

표지

(옆면)

(앞면)

과제 번호	보안 과제(), 일반 과제(√) / 공개(), 비공개()발간등록번호() 국토교통기술사업화지원사업 제3차 연도 최종 보고서
	R&D / 17TBIP-C125224-01
1 7 T B I P - C 1 2 5 2 2 4 - 0 1	SDN 기반 도로통신 네트워크 시스템 개발 최종보고서
최 종 보 고 서	2020. 1. 22.
2019	주관연구기관 / 아토리서치(주) 공동연구기관 / 한국도로공사 위탁연구기관 / 한국과학기술원
국 토 교 통 과 학 진 흥 원	국토교통부 (전문기관) 국토교통과학기술원

아
토
리
서
치

제출문

제 출 문

국토교통과학기술진흥원장 귀하

‘SDN 기반 도로통신 네트워크 시스템 개발’(연구개발 기간 : 2017. 04. ~ 2019. 12.) 과제의 최종보고서 000부를 제출합니다.

2020 . 01. 22.

주관연구기관명 : 아토리서치(주) (대표자) 정재웅(인)
공동연구기관명 : 한국도로공사 (대표자) 이강래(인)
위탁연구기관명 : 한국과학기술원 (대표자) 신성철(인)

주관연구기관책임자: 송용주
공동연구기관책임자: 김성국
위탁연구기관책임자: 신승원

국토교통부소관 연구개발사업 운영규정 제29조에 따라 최종보고서 열람에
동의합니다.

제출문

제 출 문

국토교통과학기술진흥원장 귀하

‘SDN 기반 도로통신 네트워크 시스템 개발’(연구개발 기간 : 2017. 04. ~ 2019. 12.) 과제의 최종보고서 부를 제출합니다.

2020 . 01. 22.

주관연구기관명 : 아토리서치(주) (대표자) 정채동(인)

공동연구기관명 : 한국도로공사 (대표자) 진규동(인)

위탁연구기관명 : 한국과학기술원 (대표자) 신성철(인)

주관연구기관책임자: 송용주

공동연구기관책임자: 김성국

위탁연구기관책임자: 신승원

국토교통부소관 연구개발사업 운영규정 제29조에 따라 최종보고서 열람에 동의합니다.

제출문

제 출 문

국토교통과학기술진흥원장 귀하

‘SDN 기반 도로통신 네트워크 시스템 개발’(연구개발 기간 : 2017. 04. ~ 2019. 12.) 과제의 최종보고서 1부를 제출합니다.

2020 . 03. 25.

주관연구기관명 : 아토리서치(주) (대표자) 정재웅(인)
공동연구기관명 : 한국도로공사 (대표자) 이강래(인)
위탁연구기관명 : 한국과학기술원 (대표자) 신성철(인)



주관연구기관책임자: 송용주
공동연구기관책임자: 김성국
위탁연구기관책임자: 신승원

국토교통부소관 연구개발사업 운영규정 제29조에 따라 최종보고서 열람에 동의합니다.

보고서 요약서

보고서 요약서

과제 고유 번호	17TBIP-C125224-01	해당 단계 연구 기간	12개월	단계구분	(3단계) / (3단계)
연구사업명	중사업명				
	세부사업명	국토교통기술사업화지원사업			
연구과제명	대과제명				
	세부과제명	SDN 기반 도로통신 네트워크 시스템 개발			
연구책임자	송 용 주	해당단계 참여연구원 수	총: 17명 내부: 17명 외부: 명	해당단계 연구비	정부:405,000천원 민간:405,000천원 정부외: 천원 상대국: 천원 계:810,000천원
		총 연구기간 참여연구원 수	총: 44명 내부: 44명 외부: 명	총 연구비	정부:1,268,000천원 민간:1,268,000천원 정부외: 천원 상대국: 천원 계:2,536,000천원
연구기관명 및 소속 부서명				아토리서치(주)	
국제공동연구	상대국명:			상대국 연구기관명:	
위탁연구	연구기관명: 한국과학기술원			연구책임자: 신승원	
※ 국내·외의 기술개발 현황은 연구개발계획서에 기재한 내용으로 같음					
연구개발성과의 보안등급 및 사유	일반				

9대 성과 등록·기탁번호

구분	논문	특허	보고서 원문	연구시설 ·장비	기술요 약 정보	소프트 웨어	화합 물	생명자원		신품종	
								생명 정보	생물 자원	정보	실물
등록· 기탁 번호		10-2017-0117103, 10-2018-0038069, 10-2018-0106280, 10-2018-0135037, 10-2019-0122865 / 10-1931139, 10-2023901				C-2018-027848, C-2018-027847, C-2019-026625, C-2019-026626					

국가과학기술종합정보시스템에 등록된 연구시설·장비 현황

구입기관	연구시설 ·장비명	규격 (모델명)	수량	구입연월일	구입가격 (천원)	구입처 (전화)	비고 (설치장소)	NTIS 등록번호

요약	보고서 면수
- 도로통신 네트워크 SDN 테스트베드를 경부/영동/여주 고속도로에 구축 및 실증 운영 - SDN기반 도로통신 네트워크 SW를 개발 및 실증 후 조달 우수제품 등록으로 상용화 완료 - 도로통신 네트워크 보안 기법을 연구하여 13개 공격 벡터도출 및 5개 방어전략 시험 - 도로통신 네트워크 통합 관제 SW로 자율협력주행 시스템 관리 효율화	

요약문

연구의 목적 및 내용	본 연구의 목적은 SDN기반 도로통신 네트워크 시스템을 개발하는데 있고, 그 연구 내용은 아래와 같다. - SDN기반 도로통신 네트워크 구축 - 도로통신 네트워크 분석 - SDN기반 네트워크 구축 - SDN기반 도로통신 네트워크 트래픽 최적화 SW 개발 - 서비스 별 접근 제어 - 대역폭 할당 - 우선순위 지정 - 도로통신 네트워크 보안 기술 연구 - 도로통신 네트워크 특화 공격 분석 - 도로통신 네트워크 특화 방어 시스템 구현 - 도로통신 네트워크 통합 관제 SW 개발 - 도로통신 네트워크 중앙 관제 - 장애 감시 및 응급 대응 시스템 - 장애 예측 시스템				
연구개발성과	- 도로통신 네트워크 SDN 테스트베드 - SDN기반 도로통신 네트워크 트래픽 최적화 SW - 도로통신 네트워크 보안 기법 - 도로통신 네트워크 통합 관제 SW				
연구개발성과의 활용계획 (기대효과)	(활용계획) - 고속도로를 중심으로 하는 도로교통 네트워크 시스템 신규 구축 사업 우선 적용 - 스마트 시티를 중심으로 실증 단지 조성 - 국내도로 실적을 발판으로 미국/유럽/일본 등 해외 ITS 사업 진출 (기대효과) - 도로운영자 ITS 인프라 운영비용 절감 - 도로교통 분야 교통정보 품질 향상 및 차세대 ITS 활성화에 기여 - 사물인터넷(IoT) 기술을 활용한 스마트 시티 시장 지배력 강화				
국문핵심어 (5개 이내)	SDN	NFV	네트워크 보안	장애 대응	지능형 교통체계
영문핵심어 (5개 이내)	SDN	NFV	Network Security	Failure management	ITS

< 목 차 >

1. 연구개발과제의 개요	1
2. 연구수행내용 및 성과	9
3. 목표 달성도 및 관련 분야 기여도	60
4. 연구개발성과의 활용 계획 등	66
붙임. 참고 문헌	78

<별첨> 주관연구기관의 자체평가 의견서

1. 연구개발과제의 개요

가. 연구개발 목적 및 필요성

(1) 연구 개발의 배경 및 필요성

C-ITS, 자율협력 주행 등 4차 산업 혁명 기술의 등장으로 도로에서 네트워크는 필수 인프라가 되었으나, 현재의 도로통신 네트워크 시스템은 자율협력주행의 확산에 대비되어 있지 않으며 아래와 같은 문제점들이 있다.

- 자율 주행 차량, 단말, IoT 장치의 폭발적 증가에 대비되어 있지 않음
- 비디오, 오디오, 주행 정보 등 자료의 폭발적 증가에 대비되어 있음
- 도로통신 환경에 대한 네트워크 보안이 대비되어 있지 않음
- 따라서 이를 해결하기 위한 기술들을 사업화하여 도로통신 네트워크를 안전하고 효율적으로 운영하고자 하는데 연구의 목적이 있다.

(2) 연구의 목표

(가) 최종 목표

도로통신 네트워크를 소프트웨어 기반 제어를 통해 안전하고 효율적으로 운영할 수 있는 시스템을 구축하는 것이며, 다음의 사항에 중점을 둠

- 트래픽을 구분 처리하여 중요한 트래픽의 안정성 확보
- 위험한 단말 감지 및 빠른 차단으로 보안성 확보
- 중앙 통합 관리 및 긴급 장애 대응으로 운영 편의성 확보

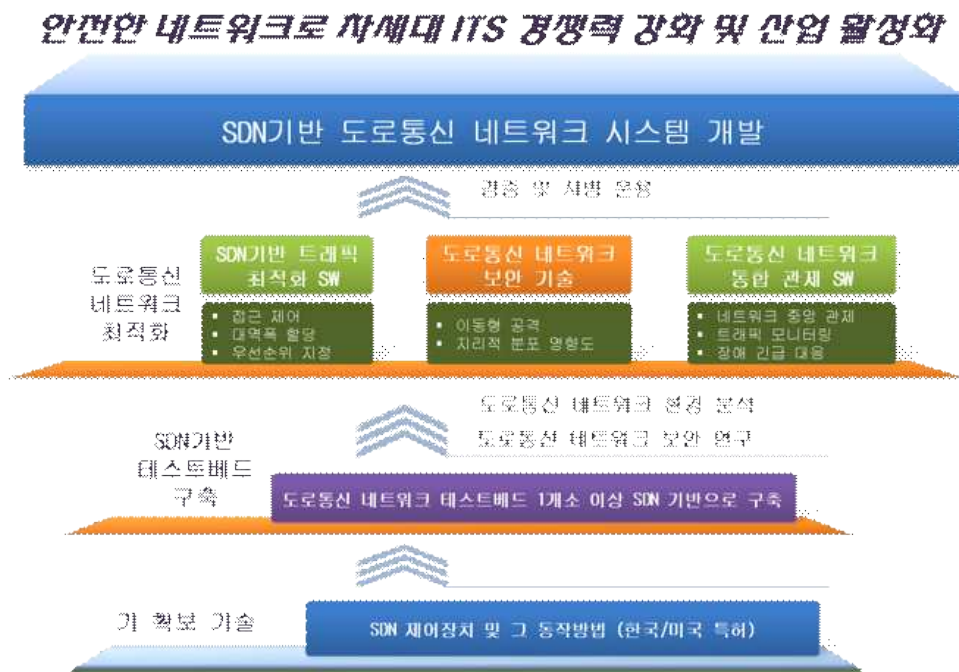


그림 1 최종 목표

(나) 기술의 장점

① 기존 기술 대비 차별성

구분	SDN기반 도로통신 네트워크 시스템	기존 도로 네트워크 시스템
■ 기능/성능	• 비인가 장비 접근 제어 • 서비스 별 대역폭 할당 • 이동형 네트워크 공격 대비 • 전국 네트워크 중앙 관제 • 장애 긴급 대응	• 네트워크 수준 접근 제어 없음 • 서비스 별 구분 없음 • 일반 방화벽 의존 • 서비스 수준 모니터링 • 장애 시 현장 출동
■ 장/단점	• 네트워크 중앙 제어 • 네트워크 보안 향상 • SDN 기반 스위치로 장비 교체 필요	• 별도의 보안 장비 필요 • 운영 및 장애 대응 인력 다수 필요
■ 경제성	• 공사비, 공사 기간 등 설치비용은 동일 • 이후 유지 관리비 절감 가능	

② 기술 경쟁력

소프트웨어를 기반으로 네트워크를 제어하는 기술은 일반적으로 데이터센터와 통신사를 중심으로 적용되고 있으며, 도로 네트워크 분야에서 실제 적용된 사례는 서일본 고속도로가 유일하고 독일 등 유럽에서도 이제 적용하려는 단계이다. 본 기술을 적용하면 C-ITS, 자율협력주행 시스템의 빠른 상용화가 가능해 진다.

