5G 네트워크 슬라이싱별 성능지표와 보안 요구사항의 상관관계 분석

정유진, 나승준, 김환국 (국민대학교)

ICSR Intelligent Cyber Security Research Lab

I. 서론

5G 네트워크는 eMBB, mMTC, URLLC 서비스를 지원하기 위해 네트워크 슬라이싱 개념을 도입하였다. 이는 물리적 인프라를 가상 슬라이스로 분리하여 서비스별 성능 요구와 보안 정책을 독립적으로 적용하는 구조이다. eMBB는 10Gbps급 고속 전송, mMTC는 10^6 devices/km² 수준의 대규모 연결, URLLC는 1ms 이하 초저지연 등 다양한 성능 목표를 가진다. 그러나 고성능 환경에서도 다양한 보안 위협이 발생할 수 있으므로, 슬라이스 특성에 적합한 보안 요구사항을 충족하는 것이 중요하다. 본 연구는 3GPP 표준과 기존 연구를 기반으로 슬라이스별 성능지표와 보안 요구사항의 상관관계를 분석하고, 공통 및 차별화된 보안 특성을 도출하는 것을 목표로 한다.

II. 배경 지식

네트워크 슬라이싱은 SDN(Software Defined Networking)과 NFV(Network Function Virtualization) 기술을 기반으로 물리적 네트워크를 다수의 논리적 슬라이스로 분리하는 구조이다. 각 슬라이스는 제어 평면과 데이터 평면을 독립적으로 구성할 수 있어, 서비스별 요구에 따른 자원 관리 및 보안 정책 적용이 가능하다. 이러한 구조는 네트워크 자원을 효율적으로 활용할 수 있을 뿐만 아니라, 서비스 특성에 따른 맞춤형 품질 보장(QoS)을 제공한다. 또한 슬라이스 간 격리를 통해 특정 슬라이스의 장애나 공격이 다른 슬라이스로 확산되는 것을 방지하는 보안 메커니즘을 제공한다.

III. 성능지표 및 보안 요구사항

3.1 성능지표

eMBB, mMTC, URLLC는 서로 다른 서비스 요구를 충족하기 위해 설계된 슬라이스로, 성능 목표가 명확히 구분된다. eMBB는 고속 · 대용량 데이터 전송을 위해 최대 10Gbps급 속도와 99.9% 수준의 신뢰성을 제공하며, 초고화질 스트리밍 · VR · AR 등 고대역폭 서비스에 적합하다. mMTC는 제곱킬로미터당 최대 10^6개 이상의 기기가 접속하는 환경에서 저속 · 저전력 통신을 지원하며 스마트 시티 및 센서 기반 IoT 응용에 활용된다. URLLC는 1ms 이하의 초저지연과 99.999% 이상의 높은 신뢰성을 요구하는 실시간 제어 기반 서비스로, 자율주행 · 공장 자동화 · 원격 의료 등 산업 환경에 적용된다.

표 1 네트워크 슬라이싱별 성능지표

구분	eMBB	mMTC	URLLC
주요 목적	초고속 대역폭	초대규모 연결	초저지연, 초신뢰
지연	수 ms ~ 수십 ms	〈 100 ms	≤ 30 ms
신뢰성	약 99.9%	〉 99.9999%	99.999%
가용성	〉 99%	〉 99.9999%	99.9999%
데이터 속도	최대 1Gbit/s	〈 1Mbit/s	약 10 Mbit/s
연결 밀도	25만/km²	최대 100만/km²	1천/km²

3.2 보안요구사항

eMBB슬라이스별 보안 요구사항은 서비스 특성과 위협 모델에 따라 크게 달라진다. eMBB는 대용량 데이터 전송 과정에서 데이터 노출 위험이 높기 때문에 전송 및 저장 구간 모두에서 강력한 암호화가 요구된다. mMTC는 수많은 IoT 단말의 동시 인증 과정에서 부하가 발생할 수 있어, 경량 인증을 적용하는 것이 효과적이다. URLLC는 실시간 서비스 특성상 지연 증가가 치명적이므로 End-to-End 암호화와 저지연 인증이 필수적이며, 변조 · 재전송 공격에 대비한 무결성 · 가용성 보장이 중요하다.

