

# 전술망의 서비스 품질 보장을 위한 다계층 네트워크 가상화 기법

김요한<sup>1)</sup> · 안남원<sup>1)</sup> · 박주만<sup>2)</sup> · 박찬이<sup>2)</sup> · 임혁<sup>\*,1)</sup>

<sup>1)</sup> 광주과학기술원 전기전자컴퓨터공학부

<sup>2)</sup> 국방과학연구소 제2기술연구본부 1부

## Multi-layer Network Virtualization for QoS Provisioning in Tactical Networks

Yohan Kim<sup>1)</sup> · Namwon An<sup>1)</sup> · Juman Park<sup>2)</sup> · Chan Yi Park<sup>2)</sup> · Hyuk Lim<sup>\*,1)</sup>

<sup>1)</sup> School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology(GIST), Korea

<sup>2)</sup> The 2nd R&D Institute-1st Directorate, Agency for Defense Development(ADD), Korea

(Received 19 January 2018 / Revised 18 June 2018 / Accepted 20 July 2018)

### ABSTRACT

Tactical networks are evolving into an All-IP based network for network centric warfare(NCW). Owing to the flexibility of IP based network, various military data applications including real-time and multi-media services are being integrated in tactical networks. Because each application has diverse Quality-of-service(QoS) requirements, it is crucial to develop a QoS provisioning method for guaranteeing QoS requirements efficiently. Conventionally, differentiated services(DiffServ) have been used to provide a different level of QoS for traffic flows. However, DiffServ is not designed to guarantee a specific requirement of QoS such as delay, loss, and bandwidth. Therefore, it is not suitable for military applications with a tight bound of QoS requirements. In this paper, we propose a multi-layer network virtualization scheme that allocates traffic flows having different QoS requirements to multiple virtual networks, which are constructed to support different QoS policies such as virtual network functions(VNFs), routing, queueing/active queue management(AQM), and physical layer policy. The experiment results indicate that the proposed scheme achieves lower delays and losses through multiple virtual networks having differentiated QoS policies in comparison with conventional networks.

Key Words : Tactical Information Communication Network(전술정보통신체계), Network Centric Warfare(네트워크 중심전), Multi-Layer Network Virtualization(다계층 네트워크 가상화), Quality-of-Service(서비스 품질)

### 1. 서론

정보통신 기술의 발전에 따라 전장의 부대들을 네트

\* Corresponding author, E-mail: hlim@gist.ac.kr

워드로 연결하여 정보 우위를 점하고 전투력을 강화하려는 움직임이 전 세계적으로 나타나고 있다. 이러한 네트워크 중심전(Network Centric Warfare, NCW)은 빠르고 정확한 데이터 통신을 통해 전장에서의 지휘 속도를 증가시키고 빠른 작전을 구사하여 전투력을 높이는 정보 우위 전쟁을 말한다<sup>1)</sup>. NCW의 실현을 가능하도록 하려면 전장의 모든 부대와 지휘통제체계, 감시정찰체계, 정밀타격체계 등의 다양한 특성의 이기종 통신망을 하나의 네트워크로 연결하는 것이 필수적이다. 과거에는 통신망 간의 통신 프로토콜 및 인터페이스가 서로 달라 연동이 어려웠지만, NCW를 위한 All-IP 통합 네트워크의 연구 및 개발로 인하여 이기종 통신망 간의 연동이 가능해졌고 이에 따라 네트워크의 실시간 모니터링, 운영 통제 및 관리가 가능해졌다. 전화망과 데이터망의 통합에 따라 장비 활용의 효율성이 제고되었고, 전술망에서는 전술 상황을 위한 전문 정보 전달 및 실시간 VoIP 음성 서비스뿐만 아니라, 급여, 재고, 메일 등 다양한 일반 업무를 위한 상용망 기반의 응용 서비스까지 모두 사용할 수 있게 되었다. 하지만 전장의 수많은 단위들이 하나의 통합된 망으로 트래픽을 보내게 되면서 전술망의 부족한 대역폭 관리가 매우 중요한 사항이 되었고, 지연, 패킷 손실, 대역폭, 지터(jitter), 서비스 가용성, 기밀성 등의 quality-of-service(QoS)에 대한 서로 다른 요구사항을 갖는 응용 서비스 트래픽을 위한 효과적인 서비스 품질 제공 기법이 요구되어졌다.

상용망에서 응용 서비스의 QoS를 제공하기 위한 대표적인 방법으로는 IETF에서 제안한 integrated service (IntServ)와 differentiated service(DiffServ)가 있다<sup>2,3)</sup>. IntServ는 트래픽의 자원 예약을 위해 경로상의 모든 라우터(router)에서 플로우(flow)의 상태 정보를 유지해야 하므로 트래픽이 집중되는 코어망에서 상당한 부담이 되며 확장성이 낮다는 단점이 있다. 이에 대한 솔루션으로 제안된 DiffServ는 패킷의 IP 헤더에 서비스 클래스를 나타내는 differentiated service code point (DSCP)를 표시하여 패킷별로 차등화 된 서비스 품질을 제공하는 방식으로, 코어 라우터가 단순히 DSCP 값에 따른 per hop behavior(PHB)만 수행하면 된다. 따라서 패킷 처리가 매우 단순하고 구성의 복잡도가 낮아 대부분의 기존 대규모 전술망에서 사용된다. 하지만 DiffServ는 원래 상용망을 대상으로 제안된 기법으로써 서비스 클래스에 따른 지연, 패킷 손실, 대역폭 등의 요구 성능(performance) 보장에만 초점이 맞춰져

있다. 시시각각 변하는 전술 상황에서 발생하는 전술망 내 트래픽은 단순한 성능 보장 외에도 긴급성, 중요도 등 다양한 요구사항을 가지며, 이에 대한 서비스 품질을 보장하기 위해서는 전술 상황에 따른 동적인 QoS 요구사항을 고려해야 한다.

한편 미래 통신 네트워크의 QoS 보장과 서비스 차별화를 위한 핵심 기법으로 소프트웨어 정의망(Software-Defined Network, SDN)과 네트워크 가상화를 이용한 네트워크 슬라이싱(network slicing) 기법에 대한 연구가 활발히 진행되고 있다<sup>4)</sup>. 네트워크 슬라이싱은 다른 특성을 갖는 다양한 응용 서비스의 요구사항을 만족시키기 위하여 하나의 물리적 네트워크를 논리적으로 분리된 다중 슬라이스로 구성하고, 각 슬라이스에서 트래픽별로 차별화된 자원 관리 및 QoS 정책을 제공하는 기법이다. QoS 관점에서 DiffServ와 같은 광범위한 트래픽 차등화 서비스와 비교하면, 네트워크 슬라이싱은 특정 네트워크, 사용자, 서비스에 대하여 세밀한 종단 간 가상 네트워크 생성 및 자원의 제공이 가능하다는 점에서 차별화된다. 예를 들어, DiffServ는 비슷한 QoS 요구사항을 갖는 음성 트래픽들을 더욱 세분화하여 구분하는 기능을 제공하지 않기 때문에 이를 동일한 음성 클래스에 할당하고, 클래스에 따라 서비스 품질을 제공한다. 반면에 네트워크 슬라이싱을 QoS 보장에 적용하면 같은 음성 트래픽이더라도 특정 네트워크, 사용자에 따라 세분화하여 구분할 수 있기 때문에 같은 클래스 내에서도 세밀한 서비스 품질 차별화가 가능하다.

