J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

차세대 mBcN을 위한 5G+ 연동보안게이트웨이☆

A Cooperative Security Gateway cooperating with 5G+ network for next generation mBcN

남 구 민[1] 김 형 식[2*] 이 현 진[3] 조 학 수[4]
Gu-Min Nam Hyoungshick Kim Hyun-Jin Lee Hark-Su Cho

요 약

차기 mBcN에서는 초고속·초연결을 지원할 수 있는 무선망과 연계할 수 있도록 구축되어야 한다. 본 논문에서는 5G 무선망과 mBcN의 연계하기 위한 연동망 구조와 연동에 필요한 연동보안게이트웨이의 구조를 제안한다. 제안하는 연동보안게이트웨이는 gNB와 UPF의 사이에 위치하며 LBO 기능, SFC 기능 및 다양한 보안 기능을 제공한다. 제안하는 연동망 구조 및 연동보안게이트웨이를 통해 다양한 이점을 확보할 수 있다. 첫 번째는 mBcN망과 연결이 필요한 사용자 단말은 5G망의 무선망을 활용하여 mBcN망과 연결할 수 있다. 두 번째는 mBcN으로 전달되는 트래픽은 5G 코어망을 경유하지 않고 mBcN으로 전송되어 5G 코어망에 망부하를 야기하지 않으면서 종단간 전송 지연을 감소시킬 수 있다. 마지막으로 군응용체계 패킷이 5G코어망으로 전파되지 않고 연동 보안게이트웨이와 연결된 기지국을 통해서만 mBcN과 연결할 수 있어 보안을 유지할 수 있다. 마지막으로 본 논문에서는 5G 테스트배드 환경에서 실험을 통해 제안하는 연동 보안 게이트웨이의 LBO 기능, SFC 기능 및 보안모듈의 기능을 제공 가능함을 제시한다.

☞ 주제어 : 국방광대역통합망, 5G, MEC, LBO, SFC

ABSTRACT

The next generation mBcN should be built to cooperate with the wireless network to support hyper-speed and hyper-connectivity. In this paper, we propose a network architecture for the cooperation mBcN and 5G commercial network and architecture of the cooperative security gateway required for the cooperation. The proposed cooperative security gateway is between gNB and UPF to support LBO, SFC, and security. Our analysis shows that the proposed architecture has several advantages. First of all, user equipment connected with the mBcN can be easily connected through the 5G commercial radio network to the mBcN. Second, the military application traffic can be transmitted to mBcN without going through the 5G core network, reducing the end-to-end transmission delay without causing the traffic load on the 5G core network. In addition, the security level of the military application can effectively be maintained because the user equipment can be connected to the cooperative security gateway, and the traffic generated by the user equipment is transmitted to the mBcN without going through the 5G core network. Finally, we demonstrate that LBO, SFC, and security modules are essential functions of the proposed gateway in the 5G test-bed environment.

☞ keyword : military broadband convergence network, 5G, multi-access edge computing, local breakout, service function chaining

1. 서 론

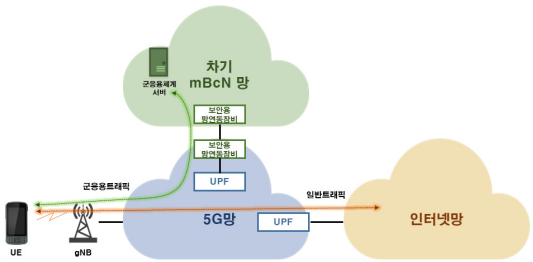
국방광대역통합망(mBcN; military Broadband convergence Network)은 네트워크중심전(NCW; Network Centric Warfare)을 효과적으로 제공하기 위하여 군전화망 및 각 군 C4I 체계 등 다양한 군응용체계를 단일네트워크에서 제공하기 위하여 2006년부터 구축을 진행하였으며 2023년 운영 만료를 앞두고 있다. 이에 차기 mBcN은 민간투자사업자 선정을 진행하여 21년 8월 사업자가 선정되었으며, 2024년부터 향후 10년간 운영될 예정이다[1].

차기 mBcN 구축 사업은 전·평시 안정적인 통신지원과 미래 신규 서비스 요구를 충족하는 초고속·초연결의

[1] Leading Dev. Team, R&D Dept., WINS Co., Ltd, Seongnam, 13487, Korea
[2] Dept. of Computer Science and Engineering, Sungkyunkwan Univ., Suwon, 16419, Korea.
[3] Platform Tech team, R&D Dept., WINS Co., Ltd, Seongnam, 13487, Korea.
[4] R&D Dept. WINS Co., Ltd. Seongnam, 13487, Korea
* Corresponding author (hyoung@skku.edu)
[Received 12 October 2021, Reviewed 20 October 2021, Accepted 5 November 2021]
☆ This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MIST) (No.2020-0-00952, Development of 5G Edge Security Technology for Ensuring 5G+ Service Stability and Availability)

국방 분야 유·무선 통신을 제공하기 위한 핵심 기반 통신 체계를 구축하는데 목적이 있다[2]. 따라서 차기 mBcN은 육·해·공군·해병대사 및 국직 부대 등 전군 범위에서 구축될 예정이다. 개별 항목 별로 살펴보면 차기 mBcN 구축을 통해 후방 및 서북도서 네트워크 개선, 군 자체 운용·제어 가능한 통합망 관리체계 구축, 미래 전장 환경을 고려한 대용량 전송망 구축, 국방 모바일 업무 환경 조성 등 무선망과 연계된 네트워크 구축, 유사통신망 네트워크 통합체계 지원 및 대용량 처리 가능 암호 장비 적용, 통합망 관리 시스템(NMS; Network Management System) 및 망 관리센터 구축이 이루어질 예정이다.

본 논문에서는 초고속·초연결을 지원할 수 있는 국방 모바일 업무 환경 조성에 초점을 두고자 한다. 특히, 초고속·초연결을 지원하기 위해서는 다수의 무선 단말을 수용할 수 있는 광대역 무선 장비의 도입이 요구된다. 그림 1은 차기 mBcN망을 5G 상용망과 연동할 경우의 망구조를 나타내고 있다. 그러나 mBcN만을 위한 광대역 무선 장비를 전국 단위로 구축하는 것은 실효성이 떨어질 뿐만 아니라 구축비용도 기하급수적으로 늘어날 수 있다. 이와 같은 요인을 고려할 경우 민간 통신 서비스를 제공하기 위하여 구축된 5G 무선 장비를 활용하는 것이 필요하다. 그러나 단순히 기존 5G 망과 차기 mBcN을 연동할 경우, 군 응용 체계에서 발생한 트래픽들이 5G 코어망을 경유하여 군 응용 체계 트래픽의 종단간 전송지연(End-to-End transmission delay)이 증가될 뿐만 아니라, 5G 코어망에 다량의 트래픽이 추가로 인가되어 망 혼잡을 야기할 수 있다. 또한, 서비스 요구사항이 다른 다양한 군응용체계가 5G망을 경유해하기 때문에 망 관리 및 제어 측면에서도 문제를 야기할 수 있다. 가장 중요한 문제는 군 트래픽의 특성상 극도의 보안이 요구되는 군응용체계 트래픽들이 5G망을 관통하여 보안상의 문제가 발생할 수 있다는 것이다.



