시장 조사 및 경쟁력 분석:
서비스 프로바이더와 벤더를 위한
차세대 비즈니스 및 기술 솔루션

HEAVY READING
WHITE PAPER

# 5G 보안 전략 고려 사항

*Heavy Reading 백서 (Juniper Networks Inc. 의뢰)*

저자: JIM HODGES, 수석 애널리스트, HEAVY READING

## 소개

5G 는 다양한 수준에서 네트워킹 패러다임을 혁신할 전망입니다. 5G 는 네트워크 속도를 향상시킬 뿐 아니라 IoT(Internet of Things) 기반 애플리케이션을 비롯해 다양한 최신 서비스와 관련 산업 애플리케이션을 지원할 것입니다. RAN, 코어 및 전송 아키텍처에 대한 획기적인 혁신이 이루어졌고 설계는 완성 단계에 있습니다. 하지만 서비스 프로바이더가 5G 전략을 수립하는 과정에서 가장 중요한 사항은 보안이며, 다양한 기기와 애플리케이션에 따른 보안 영향과 요구를 변수로 고려하게 됩니다.

다양하게 얽혀 있는 관련 산업 모두에 5G 네트워크를 제공하는 데 보안은 필수적입니다. 5G 네트워크는 상당한 수의 디바이스를 연결하고 각기 다른 보안 요건을 지닌 다양한 애플리케이션과 고객을 지원할 것입니다. 5G 애플리케이션의 다양성, 확장성, 처리량, 지연 시간 관련 요구 사항으로 인해 보안 관리 및 보안 정책의 효율성, 일관성 및 정확성을 조율하기 어렵습니다. 또한 MEC(Multi-Access Edge Computing), 가상화, CUPS(Control-User Plane Separation), 네트워크 슬라이싱이 도입됨에 따라 새로운 공격경로(attack surface)가 만들어집니다. 이 역시 서비스 프로바이더가 반드시 해결해야 할 문제입니다.

이 백서에서는 5G 의 새로운 기능, 5G 의 보안 영향, 서비스 프로바이더가 5G 로 전환할 때 직면하게 되는 보안 관련 과제와 기회에 대해 설명합니다.

## 5G – 4G 와 다른 기능은 무엇인가?

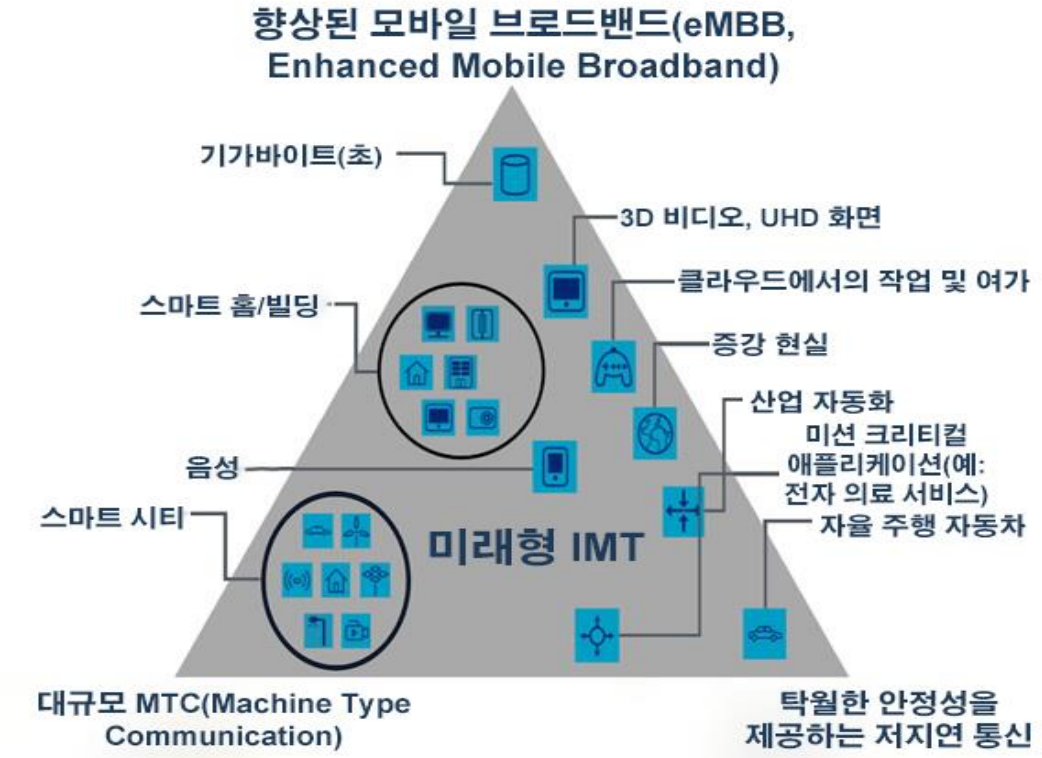
5G 는 1ms 지연, 최고 데이터 속도 10Gbit/s 를 포함하는 탁월한 성능을 목표로 하며 이는 모두 4G 네트워크에 비해 비약적인 발전을 의미합니다. 이러한 높은 성능을 달성하려면 5G 네트워크의 보안 성능도 발전해야 합니다.

