

## 미래 전술망의 지능적 트래픽 QoS 조율을 위한 전술 서비스 메쉬

강문중<sup>1)</sup> · 신준식<sup>1)</sup> · 박주만<sup>2)</sup> · 박찬이<sup>2)</sup> · 김종원<sup>\*,1)</sup>

<sup>1)</sup> 광주과학기술원 전기전자컴퓨터공학부

<sup>2)</sup> 국방과학연구소 제2기술연구본부

### Tactical Service Mesh for Intelligent Traffic QoS Coordination over Future Tactical Network

Moonjoong Kang<sup>1)</sup> · Jun-Sik Shin<sup>1)</sup> · Juman Park<sup>2)</sup> · Chan Yi Park<sup>2)</sup> · JongWon Kim<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 Research and Development Institute, Agency for Defense Development(ADD), Korea

(Received 31 January 2019 / Revised 1 April 2019 / Accepted 24 May 2019)

#### ABSTRACT

As tactical networks are gradually shifting toward IP-based flexible operation for diversified battlefield services, QoS(Quality-of-Service) coordination for service differentiation becomes essential to overcome the heterogeneous and scarce networking resources limitations. QoS coordination for tactical network traffic should be able to monitor and react the dynamic changes in underlying network topology and service priorities. In this paper, by adopting the emerging cloud-native service mesh concept into tactical network context, we study the feasibility of intelligent QoS coordination by employing tactical service mesh(TSM) as an additional layer to support enhanced traffic quality monitoring and control. The additional TSM layer can leverage distributed service-mesh proxies at tactical mesh WAN(Wide Area Network) nodes so that service-aware differentiated QoS coordination can be effectively designed and integrated with TSM-assisted traffic monitoring and control. Also, by validating the feasibility of TSM layer for QoS coordination with miniaturized experimental setup, we show the potential of the proposed approach with several approximated battlefield traffics over a simulated TSM-enabled tactical network.

Key Words : QoS Coordination(서비스 품질 조율), Tactical Service Mesh(전술 서비스 메쉬),  
Traffic Monitor and Control(트래픽 관제), Tactical Information Communication Network(전술정보통신망)

#### 1. 서론

\* Corresponding author, E-mail: jongwon@gist.ac.kr  
Copyright © The Korea Institute of Military Science and Technology

킹을 통해 전장에서의 지휘 속도를 증가시키고 빠른 작전을 구사하여 전투력을 높이는 정보 우위 전쟁인 네트워크 중심전이 지속적으로 확산되고 있다<sup>[1]</sup>. 또한 전장 환경에서의 대화, 실시간 정보 전달 및 응용을 망라하는 다양한 전장 서비스들을 IP 기반 네트워킹으로 통합 지원하기 위한 All-IP 통합 전장 네트워크로의 전환도 계속 진행되고 있다. 전장 환경에서 전투원을 중심으로 벌어지는 네트워킹 상황은 Fig. 1과 같이 미국 육군의 사례를 통해 전체적으로 살펴볼 수 있다<sup>[2]</sup>. 각종 전술제대들 사이의 통신을 담당하는 무선 중심 네트워크인 전술망(tactical network)은 전장 환경의 다양한 지휘통제체계 간 협력적인 상호운용성을 강화하여 네트워크 중심전을 위한 중단 신경망 역할을 수행한다.

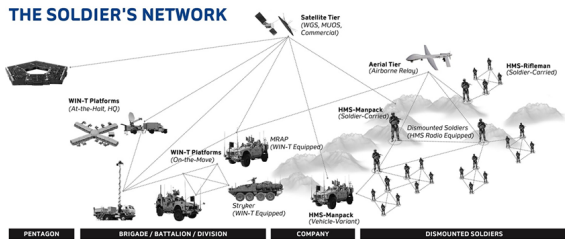


Fig. 1. Tactical networks from soldier's viewpoint<sup>[2]</sup>

이상적인 미래의 전술망은 모든 야전 무기체계의 기반이다. Fig. 1과 같이 지상, 해상, 공중, 우주에 구성된 네트워크들이 상호 연결된 고속 대용량의 다계층 통합 네트워크를 기반으로, 감시-정찰-결정-타격체계간 실시간 데이터 및 음성정보의 유통과 이에 기반한 응용 서비스들의 품질을 보장할 필요가 있다. 하지만 우선 전장에 산재한 전투원들과 무기체계들의 네트워킹을 IP 기반으로 통합하는 단일화가 필요하다. 추가하여 현재 시점에서 가용한 무선 위주의 전술망 대역폭은 매우 제한적이다. 따라서 응용 서비스의 중요도에 따라 제한된 대역폭 활용을 적절하게 조율하여 품질을 최대화하는 QoS 조율 문제의 해결은 매우 어려운 상황이다<sup>[3,4]</sup>. 이는 전술제대의 이동을 포함한 다양한 전장환경의 동적인 상황 변화에 따라, 전술망 전체의 네트워크 구조 및 상태가 바뀌기 때문이다. 또한 전투원들에게 필요한 응용 서비스들의 종류와 중요도도 수시로 변경되기 때문이다.

관련하여 전술망 상의 응용 서비스 QoS를 효과적으로 보장하기 위한 무선 네트워킹의 성능향상, 미리 정

의된 트래픽 우선순위에 따라 패킷을 차등 처리하는 정적인 QoS 향상 기술들이 제안되었다<sup>[5,6,7]</sup>. 하지만 전술망의 동적인 구조 및 상태 변화, 응용 서비스 트래픽들의 유형과 규모에 따라 중요도 분포가 동적으로 변화하는 전술망 트래픽의 특성을 고려한 응용 서비스의 지능적인 QoS 조율을 위해서는, 정적인 수준에 머무르는 응용 서비스 트래픽에 대한 QoS 조율을 보다 동적으로 개선하는 것이 핵심적이다. 따라서 상기 전술망의 특수성을 모두 감안하는 유연하고 동적인 QoS 조율을 수행할 수 있는 유연성있는 소프트웨어 구도(framework) 차원의 체계화된 접근 방식을 새롭게 모색하는 것이 매우 중요하다.

본 논문에서는 체계적으로 지능화된 QoS 조율을 위한 전술망의 트래픽에 대한 관제(모니터링 및 제어)를 수행할 수 있는 별도의 계층을 추가하는 방안을 제안한다. 인프라 계층과 응용 서비스 계층 사이에 존재하는 추가적인 계층을 통하여 전술망 QoS 트래픽 관제를 위한 실무적인 작업들을 수행하도록 구성한다. 인프라와 응용 계층을 연계하면서 QoS 관제를 지원하는 추가계층은 전술망 상의 응용 서비스별로 대역폭/지연/손실 등을 제어하는 지능화된 QoS 조율을 담당하는 주체(entity)인 QoS 관제타워와 함께 협력한다. 구체적으로는 클라우드-기반 컴퓨팅 분야에서 최근 주목받는 서비스 메쉬(service mesh) 개념을 전술망에 맞도록 변형하고 확장하여 미래 전술망에 적용이 가능한 '전술 서비스 메쉬(TSM: Tactical Service Mesh)'를 제안한다. 그리고 이를 활용하는 보다 동적인 QoS 조율의 가능성을 모색하기 위하여 실증을 위한 구현 방안과 간략화된 전술망을 대상으로한 모의실험을 통한 가능성 검증 결과를 논의하고자 한다.

## 2. 관련 연구 및 요구사항 분석

### 2.1 전술망 서비스 QoS 조율 관련연구

제한되고 변동이 심한 네트워킹 자원을 활용하면서 동적인 네트워킹 수요를 만족시켜야 하는 전술망 상의 응용 서비스 QoS를 조율하는 난제를 해결하기 위해 여러 방법의 접근들이 탐색되어 왔다. 먼저 전장상황의 변동에 적응화를 통한 무선 네트워킹 자체의 효율성 개선에 치중하여 상호연결 대역폭을 최대로 유지하려는 시도들이 있다. 미국 DARPA는 WNaN(Wireless Network after Next) 프로그램을 통해 DTN(Delay and

disruption Tolerant Networking) 방식을 연구하였다. DTN 방식으로 상용화된 하드웨어의 채택을 늘려서 단가를 절감함과 동시에, 연결성 확보의 애로 상황에 맞춰 MIMO(Multiple Input Multiple Output)를 통한 대역폭 확보, 빔포밍을 이용한 연결거리 증가, 주파수 도약 및 회피할 수 없는 전파에 대한 상쇄간섭 등을 활용하는 DSA(Dynamic Spectrum Access) 방식을 제안하였다<sup>5)</sup>. 또한 DARPA CBMANET(Control-Based Mobile Ad-hoc Networking) 프로그램을 통해 상시 이동 중인 노드간의 Ad-hoc 네트워킹의 개선도 시도하였다. 즉 노드간 Ad-hoc 연결의 품질을 측정하여 가용 대역폭을 산출하고, 패킷에 경로 정보를 덧붙여 멀티캐스팅 하면서 네트워크 코딩을 적용하여 최적으로 경로를 파악하고 활용하는 라우팅 제어를 제안한 바 있다<sup>6)</sup>.