(그림 1) 5G 상용망과 연동한 차기 mBcN망구조도
(Figure 1) Network Architecture of next generation mBcN cooperated with 5G commercial network

이러한 요인들을 고려할 경우 5G망을 통한 차기 mBcN의 모바일망 구성하는데 있어 MEC(Multi-access Edge Computing)개념을 고려할 필요가 있다[3]. MEC는 ETSI(European Telecommunications Standards Institute)에서 Mobile Edge Computing으로 처음 제시된 개념으로 응용서비스를 제공하기 위한 서버를 모바일망의 엣지로 전진 배치하여 전송지연을 최소화시키는 것이다. MEC로 전송되는 서비스 플로우는 LBO(Local Break-Out)를 통해 MEC와 연결된 사설망으로 직접 전달하고, 일반 서비스 플로우는 5G 코어망을 경유하여 인터넷망으로 전달한다. 이와 같은 기능을 통해 MEC용 응용 서비스는 종단간 지연을 감소시킬 수 있으며 코어망의 망부하를 감소시킬 수 있다. 보안 측면에서도 MEC 망으로 전송되는 트래픽은 제어평면에서는 5G 코어망으로 전달되나, 사용자 트래픽은 5G 코어망을 경유하지 않고 MEC 망으로 직접 전달되므로 유리한 이점이 있다.

본 논문에서는 mBcN망과 5G망의 연동 방안과 연동보안게이트웨이에 요구 기능 구성을 제안하고, 시험환경에서 해당 기능들의 제공가능성을 검증하고자 한다. 제안하는 mBcN망과 5G망의 연동 구조는 UPF(User Plane Function)의 앞에 위치한 연동보안게이트웨이를 통한 연동 방안이다. 연동보안게이트웨이는 UE(User Equipment)에서 생성한 서비스 패킷을 확인한 후 전송 경로를 결정하는 LBO 기능, 차기 mBcN망으로 전송되는 패킷에 대해 정상·악성 유무를 판단하는 다양한 보안 기능, 군응용체계별 요구사항에 따라 보안 기능을 선택할 수 있는 SFC(Service Function Chaining) 기능으로 구성된다.

제안하는 망구성 및 연동보안게이트웨이를 적용하면 다음과 같은 장점을 얻을 수 있다. 첫 번째는 5G망과 연동되는 mBcN망은 5G망의 무선접속망(RAN; Radio Access Network)을 사용할 수 있기 때문에 초고속·초연결을 지원할 수 있을 뿐만 아니라, 군응용체계별 요구사항에 따른 네트워크 슬라이스를 할당받을 수 있어 서비스 품질(QoS; Quality of Service)을 향상시킬 수 있을 것으로 예상된다. 두 번째는 연동 보안게이트웨이와 연결된 일부 5G 기지국(gNB; next generation Node-B)을 통해서만 mBcN으로 연결할 수 있어 서비스 반경을 군이 제어할 수 있을 경우, 접속 가능한 단말을 제한할 수 있어 보안 측면에서도 우수한 장점이 있다. 마지막으로 군응용체계의 사용자평면 트래픽은 5G코어망을 경유하지 않고 mBcN망으로 직접 유통되므로 5G 코어망의 망부하를 낮

게 유지할 수 있고 보안 측면에서도 좋은 장점이 될 수 있다.

본 논문은 2장에서는 관련기술의 연구 동향을 살펴보고 3장에서는 본 논문에서 제안하는 5G망과 mBcN의 연동 구조와 연동보안게이트웨이의 요구기능을 기술한다. 4장에서는 제안하는 연동망 구조 및 연동보안게이트웨이의 기능 검증을 위한 시험 환경을 기술하고, 5장에서는 주요 기능에 대한 검증 결과를 기술한다. 마지막으로 6장에서 결론을 맺는다.

2. 관련기술의 연구 동향

2.1 mBcN 기술 동향

mBcN에 대한 구성 및 기술 동향은 군의 보안 특성상 접근 및 분석에 어려움이 있다. [4]에서는 국방종합구조설계방법론(MND-AF; Ministry of National Defence - Architecture Framework) 기반으로 군응용체계별 단독망 구성, BcN망, mBcN망에 대한 네트워크 계층 별 장단점을 분석하고 있다. [5]에서는 NCW를 위한 mBcN망의 요구사항과 아키텍처에 대하여 제시하고 있다. [6]에서는 미래 지휘통제체계를 위한 보안 규정 개선 요구사항을 분석하고 있다. 특히 통합 네트워크 운영관점에서 다계층 전달망을 복수로 구성하고 운용하는 것을 제안하고 있으며, 상용 모바일망 등 외부망과 연결을 확장할 필요성이 있음을 제시하고 있다. [7]에서는 BcN 서비스들이 악성 공격에 대해 지속적인 서비스 운영을 보장하기 위한 네트워크 설계 방법을 제안하고 있다. 이를 위해 서비스 시간과 공간 중요도를 바탕으로 BcN 필수 서비스 구성요소를 서버/게이트웨이/복합 유형으로 분류하고 발생 가능한 공격시나리오들을 통해 BcN 필수 서비스의 침입 감내 기술 적용 방안을 분석하였다. [8]에서는 mBcN을 구성하는데 있어서 네트워크 측면의 핵심 요구 기술에 대하여 정리하고 있으며, 군응용체계별 독립망에서 통합망으로 진화하는데 있어서 각 단계별 참조망 구조 등을 제시하고 있다.

2.2 MEC 기술 동향

5G망에 MEC 서비스를 제공하기 위한 다양한 방안에 대한 연구는 활발히 이루어지고 있다[3],[9-13].

[3], [9]에서는 5G 환경에서 MEC를 구성하기 위한 다양한 망구성 방안, 요구 기능 및 5G 서비스 제공 방안, 기술적인 고려사항, 활용방안 등에 대하여 기술하고 있다. 망구조를 살펴보면 주로 UE를 기준으로 UPF의 뒷단 또는 동일 위치에 MEC를 배치하는 안을 제시하고 있다.

[10]에서는 MEC의 개념과 다양한 서비스 시나리오, MEC 플랫폼 구조 및 기술 동향, 기술적인 과제들에 대하여 분석하고 있다. 특히 Enterprise Deployment 시나리오는 IP-PBX(IP-Private Branch Exchange)와 MEC 플랫폼을 결합함으로써 네트워크 사업자의 엔터프라이즈용 스몰셀과 기업의 WLAN(Wireless Local Area Network)간 통합된 통신서비스를 제공할 수 있다. 이를 위해 MEC 기반의 Breakout을 통하여 사용자의 망 선택에 대한 부하분산, 스몰셀과 WLAN간 접속망 선택, 내부 직원에 대한 접근 제어, IT 정책에 따라 사용자 단말에 대한 관리, 새로운 서비스 및 단말에 대한 보안, 새로운 직원에 대한 신규 접근 제어 및 검증 등에서 효율성을 제공할 수 있다고 명시하고 있다.

