전자통신동향분석, 41권 4호 2026, 107-120

5G특화망·유·무선 통합환경에서 네트워크 슬라이싱 기반 보안 리질리언스 기술 동향

Technology Trends of Security Resilience based on Network Slicing in Converged Private 5G Networks

이훈기 (H.K. Lee, lhk@etri.re.kr) 지능형네트워크보안연구실 책임연구원
김정태 (J.T. Kim, jungtae_kim@etri.re.kr) 지능형네트워크보안연구실 책임연구원/기술총괄
신용윤 (Y.Y. Shin, uni2u@etri.re.kr) 지능형네트워크보안연구실 책임연구원
김현진 (H.J. Kim, be.successor@etri.re.kr) 지능형네트워크보안연구실 선임연구원
김국진 (K.J. Kim, kjkim23@etri.re.kr) 지능형네트워크보안연구실 선임연구원
박종근 (J.G. Park, queue@etri.re.kr) 지능형네트워크보안연구실 책임연구원

ABSTRACT

As digital transformation continues accelerating, the demand for Private 5G networks is growing rapidly across industries, including smart factories, autonomous vehicles, and digital healthcare. This paper systematically investigate security resilience technologies for network slicing-based services in environments where Private 5G networks, converged wired/wireless infrastructures, and Non-3GPP access technologies are integrated. This study provides a comprehensive analysis of slicing architecture structures and roles, threat models and attack scenarios, countermeasure technologies, case studies from domestic and international enterprises and research institutions, standardization and policy trends, and future research directions, with the goal of contributing to both academic research and practical implementation.

KEYWORDS Private 5G, Converged wired/wireless, Network Slicing, Non-3GPP Access, Security Resilience

I. 서론

디지털 전환이 빠르게 진행됨에 따라 다양한 산업 분야에서 실시간성, 고신뢰성, 대규모 연결성을 요구하는 통신 수요가 증가하고 있다. 특히, 스마트 팩토리, 스마트시티, 자율주행, 디지털 헬스케어 등은 고도의 통신 안정성과 보안성을 전제로 하는 서비스들이며, 이를 구현하기 위한 기반 인프라로서 5세대 이동통신(5G: The Fifth Generation) 기술이 중심에 있다.

* DOI: https://doi.org/10.22648/ETRI.2026.J.410411
* 이 논문은 2026년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구 결과임[RS-2024-00438156, 5G특화망·유·무선 통합환경에서 네트워크 슬라이싱 기반 서비스 보안 리질리언스 기술개발].

이러한 환경에서 5G특화망(Private 5G)은 고유의 물리적 또는 가상 네트워크를 통해 특정 조직이나 산업 현장에서 요구하는 통신 요건을 충족시키기 위한 독립적 네트워크 인프라로 주목받고 있다. 특히, 유 · 무선 통합환경에서는 3GPP(3rd Generation Partnership Project) 기반의 모바일 기술뿐만 아니라 Wi-Fi, Zigbee, LoRa 등과 같은 Non-3GPP 접속 기술의 통합적 운용이 필수적으로 요구되며, 이를 통해 다양한 기기와 응용서비스가 유기적으로 연결되는 환경을 조성할 수 있다.

이러한 복합 네트워크 환경을 효율적으로 운영하기 위해서는 네트워크 슬라이싱(Network Slicing) 기술이 필요하다. 이 기술은 물리적 네트워크를 기반으로 다수의 논리적 네트워크를 생성하고, 각각의 슬라이스에 서비스 특성에 맞는 보안 정책과 QoS(Quality of Service)를 적용함으로써 다중 서비스를 동시에 안정적으로 제공할 수 있게 한다. 그러나 슬라이싱 구조는 그 유연성만큼이나 보안 측면에서는 새로운 위협 벡터가 될 수 있으며, 이에 대한 대비로서 보안 리질리언스(Security Resilience) 기술이 핵심 이슈로 떠오르고 있다[4,18].

본고에서는 5G특화망과 유 · 무선 통합환경, Non-3GPP 접속 기술이 융합된 구조 내에서 네트워크 슬라이싱 기반 서비스의 보안 리질리언스 기술에 대해 고찰하고자 한다. 구체적으로는 기술적 개념, 보안 위협 모델, 실제 대응 기술, 기업과 연구기관의 적용 사례, 관련 표준화 및 정책 흐름, 특히, 네트워크 슬라이싱 기반의 보안 리질리언스 제안 시스템을 소개하고자 한다.

II. 5G특화망과 유·무선 통합환경의 이해

1. 5G특화망의 개념과 구축 유형

5G특화망은 상용 이동통신망과는 달리 특정 조직이 독립적으로 구축하고 운영하는 전용 네트워크를 의미한다. 이러한 특화망은 일반적으로 고도화된 보안 요구사항, 낮은 지연 시간, 높은 신뢰성과 같은 요건을 만족해야 하며, 이를 위해 별도의 주파수 대역과 장비를 활용한다. 국내의 경우 자체 5G 특화망을 통해 스마트제조 및 물류, 스마트시티, 병원 · 의료, 국방 · 재난 등 다양한 분야에서 고유의 독립망을 구축하고, 특정 단말과의 연동을 통한 서비스 운용에 활용되고 있다[11,19].

특화망의 구축 유형은 표 1과 같이 크게 세 가지로 구분된다.

- **독립형(Standalone):** 전용 RAN(Radio Access Network)과 코어 장비를 현장에 설치하여 완전히 독립적으로 운용하는 방식임. 보안성과 신뢰성이 가장 높으나 초기 투자 비용 소요됨
- **공공망 연동형(NPN-PNI: Non-Public Network with Public Network Integration):** 상용 통신망의 일부 기능을 임차하면서 코어만 분리 운용하는 형태임
- **가상화 기반 특화망(Virtualized Private 5G Network):** 클라우드 기반의 가상 코어를 활용하여 유연하게 운용하는 방식으로 소규모 기업에 적합함

표 1 5G특화망 구축 유형 비교

구축 유형	특징	보안성	비용	적합 규모
독립형 (Standalone)	전용 RAN+Core, 완전 독립 운용	매우 높음	높음	대기업·공공
공공망 연동형 (NPN-PNI)	상용망 기능 임차, Core 분리	높음	중간	중견기업
가상화 기반 (vPN)	클라우드 가상 코어 활용	중간	낮음	중소기업·스타트업

2. 유·무선 통합환경과 Non-3GPP 접속 기술

유 · 무선 통합환경은 유선 네트워크와 무선 네트워크를 동일한 관리 체계하에서 통합적으로 운영하는 구조를 의미한다. 이 환경에서는 5G 이동망 기술은 물론, Wi-Fi · WLAN 계열과 IoT 연결용 Bluetooth, Zigbee, LoRa 등 다양한 접속 기술이 함께 활용된다. 특히, Non-3GPP 접속 기술은 비용 효율성과 구축 용이성을 바탕으로 많은 IoT 환경에서 채택되고 있다.

