하면 Table 1과 같다.

Table 1. Cell Selection and Reselection [12]

	Procedure
Cell Selection	· Perform measurements needed to support cell selection. · Detect and synchronise to a broadcast channel. Receive and handle broadcast information. Forward NAS system information to NAS. · Search for a suitable cell. The cells broadcast one or more 'PLMN identity' or 'SNPN identity' (for a UE operating in SNPN access mode) in the system information. Respond to NAS whether such cell is found or not. · If associated RATs is (are) set for the PLMN, perform the search in this (these) RAT(s) and other RATs for that PLMN as specified in TS 23.122. · If a cell is found which satisfies cell selection criteria, camp on that cell.
Cell Reselection	· Perform measurements needed to support cell reselection. · Detect and synchronise to a broadcast channel. Receive and handle broadcast information. Forward NAS system information to NAS. · Change cell if a more suitable cell is found.

본 논문은 5G SNPN (Standalone Non-Public Network)만을 고려하고 있으므로, 3GPP TS 38.304 [12]에서 “5.1.2 Support for SNPN selection”에 명시된 SNPN의 선택에 관한 절차를 요약 정리하면 아래와 같다.

1) UE는 사용 가능한 SNPN을 검색하기 위해, NR 대역의 모든 RF 채널을 스캔해야 한다.
2) UE는 가장 강한 신호 (RSRP, Reference Signal Received Power)를 가진 셀을 검색하고, 시스템 정보를 읽어야 한다.
3) UE가 가장 강력한 셀에서 하나 또는 여러 개의 SNPN identity를 읽을 수 있는 경우, 각각의 발견된 SNPN (TS 38.331 [13]의 SNPN 참조)을 NAS에 보고해야 한다.
4) SNPN 검색은 NAS의 요청에 따라 중지될 수 있다.
5) UE가 SNPN을 선택하면, 해당 SNPN의 적합한 셀을 선택하기 위해 셀 선택 절차가 수행되어야 한다.

UE는 3GPP TS 38.133 [14]에 명시된 셀선택 및 재선택을 위해 측정 (Measurement)을 수행해야 하며, 셀에 캠프했을 때 UE는 셀 재선택 기준에 따라 더 나은 셀을 정기적으로 검색해야 한다. 더 나은 셀이 발견되면 해당 셀이 선택되며, 셀 재선택을 위한 성능 요구 사항에 대한 자세한 내용은 TS 38.133 [14]에서 찾을 수 있다.

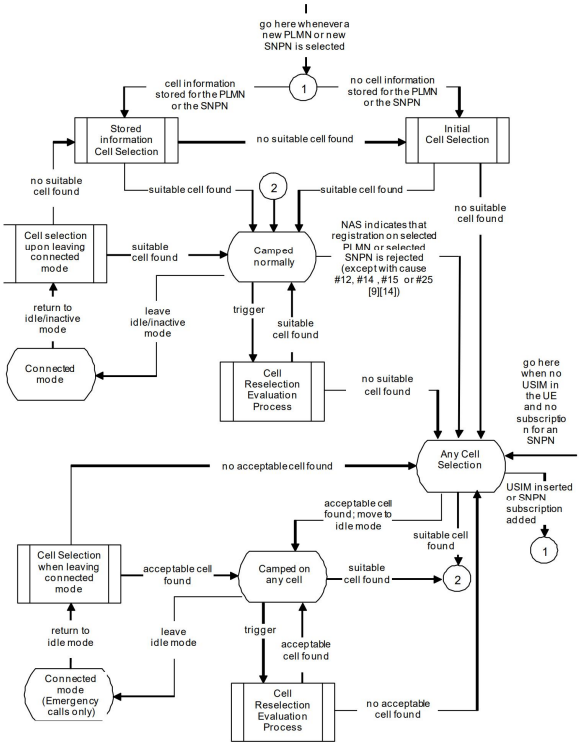


Fig. 2. RRC_IDLE and RRC_INACTIVE Cell Selection and Reselection [12]

셀 선택과 재선택의 상세한 분석을 위해서, 3GPP 38.304 [12]의 “Figure 5.2.2-1: RRC_IDLE and RRC_INACTIVE Cell Selection and Reselection”를 보

면, 셀 선택과 재선택에 관련된 RRC_IDLE 및 RRC_INACTIVE의 상태 천이 절차를 보여준다.