[11]에서는 사설 5G망을 구축하는 7가지 안에 대해서 기술하고 있다. 사설 5G망을 구축할 때 공중 5G망과 무관한 독립적인/고립된 사설 5G망을 구축하는 방법, 공중 5G망의 자원을 공유하여 사설 5G망을 구축하는 방안들의 망구성 형태, 서비스 제공 방안, CAPEX(Capital Expenditures)/OPEX(Operating Expenditure) 등에 대하여 비교 정리하고 있다. 특히 6안에서는 MEC-DP(Data Plane)을 활용하여 N3 인터페이스에서 LBO를 제공함으로써 기업망과 공중 5G망을 연동하는 방안을 제시하고 있으며 대표적인 사례로 SKT와 Intel이 MEC-DP를 이용한 사설 5G망을 구축[12]을 명시하고 있다. 본 논문에서는 [11]에서 제시한 다양한 구축 방법 중 6안을 기반으로 MEC를 구축하였다.

[13]에서는 5G 클라우드 환경 및 MEC 환경에서 보안 측면에서 예상되는 다양한 공격 시나리오와 이를 극복하기 위한 보안 구조에 대하여 제시하고 있다.

2.3 5G 테스트베드 기술

5G 관련 기술을 연구하고 개발하는데 있어서 5G 기술 표준의 만족 여부 및 다양한 5G 망요소들과 호환성 유지 여부를 확인하는 것은 기술을 개발하는 것만큼이나 중요한 사항이다. 이를 위해서는 5G망의 다양한 망요소를 모의할 수 있는 테스트베드가 요구된다. 이를 위해 다양한 연구를 통해 공개 소프트웨어 기반의 5G 테스트베드 기술이 제안되었다[14-17].

OpenAirInterface[14]는 4개의 프로젝트 (5G RAN, 5G Core Network, MOSAIC5G, CI/CD)로 구성되어 있으며 C

언어를 사용하여 개발되었다. 3GPP release 15를 기반으로 AMF(Access and Mobility Function), SMF(Session Management Function), UPF와 부분적으로 UE 및 gNB에 대한 개발이 완료된 상태이다. 올해부터 SA 기반의 5G 코어 구현을 진행하고 있다.

Open5GS[15]는 3GPP release 16을 준수하는 C언어 기반의 5G 코어 오픈소스 프로젝트로 AMF, SMF, UPF에 추가로 NRF(Network Repository Function), UDR(Unified Data Repository) 등의 코어 요소들이 구현된 상태이며, 5G RAN은 UERANSIM[16]과 연결해 구성할 것을 권장하고 있다.

Free5GC[17]는 Go 언어 기반의 5G 코어 오픈소스 프로젝트로 3GPP release 15를 기반으로 5G 코어 개발 환경을 제공한다. Free5GC는 3단계로 구성되어 있으며, 1단계는 AMF, SMF, UPF를, 2단계에서 SBI (Service Based Interface) 기반으로 추가적인 5G 코어 요소를 구현한다. 3단계는 Non-3GPP 액세스를 지원하는 코어 요소인 N3IWF (Non-3GPP Inter-Working Function)와 ULCL (Uplink Classifier)를 추가로 구현하며, 3단계까지 모두 개발이 완료된 상태이다. 그러나 Free5GC와 연계되는 RAN 솔루션은 아직까지 명확하지 않은 상태이다.

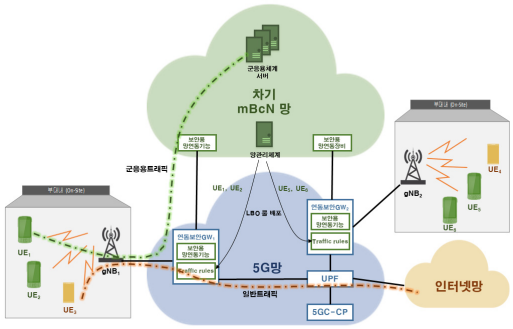
UERANSIM[16]은 SA 5G RAN을 지원하는 유일한 공개 소프트웨어 기반 프로젝트로 5G RAN의 제어 평면과 사용자 평면을 모두 지원한다. UERANSIM은 Open5GS 등의 5G 코어 오픈소스 프로젝트와 결합되어 사용될 수 있다.

본 논문에서는 5G망과 mBcN망의 연동 가능성을 평가하기 위하여 free5GC와 UERANSIM을 기반으로 테스트베드를 구축하였다.

3. mBcN 및 5G 연동 방안

3.1 mBcN과 5G망 연동 망구조

본 논문에서 제안하는 mBcN과 5G망의 연동망 구조는 그림 2와 같다. 구조를 살펴보면 제안하는 연동보안게이트웨이는 gNB와 UPF 사이에 위치한다. 연동보안게이트웨이 내에 보안용망연동기능은 망 분리/연계 기능, 네트워크 보안 기능, 암호화 기능, 기기/사용자/서비스 인증 기능, SFC 기능, LBO 기능 등을 제공한다. 그리고 LBO에 따른 전송 경로 선택 룰은 Traffic rules에 의해 결정되며 해당 정보는 mBcN의 망관리체계가 배포한 정보에 따라 결정한다. 즉, 군사용자단말은 5G 상용망의 기지국 자

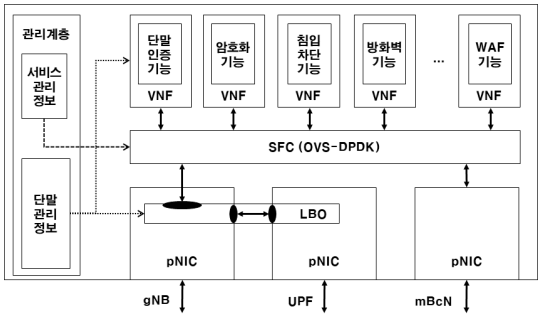


(그림 2) 제안하는 mBcN 및 5G 상용망 연동 망구조
(Figure 2) Proposed network architecture for mBcN cooperated with 5G commercial network

원만을 활용할 뿐 가입자 인증, 트래픽 전송 등과 같은 기능은 모두 mBcN의 망관리체계를 통해 이루어진다. 따라서 군사용자단말에 대한 사용자 정보도 통신사업자가 보관하는 것을 회피할 수 있다. 두 번째로 보안용망연동기능을 통해 군응용트래픽은 mBcN으로 전달되므로 보안을 유지할 수 있을 뿐만 아니라 5G코어망의 망부하 발생도 억제할 수 있다. 또한 일반 사용자 단말은 traffic rule에 의해 UPF로 전송되고 인터넷망을 통한 서비스 제공을 받을 수 있다. 예를 들어 그림 2를 살펴보면 mBcN에 위치한 망관리체계는 연동보안게이트웨이$_1$에게 UE$_1$과 UE$_2$는 군사용자단말이라는 정보를 배포한다. UE$_1$이 군응용트래픽을 발생시키면 연동보안게이트웨이$_1$은 해당 패킷을 수신한 후 보안용망연동기능에 탑재된 보안기능을 통해 해당 패킷의 침해여부를 판단한 후 보유한 traffic rule를 참조하여 mBcN으로 패킷을 전송한다. 만약 UE$_3$으로부터 연동보안게이트웨이$_1$이 패킷을 수신하면 traffic rule에 단말 정보가 없음을 인지한 후, UPF로 전달한다.

