# 드론 바인딩에서 5G RRC 접속으로의 전환에 대한 위협 분석: 보안 영향 및 신규 공격 벡터 도출

박준범, 윤상범*

LIG넥스원

junbeom.park@lignex1.com, *sangbom.yun@lignex1.com

# Threat Analysis of the Shift from Drone Binding to 5G RRC Connection: Security Implications and Emerging Attack Vectors

Park Jun Beom, Yun Sang Bom*

LIG Nex1

요 약

본 논문은 드론 바인딩 기반 C2 링크가 5G 상업망의 RA 및 RRC 연결 절차로 대체되면서, 공격면이 전용 링크에서 셀룰러 제어평면 및 빔 기반 복구 절차로 확장됨을 분석한다. 특히 A2G 채널과 이동성으로 인해 빔 회복 이벤트가 빈발할 수 있으며, 물리계층 교란(오버샤도잉) 및 드론 식별자(SUCI 등) 관측 가능성이 가용성과 프라이버시 위험을 누적적으로 증폭시킬 수 있음을 논의한다. 마지막으로 시뮬레이션을 통해 SNR 저하 구간에서 5G 드론의 BFR 빈도가 지상 단말 대비 증가할 수 있음을 정량적으로 보이고, 오버샤도잉 위협 모델 하에서 통신 장애로의 확산 가능성을 제시한다.

## Ⅰ. 서 론

최근 드론은 BNLOS 원격 임무와 군집·고밀도 운용으로 확장되며, 상시 연결성, 저지연 C2, 대용량 영상 전송에 대한 요구가 빠르게 증가하고 있다.[1] 이러한 요구는 3GPP의 UAS 서비스 요구사항 정의로도 반영되며, 5G 상업망 기반의 셀룰러 연결형 드론 수요를 견인하고 있다. 또한, 3GPP는 UAS 연결·식별·추적을 위한 시스템 기능을 규정하여, 드론이 3GPP 네트워크 절차 내에서 운용되는 방향을 제도권으로 명확히 하고 있다.[2] 이와 동시에 통신 패러다임이 ISM 기반의 전용 바인딩 링크에서 5G RRC 및 RA 절차로 이동하면서, 보안 위협이 셀룰러 제어평면 전반으로 확장될 수 있다. 실제로 위장 기지국(fake BS)을 통한 가용성 저해·연결 고착·DoS 등 제어평면 공격 가능성이 활발히 논의되어 왔다.[3-4]

5G 드론 역시 5G 단말과 동일한 RRC 및 RA 절차로 접속하므로, 동일한 취약점의 영향을 직접적으로 받을 수 있다. 더불어, 드론은 A2G 채널에서 LoS 노출이 증가해 다수 셀 간섭이 심화될 수 있으며, 이를 완화하기 위해 빔포밍·빔 관리 의존도가 높아진다. 이러한 환경은 접속·이동성·복구 절차의 빈도를 높여 제어평면 공격의 기회를 확대할 가능성이 있다.[5]

본 논문에서는 드론 바인딩에서 RRC 접속으로의 전환을 중심축으로 위협 모델을 정립하고, 5G 드론의 보안 영향과 부상하는 공격 벡터를 체계적으로 도출한다.

## Ⅱ. 본론

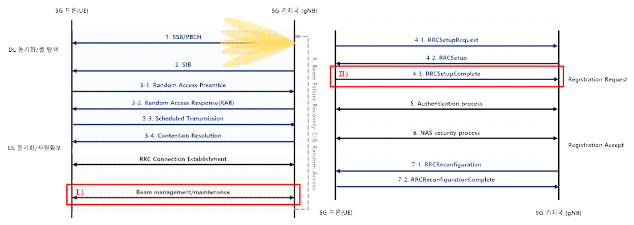


그림 1 5G 드론 RA, RRC 및 빔 회복 절차[2]