이러한 접속 기술들을 5G Core와 연동시키기 위해서는 N3IWF(Non-3GPP Inter-Working Function)와 같은 중간 게이트웨이 기능이 필요하며, 이를 통해 단말 인증, 암호화된 통신, 정책 제어 등을 가능하게 한다. 3GPP Release 16 이후부터는 Untrusted Non-3GPP Access뿐만 아니라 Trusted Non-3GPP Access도 지원하는 TNGF(Trusted Non-3GPP Gateway Function)가 도입되어, 유 · 무선 통합환경의 보안 연동 수준이 한층 높아졌다. 최근 국내 대학 및 연구기관들은 스마트 캠퍼스 고도화를 위해 기존의 Wi-Fi 인프라에 5G특화망을 결합한 복합망을 적극 도입하고 있으며, 네트워크 슬라이싱 기술을 적용해 AR · VR 기반 스마트 강의실, 대용량 연구데이터 전송, 지능형 통합 관제 시스템 등 서비스별 요구사항에 최적화된 독립적 논리망을 운용하는 추세이다[15].

III. 네트워크 슬라이싱 기술

1. 네트워크 슬라이싱 구조 및 역할

1.1 슬라이싱 아키텍처 개요

네트워크 슬라이싱은 하나의 물리적 네트워크 인프라 위에서 서로 다른 요구 조건을 갖는 논리적 네트워크를 다수 생성할 수 있는 기술이다. 이 구조는 마치 하나의 고속도로에 다양한 목적지로 향하는 차량이 각기 다른 전용 차선을 이용하는 것과 같은 개념으로 설명할 수 있다. 각 슬라이스는 특정한 트래픽 패턴(데이터 유형), 보안 정책, 대역폭 요구를 갖는 서비스에 맞추어 최적화되어 제공된다.

슬라이스는 일반적으로 RAN 슬라이스, 전송망 슬라이스, 코어 슬라이스, 그리고 경우에 따라 MEC(Multi-access Edge Computing)나 응용서비스 레벨에서의 슬라이스까지 포함된다. 각 구성 요소는 분리된 정책과 자원 관리 체계를 갖추고 있으며, 이러한 구조는 SDN/NFV(Software Defined Networking/Network Functions Virtualization) 기반의 네트워크 오케스트레이션 시스템을 통해 제어된다. ETSI MANO 아키텍처에 기반하여, 슬라이스 생성, 배포, 확장, 복구 등 생명주기 전반에 걸친 관리가 가능하게 설계되고 있다[1,11].

1.2 슬라이싱 유형별 특성

3GPP 규격에서 정의한 표준 슬라이스 유형은 표 2와 같이 초광대역 서비스인 eMBB(Enhanced Mobile Broadband), 초고신뢰 · 저지연 통신의 URLLC(Ultra-Reliable Low Latency Communication), 대규모 사물통신의 mMTC(Massive Machine Type Communication)

표 2 네트워크 슬라이스 유형별 특성 비교

슬라이스 유형	적용 예시	목표 지연	신뢰성	연결 밀도	보안 중점
eMBB	HD 스트리밍, VR/AR	~10ms	중간 (99%)	낮음	콘텐츠 암호화
URLLC	원격제어, 자율주행	~1ms	매우 높음 (99.9%)	낮음	무결성·가용성
mMTC	스마트 센서망	~수 초	중간	매우 많음 (100만/km²)	경량 인증
Industrial Slice	스마트 팩토리, AMR	<5ms	높음 (99.99%)	중간	물리적 격리

로 구분된다. 최근 5G특화망 환경에서는 이러한 표준 SST(Slice Service Type) 외에도, 스마트팩토리나 의료 인프라 등 특정 산업별 요구사항을 충족하기 위한 산업 전용 슬라이스(Industrial Slice) 및 V2X 등 특수 목적 슬라이스가 확장되어 적용되는 추세이다[1,11].

1.3 슬라이싱 관련 핵심 기능 요소

5G 네트워크 슬라이싱 구현을 위한 핵심 요소는 크게 식별 체계, 제어 기능, 그리고 관리 기능으로 구분할 수 있으며, 그 세부 역할은 다음과 같다.

- **슬라이스 식별(S-NSSAI: Single Network Slice Selection Assistance Information):** 특정 슬라이스를 식별하는 정보로, 서비스 특성을 정의하는 SST와 이를 구분하는 SD로 구성됨. 5G 특화망에서는 주로 이 값을 기반으로 트래픽과 서비스를 분배함
- **슬라이스 선택(NSSF: Network Slice Selection Function):** 단말의 접속 요청 시, 요구사항에 맞는 최적의 네트워크 슬라이스 인스턴스(NSI)를 선택하고 연결을 중재함
- **슬라이스 인스턴스(NSI: Network Slice Instance):** 물리적 네트워크 자원 위에 특정 서비스 요구사항을 충족하도록 논리적으로 구성된 실제 운용 단위임
- **생명주기 관리(NSMF & NSSMF):** NSMF(Network Slice Management Function)와 NSSMF(Network Slice Subnet Management Function)는 네트워크 슬라이스의 생성, 수정, 폐기에 이르는 End-to-End 생명주기 관리를 총괄함

통상적인 통신사업자의 5G특화망 구축 환경에서는 주로 이 SST 및 SD 값을 기준으로 네트워크 자원을 할당하고 서비스를 분배한다.

2. 보안 리질리언스 개념과 기술적 접근

2.1 보안 리질리언스 정의와 구성 요소

보안 리질리언스(SR: Security Resilience)는 단순히 위협을 탐지하고 방어하는 것을 넘어, 보안 사고 발생 이후에도 서비스의 연속성을 유지하고 빠르게 정상 상태로 복원할 수 있는 능력을 포함한다. 이는 기존 보안 시스템이 주로 사전 예방과 방어에 초점을 두고 있었던 데 반해, 사고 발생 후의 대처 능력과 회복 과정까지 포함하는 더 확장된 개념이다. NIST에서는 사이버 리질리언스를 “사이버 위협 및 공격을 예측(Anticipate)하고 저항(Withstand)하며, 피해로부터 신속히 회복(Recover)하고 환경 변화에 적응(Adapt)함으로써 사이버 자원에 의존하는 미션 및 비즈니스 기능을 지속하는 능력”으로 정의하고 있으며[4], 보안 리질리언스를 구성하는 핵심 단계는 다음과 같다.