5G 는 모든 이전 세대 대비 다양한 사용 사례를 지원하도록 설계된 최초의 모바일 아키텍처입니다. 특정 도메인과 해당 사용 사례 구성을 보여주는 구조를 제공하기 위해 국제전기통신연합(ITU)에서는 5G 서비스 구조를 게시한 바 있습니다.

**그림 1** 에 표시된 대로 이 구조에서는 5G 서비스를 세 개의 구체적인 도메인으로 분류합니다. 바로 기존의 eMBB(enhanced mobile broadband) 도메인, 그리고 새로운 두 도메인인 mMTC(massive Machine-Type Communications) 및 URLLC(Ultra-Reliable and Low Latency Communications)입니다. 각 도메인에는 고유한 보안 요구 사항이 있습니다. 하나의 통합된 5G 네트워크를 통해 다양한 액세스 및 서비스 요구 사항을 모두 보호하는 것이 물론 쉬운 일이 아닙니다.

예를 들어, 5G 는 스마트 시티의 기반이 되는 트래픽 센서, V2I(Vehicle-to-Infrastructure) 서비스를 비롯한 대규모 IoT 애플리케이션을 지원합니다. 해커가 데이터에 액세스하거나, IoT 디바이스를 하이재킹하거나, 서비스를 훼손하지 못하도록 방어하는 것이 중요합니다.

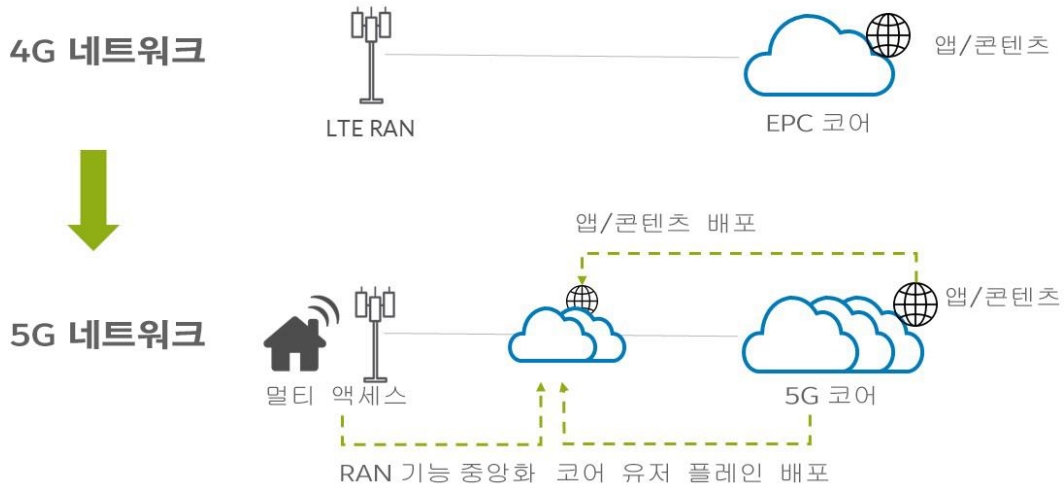
그림 **1: ITU 5G** 서비스 구조




*출처: ITU-R M.2083-0*

이렇게 다양한 성능 지표를 실현하기 위해 5G 에는 MEC, CUPS(Control and User Plane Separation), 네트워크 슬라이싱을 포함한 새롭고 다양한 네트워크 설계 방식이 통합되었습니다. **그림 2** 에서 볼 수 있듯이 이러한 네트워크 아키텍처의 변화에 따라 보안 아키텍처도 진화해야 합니다. 새로운 기술이 도입되면 보안 전략을 통해 해결해야 하는 새로운 보안 취약성이 생겨납니다. 이러한 잠재적 위험 시나리오에 대해서는 이 백서의 다음 섹션에서 살펴봅니다.