그림 1은 5G 드론에서 기존 바인딩 절차를 대체하는 Random Access(RA), RRC connection, 그리고 빔 회복(beam recovery) 과정을 나타낸다. 5G 드론은 전통적인 바인딩 기반 C2 링크가 아니라, 셀룰러 상업망의 RA 및 RRC 연결 절차에 의존해 접속 및 통신을 수행한다. UE는 SSB 탐색을 통해 시간·주파수 동기를 맞추고, PBCH/MIB 및 SIB1을 수신하여 RACH 설정 정보를 획득한다. RA 절차는 PRACH 프리앰블(UE) - RAR(gNB) - RRCSetupRequest(UE) - RRCSetup(gNB)의 순서로 진행되며, 이를 통해 UE는 UL 동기 및 초기 자원을 확보한다. 이후 UE는 RRCSetupComplete를 통해 NAS Registration Request를 전달하며, 이 메시지에는 SUCI와 같은 UE 식별에 필요한 정보가 포함될 수 있다. 연결 성립 후에는 RRCReconfiguration을 통해 데이터 베어러 구성, 측정 및 이동성 관련 설정이 수행된다. 결과적으로 본 절차는 (i) RA 기반 자원 획득 구간에서의 접속 방해와, (ii) NAS Registration 구간에서의 식별자 기반 프라이버시 노출 또는 추론 위험을 동시에 내포한다.

5G 드론은 A2G 채널 및 이동성 특성으로 인해 링크 품질 변동이 커지고, 그 결과 접속 재시도, 재등록, 복구 절차가 지상 단말 대비 더 자주 발생할 수 있다. 공중 단말은 LoS 노출 증가로 다수 셀 간섭의 영향을 더 크게 받을 수 있으며, 이를 완화하기 위해 빔포밍과 빔 관리에 대한 의존도가 증가한다. 이러한 환경에서는 링크 품질 저하가 단순 데이터 채널 성능 저하를 넘어 빔 정렬 실패 및 빔 회복 절차의 빈발로 이어지며, 결과적으로 RA 기반 자원 획득·유지 구간이 반복적으로 호출된다. 따라서 공격자 관점에서 “빔 복구가 자주 발생되는 구간”은 제어평면 가용성을 겨냥한 유효한 공격 표면이 될 수 있고, 물리계층 신호 오버샤도잉 계열의 교란이 빔 관련 제어 신호의 판별을 왜곡하거나 회복 절차를 반복 유발함으로써 접속 지연·실패 및 연결 유지 실패로 이어질 가능성을 시사한다. 본 논문은 이러한 “절차 빈발성”이 5G 드론에서 접속 방해 기반 가용성 공격의 영향을 증폭시킬 수 있다는 점에 주목한다. 그림 2는 SNR 변화에 따른 빔 회복 수행 빈도수를 나타낸다. 지상 단말과 5G 드론 간 빔 회복 수행

빈도수가 유의미한 차이를 보인다.

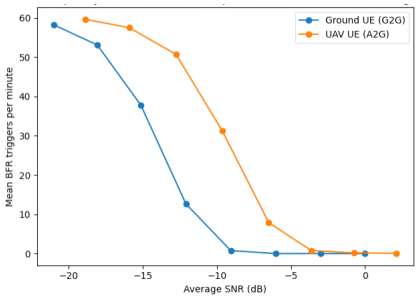


그림 2 SNR 변화에 따른 빔 회복 수행 빈도수

5G 초기 RRC 연결 성립 단계에서 UE는 RRCSetupComplete의 dedicatedNAS-Message를 통해 NAS 메시지를 전달하며, 이때 Registration Request의 5GS mobile identity에 SUCI가 포함된다. 또한 네트워크는 Identification 절차에서 IDENTITY REQUEST로 SUCI 제출을 요구할 수 있고, UE는 IDENTITY RESPONSE로 SUCI를 전송한다. SUCI는 무선 구간에서 관측 가능한 식별자로서 수동 스니핑 환경에서 수집될 수 있으며, 실제 운용에서는 추적 가능성(linkability) 및 존재 확인과 같은 프라이버시 위험이 논의되어 왔다. 더 나아가 물리계층 신호 오버샤도잉(overshadowing) 계열 위협 모델은 초기 절차의 안정성을 저하시켜 접속 실패·지연을 유발할 뿐 아니라, 식별 절차의 재시도 빈도를 증가시켜 SUCI 전송 이벤트의 관측 기회를 확대할 수 있다. 이러한 조건은 공격자가 위장 단말(rogue UE)을 통한 부정 접속 시도 또는 네트워크 절차를 악용한 식별·프라이버시 침해 시나리오를 전개할 여지를 키운다. 특히 드론 환경에서는 A2G 채널 및 이동성으로 인해 접속·복구 이벤트가 빈발할 가능성이 높아, 동일한 위협 모델 하에서 프라이버시 노출·추론 위험이 누적적으로 증폭될 수 있으므로, 드론 시나리오를 반영한 정량적 분석과 방어 기법 설계에 대한 추가 연구가 필요하다.

