

5G UPF 오프로드 기반 MEC 기술 동향



이문원 _ 나인테일 시 대표, 애지컴퓨팅 아키텍트
박선례 _ TTA 지능정보융합소프트웨어단 수석연구원

1. 머리말

5G UPF의 등장은 MEC의 설치 방식에 근본적인 변화를 가져왔다. UPF의 UL-CL(Uplink Classifier) 기반 트래픽 오프로드 기능은 기존 MEC를 In-line 방식으로 설치할 때 발생하는 이동성, 과금, 감청 지원 등의 문제를 효율적으로 해결한다. 본고에서는 이러한 변화가 MEC 기술에 미치는 영향을 네트워킹과 컴퓨팅 사이드로 나누어 살펴보고, 새롭게 부상하는 PAC(Programmable Acceleration) 기술 기반으로 UL-CL 오프로드 성능을 개선하는 방안을 제시한다.

2. LTE망에 MEC 도입 시 기술적 어려움

MEC는 모바일 백홀 구간의 S1 트래픽을 탭(Tap) 또는 DPI와 같은 In-line 장비처럼, ‘Bump in the wire(BIW)’ 방식으로 오프로드하는 장비로 설계되었다¹⁾. 태생이 3GPP 기술 표준과 합의 없이 만들어

진 ‘외부’ IT 장비였으므로, BIW 방식으로 망에 배치되기 위해서는 기존 3GPP 장비들의 설정이나 운용에 변화를 요구하지 않는 투명성이 요구되었다.

따라서 LTE 상용망에 MEC 장비를 도입하려면 <표 1>에 나열된 GTP 핸드링, DSCP 매칭, 트래픽 오프로드 정책, C-플레인 패시브 탭핑과 같이 S1 트래픽 오프로드와 관련된 MEC 본연의 기능들이 통신사업자 기준(carrier-grade, 통상 99.999% 가용성)에 부합하는 것 외에 보안, 이동성 관리, 계량/과금/합법적 감청[3] 지원, 페이징 지원 등 3GPP 플로우의 무결성을 보장하기 위한 추가적인 수단이 필요했다⁴⁾.

즉, 로컬 기지국 인근에 배치된 MEC가 애플리케이션 트래픽을 오프로드할 경우, 원래 S1 트래픽이 거쳐 갔어야 할 코어망의 SeGW, S-GW, P-GW 등 앵커(anchor) 노드들이 데이터를 수신하지 못하게 되고, 결국 망 운용을 위한 필수 기능을 수행할 수 없는 문제가 발생한다(<표 2>).

1) ETSI MEC 표준 그룹은 백홀 구간 상에서, MEC 설치 위치와 상관 없이, S1 트래픽을 오프로드하는 모든 방식을 ‘Bump in the wire’로 구분한다[1].

<표 1> S1 트래픽 오프로드 관련 MEC 주요 기능[2]

Category	Description
U-Plane Support	<ul style="list-style-type: none"> U-Plane interception <ul style="list-style-type: none"> GTP-U header reconstruction(w/PDCP SN & GTP-U SN persistence) TNL IP header reconstruction(w/DSCP persistence) Fast IP rerouting based on link supervision(e.g. w/BFD) DSCP(in TNL IP)-based traffic bypass
C-Plane Support	<ul style="list-style-type: none"> Passive tapping on RRC & NAS messages <ul style="list-style-type: none"> Signaling and data radio bearers(SRBs & DRBs), S1-AP, NAS messages Monitoring on Cell Trace(LTE644 & LTE459) interface
Traffic Offload Policy (TOP)	<ul style="list-style-type: none"> eRAB admission policy decision <ul style="list-style-type: none"> Subscriber profile ID filter QCI(Quality Class Indicator) filter eRAB ARP filter Packet admission policy decision <ul style="list-style-type: none"> 3-tuple filter (*Application-specific filters are off the TOP scope)
Security Support	<ul style="list-style-type: none"> IPSec-based Backhaul Security <ul style="list-style-type: none"> IPSec in tunnel mode, w/Encapsulated Security Payload(ESP) Encryption(e.g. AES-128-CBC), integrity protection(e.g. HMAC-SHA) Connection negotiation(e.g. IKEv1), authentication(e.g. X.509)