③ 경제적 효과

기존 도로 네트워크 시스템에 비해 중앙에서 다수의 단말 및 인프라 관리가 가능해 지며, 운영 편의성의 향상으로 한 명이 다수의 인프라 관리를 할 수 있고, 장애 복구 시간이 단축되어 운영비용 절감의 효과가 있다.

나. 연구개발의 범위

(1) 연구 대상 기술의 정의

(가) SDN(Software Defined Networking)

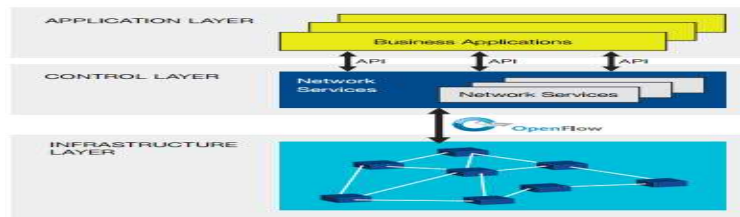


그림 2 SDN의 개념과 구조

*미래창조과학부, 보도자료(2015.5.21), ONF, OpenFlow-enabled SDN and Network Functions Virtualization(2014.2.17)

소프트웨어 정의 네트워킹은 네트워크 인프라를 소프트웨어 프로그래밍을 다루듯 중앙에서 제어하는 기술. 스위치나 미들박스 네트워크 장비의 제어부분을 데이터 전송부분과 분리하여 중앙으로 집중시키고 개방형 인터페이스 API를 통해 프로그램화된 소프트웨어로 다양한 네트워크 경로를 설정하거나 제어할 수 있는 기술. 시스코에서 발표한 인터넷 추이에 따르면 2012년부터 연평균 20%씩 증가하여 2017년에는 2014년의 2배인 월 120,643PB에 달할 것으로 전망되는 상황에서, 이러한 트래픽 처리를 위해 끊임없이 네트워크에 투자하고 있으나 구조적 특징으로 현재 네트워크는 매우 복잡하고 유연하지 못한 문제점이 발생하고 있음

○ 국내 SDN 시장 연평균 56.6% 성장 전망

- 데이터 센터의 효율적인 운영을 위해 SDN 도입이 증가하면서 향후 5년간 연평균 56.6% 성장하여 2019년에는 1,390억 규모전망
- 디바이스의 수 증가 및 데이터 처리량 급증으로 인한 데이터센터 CAPEX 및 OPEX 절감을 위한 SDN과 NFV 도입이 늘어날 전망

○ 클라우드 데이터센터(SDDC)를 중심으로 빠르게 확산 중

- 정부의 공공 클라우드 활성화 정책에 의해 공공기관/지자체를 중심으로 클라우드 데이터센터를 다수 구축하면서 SDN/NFV의 실제 도입도 급격히 늘고 있음

- 인천 U-city는 송도 지구 데이터센터에 SDN/NFV를 도입하여 100억 원의 도입비용 절감
- 제주 신화월드, 코스콤, 하나금융 등 공공과 금융권을 중심으로 SDN/NFV를 실제로 도입하는 사례가 늘고 있음

(나) NFV(Network Function Virtualization)은 주로 미들박스과 같은 네트워크 서비스 기능들을 하드웨어 전용장비로부터 고성능 범용 서버 등으로 분리시켜 소프트웨어적으로 유연하게 제어와 관리가 가능하도록 가상화 시키는 기술. NFV는 사실상 새로운 기술이 아니라 계속 연구되어 오던 네트워크 가상화의 현실화된 버전. 표준화하기 위해 유럽 표준화 기구인 ETSI에서 통신 사업자 중심으로 2012년 말, NFV ISG(Industry Specification Group)를 구성해 표준 개발.

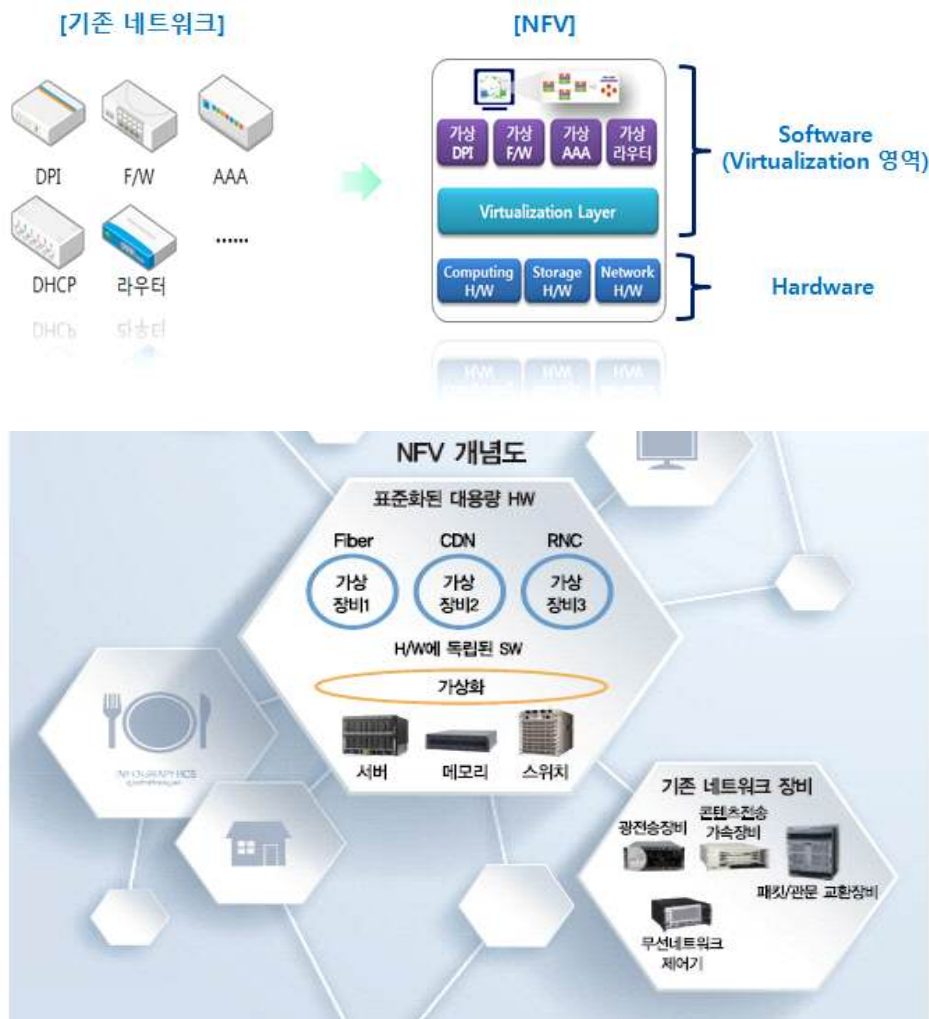


그림 3 NFV 개념

*자료 : 미래창조과학부, 보도자료(2015.5.21), 디지털타임스(2015.2)

- (다) SDN과 NFV 모두 캐리어 규모에서의 동적 클라우드 환경에 최적화 된 기술로, OPEX(운영비용)와 CAPEX(투자비용)를 절감하면서 더 빠르고 효율적인 운영을 위해 자동화와 가상화를 추구함

그러나 NFV는 방화벽, DNS, 로드 밸런스와 같은 네트워크 기능의 구축을 최적화하는 기술이며 SDN은 기본적인 네트워크 최적화에 초점이 맞춰짐

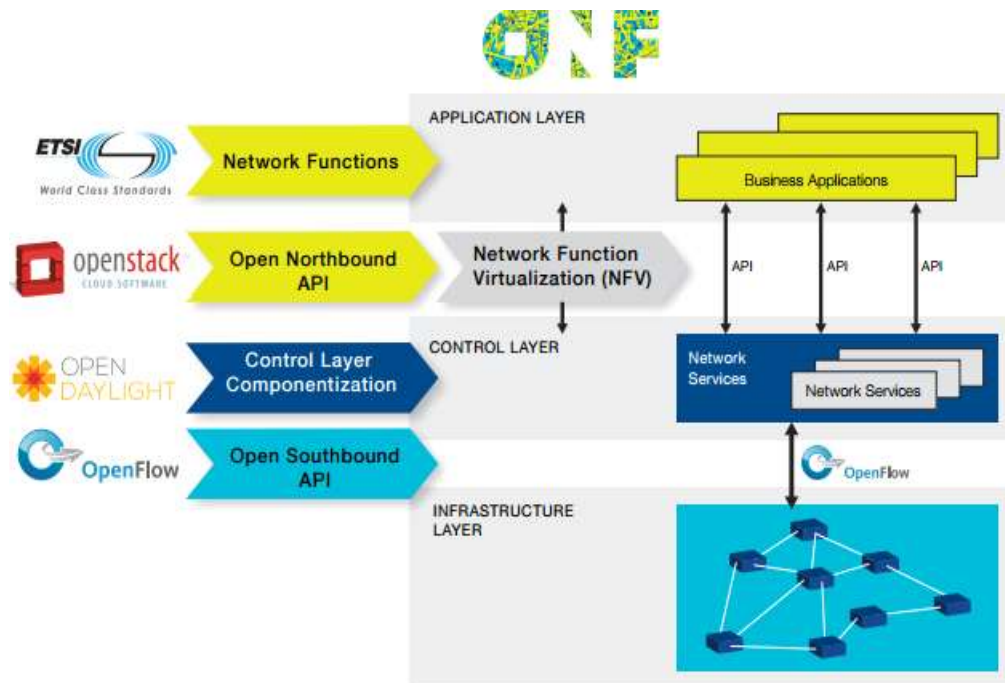


그림 4 SDN과 NFV의 관계

자료 : ONF, OpenFlow-enabled SDN and Network Functions Virtualization (2014.2.17)

(2) 추가 연구개발 필요성

(가) 서비스 측면의 필요성

① SDN 기술은 성숙기, 서비스는 아직

- 2007년부터 시작된 SDN 열풍은 네트워크 패러다임의 일대 변혁을 가져옴
- Nicira, Big switch를 시작으로 수많은 SDN 벤처기업이 미국을 중심으로 발전
- 데이터 센터 위주의 SDN 적용도 활발하게 진행
- 그러나 SDN을 위한 킬러 서비스는 없는 상태
- 보수적인 국내 네트워크 시장의 경우는 더욱 심각
- SDN 기술의 필요성은 모두 공감하나 실제 도입된 사례는 적음
- 당 사 보유 기술은 SDN 제어기의 안정성에 관한 원천기술로서 큰 의미를 가지지만 이를 이용한 킬러 서비스는 아직 개발되지 않은 상태
- 특히 ITS로 대표되는 도로통신 네트워크는 SDN을 적용하기 좋은 구조를 가지고 있으므로, SDN을 적용한 다양한 서비스를 개발한다면 SDN기술의 사업화에 중요한 신시장이