전술망에서 네트워크 슬라이싱의 적용은 단순히 서비스 형태에 따른 성능을 보장할 뿐만 아니라 다양한 종류의 서비스 차별화 정책을 슬라이스들에 적용함으로써, 전술망의 수많은 단위들이 갖는 QoS 요구사항에 특화된 슬라이스를 세분화되고 격리된 형태로 제공할 수 있다. 트래픽을 서비스 클래스에 따라 특정 슬라이스로 보내어 처리할 수 있고, 갑자기 트래픽의 요구 성능이 변하는 경우에도 트래픽의 서비스 클래스와 관계없이 트래픽이 할당된 슬라이스만 변경하여 전송할 수 있다. 정보 보호 및 보안이 매우 중요한 트래픽은 intrusion detection system(IDS)이 적용된 독립 슬라이스를 통해 악성 코드 및 해킹 감지를 강화할 수 있고, 기밀 DB에 접근할 수 있도록 경로를 달리 지정할 수도 있다. 대역폭이 매우 부족한 위성 전술망의 경우, 부족한 대역폭을 보완할 수 있는 정책이 적용된 슬라이스를 별도로 사용하여 처리할 수도 있다.

본 논문에서는 전술망에서 다양한 트래픽의 QoS를 효과적으로 만족시키기 위한 네트워크 슬라이싱 구조와 서비스 품질 제공 기법을 제안한다. 제안한 구조의 평가를 위하여, 기존 국내외 전술망의 DiffServ 기반 QoS 제공 방식에 대해 분석하고 네트워크 슬라이싱 기반 구조와의 차이점을 서술한다. 또한, 제안하는 전술망의 네트워크 슬라이싱 기반 서비스 품질 제공 기법에 대한 성능 평가를 수행한다.

## 2. 관련 연구

### 2.1 전술망에서의 QoS 요구사항

전술망의 응용 서비스는 VoIP 음성 서비스, 화상 서비스, 파일전송 서비스 등으로 구성되며, 이러한 응용 서비스들은 트래픽의 형태에 따라 정보유통 품질에 영향을 주는 지연, 패킷 손실, 대역폭, 지터에 대한 요구사항이 다르므로 최적의 요구사항을 결정하여 서비스 품질을 보장해야 한다. 정밀타격체계 장비의 경우 전송 지연에 민감하며, 감시정찰 장비의 경우 대용량 영상 데이터를 위한 대역폭 할당에 민감할 수 있다. 다양한 응용 서비스의 트래픽 특성을 고려하지 않고 함께 네트워크상에 유통할 경우, 불규칙한 지연이 발생하거나 부족한 대역폭으로 인해 패킷 손실이 발생할 수 있다. 전술망에서의 불규칙한 지연이나 패킷 손실은 경우에 따라 아군의 생존에 큰 영향을 미칠 수도 있다. 또한, 전술망에서는 작전 상황에 동적으로 변함에 따라 트래픽의 우선순위를 동적으로 변경할 수 있어야 한다. 일반적으로 낮은 우선순위로 처리되는 파일전송 서비스라도 임무 상황에 따라 정찰 영상을 전송하는 경우에는 데이터 전송의 긴급성이 요구될 수 있고, 따라서 높은 우선순위로 처리될 필요가 있다.

전술망의 응용 서비스별 QoS 요구사항은 Fig. 1과 같이 전송 성능(performance)과 작전 상황에 따라 임무의 긴급성(urgency), 정보의 중요도(importance)를 포함한 3-축 모델로 나타낼 수 있다<sup>[5]</sup>. 성능은 지연, 패킷 손실, 대역폭 등의 기본적인 QoS 요구 사항을 의미하며, 긴급성은 작전 상황에 따른 정보 전달의 신속한 정도를, 그리고 중요도는 정보의 중요한 정도를 뜻한다. 전술통신 환경에서는 각 응용 서비스별 요구 성능을 위주로 한 QoS 보장뿐만 아니라, 군 우선순위(military precedence)에 해당하는 임무의 긴급성, 정보의 중요도를 필수적으로 고려하여 작전 상황에 따라 발생

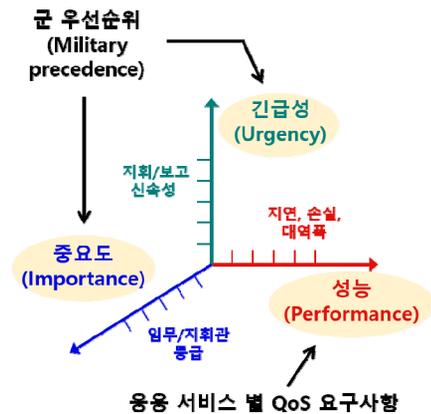


Fig. 1. QoS triple metric model for tactical networks<sup>[5]</sup>

하는 트래픽에도 적절한 QoS를 제공해야 한다. 따라서, 전술망에서는 이러한 QoS 요구사항을 종합적으로 고려한 QoS 제공 구조를 설계해야 한다.

### 2.2 전술망의 QoS 제공 방식

한국군에서는 기존에 회선 교환 방식과 제한된 IP 통신 방식으로 운영되는 SPIDER 디지털 통신체계를 사용해 왔으며, 최근 대용량의 음성·영상·데이터를 통한 전술 정보를 실시간으로 고속 전송할 수 있는 All-IP 기반 격자형 전술망인 TICN(Tactical Information Communication Network)의 전력화를 추진 중이다<sup>[6]</sup>. TICN에서는 DiffServ방식을 적용하여 전술통신체계 및 응용체계를 위한 통합된 차등화 된 서비스를 제공한다<sup>[7]</sup>. Table 1은 전술망 내 서비스별 QoS 제공을 위하여 각 서비스에 대한 DSCP 코드 별 QoS 클래스 큐 매핑(안)을 나타낸다<sup>[8]</sup>. 전술망은 QoS 지원을 위한 장비와 각 장비에 대한 큐가 다르게 구성된다. 특정 장비는 두 개의 PQ(Priority Queue)와 WFQ(Weighted Fair Queue), 그리고 BE(Best Effort)로 구성된다. 표준 DSCP 코드의 PHB는 라우터 내에서 클래스 별 패킷 전달 방식을 나타내며 BE(Best Effort), CS(Class Selector), AF(Assured Forwarding), EF(Expedited Forwarding)로 구분된다. 가장 높은 우선순위를 나타내는 EF는 최고의 서비스를 보장받는다.