<표 2> MEC 도입에 의한 LTE망의 무결성 훼손 문제

LTE 코어망 기능	앵커 노드	'BIW' MEC 설치 방식의 문제점
보안(IPSec)	SeGW	S1 링크에 IPSec이 적용된 경우 트래픽 오프로드가 불가능하므로, 보안 게이트웨이(SeGW) 상단으로 MEC 설치 위치를 제한하거나, 통신사업자와 합의를 통해, IPSec 적용을 해제해야 함. IPSec 인증서를 복사하는 등의 방식으로 트래픽 오프로드를 허용할 경우, 3GPP 보안의 무결성이 훼손됨
이동성 관리	S-GW	UE-AF 간 세션이 이동성 앵커인 S-GW를 거치지 않으므로, UE가 핸드오버할 경우 애플리케이션 세션의 연속성이 보장되지 않음
계량 & 과금	P-GW (& S-GW)	UE-AF 간 세션이 계량 & 과금 앵커인 S/P-GW를 거치지 않으므로, 데이터 사용량을 계량하고 요금 정산을 하기 위한 CDR을 생성할 수 없음 ²⁾
합법적 감청	S-GW	UE-AF 간 세션이 합법적 감청(lawful interception) 앵커인 S-GW를 거치지 않으므로, 법집행기관(LEA)의 감청 요청 시 탐핑 지원이 불가능함
페이징(Paging)	MME	MEC 앱이 푸쉬 메시지를 전송할 경우, 먼저 페이징으로 IDLE 모드인 사용자 단말을 깨워야 하지만, 페이징 요청을 보낼 SGW-MME 간 S11 인터페이스가 없음 ³⁾

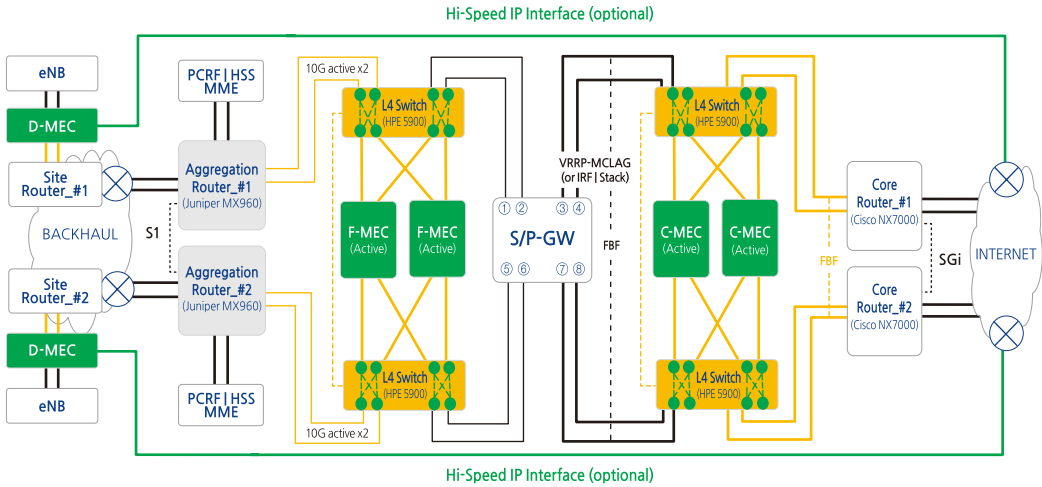
3. MEC 무결성에 요구되는 기술적 복잡성

BIW 방식의 무결성 문제를 해결하면서 MEC를 LTE 상용망에 배치하는 검증된 방안은 코어망의 S/P-GW

상단에 C(core)-MEC, 하단에 F(Filter)-MEC 노드를 추가하는 것이었다. 즉 계량, 과금, 합법적 감청, 페이징 기능이 온전히 수행되려면, 사용자 데이터 플로우가 앵커 노드인 S/P-GW를 완전무결하게 거쳐야만

2) MEC는, S-GW와 달리, IMSI, IMEI, (User) IP, APN, (셀 수준의) 사용자 위치 정보에 대한 접근이 불가능하기 때문에 CDR을 직접 생성할 수 없다[5].

3) MEC는 S1-MME (NAS) 메시지를 투명하게 처리하므로, 인바운드 콜/SMS의 경우 페이징은 정상 동작한다.