될 수 있음

②도로 교통 네트워크와 SDN

- 현재의 도로 교통 네트워크는 연결성을 제공하는 것에 그침
- 자율 주행 차량, 차량 단말, IoT 장치 등 향후에는 네트워크를 이용하는 장치가 폭발적으로 증가할 것으로 예상됨
- 도로 교통 네트워크를 이용하는 서비스도 현재는 Broadcast 밖에는 없으나 향후에는 비디오/오디오 스트림, 정보성 방송, 메시지, 사진, 웹페이지 등 다양한 정보가 다양한 프로토콜을 이용해서 통신할 것으로 예상됨
- 특히, 도로 교통 네트워크는 지리적으로 길게 퍼져있다는 점, 단말이 고속으로 이동하면서 통신한다는 점, 일부 통신은 사람의 생명이 연관될 정도로 매우 중요하다는 점에서 일반적인 데이터센터 네트워크와 크게 차이를 보임
- SDN은 동적이고 다양한 트래픽이 지나가는 네트워크에 최적화된 기술이므로 도로 교통 네트워크에 최적이라고 할 수 있음
- 다만, 지금까지의 SDN은 데이터 센터를 중심으로 발전되어 왔기 때문에 도로 교통 네트워크에 맞는 SDN서비스가 전무한 상태
- 따라서 도로 교통 네트워크를 위한 SDN서비스를 개발할 필요가 있음

(나) 보안 측면의 필요성

① 아무리 강조해도 지나치지 않은 네트워크 보안

- 네트워크 공격의 대표적인 사례인 DDoS 공격은 일부 해커의 장난 수준을 넘어서 경쟁 쇼핑몰 방해와 같은 명확한 목적으로 수없이 발생하고 있음
- 보안이라는 측면에서 강조되는 서버 보안과 달리 네트워크 보안은 상대적으로 사각지대에 있음

② 도로 네트워크에서의 보안

- 기업이나 불특정 다수를 주요 대상으로 하는 네트워크 공격뿐만 아니라 도로 네트워크와 같은 공공 인프라에 대한 공격은 사이버 테러로 규정할 수 있을 만큼 파급효과가 큼
- 도로 네트워크에서의 주요 통신은 아래와 같이 V2V(Vehicle-to-Vehicle), V2I(Vehicle-to-Infrastructure) 두 가지 방식이 있음

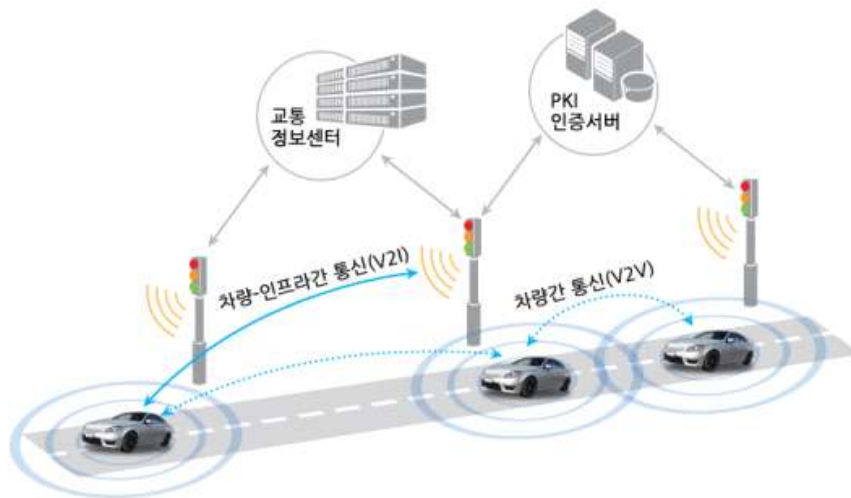


그림 5 차량-인프라 간 통신(V2I)와 차량 간 통신(V2V)
(<http://news.join.com/article/14223283>)

- 위의 통신에서는 차량 간의 간격 유지를 위해 차량 속도를 교환하거나 차량에서 관찰한 도로 상황 등을 중앙 시스템에 전달 등이 이루어짐
- 새로운 아키텍처인 C-ITS에서는 기존 네트워크에서 발생할 수 있는 공격들뿐만 아니라 ITS 아키텍처나 CAN frame replay와 같은 네트워크가 내장된 무인자동차에 한정된 공격들도 발생할 가능성도 충분함
- 기존 네트워크 공격에는 대표적으로 인프라의 서비스를 이용하기 어렵게 하는 flooding, black hole 등과 같은 DDoS공격에서부터 메시지 변조를 통한 왜곡된 데이터를 전달하는 공격 등이 존재함
- C-ITS에 한정된 공격으로는 차량에 탄 개인의 위치를 추적하는 공격에서부터 차량의 센서 스푸핑을 통해 차량 간 통신 프로토콜을 준수하는 잘못된 데이터를 보내는 공격 등이 존재함
- 이러한 철도, 도로 네트워크와 같이 생명과 직결되는 인프라에 대한 공격은 서비스 중단이 곧 인명과 연결되므로 장애 범위와 대응 시간 감소가 큰 이슈가 됨
- 차량-인프라 간 통신에는 기존에 발생할 수 있는 다양한 네트워크 공격이
- 차량들 간의 통신은 주로 인프라의 개입 없이 애드혹 방식을 이용함
- 일반적인 컴퓨터 네트워크에서 사용되는 애드혹 방식과 달리 도로 네트워크 환경에서는 짧은 시간 안에 수십 대의 차량들이 통신하게 되므로 네트워크로 전달되는 패킷이 공격자에 의해 무결성이 깨질 경우, 잘못된 정보가 순식간에 퍼질 수 있음

③ 네트워크 보안에서 SDN의 중요성

- 네트워크 보안의 트렌드는 기존의 Known attack 방어에서 Unknown attack 방어로 무게 중심이 옮겨가고 있음
- 공격이 확인되면 공격 방법을 분석한 후에 IDS/IPS와 같은 방어 시스템에 signature를

등록해서 이후의 공격을 막는 것이 전통적인 네트워크 보안에 해당

- 최신 네트워크 공격은 기존 공격기법을 포함한 다양한 시도를 공격 대상 네트워크에 시험해보고, 미처 방어가 안 된 방법을 찾아서 공격하는 방식이기 때문에, 기존 보안 장비로는 감지 및 대응이 쉽지 않음
- SDN 기술은 네트워크를 소프트웨어로 제어한다는 개념으로, 보안과 직접적인 연결이 있는 기술은 아니지만, Unknown 공격을 막는 다는 차세대 보안 방식을 구현하기에 최적화된 기술이기 때문에 주목 받고 있음
- SDN 기술을 활용하면 한 곳에서 발견된 공격을 네트워크 전반에 바로 적용할 수 있는 '면역'시스템이나, 네트워크 전체 트래픽을 분석해서 submarine attack을 잡아내는 방법 등 차세대 보안 방식을 쉽게 구현 가능
- 예를 들어, 감염된 차량 인터페이스를 통해서 도로 교통 인프라에 DDoS공격을 시도하고자 할 때, 특정 인프라로 가는 것을 쉽게 탐지하고 분산시키는 것이 가능

④ 도로 교통 네트워크 보안과 SDN

- 현재 도로 교통 네트워크를 이용하는 서비스는 교통정보 수집 정도의 간단한 서비스 뿐
- 약 1km간격으로 차로별 교통량, 지점속도 등의 정보를 상호 교환하는 것이 주요 기능
- 도로 교통 네트워크는 단말이 빠른 속도로 이동하기 때문에 고정된 곳에서 통신하는 시간이 수초에 그침. 위치가 고정된 곳에서 공격을 분석하는 기존의 네트워크 보안 장비로는 공격 패턴을 감지하기 어려움
- 도로 교통 네트워크를 이용하는 서비스도 기존의 웹/모바일 트래픽뿐만 아니라 교통 정보, CCTV 등 다양한 서비스가 섞여 있기 때문에 새로운 보안 방안이 필요
- SDN의 네트워크 보안 방식이 key point가 될 수 있음

2. 연구수행내용 및 성과

가. 연구수행내용

구분(연도)	세부 과제명	세부 연구 목표	연구개발 수행 내용
1차 연도 (2017)	■ 도로통신 N/W 테스트베드에 SDN 적용 - ITS 네트워크 분석 - SDN 적용 구조 설계 및 구축 - SDN 개별 요소 기능 검증 ■ 도로통신 네트워크 보안 연구	■ 도로통신 네트워크 환경 분석	- ITS(Intelligent Transport Systems) 네트워크 분석
		■ SDN 기반 도로통신 N/W 시스템 구축	- SDN 기반 테스트 베드 구축
		■ SDN 개별 요소 검증	- SDN 망 테스트 실시
		■ 도로통신 네트워크 보안 연구	- 도로통신 네트워크 공격 분석
2차 연도 (2018)	■ SDN 이용 도로통신 N/W 안전성 확보 - 도로통신 네트워크 트래픽 최적화 - 도로통신 네트워크 보안 방어 개발 - 중앙 관제 시스템 개발	■ 도로통신 네트워크 트래픽 최적화	- 네트워크를 이용하는 서비스 종류 분류 - 서비스별 우선순위 할당 - 우선순위에 따른 대역폭 제한 설계 - 특정 조건에 맞는 트래픽 차단 기능 추가 - 트래픽 최적화 시스템을 SDN 서비스의 형태로 구현
		■ 도로통신 네트워크 보안 방어 개발	- 도출된 공격에 대한 방어 방안 개발 - SDN기반 탐지 및 방어 기술 개발 - 보안 박스의 기존 보안 기능을 업그레이드, 또는 새로운 보안 기능을 추가 - 모의 공격 및 방어를 통한 기술 검증
		■ 중앙 관제 시스템 개발	- 도로통신 네트워크를 관제할 수 있는 UI/UX 개발 - 도로통신 네트워크 정보 수집 시스템 개발 - 도로통신 네트워크 장애 대응 시스템 개발
		■ 통합 연동 테스트	- 개별 기능 개발 후, 전체 시스템을 이용한 통합 테스트 - 중앙 관제 시스템에서 트래픽 최적화 설정 테스트 - 중앙 관제 시스템에서 네트워크 보안 공격 상황 모니터링 테스트 - 중앙 관제 시스템에서 장애 대응 테스트
3차 연도 (2019)	■ SDN 기반 도로통신 네트워크 실증 - 테스트베드에서의 기능/성능 검증 - 시범운용	■ 테스트베드에서의 검증	- 단말, 스위치, 회선, 센터 장비 장애 테스트 - 서비스 장애 유발 공격에 대한 방어 테스트 - 과부하 트래픽 발생 테스트 - 다양한 종류의 서비스 동시 발

			생 테스트 - 차량 에뮬레이션을 통한 시나리오 테스트
		■ 시범 운용	- 테스트베드에서 V2X 단말기 탑재 차량 운용으로 안정성 테스트 - 외부 전문가 시연 및 평가서
		■ 공인기관 시험검증	- ETRI 시험 인증 - GS 인증 - 조달청 우수제품 등록
		■ 신기술 인증	- 특허 출원 및 등록 2건 - SW 저작권 등록 2건

나. 연구 성과

(1) 1차년도(2017)

(가) 도로통신 네트워크 환경 분석 - 결과물: ITS 네트워크 분석 보고서

- 자율주행자동차가 도로 인프라와 협력하여 안정하고 효율적인 자율주행이 가능하도록 지원하는 도로시스템 기술 개발
- 이에 필요한 ITS(Intelligent Transport Systems) 네트워크를 위한 기존의 자율협력주행 테스트베드를 분석
- 기존 자율협력주행 테스트베드를 구성하는 장비 조사