**그림 2: 4G 와 5G 의 네트워크 아키텍처 혁신 비교**




*출처: 5G Americas, '5G 의 보안 혁신' 해석도*

## 전략적 고려 사항 **#1:** 확장 가능한 보안 성능 및 보안 운영

4G 의 경우처럼 5G 으로의 전환도 갑자스럽게 다가오지는 않을 것입니다. 대신 5G 는 향후 10 년 동안 논리적 진화 과정을 통해 4G 와 나란히 발전할 것이며, 따라서 4G 는 다가올 몇 년 동안 중요한 역할을 계속할 것입니다.

실례로 GSMA 에서는 2025 년에도 4G 가 전 세계 연결의 59%를 차지할 것으로 예측합니다.* 대부분의 5G 구축은 5G NSA(non-standalone) 아키텍처로 시작될 것입니다. NSA 아키텍처는 보다 빠른 5G 서비스 출시를 위해 기존 4G 코어와 5G RAN 을 페어링합니다.

결과적으로 서비스 프로바이더의 5G 보안 전략에서는 먼저 기존 4G 네트워크 보안을 평가하여 4G 와 5G 에서의 보안이 일관되게 구현될 수 있도록 해야 합니다. 이 평가를 수행하기 위해서는 우선 4G 네트워크 보안 성능이 5G NSA 의 네트워크 용량 증가 시 문제가 없는지 확인하는 것이 필요합니다. 대부분의 경우 보안은, 확대를 위한 물리적 인프라의 업그레이드 및 확장과 확대 모두를 위한 가상 인프라의 업그레이드가 필요로 합니다.

추가적인 성능에 대한 투자가 없다면 보안으로 인해 전체 네트워크에서 병목현상이 발생할 것입니다. 제품 수준에서는 3G/4G Gi/SGi 방화벽, 보안 게이트웨이(SEG), Gp/S8 로밍 방화벽을 비롯한 현재 모바일 보안 사용 사례에서의 보안 성능(처리량, 연결 규모, 세션 설정률 등)을 평가해야 합니다.

점검해야 하는 다른 사용 사례로는 분산 서비스 거부(DDoS) 보호가 있습니다. IoT 의 부상으로, 규모가 있고 일반적으로 보안 기능이 제한된 커넥티드 디바이스는 해커의 선호하는 공격 대상이 되어가고 있습니다.

일례로 2016 년 Mirai IoT 봇넷은 전 세계적으로 약 10 만 커넥티드 디바이스에 피해를 입혔습니다. 감염된 디바이스는 DNS(domain name system) 서비스 프로바이더 Dyn 에 대해 최대 용량 1.2Tbit/s 로 DDoS 공격을 감행하여 4 시간 이상의 서비스 중단 및 다운타임을 초래했습니다. Mirai 는 시작에 불과했습니다. 그 후 JenX, Hajime, Satori, Reaper 등과 같은 변종이 발생하면서 공격이 점점 더 정교해지고 있으며, 그만큼 방어하기도 어려워지고 있습니다.

5G 의 도입으로 사용 가능한 대역폭이 증가하고 감염된 커넥티드 디바이스가 공격 트래픽을 생성할 수 있는 더욱 강력한 네트워크가 조성되면서 문제는 더욱 복잡해졌습니다. 대규모 DDoS 공격의 빈도, 크기, 정교함이 증가함에 따라 대역 외 스크러빙 센터(scrubbing center), 수동 개입 등과 같은 기존의 방어망은 더 이상 통하지도 않을뿐더러 막대한 비용도 유발합니다.