3.2 연동보안게이트웨이 제공 기능

제안하는 연동보안게이트웨이의 주요기능은 gNB로부터 수신된 패킷에 대한 LBO와 다양한 보안 모듈의 군응용체계 특성에 맞게 선택하여 전달하는 SFC 기능이다. 그림 3은 본 논문에서 제안하는 연동보안게이트웨이의 기능블록 구성도를 나타내고 있다. 먼저 gNB로부터 수신된 패킷은 물리적인 NIC(Network Interface Card)에 탑재된 LBO에서 단말정보를 확인한 후, mBcN으로 전달되어

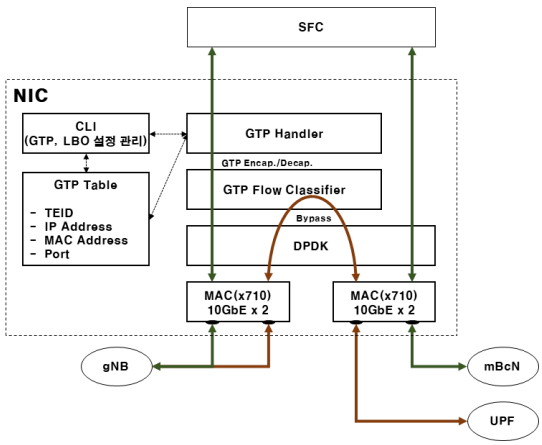


(그림 3) 제안하는 연동보안게이트웨이의 기능블록도
(Figure 3) Function block diagram of the proposed security cooperative gateway

야하는 패킷은 GTP(GPRS Tunnelling Protocol) header를 decapsulation한 후 상위계층으로 전달하고, 그렇지 않은 경우에는 UPF와 연결될 NIC로 바이패스 시킨다. 이때, mBcN으로 전달이 필요한 패킷은 단말관리정보에 명시된 단말정보를 기반으로 인지하며, 단말정보는 mBcN의 망관리체계로부터 수신 받는다. 또한 단말정보는 단말인증기능에서 단말 인증에 활용될 수 있다. mBcN으로 전달되는 패킷은 OVS-DPDK(Open Virtual Switch-Data Plane Development Kit)로 구성한 SFC로 전달된다[18]. SFC에서는 서비스관리정보로부터 수신된 군응용체계별 요구사항을 식별하여 필요한 보안모듈이 있는 VNF(Virtual Network Function)로 전달한다. 필요한 보안모듈을 모두 통과한 패킷은 mBcN과 연결된 NIC로 전달함으로써 mBcN과 연동한다. 본 논문에서는 연동보안게이트웨이의 필요 기능 중 LBO, SFC와 보안모듈 중 일부(FW; Firewall, IPS; Intrusion Prevention System, WAF; Web Application Firewall)에 대해서 세부적으로 기술한다.

3.2.1 LBO 기능

LBO 기능은 gNB로부터 수신한 GTP 트래픽이 mBcN으로 전달되는 트래픽인지, UPF로 전달되는 트래픽인지 분류하고 mBcN으로 전달되는 트래픽인 경우 GTP decapsulation된 패킷을 연동보안게이트웨이의 SFC로 전달하는 역할을 수행한다. 본 논문에서는 LBO를 고속으로 처리하기 위하여 연동보안게이트웨이의 NIC 에 내장된 MCP (Micro Processor)로 구현하였다. 그림 4는 제안하는 LBO의 기능 블록을 나타내고 있다. GTP Flow Classifier에서는 해당 서비스 플로우가 GTP Table에 명시되어 있는지를 판단한다. 서비스 플로우가 GTP Table에 명시된 플로우인 경우 GTP Handler로 전달하고, GTP decapsulation을 수행한다. 만약, 명시되어 있지 않은 서비스 플로우인 경우 UPF로 연결되는 물리적 포트로 바로 전달한다. mBcN망에서 전달된 서비스 플로우의 경우, 반대로 GTP Handler에서 GTP encapsulation을 수행하고 gNB와 연결된 물리적 포트로 전달한다.

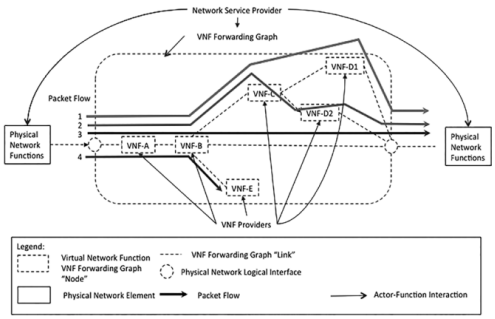


(그림 4) 제안하는 연동보안게이트웨이의 LBO 기능 블록도
(Figure 4) The block diagram for LBO functionality for the proposed security cooperative gateway

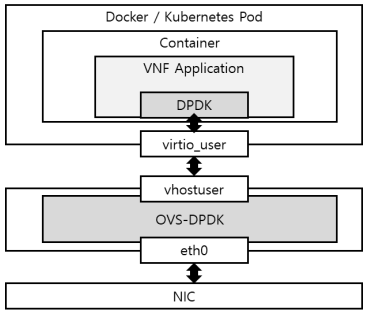
3.2.2 SFC 기능

SFC는 IETF SFC WG(Working Group)에서 논의된 기술로 트래픽에 따라 필요한 네트워크 기능들을 선택적으로 조합 및 실행하여 하나의 네트워크 서비스를 구현하는 기술이다[19]. 그림 5는 6개로 구성된 VNF에 대하여 SFC를 통해 4개의 서비스 플로우를 각기 다른 경로로 전달하는 예시를 나타내고 있다. 예를 들어 1번 서비스 플로우의 경우 VNF-A, VNF-B, VNF-C, 그리고 VNF-D1 기능을 수행하고, 3번 서비스 플로우의 경우 VNF-A와 VNF-B만을 수행함으로써 서비스 플로우의 요구사항에 따라 기능을 선택적으로 수행할 수 있도록 한다. 본 논문에서는 오픈소스 SDN인 Openvswitch 기반으로 openflow를 통한 서비스별 트래픽 분류 및 경로 설정을 수행하였다. Openvswitch는 ovs-ofctl API를 이용하여 L2(MAC), L3(IP), L4(Port) 등 다양한 조건으로 플로우를 핸들링할 수 있다. 또한 openvswitch-dpdk를 통해 호스트에서 생성한 인터페이스를 컨테이너에서 dpdk binding 인터페이스

로 인식할 수 있도록 vhostuser 가상인터페이스를 생성하였으며, vhostuser는 호스트와 컨테이너 간에 트래픽을 unix domain socket 방식으로 전달한다.