하지만 근본적으로 한정된 네트워크 대역폭이라는 제약은 가지는 전술망을 운용하는 전장환경에서는 응용 서비스들의 중요도에 따른 트래픽 관제를 통해 QoS를 개선하는 방식이 필수적이다. 이 때 All-IP 기반으로 수립된 전술망 상의 주요 응용 서비스들은 대역폭, 지연, 손실 등에 대한 요구 수준이 모두 다르다. 미국 육군의 WIN-T(Warfighter Information Network-Tactical) 전술망 사례에서는 응용 서비스들의 상대적인 차등화를 통한 QoS 조율 방식인 DiffServ 방식을 근간으로 긴급한 트래픽을 예외적으로 우선 처리하는 구조를 채택하여 활용하고 있다<sup>7)</sup>. 채택된 DiffServ 방식에서는 트래픽 분류 기법과 연동하면서 미리 약속된 트래픽 별 우선순위(priority) 정책 등에 따라 IP 패킷 헤더에 DSCP(DiffServ Code Point)를 표기한다. 그리고 패킷들이 경유하게 되는 각 전술망 라우터에서 차등화된 처리(즉 PHB: Per Hop Behavior)를 받도록 조정한다. 이를 위해서는 산재된 전술망의 핵심 네트워크 노드들을 중심으로 사전에 검증되고 확인된 설정 값들을 적용하고 유지하는 정적인 QoS 조율 과정에 크게 의존하게 된다.

## 2.2 마이크로서비스 구조와 서비스 메쉬

새롭게 부상하는 클라우드 기반 컴퓨팅(cloud-native computing) 기술과 네트워크에 기반한 다양한 응용 서비스들이 활성화됨에 따라, 응용 서비스의 구조는 모놀리딕(monolithic) 구조가 아닌 마이크로서비스

(microservices) 구조로 점차적으로 전환되어 구현되고 있다<sup>8)</sup>. 마이크로서비스 구조는 응용 서비스 내부의 여러 요소들을 복수의 기능(function)들로 분할하고 이들을 네트워킹으로 연결(inter-connect)하여 합성하는 방식으로 서비스를 실현한다. 이로 인해 개발 및 유지보수의 용이성 등의 장점을 갖고 있다. 상기한 응용 서비스 실현 구조의 전환으로 미래형 응용 서비스의 QoS는 기능들을 서로 연결하는 네트워킹 품질에 크게 영향을 받게 되었다. 하지만 네트워킹의 품질은 서비스들이 실현되는 네트워킹 인프라에 따라 변동되는 특성을 지닌다. 따라서 서비스 요소 기능들을 연결하는 네트워킹의 QoS 보장을 전적으로 망 인프라에만 맡길 수 없으므로 이를 추가로 감안하는 응용 서비스를 구현하는 부담이 있다<sup>9)</sup>.

클라우드 기반 컨테이너 요소 기능들을 서비스 합성하는 동적인 마이크로서비스 구조로 구현된 미래형 응용 서비스를 대상으로, 상기한 상호 연결 문제를 인프라 계층과 응용 계층 사이에 새로운 계층을 추가하여 해결코자 하는 방식이 서비스 메쉬(Service Mesh)이다<sup>10)</sup>. 서비스 메쉬는 응용 서비스가 요구하는 견실한 QoS 제공을 지원하도록 관제(즉 모니터링 및 제어)를 기반한 QoS 조율을 수행하며, 이를 위해 대역폭이 한정되거나 변동이 심한 네트워킹 인프라를 파악해야 한다. 견실한 QoS 보장이란 네트워킹 인프라의 상태와 응용 서비스 QoS 요구사항의 동적인 변동을 실시간으로 감안하여, 응용 서비스의 품질을 안정적으로 보장하는 것을 의미한다. 이를 위해서는 개별 노드 수준의 미리 정의된 알고리즘 보다는 전술망 전체 인프라와 응용 서비스의 상태를 실시간 모니터링하여 파악하고, 이를 기반으로 두 계층의 QoS를 함께 제어하는 것이 효과적이다. 그런데 일반적으로 네트워킹 인프라의 핵심인 스위치, 라우터 등은 대부분 특화된 폐쇄형 하드웨어에 의존하므로, 이와 같은 트래픽에 따른 동적인 맞춤형 관제가 힘든 상황이다. 서비스 메쉬는 이러한 문제점을 극복하고자 컴퓨팅 서버 내부의 컨테이너 기반 요소 기능들에 에이전트(agent)를 부착하는 방식으로 응용 서비스를 위한 트래픽을 밀접하게 모니터링한다<sup>11)</sup>. 이를 통해 단순한 패킷 통계 수준의 트래픽 모니터링을 벗어나 응용 서비스를 위한 트래픽을 서비스 진행 단계별로 구분하는 수준의 모니터링과 이에 기반한 트래픽 제어가 가능하다. 즉, 서비스 메쉬 계층을 추가함으로써 응용 서비스에 집중된 트래픽 QoS 모니터링 및 제어를 효과적으로 보

1) 모놀리딕 구조에서는 서비스 요소 기능 중 하나만 오류가 생기더라도 전체 서비스가 영향을 받게 되며, 서비스 확장성이 극히 제한되는 문제가 있음.

조할 수 있음에 주목해야 한다.

### 2.3 전술망의 변동성과 이에 대응하는 QoS 관제 요구사항

본 논문에서는 트래픽 QoS에 대한 관제(모니터링/제어)의 적용 대상으로 Fig. 2와 같은 구성을 지니는 간략화된 전술망을 가정한다. 즉 지향성 또는 섹터 안테나를 통해 서로 연결된 전술망 WAN 노드들이 수십 km에 걸쳐 메쉬 구조로 WAN을 이루고 있다. 장거리 무선 연결의 특성상 WAN 노드들은 제한된 대역폭을 가진다. 또한 상황에 따라 상호 연결이 불안정해지며, 때로는 릴레이 노드를 경유해서 연결되어야 한다. 즉 전술망은 구조와 연결성이 동적으로 크게 변동하는 제약을 가진다. 그러나 서론에서 설명한 바와 같이 열악한 전술망 상황을 통제하면서 전술망 상의 다양한 응용 서비스들의 QoS를 적정수준으로 제공할 필요성이 있다. 따라서 사용자 및 임무에 따른 응용 서비스의 중요도가 상이함에 착안하여, 트래픽에 대한 대역폭/지연/손실 등을 중요도에 따라 차별적으로 관제하는 방식을 통해, 네트워크 QoS와 전술망의 제약을 절충하는 해결 방법이 필요하다.

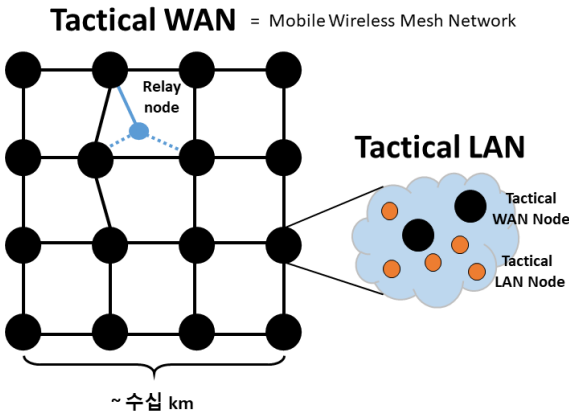


Fig. 2. Tactical WAN and LAN

전술한 바와 같이 변동이 심한 전술망을 대상으로 트래픽 QoS 보장을 위해서는 단순히 사전에 설정된 기준 값에 따라 정적으로 QoS 관제를 수행하는 방식으로는 역부족이다. 따라서 Fig. 3과 같은 구도의 지능화된 QoS 조율(Intelligent QoS coordination)이 필수적이다. 지능화된 QoS 조율을 위해 주요 트래픽의 우선 순위 및 규모 등에 대한 정보를 사전에 확보하고, 응

용 서비스 별 중요도에 따른 트래픽 관제 정책(policy) 등에 따라 적정한 QoS 관제의 동작범위를 설정한다. 그리고 실시간으로 모니터링되는 전술망 응용 서비스 트래픽의 초당 송수신량, 응답성공률, 전송지연 등의 메트릭(metric)들에 따라 지능적인 트래픽 제어가 이뤄지도록 지원해야 한다.