대규모 공격의 경우 의심스러운 트래픽을 스크러빙 센터로 리디렉션하려면 지연 시간이 증가할 뿐 아니라 완화 비용이 데이터 트래픽의 양과 직접적인 연관이 있으므로 재정적으로 엄청난 부담을 초래합니다. 서비스 프로바이더는 텔레메트리, 기계 분석, 네트워크 기반 완화를 통합하여 감지 및 완화 프로세스를 보다 비용 효율적이고 지능적으로 자동화하는 최신 DDoS 보호 접근 방식의 도입을 고려해야 합니다.

* GSM Association, *모바일 경제 2019*.

성능과 함께 보안 운영도 확장이 가능해 PNF(physical network function) 및 VNF(virtual network function)를 포함하는 분산형 텔코 클라우드 환경을 지원할 수 있어야 합니다. 이를 위해서는 물리적 도메인과 가상 도메인을 모두 관리하고 이러한 도메인에 대한 통합적인 뷰를 제공하는 통합 보안 관리 시스템이 필요합니다. 다시 말해서 보안 관리는 전체 시스템 차원의 가시성을 제공해야 합니다. 이 전략을 구성하는 또 다른 요소는 프로그래밍 가능한 보안 정책을 통해 자동화된 정책 오케이스트레이션을 활용하는 데 있습니다. 이는 SLA(service-level agreement)를 충족하는 안정적이고 안전한 네트워크를 보장하는 데 필요합니다.

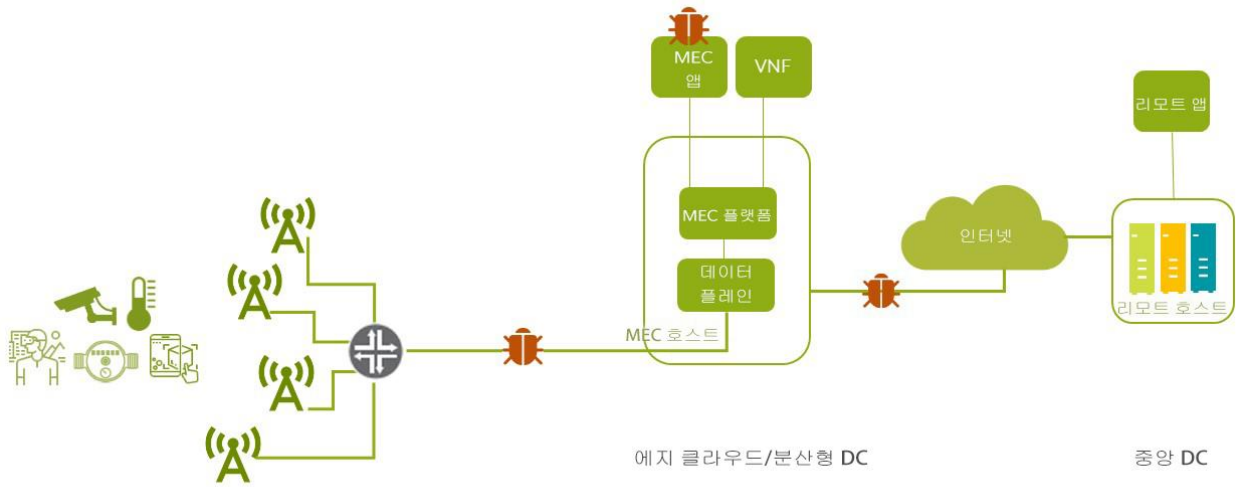
또한 5G 인프라의 이질성과 복잡성에 따라 여러 도메인에 걸쳐 다양한 수준(예: 슬라이스, 서비스 또는 리소스에 연결)으로 보안을 적용해야 합니다. 따라서 보안 자동화와 오케스트레이션은 서비스 프로바이더가 보안 운영의 어려움을 선제적으로 해결하는 데 핵심적입니다.

## 전략적 고려 사항 #2: 네트워크 아키텍처의 발전과 새로운 구현 기술로 인한 새로운 공격 경로 노출

에지 컴퓨팅은 진환된 형태의 클라우드 컴퓨팅으로, 애플리케이션 호스팅 및 데이터 처리가 중앙 집중화된 데이터센터에서 모바일 애플리케이션과 인접한 네트워크 에지로 이동할 수 있도록 합니다. 에지 컴퓨팅은 5G 의 까다로운 요구 사항을 충족하기 위한 핵심 요소입니다. 특히, 저지연 대역폭 효율이 필수적인 사용 사례를 위한 핵심 요소입니다.