5G 드론은 비행 중 빔 실패로 인해 BFR이 빈발하고, 이 과정에서 BFR 전용 PRACH 자원이 반복적으로 사용된다. 본 논문은 반복되는 PRACH 기반 복구 구간을 핵심 공격 표면으로 보고, 무선 구간 신호 오버샤도잉 위협 모델 하에서 PRACH 단계의 교란이 빔 복구 실패 누적 및 장시간 접속/연결 가용성 저하로 이어질 수 있음을 분석하였다.

## Ⅲ. 결론

본 논문은 기존 드론의 바인딩 기반 C2 링크가 5G 상업망의 RA 및 RRC 연결 절차로 대체되면서, 드론 통신의 공격면이 전용 링크 중심에서 셀룰러 제어평면 전반으로 확장됨을 논의하였다. 특히 5G 드론은 스마트폰과 동일한 RA/RRC 절차를 따르지만, A2G 채널의 LoS 노출 및 다중 셀 간섭, 그리고 높은 이동성으로 인해 링크 품질 변동이 커져 접속·복구 이벤트가 빈발할 수 있다. 이러한 환경에서 빔포밍 및 빔 관리 의존성이 증가하며, 빔 회복 절차가 통신 가용성을 좌우하는 핵심 방법으로 부상한다. 결과적으로 물리계층 신호 오버샤도잉과 같은 교란 위협은 접속 지연·실패를 유발하는 동시에, 빔 회복의 반복 및 연결 유지 실패를 통해 임무 수준의 통신 장애로 확대될 가능성을 시사한다. 또한 초기 NAS 등록 구간에서 관측 가능한 식별자(SUCI 등)의 전송은 수동 스니핑 및 절차 반복 유도 상황에서 프라이버시 노출·추론 위험을 누적시킬 수 있다. 시뮬레이션 결과는 제어평면 교란이 접속 성공률, 연결 지연, 복구 시도 횟수 등 핵심 지표를 악화시킬 수 있음을 보여주었다. 향후 연구에서는 5G 드론 운용 조건을 반영한 정량적 측정(빔 복구 발생률, 노출 빈도, 임무 영향)을 통해 위협의 실질적 위험도를 평가하고, 절차 기반 이상 징후 탐지, 5G 드론 특화 이동성/빔 정책, 다중 링크 페일세이프 등 가용성과 프라이버시를 동시에 고려한 방어 기법을 설계할 필요가 있다. 향후 연구에서는 5G 드론 공격 위협 모델을 정의하여 5G 상용드론에서의 적용 가능성을 검증하고, 방어기법에 대해 제시할 예정이다.

## ACKNOWLEDGMENT

Put sponsor acknowledgments.

## 참 고 문 헌

[1] Ericsson, “Ericsson Mobility Report – November 2025,” Ericsson AB, Nov 2025.

[2] 3GPP, “NR; Physical layer procedures for control,” 3GPP TS 38.213, V15.15.0, Jun 2022

[3] M. Chlosta, D. Rupprecht, C. Pöpper, and T. Holz, “5G SUCI-Catchers: Still catching them all?” ACM WiSec, Jun 2021.

[4] H. Yang, S. Bae, M. Son, H. Kim, S. M. Kim, and Y. Kim, “Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE,” USENIX Security ’19, Aug. 2019

[5] S. D. Muruganathan et al., "An Overview of 3GPP Release-15 Study on Enhanced LTE Support for Connected Drones" IEEE Communications Standards Magazine, Dec 2021