Fig. 2에서 셀 선택과 재선택에 관련된 RRC_IDLE 및 RRC_INACTIVE의 상태 및 상태 천이와 절차를 정리하면 다음과 같다. 먼저 새로운 PLMN 선택 또는 새로운 SNPN 선택을 수행될 때마다 Fig. 2의 ①에서 시작한다. “Cell Selection”은 “Initial Cell Selection”과 “Stored Information Cell Selection” 두 가지 절차 중 하나에 의해 수행된다. “Initial Cell Selection”은 저장된 PLMN 또는 SNPN에 대한 정보가 없을 때 수행된다. “Stored Information Cell Selection”은 저장된 PLMN 또는 SNPN에 대한 정보를 활용하여 셀을 선택한다. 두 경우 모두 적합한 셀을 찾으면 “Camped normally”로 이동한다. 만약 적합한 셀을 찾지 못할 경우에 “Initial Cell Selection”에서는 “Any Cell Selection”으로 이동하고, “Stored Information Cell Selection”에서는 “Initial Cell Selection”으로 이동한다.

“Camped normally” 상태는 RRC_IDLE 및 RRC_INACTIVE 상태에 적용되며, 정상적으로 캠프되면 UE는 3GPP 38.304 [12]의 “5.2.5 Camped Normally state”에 명시된 작업을 수행해야 한다. 이 과정에서 RRC_IDLE 또는 RRC_INACTIVE 상태에서 벗어 나는 경우에는 “Connected mode” 상태로 이동하며, NAS가 선택한 PLMN 또는 선택한 SNPN에 대한 등록이 거부되었음을 나타낼 경우 (cause #12, #14, #15 또는 #25 제외)에는 “Any Cell Selection”로 이동하며, 특정한 Occasion이나 Trigger일 경우 “Cell Reselection Evaluation Process”로 이동한다.

“Connected mode” 상태에서 UE가 RRCRelease 메시지 수신하여 RRC_IDLE 또는 RRC_INACTIVE 상태가 되면 “Cell selection upon leaving connected mode”로 이동한다. 이 때 UE는 RRCRelease 메시지에 redirectedCarrierInfo가 포함된 경우에 따라 적합한 셀에 캠프를 시도해야 한다. UE가 적합한 셀을 찾을 수 없는 경우, UE는 표시된 RAT의 임의의 적합한 셀에 캠프할 수 있다. RRCRelease 메시지가 redirectedCarrierInfo를 포함하지 않는 경우, UE는 NR 반송파에서 적절한 셀을 선택하려고 시도해야 한다. 만약 적합한 셀이 발견되지 않으면, UE는 캠프할 적합한 셀을 찾기 위해 저장된 정보를 사용하여 셀 선택을 수행(“Stored information Cell Selection”)해야 한다.

“Any Cell Selection” 상태는 USIM이 없고 SNPN에 가입 정보가 없을 경우일 때 이동되며, Fig. 2에서 “Any Cell Selection” 아래 부분은 이전에 설명한 내용과 유사하다.

2. Analysis of processing of false base station and UE before/after sending RRCReject in incarceration attacks

이 절에서는 허위 기지국이 RRCReject를 전송할 수 있는 상황을 만들기 위해 필요한 사전 준비 과정과 RRCReject의 전송 가능 여부를 분석한다. 3GPP 38.331 [13]의 “5.3.3 RRC connection establishment”를 보면, RRC 연결 설정 절차는 UE에서 네트워크로 초기 NAS 전용 정보 (NAS Dedicated Information)/메시지를 전송하는 데 사용된다. 이러한 절차에 따라 UE는 허위 기지국에게 RRCSetupRequest를 전송하게 되며, 허위 기지국은 RRCSetup 또는 RRCReject로 응답할 수 있다.