※ 출처: 나인테일 AI(moon.lee@ninetail.ai)

[그림 1] C/F/D-MEC 네트워크 설치 구조, 10Gbps 이중화망

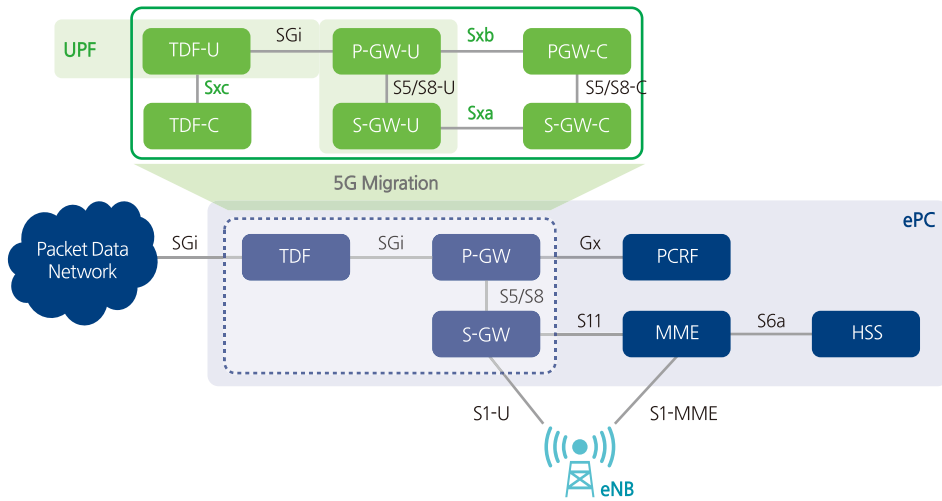
한다. 이것은 망 무결성을 위해 사용자가 요청한 콘텐츠나 앱이 D-MEC에 존재하는 경우에도, C-MEC가 의도적으로 발생시키는 인위적인 트래픽이다. 따라서 S-GW 바로 하단에서 F-MEC가 이를 제거(filtering)함으로써 고가의 S1 대역폭 낭비를 방지했다.

C-MEC는 일종의 마스터 노드로서 D-MEC 간의 끊임 없는 핸드오버를 보장하며, 실시간 MEC 자원의 상태를 관리하는 EMS 역할을 수행한다. 토폴로지 상에서 C-MEC는 한 레벨 높은 수준의 에지지만, D-MEC가 설치 안된 기지국을 포함한 코어망 커버리지 전체에 MEC 서비스를 제공한다는 점이 높은 TCO를 정당화하는 주요 가치 제안이었다(그림 1).

동시에 C/F/D-MEC 노드들로 구성된 'MEC 오버레이 네트워크'는 다수의 진보적인 전송/보안 관련 VAS를 통신망에 이식하는 플랫폼 역할을 제공했다. 대표적으로 다음과 같은 기능들은 ByteMobile, Mobixell, Flash Networks, Qwilt 등 '모바일 트래픽 최적화' 솔루션들의 핵심 기능들이기도 하다.

- ① HTTP / Transparent 캐시: 웹페이지 및 동영상, 이미지 등 정적인 콘텐츠를 로컬 전송하여 지연 및 대역폭 소비 절감
- ② Byte 캐시: 콘텐츠를 해시 기반 청크(chunk) 또는 토큰(token)으로 변환 후 전송함으로써 S1 트래픽 절감(50% 이상)[6]
- ③ TCP 혼잡 제어: CUBIC, ExLL 등 알고리즘 기반으로 병목 노드의 버퍼 오버플로우를 방지함으로써 전송 지연 개선[7]
- ④ TCP (변수)최적화: MSS, TCP-IW, 최대 소켓 수의 동적 제어를 통한 QoE(주로 비디오 다운로드 속도) 개선
- ⑤ HTTPS 프록시: SSL, TLS, HTTP/2 기반 보안 콘텐츠를 로컬 전송하여 전송속도 개선

그러나 코어망에 C/F-MEC 노드를 추가하게 되면 고가용성(High Availability[8]) 설계를 포함한 네트워크 통합(NI) 및 운용 상의 기술적 부담과 비용이(기지국 수준에서 운영하는 그것과는) 차원이 다르게 높아질 뿐만 아니라, 새로운 버전을 출시할 때마다 각 통신 인프라 벤더의 eNB, ePC, EMS 장비와 100% 호환성 인증을 마쳐야 상용망 배포가 가능했으



※ 출처: 나인테일 AI

[그림 2] CUPS: S/P-GW C-플레인과 U-플레인의 분리⁵⁾

로, 사실상 MEC 제품 개발은 노키아(Nokia), 화웨이(Huawei) 등 주요 인프라 벤더들로 제한되었다.