ETSI 에서 MEC(Multi-Access Edge Computing)를 담당하는 ISG(Industry Specification Group)에서는 MEC 를 위한 일련의 기술 표준을 정의했습니다. 해당 표준은 5G NSA, 분산 컴퓨팅, 네트워킹 장비 및 컴퓨팅 서버 가상화를 비롯하여 다양한 기술을 지원합니다. 이러한 모든 기술은 개방형 에코시스템에서 상호 운용되어 서비스 프로바이더가 분산된 애플리케이션에 구축할 수 있습니다. 하지만, **그림 3** 에서 볼 수 있듯이 MEC 환경의 이질성과 다양성으로 인해 전체 MEC 시스템에 대한 주요 위협을 야기하는 다양하고 새로운 악성 공격 및 개인정보 침해 경로가 발생하게 됩니다.

**그림 3: MEC 공격 경로(attack surface)**




*출처: 주니퍼 네트웍스*

가능한 구축 모델은 일부 VNF 와 마찬가지로 동일한 물리적 플랫폼에서 MEC 애플리케이션을 실행하는 것입니다. 이러한 애플리케이션은 모바일 서비스 프로바이더가 제어하지 않는 타사 애플리케이션일 수 있으며, 이는 네트워크 기능에 필요한 리소스의 고갈을 야기할 수 있다는 우려로 이어집니다.

또한 잘못 설계된 애플리케이션이 해커가 분산된 데이터센터에 침입하여 플랫폼에서 실행 중인 네트워크 성능에 영향을 주는 공격 경로를 제공할 위험도 있습니다. 마찬가지로 공격자는 동일한 결과를 얻기 위해 악성 애플리케이션을 삽입할 수 있습니다. 에지의 가상화 기능에서 민감한 보안 자산이 손상된 경우, 공격자가 해당 자산을 악의적으로 재사용하여 연결성을 확보하거나 스푸핑, 도청 또는 데이터 조작 공격을 감행할 수 있습니다.

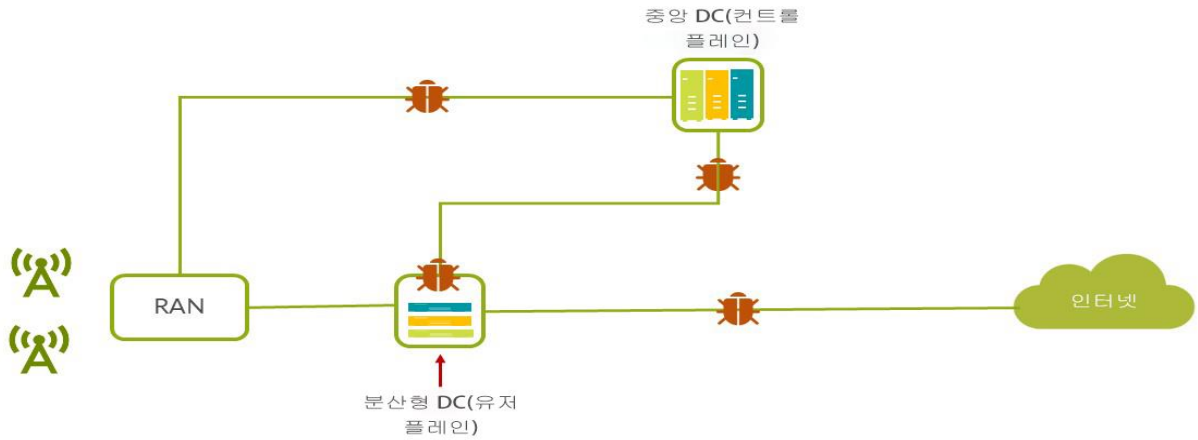
이러한 공격 방법이 반드시 새로운 것은 아닙니다. 하지만 MEC 는 새롭게 등장한 아키텍처로, 보안 문제의 잠재적 위험과 심각도가 제대로 파악되지 않았을 수 있습니다. 따라서 대규모 상용 에지 클라우드 구축을 시작하기 전 벤더 선택 시, 서비스 프로바이더는 보안 솔루션의 초기 구축 시, 광범위한 위협 요소를 충족할 만큼 충분히 유연성을 제공하는지 확인해야 합니다.

