# 네트워크 슬라이싱 기반 서비스의 보안 리질리언스 방안

김용환, 조원석, 김영재
트렌토 시스템즈
{yhkim, wsjo, yjkim}@trento.co.kr

# Security Resilience Strategies for Network Slicing-Based Services

Yong-hwan Kim, Wonseok Cho, Youngjae Kim
Trento Systems

요 약

본 연구는 5G+/6G와 Wi-Fi 융합 환경에서 발생하는 이동성, 수요 변동, 보안 위협에 대응하기 위해 네트워크 슬라이싱 기반 보안 리질리언스 아키텍처를 제안한다. 핵심 아이디어는 네트워크 슬라이스 변경 구간만 선별적으로 수정하는 Fine-grained 슬라이스 갱신으로 무중단 서비스와 신속 재구성을 보장하고, 단말 이동 시 사전-확장 → 즉시 전환 → 변경 구간 정리 절차를 수행하는 이동성-인지 핸드오프로 세션 연속성과 성능을 유지하는 것이다. 여기에 정책 기반 오토-스케일링과 제어평면 이중화를 결합해 자원 경쟁 상황에서도 네트워크 성능·격리 유지라는 KPI를 충족한다. 이러한 접근은 자율주행·스마트팩토리·XR 등 차세대 응용 서비스에 적용 가능하며, 보안성과 안정성을 동시에 강화할 것으로 기대한다.

## Ⅰ. 서 론

5G+/6G와 Wi Fi가 공존하는 통합 네트워크 환경에서 서비스는 이동성, 수요 급변, 보안 위협이 동시에 발생하는 환경을 전제로 설계되어야 한다. 이는 사용자가 이동 중이거나 여러 네트워크 기술이 공존하는 시나리오에서 특히 중요하며 다양한 네트워크 환경에서 안전하고 중단 없는 통신, 데이터 전송 및 서비스 액세스를 가능하도록 한다[1]. 이러한 조건에서 네트워크 슬라이싱은 서비스별 성능을 보장하는 핵심 수단이지만, 슬라이스가 자주 갱신·확장·축소되어야 하는 현실을 고려하면, 슬라이스의 연속성과 사이버보안 리질리언스(Resilience)를 체계적으로 확보하는 방법론이 필요하다.

네트워크 슬라이싱 기술은 5G+/6G 서비스의 높은 대역폭, 빠른 연결성, 낮은 지연 시간 등을 필요로 하는 5G 네트워크 다양한 요구사항을 충족시키기 위해 중요하다. 가령 IoT, 자율주행 차량, 가상 현실과 같은 서비스는 네트워크의 높은 유연성과 성능을 요구한다. 이에 따라, 네트워크 슬라이싱 기술은 다양한 네트워크 요구사항을 충족시키면서 효율적으로 네트워크 자원을 할당하고 관리하는 방안을 제공해야 한다[2].

이에 따라, 본 논문에서는 Fine Grained 슬라이스 갱신 및 이동성 인지 핸드오프 과정을 통한 네트워크 슬라이싱 기반 서비스의 사이버보안 리질리언스 방안을 제시하고자 한다. 본 방안을 통하여 네트워크 슬라이스의 생성·운영·갱신 전 주기에 걸친 무중단 운영과 엄격한 네트워크 통신 격리를 통한 보안성 확보를 목표로 한다.

현행 운영 방식은 새로운 요구가 발생하면 기존 슬라이스를 제거하고 재생성하는 절차가 일반적이어서, 갱신 시간이 생성 시간과 큰 차이가 없고 응용 트래픽에 불연속을 유발할 소지가 있다. 또한 6G가 지향하는 통합 인프라에서는 Wi Fi AP 간 핸드오프가 액세스 스위치 변경을 동반하는 경우까지 고려되어야 하나, 기존 핸드오프는 동일 액세스 네트워크 내부 이동을 주 대상으로 삼아 세션 연속성을 담보하기 어렵다. 또한 다수 슬라이스 간 자원 경쟁 상황에서도 우선순위·정책에 따라 신속·공정하게 자원을 재조정하는 체계가 요구된다. 요컨대, 정적·수동 중심의 슬라이싱은 동적·다변화된 서비스 요구를 감당하기에 한계가 분명하다. 즉, 수동적이고 정적인 네트워크 슬라이싱 기술로는 실시간으로 다변화하는 다양한 네트워크 요구사항들을 충족시키는 데 한계가 있으며, 동적이고 자동화된 네트워크 슬라이싱 방안이 필요하다.