① 테스트베드 네트워크 장비분석

㉠ 시험도로센터

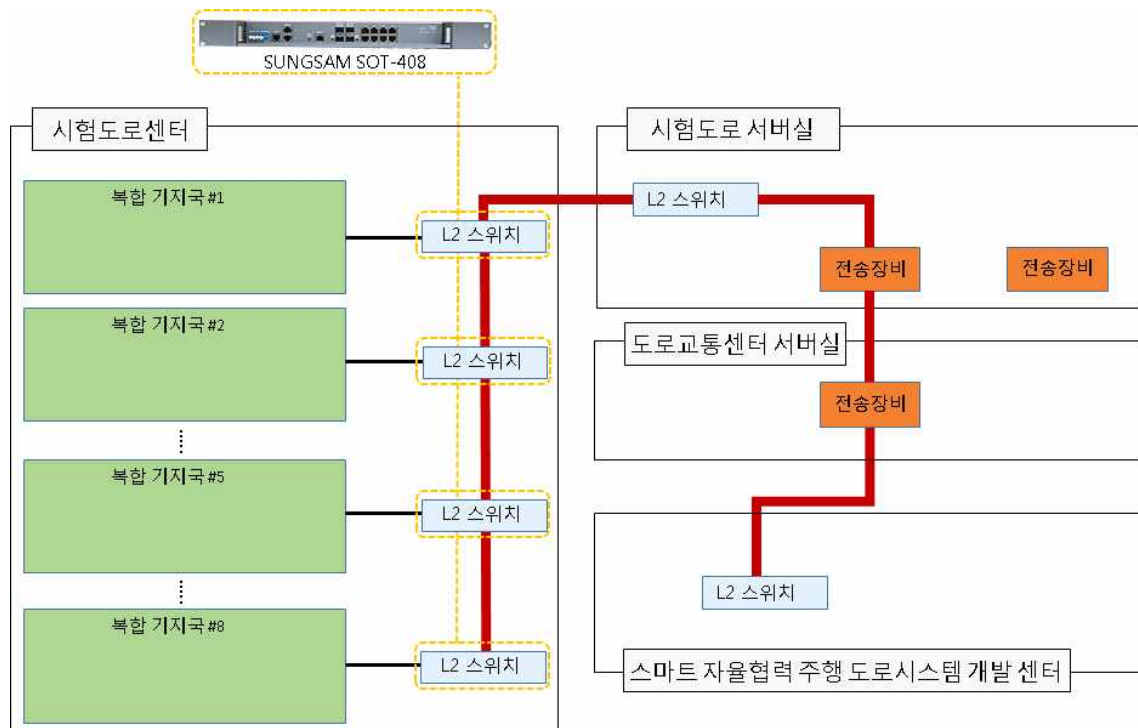


그림 6 시험도로센터 네트워크

- L2 스위치 SUNGSAM SOT-408

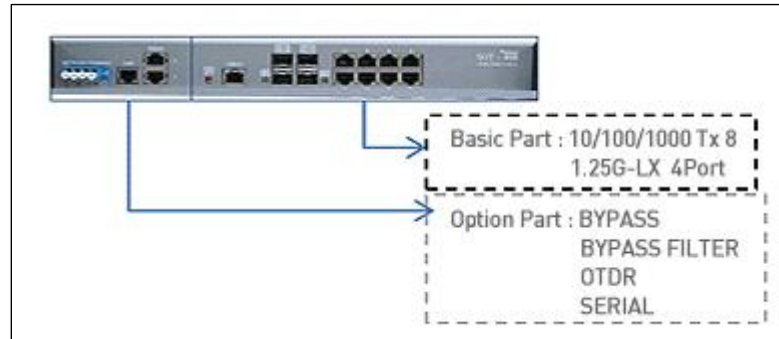


그림 7 SOT-408

주요 특징

- SOT-408 단독형 19" 1U Rack mount type
- 10/100/1000BASE TX Ethernet 신호 8 Ports 수용
- 100Base FX 또는 1000Base Sx/Lx/Zx 4 Ports 수용
- ITU-T G.8032 지원(Recovery time 50ms 이내)
- 네트워크 증설용이, Ring 형태 광 네트워크 이중화 연결지원(0.5초 이내 절체)
- LED를 통한 장비 이상 유무 및 현재 운용 상태 실시간 감시
- Ring 당 최대 250 접속 노드 지원
- 완전 그래픽 지원 가능한 사용자 편의의 EMS 지원
- 서지(Surge) 전압에 대비한 보호기능
- 과전압 및 과전류 보호기능
- 망 구성 시 사용자의 환경에 따라 다양한 망 구성 가능(Point-to-point, Linear, Ring)
- 전원차단 시 광 Bypass 기능 지원(전환시간 20ms 이내)

항 목			Specification
Network 구성			Point-to-point, Linear, Star, Ring
INTERFACE	광	방식	1.25G-LX
		PORT수	EAST / WEST 2 PORT, UPLINK 2PORT
		파장	1310 / 1550 Single Mode, 1 Core [WDM]
		전송거리	15km[default],40km[Optional],80km[Optional]
		커넥터	SC/ST/LC/FC-PC/APC(구매 시 지정)
	LAN		10/100/1000BASE TX 8 ports 10/100/1000M Auto
전원부	AC 입력		110/220V Free[50/60Hz]/이중화(구매 시 지정)
	최대소모전력		25W[RT]/200W[COT]
	DC 입력		DC12V(구매시 지정)
환경조건	Operating Temp.		-20 ℃ ~ 70 ℃
	Operating Humidity		5 ~ 90% relative humidity
크기	단독형(RT)		44[H]x350[W]x150[D]mm[Stand Alone TYPE]
	집합형(COT)		220[H]x480[W]x310[D]mm
EMS			EMS[LAN 기반 Platform]지원(구매 시 지정)
EMI/EMS			KCC 인증
OPTION			BYPASS : SOT-408-BP BYPASS Filter : SOT-408-BPF OTDR : SOT-408-OTDR Serial : SOT-408-SERIAL
OPTION			BYPASS : SOT-408-BP BYPASS Filter : SOT-408-BPF OTDR : SOT-408-OTDR Serial : SOT-408-SERIAL

표 1 SOT-408 시스템 사양

㉠ 시험도로 서버실

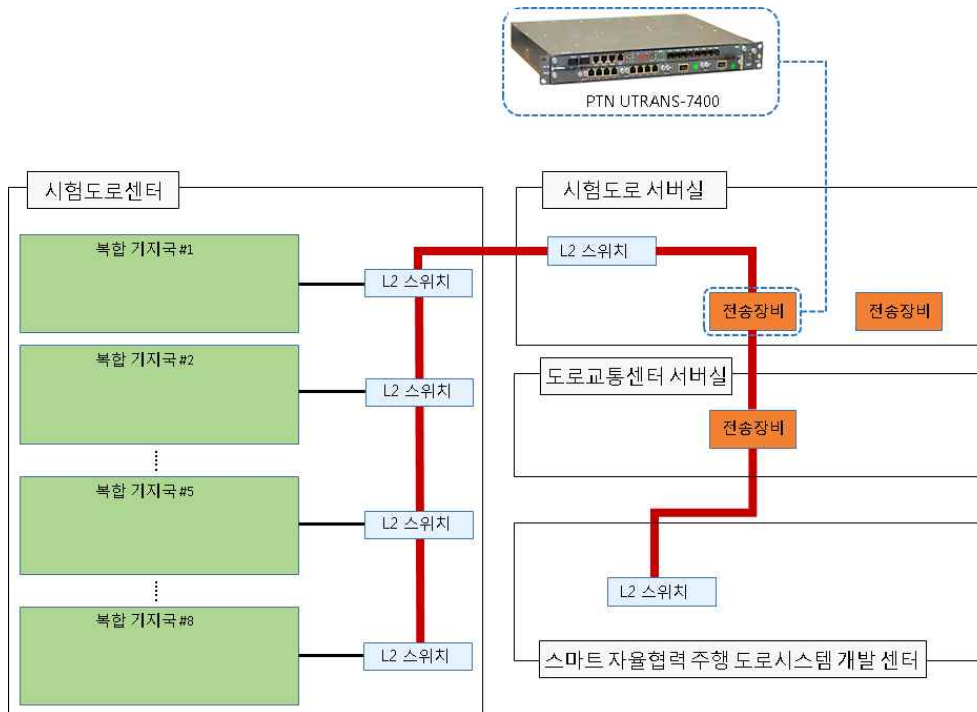


그림 8 시험도로 서버실 전송장비 - Coweaver UTRANS-7400(PTN)

- 전송장비 Coweaver UTRANS-7400(PTN)



그림 9 Coweaver UTRANS-7400(PTN)

주요 특징

- MPLS-TP가 탑재된 48G급(양방향) 장비
- 패킷 기반(Ethernet, IP) 서비스와 회선 기반(PDH) 서비스를 수용하는 가입자(Access) 망 구성에 효과적으로 대응할 수 있는 소 용량 급 PTN 장비
- 가입자망에 대한 투자비(CAPEX) 및 운용비용(OPEX) 절감에 효과적인 장비
- 가입자 인터페이스(UNI) / 네트워크 인터페이스(NNI) 구분 없이 포트/선로/유니트 이중화 기능을 제공하여 써킷 수준의 신뢰성 높은 절체 기능을 제공
- 모든 유니트는 탈/실장 구조로 설계되어 있고, 원격 초기화 기능 제공으로 장애 시 긴

급 복구가 가능

- 연결 지향성(Connection-oriented) 기반의 MPLS-TP 기술을 적용으로 캐리어 전달 망에서 요구되는 회선관리(OAM), 50msec이내의 절체(Protection), 세분화된 다단계 대역 관리(H-QoS)등의 기능이 제공
- PtP, Mesh, Ring, Linear등의 다양한 망구성(Topology)을 통해 E-LINE, E-LAN, E-TREE 서비스가 가능
- NetMgr(NMS/EMS)를 통한 종단 간(End-to-End) 회선 구성/삭제 및 관리가 가능
- 성능, 경보, 운용 설정, 회선 구성 및 대역정보 관리가 용이한 운영자 친화적인 장비

ITEM			DESCRIPTION
Chassis			19" x 1RU x 310mm (W x H x D)
Redundancy			Packet Line Card, Power, FAN
System	망 구성	Network	Linear, Ring, Mesh
		Access	Packet: Linear, Ring, Mesh
	NNI		10GE, GE
	UNI		10GE, GE, FE, E1(CES)
	Switching Capacity		48G FD
System Clock	Clock 인터페이스		External E1 Clock Sync-E Clock Internal OSC Clock (4.6ppm or 16ppb) Holdover (24h or 72h)
	External Synchronou s Port		Framed E1 (2,048 Kbps) 2 Ports Wrapping Terminal
System Mgmt.	Node Management		1K Nodes per Server 32 clients 동시접속
	EMS		Server, Client, CIT
	인터페이스		RS-232c, Ethernet
	NMS		TL-1, SNMPv2, REST-NETCONF(future)
전원조건	입력전원		DC -48V (-43.5V ~ -56.5V) AC 110V/220V
	절연저항		100M Ω 이상(DC 500V기준)
보호절체	Ethernet(FE, 1GbE, 10GbE)		None, Inter-/Intra-LAG
환경조건	동작조건(온 습도)		온도: 2°C ~ 50°C, 습도: 20% ~ 80%
	보관조건(온 습도)		온도: -30°C ~ 70°C, 습도: 0% ~ 90%