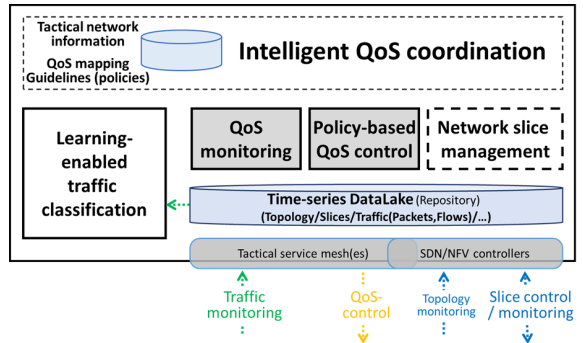


Fig. 3. Intelligent QoS coordination with traffic QoS monitor & control for tactical network

Fig. 3을 추가적으로 살펴보면, 지능화된 QoS 조율을 수행하는 트래픽 관제를 위해서는 학습(machine/deep learning)기반으로 전술망 트래픽 패킷들을 서비스 유형과 중요도 등으로 구분하여 분류할 수 있도록 뒷받침해야 한다. 또한 전술망 전체의 구조 및 상태 변화, 전술망 트래픽의 대용량 QoS 모니터링 데이터를 시계열(time series) 기반으로 축적할 저장소(repository)인 데이터레이크(DataLake)도 필요하다. 향후에는 네트워크 가상화 기술의 발전에 따라 전술망의 고도화가 이뤄질 경우, 전술망을 논리적으로 분할하여 서로 다른 특성을 지니도록 특화시킨 가상 네트워크들을 지칭하는 네트워크 슬라이스들이 적용될 것으로 예상된다. 따라서 네트워크 슬라이스들을 활용하는 트래픽 QoS 조율이 가능하도록 지원해야 한다.

### 3. 서비스 메쉬를 도입한 전술망을 위한 트래픽 QoS 조율 방식

#### 3.1 변동에 대응하는 QoS 관제를 위한 계층화

서론에서 밝힌 것처럼 본 논문에서는 논리적으로 중앙 집중화된 QoS 트래픽 관제를 위하여, 소프트웨어 중심의 계층을 추가하면서 이를 활용하여 지능화된

QoS 조율을 주관하는 주체인 지능적 QoS 관제타워의 필요성을 제안하고 있다. 즉 QoS 관제타워가 원활하게 동작하려면, 뇌의 지시에 따라 움직이는 손발처럼 실제로 미래 전술망 트래픽에 대한 관제(모니터링과 제어)를 수행하는 지원 계층이 필요한 것이다.

이와 같은 트래픽 관제에 대한 실무를 담당하는 지원 계층으로 제어/데이터 평면의 분리를 통해 소프트웨어-기반으로 네트워킹을 제어하는 논리적으로 중앙 집중화된 SDN(Software-Defined Networking) 제어기를 확장하는 접근 방식을 고려할 수도 있다. 하지만 SDN 방식은 분산된 네트워크 스위치/라우터에 대해서 플로우 중심의 Tag-Steer-Map 개념의 중앙 집중형 네트워킹 경로 조정에 치중한다. 따라서 전술망 상에 퍼져있는 응용 서비스 트래픽 별 대역폭/지연/손실 등을 직접적으로 파악하고 대응하기에는 힘들다. 유사하게 5G 모바일 네트워킹에서 점차 상용화가 시작될 고수준의 네트워크 가상화 기술인 네트워크 슬라이싱(network slicing)의 관리주체를 상기한 지원 계층을 주관하도록 적용하는 방안도 예상할 수 있다. 하지만 SDN/NFV<sup>2)</sup> 제어기들을 포용하면서 목적하는 네트워크 가상화를 수행하고 관리하는 네트워크 슬라이스 관리 주체를 활용하는 방식도 현시점에서는 현실적이지 못하다. 현재 활발하게 개발 중인 네트워크 슬라이싱 기술은 5G 이동 통신 분야에서 성숙과 검증은 거친 이후에야 운용상의 제약이 큰 전술망에 도입하여 적용하는 것이 가능해질 것으로 판단되며, 트래픽 QoS 관제까지 함께 주관하도록 추가로 확장하는 것은 향후의 과제로 보는 것이 적절하다<sup>12)</sup>.

따라서 QoS 관제타워의 지시에 따라 QoS 관제에 대한 실무를 보조하는 추가 계층을 다음과 같은 요구 사항들을 반영하면서 새롭게 도입하는 것이 필요하다고 제안한다. 첫째로 응용 서비스별 차별화된 QoS 조율을 위해, 관제하는 트래픽 패킷을 신속하게 수집 및 분류한 후 분류된 유형별로 트래픽 특징을 파악하여 응용 서비스를 식별하는 서비스-인지형(service-aware) QoS 모니터링을 제공해야 한다. 둘째로 전술망 상의 트래픽에 대한 제어를 SDN 제어기를 통한 경로 제어와 향후 추가될 미래형 네트워크 슬라이스들과 연계하여 수행하는 것도 필요하다. 이를 통해 응용 서비스 트래픽 별로 차별화된 QoS 제어를 제공함으로써 지능화된 QoS 조율을 지원해야 한다. 셋째로 QoS 관제를

위해 추가하는 지원 계층에서 발생하는 트래픽은 전술망의 응용 서비스들의 트래픽과 분리되어, 제어(및 모니터링) 평면과 데이터 평면으로 나뉘어져야 한다. 이를 통해 서비스를 이용하는 하급 제대가 전술망을 관리하는 상급 제대의 권한을 침범하지 못하게 방지한다. 또한 QoS 모니터링 및 제어는 동적인 변동이 심한 전술망의 상태에 전적으로 의존하지 않으면서 견실하게 수행되도록 특별 대우를 하는 것도 요구된다.

### 3.2 전술 서비스 메쉬를 활용한 QoS 조율

전술한대로 본 논문에서는 QoS 관제타워를 중심으로 하부에서 발생하는 네트워크 토폴로지 및 트래픽 규모/우선순위 등의 동적인 변화를 극복하는 접근 방식으로, 2.2절에서 설명한 서비스메쉬를 미래 전술망 환경에 맞춰서 변형하고 확장하는 방식을 제안하고자 한다. 즉 미래 전술망의 데이터 평면과 모니터링/제어 평면을 분리하고 전술망 상의 응용 서비스 트래픽별 QoS 조율을 위한 관제에 대한 실무를 담당하는 추가적인 지원 계층인 전술 서비스 메쉬(TSM: Tactical Service Mesh)를 제안한다. 그리고 이를 통해 전술망 상의 트래픽 QoS 관제를 견실하고 확장성 있게 수행하는 문제에 접근하고자 한다.