RRCSetupRequest, RRCSetup, RRCSetupComplete 메시지 포맷과 IE (Infomation Element)를 확인하기 위해서 3GPP TS 38.331 [13]을 보면 다음과 같이 정리할 수 있다. RRCSetupRequest 메시지의 Signalling Radio Bearer는 SRB0이고 Logical Channel은 CCCH (Common Control Channel)이다. RRCSetupRequest에 대한 응답 중 하나인 RRCSetup 메시지는 SRB1을 설정하기 위해서 사용된다고 명시되어 있고, RRCSetup 메시지의 Signalling Radio Bearer는 SRB0이고 Logical Channel은 CCCH라고 명시되어 있다. RRCSetup에 대한 응답인 RRCSetupComplete 메시지의 Signalling Radio Bearer는 RRCSetup 메시지에서 설정한 SRB1이고 Logical Channel은 DCCH라고 명시되어 있다. 따라서 RRCReject와 RRCSetup 메시지는 CCCH 논리 채널로 전송되기 때문에 누구나 도청이 가능하다. 여기까지 RRC Connection에 관련된 메시지 RRCSetupRequest, RRCSetup, RRCSetupComplete, RRCReject의 특성에 관해 분석하였다.

허위 기지국이 UE에게 RRCReject 메시지를 전송 가능한지 분석하고자 한다. 이를 위해서 UE의 AS 보안 컨텍스트에 의하여 RRCReject 메시지가 어느 수준까지 보호되는지 수준을 확인하여야 한다. 3GPP TS 38.331 [13]에서 “Annex B (informative): RRC Information“의 “B.1 Protection of RRC messages”를 보면, RRCReject 메시지의 AS 보안 활성화 (AS Security Activation) 전/후에 전송 가능 여부와 메시지 보호 수준이 서술되어 있다.

이 내용에 따르면, RRCReject는 “P”, “A-I”, “A-C”에 대하여 모두 “+”로 표시되어 있다. “P”가 “+”라는 것은 AS 보안 활성화 이전에 해당 메시지가 아무런 보호 없이 전송될 수 있다는 것을 의미한다. 그리고 “A-I”가 “+”라는 것은 AS 보안 활성화가 이루어진 다음에도 해당 메시지는 무결성 보

호 없이 전송될 수 있음을 의미한다. 마지막으로 “A-C”가 “+”라는 것은 AS 보안 활성화가 이루어진 다음에도 해당 메시지는 암호화되지 않고 전송될 수 있음을 의미한다. 이상의 내용은, gNB쪽에서 RRC_INACTIVE 상태이더라도 gNB는 RRCReject 메시지를 SRB0로 전송할 수 있다.

여기까지 공격자가 UE에게 RRCReject를 보내는 것이 가능하다는 것을 확인하였고, 이후에는 UE가 RRCReject를 수신하였을 때 어떻게 동작하는지 분석하고자 한다. 3GPP TS 38.331 [13]에 “5.3.3 RRC Connection Establishment”의 “5.3.3.5 Reception of the RRCReject by the UE”를 보면 UE는 “5.3.15 RRC connection reject”에 명시된 대로 수행하라고 되어 있으며, “5.3.13 RRC Connection Resume”의 “5.3.13.10 Reception of the RRCReject by the UE”에도 동일하게 UE는 “5.3.15 RRC connection reject”에 명시된 대로 수행하라고 되어 있다. 즉, “RRC Connection Establishment”와 “RRC Connection Resume”에서의 RRCReject에 대한 처리는 동일하다는 것을 알 수 있다.

3GPP TS 38.331 [13]의 “5.3.15 RRC connection reject”에 RRCReject에 대한 처리 절차가 서술되어 있다. Table 2는 “RRC connection reject” 절차를 보여준다. 이 절차는 UE가 RRC 연결을 설정하거나 재개할 때 RRCReject를 수신하면 시작한다. 이 절차를 상세하게 분석하고자 한다.