표 2 Coweaver UTRANS-7400(PTN) 시스템 사양

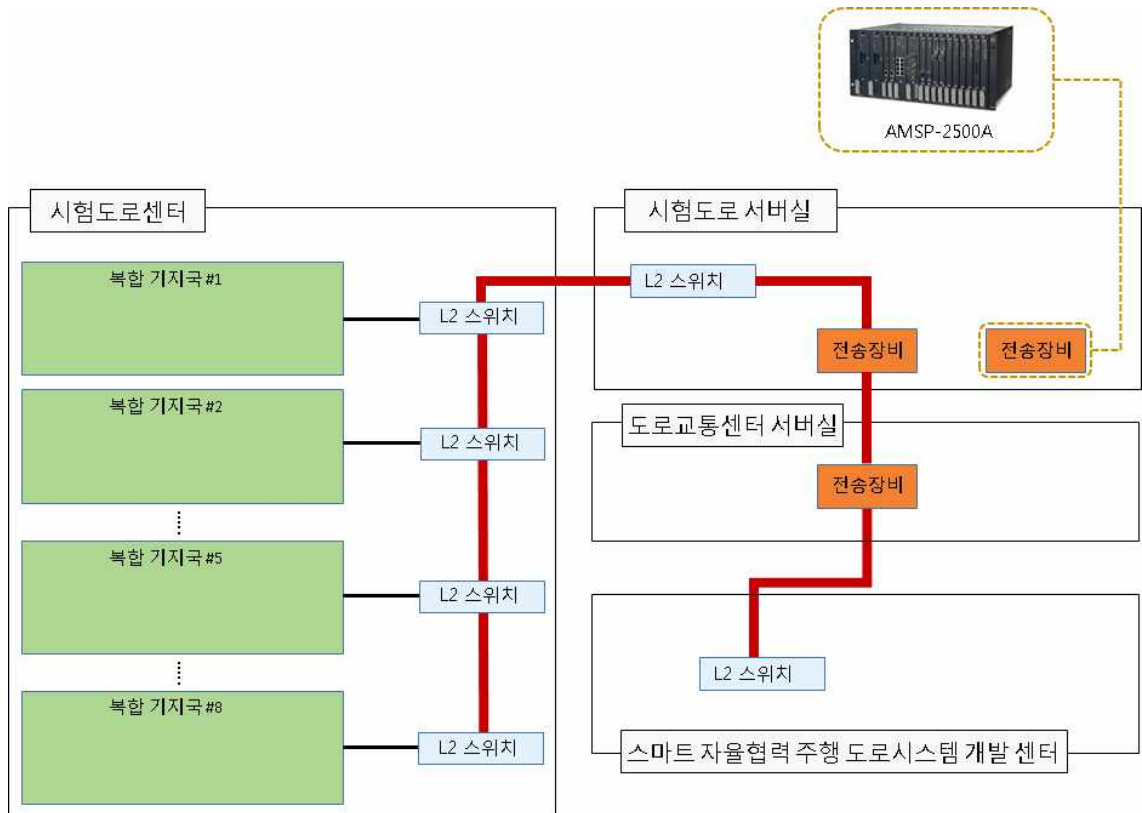


그림 10 전송장비 AMSP-C2500A(MSPP)

－ 전송장비 AMSP-C2500A(MSPP)



그림 11 우리넷 AMSP-C2500A(MSPP)

주요 특징

- 채널MUX MSPP는 단일 장치에서 음성(채널) 및 TDM, 이더넷 신호를 다중화/역다중화하여 2.5G/622M/155Mbps 이상의 속도로 광전송하는 차세대네트워크(NGN) 장치
- MSPP는 단일 장치에서 음성(DS0), TDM(DS1/E, DS3), SDH 및 Ethernet(EOS)신호

를 다중화/역다중화하여 광 전송하는 NG-SDH 장치

- 필요로 하는 회선 사용량에 원활하게 대처하기 위하여 대용량, 중용량, 소용량, 초소용량 및 음성을 지원하는 CH-MUX 장치로 구분
- 사용 환경에 따라 PTP, PTMP, Ring, Multi Ring 및 Subtending Ring 등 다양한 망운영 형태를 지원
- 필요로 하는 다양한 인터페이스 제공: DS0, DS1/E, DS3, STM-1/4/16, 이더넷 100 Mbps/1Gbps
- 안정적인 보호절체 제공
- GUI 방식 운용터미널 제공으로 쉬운 운용관리
- 광모듈 실/탈장 가능한 SFP 적용, DDMI(Digital Diagnostic and Monitoring) 기능으로 설치 및 운용관리 용이

스위칭 용량 (HO/LO)	25 Gbps / 10Gbps
슬롯수	공통부: 4 Slot 채널부: 126 Slot
인터페이스 용량	STM-16: 2 STM-4: 5 STM-1: 11 GE: 8 FE: 40 DS3: 18 E1/T1: 128 DS0: 192
이중화	네트워크: 1+1MSP, MSSPRing, SNCPRing 유니트: DS1/E, DS3 유니트 1:1
운용관리	인터페이스: RS-232C, 100/1000BaseT 망관리: TCP/IP, TL1, SNMP Trap
사용전원	DC -48V, AC 220V
크기 [W X H X D(mm)]	483 X 222 X 344

표 3 우리넷 AMSP-C2500A(MSPP) 시스템 사양

(나) SDN 기반 도로통신 N/W 시스템 구축) - 결과물: SDN 기반 테스트베드

① 성능 테스트를 수행함으로써 실 도로에 네트워크 시스템을 구축

- 주어진 테스트 환경(리소스) 내 검증 결과를 바탕으로 네트워크 시스템 구축에 대한 최종 품질 상태를 기록하고 구축을 위한 테스트를 실행하였음

스마트 자율협력주행 도로시스템 네트워크 구성도

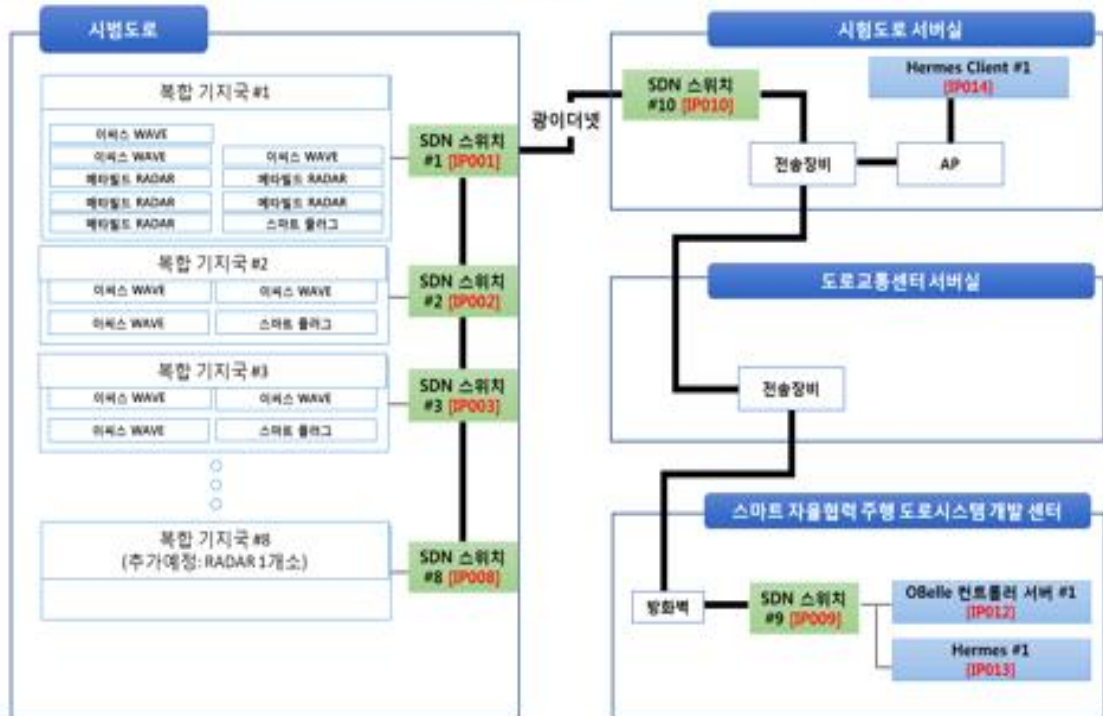


그림 12 전체 네트워크 시스템의 구성

- 테스트베드 망 구축(지리적 거리)
 - : 테스트 베드 망이 구축된 지리적 거리를 측정한다. 1차 년도 개발 목표치의 경우 10 km 이상이 요구되어짐
- 단말 - 관제 센터 간 SDN 통신(지연시간)
 - : SDN 스위치에 연결된 호스트와 관제센터간의 통신에서의 지연시간을 측정한다. 패킷을 생성하여 보낸 다음 다시 돌아오기까지의 수십 개의 패킷에 대한 평균 Round-trip time을 통해 지연시간을 평가한다. 1차 년도 개발 목표치의 경우 100 ms 미만이 요구되어짐
- 단말 - 관제센터 간 SDN 통신(대역폭)
 - : 특정 호스트와 관제센터간의 통신 대역폭을 측정한다. 대역폭의 경우 TCP 포트를 열고 윈도우 사이즈 조절을 통해 최대 대역폭을 측정하고 이를 10회 이상 반복한 다음 평균 대역폭을 통해 성능을 평가한다. 1차 년도 개발 목표치의 경우 900 Mbps 이상이 요구되어짐
- 1차 년도 최종 성과지표

핵심성과	단위성과	단위	전체 비중	개발 목표치 (1차년도)	평가방법	측정결과
SDN 기반 테스트베드	A-1 테스트베드 망 구축 (지리적 거리)	km	6	10	보고서	51.6 km (여주시험도로: 7.7 km 궁내동센터연결: 43.9 km)
	A-2-1 단말-관제 센터 간 SDN 통신 (지연시간)	ms	4	100	보고서	평균 2.91 ms
	A-2-2 단말-관제 센터 간 SDN 통신 (대역폭)	Mbps	4	900	보고서	평균 918 Mbps

표 4 1차 년도 최종 성과지표

(다) SDN 기반 도로통신 N/W 시스템 구축 성과 항목 상세

① 테스트베드 망 구축(지리적 거리)

테스트베드 망이 구축된 지리적 거리는 복합 기지국 및 컨트롤러에 의해 제어되는 SDN switch가 설치된 여주 시험도로에서 관제센터가 설치되어있는 분당구 궁내동 센터까지 직선거리 43.9 km이다. 또한 여주 시험도로의 총 길이는 7.7 km이므로 지리적 거리 합계는 51.6 km로 볼 수 있다. 이는 개발 목표치 10 km 이상을 만족하였음

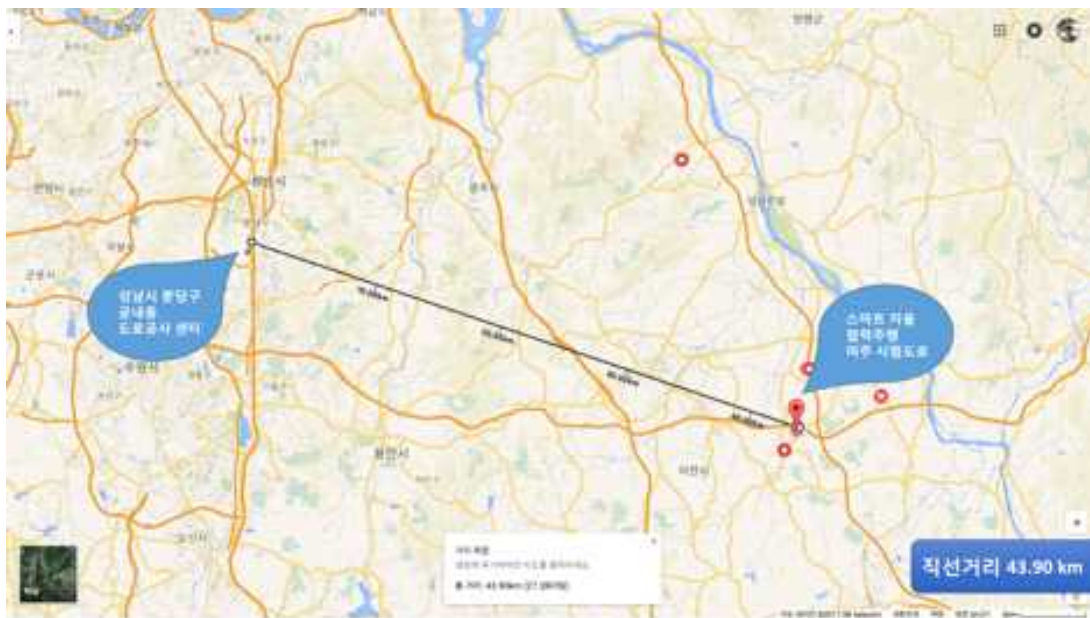


그림 13 도로공사 센터 - 여주 시험도로간 직선거리

② 단말 - 관제 센터 간 SDN 통신(지연시간)

ping 패킷을 이용하여 round-trip latency를 측정함으로써 단말-관제센터 사이의 약 43.9 km 직선 거리 간 SDN 통신의 지연시간을 측정한다. 평균적으로 측정된 RTT (Round Trip Time)은 5.8 ms로써 단방향 2.9 ms 이므로 목표치 100 ms보다 낮은 지연시간을 달성하