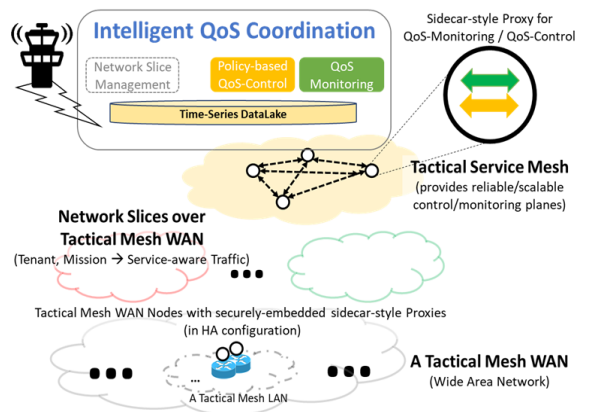


Fig. 4. Intelligent QoS coordination with TSM layer, dedicated for QoS monitoring/control planes

Fig. 4에 도시한 TSM은 네트워크 가상화 기술을 통해 분할된 복수의 데이터 평면들(네트워크 슬라이스)에 대한 논리적인 QoS 관제타워의 지능적 QoS 조율을 보조하는 지원 계층으로, 응용 서비스별로 차별화된 QoS 관제를 지원하여 전체적인 QoS 조율에 기여

2) NFV(network function virtualization): 네트워크 기능 가상화



하게 된다. Fig. 2에 제시한 간략화된 전술망의 핵심 노드이며 응용 서비스들의 트래픽들이 흐르는 중요한 교차점인 전술 WAN 노드(HA를 위해 2개 노드를 클러스터링한)를 대상으로 소프트웨어 기반의 TSM 대응 프록시(Proxy)를 부착형으로 배치한다. 이를 통해 전술망 전체에 배치한 TSM 대응 프록시들을 통해서 모든 응용 서비스(데이터) 트래픽이 거쳐 지나가도록 구성한다. 즉, 분산 배치한 프록시들을 QoS 관제를 지원하기 위한 에이전트로 삼으면서, 이들을 상호 메쉬 형태로 연계하고 통합하는 것이다.

추가한 TSM은 분산 배치된 프록시들이 필요에 따라 동적으로 상호 연계되는 메쉬 구조가 중심이지만, 소프트웨어-기반 TSM API(Application Programming Interface)들을 통해 QoS 관제타워에 의해 논리적으로 중앙제어 됨으로써 하나의 통합된 계층으로서 QoS 관제의 실무역할을 수행한다. 프록시는 관제타워가 필요로 하는 다양한 형식의 QoS 모니터링 데이터를 수집하고 보고하거나, 반대로 QoS 제어를 SDN/NFV 제어기와 협력하면서 수행하게 된다. 이 때 전술망 환경의 특성을 고려하여 QoS 관제타워와 프록시들 간에 안전하고 견실한(secured & reliable) 연결성을 확보하는 것이 필수적이다. 따라서 데이터 평면과는 분리한 별도의 모니터링/제어 평면을 통해서 암호화된 수준으로 모니터링 및 제어 데이터를 교환하는 것을 가정한다. 전술망과 같은 무선 기반 네트워크에서 물리적인 평면 분리가 어려움을 감안하여 In-band 네트워크를 지원하는 상태에서 논리적인 평면 분리가 이뤄지도록 지원하는 것이 필요한 상태이다.

QoS 관제타워는 분산된 TSM 대응 프록시들과 안전하게 대화하면서 응용 서비스 트래픽에 대한 Tagging을 동반하는 맞춤형 QoS 모니터링을 수행한다. 동시에 관제타워의 지시에 따라 SDN/NFV 제어기와 협력하면서 트래픽에 대한 필터링(conditioning), 우선순위 조정(queueing & scheduling), 차별화된 경로제어(steering via routing/forwarding coordination) 등을 통한 차별화된 QoS 제어가 가능하도록 지원한다.

#### 4. TSM 기반 전술망 트래픽 QoS 조율의 구현방안

##### 4.1 TSM의 동적인 QoS 관제를 위한 전술 메쉬 WAN 노드

기존 전술망을 구성하는 폐쇄적인 상용 스위치/라우

터는 제한적인 개방성 및 유연성으로 인하여, 임의의 소프트웨어-기반 도구나 기술들을 추가 적용하는 것에 제한적이다. 이에 따라 TSM이라는 추가적인 계층을 기반으로 응용 서비스 트래픽에 대한 동적인 QoS 관제를 수행하는 미래 전술망의 전술 WAN 노드로 폐쇄형 네트워킹 박스를 활용하는 것은 어려운 상황이다. 따라서 TSM을 위하여 특별하게 하드웨어 및 소프트웨어를 통합 설계하는 전술 메쉬 WAN 노드를 Fig. 5와 같이 제안한다. 전술 메쉬 WAN 노드는 리눅스 계열 운영체제를 기반으로 SDN 기능들을 응용 서비스 형태로 운용하여, 전술망 메쉬 LAN 노드 및 다른 전술망 메쉬 WAN 노드들과의 스위칭/라우팅 등의 네트워킹을 제공하는 범용(commodity) 화이트박스 서버/스위치로 설계한다.

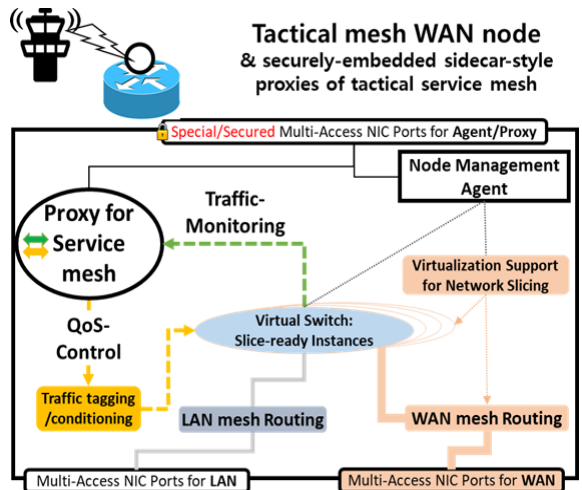


Fig. 5. Tactical mesh WAN node

이러한 화이트박스 서버/스위치에 기반한 네트워킹은 최근 통신사를 중심으로 고수준의 성능과 안정성/보안성이 확보 및 검증되어 실제 서비스 환경에 투입되기 시작하였다. 일례로 미국의 통신사 AT&T는 수십 Gbps 수준의 5G 대응 액세스(access) 네트워킹을 종단 사용자들에게 제공함에 있어서, 화이트박스로 구축한 셀 타워(cell tower)를 배치하는 단계이다<sup>[13]</sup>. 이러한 추세를 감안하여 제안하는 전술 메쉬 WAN 노드는 제약된 대역폭을 갖는 전술망 환경에서 요구하는 성능(Gbps급)을 무난하게 제공할 수 있다고 예상된다. 또한 무기체계/전술제대 별로 상이할 수 있는 이종의 네트워킹을 호환성 있게 지원하기 위한 하드웨어 확

장이나 QoS 조율을 위한 다양한 리눅스 기반의 소프트웨어 기능들을 쉽게 수용하는 유연성을 제공할 수 있다.

전송망에서 전송 메쉬 WAN 노드의 기본적인 역할은 트래픽을 중계하여 인접한 전송 LAN/WAN 노드들을 연결하는 네트워킹 박스로서 동작하는 것이다. 이에 따라 전송 LAN 노드들과 전송 WAN 노드들을 위해 각각 확보한 다중-액세스 네트워킹 인터페이스를 통해 송수신되는 트래픽들을 내부에 구성된 가상스위치를 기반으로 포워딩/라우팅하는 네트워킹 기능을 제공해야 한다. 이 때 향후 네트워크 슬라이싱 기술이 적용될 미래 전송망을 고려하여, 복수의 네트워크 슬라이스에 각각 대응하는 복수의 가상스위치 생성 및 관리를 지원한다. 상기 구성으로 제공되는 네트워킹 기능을 통해 모든 응용 서비스 트래픽들은 전송 메쉬 WAN 노드를 통해 송수신된다. 이 때 전송 메쉬 WAN 노드의 핵심 구성 요소이자 QoS를 위한 에이전트 역할을 수행하는 TSM 대응 프록시는 논리적인 QoS 관제타워와의 상호작용을 바탕으로 노드를 통과하는 응용 트래픽에 대한 QoS 관제를 수행한다. 이를 위해 TSM 대응 프록시는 응용 서비스 트래픽이 전송되는 데이터 평면용 인터페이스와는 별개로, 모니터링/제어 평면을 위한 특별한 다중-액세스 네트워킹 인터페이스들을 통해 QoS 관제타워와 안전하고 견실한 네트워킹 연결성을 확보한다. 그리고 프록시는 응용 서비스 트래픽이 통과하는 가상스위치에서 측정/추적(measurement and tracing)을 통한 QoS 모니터링을 수행하고, 이를 안전한 네트워킹 인터페이스를 통해 QoS 관제타워로 전송한다. 반대로 QoS 관제타워로부터 전송망 상의 응용 서비스들의 대역폭/지연/손실 등을 조정하는 QoS 조율 메시지를 수신하면, TSM 대응 프록시는 수신한 제어 명령에 따라 선택된 트래픽에 대한 컨디셔닝, 우선순위 조정, 차별화된 경로제어 등의 QoS 제어를 가상스위치를 대상으로 적용한다. 상기한 전송 메쉬 WAN 노드의 구성 및 관제방식을 활용하면 QoS 관제타워는 전송망 상의 응용 서비스 트래픽에 대한 QoS 모니터링 및 제어를 연계함으로써 동적인 전송망 상태를 실시간으로 반영하는 지능적 QoS 조율이 가능하다.

