5G 환경을 위한 멀티 클러스터 기반 보안 강화 아키텍처 설계

서강[1], 김지수[2], 남재현[3]
[1]단국대학교 소프트웨어학과 학부생
[2]단국대학교 인공지능융합학과 석사과정
[3]단국대학교 컴퓨터공학과 교수
tjrkd3869@dankook.ac.kr, imjs0807@dankook.ac.kr, namjh@dankook.ac.kr

A Security-Enhanced Multi-Cluster Architecture for 5G Networks

Kang Seo[1], Ji-Su Kim[2], Jaehyun Nam[3]
[1]Dept. of Software Science, Dankook University (Undergraduate Student)
[2]Dept. of AI-based Convergence, Dankook University (Graduate Student)
[3]Dept. of Computer Engineering, Dankook University (Professor)

요 약

5G 네트워크는 클라우드 네이티브 및 마이크로서비스 아키텍처 기반으로 설계되어 고속성, 저지연성, 대용량 연결을 지원하는 차세대 통신 인프라로 자리 잡고 있다. 이에 따라 각 네트워크 기능(NF)은 컨테이너 단위로 구성되어 클러스터 환경에서 운영되며, 확장성과 유연성을 제공하는 한편, 기능 혼재에 따른 보안 경계의 불명확성과 구조적 복잡성으로 인해 다양한 보안 취약점을 내포하게 된다. 본 논문에서는 5G 코어 네트워크를 기능적 역할 기준으로 분류하고, 현재 구조의 보안 및 운영상 문제점을 분석하였다. 이를 해결하기 위한 방안으로, 민감도 기반의 NF 분리를 통해 각 기능을 독립적인 클러스터에 배치하고, mTLS 기반의 클러스터 간 통신 보호를 적용한 멀티 클러스터 보안 강화 아키텍처를 제안한다. 이를 통해 민감 정보 보호, 침해 확산 억제, 정책 기반 흐름 제어를 실현하고, 5G 네트워크의 보안성과 운용 유연성을 동시에 향상시키고자 한다.

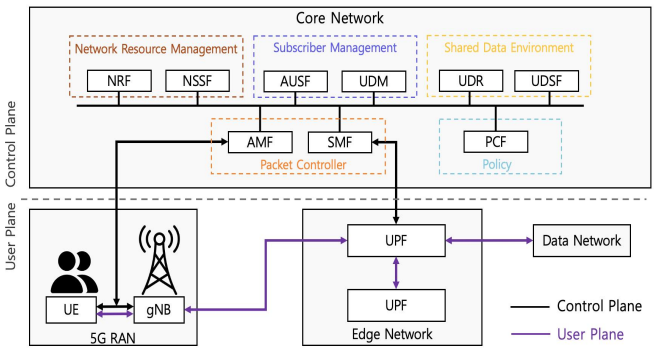
1. 서론

5G 이동통신 기술은 초고속, 초저지연, 초연결이라는 핵심 목표를 달성하기 위해 클라우드 네이티브 및 마이크로서비스 아키텍처를 적극적으로 채택하고 있다 [1]. 이에 따라 5G 코어 네트워크는 각 네트워크 기능(Network Function, NF)을 컨테이너 단위로 분리하여 구성하고, 이를 클러스터 환경에서 운영함으로써 유연성과 확장성을 확보하고 있다. 그러나 이러한 구조는 운영 복잡성과 함께 새로운 보안 위협을 동반하며, 특히 민감한 기능이 단일 클러스터에 혼재되어 배치될 경우 보안 경계가 불분명해지는 문제가 발생한다 [2].

본 논문에서는 일반적인 5G 네트워크 구조를 기반으로, 기존 구조가 지니는 구조적·보안적 한계를 분석하고, 이를 개선하기 위한 멀티 클러스터 기반 아키텍처를 제안한다.

2. 5G 네트워크 구조 및 역할 분석

5G 네트워크는 기능적 역할에 따라 다양한 네트워크 기능(Network Function, NF)으로 구성되며, 이



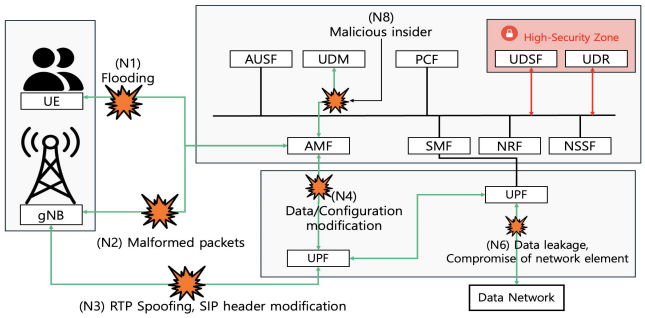
(그림 1) 서비스 역할에 따른 주요 컴포넌트 구조

를 크게 다섯 가지 범주로 구분할 수 있다. Packet Controller는 AMF와 SMF로 구성되어 단말의 접속, 이동성, 세션 생성 및 트래픽 경로 설정을 담당하며, 제어 평면의 핵심 구성 요소로 사용자 트래픽이 설정된 경로를 따라 효율적으로 전송되도록 한다. Network Resource Management는 NRF와 NSSF를 통해 서비스 디스커버리와 네트워크 슬라이싱 기능을 제공한다. Subscriber Management는 AUSF와 UDM이 사용자 인증 및 가입자 데이터 관리를 수행하며, 단말의 정당한 접속을 보장하고 사용자 상태

의 일관성을 유지하는 데 기여한다. Policy 기능은 PCF가 담당하여 QoS, 접근 제어와 같은 네트워크 정책을 제어하고 관련 정보를 각 기능에 전달한다. Shared Data Environment는 UDR과 UDSF로 구성되며, 각 NF가 참조 가능한 공통 데이터 저장소로서 서비스 연속성과 데이터 일관성을 보장한다.