이후 2014년 ETSI 표준화와 함께 MEC 개발 생태계가 크게 확산되었지만, 주요 인프라 벤더 외에 3G/LTE/5G 망을 모두 지원하는 ‘Multi-RAT’ MEC 솔루션을 내놓은 기업은 Athonet, AlefEdge, MobilEdgeX, Saguna 정도로 여전히 제한적이다⁴⁾.

4. 5G CUPS 도입과 MEC 설치의 단순화

3GPP 릴리스 14 표준[11]에 정의된 CUPS는 S-GW와 P-GW의 C-플레인 기능(CPF)을 중앙의 코어망에 U-플레인 기능(UPF)을 여러 지역에 분산 배치함으로써, 사용자 단말의 세션이 현재 연결(attach)된 기지국

과 가장 가까운 UPF를 통해 서비스되도록 설계된 아키텍처이다. 새로 정의된 UPF-CPF 간 Sxa, Sxb, Sxc 인터페이스를 통해 사용자 세션이 가까운 Immediate-UPF에서 오프로드 되거나, N9 인터페이스를 통해 다른 PDN 세션 앵커로 릴레이되는 모든 경우에 <표 2>의 보안, 이동성, 과금, 감청, 페이징 등 상용망의 무결성 보장을 위한 투명한 시그널링을 제공한다(그림 2).

CUPS는 4G LTE 표준에 속하지만, 5G의 핵심 서비스인 고신뢰 초저지연(URLLC) 애플리케이션과 네트워크 슬라이싱 지원을 위해, 처음부터 MEC 연동을 고려하여 설계되었다. CUPS에 의해 기지국 레벨에 분산 배치된 UPF의 주요 기능은 <표 3>과 같다[13].

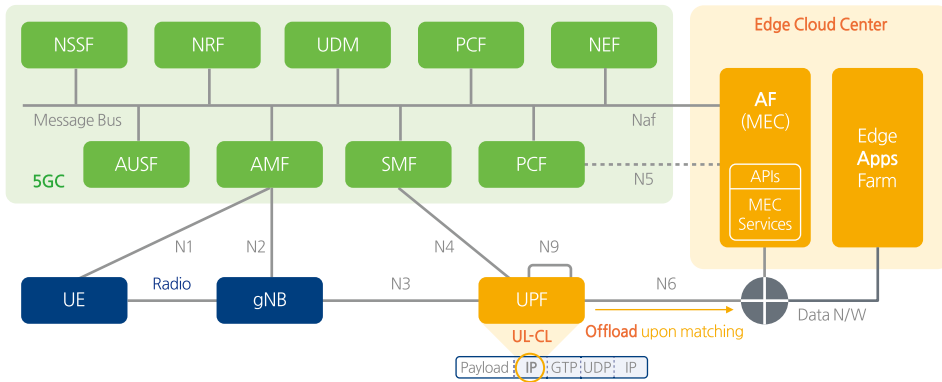
UPF는 <표 3>의 ‘L3 라우팅 & 오프로드’에 명시된 UL-CL 기반의 분기점(Branching Point) 역할을 수행

4) BIW 방식 외에, S-GW 또는 S/P-GW를 기지국 레벨에 분산 배치하고 S1 트래픽을 MEC 방향으로 스티어링하는 LBO 방식이 vEPC/MEC 벤더인 Athonet에 의해 상용화된 바 있다[9]. ① 재난망, 독립형 엔터프라이즈 LTE망용으로 설계된 분산 S/P-GW 솔루션은 APN, CSG 기반으로 트래픽을 오프로드하는 LIPA와 유사하고, ② 통신사업자 MEC용으로 설계된 SGW-LBO 솔루션은 정책에 따라 선택적으로 트래픽을 오프로드하는 동시에 코어망과의 S1 연결을 계속 유지한다는 점에서 SIPTO에 가깝다[10]. 지면 관계 상, 분산 S-GW, P-GW를 이용한 LBO 방식의 세부 내용은 본고에서 다루지 않는다.

5) TDF의 L7 트래픽 식별 방식은 DPI와 동일하지만, PCRF에 대한 Gx/Sd 인터페이스와 과금 시스템(OCs)에 대한 Gy/Gyn 인터페이스를 지원한다는 점이 주요한 차이점이다. 식별된 서비스에 대해서는 charging report, redirection, limitation 등의 기능을 수행할 수 있다[12].