### 2.3 미군 WIN-T의 QoS 제공 방식

미군의 경우 Table 2와 같이 미군 정보유통체계의 기반 구조인 GIG(Global Information Grid)에서 서비스 클래스 매핑을 정의하고 있다<sup>[9]</sup>. GIG는 군 특성에 적

Table 1. Example of DSCP mappings in tactical networks<sup>[8]</sup>

서비스	표준 DSCP 코드	예비 DSCP 코드	백본망	간선망	Ad-hoc 망	이동 통신망
음성 데이터 (1,2등급)	46 (EF)	1~15	1 <sup>st</sup> PQ	1 <sup>st</sup> PQ	1 <sup>st</sup> PQ	PQ
일제 지령						
핫라인						
단문 메시지 (1,2등급)	40 (CS5)	16~31	2 <sup>nd</sup> PQ	2 <sup>nd</sup> PQ		FIFO
음성 데이터 (3~5등급)						
라우팅 제어 메시지						
SNMP 메시지	24 (CS3)	33~47	WFQ (13개)	3 <sup>rd</sup> PQ	2 <sup>nd</sup> PQ	FIFO
영상 데이터	34 AF(41)					
통화 제어 메시지 (1~4등급)	36 (AF42)					
단문 메시지 (3,4등급)						
통화 가능 수단 확인 (1~4등급)						
타체계 연동 단말 트래픽	38 (AF43)	49~63	BE	4 <sup>th</sup> PQ	3 <sup>rd</sup> PQ	FIFO
통화 제어 메시지 (5등급)						
단문 메시지 (5등급)						
통화 가능 수단 확인 (5등급)						
기타 미식별 트래픽	0 (BE)					

Table 2. GIG's service class mapping<sup>[9]</sup>

서비스 클래스	MLPP	DSCP	PHB
제어 / 네트워크 관리	해당 없음	56	망 간 제어
		48	망 제어
연속적인 대화형 음성	FO, F, I, P, R	42, 41, 44, 45, 46, 40	EF
연속적인 대화형 영상	FO, F, I, P, R	34, 33, 36, 37, 38, 32	AF4
멀티미디어 스트리밍 / 멀티캐스트	FO, F, I, P, R	26, 25, 28, 29, 30, 24	AF3
짧은 블록 / 트랜잭션형	FO, F, I, P, R	18, 17, 20, 21, 22, 16	AF2
긴 블록 / 대용량 배치 전송	FO, F, I, P, R	10, 9, 12, 13, 14, 8	AF1
최선 노력형	R	00	BE

합한 응용 서비스의 종류를 제어 클래스 및 최선 노력(best effort) 클래스를 포함한 7가지로 분류하고 DiffServ의 DSCP 및 PHB를 부여하였다. PHB는 클래스 기반의 패킷 전달 방식으로 EF(Expedited Forwarding), AF(Assured Forwarding), BF(Best Effort)로 구분되며, EF는 DSCP 중에서 우선순위가 가장 높은 클래스를 뜻한다. 라우터는 PHB에 따라 트래픽에 우선순위 큐잉, 패킷 드롭 등의 규칙을 적용하여 클래스별로 차등화된 서비스를 제공한다.

NCW의 실현을 위해 막대한 예산을 투입한 미 육군의 최신형 전술통신체계인 WIN-T(Warfighter Information Network-Tactical)는 지상, 공중, 그리고 우주의 3-계층 기반통신체계를 바탕으로 전장에서의 전술 정보를 효과적으로 전달하기 위한 All-IP 기반 전술 백본망을 말한다. WIN-T는 전술망에서의 QoS 제공을 위하여 응용 서비스에 대한 DiffServ 기반 차등화 서비스를 기본적으로 제공하며, 작전 임무 상 발생하는 트래픽의 서비스 품질 보장에 대한 솔루션으로 RT-ECN(Real-Time Explicit Congestion Notification), BB(Bandwidth Broker), RSVP(Resource Reservation Protocol), ARSVP(Aggregated RSVP) 등 다양한 연구를 진행해왔다<sup>[10]</sup>. 예를 들어, DiffServ 기반 차등화 서비스에 RSVP와 같은 시그널링(signaling) 기법이 결합된 하이브리드 방식을 이용할 수 있다. 시그널링 기법은 갑자기 긴급하거나 중요한 트래픽이 발생하면 각 라우터에 해당 트래픽의 우선

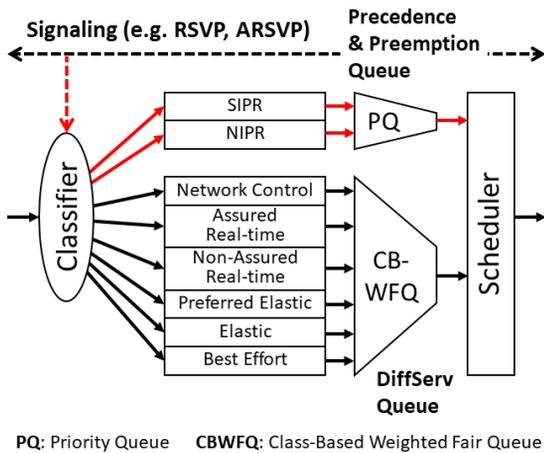


Fig. 2. Hybrid queue design of WIN-T

순위 및 선점(preemption)을 위한 RSVP 기반의 신호를 보내는 기법이다. 신호를 받은 라우터는 DiffServ를 기반으로 할당된 트래픽의 서비스 클래스와 상관없이 시그널링의 선점 처리 정책에 따라 해당 트래픽을 우선적으로 처리한다.

Fig. 2는 하이브리드 방식을 이용한 라우터 내 큐 설계의 예를 나타낸다. 라우터는 두 가지 큐로 구성되는데, 첫번째는 기본적으로 응용 서비스의 클래스에 따른 DiffServ 기반 서비스 차별화를 제공하기 위한 CBWFQ(Class-Based Weighted Fair Queue)이며, 두 번째는 라우터 내에서 시그널링을 기반으로 특정 플로우에 우선순위 및 선점 처리를 제공하기 위한 PQ이다. 작전 상황에 따라 긴급하거나 중요한 플로우에 대해서는 시그널링을 전송하여 PQ를 통해 낮은 우선순위의 패킷을 선점하고 QoS를 보장받게 할 수 있다.

