

5G 네트워크 슬라이싱 공격 시나리오 개발

과제명: 5G특화망 · 유 · 무선 통합환경에서 네트워크 슬라이싱 기반서비스의 보안 리질리언스 기술 개발

5G는 초고속 · 초저지연 · 초연결 특성을 기반으로 다양한 산업 서비스(eMBB, URLLC, mMTC)를 지원하며, 네트워크 슬라이싱은 이러한 서비스별 요구사항을 충족하기 위한 핵심 기술로 주목받고 있다. 네트워크 슬라이싱은 서비스별 격리를 제공하지만, 자원 공유와 관리 취약점을 악용하면 전체 슬라이스에 영향을 미치는 보안 위협이 발생할 수 있다. 본 연구는 5G 네트워크 슬라이싱 환경에서 발생 가능한 주요 보안 위협을 분석하고, 실제 서비스 사례(CCTV, 스마트 미터, 실시간 영상회의)를 대상으로 SQL Injection, MQTT 취약점, DTLS 취약점 기반 공격 시나리오를 설계하였다.

정보보안암호수학과

20232106 정유진

alice2002@kookmin.ac.kr



5G 네트워크 & 네트워크 슬라이싱

5세대 이동통신(5G)은 초고속 · 초저지연 · 초연결을 통해 스마트 시티, 자율주행차, 원격 의료 등 다양한 산업 혁신을 지원한다. 3GPP는 서비스 기반 아키텍처(SBA)를 도입해 사용자 단말(UE), 무선 접속망(RAN), 코어 네트워크(5GC) 간 안정적 통신을 보장한다[1]. 5GC는 AMF, UPF, UDM, NRF, NSSF 등 다양한 네트워크 기능(NF)으로 구성되어 인증, 세션 관리, 슬라이스 선택, 정책 제어를 수행한다. 이러한 구조를 기반으로 eMBB(초고속 모바일 브로드밴드), URLLC(초신뢰 · 초저지연 통신), mMTC(대규모 IoT) 서비스를 제공할 수 있으며, 네트워크 슬라이싱을 통해 자원 격리와 보안을 보장한다. 네트워크 슬라이싱은 하나의 물리적 5G 인프라 위에 여러 개의 독립적 가상 네트워크를 생성해 서비스별 상이한 QoS와 보안 요구를 충족하도록 하는 기술이다[2][3][4].