TSM 대응 프록시들은 네트워크의 안정성이 보장되지 않는 전송망에서도 동작하는 견실성을 유지할 필요가 있다. 하지만 변동이 극심한 전송망과 연결된 모든 프록시들이 관제 타워와 QoS 모니터링/제어 평면을 통

해 상시 연결됨을 보장하기 어렵다. 따라서 QoS 모니터링/제어 평면을 위해서는 특정 트래픽을 처리할 때마다 매번 관제타워가 모든 동작 명령을 프록시들에게 직접 지시하는 대신, 관제타워가 결정한 특정 조건 하에는 특정 행동을 수행하도록 지시하는 규칙 형태의 지침을 정기적 또는 비정기적으로 분산된 프록시들에게 배포하는 방식을 활용한다. 이를 통해 관제타워와의 연결이 일시적으로 단절되는 상황에서도 프록시들은 저장된 지침에 따라 지속적으로 QoS 관제를 수행하며, 네트워킹 연결이 복구되면 관제타워로부터 지침을 다시 내려받아 QoS 관제 방식을 갱신하게 된다.

#### 4.2 TSM 기반 QoS 모니터링 및 QoS 제어

응용 서비스 트래픽에 대한 대표적인 모니터링 방식으로 스위치, 라우터 등 네트워킹 박스를 통과하는 트래픽을 샘플링/미러링하여 별도로 준비된 모니터링 주체로 보내 처리하거나 패킷을 세밀하게 살피는 DPI (Deep Packet Inspection) 방식이 있다<sup>[4][6]</sup>. 이러한 물리적 인프라에 의존하는 방식들은 네트워크 슬라이스들로 구분된 복수의 데이터 평면들을 다루는 가상화된 네트워킹들에 대한 모니터링에는 적합하지 않다. 반면 NFV 에 대응하는 가상화된 네트워크 기능의 하나로 간주할 수도 있는 TSM 대응 프록시들을 실제 트래픽이 흐르는 네트워킹 교차점에 위치시키면 가상화에 무관하게 모든 응용 서비스 트래픽에 대한 관제가 가능하다. 그리고 데이터 평면의 트래픽을 실시간으로 모니터링하는 프록시들에 트래픽 분석을 추가로 수행하면 응용 서비스를 이해하는 소위 서비스-인지형(service-aware) QoS 모니터링을 지원할 수 있다. 이를 위해 관제타워가 각 전송망 응용 서비스 별 세부 정보를 프록시에게 전달하면, 프록시는 수신한 트래픽에 대해 확보한 정보를 활용하여 응용 서비스 식별을 개선할 수 있다.

이러한 실시간 지향의 QoS 모니터링은 전송망 WAN 노드들에 분산된 모든 프록시들에서 수행되며, 수집된 모니터링 데이터는 암호화된 연결을 통해 안전하게 논리적 관제타워 내의 시계열 데이터레이크로 전송되고 저장된다. 이때 응용 서비스 트래픽의 패킷 헤더를 읽는 방식의 QoS 모니터링은 논리적인 중앙집중형 관제타워 입장에서 전송망 내에서 사용하는 응용 서비스별 헤더 정보 세트가 제공된다면 최소화된 연산만으로 각 모니터링 지점에 대한 서비스-인지형 QoS 모니터링의 수행이 가능하다. 이를 통해 QoS 모

니터링의 오버헤드를 줄여 대역폭에 제한된 전술망에서도 충분히 사용할 수 있다. 이를 통해 학습기반 트래픽 분류(learning-enabled traffic classification) 및 트래픽 우선순위에 대한 동적인 변화를 흡수하면서, QoS 조율을 위한 의사결정을 위한 참고자료로 사용하기 위한 형태로 보관하도록 구성한다.

반면에 QoS 제어 평면은 QoS 모니터링을 통해 식별한 응용 서비스별 트래픽을 주어진 QoS 정책에 맞도록 실제로 제어한다. 앞서 논의한 바와 같이 전술망의 토폴로지 및 응용 서비스 관련 각종 변동에 유연하게 대응하려면, QoS 제어 평면도 QoS 모니터링 평면과 유사하게 서비스-인지형 제어를 지원해야 한다. 추가로 전술망 네트워크 인프라 자체를 상세하게 이해하는 네트워크-인지형(network-aware) 속성도 매우 유용하다. QoS 제어가 TSM 중심으로 응용 서비스 트래픽에 적용할 수 있는 명령에는 대역폭/응답속도 등을 만족시키도록 강제하는 컨디셔닝이나 우선순위의 조정(prioritized queuing & scheduling) 등이 있다. 또한 SDN/NFV 제어기와 협력하는 QoS 제어에는 해당 응용 서비스 상태와 네트워크 상황 조건에 따라 패킷 경로를 조정하는 방식 등이 있다.

## 5. 전술 서비스 메쉬를 활용하는 QoS 조율의 가능성 검증

### 5.1 PoC 검증 환경

TSM을 활용한 동적인 QoS 조율의 가능성을 검증하기 위해, Fig. 2에서 가정하는 간략한 미래 전술망 구도에 따라 7개의 전술망 메쉬 WAN 노드와 지능화된 QoS 조율 담당 주체에 대응하는 관제타워로 구성된 검증환경을 구축한다(Fig. 6 참고). 화이트박스 서버/스위치로 설계한 전술망 메쉬 WAN 노드는 AMD64 아키텍처 기반에 Ubuntu 리눅스 배포판이 설치된 범용 서버 노드를 활용한다. 또한 전술망 환경의 지향성 안테나를 활용한 무선 중심의 네트워킹을 고려할 때, 실제 전술망의 안테나를 활용한 검증환경을 구축하는 것은 현실적으로 어려운 상황이다. 따라서 TSM 계층의 가능성 검증 환경에서는 전술망이 갖는 제한된 대역폭을 고려하여, 각 전술망 메쉬 WAN 노드를 전송 속도를 100 Mbps로 제한한 단일 유선 네트워킹 인터페이스들을 갖도록 구성한다.

위와 같이 구성된 검증환경에서 각 전술망 메쉬

WAN 노드에 직결된 전술망 LAN에서 실행되는 미래형 전술망 응용 서비스들을 마이크로서비스 구조에 대응하여 컨테이너 형태로 배포하는 경우를 가정한다. 즉 전술망 메쉬 WAN 노드를 컨테이너를 지원하는 클러스터 노드로 구성한다. 그리고 전술메쉬 WAN 노드의 TSM 대응 프로시저를 오픈소스 Envoy 소프트웨어로 준비하고, 이들을 상호 메쉬형태로 연결하고 관리하는 오픈소스 Istio 서비스메쉬 소프트웨어를 논리적인 관제타워에 적용함으로써 TSM 계층을 구성한다. 이 때 TSM 프로시저의 모니터링/제어 평면과 데이터 평면을 암호화 기술을 이용하여 논리적으로 분리하도록 구성한다. 이와 같은 구성을 통해 전술망 상의 응용 서비스들이 컨테이너 기반으로 배포되어 운용될 때, 관제타워에서 프로시저들을 컨테이너에 부착된 형태로 함께 배포함으로써, TSM 대응 프로시저들이 메쉬 구조로 연결된 TSM 계층을 완성한다.

지능화된 QoS 조율을 위한 관제타워는 QoS 모니터링을 통해 실시간으로 수집한 데이터를 저장하는 데이터레이크를 오픈소스 시계열 데이터베이스인 Prometheus를 활용하여 구성한다. 그리고 QoS 모니터링 및 제어 지원 기능의 검증 결과를 제시하고자, 수집한 데이터를 그래프 형태로 가시화하는 Grafana 기반의 가시화 대시보드를 추가하여 구성한다. 그리고 전술망 운영자가 관제타워를 통한 중앙 집중형 QoS 조율을 수행하도록 별도로 개발한 Golang 기반의 API 서버를 운영한다.