#### 2.4 네트워크 슬라이싱

네트워크 슬라이싱은 차세대 네트워크망인 5G를 구성하기 위한 주요 기법으로써 하나의 물리 네트워크를 다수의 논리 네트워크로 구성하여 응용의 특성이나 QoS 요구사항에 따라 트래픽을 분리하여 맞춤형 서비스를 제공하기 위한 기법이다. 미래의 NCW에서는 전술망을 통해 음성, 화상, 대용량 파일, 기밀 데이터 등 다른 특성과 QoS 요구사항을 가진 트래픽들이 하나의 인프라에서 제공되어야 한다<sup>[11]</sup>. 이를 위해 트래픽을 특성에 따라 분류하고, 네트워크 기능(network function)과 구성을 맞춤화(customization)한 개별 논리 네트워크를 구성하여 서비스함으로써 관리의 복잡성을

완화할 수 있고 응용의 특성과 트래픽의 QoS 요구사항을 충족시키기 위한 최적화된 알고리즘 및 정책을 적용할 수 있다. 예를 들어, 시간 지연에 민감한 실시간 트래픽과 대용량 전송 트래픽을 위한 슬라이스를 따로 구성하여, 전자는 지연시간 보장을 위해 지연시간 인지(delay-aware) 라우팅을 수행할 수 있으며, 후자는 링크 대역폭 이용률(utilization) 및 균형을 고려한 라우팅을 수행하여 버퍼 오버플로우(buffer overflow) 및 패킷 드랍으로 인한 패킷 재전송을 최소화할 수 있다.

네트워크 슬라이싱을 위한 핵심기술은 NFV(Network Function Virtualization)와 SDN을 이용한 가상 네트워크 구성 기법이다. 물리 스위치를 가상화하여 가상화된 스위치/라우터나 미들박스를 생성하고, 이들을 연결한 SDN 기반 가상 네트워크를 구축할 수 있다. 중앙화 된 SDN 제어기를 통해 가상 네트워크를 구성하고 있는 장비를 중앙에서 유연하게 제어할 수 있다<sup>[12]</sup>. 따라서, 슬라이싱을 전술망에 적용할 경우 소프트웨어 기반의 네트워크 구성 및 트래픽 관리 기법을 통해 성능, 군 우선순위, 보안, 이동성 등 지휘 통제, 작전을 위한 다양한 군사적 서비스를 유연하고 효율적으로 제공할 수 있다. 본 논문에서 네트워크 슬라이싱 환경 구현을 위해 사용된 플로우바이저(FlowVisor) 플랫폼은 SDN의 제어 평면과 물리적인 네트워크 자원으로 구성된 데이터 플레인 사이에 위치하여 동작한다. 플로우바이저는 네트워크 슬라이스를 구성하고, 데이터 평면에서 발생한 패킷이 어떤 슬라이스에서 요청된 것인지를 판단하여 제어 평면을 통해 해당 슬라이스의 제어가 패킷을 관리하도록 처리한다. 네트워크 슬라이싱을 전술망에 적용하여 구현하기 위해서는 이로 인한 네트워크 오버헤드를 고려해야한다. 이전의 연구<sup>[13]</sup>에서는 제어 평면과 데이터 평면 사이에 플로우바이저를 구현하였을 때 발생하는 오버헤드를 측정하였는데, 실험 결과는 제어 평면과 데이터 평면에서의 오버헤드는 발생하지 않으며, 제어 평면과 데이터 평면 사이를 교차하는 작업에서 약간의 오버헤드가 발생함을 보여주었다. 플로우바이저를 통해 새로운 플로우를 처리하는데 걸리는 대기 시간은 약 16 ms로, 네트워크 슬라이싱을 하지 않았을 때(약 12 ms)보다 약간의 오버헤드가 발생한다. 하지만, 플로우 엔트리가 한 번 라우터에 입력될 경우에 이러한 교차 평면 오버헤드는 발생하지 않기 때문에 대용량 서비스나 지연에 민감하지 않은 서비스에는 심각한 수준

이 아니다. 반면, 긴급하고 중요한 트래픽이 존재하는 전술망에서 지연에 민감한 서비스에는 충분히 큰 지연이 될 수 있기 때문에 네트워크 슬라이싱을 적용할 경우 이에 대한 대책이 요구되어진다.

### 3. 전술망 QoS 보장을 위한 슬라이싱 기법

#### 3.1 문제 정의

기존 연구에서는 주로 전술망 QoS 보장을 위해 DiffServ를 기반으로 한 군 트래픽 클래스 분류 및 서비스 차등화 방법이 연구됐다. 하지만 앞서 언급한 바와 같이 전술망에서는 작전 상황에 따른 긴급성이나 중요도에 따라 군 트래픽의 우선순위가 동적으로 변하게 되며, DiffServ는 이러한 동적인 QoS 요구사항 변화에 대응하여 서비스 정책을 변경하는데 어려움이 있다. 이를 위해 전장 상황에 따라 변하는 트래픽의 긴급성 및 중요도에 대응하여 중요한 패킷을 우선적으로 서비스하여 지연과 패킷 손실률을 줄일 수 있는 기법이 요구된다.

앞서 2.3 절에 기술한 바와 같이 미군 WIN-T에서는 시그널링을 이용함으로써 동적인 군 우선순위에 따라 긴급하거나 중요한 트래픽이 네트워크 자원을 선점하고 일반 트래픽보다 우선적으로 처리될 수 있는 기능을 제공하고 있다. 따라서 갑자기 긴급하거나 중요한 트래픽이 발생한 경우, 트래픽에 고정적으로 할당된 DiffServ 기반 서비스 클래스와 상관없이 가장 먼저 처리될 수 있도록, 라우터에 RSVP 기반 신호를 보내어 해당 트래픽이 일반 트래픽을 선점하여 우선 처리되도록 한다. 시그널링 기법은 QoS 요구사항이 변하는 동적 전술 상황에서 발생하는 DiffServ의 문제점에 대하여 유용하게 사용될 수 있지만, 여전히 전술망 트래픽의 다양한 QoS 요구사항을 만족시키는 데 한계가 있다. 예를 들어, 요구 지연이 100 ms인 적군 정찰 영상과 10 ms인 일반 음성 트래픽이 있을 때, 시그널링을 이용하면 서비스의 중요도에 따라 정찰 영상이 음성 트래픽을 선점하여 우선 처리되도록 할 수 있지만, 지연이 중요한 음성 트래픽은 정보의 품질(패킷 손실)뿐만 아니라 지연이 매우 심해질 수 있다. DiffServ와 시그널링은 이를 위한 라우팅 경로나 스케줄링 등의 세분화된 QoS 정책을 지원하지 않는다.

다양한 종류의 트래픽이 하나의 네트워크로 집중되는 All-IP 기반의 미래 전술망을 위해서는 군 트래픽

의 우선순위 변화에 따라 긴급하거나 중요한 트래픽에 신속히 대응할 수 있을 뿐만 아니라, 동시에 트래픽의 QoS 요구 성능을 보장하기 위해 더욱 체계적이고 세분화된 서비스 정책을 적용하여 QoS를 제공할 수 있는 기법이 요구된다.