- 첫째, 예방(Prevent) 단계에서는 사전에 위험 요인을 식별하고 위협을 차단하기 위한 정책 설정과 접근 제어가 이루어짐
- 둘째, 탐지(Detect) 단계에서는 이상 징후를 조기에 감지할 수 있는 트래픽 분석, 로그 수집, 사용자 행위 모니터링이 수행됨
- 셋째, 대응(Respond) 단계에서는 실제 위협이 발생했을 때 시스템이 이를 자동으로 차단하거나 슬라이스 단위로 격리하여 피해 확산을 차단함
- 넷째, 복구(Recover) 단계에서는 중단된 서비스를 최소한의 시간 내에 재구성하거나 재배치하여 서비스 가용성을 확보하는 절차를 수행함
- 다섯째, 적응(Adapt) 단계에서는 사건 발생 이후 수집된 정보를 기반으로 정책을 개선하고, AI 기반으로 위협 모델을 진화시킴으로써 유사한 사고 재발을 방지함

2.2 슬라이싱 구조와 보안 리질리언스 내재화

보안 리질리언스는 네트워크 슬라이싱 구조와 결합할 때 더욱 효과적인 방어 체계를 구성할 수 있다. 슬라이싱의 논리적 분리 구조를 활용하여 슬라이스 단위로 보안 정책을 다르게 적용하고, 침해가 의심되는 슬라이스를 신속하게 격리하는 방식으로 피해 범위를 최소화할 수 있기 때문이다. 즉, 슬라이싱 구조 자체에 보안 리질리언스 기능이 깊숙이 스며들어 본연의 기능처럼 작동하도록 설계할 수 있다.

구체적으로, URLLC 슬라이스에는 무결성 · 가용성 중심의 엄격한 정책을, eMBB 슬라이스에는 기밀성 중심의 정책을 차별화하여 적용할 수 있다. 또한, 슬라이스별 독립적인 보안 감사 로그(Audit Log)와 이상 탐지 엔진을 운용함으로써 하나의 슬라이스에서 발생한 침해가 전체 네트워크로 확산되는 것을 방지하는 "보안 격벽(Security Bulkhead)" 효과를 얻을 수 있다. 이는 마이크로 세그멘테이션 기법과 결합하면 더욱 세밀한 보안 경계를 구현할 수 있다.

2.3 제로 트러스트 아키텍처와의 연계

제로 트러스트 아키텍처(ZTA: Zero Trust Architecture)는 "신뢰하지 말고, 항상 검증하라(Never Trust, Always Verify)"라는 원칙을 기반으로 하며, 5G특화망 슬라이싱 환경에서의 보안 리질리언스 강화에 핵심적인 역할을 담당한다. ZTA에서는 모든 접속 요청에 대해 사용자 신원, 디바이스 상태, 네트워크 위치와 무관하게 지속적인 검증을 수행하며, 최소 권한 원칙(Principle of Least Privilege)에 따라 접근 권한을 부여한다.

5G 슬라이싱 구조에 ZTA를 내재화할 경우, 슬라이스 간 이동성(Inter-slice Mobility) 환경에서도 끊김 없는 인증 · 인가 정책의 적용이 가능하다. 무엇보다 "기기 무결성 및 보안 상태(Device Posture)"를 지속적으로 검증하는 접속 제어 메커니즘은 취약한 IoT 기기가 대량 수용되는 mMTC 슬라이스 환경에서 필수적인 보안 요소로 작용한다.

2.4 클라우드 네이티브 환경의 보안 강화 방안

5G특화망의 네트워크 기능들이 클라우드 기반 소프트웨어 형태로 구현되고, Non-3GPP 기기(Wi-Fi 등 WLAN 계열)의 연동 기능과 IoT 게이트웨이를 통해 유입되는 Zigbee · LoRa 등 이기종 기기의 트래픽이 클라우드 환경에 함께 수용됨에 따라 새로운 보안 위협이 등장하고 있다. 소프트웨어로 구현된 네트워크 기능들은 서버 자원을 공유하는 특성상, Non-3GPP 연동 구간처럼 보안 수준이 상대적으로 낮은 접점을 통한 침투가 클라우드 내부 전체로 확산되는 경로가 될 수 있다.

이에 대응하기 위해 5G 코어를 수용하는 컨테이너 오케스트레이션(Kubernetes 등) 환경에 고도화된 보안 기제를 적용한다. 첫째, eBPF(extended Berkeley Packet Filter) 기반의 CNI 플러그인을 도입하여 슬라이스 간 트래픽 라우팅을 통제하고, 악성 트래픽 발생 시 패킷 드롭(Drop) 정책을 커널 수준에서 즉각 수행한다. 둘째, 런타임 보안 위협 탐지 엔진을 연동하여 네트워크 기능 내부에서 발생하는 비정상적인 권한 상승이나 쉘(Shell) 실행 시도를 실시간으로 차단한다. 셋째, 보안 요구 수준이 다른 3GPP 제어 평면 기능과 Non-3GPP 연동 기능은 서로 다른 전용 워커 노드(Dedicated Worker Node)에 격리 배치하고, 네임스페이스(Namespace)를 별도로 구성하여 위협의 전이 경로를 원천 차단한다.

클라우드 네이티브 기반 5G특화망에서 보안 리질리언스의 핵심은 침해 발생 시 서비스가 중단되지 않는 연속성 보장에 있다[10]. 특정 슬라이스에서 침해가 감지되면 해당 슬라이스를 즉시 격리하는 동시에 대체 슬라이스로 트래픽을 끊김 없이 전환하며, Kubernetes 오케스트레이터 및 통합 보안 제어 체계가 침해된 CNF(Cloud Native Network Func-

tion) 파드를 즉시 축출(Eviction)하고 자동 재배포(Automated Re-deployment)를 통해 신뢰 상태의 파드로 신속히 교체하며 대체 슬라이스의 용량을 탄력적으로 확장한다. 이 과정에서도 제로 트러스트 아키텍처와 연계하여 전환 대상 슬라이스에 대한 동일 수준의 접근 검증이 지속적으로 유지됨으로써 서비스 전환 자체가 새로운 보안 취약점으로 이어지지 않도록 철저히 통제한다[10].

3. 네트워크 모델 및 공격 시나리오

3.1 슬라이싱 기반 네트워크 위협 분류

슬라이싱 기반 네트워크에서는 전통적인 통신망보다 더 다양한 형태의 보안 위협이 발생할 수 있으며, 그에 따른 대응 전략도 정교하게 설계되어야 한다. 위협 유형은 크게 슬라이스 간 침투 공격, 서비스 거부 공격, 인증 우회, 내부자 공격, 패킷 위조 및 데이터 조작, 오케스트레이션 레이어 공격으로 분류할 수 있다[9,17].

슬라이스 간 침투 공격은 격리 정책이 제대로 설정되지 않았을 때 하나의 슬라이스에 침투한 공격자가 이를 발판 삼아 다른 슬라이스로 확산해가는 시나리오이다. 이는 내부망의 단일 접점(Attack Surface)이 침해된 후, 그 피해가 물리적 · 논리적으로 연결된 인접 도메인으로 연쇄 확산되는 현상과 같다. DoS/DDoS 공격은 슬라이스에 과도한 트래픽을 집중시켜 자원 고갈을 유도하는 형태이며, 특히 공유 RAN 자원을 가진 슬라이스 구조에서는 한 슬라이스에 대한 과부하가 다른 슬라이스의 QoS에도 영향을 줄 수 있다. 표 3은 위협 유형에 따른 슬라이싱 기반 네트워크 위협을 분석하고, 잠재적 영향과 대응 방안을 나타낸 것이며, 표 4에서는 분야별 슬라이스 구성 및 보안 위협, 리질리언스를 위한 동작 방안을 정리한 것이다.