## 분산된 코어 공격 경로

4G EPC(Evolved Packet Core)에서의 CUPS(Control and User Plane Separation) 도입으로 5G 코어 아키텍처가 획기적으로 발전할 수 있었습니다. CUPS 는 기존 4G EPC 를 통해 네트워크 전반에 걸쳐 사용자 플레인 리소스를 분산시킬 수 있으므로 3GPP 릴리스 14 표준을 구성합니다. 5G 코어 네트워크의 새로운 서비스 기반 아키텍처를 최종적으로 도입하기 전 CUPS 를 통한 리소스 분산을 수행할 수 있습니다. CUPS 를 사용하면 운영업체는 EPC 노드의 컨트롤 플레인와 사용자 플레인 리소스를 찾고 개별적으로 확장할 수 있습니다. 비디오와 같은 고대역폭 애플리케이션에도 적합합니다. 코어 사용자 플레인은 최종 사용자에 가깝게 위치하므로 운영업체는 트래픽을 중앙 데이터센터로 백홀할 필요가 없습니다. 따라서 지연 시간을 줄이고 백홀 비용을 절감할 수 있습니다.

CUPS 는 그 자체로는 5G 기능이 아니지만 신뢰 경계(trust boundaries)와 위협 경로(threat surfaces)가 5G 네트워크 구축 환경과 동일합니다. 즉, **그림 4** 에 표시된 대로 Sx 및 SGi 를 비롯한 모든 인터페이스가 DoS 또는 DDoS 공격 감행을 위한 수단이 될 수 있습니다.