#### 3.2 제안한 네트워크 슬라이싱 기법

본 논문에서는 미래 전술망의 서비스 품질 보장을 위한 네트워크 슬라이싱 기법을 제안한다. 네트워크 슬라이싱 기법이 적용된 전술 WAN(Wide Area Network)은 Fig. 3에서와 같이 엣지(edge) 라우터를 양 끝단으로 하여, 물리 네트워크가 논리적으로 분리된 다중 계층의 가상 네트워크 슬라이스로 구성되며, 각 슬라이스는 다른 슬라이스와 차별화된 QoS 정책에 따라 트래픽을 서비스한다.

전술망의 트래픽은 각각 성능, 군 우선순위, 보안 이동성 등의 QoS 요구사항에 따라 가장 적합한 토폴로지, 라우팅, 큐잉, 보안 등의 정책을 갖는 슬라이스로 할당되어야 한다. 이를 위하여 중앙 제어 시스템(central control system)은 플로우별 QoS 요구사항을 관리하는 QoS database(DB), QoS 요구사항에 따라 플로우를 슬라이스로 분류하는 트래픽 분류기(traffic classifier), 그리고 슬라이스를 제어/관제하는 슬라이스 제어기(slice controller)의 세가지 기능을 가진다. 첫번째로, 트래픽 분류기는 트래픽의 QoS 요구사항을 파악하고, 트래픽이 최적의 슬라이스에서 서비스될 수 있도록 슬라이스 선택, 생성, 재설정 등의 총괄적인

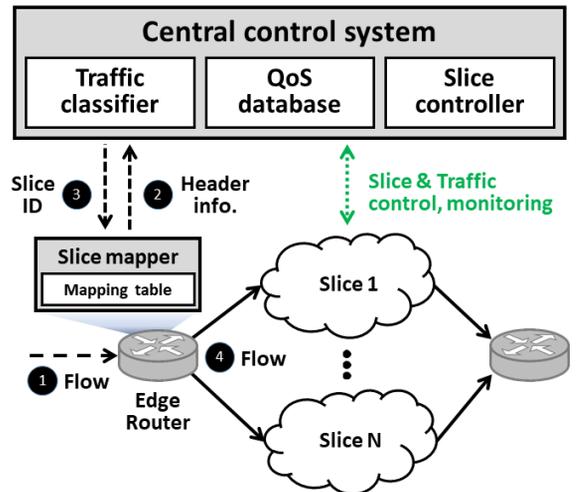


Fig. 3. Network slicing-based tactical WAN architecture

QoS-Set table		
Address		Urgency
Protocol		Importance
Port	DSCP	Performance
Flow Info.		Security
Military Priority		Mobility

Fig. 4. QoS-set record table in QoS database

슬라이스 관리 역할을 담당한다. 옛지 라우터에 새로운 플로우가 유입되면 옛지 라우터 내 슬라이스 맵퍼 (mapper)가 해당 플로우에 대한 정보를 트래픽 분류기로 전송하여 트래픽 분류기가 동작하도록 한다. 이러한 정보는 플로우의 기본 패킷 헤더 정보(IP/MAC addresses, port)와 패킷 헤더에 포함된 DSCP 값 등이 이용될 수 있다. 두번째로, 트래픽 분류기는 플로우의 QoS 요구사항에 따른 적합한 슬라이스를 결정하기 위하여 QoS DB에 저장된 플로우별 QoS 요구사항 정보를 활용한다. 전술망에서 플로우별 QoS 요구사항은 트래픽의 성능, 군 우선순위, 보안, 이동성 등이 해당되며, Fig. 4와 같이 QoS DB 내에서 QoS-Set 형태로 관리한다. QoS DB는 사용자/응용의 피드백이나 플로우의 패킷 헤더 정보, DSCP, payload, 유사한 플로우의 QoS 요구사항을 활용하여 주기적으로 업데이트된다. 마지막으로, 트래픽 분류기는 슬라이스 제어기로부터 획득한 현재 슬라이스 및 트래픽 정보에 따라 플로우가 할당될 슬라이스를 결정한다. 트래픽 분류기가 이미 생성된 슬라이스 중에서 적절한 슬라이스를 결정하지 못할 경우에는 새로운 슬라이스를 생성하거나 슬라이스를 재설정 할 수 있다. 슬라이스 제어기는 트래픽 분류기에서 결정된 슬라이스 정보와 정책에 따라 코어망 라우터를 제어 평면을 통해 설정한다. 슬라이스 맵퍼는 트래픽 분류기에서 결정된 슬라이스 ID에 따라 플로우를 해당 슬라이스로 할당한다.

Fig. 5는 QoS 요구사항에 따라 트래픽 분류기를 통해 분류된 서비스와 슬라이스별 정책 차별화의 예를 나타낸다. 각 슬라이스는 각기 다른 요구사항을 갖는 트래픽을 처리하며, 이러한 트래픽들은 슬라이스 내에서 정한 정책에 따라 차별화된 서비스를 통해 QoS를 보장받는다. 슬라이스의 생성, 삭제, 관리와 슬라이스 내 차별화 정책의 결정은 네트워크 슬라이싱 기반 전술망을 관리하는 부대에서 트래픽의 상황과 유져, 서비스의 요구를 모니터링하고 피드백에 따라 결정한다. 차별화 정책은 대표적으로 라우팅 정책, 큐잉 정책,

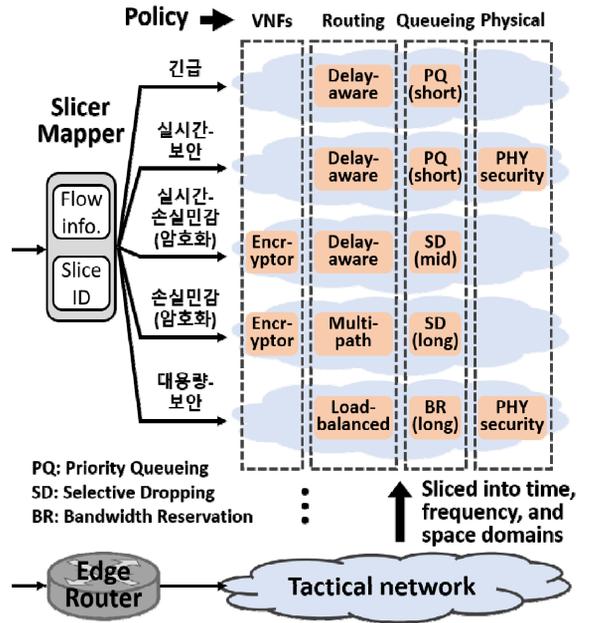


Fig. 5. Example of slice differentiation policies according to QoS requirements

물리계층 정책, virtual network function(VNF) 등이 있다. 각 정책은 긴급, 실시간-보안, 손실민감 등의 서비스, 트래픽 종류에 따라 생성된 슬라이스의 상황에 맞게 적용될 수 있다. 긴급한 트래픽에 해당하는 슬라이스 ID가 마킹된 트래픽이 옛지 라우터의 슬라이스 맵퍼로 들어오면 ID에 따라 트래픽 분류가 이루어지고 긴급 슬라이스에 해당하는 데이터 평면으로 전송된다. 이 때 해당 슬라이스는 지연 인지 라우팅 정책, 우선 순위 큐잉 정책을 사용하여 트래픽이 낮고 안정된 지연을 보장받을 수 있게 해준다. 아래는 사용될 수 있는 정책의 예시와 이에 대한 설명을 나타낸다.