(그림 5) SFC 기능을 통한 VNF 전달 그래프
(Figure 5) VNF transfer graph by the SFC function

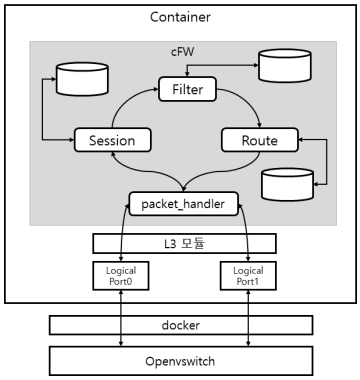


(그림 6) ovs-dpdk 및 컨테이너 인터페이스 연동 구조도
(Figure 6) ovs-dpdk and container interface interworking structure diagram

3.2.3 컨테이너 기반 보안 모듈

본 논문에서는 연동보안게이트웨이에 포함된 보안 모듈은 컨테이너 형태로 구성하고, 쿠버네티스 등의 오케스트레이션을 통해 부하에 따른 Scale-in/out 기능을 제공할 수 있도록 구현하였다. 연동보안게이트웨이에 설치된 openvswitch-dpdk를 통해 가상인터페이스(vhostuser)를 생성하고 컨테이너 내에서 구동되는 보안 모듈에서 이를 no-pic 옵션을 통해 unix domain socket 방식으로 연동할 수 있다[20]. 그림 6은 NIC로 부터 수집된 패킷을 컨테이너 기반의 VNF에 전달하기 위해 필요한 모듈과 연동 구조를 나타낸 그림이다. 본 논문에서는 연동보안게이트웨이의 보안 모듈 중 FW, IPS, WAF 기능에 대한 구현을 진행하였으며, 단말 인증 기능 및 암호화 기능은 추가로 구현할 예정이다.

컨테이너 기반 방화벽(cFW): 방화벽은 내부망으로 들어오는 트래픽에 대한 최초 보안을 담당하는 보안 기능으로 허가되지 않은 외부트래픽의 내부망으로 인입을 차단하고 룰에 따른 트래픽 제어 기능을 제공한다. 본 논문에서는 그림 7과 같이 cFW을 적은 리소스에서도 구동이 가능하도록 DPDK 기반의 패킷 입출력 처리 모듈, 세션관리 모듈, 라우팅 관리 모듈, 필터 관리 모듈로 구성하였다.

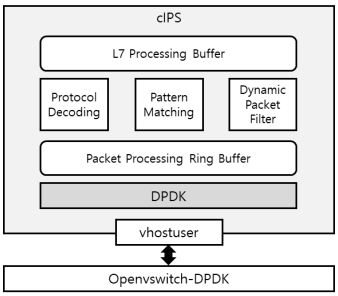


(그림 7) 컨테이너 기반 방화벽 기능 구성도
(Figure 7) Container-based firewall function diagram

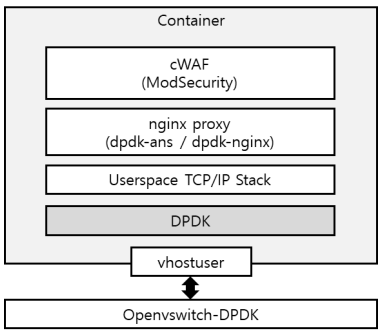
세션관리 모듈은 DPDK[21]의 cockoo hash 기반의 rte_hash API를 기반으로 구현하여 세션 검색 시 O(2) 타임 내에 검색이 가능하다. 또한 상태 기반 세션 관리를 제공하고 세션 생성 및 세션 삭제(Timeout, TCP Fin/Rst) 기능을 수행한다. 라우팅 모듈은 DPDK의 LPM(Longest Prefix Match) API를 기반으로 구현되어 라우팅 검색 시 O(2) 타임 내에 검색이 가능하다. 그러나 멀티 포트 기반의 라우팅 기능은 SFC 기능과 간섭이 발생하여 비활성화 시켰다. 필터 관리 모듈은 DPDK의 rte_acl API를 기반으로 구현되었다. rte_acl 은 5tuples(src ip/port, dst ip/port, protocol)을 기준으로 필터링 기능을 제공하고 ip 에 대해 prefix, 범위지정 조건 방식을 제공하고 port, protocol에 대해서도 범위지정 조건을 줄 수 있다.

컨테이너 기반 침입방지시스템(cIPS): 침입방지시스템은 DPI(Deep Packet Inspection) 기술을 통해 패킷의 페이로드에서 악성코드 및 취약점을 탐지하고 차단하는 보안 기능이다. 그림 8은 cIPS의 기능 구성도를 나타내고

있다. dpdk 바인딩 된 가상인터페이스(vhostuser)를 통해 패킷을 변조 없이 쌍으로 맵핑된 포트에 전달한다. cIPS는 vhostuser를 통해 인입된 트래픽에 대한 프로토콜 분석, Regex 및 Snort 룰 기반의 탐지/차단, 로직 기반 필터링 기능을 수행하고 L7 응용에 대한 분석 기능을 추가로 제공한다.



(그림 8) 컨테이너 기반 IPS 구성도
(Figure 8) Container-based IPS function diagram



(그림 9) 오픈소스 기반 웹방화벽 기능 구성도
(Figure 9) open source-based WAF function diagram

컨테이너 기반 웹방화벽(cWAF): 웹방화벽은 웹서버에 대한 웹 애플리케이션 취약점 공격을 방어하여 웹서버를 보호하는 기능으로 reverse proxy 기능을 통해 암호화된 HTTPS 트래픽에 대한 암·복호화를 수행할 수 있다. 암호화 방식이 RSA 방식이 아닐 경우 웹방화벽에서 웹서버의 인증키만으로 트래픽 복호화를 할 수 없다. 따라서 reverse proxy 방식으로 클라이언트와 웹방화벽간의 세션, 웹방화벽과 웹서버간의 세션으로 구분하여 각 세션에 대한 암·복호화가 수행되어야 한다. 이러한 기능은 nginx 에서 수행할 수 있지만 dpdk-nginx[22]는 kernel socket 방식으로 트래픽 입출력 처리를 하므로 유저공간에서의 TCP/IP 스택 기능 제공이 필요하다. dpdk 는 이러한 스택 기능을 제공하지 않으므로 dpdk-ans[23]를 통해 User Space TCP/IP 스택 기능과 연동하여 구현하였다. 그림 9는 WAF에 대한 기능 구성도를 나타내고 있다.