는 것을 볼 수 있음

```

ginjaehos-MacBook-Pro-2:Downloads zzero$ ping 172.18.200.73
PING 172.18.200.73 (172.18.200.73): 56 data bytes
64 bytes from 172.18.200.73: icmp_seq=0 ttl=64 time=5.820 ms
64 bytes from 172.18.200.73: icmp_seq=1 ttl=64 time=5.820 ms
64 bytes from 172.18.200.73: icmp_seq=2 ttl=64 time=5.834 ms
64 bytes from 172.18.200.73: icmp_seq=3 ttl=64 time=5.817 ms
64 bytes from 172.18.200.73: icmp_seq=4 ttl=64 time=5.863 ms
64 bytes from 172.18.200.73: icmp_seq=5 ttl=64 time=5.876 ms
64 bytes from 172.18.200.73: icmp_seq=6 ttl=64 time=5.832 ms
64 bytes from 172.18.200.73: icmp_seq=7 ttl=64 time=5.860 ms
64 bytes from 172.18.200.73: icmp_seq=8 ttl=64 time=5.832 ms
64 bytes from 172.18.200.73: icmp_seq=9 ttl=64 time=5.838 ms
64 bytes from 172.18.200.73: icmp_seq=10 ttl=64 time=5.866 ms
64 bytes from 172.18.200.73: icmp_seq=11 ttl=64 time=5.853 ms
64 bytes from 172.18.200.73: icmp_seq=12 ttl=64 time=5.847 ms
64 bytes from 172.18.200.73: icmp_seq=13 ttl=64 time=5.863 ms
64 bytes from 172.18.200.73: icmp_seq=14 ttl=64 time=5.845 ms
64 bytes from 172.18.200.73: icmp_seq=15 ttl=64 time=5.843 ms
64 bytes from 172.18.200.73: icmp_seq=16 ttl=64 time=5.855 ms
64 bytes from 172.18.200.73: icmp_seq=17 ttl=64 time=5.852 ms
64 bytes from 172.18.200.73: icmp_seq=18 ttl=64 time=5.832 ms
64 bytes from 172.18.200.73: icmp_seq=19 ttl=64 time=5.836 ms
64 bytes from 172.18.200.73: icmp_seq=20 ttl=64 time=5.838 ms
64 bytes from 172.18.200.73: icmp_seq=21 ttl=64 time=5.848 ms
64 bytes from 172.18.200.73: icmp_seq=22 ttl=64 time=5.858 ms
  
```

그림 14 SDN switch #9에 연결된 호스트 단말과 관제센터(172.18.200.73) 간의 지연시간

③ 단말 - 관제센터 간 SDN 통신(대역폭)

SDN 스위치에 연결된 호스트와 관제센터간의 대역폭을 iperf3을 통해 측정한다. TCP 연결이며 Line-rate인 1 Gbps의 90%이상의 대역폭 성능이 나오는 것을 알 수 있음

```

/Users/atto$ iperf3 -c 172.18.200.73
Connecting to host 172.18.200.73, port 5201
[ 4] local 172.18.200.5 port 52893 connected to 172.18.200.73 port 5201
[ ID] Interval           Transfer    Bandwidth
[ 4]  0.00-1.00   sec    104 MBytes  873 Mbits/sec
[ 4]  1.00-2.00   sec    110 MBytes  923 Mbits/sec
[ 4]  2.00-3.00   sec    111 MBytes  933 Mbits/sec
[ 4]  3.00-4.00   sec    110 MBytes  920 Mbits/sec
[ 4]  4.00-5.00   sec    108 MBytes  907 Mbits/sec
[ 4]  5.00-6.00   sec    109 MBytes  915 Mbits/sec
[ 4]  6.00-7.00   sec    109 MBytes  918 Mbits/sec
[ 4]  7.00-8.00   sec    111 MBytes  929 Mbits/sec
[ 4]  8.00-9.00   sec    111 MBytes  934 Mbits/sec
[ 4]  9.00-10.00  sec    111 MBytes  935 Mbits/sec
-----
[ ID] Interval           Transfer    Bandwidth
[ 4]  0.00-10.00  sec   1.07 GBytes  919 Mbits/sec
[ 4]  0.00-10.00  sec   1.07 GBytes  918 Mbits/sec
iperf Done.
  
```

그림 15 iperf3으로 측정한 호스트-관제 센터 간 대역폭 - 평균 918 Mbps

④ SDN 스위치 설치를 위한 네트워크 토폴로지 분석

기존 여주 시범도로의 경우 각 기지국마다 Legacy L2스위치가 설치되어있으며 광 이더넷을 통해 도로교통센터 서버실의 전송장비로 이어진다. 이는 자율협력주행 개발센터의 방화

스마트 자율협력주행 도로시스템 네트워크 구성도

- 경부고속도로 서울IC ~ 신갈IC 8개소
- 영동고속도로 신갈IC ~ 호남IC 10개소

시범도로

복합 기차국 #1 (경부선)

복합 기차국 #2 (경부선)

복합 기차국 #3 (경부선)

복합 기차국 #4 (영동선)

복합 기차국 #5 (영동선)

복합 기차국 #10 (영동선)

도로교통센터 서버실

전송장비

스마트 자율협력주행 도로시스템 개발 센터

일화백

L2 #1

서버실

L2 #2

상환실

상황판

교통센터 옥상

L2 #3

지휘수신국 (2차)

지령제어국 (2차)