**그림 4: 분산된 코어 공격 시나리오**



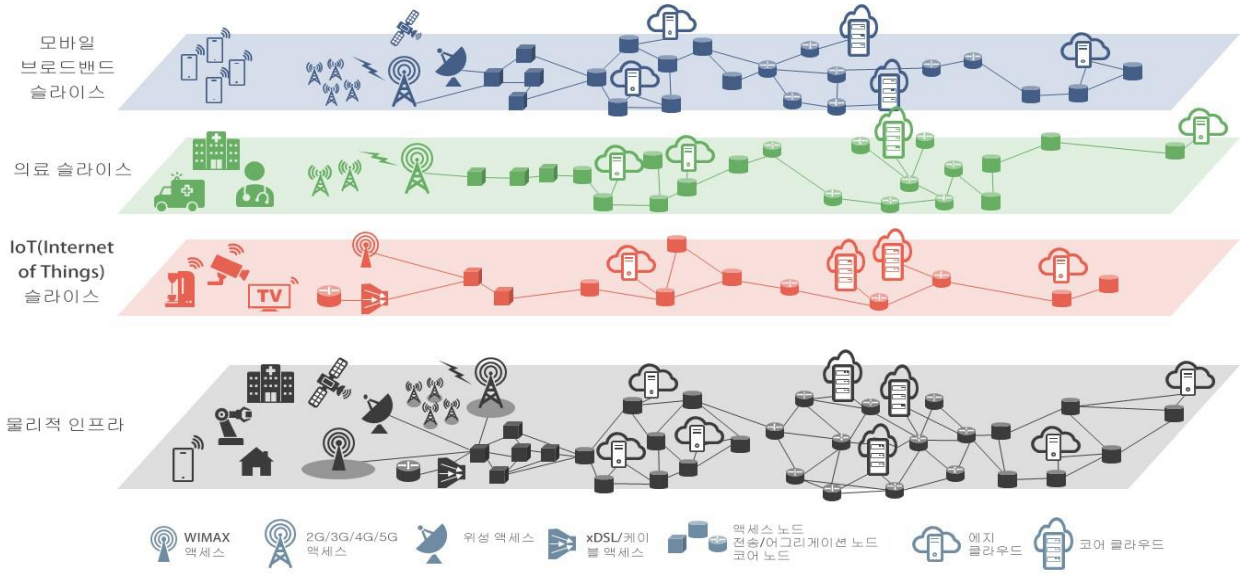

*출처: 주니퍼 네트웍스*

## 네트워크 슬라이싱 공격 경로

네트워크 슬라이싱은 가상화의 한 형태로 여러 논리 네트워크가 공유된 물리적 네트워크 인프라 위에서 실행될 수 있도록 해줍니다. 네트워크 슬라이싱을 사용하면 모바일 서비스 프로바이더가 네트워크 리소스를 분할하여 사용자별로 다른 성능 및 기능을 요구하는 다양한 사용 사례를 해결할 수 있습니다. 단일 물리적 인프라를 통해 이러한 사용 사례를 멀티플렉싱할 수도 있습니다.

예를 들어, **그림 5** 에 표시된 것처럼 이제 고유한 애플리케이션 슬라이스 유형을 생성하여 산업용 IoT, 의료 관련 산업별 애플리케이션을 비롯한 광범위한 서비스를 지원할 수 있습니다.

**그림 5: 5G 네트워크 슬라이싱**




*출처: IEEE, SDN/NFV 를 통한 5G 네트워크 슬라이싱: 개념, 아키텍처, 과제*

5G 에서 지원하는 새로운 서비스와 사용 사례의 규모로 인해 네트워크 슬라이싱은 5G 네트워크에서 중요할 역할을 할 것으로 예상됩니다. 새로운 사용 사례 및 서비스로 인해 기능 측면에서 네트워크에 대한 다양한 요구 사항이 등장할 것입니다. ITU 5G 서비스 구조에 표시된 것처럼 처리량, 서비스 품질, 지연, 보안 측면에서 성능 요구 사항이 크게 달라질 수 있습니다(**그림 1** 참조).

5G 에서는 흔히 대용량 IoT, MBB(mobile broadband), URLLC 애플리케이션이 하나의 물리적 네트워크에서 동시에 실행됩니다. 예를 들어, IoT 는 일반적으로 매우 많은 수의 디바이스를 지원하지만, 각 디바이스의 처리량은 매우 낮을 수 있습니다. 반면 MBB 는 훨씬 적은 수의 디바이스를 지원하지만 각 디바이스가 매우 큰 대역폭의 컨텐츠를 전송하거나 수신할 수 있습니다.

이러한 다양한 서비스 슬라이스 성능 프로필은 보안 프로토콜 선택과 정책 구현에 직접적인 영향을 줍니다. 예를 들어, 한 슬라이스의 서비스가 매우 긴 디바이스 배터리 수명을 요구하고 보안 프로토콜을 몇 가지 방식(예: 재인증 빈도)으로 제한할 수 있습니다. 또는 한 슬라이스의 서비스가 개인정보 보호에 매우 민감하여 매우 강력한 보안 절차(예: 임시 ID 를 매우 빈번하게 재할당)가 요구될 수 있습니다.

서비스 프로바이더는 이러한 슬라이스가 얼마나 상호 간에 잘 격리될 수 있는지를 고려해야 합니다. 주요 보안 우려 사항 중 하나는 공격자가 "하위" 보안 슬라이스를 통해 광범위한 네트워크 액세스 권한을 획득하는 것입니다.

**그림 6** 에 표시된 것처럼 공격 시나리오는 하나의 슬라이스에서 리소스를 고갈시키는 공격자를 포함할 수 있습니다. 이때 공격자가 여러 슬라이스에 공통적인 리소스를 고갈시켜 다른 슬라이스에서 DoS 또는 서비스 저하를 야기할 수 있습니다.

**그림 6: 슬라이스 고갈 공격 시나리오**


*출처: 주니퍼 네트웍스*

## 전략적 고려 사항 #3: 수익 차별화 요소이자 창출 요소로서의 보안

서비스 프로바이더는 5G 보안 전략을 수립할 때 보안을 활용하여 네트워크 구축 환경을 차별화하고 수익을 창출할 수 있는 방법을 고려해야 합니다.