표 3 슬라이싱 기반 네트워크 주요 위협 분석

위협 유형	공격 대상	공격 기법	잠재적 영향	대응 방안
슬라이스 간 침투	격리 정책 취약점	측면 이동 (Lateral Movement)	전체 서비스 중단	마이크로 세그멘테이션
DoS/DDoS	공유 RAN·Core 자원	트래픽 폭주, 자원 고갈	성능 저하, 서비스 중단	트래픽 쉐이핑, 슬라이스 격리
인증 우회	5G-AKA, EAP-AKA'	프로토콜 취약점 악용	무단 슬라이스 접근	다중 인증 (MFA), AMF[1] 강화
내부자 위협	MANO, 오케스트레이터	권한 남용, 설정 변경	탐지 어려움, 피해 큼	RBAC, 감사 로그
오케스트레이션 공격	NFVO, VNFM	API 취약점, 공급망 공격	슬라이스 전체 장악	API 보안, 코드 서명
Non-3GPP 접속 취약점	N3IWF, Wi-Fi AP	중간자 공격 (MITM)	트래픽 도청·조작	IPsec/TLS 강제화

1) AMF: Access and Mobility management Function

3.2 Non-3GPP 환경의 위협

Non-3GPP 접속 환경에서는 레거시 프로토콜(예: WPA2, BLE) 접속에 따른 한계로 인해 5G 코어 수준의 보안을 보장하기 어렵다. 이를 보완하기 위해 N3IWF 기반의 IPsec 터널링이 필수적으로 요구되지만, 터널 외부의 무선 구간 취약점은 여전히 존재한다[2]. 최근에는 고도화되는 네트워크 스니핑 및 데이터 탈취 공격에 대응하고자 IPsec 구간에 양자키분배(QKD: Quantum Key Distribution) 및 양자내성암호(PQC: Post-Quantum Cryptography) 기술을 접목하여 보안 리질리언스를 강화하는 연구가 활발히 진행되고 있다. 아울러 MEC 결합 환경에서는 에지 노드의 지리적 분산 특성으로 인해 물리적 공격에 대한 선제적 방어 방안도 함께 고려되어야 한다[3].

IV. 국내·외 기술 적용 사례

1. 국내 주요 사례

국내에서는 5G 슬라이싱 환경의 안전성 확보를

표 4 분야/유형별 보안 리질리언스 시나리오

유형	스마트제조	스마트물류	스마트시티	병원·의료	국방·재난
서비스 구성	• Slice 1(URLLC): 로봇 제어, PLC 제어 • Slice 2(eMBB): 공정 모니터링 영상 • Slice 3(mMTC): 센서/설비 상태 수집	• Slice 1(URLLC): 무인 크레인 제어 • Slice 2(eMBB): 관제 영상 • Slice 3(mMTC): 출입/자산 관리	• Slice 1: 긴급 통신(소방 · 경찰) • Slice 2: 교통 관제 • Slice 3: 공공 Wi-Fi	• Slice 1(URLLC): 원격 수술/의료 기기 • Slice 2(eMBB): 의료 영상 • Slice 3(mMTC): 환자 웨어러블	• Slice 1(URLLC): 지휘/작전 통신 • Slice 2(eMBB): 영상/드론 • Slice 3(mMTC): 센서/상황 정보
보안 위협 (공격)	• mMTC슬라이스에서 감염된 IoT 단말이 비정상 트래픽 발생	• 관제 영상 슬라이스에 DDoS/대량 Flooding 공격	• 공공 Wi-Fi 슬라이스에서 악성 단말 유입	• 의료 영상 서버 침해 시도 발생	• 특정 슬라이스에 대한 지능형 침투 공격
보안 리질리언스 동작	① AI 기반 IDS가 Slice 3 이상징후 탐지 ② 해당 슬라이스 트래픽 격리 ③ URLLC슬라이스(로봇 제어)는 무중단 유지 ④ 필요시 Slice 3을 자동 재생(Scale-out)	① eMBB슬라이스에서 트래픽 폭증 감지 ② 공격슬라이스에 Rate-limit/트래픽 차단 ③ 무인 크레인 제어 슬라이스는 QoS 보장 ④ 공격 종료 후 자동 복구	① 공공 Wi-Fi 슬라이스에서 이상 트래픽 탐지 ② 해당 슬라이스 즉시 격리 ③ 긴급 통신 슬라이스는 격리 영향 없이 완전 독립 운영 유지 ④ 보안 분석 후 정상 서비스 재개	① eMBB슬라이스에서 비정상 세션 탐지 ② 해당 세션/슬라이스 차단 ③ 의료 기기 슬라이스는 지연/패킷 손실 없이 유지 ④ 보안 이벤트 자동 보고	① 침해된 슬라이스를 논리적으로 격리 ② 작전 슬라이스는 우선 자원 재할당 ③ 필요시대체슬라이스 자동 생성 ④ 공격 종료 후 단계적 복구
시나리오 목적/가치	• OT/IT분리및침해확산 차단 • 생산 중단 없음 • 침해 확산 방지 • 서비스 연속성 보장	• 관제/운용 슬라이스 보호 • 핵심 운영 서비스 보호 • 공격 중에도 현장 운영 지속	• 공공안전서비스 보호 • 시민 안전 서비스 무중단 • 공공 인프라 신뢰성 확보	• 생명직결서비스 보호 • 생명 안전 보장 • 의료 서비스 신뢰성 강화	• 미션 수행 통신 보호 • 미션 지속성 확보 • 고가용성 · 생존성 보장

위해 AI 분석, 정책 자동화, 에지 보안 등 다양한 기술적 접근이 시도되고 있다[5].

- **지능형 위협 탐지 및 격리(삼성전자):** 삼성전자 스마트팩토리 환경에서 이기종 슬라이스(URLLC, eMBB) 간 자원 격리 및 AI 기반 트래픽 분석 체계를 적용함
- **보안 정책 자동화 및 오케스트레이션(ETRI):** ETSI ZSM(Zero-touch Service Management) 프레임워크 기반 슬라이스 생명주기 자동화 보안 관리 연구를 수행 중이며, 위협 탐지부터 자동 복구까지 아우르는 SDN/NFV 통합 플랫폼 시범망을 구성함
- **MEC 인프라 기반 현장 보안 실증(LG유플러스):** 5G MEC 보안 과제 참여를 통해 MEC 기반 산업현장에 침입 탐지 · 방지(IDS/IPS) 기술을 적용하고, 스마트팩토리 환경에서 에지 보안 체계 실증을 추진함

2. 해외 주요 사례

글로벌 5G 선도 기업들은 슬라이싱 보안 리질리언스를 달성하기 위해 자동화된 위협 대응, 제로 트러스트 접목, 전주기 컴플라이언스 관리 등의 기술을 상용망에 적극 도입하고 있다[12-14].