표 2 슬라이스별 보안 요구사항

구분	eMBB	mMTC	URLLC
주요 위험	대용량 데이터 노출, 슬라이스 간 간섭	대규모 IoT 단말 침해, 인증 부하	지연 증가로 인한 실시간 서비스 중단, 변조, 재전송
암호화 적용 구간	전송, 저장	저장 중심	전송
암호화 강도	상	중	중~상
인증 방식	표준 인증	경량 인증	저지연 인증, 경량 인증
핵심 보안 속성	기밀성, 격리	무결성, 인증, 격리	무결성, 가용성

IV. 상관관계 분석

표 1의 성능지표와 표 2의 보안 요구사항을 비교한 결과, 각 슬라이스의 성능 특성은 보안 속성의 우선순위에 직접적인 영향을 미치는 것으로 나타났다. eMBB는 최대 1Gbit/s 수준의 높은 전송 속도와 낮은 지연 특성을 갖기 때문에 대용량 데이터 노출 위험이 높다. 이에 따라 전송 및 저장 구간에서의 강력한 암호화와 기밀성 확보가 필수적이며, 약 25만 단말/km² 환경에서는 슬라이스 간 간섭을 방지하기 위한 논리적 격리가 요구된다. 즉, eMBB의 초고속 · 대역폭 중심 특성은 기밀성 및 격리 강화가 핵심 보안 요구로 이어진다.

mMTC는 제곱킬로미터당 최대 100만 단말이 접속하는 초대규모 연결 환경을 가지며, 낮은 데이터 속도와 100ms 이하의 지연 특성을 특징으로 한다. 단말 수가 매우 많기 때문에 인증 과정에서의 부하가 전체 성능 저하로 이어질 수 있어, 확장 가능한 경량 인증 방식이 필요하다. 또한, 99.999% 이상의 가용성을 유지하기 위해 구독자 데이터 및 저장 정보를 HSM 기반 암호화로 보호하여 무결성을 확보해야 한다. HSM은 키 생성 · 저장 · 서명 연산을 안전하게 처리하는 전용 하드웨어로, 슬라이스 간 자격 정보 노출을 구조적으로 차단하며 서비스 연속성을 보장한다. 이러한 이유로 mMTC는 인증 · 무결성 중심의 보안 요구가 강조된다.

URLLC는 30ms 이하의 초저지연과 99.9999% 이상의 초신뢰성을 요구하는 실시간 제어형 서비스이다. 보안 검증 과정이 지연 증가로 이어지면 서비스 품질이 훼손되므로, 저지연 인증과 경량화된 무결성 검증이 필요하다. 자율주행 · 원격제어 · 공장 자동화 등 안전과 직결되는 서비스 특성상 단일 장애가 치명적 사고를 야기할 수 있기 때문에, 높은 수준의 가용성 보장 또한 필수적이다. 이에 따라 URLLC는 무결성과 가용성 중심의 보안이 요구된다.

종합적으로, 각 슬라이스의 성능 특성은 적용해야 할 보안 속성의 방향성과 수준을 결정하는 핵심 요인으로 작용하며, 이러한 분석 결과는 표 3에 정리되어 있다.

표 3 슬라이스 성능지표(KPI)와 보안 속성 간 상관성

구분	eMBB	mMTC	URLLC
데이터 속도	상	하	하
지연시간	하	중	상
신뢰성	하	중	상
연결밀도	하	상	중

V. 결론

본 연구는 5G 네트워크 슬라이싱 환경에서 성능지표와 보안 요구사항의 상관관계를 분석하였다. 분석 결과, eMBB는 기밀성, mMTC는 무결성과 인증, URLLC는 가용성이 핵심 보안 요소로 도출되었으며, 이는 슬라이스별 성능 특성이 보안 요구의 우선순위를 결정함을 보여준다. 따라서 5G 보안은 슬라이스 특성을 고려한 차등적 설계가 필요하며, 향후에는 KPI 기반의 정량적 평가와 성능 저하를 최소화하는 보안 프레임워크 연구가 요구된다.

Acknowledgement

논문은 2025년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구 결과임. (No.RS-2024-00438156, 5G특화망 · 유 · 무선 통합환경에서 네트워크 슬라이싱 기반서비스의 보안 리질리언스 기술 개발)

Reference

[1] 3GPP TS 23.501, System architecture for the 5G System (5GS), v18.9.0, 3rd Generation Partnership Project, Apr. 2025.
[2] 3GPP TS 22.261, “Service requirements for the 5G system; Stage 1,” v17.10.0, 3rd Generation Partnership Project, Jun. 2024.
[3] 3GPP TS 22.104, Service requirements for cyber-physical control applications in vertical domains, v18.4.0, 3rd Generation Partnership Project, Jul. 2024.
[4] CISA & NSA, 5G Network Slicing: Security Considerations for Design, Deployment, and Maintenance, ESF, 2023.