- **라우팅 정책:** 트래픽 특성에 따라 라우팅 정책을 선택적으로 적용한다. 라우팅 정책에는 토폴로지 공유/격리 및 라우팅 기법이 있는데, 토폴로지 공유/격리는 링크의 부하를 고려하여 슬라이스별 가상 토폴로지를 설정할 수 있다. 라우팅 기법으로는, 실시간 트래픽은 지연에 유리한 통신 방식 및 지연 인지 라우팅을 사용하여 요구 지연을 충족시킬 수 있으며, 손실 민감 트래픽은 다중 경로 라우팅을 사용하여 패킷 손실을 줄일 수 있다. 대용량 트래픽은 라우터의 부하를 고려한 라우팅을 통해 병목현상을 최소화할 수 있다.

- **큐잉 정책:** 전장 상황에서는 응용 서비스가 요구하는 성능을 위주로 한 QoS 제공뿐만 아니라 임무의 긴급성, 정보의 중요도에 따른 QoS 제공이 필수적으로 고려되어야하기 때문에 긴급하거나 중요한 플로우를 처리하는 슬라이스에 높은 우선순위를 부여하거나 대역폭을 예약할 수 있다. 슬라이스 간 우선순위 외에도, 슬라이스 내에서 우선순위 큐잉을 이용하여 플로우의 긴급성에 따라 전송 우선순위를 스케줄링할 수 있다. 또한, 슬라이스 내 트래픽의 특성에 따라 큐 사이즈를 조절하여 최적화 할 수 있다.

- **VNF:** 트래픽이 요구하는 서비스/기능을 가상화 기반 VNF로 제공하여 QoS를 보장한다. 방화벽이나 암호화 등의 보안이 필요한 트래픽이 할당된 슬라이스의 경우 보안 서비스를 VNF로 생성 및 제공하여 트래픽이 보안 시스템을 거치도록 하거나 암호화 수준을 달리 설정할 수 있다.

- **물리계층 정책:** 무선 채널의 전송 방식, 전송 전력, 노이즈(noise), 다중 안테나(antenna), 릴레이(relay) 등의 자원을 이용하여 슬라이스에 알맞은 QoS 제공이 가능하며, 물리 계층 보안을 상위 계층 보안과 융합하여 효과적으로 보안 위협에 대처할 수도 있다. 무선에서 공유키 형태의 암호화를 사용할 시 중간자 공격(man-in-the-middle attack)과 같은 도청 형태 공격에 취약할 수 있으므로, 이에 대한 해결책으로 해당 슬라이스에 물리 계층 보안을 적용하여 보안을 강화할 수 있다.

- **이동성:** OTM(On The Move) 통신 기능이 요구되는 기동 통신소, 지휘관 차량 및 무인체계로 구성된 무선 네트워크의 경우, 고정 지휘소 및 고정 감시정찰 체계와는 다른 통신 능력을 가진다. 따라서 이동성에 대한 서로 다른 QoS 정책을 적용하고, 이동성을 예측하여 사전에 라우팅을 변경하는 등의 예측 기반 정책 또한 적용할 수 있다.

#### 4. 성능 평가

##### 4.1 테스트베드 구축

전송망의 서비스 품질 보장을 위한 다계층 네트워크 가상화 기법의 성능 평가를 위해 Fig. 6과 같이 테스트베드를 구축하였다. 본 테스트베드는 오픈소스 소프트웨어를 활용하여 4가지로 구성되며, 가상화된 네트워크 슬라이스(network slice)를 구현하기 위한 네트

워크 에뮬레이터(network emulator), 네트워크 제어기(network controller), 슬라이스 제어기(slice controller)의 3가지 요소로 구성된다. 각 요소에 대한 설명은 다음과 같다.

- **네트워크 에뮬레이터:** Mininet 에뮬레이터를 기반으로 격자 토폴로지의 전송망을 에뮬레이션하였다. OVS (Open vSwitch) 기반의 SDN 스위치로 구성된 코어망은 제어 평면을 통해 연결된 외부 PC의 네트워크 제어기에 의해 관리된다. 엣지 노드는 호스트로부터 유입되는 플로우가 처리될 슬라이스 ID(VLAN ID)를 플로우에 할당하기 위하여 VLAN tagging을 통해 플로우의 패킷에 슬라이스 ID 마킹(marking)을 수행한다. 엣지 노드에 새로운 플로우가 들어오면 신속한 처리를 위하여 우선 일반 트래픽 슬라이스(예, best-effort)로 마킹하며, 동시에 QoS DB 검색을 통해 해당 플로우의 슬라이스 ID를 찾아 재마킹한다.

- **네트워크 제어기:** 네트워크 제어기는 플로우에 부여된 슬라이스 ID에 따라 플로우를 특정 슬라이스에 할당한다. 본 테스트베드에서는 네트워크 슬라이싱을 위한 오픈소스 소프트웨어인 FlowVisor를 이용하여 트래픽의 슬라이스 ID에 따라 플로우와 슬라이스를 매핑하기 위한 플로우 스페이스(flow space)를 정의한다. 그리고 슬라이스에 속한 플로우의 제어 및 관리는 각 슬라이스 제어기가 수행할 수 있도록 연결하였다.