- **AI/ML 및 SOAR 연계 보안 제어 자동화(Nokia):** 'NetGuard Cybersecurity Dome' 플랫폼 내에 머신러닝 이상 탐지 엔진과 SOAR를 통합하여, 5G 슬라이싱 환경의 침해 위협을 신속히 감지하고 자동 복구하는 통합 보안 프레임워크를 상용 제공함
- **ZTA 기반의 세밀한 접근 제어 적용(Verizon):** 5G 슬라이스 접근에 Zero Trust 개념을 적용하여, 사용자 · 디바이스 인증 기반으로 슬라이스 단위 접근을 제어하는 모델을 구현함. NIST SP 800-207 프레임워크를 준수하는 Zero Trust

Dynamic Access 솔루션을 상용 제공함

- **생명주기 전반의 컴플라이언스 및 감사 관리 (Ericsson, Deutsche Telekom):** Ericsson은 'Ericsson Security Manager(ESM)'를 통해 네트워크 설정 변경 탐지, 보안 정책 자동화 및 컴플라이언스 모니터링을 지원하며 GSMA NESAS 기반 보안 감사 인증을 획득함. Deutsche Telekom은 Ericsson · Mavenir와 협력하여 E2E 5G 네트워크 슬라이싱에서 SLA 보장 기반 슬라이스 서비스를 상용 제공하고 슬라이스 생명주기 자동화 오케스트레이션을 구현함

표 5 국내외 기업·연구기관 5G특화망 기술 적용 사례

기관/기업	활용 내용 (Use Case)	핵심 보안 기술 (Core Tech)
삼성전자	AI 기반 슬라이스 트래픽 분석 및 자원 격리	AI IDS, 슬라이스 격리
ETRI	ETSI ZSM 기반 슬라이스 생명주기 보안 자동화, 자동 복구 시범망	SDN/NFV 통합 보안 플랫폼 구성
LG 유플러스	MEC 기반 산업현장 IDS/IPS 적용 및 에지 보안 실증	MEC 기반 IDS/IPS
경남 테크노파크	사용자 평면·gNB 현장 구축, 제어 평면 본부 집중, 스마트 팩토리 도입	UPF 로컬 분리 기반 트래픽 격리
분당 서울대병원	자율주행 휠체어·무인이송 로봇·3D 수술 모의 실험, 환자 편의 서비스	URLLC 슬라이스 무결성·가용성 정책 적용
국민 대학교	5G특화망 기반 인트라넷, 24시간 끊김 없는 서비스 제공	eMBB 슬라이스 콘텐츠 암호화 정책
다카시마 병원 (일본)	Local 5G 기반 원격 첨단 의료·응급의료 연계 고도화	원격의료 5G 보안 시나리오 적용
Bosch (독일)	5G SA망 자가 구축, 스마트 팩토리 무인화, 지능형 로봇 운영	Nokia NetGuard ML·SOAR 연계 가능
Fisk 대학교 (미국)	CBRS 기반 고해상도 콘텐츠 몰입형 교육	eMBB 슬라이스 고대역폭 보안 제어
Nokia (핀란드)	NetGuard Cybersecurity Dome ML 이상탐지·SOAR	ML 기반 위협 인텔리전스 및 보안 가시성
Ericsson (스웨덴)	ESM 기반 보안 정책 자동화 및 컴플라이언스 모니터링	Continuous Compliance Audit
Verizon (미국)	슬라이스 단위 Zero Trust 기반 접근 제어	Zero Trust Architecture (IdP/PDP 분리)
Deutsche Telekom (독일)	E2E 5G 슬라이싱 SLA 보장 및 생명주기 자동화 오케스트레이션	슬라이스 SLA 보장 및 격리

표 5는 5G특화망 및 네트워크 슬라이싱 적용사례와 보안 리질리언스 확보를 위한 국내외 주요 선도 기업들의 기술 활용 내용과 핵심 보안 기술을 요약한 것이다.

3. 표준화 및 정책 동향

3.1 국제 표준화 동향

현재 네트워크 보안 리질리언스 관련 기술은 주요 국제 표준화 기구 및 기관을 중심으로 활발히 논의되고 있으며, 주요 동향은 다음과 같다.

- **3GPP:** TS 23.501을 통해 5G 네트워크 슬라이싱의 기본 아키텍처를 정의하고, TS 33.501에서 슬라이싱 보안 기능 및 위협 모델을 명시함. 특히, Release 16 및 17을 거치며 슬라이스별 인증 및 인가 기능이 고도화되어 슬라이스 접속 구간의 보안이 한층 강화됨
- **ETSI:** ZSM(Zero-touch Service Management) 프레임워크를 통해 슬라이스 생명주기 전반의 자동화된 보안 관리를 제안함. 또한 ENI(Experiential Networked Intelligence) 규격을 통해 AI/ML 기반의 의도 기반 네트워크(Intent-Based Networking)와 연계된 보안 제어 자동화 기능을 정의함[5,6]
- **ITU-T:** X.1816을 통해 IMT-2020 네트워크 슬라이스의 보안 역량 분류 체계를 정의하고, 접근제어 · 인증 · 데이터 기밀성 · 통신보안 · 무결성 · 가용성 · 프라이버시 등 보안 차원에

따른 슬라이스 보안 유형 분류 방법론을 제시함[7]

- **O-RAN Alliance:** WG11(Security Focus Group)을 중심으로 오픈 인터페이스(E2, O1, A1, Open Fronthaul)의 보안 위협 분석과 대응 방안을 표준화함. 개방형 환경이 초래할 수 있는 공급망 보안(Supply Chain Security) 위험을 통제하기 위해 그 역할이 점차 강조됨[8]
- **NIST(글로벌 참조 프레임워크):** 사실상의 글로벌 보안 표준을 주도하는 NIST는 사이버 리질리언스 엔지니어링 프레임워크를 제시하였으며, 이는 5G특화망의 보안 설계에 광범위하게 참조됨[4]

3.2 국내 정책 동향

국내에서도 과학기술정보통신부 및 주요 정보보호 연구기관을 중심으로 5G특화망과 네트워크 슬라이싱 환경에 특화된 보안 정책 수립 및 가이드라인 마련이 적극적으로 추진되고 있다.