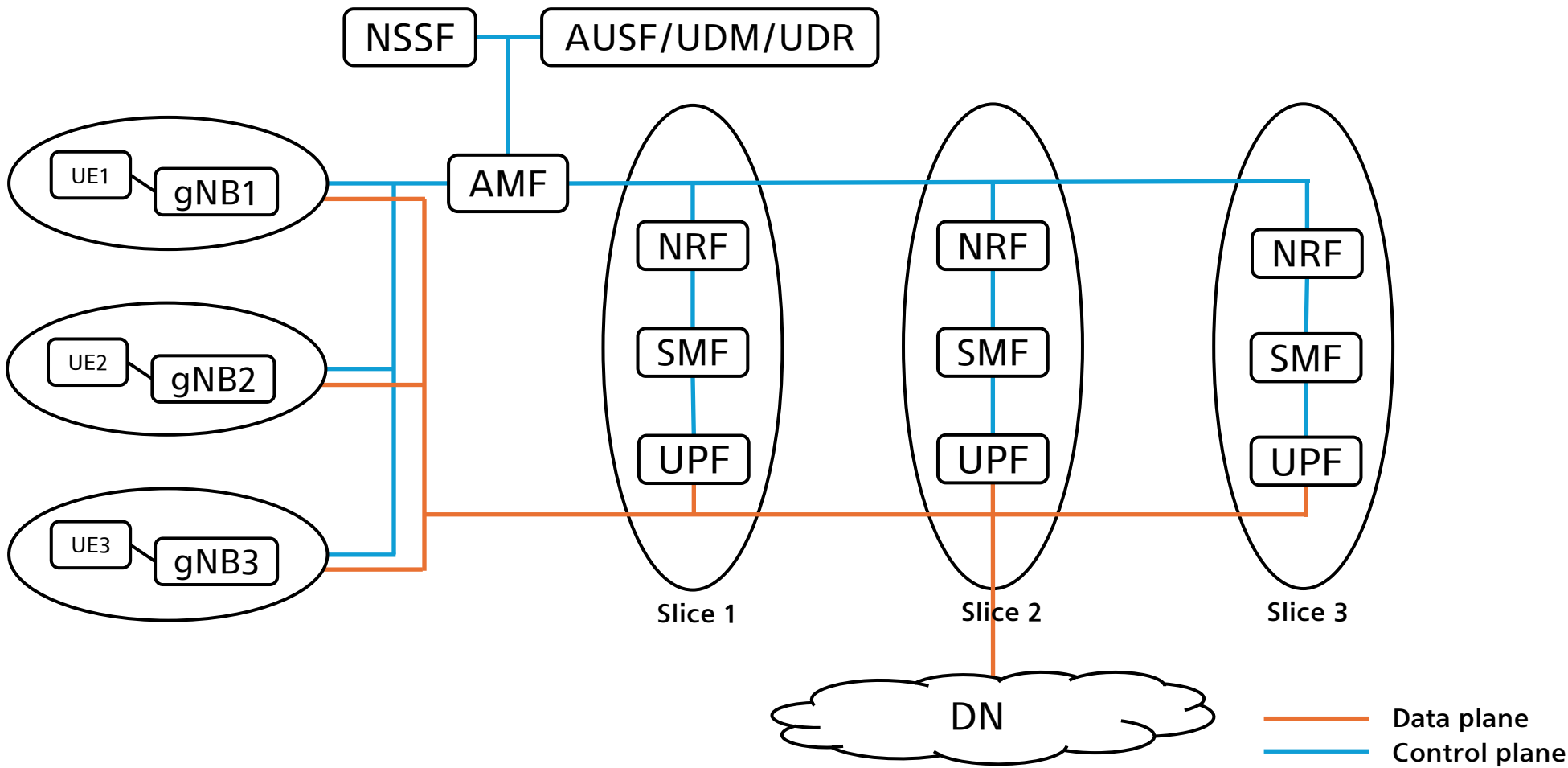


그림 1. 네트워크 슬라이싱

네트워크 슬라이싱 위협

주요 위협 벡터는 소프트웨어 구성, 네트워크 보안, 네트워크 슬라이싱, 레거시 인프라, MEC, 스펙트럼 공유, SDN으로 구분된다. 취약점은 3GPP, ITU, ETSI, NIST, GSMA 등 다양한 표준을 종합해 평가된다[5]. 아래 표는 네트워크 슬라이싱 환경에서 발생할 수 있는 다양한 위협 벡터를 구체적으로 분류하고, 각 벡터에 따른 공격 방식과 특징을 설명한다.

표 1. 네트워크 슬라이싱 위협

위협 벡터	설명	관련도
DoS 공격	중앙 집중식 제어 요소에 대한 DoS 공격	H
구성 공격	잘못 구성된 시스템 제어를 이용한 공격	H
중간자 공격	암호화되지 않은 채널이나 네트워크 링크에 접근하여 두 당사자 간의 통신을 중계하는 공격	H
포화 공격	서비스 포화로 인한 액세스 포인트와 MME에서의 핑퐁 행동	M
침투 공격	구독자 정보를 노출하는 악성코드 공격	M
사용자 신원 도용	사용자 정보 데이터베이스에 침입하여 사용자 자격 증명을 도용	M
TCP 레벨 공격	게이트웨이 및 라우터에서의 TCP 세션 또는 SYN 플러딩	M
NAS 신호 폭풍	UE 트래픽과 코어 네트워크에 대한 신호 메시지에 대한 공격	M
하이재킹 공격	SDN 하이퍼바이저 컨트롤러에 대한 공격	L
무단 접근	저전력 액세스 포인트를 통한 무단 접근	L
채널 예측 공격	무선 인터페이스에 대한 공격	L
키 노출	인증 및 키 협상 타협으로 세션 키나 장기 키가 유출되어 트래픽 복호화와 세션 위조가 발생하는 공격	L