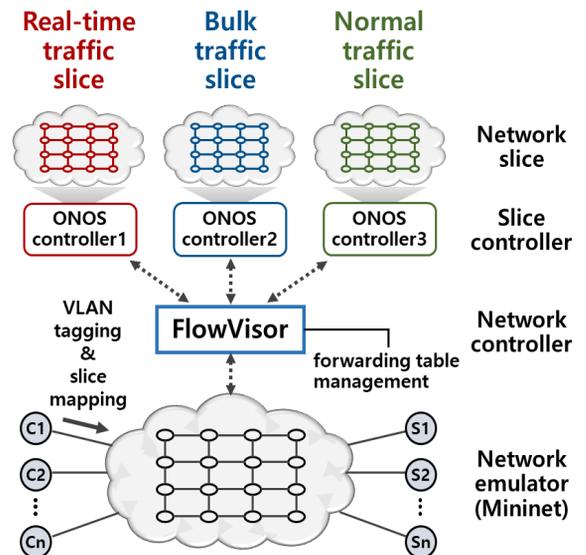


Fig. 6. Multi-layer network virtualization test-bed

• **슬라이스 제어기:** VMware 기반 서버 가상화를 통해 여러 대의 가상머신(VM)을 생성하고, 각 VM에 슬라이스 제어기를 실행하였다. 본 테스트베드에서는 오픈소스 기반의 ONOS SDN 제어기를 사용하였다. 슬라이스 제어기는 라우팅 및 QoS 정책을 어플리케이션 형태로 구현할 수 있기 때문에 이를 활용하여 슬라이스별로 트래픽에 맞춤형된 제어를 수행할 수 있다.

4.2 실험 수행 및 결과

제안하는 전술망에서의 다계층 네트워크 가상화 기법의 성능 평가를 위해, 구축한 Mininet 기반 테스트베드에서 TICN 백본망을 가정하여 100 Mb/s 링크를 갖는 4x4 격자형 토폴로지를 구성하였다. 본 실험에서는 트래픽을 임의의 경로를 갖는 실시간(real-time), 손실민감-대용량(bulk data), 일반(normal) 서비스 플로우로 구성하였고, 각각의 rate은 1 Mb/s, 10 Mb/s, 4 Mb/s로 설정하였다. 또한, 각 서비스 플로우 개수의 비율은 1:1:2로 구성하여 총 플로우 개수가 200개인 경우에 실시간 서비스 50개, 손실민감-대용량 서비스 50개, 그리고 일반 서비스 100개가 되도록 하였다. 시뮬레이션 시간은 총 100초이며, 따라서 손실민감-대용량 서비스의 경우 인가된 트래픽의 총 양은 50 Gbit이다.

본 실험에서는 지연에 민감한 실시간 서비스와 패킷 손실에 민감한 대용량 서비스에 대하여 제안하는 다계층 네트워크 가상화 기법을 적용할 때의 서비스 지연 및 패킷 손실을 측정하고 이를 적용하지 않은 경우와 비교하였다. 실험에서는 트래픽 유형을 가장

일반적인 특성을 나타내는 실시간, 대용량, 일반 트래픽으로 나누었고, 이는 네트워크 트래픽의 통계, 특성에 따라 세분화 정도를 설정할 수 있다. 다계층 네트워크 가상화 기법의 적용은 QoS 요구사항이 서로 다른 세 종류의 서비스 플로우를 3개의 슬라이스에 각각 할당하여 구현된다. 또한, 서로 다른 서비스 슬라이스에 차별화된 QoS를 제공하기 위하여 실시간 서비스의 경우에는 우선적으로 처리될 수 있도록 해당 슬라이스의 우선순위를 가장 높게 설정하고, 대용량 서비스의 경우에는 대역폭을 예약하여 충분한 품질 제공이 될 수 있도록 설정한다.

Fig. 7은 총 플로우 개수가 200개일 때, 대용량-손실민감 트래픽 슬라이스의 예약 대역폭에 따른 서비스별 패킷 손실 및 지연에 대한 평가를 나타낸다. 단일 네트워크에서 트래픽을 서비스하는 경우 대용량-손실민감 트래픽의 평균 패킷 손실률은 약 18%이며, 슬라이싱을 통해 예약 대역폭을 조절하여 패킷 손실률을 크게 감소시킬 수 있다. 본 결과에서 75 Mb/s 이상 대역폭을 예약할 때 대용량 트래픽의 패킷 손실률이 크게 감소하는 것을 확인할 수 있다. 75 Mb/s 이하 구간에서 대용량 트래픽의 지연이 높은 이유는 대역폭이 낮을수록 큐에 패킷이 쌓여 지연이 발생하기 때문이다. 이와 더불어, 실시간 서비스의 지연은 낮은 수준(< 1 ms)을 유지함을 확인할 수 있다. 본 실험은 슬라이싱의 사용이 대용량-손실민감 트래픽에 대한 낮은 손실률을 달성할 수 있음을 보여주며, 큰 패킷 전송량으로 인해 큐잉 지연을 발생시킬 수 있는 대용량

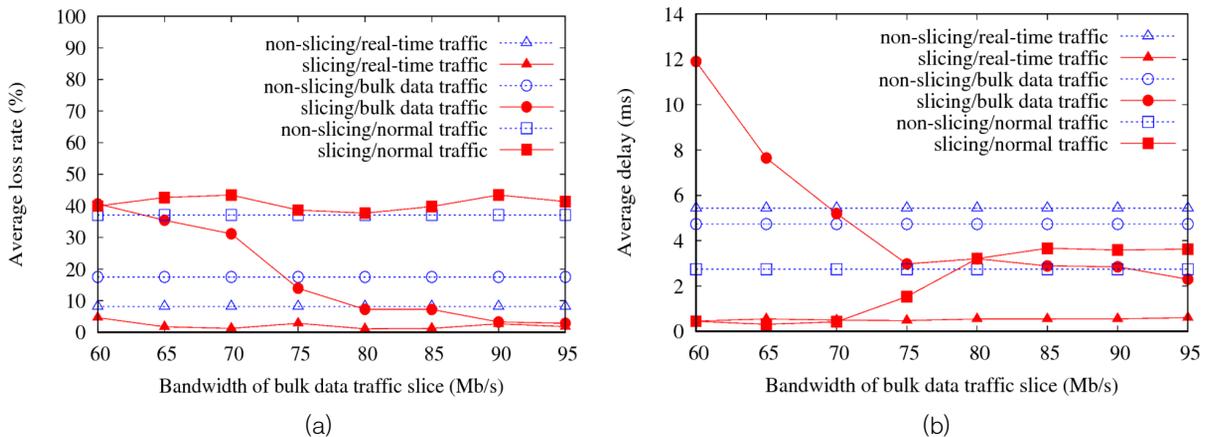


Fig. 7. Packet loss rate and delay with respect to the bandwidth allocation for bulk data traffic (number of flows: 200)