- **특화망 보안 가이드라인 제정 및 인증제도 추진(과학기술정보통신부, TTA):** 2023년 '5G특화망 보안 가이드라인'을 발표하여 특화망 도입 기업이 준수해야 할 보안 요구사항과 점검 기준을 구체화함[16]. 네트워크 슬라이싱 환경에 맞춘 보안 시험 방법론을 개발하고 특화망 구축 기업 대상의 공식적인 보안 인증제도 도입 검토
- **슬라이싱 특화 취약점 분석 및 침투 테스트(한국인터넷진흥원, KISA):** '5G 보안 위협 분석 및 대응 방안' 연구를 수행하여, 논리적으로 분할된 슬라이싱 환경의 구조적 특성을 반영한 전용 취약점 분석 도구와 실효성 있는 침투 테스트 방법론 개발[17]
- **국산 암호 알고리즘 기반 5G 보안 지침 수립(국가보안기술연구소, NSR):** 5G특화망 내 데이터 보호 강화를 위해 ARIA, SEED 등 국산 표준 암호 알고리즘의 5G 슬라이싱 환경 적용 가능성과 안전성 검토를 추진 중임

V. 다중 슬라이스 기반 보안 리질리언스 시스템

1. 보안 리질리언스 제안 시스템 개요

본 절에서는 그림 1과 같이 5G특화망 · 유 · 무선 통합환경에서의 보안 리질리언스 기술을 실제 시스템으로 구현하기 위한 아키텍처를 제안한다. 제안 시스템은 ① Front-end Service Layer, ② Back-end Layer, ③ Infra Cloud Layer, ④ Service Slices의 4계층 구조로 설계되며, 계층 간 데이터 흐름은 데이터 평면과 제어 평면으로 이중화된다. 그림 상단에는 영역별 주요 보안 위협을 분류하여, 각 계층에서 대응해야 할 위협 벡터를 함께 제시한다.

Back-end Layer는 3GPP 표준 NF를 수용하는 5G Core Cluster와 보안 리질리언스 기능을 전담하는 5G 보안 리질리언스 Cluster의 두 클러스터가 병렬로 배치된다. 두 클러스터의 논리적 분리를 통해 보안 컴포넌트의 장애나 침해가 코어 기능으로 확산되는 것을 차단하며, 슬라이스 단위의 독립적인 보안 정책 적용과 자동화된 위협 대응이 가능하게 설계되었다. SR Cluster의 핵심 컴포넌트 구성 및 기능은 그림 1 및 표 6과 같다.

Infra Cloud Layer는 Kubernetes 클러스터 기반으로 Node 1(SR Platform)과 Node 2(Private 5GC)의 두 워커 노드가 중앙 CP(Control Plane)의 통제하에 CNF 배포 · 확장 · 복구를 자동화한다. Service Slices 계층에서 각 슬라이스는 Front-end Service Layer에서 Secure UE와 매핑되며, cIPS 필터링과 Zero Trust 기반 접근 검증을 거쳐 최종 데이터 네트워크(DN)

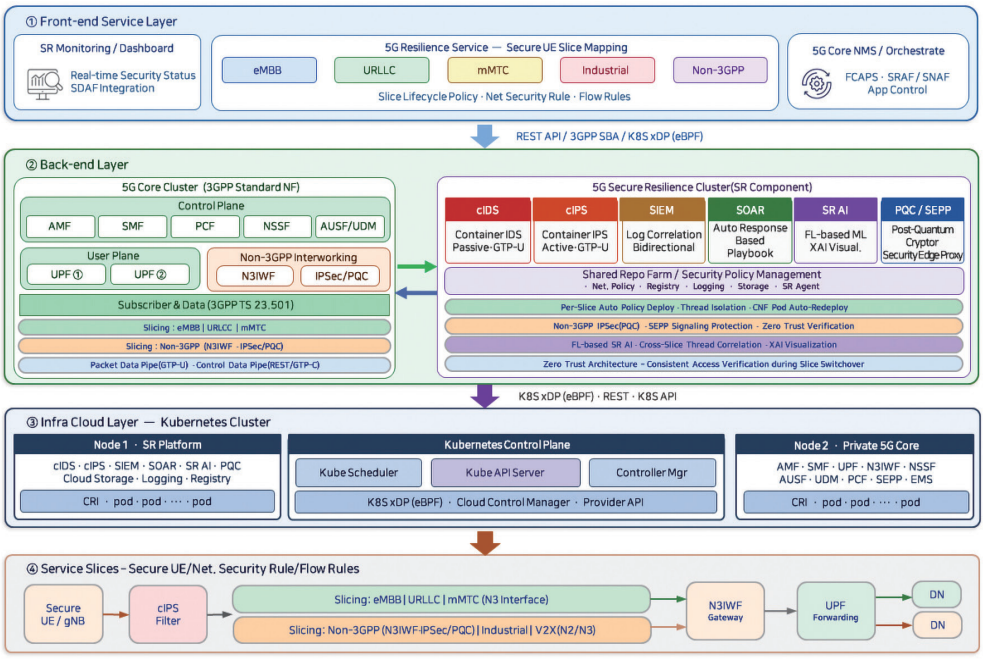

그림 1 5G특화망 유·무선 통합환경에서의 네트워크 슬라이스 기반 보안 리질리언스 아키텍처

표 6 보안 리질리언스 Component Sub-Layer 핵심 컴포넌트 기능 명세

컴포넌트	기능 설명	탐지/대응 유형	연동 파이프
cIDS (Container IDS)	컨테이너 기반 실시간 트래픽 침입 탐지·슬라이스별 이상 패턴 감지	수동 탐지 (Passive)	Packet Data Pipe (GTP-U)
cIPS (Container IPS)	컨테이너 기반 위협 차단 및 트래픽 필터링·Net Security Rule 적용	능동 차단 (Active)	Packet Data Pipe (GTP-U)
SIEM (Security Information and Event Management)	슬라이스별 이벤트 로그 통합·상관관계 분석· 복합 위협 탐지	사후 분석+ 실시간	양방향 (Data/Control)
SOAR (Security Orchestration, Automation and Response)	플레이북 기반 자동 대응 절차 실행·AMF·SMF·PCF 정책 자동 변경	자동 대응 (Automated)	Control Data Pipe (REST/GTP-C)
Secure Resilience(SR) AI	연합학습(FL: Federated Learning) 기반 슬라이스별 ML 이상탐지·위협 예측·XAI(Explainable AI) 시각화	지능 탐지 (AI-driven)	양방향 (Data/Control)
PQC(Post-Quantum Crypto)	양자내성암호 적용·N3IWF 구간 IPSec 암호화·미래 양자 위협 대비	예방 (Prevention)	Packet Data Pipe (GTP-U)
SEPP(Security Edge Protection Proxy)	슬라이스 간 및 외부망 연동 구간 시그널링 보호·N32 인터페이스 보안	예방 (Prevention)	Control Data Pipe (REST)
Network Policy	슬라이스별 네트워크 접근 정책 관리·Zero Trust 연계	자동 대응 (Automated)	Control Data Pipe
Registry	컨테이너 이미지 무결성 검증·신뢰 이미지 관리·공급망 공격 방지	예방 (Prevention)	Control Data Pipe
Logging	슬라이스별 보안 이벤트 로그 수집·SIEM 연동·감사 데이터 저장	사후 분석	Control Data Pipe
SR Agent	NF별 이벤트 로그 수집·취약점 분석·정책 배포 중개	에이전트 기반	Control Data Pipe

로 전달된다.