① 만약 타이머 T300, T319, T302가 작동 중이면 중지시킨다. 3GPP TS 38.331 [13]의 “7.1.1 Timers (Informative)”에서 이러한 타이머들의 시작과 중지에 관한 내용이 서술되어 있다. 이러한 내용을 요약하여 정리하면, 타이머 T300은 RRCSetupRequest를 전송할 때 시작되고, RRCSetup 또는 RRCReject를 수신하면 중지된다. 타이머 T319는 RRCResumeRequest 또는 RRCResumeRequest1을 전송할 때 시작되고, RRCResume, RRCSetup 등을 수신하면 중지된다. 감금 공격과 관련이 있는 타이머 T302는 RRC 연결의 설정 또는 재개 과정 동안 waitTime을 가진 RRCReject 또는 RRCRelease를 수신하였을 때 시작된다. 타이머 T302가 중지되는 때는, 첫째, RRC_CONNECTED 또는 RRC_IDLE 상태로 천이할 때, 또는 둘째, 셀 재선택과 RRCReject 메시지를 수신하였을 때 중지된다.

② 3GPP 38.300 [15]의 “6.2 MAC Sublayer”에 따르면, MAC (Media Access Control)에서 DCCH와 같은 논리 채널 관리를 담당한다. 따라서 RRCReject를 수신하면 MAC을 리셋하고 “default MAC Cell Group” 설정을 해제한다. 즉, UE가 현재 연결되어 있던 셀에 대해 알고 있던 정보 (예: DCCH와 같은 논리 채널)를 리셋(Reset)하는 것이다.

③ RRCReject에 waitTime이 설정되어 있으면, T302를 waitTime 값으로 설정하여 처음 시작 (또는 재시작)시킨다.

④ 상위 계층의 요청에 대한 응답으로 RRCReject를 받은 경우이다.

⑤ RRCSetupRequest에 대한 응답으로 RRCReject를 수신하였을 경우이다. 이 때는 “RRC connection” 설정의 실패를 상위 계층에 알리고, 현재 절차를 끝낸다.

⑥ RRCResumeRequest 또는 RRCResumeRequest1에 대한 응답으로 RRCReject를 받은 경우이다. 이 경우는 상위 계층에 의해 Resume이 발생한 경우에는 상위 계층에 알리고, RNA 업데이트로 인해 발생한 경우는 pendinggRNA-Update를 true로 설정하고, 현재 가지고 있는 여러 키들을 폐기하고, SRB1

Table 2. The procedure of RRC connection reject by the UE [13]

①	1> stop timer T300, if running; 1> stop timer T319, if running; 1> stop timer T302, if running;
②	1> reset MAC and release the default MAC Cell Group configuration;
③	1> if waitTime is configured in the RRCReject: 2> start timer T302, with the timer value set to the waitTime;
④	1> if RRCReject is received in response to a request from upper layers: 2> inform the upper layer that access barring is applicable for all access categories except categories '0' and '2';
⑤	1> if RRCReject is received in response to an RRCSetupRequest: 2> inform upper layers about the failure to setup the RRC connection, upon which the procedure ends;
⑥	1> else if RRCReject is received in response to an RRCResumeRequest or an RRCResumeRequest1: 2> if resume is triggered by upper layers: 3> inform upper layers about the failure to resume the RRC connection; 2> if resume is triggered due to an RNA update: 3> set the variable pendingRNA-Update to true; 2> discard the current KgNBkey, the KRRCenckey, the KRRCintkey, theKUPintkey and the KUPenckey derived inaccordance with 5.3.13.3; 2> suspend SRB1, upon which the procedure ends;
⑦	The RRC_INACTIVE UE shall continue to monitor paging while the timer T302 is running. NOTE: If timer T331 is running, the UE continues to perform idle/inactive measurements according to 5.7.8.

을 중단하고, 현재 절차를 끝낸다. 현재 분석과 관련이 있는 것은 ⑤ 과 ⑥ 인 경우이며, 두 경우 모두 RRCReject가 수신되었을 때, AS Security Context가 없거나 폐기된다는 것을 유추할 수 있다.

⑦ RRC_INACTIVE 상태의 UE는 타이머 T302가 실행되는 동안 계속해서 페이징을 모니터링해야 한다. 타이머 T331이 실행 중이면, UE는 idle/inactive 측정을 계속 수행한다.