공격 시나리오

CCTV 서비스 공격	엣지 컴퓨팅 서비스 공격	영상 회의 서비스 공격
<div>공격 대상</div> eMBB 슬라이스 상에서 운영 되는 CCTV 서버	mMTC 슬라이스 상에서 운영되는 스마트 미터 데이터 수집 시스템	eMBB 슬라이스 상에서 운영되는 Web RTC 기반, 실시간 영상회의 애플리케이션
<div>공격 기반</div> SQL Injection 기법을 통해 영상 데이터에 무단 접근	MQTT 프로토콜의 보안 설정 미흡(인증 비활성화, ACL 미흡, 평문 전송 등)인 경우 악성 단말을 이용한 비인가 접근 시도	DTLS handshake 구간의 취약점을 이용한 세션 오류 및 서비스 마비
<div>대응 절차</div> 트래픽 모니터링을 통한 비정상 SQL 쿼리 패턴이나 권한 범위를 초과한 데이터 조회 요청이 탐지될 경우, 해당 단말의 접근을 즉시 차단 후 eMBB 슬라이스 내 CCTV 관리 서버를 격리 및 재조정	네트워크는 비인가 Topic 발행을 차단하기 위해 PDU 세션 해제나 슬라이스 권한 변경을 수행한다. MQTT는 TLS와 Mutual TLS로 단말을 인증해 공격 단말 유입을 막는다. 중앙 제어 시스템은 이상 데이터 발생 시 정책을 갱신해 단말이나 세션을 차단한다.	트래픽 모니터링을 통한 DTLS handshake 실패율 증가나 비정상 세션 증가가 탐지될 경우, 해당 슬라이스 격리 및 재조정