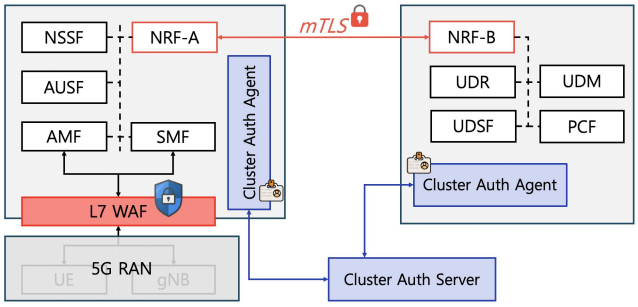
이러한 역할 기반 구조는 5G 코어 네트워크의 복잡성을 기능 단위로 분해하고, 보안성 및 확장성 측면에서 클러스터 분리를 설계하는 데 유의미한 기준을 제공한다.

3. 기존 5G 네트워크 구조의 보안 문제점



(그림 2) 기존 5G 네트워크 구조의 보안 문제점

(그림 2)에서 볼 수 있듯이 현재의 5G 네트워크는 보안성과 운영 측면에서 여러 한계를 내포하고 있다. 민감 정보(예: 가입자 인증 정보 등)를 처리하는 NF들이 일반 제어 기능과 동일한 보안 영역에서 운영될 경우, 침해 발생 시 피해가 연쇄적으로 확산될 수 있다. 또한 클러스터 간 통신이 암호화되지 않거나 단일 인증서 체계에 의존하면 내부자 공격이나 인증 우회에 취약해진다. 제어 평면과 사용자 평면 간 경계가 불분명할 경우, DoS나 Flooding 공격이 전체 트래픽 경로를 마비시킬 수 있으며 [2], 예를 들어 AMF 침해를 통해 UDM 접근이 가능해질 경우 가입자 데이터의 무단 조회나 조작이 발생할 수 있다. 이러한 구조적 문제는 기능 분리와 보안 경계 강화를 통해서만 근본적으로 해결될 수 있다.



(그림 3) 멀티 클러스터 기반 보안 강화 아키텍처

4. 멀티 클러스터 기반 보안 강화 아키텍처

이러한 문제점을 해결하기 위해 (그림 3)과 같이 네트워크 기능의 민감도를 기준으로 각 NF를 별도의 클러스터로 분리하여 운영하는 멀티 클러스터 기반 아키텍처를 제안한다.

제안 구조는 크게 세 가지 클러스터로 구성된다. 첫째, UDM, UDSF 등 민감 데이터를 처리하는 기능은 '민감 클러스터'로 별도 분리하여, 외부 노출 가능성을 최소화한다. 둘째, AMF, SMF, PCF 등 세션 제어 및 정책 적용을 수행하는 기능은 '제어 클러스터'에 배치하여 운영 효율성을 높이고, 민감 클러스터와는 mTLS 기반 상호 인증을 통해서만 통신하도록 제한한다. 셋째, 사용자 트래픽을 처리하는 UPF는 '사용자 평면 클러스터'로 독립 운영되어, 제어 트래픽과의 경계를 명확히 한다. 이 구조는 각 클러스터 간 통신을 mTLS 기반으로 보호하고, 클러스터 단위의 정책 적용 및 트래픽 제어를 통해 구조적 보안성과 운영 유연성을 동시에 확보할 수 있도록 한다.

5. 결론

본 논문에서는 현재 5G 네트워크 구조의 보안적 한계를 식별하고, 이를 해결하기 위한 멀티 클러스터 기반 아키텍처를 제안하였다. 기능 간 민감도를 기준으로 NF를 클러스터 단위로 분리하고, 클러스터 간 통신을 암호화하고 제어함으로써, 보안성과 운영 효율성을 동시에 확보할 수 있는 구조를 설계하였다. 향후 연구에서는 제안 구조를 실제 네트워크 시뮬레이션 환경에 적용하여, 성능 및 보안성에 대한 정량적 평가를 수행할 계획이다.

Acknowledgement

이 논문은 2025년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임. (No.RS-2024-00398379, (총괄4-세부2) 텔코용 고성능/고가용성 6G 크로스-클라우드 인프라 기술개발)

참고문헌

[1] J. Pang, et al., "A new 5G radio evolution towards 5G-Advanced.", Science China Information Sciences, 2022.

[2] A. Dutta, et al., "5G security challenges and opportunities: A system approach.", 5GWF, IEEE, 2020.