복역주행일소

L2 #4

지휘수신국

지령제어국

오산면일소

L2 #5

지휘수신국

지령제어국

⑤ SDN 스위치, 보안박스, 제어기, 관제 시스템 구축

– 20 –



그림 18 스마트 자율협력주행 통합 제어기



그림 19 스마트 자율협력주행 통합 제어기 - SDN 스위치 구축

(라) SDN 개별 요소 기능 검증 - 결과물: SDN 망 테스트 결과서

① 보안박스 기본 기능 검증

방화벽이 가능한 보안 기능을 가상화 네트워크 서비스로 동작시킴

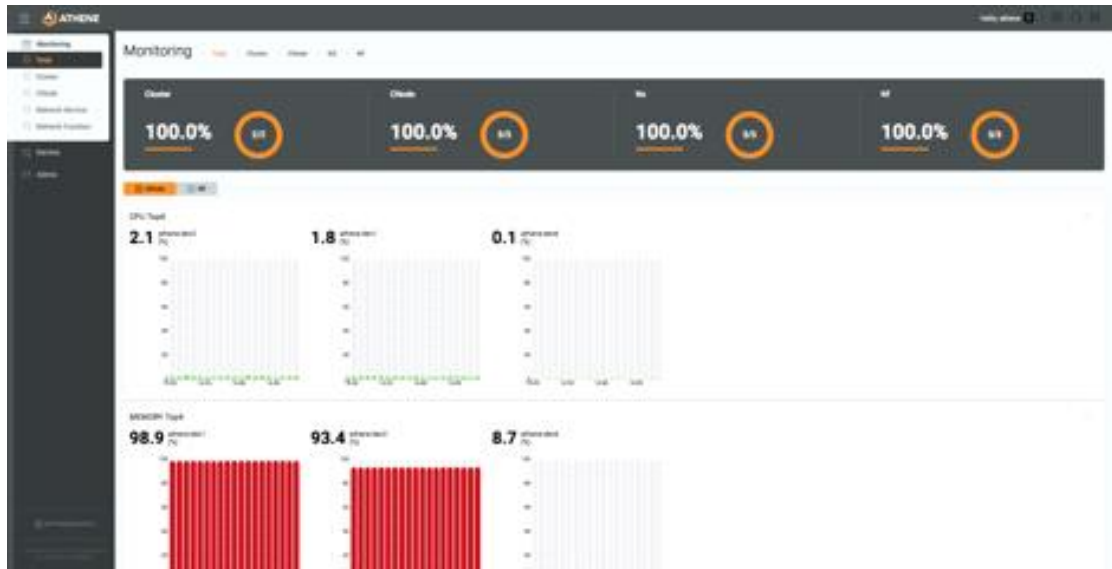


그림 20 보안박스 Resource 모니터링

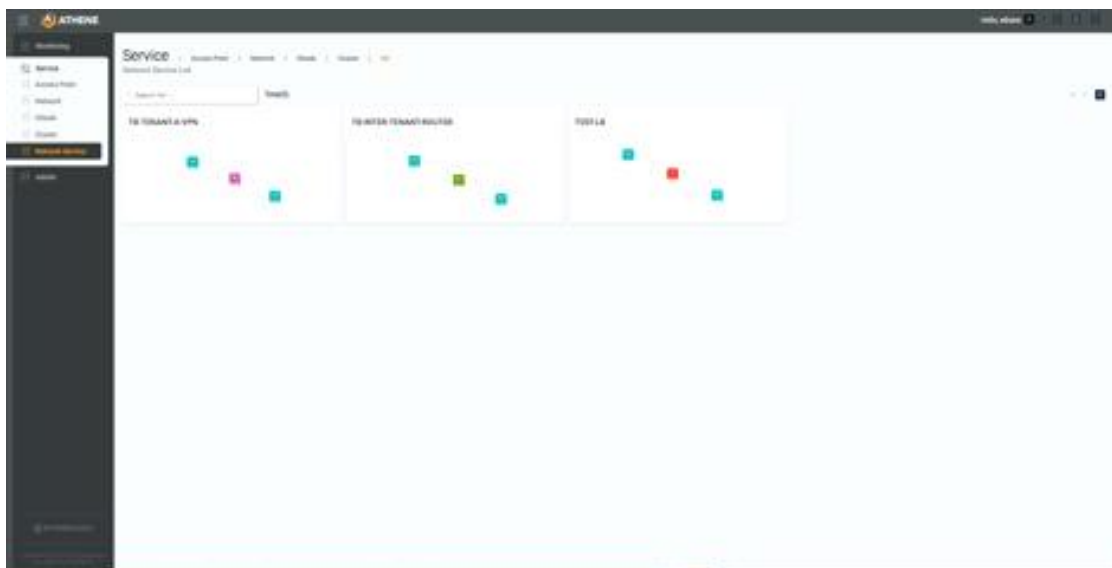


그림 21 보안박스서비스모니터링

② 중앙관제 시스템 기본 기능 검증

도로통신 네트워크에서의 관리 및 제어가 중앙 시스템을 통해 관제됨



그림 22 스마트 자율협력주행 체험도로 체험도로 GUI Topology

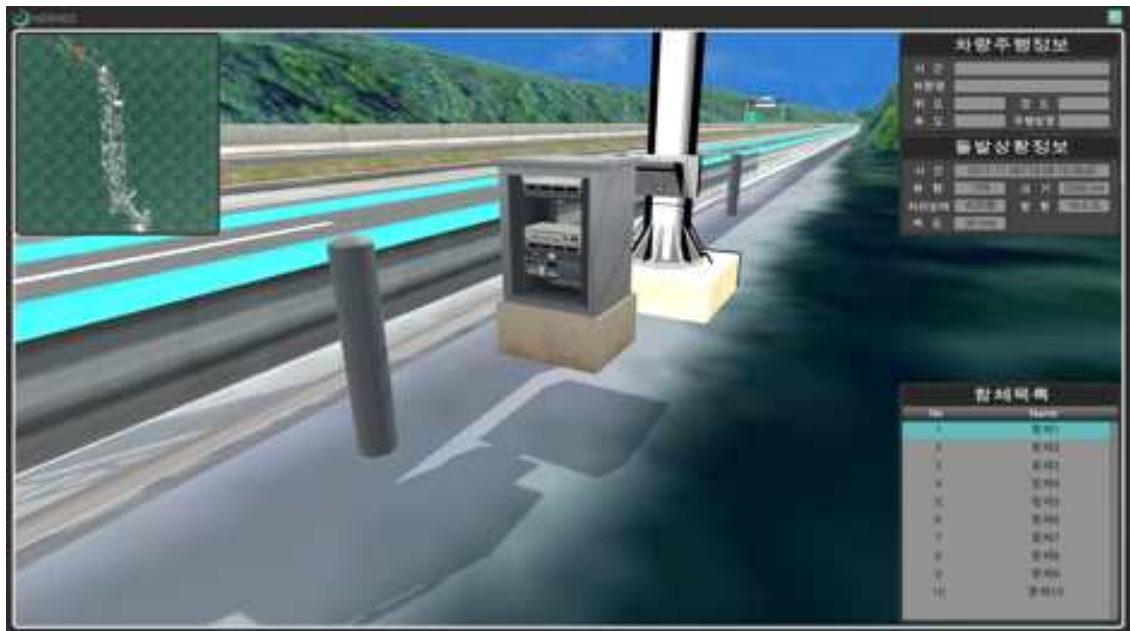


그림 23 스마트 자율협력주행 통합 제어기

(마) SDN 개별 요소 검증

① 한국도로공사 여주시험도로 시연검증

- 국가 R&D로 진행 중인 “스마트 자율협력주행 도로시스템 개발” 연구 중간 기술시연
- 시연내용: 돌발 상황, 기상정보, POI 서비스 등



그림 24 한국도로공사 여주시험도로 시연 사진

(바) 국토교통부 정보화사업 보안기능인증 시험 결과

① 시험개요

제 품 명	OBelle fabric v3.0
제 조 회 사	아토리서치
펌웨어/ 소프트웨어 버전	obv3.tar.gz
	CCB7C7A0BA3CDB2EF3042095264BD22A3F8366465E66FD854790EC
	F98E84DF8212BC324B5BEB90122A2D970AA237A9770815010F56027 2BC2E9F80F3F1D908A7
하드웨어 모델명	‘해당사항 없음’ 일반(COTS) x86 서버에 설치 됨.
시험기관	한국전자통신연구원, 박상길(042-860-5336)
CC인증	-
검증필 암호모듈	-
도입기관	한국도로공사, (주)코스콤
적용 규격	SDN 컨트롤러 보안기능 요구사항
비고	최초시험

표 5 보안 기능 인증 시험 개요

② 주요 시험환경

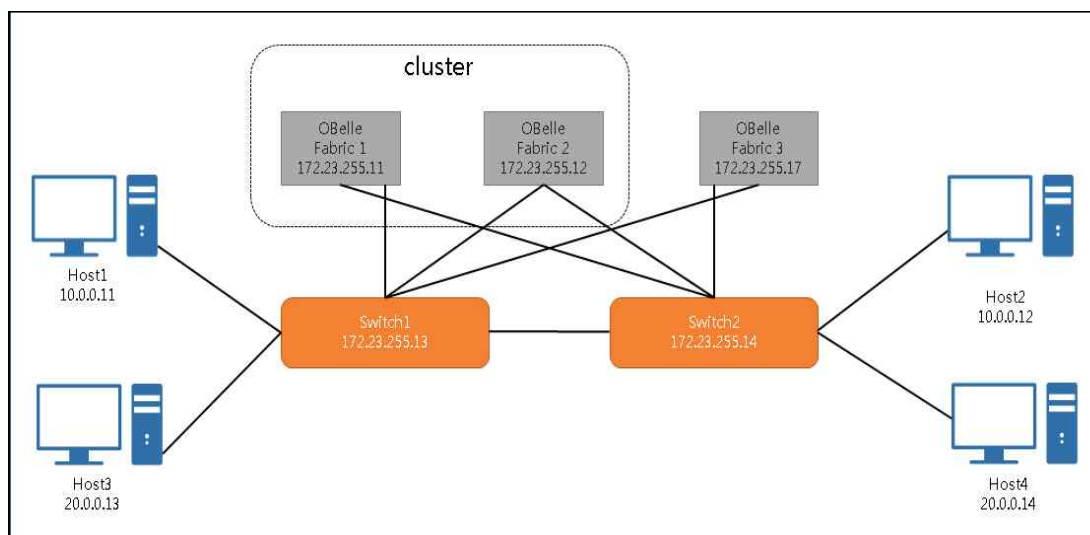


그림 25 보안 기능 인증 시험 환경

③ 종합 시험 결과

	필수			선택				총합
	만족	불만족	해당사항 없음	기능 제공	기능 미흡	기능 미제공	해당사항 없음	
제 품 모델명	25	1	6	14	—	2	2	50

표 6 보안 기능 인증 시험 결과

(주)아토리서치의 SDN 컨트롤러인 OBelle Fabric v3.0에 대해 업체에서 제출한 보안기능 운용설명서와 시험결과서를 비교하여 분석하였음
해당 장비가 운용되는 기관에서는 ‘보안기능 운용설명서’와 업체가 배포하는 장비설명서등을 통하여 보안성을 제공하는 운용이 가능하리라 판단.

(사) 도로통신 네트워크 보안 연구 - 결과물: 도로통신 네트워크 공격 분석 보고서(13건 도출)

① 도로통신 네트워크 공격사례

차량 간 통신 네트워크 공격사례

- 크라이슬러 Uconnect 해킹 사례
- 2015년 블랙햇에서 공개되었으며, 외부 해킹 프로그램을 통해 차량의 모든 운행 동작을 조작할 수 있는 보안 문제를 공개



그림 26 해커가 할 수 있는 자동차 공격 목록

차량-인프라간 통신 네트워크 공격사례

- 스웨덴운송 관리국의 V2I 네트워크 DDoS 공격 사례
- 2017년 10월 스웨덴 운송관리국이 DDoS 공격을 받아 열차운행에 차질을 빚음

② 도로통신 네트워크 공격백터

보안 요구사항에 따른 공격벡터

– 인증 및 데이터 무결성, 기밀성, 부인 봉쇄, 가용성

보안 요구 사항	세부 공격	설명
인증 및 데이터 무결성	라우팅 테이블, LDM 변조 공격	다른 차량 내의 라우팅 테이블, LDM 등을 변조하기 위해, 근처에 존재하지 않는 차량의 정보 등을 거짓으로 조작하여 전송하거나, GPS의 신호 정보를 조작하는 공격이 가능함
	Sybil 공격	차량 간 제대로 된 인증과정이 부족한 것을 이용하여, 임의의 공격자가 다수의 차량 ID를 가지고 네트워크를 공격하는 방법을 말함. 가능한 공격 시나리오의 하나로, 공격자가 다수의 차량 ID를 도용하여 주변 차량들에게 보냄으로써, 도로가 병목 상에 있다고 교통 상황에 대한 거짓 정보를 전파할 수 있음
	라우팅 메시지의 위/변조 공격	차량 간 통신에서 각 차량은 자신의 주변 상황에 대한 정보를 전달하거나 앞선 차량의 상태 정보를 받아서 자신이 처리하고 또 뒤 따라오는 차량에 전달해주는 역할도 할 수 있음. 이 과정에서 중간 노드가 되는 자신이 전달하게 되는 메시지를 위조, 변조함으로써 뒤 따라오는 차량에 거짓 정보를 전달하는 것이 가능함
	차량 비밀 정보 유출 공격	차량의 개인키 및 고유 정보에 대한 위, 변조 및 비인가 된 사용을 의미
	서비스 인프라에 대한 공격	PKI 인증 센터에게 OBU의 거짓 침해 정보를 전달하여, 잘못된 인증서 취소 목록을 생성하게 하는 공격임
기밀성	차량 통신 메시지의 도청 공격	차량 통신 메시지의 도청은 차량 간 통신, 차량-인프라 간 통신 모두에서 가능하며, 공격자는 차량 내 또는 노변 기지국 근처에서 차량의 OBU 메시지나 도로 상의 RSU 메시지를 도청하는 것이 가능함
	OBU, RSU의 비밀 소프트웨어에 대한 도청 공격	OBU 또는 RSU의 원거리 업데이트 중에 소프트웨어를 가로채거나, 가로챈 소프트웨어로부터 차량의 비밀 정보를 유출하는 공격을 의미
부인 봉쇄	디지털 서명 공격	CA(Certificate Authority)에 저장된 가명 DB를 위조하거나, 장기 인증서(Long Term Certificate)와 가명 인증서(Short Term Pseudonym Certificate) 간의 관계를 조작하는 형태의 공격이 가능함
가용성	전파 방해 (Jamming) 공격	전파 방해 공격은 일정 구역에서 차량 통신에 장애를 일으키는 신호를 발생시키는 공격으로서 네트워크 계층 또는 물리 계층에서의 공격을 의미
	V2X 통신에 대한 DDoS 공격	플로딩은 단일 홉 또는 멀티 홉 통신 구간에 다량의 무의미한 메시지를 전파하는 공격으로, 블랙홀은 다음 홉으로 라우팅해야 할 메시지를 전송하지 않는 공격이다. 라우팅 노드가 특정 메시지만을 재전송하는 공격도 포함됨

표 7 보안 요구사항에 따른 공격벡터

도로통신 네트워크에 따른 공격벡터

- CAN (Controller Area Network), VANET (Vehicle Ad Hoc Network)

네트워크 타입	취약점	설명
Controller Area Network (CAN)	브로드캐스트 이슈	CAN에서 ID 헤더는 패킷의 종류를 표시하는 데 사용되며, 처리해야 할 패킷이 생길 경우, 우선 CAN 상의 모든 컴포넌트에게 브로드 캐스팅함. 따라서 CAN은 공격자의 도청에 취약한 문제점을 가지고 있음
	인증 시스템의 부재	CAN에 존재하는 DATA 타입의 프레임은 ECU간의 실질적인 통신에 이용됨. 그러나, DATA 프레임 내에 메시지를 송신하는 ECU에 대한 인증을 위한 필드가 없는 문제점이 존재함
Vehicular Ad Hoc Network (VANET)	잘못된 정보의 확산	빠른 속도로 이동하는 차량들 사이에서 메시지를 빠르게 주고받기 위해 메시지의 암호화 과정이 적절히 이루어지지 않는 문제가 발생할 수 있음. 공격자는 이러한 점에 착안하여 잘못된 정보를 네트워크에 확산시켜 다른 운전자의 행동에 영향을 미치거나 메시지 전송 과정에서 메시지를 변조, 삭제하는 행위와 같은 트래픽 변조가 가능함

표 8 차량 통신 네트워크에 따른 공격 벡터

(아) 1차년도 보완 사항

수정·보완요구사항		반영내용 요약
1	질적성과물 중 공동기관(카이스트)의 보고서의 구체적인 결과물이 명확하지 않음	KAIST 결과 보고서 보완 제출(별도 제출)
2	2차년도 연구비 및 연구인프라 대비 성과목표가 너무 부족함	2차년도 특허 성과 추가
3	3차년도 연구성과목표로 신기술 인증만 설정하고 있어 다른 성과지표를 추가할 필요가 있음	3차년도 특허 성과 추가
4	주관연구기관 연구과제추진비 중 야근 식대가 과다함(총 3,160회)	야근식대 변경
5	주관기관 및 공동연구기관 국외출장비의 경우 사업화 취지의 적합성 미흡	국외출장지 변경
6	위탁연구기관 연구비(카이스트, 30,000천원) 소명이 필요함	KAIST 결과 보고서 보완 제출(별도 제출)
7	양적 성과목표 추가할 예정임(출원 2건, 등록 1건) : 2차년도	2차년도 특허 성과 추가
8	3차년도 성과 추가 예정	3차년도 특허 성과 추가
9	주관기관 연구활동비 중 S/W 등록비, 세미나 부스, 참가비를 간접비로 조정	세미나 부스, 참가비를 간접비로 조정