<표 3> UPF의 기능

UPF 기능	설명
DN 게이트웨이 (GTP 핸드러링)	Interconnect point between the mobile infrastructure and the Data Network(DN), i.e. encapsulation and decapsulation of GPRS Tunneling Protocol for the user plane(GTP U)
Mobility 앵커 for intra/inter-RAT)	Protocol Data Unit(PDU) session anchor point for providing mobility within and between Radio Access Technologies(RATs), including sending one or more end marker packets to gNB
L3 라우팅 & 오프로드	Packet routing and forwarding, including performing the role of an Uplink Classifier / UL-CL(directing flows to specific data networks based on traffic matching filters) and a Branching point, when acting as an Intermediate UPF(I-UPF) multi-homed to more than one PDU session anchor(PSA)
L2 스위칭 (addressing)	Functionality to respond to Address Resolution Protocol(ARP) requests and / or IPv6 Neighbor Solicitation requests based on local cache information for the Ethernet PDUs
L7 애플리케이션 식별	Application detection using Service Data Flow(SDF) traffic filter templates[14] or 3-tuple(protocol, server-side IP address and port number) Packet Flow Description(PFD) received from SMF
플로우 기반 QoS	Per-flow QoS handling, including transport level packet marking for UL/DL, rate limiting and reflective QoS(DSCP) marking on DL. Uplink Traffic verification(SDF to QoS Flow mapping)
트래픽 정책 (Policing)	User Plane part of policy rule enforcement, e.g. Gating, Redirection, Traffic steering
과금 & 감청 지원	Traffic usage reporting for billing and Lawful Intercept(LI) collector interface



※ 출처: 나인테일 AI

[그림 3] 5GC UL-CL 기반 에지 클라우드 센터의 구성

하며, 이는 <표 1>에 나열된 MEC의 ‘S1 트래픽 오프로드 주요 기능’을 대체한다⁶⁾. 따라서, MEC는 3GPP 5G 표준 상의 AF로 역할이 축소된 한편, PCF와 직접 메시

징을 주고받을 수 있는 N5 인터페이스가 추가되면서 3GPP 5G 네트워크와의 연동이 한층 강화되었다(그림 3).

6) UPF UL-CL 트래픽 오프로드의 새로운 기능은 ① IPv6 (IPv4 동시) 지원, ② 소스 IP 기반의 UL-CL, ③ S1 구간의 N3(to gNB), N9(between I-UPF and other PSA(s)) 인터페이스에 GTP(w/ header extensions for 5G) 외 세그먼트 라우팅(SRv6 or NSH) 또는 ICN 프로토콜의 지원한다.

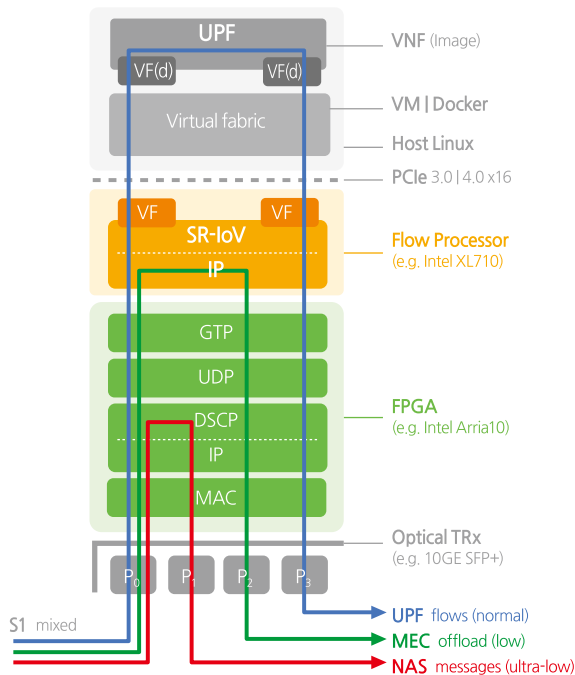
5. UL-CL 오프로드 성능의 최적화: PAC (Programmable Acceleration)

TaaS(Telco as a Service) 비전을 실현하기 위한 인프라 환경으로 넷옵스(NetOps)가 부상하면서 x86 화이트박스 기반의 5G NF 도입이 보편화되고 있다. 통상 UPF도 멀티코어 Xeon 리눅스 호스트와 오픈스택/VM 또는 Kube/Docker 컨테이너 기반 가상화 인프라 상의 VNF로 운영되는 것이 일반적이다. 문제는 U-플레인 성능인데, CPU 코어/소켓 수와 S1 트래픽 처리량은 선형적으로 비례하지 않으며, CPU pinning, SR-IoV, OVS-DPDK 등 성능 튜닝을 해도 8-10Mbps 수준을 벗어나지 못하는 경우가 많다.