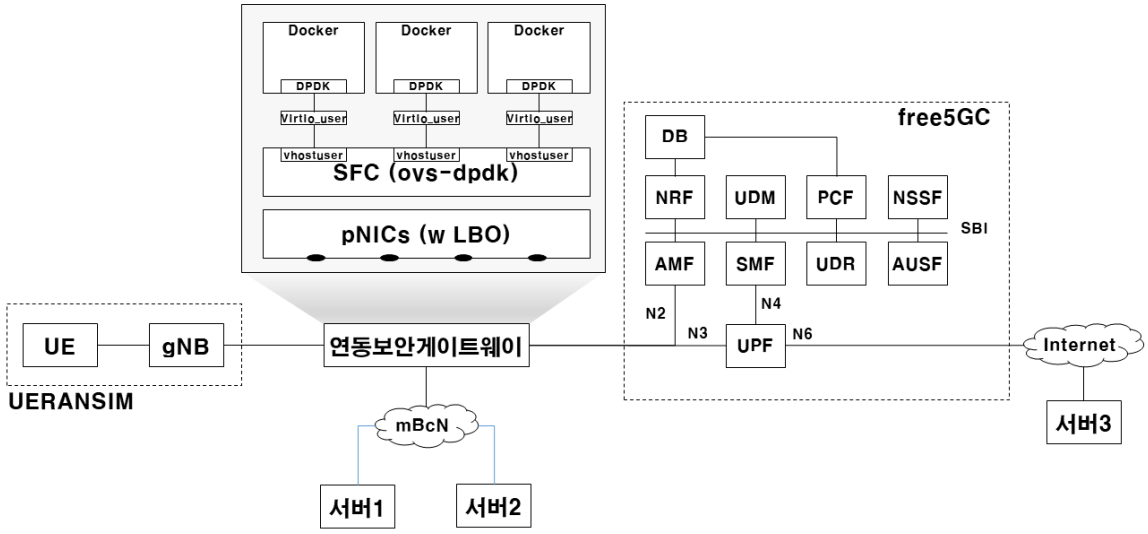
보안 기능을 수행하는 ModSecurity는 OWASP ModSecurity CRS(Core Rule Set)를 통해 OWASP Top 10 취약점 공격에 대한 보안을 제공한다. ModSecurity와 Nginx의 연동은 ModSecurity-nginx connector를 통해 수행된다.

4. 실험 환경 구성

본 논문에서는 제안하는 연동보안게이트웨이의 기능 검증을 위하여 UERANSIM과 free5GC를 기반으로 5G 망 환경을 구축하였다. 그림 10은 시험망 환경을 도시한 그림이다. UE는 3개의 서비스 플로우를 발생시키며, 각각 서버1, 서버2, 서버3으로 전달된다. 첫 번째로 서버 3으로 전달되는 서비스 플로우를 확인함으로써 5G 망과 정상적으로 연결이 가능함을 확인할 수 있다. 두 번째로 서버1/2로 전달되는 서비스 플로우와 서버3으로 전달되는 서비스 플로우를 확인함으로써 LBO의 기능을 확인할 수 있다. 마지막으로 서버1과 서버2로 전달되는 서비스 플로우를 확인함으로써 SFC의 기능을 확인할 수 있다.

(표 1) SFC를 위한 openflow 설정
(Table 1) Setting up openflow for SFC

```
// for all traffic
① in_port=1,action=output:3
② in_port=4,arp,action=output:5
③ in_port=2,arp,action=output:6
④ in_port=3,action=output:1
// for web traffic: UE → Internal Network
⑤ priority=65535,in_port=4,tcp,tp_dst=80,action=output:7
⑥ in_port=8,action=output:2
// for web traffic: UE ← Internal Network
⑦ priority=65535,in_port=2,tcp,nw_src=80,action=output:8
⑧ in_port=7,action=output:4
// for non-web traffic: UE → Internal Network
⑨ in_port=4,action=output:5
⑩ in_port=6,action=output:2
// for non-web traffic: UE ← Internal Network
⑪ in_port=2,action=output:6
⑫ in_port=5,action=output:4
```

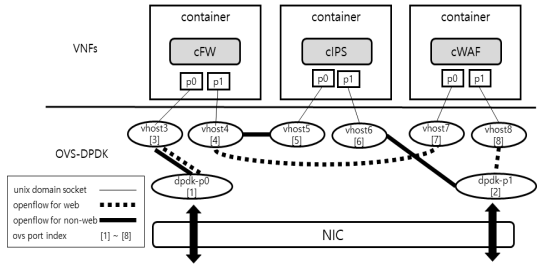


(그림 10) 제안하는 연동보안게이트웨이의 기능 검증을 위해 5G망과 mBcN을 연동한 시험망 환경
(Figure 10) The test network environment to validate the functionality of the proposed cooperative security gateway in the mBcN cooperated with 5G network

5G 접속망 환경은 UERANSIM를 이용하여 UE와 gNB를 구축하였으며, 5G 코어망 환경은 free5GC stage 2를 이용하였다. 5G 코어망은 AMF, SMF, UPF외에 NRF, NSSF(Network Slice Selection Function), UDM(Unified Data Management), UDR, AUSF(Authenticate Server Function), PCF (Policy Control Function)이 있으며 SBI (Service Based Interface)로 연결되어 있다.

gNB로부터 전달된 트래픽은 GTP Flow Classifier에서 전달 경로를 확인한 후 LBO 스티어링을 수행한다. mBcN망으로 전달되는 트래픽은 GTP Decapsulation 후 SFC로 전달하고, UPF로 전달되는 트래픽은 UPF로 전달되는 물리적 인터페이스로 바이패스 한다. UPF 및 mBcN에서 전송된 트래픽은 GTP Flow Classifier를 통해 gNB로 전송된다. 이때, mBcN에서 전달된 패킷은 GTP Encapsulation 후 gNB로 전송한다.

LBO에 의해 GTP decapsulation 된 모든 패킷은 방화벽의 포트(p0)로 전달된다(①). 방화벽의 포트(p1)에서 출력된 패킷 중 목적지 포트가 80인 경우 웹방화벽을 거쳐 내부망으로 전달된다(⑤~⑥). 웹서버에서 생성된 응답 패킷은 웹방화벽을 거쳐 방화벽으로 전달된다(⑦~⑧). 방화벽의 포트(p1)에서 출력된 패킷 중 목적지 포트가 80이 아닌 경우 IPS를 거쳐 내부망으로 전달된다(⑨~⑩). 서버에서 생성된 응답 패킷은 IPS를 거쳐 방화벽으로 전달된다(⑪~⑫). 방화벽의 포트(p0) 에서 출력되는 모든 패킷은 LBO로 전달된다(④). ARP 패킷에 대한 처리는 IPS를 거쳐 내부망으로 송수신된다(③~④).