추가적으로 검증을 위해 배포하는 마이크로서비스 구조의 예제 서비스에서 내부적인 트래픽 교환을 유발하는 전술망 응용 서비스 사용자의 요청을 시뮬레이션하기 위하여, 2 vCPU, 4GB RAM 사양의 가상머신 3대를 활용하여 서비스 요청 트래픽을 지속적으로 송신한다. 이러한 실험환경을 활용하여 지능화된 QoS 조율을 위해 TSM 계층을 통한 관제타워와의 상호작용을 수행한다. 세부적으로는 TSM 계층을 활용함으로써 QoS 모니터링과 제어 지원을 중앙집중형으로 수행 가능함을 다음 실험을 통해 검증한다.

### 5.2 QoS 모니터링: TCP 및 HTTP 트래픽

첫 번째 실험은 전장환경의 응용 서비스 간 트래픽에 대한 QoS 모니터링을 TSM 계층을 통해 쉽게 수행할 수 있는지 검증한다. 이를 위해 전장환경 응용 서비스를 가정한 예제 서비스로 Fig. 6의 하단부에 나타난 마이크로서비스 구조의 응용 서비스들을 컨테이



너 형태로 배치하였다. 예제 서비스는 9종류의 세부 서비스들이 트리구조로 상호 연결되어 있으며, 외부로부터의 서비스 요청이 발생한 경우 TCP 및 HTTP 프로토콜 기반의 트래픽들을 서로 주고받는다.

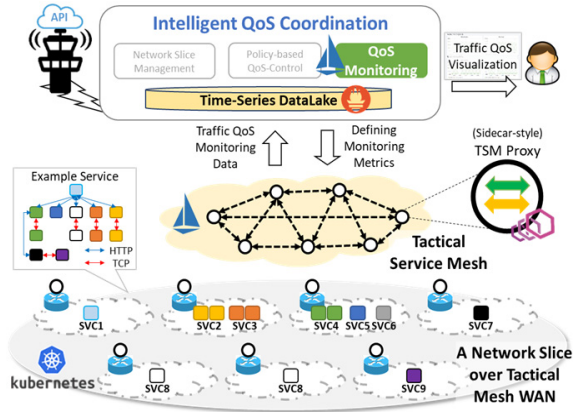


Fig. 6. Implementation and environment configuration for TSM-ready QoS monitoring

상기한 시나리오에 따라 배포한 응용 서비스들간 트래픽을 TSM 계층에서 실시간 모니터링한 결과를 Fig. 7을 통해 확인할 수 있다. 이는 관제타워와 각 응용 서비스에 부착된 프록시들이 대화하여 정의한 모니터링 메트릭에 따라, 응용 서비스 간 트래픽에 대한 QoS 모니터링 데이터를 수집하고 이를 관제타워의 데이터레이크에 저장한 후에 그래프 형태로 가시화한 것이다. Fig. 7의 그래프 제목에서 알 수 있듯, 상단의 6개 행은 HTTP 기반의 네트워킹을 수행하는 각각의 응용 서비스들을 대상으로 좌측부터 순서대로 수신한 요청 트래픽 양, 전송 성공률, 요청 후 응답 패킷 수신 시간, 응답 패킷의 크기를 가시화한다. 즉, TSM 계층의 프록시와 관제타워가 상호작용함으로써, 응용 서비스 수준의 트래픽의 QoS 정보를 실시간으로 모니터링하는 것이 가능함을 확인할 수 있다. 한편 Fig. 7의 하단 3줄은 TCP 기반 응용 서비스들의 그래프들로, TCP 트래픽은 HTTP와 달리 헤더가 없으므로 단순히 초당 입출력 바이트 수와 같은 트래픽 메트릭을 파악할 수 있다.

추가적으로 TSM 계층의 QoS 모니터링 지원이 견실하게 수행할 수 있는지 검증하기 위해, 2번/3번 서비스(SVC2/3)가 배치된 2번 WAN 노드의 네트워킹 인터페이스를 의도적으로 비활성하여 일시적인 장애를

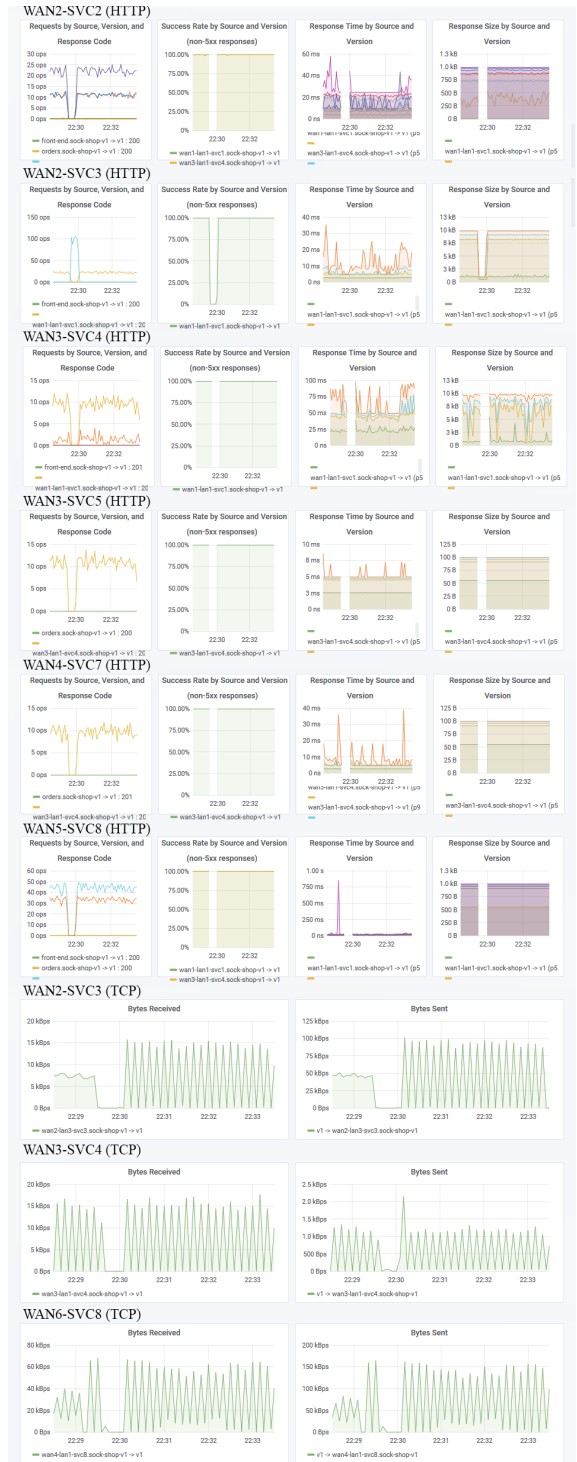


Fig. 7. Visualization of service-aware traffic QoS monitoring data collected by TSM

발생시킨 후 이를 다시 복원한다. 이 경우 Fig. 7의 1행과 2행의 그래프로부터, 2번 WAN 노드 내 서비스 트래픽의 요청 성공률이 저하됨과 동시에 응답실패 횟수가 증가하나, 해당 노드의 네트워크 연결이 복원 되었을 때 곧바로 트래픽 전송과 함께 모니터링 기능이 다시 복원됨을 확인할 수 있다. 이를 통해 일시적인 장애발생 후 프록시의 연결성이 자동으로 복원되는 TSM 계층의 안정성을 확인할 수 있다. 동시에 TSM 계층이 트래픽 QoS 모니터링 및 제어를 견실하게 지원하도록 프록시와 관제타워 간 모니터링/제어 트래픽을 위해 특별하게 준비한 멀티-액세스 네트워크 인터페이스가 필요함을 재확인할 수 있다.

5.3 QoS 제어: 트래픽 컨디셔닝과 차별화된 라우팅

본 절에서는 TSM 계층이 관제타워와의 상호작용을 통해 트래픽 QoS 제어 기능을 지원할 수 있음을 두 가지 검증 시나리오를 통해 부분적으로 검증한다. 이때 예제 서비스로 Fig. 8의 좌하단부에 표기한 것과 같이 네 종류의 세부 응용 서비스들이 네트워크 상호 연결된 마이크로 구조 형태의 서비스를 활용한다. 예제 서비스의 규모에 맞추어 검증환경을 7대의 전술메쉬 WAN 노드 중 4대만을 활용하도록 구성한다(Fig. 8). 예제 서비스를 세부적으로 살펴보면 응용 서비스 사용자가 1번 서비스로 접근하면 2번 서비스에 요청메시지를 전달하고, 2번 서비스는 4번 서비스로부터 필요한 정보를 획득하여 1번 서비스에 응답하는 방식으로 동작한다.