결과적으로 UE가 허위 기지국에게 RRCSetupRequest를 전송하였을 때, 이를 수신한 허위 기지국은 UE에게 RRCReject를 전송할 수 있다. 여기서 RRCReject 메시지의 RejectWaitTime IE에 임의의 값 (최대 16초)을 설정할 수 있으며, 이러한 RRCReject 메시지를 수신한 UE는 아무런 의심 없이 수신한 RRCReject 메시지를 처리할 것으로 판단된다. 또한 RRCReject 메시지를 계속해서 전송할 경우, 타이머 T302가 계속 연장되어 피해자 UE가 RRC 연결 설정에 계속 머무르게 할 수 있을 것으로 판단된다.

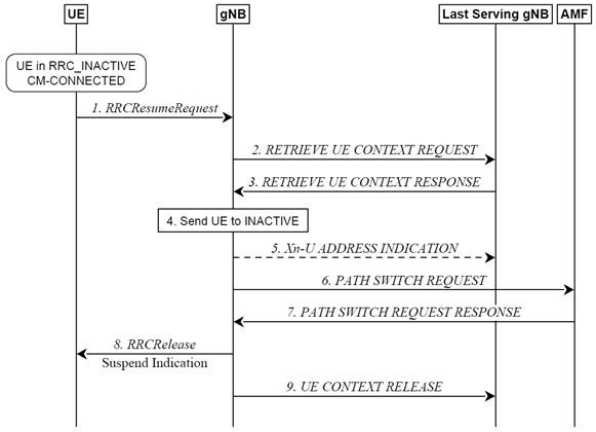


Fig. 3. Resume request responded with Release with Redirect, with UE Context relocation [15]

3. Analysis of processing of false base station and UE before/after sending RRCResumeRequest in incarceration attacks

분석하고 있는 Hussain 등 [8]이 제안한 감금 공격에서 "Redirect Indication" 정보가 포함된 RRCRelease 메시지를 이용한다. 이러한 "Redirect Indication" 정보가 포함된 RRCRelease로 응답하는 "Resume Request"의 처리 절차는 3GPP TS 38.300 [15]의 "9.2.2.6 Resume request responded with Release with Redirect, with UE context relocation"에서 찾을 수 있으며, Fig. 3와 같다.

Fig. 3에서 UE의 "Last Serving gNB"보다 강한 신호를 송신하는 허위 기지국을 공격자가 운영할 경우에 RRC_INACTIVE 상태의 피해자 UE는 "RRC Resume Request" 설정을 시도할 수 있다. gNB는 UE를 RRC_CONNECTED, RRC_IDLE, 또는 RRC_INACTIVE 상태로 천이시킬 수 있다. RRC_INACTIVE의 경우는 "Redirect Indication"이 RRCRelease에 포함될 수 있다. 이 경우 피해자 UE를 계속 감금시켜 두기 위하여 RRCRelease 메시지 안에 "Redirected Carrier Information"을 포함시킨 다음, 피해자 UE에게 RRCRelease를 전송하여, 두 번째 허위 기지국과 연결하도록 유도하는 것과 관련이 있다.

Hussain 등 [8]의 감금 공격에서 RRCRelease 메시지를 사용하는 이유는 RRCReject를 여러 번 전송할 경우 "Connection Establishment Fail Counter"가 한계치 (예: 4회)에 도달하는 것을 막기 위해서라고 기술되어 있다. 그 들은 RRCRelease 메시지에 "Redirected Carrier Information"을 넣어서 보낸다고 했다. 하지만, 3GPP TS 38.331 [13]에서 "Annex B (informative): RRC Information"의 "B.1 Protection of RRC messages"를 보면, "AS Security Activation" 전에는 RRCRelease 메시지는 "RedirectedCarrierInfo"를 포함할 수 없다고 서술하고 있다. 즉, UE가 허위 기지국에게 RRCResumeRequest를 전송하였을 때, 허위 기지국은 RRCRelease 내에 RedirectedCarrierInfo를 포함시켜서, 피해자 UE에게 RRCRelease를 전송할 수 없다. 왜냐하면, 피해자 UE와 허위 기지국 사이에 "AS Security Activation"이 되어 있지 않기 때문이다.

하지만, 허위 기지국은 공격자가 운영하기 때문에, 공격자인 허위 기지국이 표준을 무시하여 "AS Security Activation"가 없어도 UE에게 RRCRelease 내에 RedirectedCarrierInfo을 포함시켜서 전송할 수도 있다. 이러한 경우에 UE의 처리 과정을 분석할 필요가 있다.