이는 비디오, 이미지 등 데이터 병렬성이 높은 다수의 라지 패킷에 웹서치, 채팅 등 비정형 데이터 타

입의 스몰 패킷이 불규칙적으로 결합된 4G/5G 트래픽의 처리에 비효율적인 CISC 기반 범용 CPU 구조와 NIC 메모리-PCIe-CPU-메인 메모리를 오가며 잦은 풀링(Pooling)과 인터럽트(Interrupt)가 발생하는 x86 아키텍처에 기인한다.

대안으로 L3 이더넷 플로우 엔진을 탑재한 PAC(또는 Smart NIC) 카드의 FPGA에 UL-CL 로직을 추가로 구현하는 방법이 있다. S1 패킷이 'MAC-IP-UDP-GTP-IP x Parser-Filter-Classifier-Steering' 스테이지 단위로 구분된 게이트 로직을 거치는 동안, 풀링 없이, 고속의 병렬 처리를 제공하며, 플로우 숫자가 늘어나도 와이어 스피드(Wire-speed)에 이를 때까지 선형적 처리량 증가를 보장하는 솔루션은 사실상 FPGA가 유일하다. PAC에서 S1 트래픽을 오프로드하는 만큼 UPF VNF의 처리 용량이 보전되



※출처: 나인테일 AI

[그림 4] PAC 기반 UPF 트래픽 오프로드 가속

므로 TCO를 크게 절감하는 동시에, PCIe-CPU-메모리 구간 RTT 만큼의 지연 개선을 기대할 수 있다⁷⁾(그림 4).


6. 맺음말

3GPP 요소인 UPF가 MEC의 트래픽 오프로드 기능을 대체함에 따라, 트래픽 오프로드를 위해, non-3GPP VAS 장비처럼, MEC를 3GPP 파이프라인 상에 In-line 방식으로 설치하지 않아도 된다. 이는 MEC의 패브릭 네트워킹 기능 요소가 Telco 'IT'에서 메인스트림 'Telco' 영역으로 이전되었으며, MEC의 'M'(Multi-access)은 통신사업자와 주요 인프라 벤더가 사실상 주도하고, 'EC'(Edge Computing)는 기존 MEC 그룹의 주력 기술 영역으로 재편될 것임을 시사한다.

네트워킹 관점에서도 MEC의 주력은 패브릭 네트워킹이 아닌 서버 사이드 네트워킹이다. 따라서 UPF와 같은 패브릭 사이드 노드에는 VNF를 서버 사이드의 에지 컴퓨팅 노드에는 VAF를 탑재하는 것으로 컴퓨팅 사이트의 구분도 명확해졌다.

결론적으로 MEC 기술 영역은 '서버 사이드 네트워킹과 컴퓨팅, 그리고 상위의 5G URLLC와 실감형 미디어 애플리케이션을 통신사의 에지 클라우드 환경에 최적화하는 것'으로 재정의할 수 있다. 기술적 장벽이 낮아진 만큼 국내 기술 기업들의 진입이 활발해지고 MEC 생태계가 확대될 것으로 예상된다.

한편, UPF를 x86 기반 가상화 인프라 환경에서 운영 시 U-플레인 성능이 문제점으로 지목된다. 특히 UPF 워크로드를 CPU로 처리하면 프로세서 코어를 늘려도 처리량이 선형적으로 늘지 않는 확장성 문제

가 해결되어야 한다. 이를 해결하기 위해 UPF 워크로드를 CPU에서 FPGA 기반의 PAC 카드로 오프로드하는 기술이 다양하게 시도되고 있다. 다음 단계로, 선택한 PAC 하드웨어 성능을 최적화하고 5G 망에 요구되는 PAC 소프트웨어 IP 확보하고 망에 통합하는 작업이 요구된다. 