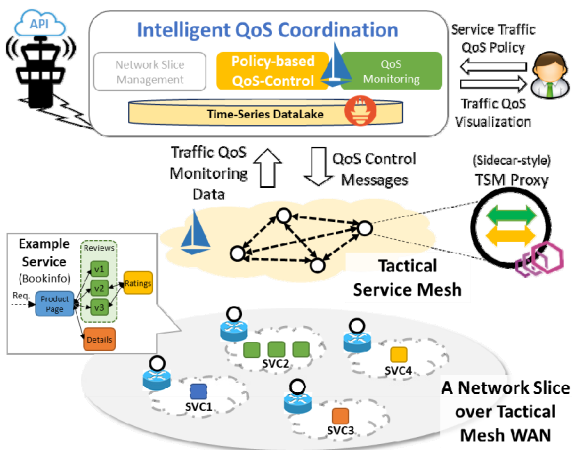


Fig. 8. Implementation and environment configuration for TSM-ready QoS control

검증 시나리오에서 전술망의 운영자는 논리적인 관제타워의 API 서버를 통해 서비스 트래픽의 QoS 제어 정책을 전달한다. 그리고 전달한 제어 정책에 따라 관제타워와 TSM 계층이 트래픽에 미친 영향을 실시간 모니터링 데이터의 가시화 결과를 통해 확인함으로써 TSM 계층의 QoS 제어 가능성을 검증한다.

QoS 제어의 첫 번째 검증 시나리오에서는 TSM 계층이 예제 서비스를 구성하는 특정 세부 서비스의 트래픽 전송을 조절하는 트래픽 컨디셔닝이 가능함을 제시한다. TSM의 트래픽 컨디셔닝을 위해 Fig. 9 상단에 나타낸 것과 같이 정책 1, 2를 적용한다. 운영자는 관제타워의 API를 통해 정책 1을 적용함으로써 4번 서비스(황색)의 요청 트래픽에 의도적인 2초 응답지연을 유발하는 트래픽 컨디셔닝을 적용한다. 그리고 트래픽 컨디셔닝이 정상 적용되었음을 검증하기 위하여, 정책 2를 적용하여 4번 서비스에 요청 트래픽을 전송하는 3번 서비스(녹색)를 대상으로 1초 내로 응답을 수신하지 않은 요청을 실패로 판단하도록 설정한다.

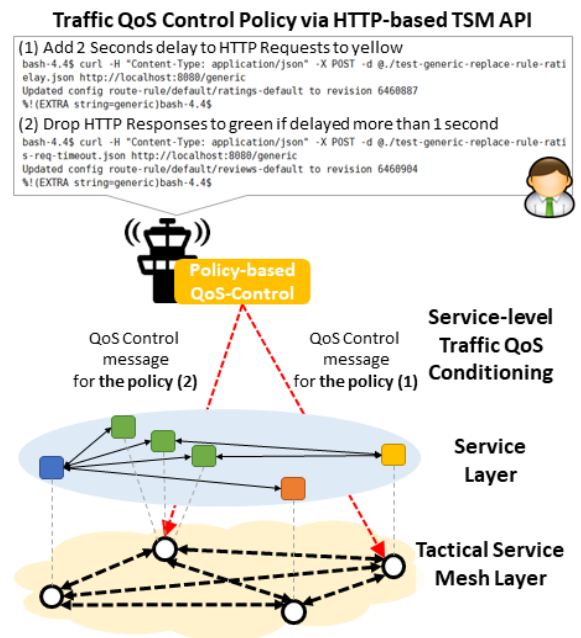


Fig. 9. Verification scenario for traffic conditioning of service traffic by TSM

TSM 계층에 트래픽 컨디셔닝을 적용하였을 때, 트래픽 전송에 미친 영향을 Fig. 10의 가시화 결과를 통해 확인할 수 있다. Fig. 10은 상단부터 순서대로 1번

(청색), 4번(황색), 3번(녹색) 서비스에 대응하며, 각 행을 구성하는 그래프는 좌측부터 초당 요청 패킷 수, 전송 성공률, 응답 시간, 응답 패킷 크기를 실시간으로 가시화한다. 본래 정상적으로 응답이 오고 가던 서비스들은 트래픽 컨디셔닝이 적용된 이후, 3번 서비스의 요청에 대한 4번 서비스의 응답이 2초 이상 지연되고, 이는 1초 이내로 응답을 수신하지 않아 실패로 간주되어 결과적으로 3번 서비스의 요청 횟수가 급감함을 볼 수 있다(3행 3열). 이에 따라 3번 서비스를 사용하는 1번 서비스의 트래픽 성능 또한 함께 영향을 받음을 확인할 수 있다(1행). 이러한 결과는 전술망 상의 트래픽이 과중한 상황에서, 비교적 낮은 우선순위의 지연에 민감하지 않은 응용 트래픽에 대한 의도적인 전송지연을 추가하여 응용 서비스의 트래픽 전송량을 제어하는 기초적인 수준의 QoS 트래픽 제어가 TSM을 활용하여 실시간으로 쉽게 적용 가능함을 보여주고 있다.

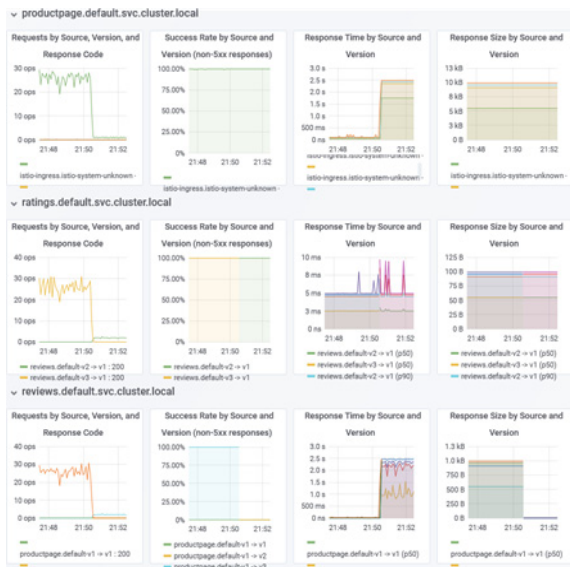


Fig. 10. Visualization of traffic QoS monitoring data before/after traffic conditioning by TSM

QoS 제어의 두 번째 가능성 검증에서는 전술망 응용 서비스에 접근하는 사용자의 권한에 따라 트래픽을 다른 경로로 제어하는 차별화된 라우팅/포워딩 사례를 제시한다. Fig. 11에 나타난 것과 같이 2번 서비스(녹색)는 3개의 세부 기능들로 구성되나, 동일한 요청을 수신하였을 때 하단의 2개 기능만 4번 서비스(황색)과

의 네트워크를 통해 추가적인 정보를 포함하는 응답을 회신한다. 1번 서비스에 외부 요청이 발생하였을 때, 해당 요청은 기본적으로 2번 서비스의 1번 세부기능으로 라우팅된다. 이 때 전술망 운영자는 Fig. 11의 상단에 표기된 정책을 관제타위의 API를 통해 적용함으로써 권한이 높은 “Jason”이라는 사용자를 위한 차별화된 라우팅 경로를 설정한다. 이를 적용하였을 때, 1번 서비스(청색)에서 반환하는 Web 기반의 결과가 다르게 나타나는 것을 통해 “Jason”의 트래픽이 일반 사용자의 트래픽과 다른 경로로 라우팅 됨을 제시한다.