2. AI 기반 다중 슬라이스 침해탐지

다중 슬라이스 환경의 지능형 침해탐지는 슬라이스 유형별로 트래픽 패턴과 정상 동작 기준, 허용 가능한 응답 시간이 서로 다르기 때문에, 하나의 탐지 모델을 모든 슬라이스에 동일하게 적용하면 실제 공격을 놓치거나 정상 트래픽을 공격으로 잘못 판단하는 문제가 빈번하게 발생한다. 이러한 한계를 극복하기 위해 3가지 원칙을 기반으로 설계된다.

- 첫째, 슬라이스마다 서비스 성격이 다르므로, 각 슬라이스가 정상적으로 동작할 때 나타나는 고유한 트래픽 특징을 학습하여 이상 여부를 판단하는 기준을 슬라이스별로 독립적으로 생성함
- 둘째, 응답 속도가 매우 중요한 슬라이스(예: 원격제어, 자율주행)에서는 탐지 과정 자체가 서비스 지연을 유발해서는 안 되므로, 분석에 사용하는 항목을 필요한 것만으로 줄여 빠르게 판단함
- 셋째, 트래픽 패턴은 시간이 지나면서 자연스럽게 변하므로 이를 이상으로 오인하지 않도록, 탐지 기준을 주기적으로 자동 갱신하여 탐지 정확도를 유지함

탐지에 사용되는 AI 모델은 슬라이스의 서비스 특성에 따라 다르게 적용된다. 대용량 스트리밍 서비스 슬라이스에서의 대규모 트래픽 폭증 공격 탐지에는 시계열 패턴 분석에 강한 모델을, 초저지연 제어 슬라이스에서의 패킷 조작 탐지에는 정상 패턴에서 벗어난 이상값을 찾아내는 모델을, 대규모 IoT 센서 슬라이스에서의 비정상 기기 행위 탐지에는 정상 범위를 벗어난 개별 데이터를 골라내는 모델을 각각 사용한다. 또한, 여러 슬라이스에 걸쳐 단계적으로 진행되는 지능형 지속 공격의 탐지에는, 슬라이스 · 네트워크 기능 · 단말 그룹 간의 관계와 연결 구조를 분석하는 방식이 보안 리질리언스 AI의 핵심 탐지 엔진으로 작동한다. 표 7은 슬라이스 유형별 탐지 모델 운용의 주요 내용이다.

표 7 AI 기반 다중 슬라이스 유형별 탐지 모델 운용

유형	위협	특징	지표
eMBB	DDoS, 콘텐츠 조작	대용량 데이터 전송 관련 정보인 전체 바이트 수, 방향별 바이트 수, 대역폭 사용량, TCP 윈도우 크기	F1-Score 처리량
URLLC	패킷 위조, 타이밍 공격	세션 지속시간 관련 정보인 TCP 플래그, 세션 생성 및 종료 패턴	탐지지연 <1ms, FPR
mMTC	봇넷, 이상 접속 폭증	데이터량과 송신 시간 정보인 지속시간, 단말 유형 및 서버 정보	이상 기기 탐지율

보안 리질리언스를 위한 AI는 여러 슬라이스에 흩어진 위협 정보를 통합하여 탐지 성능을 높이기 위해, 각 슬라이스가 협력하여 AI를 공동으로 학습시키는 연합학습 방식을 채택한다. 슬라이스마다 서비스 유형이 다르고 트래픽의 특성과 패턴도 각기 다르기 때문에 각 슬라이스의 특성에 맞는 학습 방법을 개별적으로 적용하는 것이 탐지 정확도를 높이는 데 유리하다. 각 슬라이스는 트래픽 크기 · 접속 주기 · 응답 시간 등 해당 슬라이스 고유의 특성 항목 간 상관관계를 분석하여 AI를 개별 학습시킨 뒤 학습 결과물만을 중앙으로 전달하고, 중앙에서는 이를 취합하여 더 정교한 통합 탐지 모델을 만들어 다시 각 슬라이스에 배포함으로써 결과적으로 여러 슬라이스의 다양한 위협 패턴이 하나의 탐지 모델에 반영되는 구조를 갖는다.

다만 연합학습 과정에서, 특정 슬라이스가 의도적으로 조작된 학습 결과물을 전송하여 특정 공격 유형을 정상으로 판단하도록 전체 탐지 모델을 오

도하려는 시도가 발생할 수 있다. 이에 대비하여 각 슬라이스로부터 수신된 학습 결과물이 해당 슬라이스의 서비스 특성에 부합하는지를 취합 단계 이전에 자동으로 검사하고, 부합하지 않는 결과물은 걸러낸 뒤 신뢰할 수 있는 결과물만을 모델 개선에 반영함으로써 연합학습 전체의 신뢰성을 유지한다. 또한, 탐지 결과를 보안 운영자가 쉽게 이해하고 판단할 수 있도록, AI가 특정 트래픽을 이상으로 판단한 경우, 피쳐의 중요도 및 특징별로 부여된 가중치를 분석하여 근거 사항을 관제 화면에 표시한다. 아울러 연합학습으로 만들어진 통합 탐지 모델 외에 서로 다른 방식으로 설계된 보조 탐지 모델을 함께 운용하여, 공격자가 특정 모델의 판단 방식을 파악하고 정상 트래픽처럼 위장하더라도 나머지 모델이 이를 탐지할 수 있는 추가적인 안전망을 갖춘다[10,20].

3. 데이터 흐름 및 보안 리질리언스 시나리오

제안 시스템의 계층 간 데이터 흐름은 데이터 평면(Data Plane)과 제어 평면(Control Plane)으로 이원화된다. 데이터 평면에서는 UE로부터 발생한 트래픽이 N3IWF 또는 gNB를 통해 UPF로 전달되고, Packet Data Pipe(GTP-U)를 경유하여 IDS/IPS 컴포넌트에서 실시간 딥패킷 검사(DPI: Deep Packet Inspection)가 이루어진다. 검사를 통과한 트래픽만 DN으로 최종 전달된다. 제어 평면에서는 AMF · SMF · PCF로부터 발생한 시그널링 메시지가 Control Data Pipe(REST/GTP-C)를 통해 SR 컴포넌트로 전달되며, SOAR의 플레이북 실행 결과도 역방향으로 5G Core NF에 전달되어 슬라이스 정책이 동적으로 변경된다.

5G특화망 내 단말이 3GPP 슬라이스에서 Non-3GPP(N3IWF) 기반 슬라이스로 이동하는 환경에서의 전형적인 자동 대응 시나리오는 다음과 같다.