3GPP TS 38.331 [13]의 "5.3.13 RRC connection resume"에서 "5.3.13.9 Reception of the RRCRelease by the UE"에 보면 UE는 "5.3.8"에 명시된 대로 작업을 수행해야 한다고 되어 있다. 3GPP TS 38.331 [13]의 "5.3.8 RRC connection release"에서 "5.3.8.3 Reception of the RRCRelease by the UE"의 절차 중 일부를 Table 3에서 보여주고 있다.

Table 3. Part of the RRC connection release [13]

```
...
1> if the AS security is not activated:
    2> ignore any field included in RRCRelease
       message except waitTime;
    2> perform the actions upon going to RRC_IDLE
       as specified in 5.3.11 with the release cause
       'other' upon which the procedure ends;
1> if the RRCRelease message includes redirectedCarrierInfo
   indicating redirection to eutra:
    2> if cnType is included:
        3> after the cell selection, indicate the available CN
           Type(s) and the received cnType to upper layers;
...
```

Table 3을 보면, UE가 RedirectedCarrierInfo가 포함된 RRCRelease를 수신하더라도, AS Security가 활성화되지 않은 경우에는, waitTime을 제외한 RRCRelease 메시지에 포함된 모든 필드를 무시하게 되며, 절차가 종료되며 5.3.11에 지정된 대로 RRC_IDLE로 이동하는 작업을 수행한다. 따라서 허위 기지국이 UE에게 RedirectedCarrierInfo 가 포함된 RRCRelease를 전송하더라도, AS Security Context가 없는 상태이므로 UE는 아무런 처리 없이 RRC_IDLE 상태로 이동한다. 따라서 첫 번째 허위 기지국을 운영하는 공격자가 RRCRelease 메시지를 이용하여 피해자 UE에게 두 번째 허위 기지국으로 이동하라고 설득할 수 없다.

IV. Conclusions

본 논문에서는 5G SNPN에서 RRCRejecet와 RRCRelease를 이용한 감금 공격의 가능성을 3GPP 표준 문서를 기반으로 분석하였다. 첫째, UE의 셀 선택과 재선택 절차를 분석하였다. 둘째, RRCReject와 RRCRelease의 전송 전/후의 허위 기지국과 UE의 처리 과정 분석하였다. 분석한 결과, 허위 기지국 중 하나가 UE를 유인하여, UE가 RRCSetupRequest 메시지를 전송하도록 하는 것이 가능하였고, 허위 기지국은 이에 대한 응답으로 무결성 보호가 되지 않는 RRCReject 메시지를 전송할 수 있다. 또한 피해자 UE의 RRCSetupRequest 메시지에 계속 RRCReject 메시지로 대응하여 피해자 UE가 RRC 연결 시도 과정에 계속 머무르게 할 수 있을 것으로 판단된다. 반면, RRCRelease를 이용하여 다른 허위 기지국으로의 연결 설정 시도를 유도하는 것은 불가능한 것으로 판단된다. 향후 5G 공개 소프트웨어 기반의 시뮬레이션을 통한 공격 가능 여부에 대한 검증 연구를 진행할 예정이다.

ACKNOWLEDGEMENT

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No.2020-0-00952, Development of 5G Edge Security Technology for Ensuring 5G+ Service Stability and Availability).

REFERENCES

[1] M. Agiwal, A. Roy, and N. Saxena: “Next Generation 5G Wireless Networks: A Comprehensive Survey,” IEEE Communications Surveys & Tutorials, Vol. 18, No. 3, pp. 1617-1655, 3rd Quart., 2016, DOI: 10.1109/COMST.2016.2532458

[2] M. Wollschlaeger, T. Sauter and J. Jasperneite, “The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0,” IEEE Industrial Electronics Magazine, Vol. 11, No. 1, pp. 17-27, Mar. 2017, DOI: 10.1109/MIE.2017.2649104.