네트워크 슬라이싱과 같은 5G 기능을 채택하면 제조 및 운송 부문을 비롯하여 IoT 애플리케이션에 크게 의존하는 다양한 부문에 걸쳐 높은 수익 성장을 촉진할 수 있습니다. 소비자와 달리 이러한 산업 분야에서는 대부분 더 엄격한 보안 요구 사항을 적용합니다. 따라서 전통적으로 해당 산업 분야에서는 연결을 위해 자체적인 프라이빗 네트워크를 구축해 왔습니다. 5G 제공으로 이러한 관련 산업 부문에 진출하기 위해서는 서비스 프로바이더가 고객의 요구를 충족하고 우려 사항을 해결할 수 있는 보안 역량을 갖추었음을 강조해야 합니다.

IoT 의 맥락에서 서비스 프로바이더는 엔터프라이즈 IoT 대화의 핵심인 연결을 통해 효과적으로 시장에 진입할 수 있습니다. IoT 연결에 따른 잠재력은 자체로도 크지만, 서비스 프로바이더는 많은 다른 기회를 통해 수익을 창출할 수 있습니다. 보안이 한 예가 될 수 있습니다. 보안은 엔터프라이즈의 IoT 도입을 가로막는 장벽이자 가장 큰 우려 사항으로 남아 있습니다.

IoT 를 고려하는 많은 기업들이 애플리케이션을 보호할 수 있는 내부 역량을 갖추고 있지 않으므로 고유한 보안 요건을 지원할 수 있는 서비스 프로바이더를 고려합니다. 이는 서비스 프로바이더에게 기본적인 연결 서비스를 넘어 새로운 시장에 진입할 수 있는 중요한 기회를 의미합니다. 서비스 프로바이더는 진화를 통해 IoT 연결과 보안을 제공해야 합니다.

보안을 수익 창출 요인으로 활용할 수 있는 또 다른 분야는 5G SECaaS(Security as a Service)입니다. 5G 도입의 이점은 공유 인프라를 사용함으로써 여러 관련 산업 전체가 비용과 효율성을 개선할 수 있다는 데 있습니다. 일부 관련 산업에서는 보안을 직접 제어하길 원할 수 있지만 일부 업종에서는 5G 네트워크로 제공되는 특정 보안 서비스를 아웃소싱함으로써 비용을 절감하길 원할 것입니다. 이러한 서비스는 네트워크에서 정책 실행(방화벽, 디바이스 액세스 제어), 네트워크에서 제공되는 인증/지오로케이션(geolocation) 사용 등을 포함할 수 있습니다.

SDN(Software-Defined Networking) 및 가상화 기술을 사용하면 특정 애플리케이션 또는 사용자에 대한 보안 구성이 가능합니다. 5G 서비스 프로바이더는 애플리케이션별 연결을 서로 격리함으로써 사용자별 맞춤형 보안 기능(예: 부가가치 서비스로 심층 패킷 검사 및 분석 모니터링)을 제공할 수 있습니다.

마찬가지로 서비스 프로바이더가 MEC/에지 클라우드 환경에서 타사 애플리케이션을 호스팅하는 경우 애플리케이션에 대한 보안/보장(Assurance) 서비스를 제공할 수 있습니다. 예를 들어 설치 시, 업그레이드 중, 또는 서비스 재시작 시 애플리케이션에 대한 무결성 보장 검사를 수행할 수 있습니다. 또는 사용자 식별을 위해 신뢰할 수 있는 타사 MEC 애플리케이션에 보안 서비스 API 를 노출시킬 수 있습니다.

## 결론

보안은 성공적인 5G 서비스 제공을 위한 필수 구성 요소입니다. 서비스 프로바이더는 보안 전략이 5G 혁신 로드맵의 핵심 요소로 계획되고 있는지 확인해야 합니다.

현재의 모바일 네트워크 보안 성능 및 운영은 병목현상 없이 5G 요건을 충족하면서 확장 및 확대가 가능해야 합니다. 또한 에지 컴퓨팅, CUPS/분산 코어 및 네트워크 슬라이싱은 새로운 공격 경로를 생성하므로 서비스 프로바이더는 위협을 대응할 수 있는 적절한 보안 조치를 구현해야 합니다. 마지막으로 5G 및 IoT 시대에는 보안을 단순히 의무 사항으로 여기서는 안 됩니다. 서비스 프로바이더는 주요 서비스 차별화 요소이자 필수 수익 창출 요소로 보안을 포지셔닝해야 합니다.