- **탐지:** 단말이 N3IWF를 통해 새로운 슬라이스로 진입하기 위해 IPsec 터널을 생성하는 과정에서, IDS가 비정상적인 인증 시도나 슬라이스 경계를 우회하려는 이상 트래픽 패턴을 탐지함
- **분석:** 탐지 이벤트가 SIEM으로 전달되며, 기존 3GPP 접속 로그와 N3IWF 접속 로그의 상관 분석을 통해 이종 망 간 이동성을 악용한 공격으로 위협 유형을 분류함
- **제어:** SOAR가 해당 위협 등급에 맞는 플레이북을 자동 실행하고, Control Data Pipe를 통해 SMF에 N3IWF를 경유하는 악성 PDU 세션의 강제 종료 명령을 전달함
- **격리:** SR Agent가 PCF에 동적 접근 제어 정책을 배포, AMF를 통해 해당 단말의 N3IWF 재접속 및 다른 슬라이스로의 이동(Inter-slice Mobility) 차단함
- **학습:** SR AI가 슬라이스 기반 유 · 무선 통합망(3GPP-N3IWF) 이동성 환경에서의 공격 패턴을 학습 데이터로 반영, 위협 탐지 모델을 업데이트함
- **복구:** 위협이 격리된 후, 공격 표면으로 노출되었던 N3IWF 또는 관련 UPF의 CNF Pod를 안전한 이미지로 재배포하여 무결성 확보 및 서비스 연속성을 복원함

VI. 결론

5G특화망과 유 · 무선 통합 환경, Non-3GPP 접속 기술이 융합된 네트워크 인프라에서 네트워크 슬라이싱은 다양한 서비스를 동시에 안정적으로 제공하는 핵심 기술로 자리매김하고 있다. 그러나

이러한 슬라이싱 구조는 슬라이스 간 침투, DoS/DDoS, 인증 우회, 오케스트레이션 레이어 공격 등 고도화된 보안 위협을 동반하므로, 이에 대한 능동적 대응 전략으로서 보안 리질리언스는 필수적인 요소이다.

본고에서는 슬라이싱 환경의 보안 위협 모델과 국내외 표준화 및 기술 동향을 종합적으로 분석하고, 이를 바탕으로 3GPP 표준을 준수하는 다중 슬라이스 보안 리질리언스 아키텍처를 제안하였다. 보안 리질리언스 시스템은 Front-end, Back-end, Infra 계층 간 철저한 논리적 격리를 구현하였으며, 특히 SIEM, SOAR, AI 및 클라우드를 연계한 자동화 파이프라인을 통해 5G특화망 · 유 · 무선 통합환경에서도 위협을 실시간으로 탐지, 격리, 자동 복구하는 능동적 방어 체계를 확립하였다. 나아가 이러한 제안 시스템의 연구 결과를 토대로, 제로 트러스트 아키텍처의 내재화, AI/ML 기반 자율 보안 시스템, 양자내성암호 적용 등이 향후 슬라이싱 보안의 핵심 발전 방향임을 확인하였다.

궁극적으로, 슬라이싱 기반의 보안 리질리언스 기술은 5G특화망 환경에서의 통신 연속성과 보안 신뢰도를 보장하는 중추적인 역할을 수행하며, 국가 차원의 디지털 인프라 경쟁력 강화에 이바지할 것이다. 앞으로 공공과 민간의 협력을 통한 실증 사례 축적과 글로벌 표준화 연계가 5G특화망 보안 생태계 성숙을 위한 핵심 과제가 될 것이다.

용어해설

5G특화망 건물, 공장 등 특정 지역에 한정하여 기업이 직접 5G 주파수를 할당받아 구축하는 맞춤형 네트워크

네트워크 슬라이스 5G 이동통신에서 하나의 물리적 네트워크 인프라를 소프트웨어 정의 기술을 활용해 여러 개의 독립적인 논리적 네트워크로 분할

Non-3GPP 3GPP 표준 기술이 아닌 무선 기술을 통해 단말(Wi-Fi, Zigbee, LoRa 등)이 코어 네트워크에 접속하는 네트워크

보안 리질리언스 사이버 공격이나 재난을 완전히 막는 것을 넘어, 공격당하더라도 업무 기능을 즉시 유지하고 신속하게 복구하여 이전 상태로 돌아가는 능력

참고문헌

[1] 3GPP TS 23.501, "System Architecture for the 5G System," Release 17, 2022.

[2] 3GPP TS 33.501, "Security Architecture and Procedures for 5G System," Release 17, 2022.

[3] 3GPP TS 33.558, "Security Aspects of Enhancement of Support for Edge Computing in 5GS," Release 17, 2022.

[4] NIST, "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach," NIST Special Publication 800-160, vol. 2, 2021.

[5] ETSI GS ZSM 002 V1.1.1, "Zero-touch network and Service Management (ZSM): Reference Architecture," 2019.

[6] ETSI GR ENI 001 V3.1.1, "Experiential Networked Intelligence (ENI); ENI use cases," 2022.

[7] ITU-T X.1816, "Guidelines and requirements for classifying security capabilities in IMT-2020 network slice," ITU-T Recommendation, 2023.

[8] O-RAN Alliance, "O-RAN Security Threat Modeling and Remediation Analysis," O-RAN.WG11.TR-v04.00, 2023.

[9] C. De Alwis et al., "A survey on network slicing security: Attacks, challenges, solutions and research directions," IEEE Commun. Surv. Tutor., vol. 26, no. 1, 2024, pp. 534-570.

[10] NSA/CISA, "5G Network Slicing: Security Considerations for Design, Deployment, and Maintenance," Enduring Security Framework (ESF), U.S. National Security Agency and Cybersecurity and Infrastructure Security Agency, 2023.

[11] V.P. Singh et al., "Security in 5G network slices: Concerns and opportunities," IEEE Access, vol. 12, 2024, pp. 52727-52743. doi: 10.1109/ACCESS.2024.3386632

[12] Nokia, "Security and Slicing in 5G Networks," Nokia NetGuard Whitepaper, 2022.

[13] Verizon, "How Verizon Applies Zero Trust to 5G Network Slices," Verizon 5G Edge Blog, 2023.

[14] Ericsson, "Security in 5G Network Slicing," Ericsson Technology Review, 2023.

[15] 한국인터넷진흥원(KISA), "5G 특화망 보안 안내서," 2026.

[16] 과학기술정보통신부·한국정보통신기술협회(TTA), "5G 특화망 보안 가이드라인," TTAK.KO-12.0337, 2023.

[17] 한국인터넷진흥원(KISA), "5G 보안 위협 분석 및 대응방안 연구," KISA-WP-2022-0014, 2022.

[18] R. Ni et al., "A survey on network slicing security in 5G," IEEE Commun. Surv. Tutor., 2023.

[19] A. Aijaz, "Private 5G: The future of industrial wireless," IEEE Ind. Electron. Mag., vol. 14, no. 4, 2020, pp. 136-145. doi: 10.1109/MIE.2020.3004975

[20] S. Wijethilaka and M. Liyanage, "A Federated Learning Approach for Improving Security in Network Slicing," in Proc. IEEE Global Commun. Conf., (Rio de Janeiro, Brazil), Dec. 2022, pp. 915-920.