[3] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtovand, M. Ylianttila, “Security for 5G and Beyond”, IEEE Communications Surveys & Tutorials, Vol. 21, No. 4, pp. 3682-3722, May 2019. DOI: 10.1109/COMST.2019.2916180

[4] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage: ‘‘A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions,’’ IEEE Communications Surveys & Tutorials, Vol. 22, No. 1, pp. 196-248, 1st Quart., 2020. DOI: 10.1109/COMST.2019.2933899

[5] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, “A Formal Analysis of 5G Authentication,” In Proc. the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS ’18), pp. 1383-1396, Oct. 2018. DOI: 10.1145/3243734.3243846

[6] C. Cremers and M. Dehnel-Wild, “Component-based formal analysis of 5G-AKA: channel assumptions and session confusion,” in Proc. 26th Annual Network and Distributed System Security Symposium, NDSS, pp. 24-27, Feb. 2019. DOI: 10.14722/ndss.2019.23394

[7] H. Kim, J. Lee, E. Lee, Y. Kim: “Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane,” in Proc. IEEE Symposium on Security and Privacy (SP), pp. 1153-1168, May 2019. DOI: 10.1109/SP.2019.00038

[8] S.R. Hussain, M. Echeverria, I. Karim, O. Chowdhury, E. Bertino: “5GReasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol,” in Proc. 2019

ACM SIGSAC Conference on Computer and Communications Security, pp.669-684, Nov. 2019. DOI: 10.1145/3319535.3354263

[9] K. Kim, K. Park, T.K. Park: "Analysis of Deregistration Attacks in 5G Standalone Non-Public Network," Journal of the Korea Society of Computer and Information, Vol. 26, No. 9, pp. 81-88, Sep. 2021. DOI: 10.9708/jksci.2021.26.09.081

[10] 5G-ACIA White Paper: "5G Non-Public Networks for Industrial Scenarios," July 2019.

[11] T.K. Park, J.G. Park, K. Kim: "Security Threats and Potential Security Requirements in 5G Non-Public Networks for Industrial Applications," Journal of the Korea Society of Computer and Information, Vol. 25, No. 11, pp. 105-114, Nov. 2020. DOI: 10.9708/jksci.2020.25.11.105.

[12] 3GPP TS 38.304 v16.4.0: "NR; User Equipment (UE) procedures in Idle mode and RRC Inactive state," Mar. 2021.

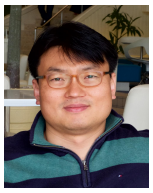
[13] 3GPP TS 38.331 v16.3.1: "Radio Resource Control (RRC) protocol specification," Jan. 2021.

[14] 3GPP TS 38.133 v.16.7.0, "NR; Requirements for support of radio resource management," Mar. 2021.

[15] 3GPP TS 38.300 v16.5.0, "NR; NR and NG-RAN Overall Description; Stage 2," Mar. 2021.

Authors

Keewon Kim received his M.S. and Ph.D. degrees in Computer Engineering from Kyungpook National University, Korea, in 2001 and 2006, respectively. He is currently an assistant professor in the department of Computer Engineering, Mokpo National Maritime University. He is interested in information security, security protocol, VLSI, and big data analysis.



Jong-Geun Park received his BS and MS degree in industrial engineering from SungKyunKwan University, Rep. of Korea, in 1997 and 1999, respectively, and received his PhD degree in computer engineering from Chungnam National University, Rep. of Korea, in 2013. From 1999 to 2001, he was a researcher at ADD, Daejeon, Rep. of Korea. Then, he joined ETRI, Daejeon, Rep. of Korea, in 2001, where he is currently working as a principal researcher. Currently, he is interested in mobile network security, SDN/NFV, and Cloud security.

Tae-Keun Park received his B.S., M.S., and Ph.D. degrees in Computer Science and Engineering from POSTECH, Pohang, Korea in 1991, 1993, and 2004, respectively. He joined POSTECH PIRL in 1993 and moved to SK Telecom in 1996. From 2000 to 2001 and from 2001 to 2002, he worked for 3Com Korea and Ericsson Korea, respectively. In 2004, he joined in the department of Multimedia Engineering, Dankook University, Korea. He is currently on the faculty of the department of Computer Engineering at Dankook University. His research interests include network security, IoT, wireless/mobile communications, and distributed services.