## Ⅱ. 본론

본 연구가 제안하는 기본 방향은 세 가지다. 첫째, Fine grained 선별적(Selective) 슬라이스 갱신으로 변경 대상 구간만 제거·추가하고, 그 외 기존 단말/응용 간 통신은 영향을 받지 않도록 보장한다. 둘째, 이동성 인지 핸드오프를 통해 단말 이동이 예측되면 이동 후 경로를 사전 확장하고 이동 직후 이전 경로만 제거하여 지연을 줄인다(액세스 스위치 변경을 수반하는 Wi Fi AP 간 이동 포함). 셋째, 정책 기반 오토 스케일링으로 우선순위에 따라 대역폭·경로·큐를 자동 조정하며, 관리 클러스터 이중화와 마스터/슬레이브 권한 마이그레이션으로 제어평면 가용성을 확보한다. 이 모든 동작은 SDN 표준 인터페이스를 통해 자동화되어 서비스 허용 범위 내에서 수행된다.

사이버보안 리질리언스 아키텍처의 주요 설계 원칙은 다음과 같다:

- 격리 우선(Underlay based Isolation): 물리/논리적으로 분리된 경로·자원으로 슬라이스 경계를 형성하여 낮은 보안 등급 슬라이스를 통한 수평 이동을 차단. 모든 갱신·복원은 해당 슬라이스 내부에서 국소적으로 수행
- 무영향 통신 유지: 갱신 대상(제거·추가) 구간을 제외한 기존 슬라이스 단말/응용 간 통신은 중단 없이 유지되어야 함
- 시간·성능 제약 준수: 갱신 절차는 서비스 허용 범위 내에서 완료되며, 지연·대역폭 성능 목표를 슬라이스 전용 경로로 보장해야 함
- 제어평면 내결함성: 관리 클러스터 이중화 및 마스터/슬레이브 권한 마이그레이션으로 제어면 가용성을 확보해야 함

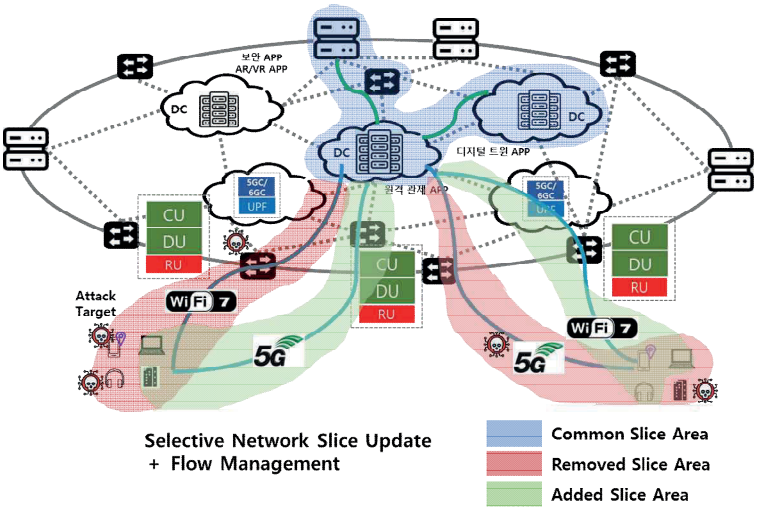


그림 1. 네트워크 슬라이싱 기반 서비스의 보안 리질리언스 시나리오

기존 운영은 슬라이스 요구가 바뀔 때 슬라이스 전체를 제거 후 재생성하는 방식이 일반적이라 생성과 갱신의 비용이 비슷하고, 응용 트래픽이 일시 중단될 위험이 크다. 이에 본 논문에서는 선별적 갱신으로 변경 대상만 해제·추가하고, 나머지 단말/응용 간 통신은 그대로 유지해 연속성을 확보한다. 운영자는 슬라이스의 단말/응용 요구를 손쉽게 추가/제거할 수 있고, 시스템은 그 차이를 자동 계산해 국소 갱신을 수행한다.

- 제거 Case: 네트워크 슬라이스 내에서 제거될 단말/응용서비스를 찾아 그들과 관련된 네트워크 자원을 네트워크 슬라이스에서 해제하는 것을 포함. 요청된 슬라이스 단말/응용서비스 집합과 이전 슬라이스 단말/응용서비스 집합을 비교하여 수행, 해당 과정은 슬라이스 재구성 과정에서 불필요해진 단말/응용서비스를 제거하고, 이에 사용되던 네트워크 자원을 해제함으로써, 자원의 효율적인 재할당과 네트워크의 유연성을 보장하는 데 기여
- 추가 Case: 새로운 사용자 요구사항을 지원하기 위해 슬라이스에 추가될 단말/응용서비스 집합을 식별하고, 이들에게 필요한 네트워크 자원을 할당, 해당 과정은 슬라이스가 새로운 사용자 요구사항에 유연하게 대응할 수 있도록 해주며, 슬라이스의 동적인 갱신을 가능하게 함