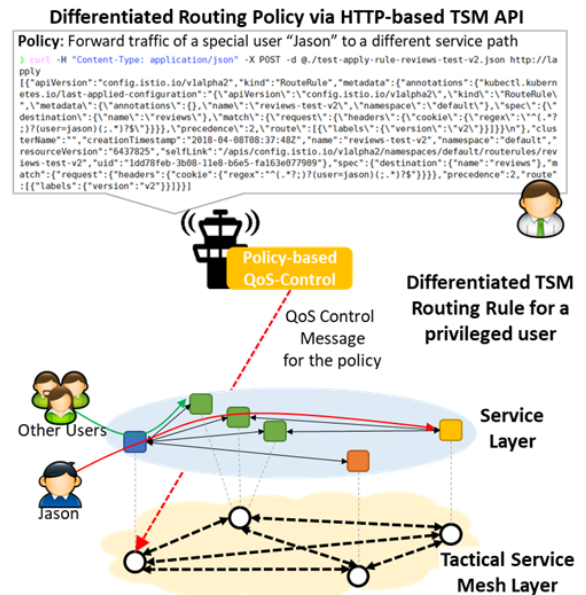


Fig. 11. Verification scenario for differentiated routing/forwarding by TSM

상기 시나리오에 따라 관제타위를 통해 TSM 계층에 “Jason” 사용자의 트래픽에 대한 차별화된 라우팅/포워딩을 적용하였을 경우 Fig. 12와 같은 결과가 반환되는 것을 확인할 수 있다. Fig. 12의 상단에 나타난 것과 같이 일반 사용자가 서비스에 접근하였을 경우 결과를 응답받는다. 하지만 높은 권한을 갖는 “Jason”이 서비스에 접근할 경우, TSM 계층에서 해당 사용자의 트래픽을 특별하게 처리하여 일반 사용자와는 달리 추가 정보를 포함하는 응답결과를 회신함을 확인할 수 있다. 이는 높은 권한을 갖는 “Jason” 사용자의 트래픽을 수신한 1번 서비스(청색)가 해당 권한에 따른 추가 정보를 4번 서비스(황색)으로부터 획득하여 제공

할 수 있도록 다른 서비스 경로로 라우팅하였기 때문이다. 따라서 응용 서비스 트래픽을 중요도에 따라 상이한 방식으로 처리하는 기본적인 QoS 제어를 TSM을 활용하여 용이하게 적용 가능함을 확인할 수 있다.

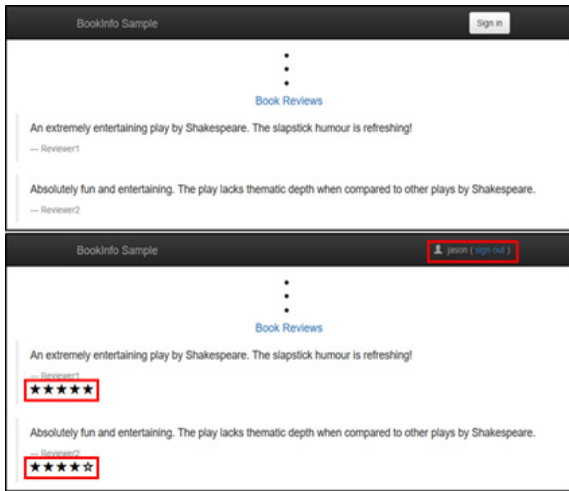


Fig. 12. Differentiated routing/forwarding only for specific “jason” by TSM

## 6. 결론

본 논문은 전송망의 동적인 네트워크의 토폴로지 변화 및 응용 서비스 트래픽 규모와 우선순위 변화 등을 고려하도록 동적인 QoS 모니터링과 제어를 연계하는 지능적인 QoS 조율을 위한 새로운 구조적인 접근 방안을 모색하였다. 즉 전송망 상의 응용 서비스 트래픽에 대한 QoS 조율 방안을 논리적으로 중앙집중화된 관제타워에서 수행하는 QoS 모니터링과 QoS 제어를 대상으로 하는 응용 서비스 데이터 평면에 적용하는 문제로 정의한다. 이를 위한 해결책으로 미래 전송망에 특화된 서비스메쉬인 전송 서비스 메쉬(TSM: Tactical Service Mesh) 계층을 도입하여 모니터링/제어 평면과 가상화를 통해 세분화된 데이터 평면들을 분리시키고 분산배치된 TSM 대응 프록시들을 메쉬 형태로 상호연계하는 방식을 제안한다. 또한 제안한 TSM을 견실하게 구현하기 위한 방향을 제시하면서, QoS 모니터링/제어를 범용 서버 노드와 오픈소스 소프트웨어를 통해 구축한 간략화된 실증환경 상에서 이를 검증함으로써 TSM을 적용한 QoS 조율의 가능

성을 제시하였다. 본 논문의 가능성 검증 단계에서 제시한 TSM의 QoS 모니터링/제어 기능은 제한적이지만, 다양한 QoS 관제 기술을 용이하게 개발할 수 있는 체계적인 기반으로, TSM을 활용한 미래형 전송망 위한 QoS 개선 알고리즘, 관제 도구 등을 향후 연구를 통해 추가적으로 검증하는 것이 필요하다.

## 후 기

본 연구는 국방과학연구소가 지원하는 운용체계의 전송망내 정보유통 품질보증 방안 연구과제(UD170050ED)의 일환으로 수행되었습니다.

## 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] General Dynamics., “WIN-T The Mobile, Expeditionary Soldier’s Network,” WIN-T Program Report, March, 2017.
- [3] V. T. S. Shi, “Evaluating the Performability of Tactical Communications Networks,” IEEE Transactions on Vehicular Technology, Vol. 53, No. 1, pp. 253-260, 2004.
- [4] S. Wang et al., “QoS Management In Disadvantaged Tactical Environments,” In Proc. of Military Communications Conference 2007(MILCOM 2007), 2007. 10.
- [5] P. Marshall, “DARPA Progress Towards Affordable, Dense, and Content Focused Tactical Edge Networks,” In Proc. Military Communications Conference 2008 (MILCOM 2008), 2008. 11.
- [6] O. Cengiz, “Adaptive, Tactical Mesh Networking Control base MANET Model,” M.S. Thesis, Dept. of Info. Sci. Naval Postgraduate School, Monterey, California, 2010. Accessed on Apr. 01, 2019. [Online]. Available: <https://apps.dtic.mil/dtic/tr/fulltext/u2/a531508.pdf>
- [7] A. Kantawala et al., “QoS Architecture for Session

- Oriented GIG Applications,” In Proc. of 2006 IEEE Aerospace Conference, 2006. 3.
- [8] D. Francesco et al., “Migrating Towards Microservice Architectures: An Industrial Survey,” In Proc. of 2018 IEEE International Conference on Software Architecture(ICSA 2018), pp. 29-39, 2018.
- [9] N. Kratzke, “About Microservices, Containers and Their Underestimated Impact on Network Performance,” In Proc. of 6th International Conference on Cloud Computing(CLOUD COMPUTING 2015), 2015.
- [10] M. Klein, “Lyft’s Envoy: Experiences Operating a Large Service Mesh,” Site Reliability Engineering Conference(SRECon) 17 America, 2017. [Online]. Available: [https://www.usenix.org/sites/default/files/conference/protected-files/srecon17americas\\_slides\\_klein.pdf](https://www.usenix.org/sites/default/files/conference/protected-files/srecon17americas_slides_klein.pdf). [Accessed Jan. 03, 2019].
- [11] F. Moyer, “Comprehensive Container Based Service Monitoring with Kubernetes and Istio,” Site Reliability Engineering Conference(SRECon) 18 Asia, 2018. [Online]. Available: [https://www.usenix.org/sites/default/files/conference/protected-files/srecon18asia\\_slides\\_moyer.pdf](https://www.usenix.org/sites/default/files/conference/protected-files/srecon18asia_slides_moyer.pdf). [Accessed Jan. 03, 2019].
- [12] H. Zhang et al., “Network Slicing based 5G and Future Mobile Networks: Mobility, Resource Management, and Challenges,” IEEE Communications Magazine, Vol. 55, No. 8, pp. 138-145, 2017.
- [13] AT&T, “Towards an Open, Disaggregated Network Operating System,” Linux Foundation Project DANOS, 2017.
- [14] S. Dharmapurikar, P. Krishnamurthy, T. Sproull, and J. Lockwood, “Deep Packet Inspection using Parallel Bloom Filters,” In Proc. of 11th Symposium on High Performance Interconnects(HOTI ’03), pp. 44-51, 2003.
- [15] R. T. El-Maghraby, N. M. A. Elazim, and A. M. Bahaa-Eldin, “A Survey on Deep Packet Inspection,” In Proc. of 12th International Conference on Computer Engineering and Systems(ICCES 2017), pp. 188-197, 2017.
- [16] M. S. Mushtaq et al., “Empirical Study based on Machine Learning Approach to Assess the QoS/QoE Correlation,” Networks and Optical Communications (NOC), 17th European Conference, pp. 1-7, 2012.