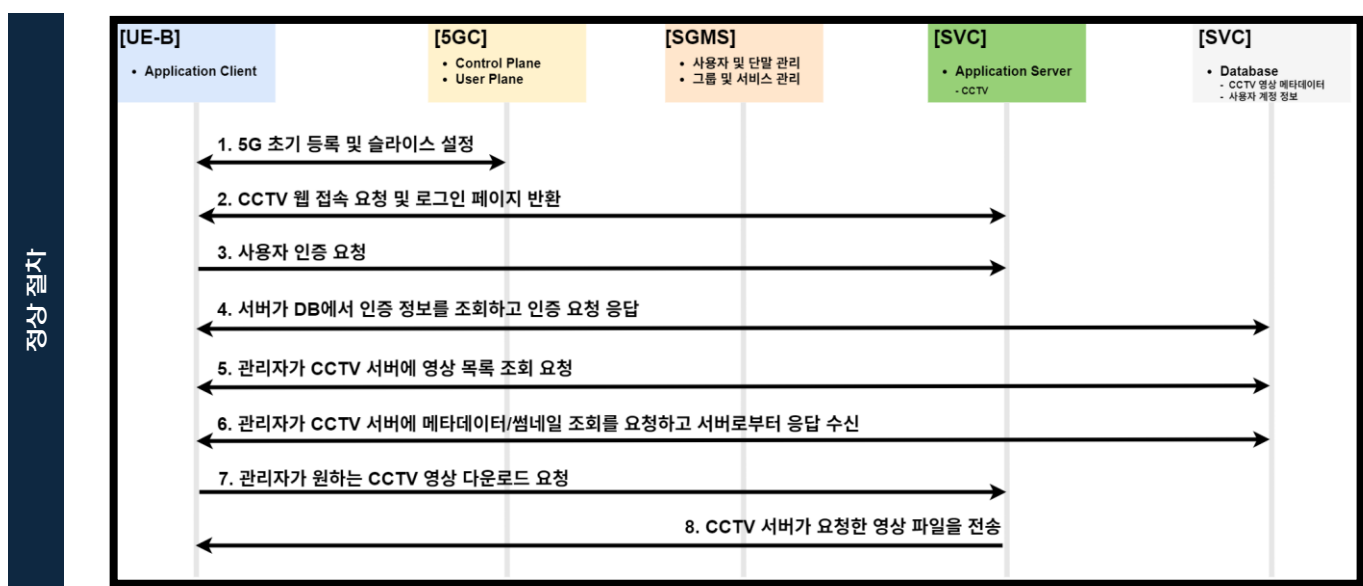


그림 2. CCTV 영상 다운로드 정상 절차

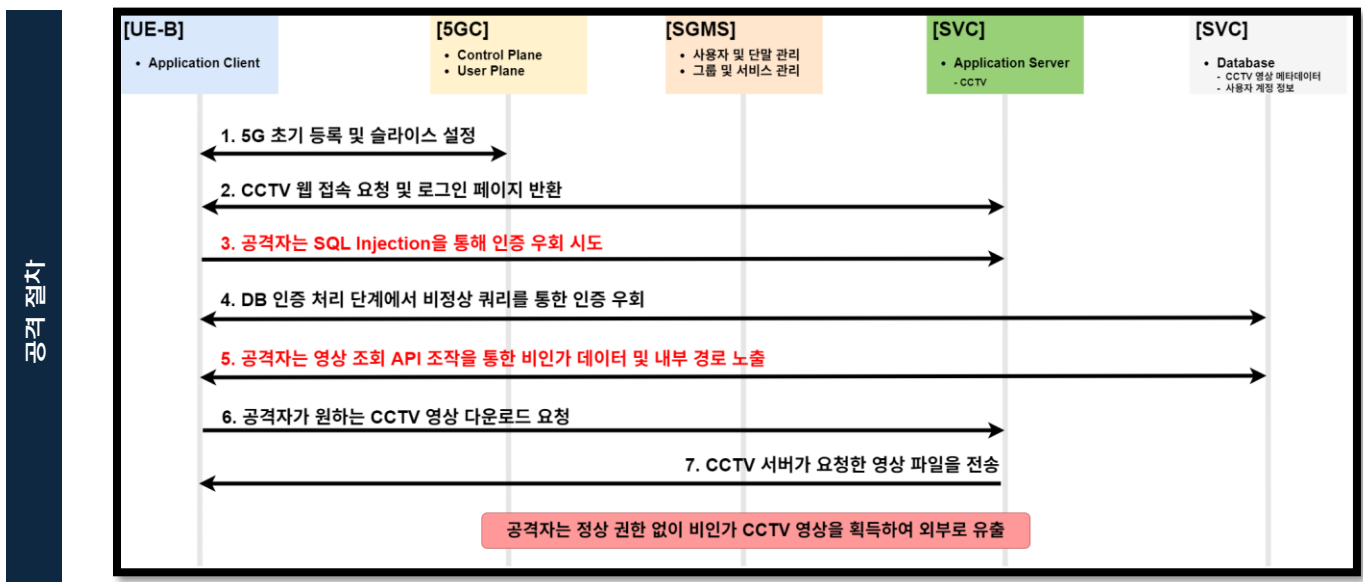


그림 3. SQL Injection 기반 CCTV 서버 공격 절차

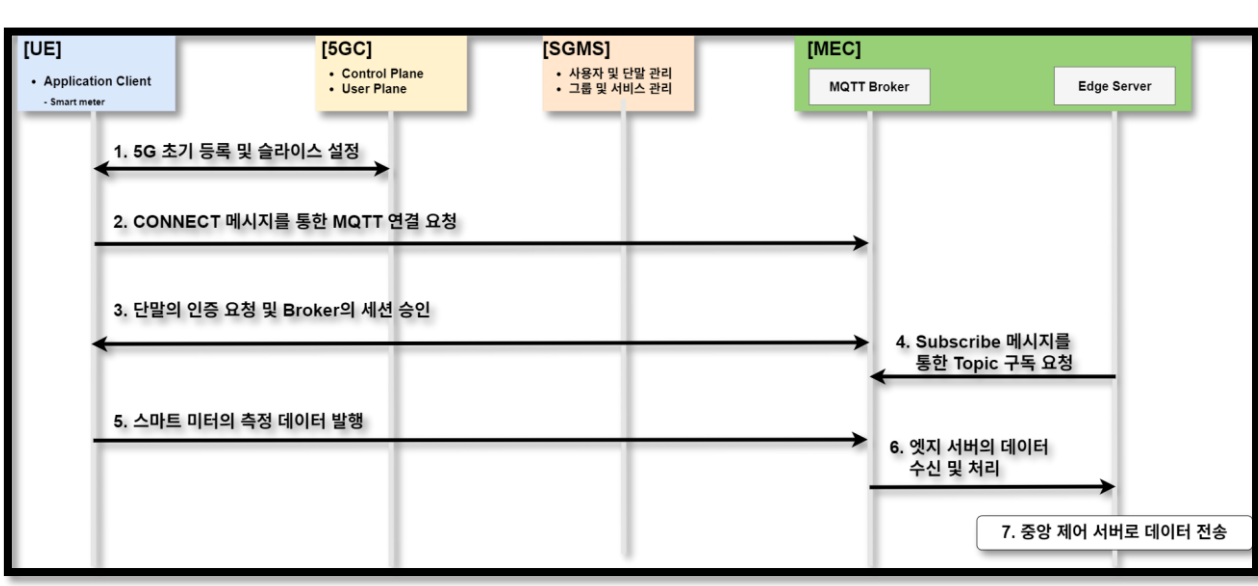


그림 4. 스마트 미터링 데이터 수집 정상 절차

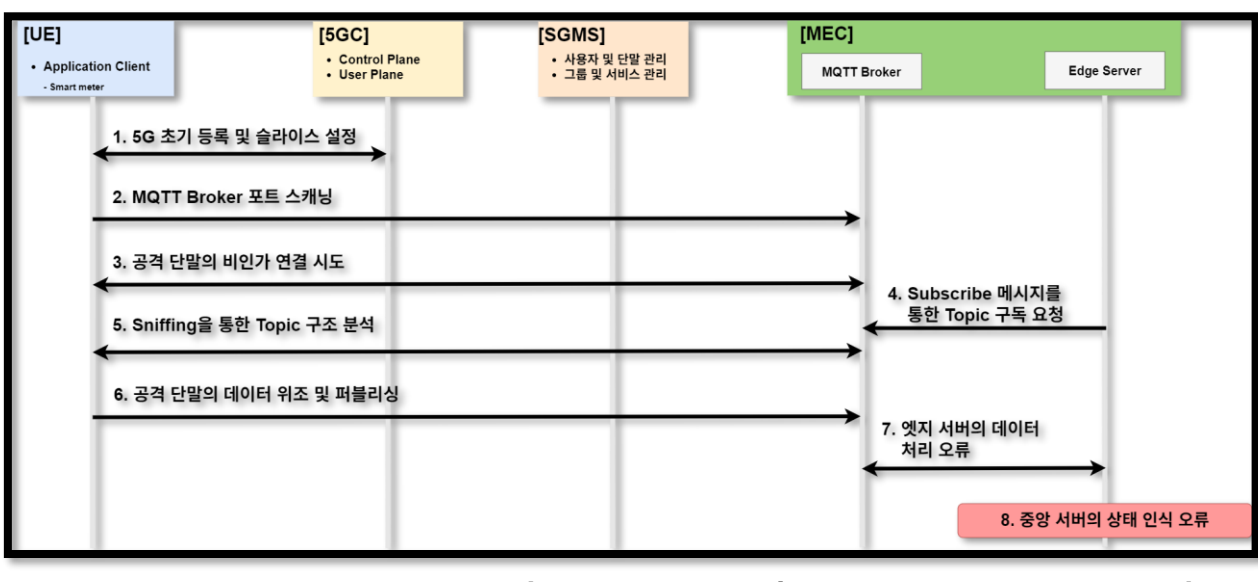


그림 5. MQTT Broker 보안 취약점을 이용한 데이터 위조 공격 절차