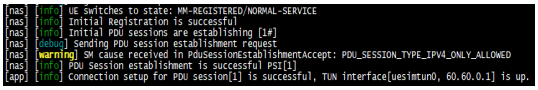
(그림 11) 서비스 체이닝을 통한 서비스 흐름도
(Figure 11) Traffic flow diagram through service chaining

5. 실험 결과

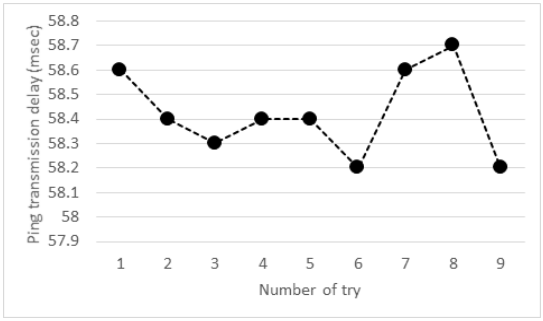
5.1 5G 사용자 인증 및 외부망 접속

UE에서 5G Core망을 통해 인증 및 IP를 할당받고 외부망으로 PING 접속을 수행하고 GTP 패킷인지 확인한다. 그림 12는 UE 단말에서 free5GC 코어망과의 인증과정을 통해 IP를 할당받은 로그의 일부를 보여주고 있다. 이 실험에서 해당 UE는 60.60.0.1 을 할당 받았다. 그림

13에서 할당 받은 IP를 통해 외부망의 8.8.8.8 로 ping 을 수행하였고 GTP encapsulation 된 ICMP가 정상 동작됨을 확인했다.



(그림 12) 사용자 인증 및 IP 할당 로그
(Figure 12) User authentication and IP assignment log



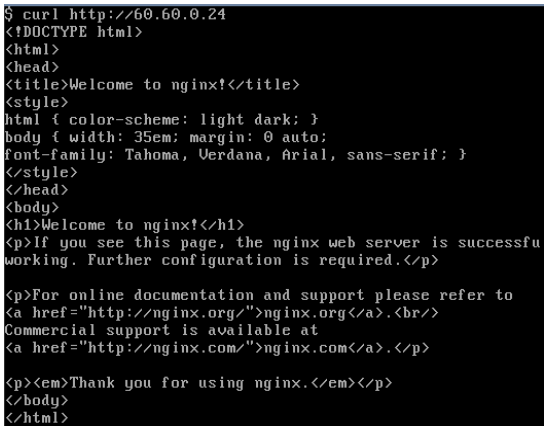
(그림 13) UE와 서버 3간의 ICMP 메시지 전송 지연
(Figure 13) Transmission delay of ICMP messages between UE and the server 3

5.2 서비스 체이닝

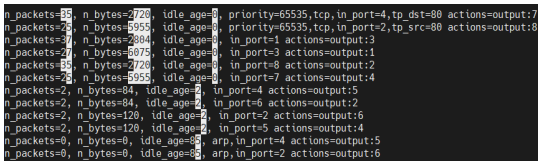
웹 트래픽과 그 외 트래픽에 대한 서비스 체이닝에 대한 수행 결과는 openvswitch의 dump-flows 로그를 통해 확인할 수 있다. 웹 트래픽의 경우 방화벽과 웹방화벽을 거쳐 내부망으로 트래픽이 전달된다. 따라서 IPS로는 트래픽이 유입되지 않는다. 반면에 그 외 트래픽의 경우 방화벽과 IPS를 거쳐 내부망으로 트래픽이 전달된다. 따라서 웹방화벽으로는 트래픽이 유입되지 않는다.

5.2.1 웹 트래픽 서비스 체이닝

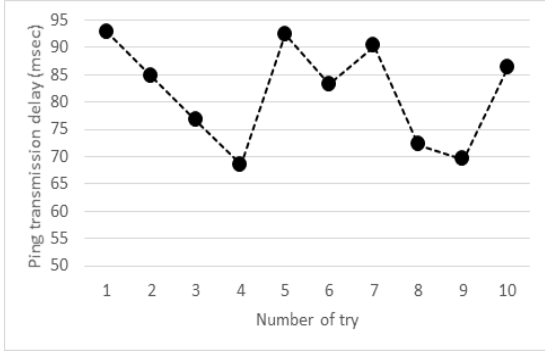
UE에서 curl 명령을 통해 내부망의 웹서버로 접속하여 웹트래픽이 방화벽 - 웹방화벽을 거쳐 내부망으로 서비스 체이닝 되는지 확인한다. 그림 14는 내부망 웹사이트에 접속하여 해당 사이트의 응답 결과를 정상적으로 받은 화면을 보여준다. openvswitch 의 ovs-ofctl API를 통해 모든 flow 에 흐르는 트래픽의 양을 조회할 수 있다. 그림 15에서 dump-flows 명령으로 조회하면 경로[1↔3, 4↔7, 8↔2] 로만 패킷 카운팅이 되는 것을 확인할 수 있다. 따라서 본 시험에서 의도한 대로 웹트래픽에 대해 방화벽 - 웹방화벽을 경유하는 서비스 체이닝이 정상적으로 수행되었음이 확인된다.



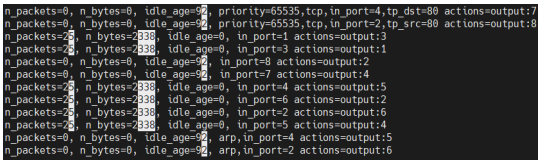
(그림 14) 내부망 웹사이트 접속
(Figure 14) Access to a website on the internal network



(그림 15) dump-flows for web traffic
(Figure 15) dump-flows for web traffic



(그림 16) UE와 서버 2간의 ICMP 메시지 전송 지연
(Figure 16) Transmission delay of ICMP messages between UE and the server 2



(그림 17) dump-flows for non-web traffic
(Figure 17) dump-flows for non-web traffic

5.2.2 웹트래픽 외 서비스 체이닝

UE에서 ping 명령을 통해 내부망의 서버로 접속하여 웹트래픽이 아닌 트래픽이 방화벽 - IPS를 거쳐 내부망으로 서비스 체이닝 되는지 확인한다. 그림 16는 내부망 서버에 ping 연결을 시도하여 응답 결과를 정상적으로 받은 화면을 보여준다. 그림 17에서 dump-flows 명령으로 조회하면 경로[1↔3, 4↔5, 6↔2] 로만 패킷 카운팅이 되는 것을 확인할 수 있다. 따라서 본 시험에서 의도한 대로 비 웹트래픽에 대해 방화벽 - IPS를 경유하는 서비스 체이닝이 정상적으로 수행되었음이 확인된다.