6G가 지향하는 통합 인프라에서는 Wi Fi·5G 환경 전반에서 단말 이동에 따른 AP 간 핸드오프가 빈번하며, 특히 액세스 스위치가 바뀌는 시나리오가 발생한다. 전통적 핸드오프는 동일 액세스 네트워크 내부 이동을 가정해 세션 연속성 확보와 지연 최소화에 한계가 있다. 따라서 네트워크 슬라이싱 기반 이동성 관리와 플로우 제어를 결합해, 변경되는 경로만 선택적으로 조정하는 Fine grained 슬라이스 갱신과의 연계가 필요하다.

이를 위하여 단말의 이동 예측을 활용해, 이동 이전에 슬라이스 경로를 이동 후 경로까지 사전 확장하고, 이동 즉시 새로운 경로로 전환한 뒤, 이동 이후 기존 경로만 제거하는 3단계를 구성한다. 이를 통하여 핸드오프 지연을 최소화하면서도 기존 통신의 불연속을 방지한다. 모든 조작은 SDN 표준 인터페이스를 통해 슬라이스 단위로 자동화된다.

- 준비(Prepare): 이동 징후(RSSI·AP 리포트·단말 이벤트)를 수집해 영향 슬라이스를 지정하고, 예상 목적지 AP·액세스 스위치를 확정. 전환 지연을 줄이기 위해 이동 후 경로까지 슬라이스를 사전 확장하고 플로우를 선 설치하며, 단말 ARP·컨트롤러 단말 정보를 미리 동기화. 액세스 스위치가 바뀌는 경우에도 새 스위치 방향으로만 증분 확장
- 전환(Switch over): 단말이 새 AP에 연동되는 즉시 사전 설치 플로우를 활성화하고 슬라이스의 QoS/대역폭 정책을 적용. 전환 직후 E2E 지연·가용 대역폭 등 KPI 충족 여부를 확인하고, 기준 미달이면 해당 슬라이스만 국소적으로 보정
- 정리(Clean up): 전환이 안정화되면 이전 경로 중 변경된 구간의 스위치들만 플로우를 제거해 정리하고, 공유 링크·큐 등 자원은 유지해 불필요한 영향 확산을 방지. 이어서 갱신 시간·격리 위반·지연·대역폭을 점검하고, 편차가 있으면 대역폭·큐·경로를 증분 조정해 목표값에 수렴시킴.

이러한 사이버보안 리질리언스 프레임은 기술·산업적 측면에서도 필요성이 높다. 기술적으로는 자율주행·스마트팩토리·AR/VR/XR 등 고대역·저지연·고신뢰를 요구하는 5G+/6G 응용이 확산되는 가운데, 슬라이스 수준에서 종단 간 전용 경로 보장과 유연한 자원 관리가 필수다. 산업적으로는 비면허 대역 활용과 소프트웨어 기반 자동화를 통해 운영비용(OPEX)과 라이선스 비용을 줄이고, 수요 변화에 신속 대응함으로써 서비스 경쟁력을 높일 수 있다. 또한 선택적 재구성과 슬라이싱 기반 핸드오프로 새로운 비즈니스 기회(모빌리티, 디지털 트윈, 메타버스 등)를 창출할 수 있다.

## Ⅲ. 결론

본 논문은 네트워크 슬라이싱 기반 서비스의 보안 리질리언스를 위해, Fine grained 슬라이스 갱신, 이동성 인지 핸드오프 아키텍처와 운영 절차를 제안했다. 특히 슬라이스 관점의 선택적 재구성 알고리즘은 전체 재생성 대비 재구성 시간을 크게 줄여 실시간 방어·복구의 실효성을 높이고자 한다. 향후 과제로는 공격 탐지 갱신 연계의 정량적 최적화, 이동 예측 정확도 향상과 사전 확장 정책의 과최적화 방지, 다중 도메인 간 슬라이스 연동 표준화 연계 등이 있다.

## ACKNOWLEDGMENT

본 연구는 2025년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구 결과 임 (RS-2024-00460803, SW 딥테크 기술 글로벌 경쟁력 강화 사업)

## 참 고 문 헌

[1] 주소영, 김소연, 이일구. "차세대 무선통신 네트워크 기술 동향 및 보안 이슈 분석." 정보보호학회지 31.3 (2021): 51-59.

[2] 3GPP. "Service requirements for the 5G system." Technical Specification (TS) 22.261 (2019).