※ 이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 '범부처 Giga KOREA 사업'의 지원을 받아 수행된 연구임[No.GK17P0400, (초저지연-총괄/세부) 저지연융합서비스를 위한 모바일 에지 컴퓨팅 플랫폼 기술 개발].

[참고문헌]

- [1] 'MEC Deployments in 4G and Evolution Towards 5G', ETSI White Paper No.24, 2018. 2.
- [2] '5G 초저지연 서비스 구현을 위한 NFV 기반 MEC 기술', 이문원, TTA 저널 174호, 2017. 11.
- [3] '3G Security: Lawful Interception Requirements', ETSI TS33.106, 1999.
- [4] 'SGW-LBO Solution for MEC Taking Services to the Edge', Athonet White Paper, 2016.
- [5] 'S-GW CDR Field Descriptions', GTPP Interface Administration and Reference, Cisco, 2017. 1.
- [6] 'A Technical Review of Caching Technologies', Symantec White Paper, 2017.
- [7] 'ExLL, An Extremely Low-Latency Congestion Control for Mobile Cellular Networks', Shinik Park et al., ACM CoNEXT 2018. 12.
- [8] 'Designing for Redundancy', Elaine Lopes, Campus Network for High Availability Design Guide, 2008.
- [9] 'Deploying CPU-Intensive Applications on MEC in NFV Systems: The Immersive Video Case', Giorgio Cattaneo et al., MDPI Computers Journal, 2018. 10.
- [10] '3GPP 데이터 오프로딩 기술', 최성구 외, 전자통신동향분석 30권 4호, 2015. 8.
- [11] 'Architecture Enhancements for Control and User Plane Separation of EPC Nodes', ETSI TS23.214, 2017. 7.
- [12] 'Policy Traffic Switch Overview', Sandvine, 2017.
- [13] 'System Architecture for the 5G System(5GS)', ETSI TS123.501, 2019. 4.

7) NAS 메시지는 DSCP 기반 오프로드 룰을 설정하면 지연을 더욱 단축할 수 있다.

[14] '3GPP Service Data Flows - LTE/HSPA/EPC knowledge nuggets', Neil Wiffen, 4G-Seminar, 2013.

[주요 용어 풀이]

- AMF: Access and Mobility Management Function
- APN: Access Point Name
- ARP: Address Resolution Protocol
- AUSF: Authentication Server Function
- BFD: Bidirectional Forwarding Detection
- BNG: Border Network Gateway
- CDR: Charging Data Record
- CSG: Closed Subscriber Group
- CUPS: Control and User Plane Separation
- DPI: Deep Packet Inspection
- DSCP: Differentiated Services Code Point
- ePC: Evolved Packet Core
- eRAB: evolved Radio Access Bearer
- EMS: Element Management System
- ETSI: European Telecommunication Standards Institute
- FPGA: Field Programmable Gate Array
- GTP: GPRS Tunneling Protocol
- HSS: Home Subscriber Server
- ICN: Information Centric Networking
- IMEI: International Mobile Equipment Identity
- IMSI: International Mobile Subscriber Identity
- IPS: Intrusion Prevention System
- LBO: Local Breakout
- LEA: Law Enforcement Agency
- LIPA: Local IP Access
- MEC: Multi-Access Edge Computing,
- MME: Mobility Management Entity
- MSS: Maximum Segment Size
- NAS: Non-Access-Stratum
- NRF: Network Repository Function
- NSH: Network Service Header
- NSSF: Network Slice Selection Function
- OCS: Online Charging System
- OVS-DPDK: Open Virtual Switch Data Plane Development Kit
- PCF: Policy Control Function
- PCRF: Policy and Charging Rules Function
- PDCP: Packet Data Convergence Protocol
- PGW: Packet Data Gateway
- QoE: Quality of Experience
- RAT: Radio Access Technology
- SeGW: Security Gateway
- SIPTO: Selected IP Traffic Offload
- SGW: Serving Gateway
- SMF: Session Management Function
- SR-IoV: Single Root I/O Virtualization
- SSL: Secure Socket Layer
- TCO: Total Cost of Ownership
- TCP-IW: TCP Initial Window
- TDF: Traffic Detection Function
- TLS: Transport Layer Security
- TNL: Transport Network Layer
- UDM: User Data Management
- UDP: User Datagram Protocol
- URLLC: Ultra Reliable and Low Latency Communication
- VAF: Virtual Application Function
- VAS: Value Added Service
- VNF: Virtual Network Function
- VPN: Virtual Private Network