6. 결 론

차기 mBcN망에서 초고속·초연결을 지원할 수 있는 국방 모바일 업무 환경을 조성하기 위해서는 현재 서비스를 제공하고 있는 상용 5G망과의 연동을 고려하는 것이 필요하다. 그러나 5G망과 인터넷망의 연결과 동일한 형태로 mBcN망과 연동할 경우 5G 코어망 부하 증가, 종단간 전송 지연 증가, 군 단말·사용자 정보 노출, 군응용체계 트래픽의 상용망 경유로 인한 보안 침해 등 다양한 문제가 발생할 수 있다. 따라서 본 논문에서는 5G 상용망과 mBcN을 연동하는데 있어서 MEC 개념을 적용하여 상기한 문제를 해결할 수 있는 망구조를 제시하고, 망 연동을 위한 연동 보안 게이트웨이를 제안한다. 제안하는 망구조는 gNB와 UPF 사이에 연동 보안 게이트웨이를 배치하고, mBcN과 연결이 필요한 단말 정보는 mBcN망에 위치한 망관리체계로부터 획득하여 사용함으로써 상기한 다양한 문제를 회피할 수 있다. 또한, 연동보안게이트웨이는 전송 경로를 결정하는 LBO 모듈, SFC 모듈, 그리고 보안모듈 등을 가짐으로써 군응용체계별 상이한 요구사항을 만족시킬 수 있고, 무선망에서 발생할 수 있는 사이버 공격에 대응할 수 있다. 마지막으로 제안하는 연동보안게이트웨이가 5G 시험 환경에서 정상적으로 동작함을 확인하였으며 향후 연동보안게이트웨이에 필요한 관리 기능 및 추가 보안 모듈에 대한 개발을 진행할 예정이다.

참고문헌(Reference)

[1] N.S. Park, “KT gets the project for the next military broadband communication network,” Information and Communication Press, 16 Aug. 21.

[2] Business Transfer Lease (BTL) for the establishment of the next military broadband communication network; Facility business basic plan, Ministry of National Defense, Apr. 2021

[3] S. Kekki, et. al., “MEC in 5G networks,” ETSI White Paper No. 28, Jun. 2018

[4] H.K. Kim, G.S. Lee, and S.J. Lee, “An Analysis for the defense broadband convergence network based on ministry of national defense - architectural framework,” in Proc. the military operations research society of korea conference, pp. 128-142, 2005. http://koreascience.kr/article/CFKO200520828924924.page

[5] S.S. Lee, Y.S. Kim, and S.Y. Kang, “An Architecture and requirement of the military-BcN for NCW,” Information and Communications Magazine, 26(3), pp. 52-59, 2009. https://scienceon.kisti.re.kr/srch/selectPORSrchArticle.do?cn=JAKO200909651053093&dbt=NART

[6] J. Kang, J.W. Moon, and S.H. Lee, “Analysis of Improving Requirement on Military Security Regulations for Future Command Control System,” Journal of convergence security, 20(1), pp. 69-75, 2020. https://doi.org/10.33778/kcsa.2020.20.1.069

[7] H. Park, S. Kim, H. Lee, C. Im, and Y. Won, “Research on Network Design for Intrusion Tolerance of BcN,” Journal of KIISE: Information Networking, 34(5), pp. 305-315, 2007. https://www.koreascience.or.kr/article/JAKO200735822308838.page

[8] J.Y. Kim, A Study of BcN and the developing plan of DISN, Hanyang Univ., Master thesis, Aug. 2008.

[9] F. Spinelli and V. Mancuso, “Towards enabled industrial verticals in 5G: a survey on MEC-based approaches to provisioning and flexibility,” IEEE

Communications Serveys and Tutoroals, 23(1), pp. 596-630, 2020. https://doi.org/10.1109/COMST.2020.3037674
[10] S.K. Kim and J.D. Park, “Status of Mobile Edge Computing Technology Towards 5G Era,” Electronics and Telecommunications Trends, 31(1), pp. 25-35, Feb. 2016. https://www.koreascience.or.kr/article/JAKO201652057195931.page
[11] H. J. Son, “7 Deployment Scenarios of Private 5G Network,” Netmanias Tech-Blog, Oct. 18, 2019.
[12] D. Lee, M. Chung, W. Nam, K. Kim, W. Kim, J. Lee, S.J. Choi, H. Hong, and E. Vandris, “Case Study of Scaled-Up SKT 5G MEC Reference Architecture,” Intel white paper, Oct. 2019.
[13] J. Okwuibe, M. Liyanage, I. Ahmad, and M. Ylianttila, A Comprehensive Guide to 5G security, Wiley-VCH Verlag, 2018, pp. 373-397.
[14] OpenAirInterface, https://openairinterface.org
[15] Open5GS, https://open5gs.org/
[16] UERANSIM, https://github.com/aligungr/UERANSIM
[17] Free5GC, https://free5gc.org/
[18] OVS-DPDK, https://docs.openvswitch.org
[19] S.I. Lee and M.G. Sin, “Service chaining technology and standardization trend,” Information and Communications Magazine, 31(9), pp. 46-51, Sep. 2014.
[20] userspace cni plugin, https://github.com/intel/userspace-cni-network-plugin
[21] DPDK, https://www.dpdk.org/
[22] dpdk-nginx, https://github.com/ansyun/dpdk-nginx
[23] dpdk-ans, https://github.com/ansyun/dpdk-ans

◐ 저 자 소 개 ◑

남 구 민(Gu-Min Nam)
1994년 경남대학교 전산통계학과(학사)
1995년~2000년 한국중공업(현. 두산중공업) 대리
2003년~2011년 (주)넷코아테크 책임연구원/팀장
2011년~현재 (주)윈스 수석연구원
2021년~현재 성균관대학교 대학원 석사과정
관심분야 : 오픈스택, 가상화, 네트워크 보안 등
E-mail : gmnam@wins21.co.kr

김 형 식(Hyoungshick Kim)
1999년 성균관대학교 정보공학과(공학사)
2001년 KAIST 대학원 전산학과(공학석사)
2012년 University of Cambridge 대학원 컴퓨터과학과(공학박사)
2013년~현재 성균관대학 소프트웨어학과 교수
관심분야 : 보안공학, 모바일 보안, 소프트웨어 보안
E-mail : hyoung@skku.edu

◐ 저 자 소 개 ◑

이 현 진(Hyun-Jin Lee)
2004년 아주대학교 전자공학과(공학사)
2006년 아주대학교 전자공학과(공학석사)
2013년 아주대학교 전자공학과(공학박사)
2014년 단암시스템즈 선임연구원
2015년~2020년 솔빛시스템 책임연구원/ M&S 팀장
2021년~현재 ㈜윈스 수석연구원/ 기반기술 팀장
관심분야: 5G 및 5G 보안, AI 보안관제, 사이버 공격 모델링, 네트워크 모델링 등
E-mail : l33hyun@wins21.co.kr

조 학 수(Harksu Cho)
1997년 서울대학교 계산통계학과 전산과학전공(공학사)
1999년 서울대학교 자연과학대학원 전산과학과(공학석사)
2001년~현재 ㈜윈스 부사장/ CTO
2017년~2019년 4차산업혁명위원회 과학기술혁신분과 혁신위원
관심분야 : 네트워크 보안, 침입방지시스템, 침입차단시스템, 악성코드 자동분석, AI 보안관제
E-mail : marius71@wins21.co.kr