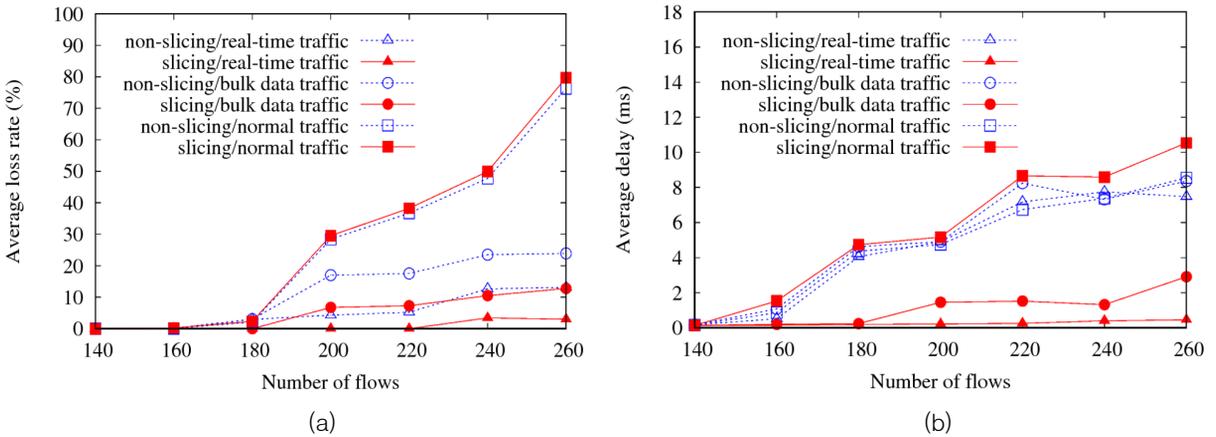


Fig. 8. Packet loss rate and delay with respect to the total number of flows(bandwidth of bulk data traffic slice: 75 Mb/s)

트래픽으로부터 실시간 트래픽을 격리함으로써 큐잉 지연의 발생을 낮출 수 있음을 확인하였다.

Fig. 8은 대용량-손실민감 트래픽 슬라이스의 예약 대역폭이 75 Mb/s일 때, 총 플로우 개수에 따른 각 서비스별 패킷 손실 및 지연을 나타내는 그래프이다. 단일 네트워크에서 트래픽을 서비스하는 경우 트래픽양이 증가함에 따라 패킷 손실과 지연이 크게 증가하는 것을 볼 수 있다. 제안하는 네트워크 가상화 기법을 적용한 경우 단일 네트워크 대비 대용량-패킷 손실민감 서비스 플로우의 패킷 손실률이 상당량 감소하였으며, 실시간 서비스 플로우의 지연은 트래픽 양에 따른 변동에 크게 영향을 받지 않고, 낮은 수준(< 1 ms)을 유지하는 것을 확인할 수 있다. 이는 전체 트래픽 양이 증가함에도 슬라이스 간 우선순위 조절 및 대역폭 예약을 통해 트래픽의 QoS 요구사항을 효과적으로 만족시킬 수 있음을 의미한다.

## 5. 결론

본 논문에서는 All-IP 기반 미래 전술통신망에서 다양한 QoS 요구사항을 가지는 응용 서비스의 품질 보장을 위한 전술망의 다계층 네트워크 가상화 구조와 서비스 품질 차별화 기법을 제안하였다. 제안하는 구조는 전술망 트래픽의 서비스 품질 요구사항에 따라 서로 다른 정책을 갖는 다계층 네트워크 슬라이스에 트래픽을 할당하여 서비스한다. 제안하는 구조에 대한

실험을 통해 트래픽을 단일 네트워크에서 처리하는 것과 비교함으로써, 패킷 손실에 민감한 트래픽의 경우 더 낮은 패킷 손실률을 달성함을, 지연에 민감한 트래픽의 경우 낮은 지연을 달성함을 검증하였다. 전술망의 네트워크 슬라이싱 구조의 적용은 본 논문의 실험에서 수행한 큐잉 정책의 차별화뿐만 아니라, 이동성, 보안, 라우팅 등의 다양한 정책 차별화를 구성하여 이를 관리하는 것에 대한 추가적인 연구가 필요하며, 이에 대한 향후 연구를 수행할 예정이다.

## 후 기

본 연구는 국방과학연구소가 지원하는 운용체계의 전술망내 정보유통 품질보증 방안 연구 과제에 일환으로 수행되었습니다(UD170050ED).

## References

- [1] A. K. Cebrowski and J. J. Garstka, "Network-Centric Warfare: Its Origin and Future," US Naval Institute Proceedings Magazine, vol. 124, no. 1, pp. 28-35, 1998.
- [2] R. Braden, D. Clark, and S. Shenker, "Integrated Services in the Internet Architecture: An Overview," Internet Engineering Task Force, RFC 1633, Fremont,

- CA, USA, 1994.
- [3] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, "An Architecture for Differentiated Services," Internet Engineering Task Force, RFC 2475, Fremont, CA, USA, 1998.
- [4] H. Zhang, N. Liu, X. Chu, K. Long, A. H. Aghvami, and V. C. Leung, "Network Slicing-based 5G and Future Mobile Networks: Mobility, Resource Management, and Challenges," IEEE Communications Magazine, Vol. 55, No. 8, pp. 138-145, 2017.
- [5] Y. Xue, C. Gedo, C. Christou, and B. Liebowits, "A Framework for Military Precedence-based Assured Services in GIG IP Networks," IEEE Military Communications Conference(MILCOM), pp. 1-7, 2007.
- [6] S. Kook, M. Chang, M. Lee, J. Jun, T. Kim, J. Choi, and B. Roh, "A Study on OSPF for Wireless Tactical Communication Networks," Communications of the Korean Institute of Information Scientists and Engineers, Vol. 37, No. 2, pp. 109-121, 2010.
- [7] Y. Kim, S. Shin, and Y. Kim, "A Priority-based Multipath Routing Mechanism in the Tactical Backbone Network," Communications of the Korean Institute of Information Scientists and Engineers, Vol. 42, No. 8, pp. 1057-1064, 2015.
- [8] Jang-wee Research Institute for National Defence in Ajou University, "Guarantee of Information Circulation for Weapon-system in All-IP Tactical Network," Research Report, 2014.
- [9] M. Marchese, "QoS over Heterogeneous Networks," John Wiley & Sons Limited, 2007.
- [10] A. Kantawala, D. Voce, and D. Gokhale, "QoS Architecture for Session Oriented GIG Applications," IEEE Aerospace Conference, pp. 1-9, 2006.
- [11] G. Choi, B. Kim, and B. Roh, "Classification of Traffic Classes for Application Services in Military Communication Networks," The Journal of Korean Institute of Communications and Information Sciences, Vol. 37, No. 1, pp. 76-88, 2012.
- [12] Y. Lu, B. Fu, X. Xi, Z. Zhang, and H. Wu, "An SDN-based Flow Control Mechanism for Guaranteeing QoS and Maximizing Throughput," Wireless Personal Communications, Vol. 97, No. 1, pp. 417-442, 2017.
- [13] R. Sherwood, G. Gibb, K. K. Yap, G. Appenzeller, M. Casado, N. McKeown, and G. Parulkar, "Flowvisor: A Network Virtualization Layer," OpenFlow Switch Consortium, Tech. Rep., Vol. 1, pp. 1-13, 2009.