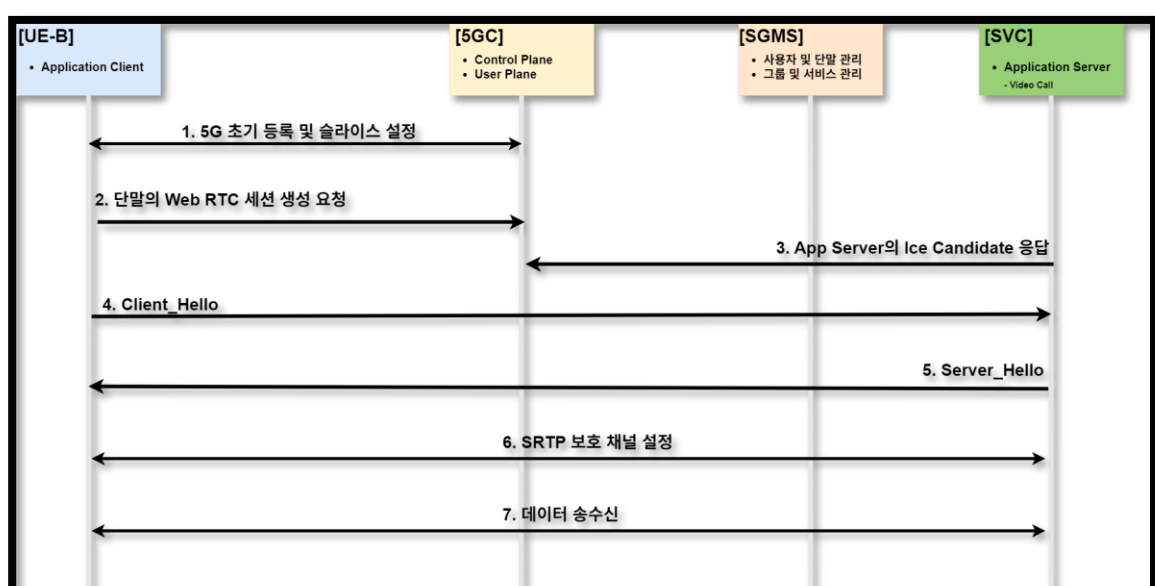


그림 6. Web RTC 기반 DTLS 정상 세션 수립 절차

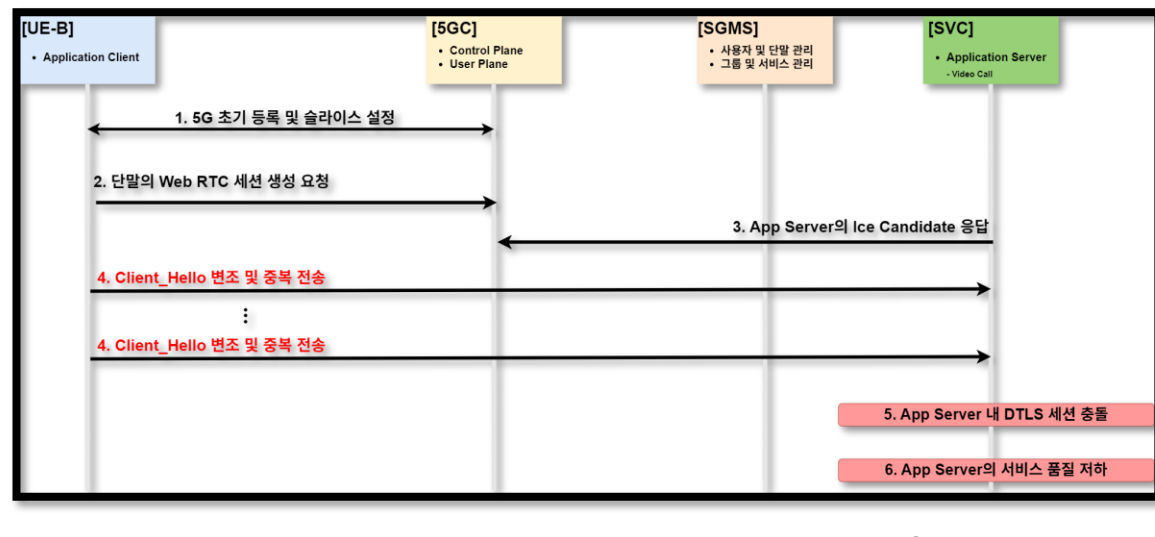


그림 7. Web RTC 기반 DTLS 공격 절차

참고 문헌

- [1] 3GPP, 5G System Overview (5GS), <https://www.3gpp.org/technologies/5g-system-overview>
- [2] VIAVI Solutions, 5G Network Slicing Explained, <https://www.viavisolutions.com/en-us/5g-network-slicing>
- [3] 3GPP News, SA5: 5G Network Slicing and Management, <https://www.3gpp.org/news-events/3gpp-news/sa5-5g>
- [4] 3GPP, Slice Management, <https://www.3gpp.org/technologies/slice-management>
- [5] ETSI, Potential Treats to 5G Network Slicing