10	연구장비 중 이동테스트용 노트북 50% 절감(6,000천원→3,000천원), SDN스위치 예산 조정(30,000천원→25,000천원)	예산 조정
11	야근식대 20% 절감(25,280천원→20,000천원)	예산 조정
12	주관연구기관 국외출장비 50% 절감	예산 조정
13	위탁연구기관(카이스트)의 연구보고서를 성과지표 중심으로 보완할 예정	KAIST 결과 보고서 보완 제출(별도 제출)
14	따라서 당초 450,000천원에서 413,000천원으로 조정	예산 조정

(2) 2차년도(2018)

(가) SDN기반 트래픽 최적화 SW - 결과물: SDN기반 트래픽 최적화 SW 테스트 결과서

① 실증 네트워크 구성도

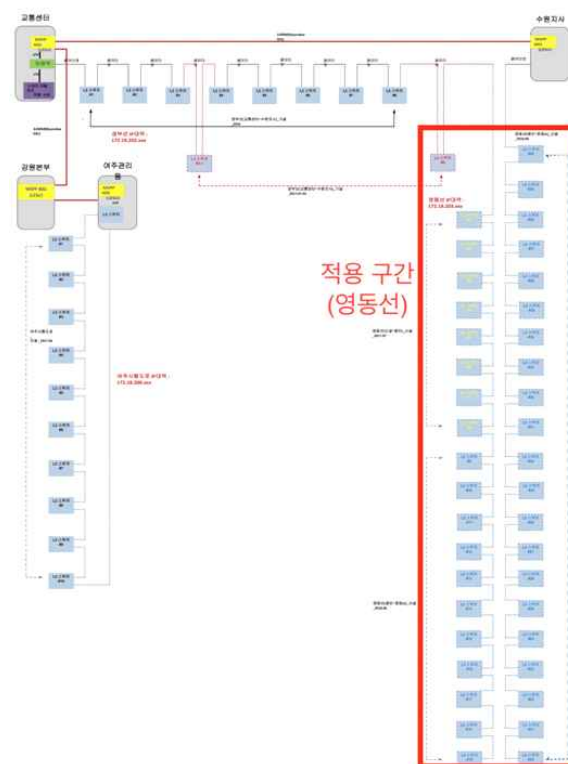


그림 27 스마트 자율협력주행 네트워크 구성도

② 주요 기능

호스트 관리	- ARP 패킷 내의 정보를 이용해서 호스트 관리 - ARP 패킷을 수신하면, 수신한 포트와 source MAC을 이용해서 호스트 등록 - 포트 상태를 이용해서, 링크가 다운되면 호스트 삭제
경로제어	- 스위치간 링크 상태를 이용해서 경로 설정 - 링 토폴로지 상에서 루프 방지 - 링 토폴로지 상에서 통신 중이던 경로 단절시 다른 경로로 변경
접근제어	- MAC address 기반으로 ACL 구현
품질관리	- 포트 사용량을 이용해서 QoS 구현

③ 내부 테스트베드

구축/테스트 기간	2018.7.20. ~ 2018. 10. 01.
구축 목적	다양한 장애상황 재현. 영동선 망은 실 운영중으로 다양한 장애 및 트래픽 생성이 어려움
사용장비	Controller server (Ubuntu 16.04, Xeon, RAM 64GB) Openflow switch 10대 (Atto Switch) Legacy switch 2대 (Atto Switch) L3 Switch 1 대

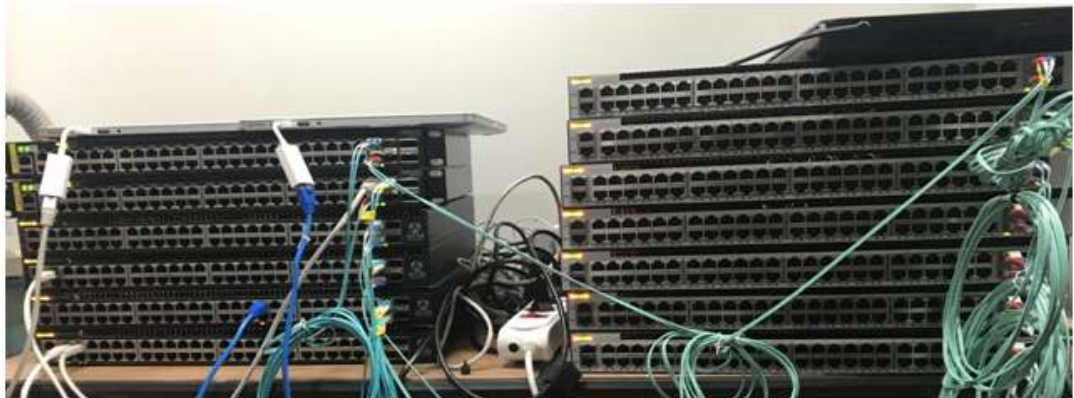


그림 28 내부 테스트베드 구성

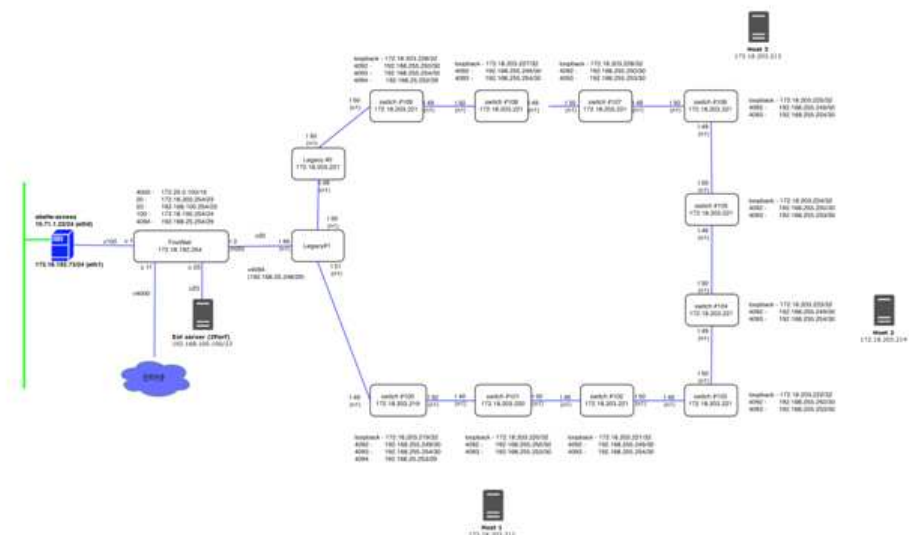


그림 29 내부 테스트베드 토폴로지

④ 테스트 결과

항목	상세 항목	결과
호스트 간 통신	OF:호스트 ↔ OF:호스트	Pass
	OF:호스트 ↔ Legacy:호스트	Pass
호스트 이동 시 통신	다른 DP로 이동	Pass
link 단절 (1 point) 시 통신	OF - OF 단절	Pass
	OF - Legacy 단절	Pass
	Legacy - Legacy 단절	-
link 단절 (2 point) 시 통신	2개 이상 트리 생성	Pass
외부 통신	gateway로 통신	Pass
	8.8.8.8 로 통신	Pass
	L3 밖 호스트와 통신	Pass
토폴로지 확장 시 통신	Legacy 추가, OF 추가	Pass
오벨 강제 종료		-
오벨 강제 종료 후 재부팅		-
OF 전원 뽑았을 경우		Pass

핵심성과	단위성과		개발목표치	측정방법	측정결과
SDN 기반 트래픽 최적화 SW	B-1	우선순위지정	5개	iperf	만족
	B-2	대역폭 제한	1Mbps	iperf	만족
	B-3	트래픽 차단	5개	iperf	만족

(나) 도로통신 네트워크 보안기술 - 결과물: 도로통신 네트워크 공격에 대한 대응책에 관한 연구 보고서

① 도로통신 네트워크 공격 분류

도로 통신 네트워크를 대상으로 하는 공격은 다음과 같은 세 가지 형태로 분류가 가능.

- 도로 통신 네트워크에서 필요한 보안 요구사항을 대상으로 하는 공격
- 차량 내부 및 외부 모듈 사이에 발생 가능한 공격
- 도로 통신 네트워크(CAN, VANET)에서 발생 가능한 공격

도로 통신 네트워크에서 필요한 보안 요구사항을 대상으로 하는 공격은 보안의 3요소라 불리는 CIA (기밀성, 무결성, 가용성)를 기반으로 한 도로 통신 네트워크 내 주요 보안 요구사항을 파괴하는 것을 목표로 하는 공격임.

② 케이스#1: 브로드캐스트 이슈

- CAN 네트워크에서는 각각의 노드(ECU)들이 메시지를 전송할 때, ID 헤더에 메시지의 종류를 표시하고 해당 메시지를 모든 노드들에게 브로드캐스트 하는 방식을 택하고 있

음.

- 이러한 방식의 가장 큰 문제점은 전혀 상관 없는 다른 노드들에게도 메시지가 노출되기 때문에 악의적인 사용자가 이를 이용해 메시지의 모든 정보를 알 수 있음.
- 브로드캐스트 이슈를 해결하기 위해, 메시지를 특정 노드에게 보내거나 여러 노드에게 보내야 하는 경우 멀티캐스트 방식을 이용해 전달하는 방식을 채택할 수 있음. 하지만 이 방법의 경우 기존의 방식을 변형하여 배포해야 하는 문제점이 존재함.
- 다른 방법으로는 공개키 암호화를 이용한 데이터 전달 방식이 있음. 이 경우 수신자는 반드시 송신자의 공개키를 알고 있어야 함

③ 케이스#2: 서비스 거부 공격

- CAN 네트워크는 노드들 간의 통신 경로를 공유하기 때문에 패킷 플러딩과 같은 공격에 굉장히 취약함.
- 이러한 문제가 발생하는 가장 큰 원인은 악의적인 노드가 통신 버스에 속하게 되는 점이기 때문에 이를 방지하기 위해 새롭게 추가되는 노드는 반드시 인증 과정을 통해 입증된 정상적인 노드들로 구성하는 방법이 있음.
- 추가적으로 각 노드별로 일정 시간 동안 보내는 메시지의 임계값을 설정하여 해당 임계값을 넘는 노드의 경우 악의적인 행위라 판단하고 차단하는 방식 또한 존재함.

④ 케이스#3: 블랙홀 공격

- 블랙홀 공격은 악의적인 노드가 도로통신 네트워크에 포함되어 있다고 가정하고 새롭게 들어온 노드가 다른 노드와 통신하기 위해 경로를 탐색하는 과정에서 중간의 공격자가 잘못된 정보를 반환하여 반드시 공격자를 거쳐 데이터가 전달되도록 하는 공격임.
- 이 공격을 통해 악의적인 공격자는 새롭게 들어온 노드가 보내거나 받는 모든 메시지를 확인할 수 있으며 일부로 패킷들을 모두 버릴 수도 있는 강력한 공격임.
- 이를 막기 위해서는 공개키 암호화 방식을 통해 수신자와 송신자 사이에서만 데이터를 확인할 수 있도록 하는 방법이 존재함.
- 고의적으로 패킷을 버리는 문제를 해결하기 위해서는 송신자가 일정 시간 응답이 없는 경우 새로운 경로를 탐색하는 것도 대응 방법이 될 수 있음.

⑤ 케이스#4: 도청 공격

- 무선 링크를 통해 통신하는 VANET 네트워크의 특성으로 인해 트랜시버를 가진 모든 장비들이 메시지를 수신할 수 있다는 단점이 존재함.
- 이에 대해 특별한 암호화가 적용되어 있지 않으면 손쉽게 도청할 수 있기 때문에 이러한 메시지들은 전부 암호화 통신을 기본적으로 제공하는 것이 필요하다.

⑥ 케이스#5: 접근제어 시스템 오류 공격

- 기본적인 차량 표준의 경우에는 여러 안전한 기능들의 경우 요청-응답 접근 제어 (Challenge-response access control) 프로토콜을 사용하여 보호하는 것을 원칙으로 함.
- 몇몇 차량의 CAN 채널과 연결된 텔레메틱스 (Telematics)들은 고정된 그리고 하드코딩 (Hard-coding)된 요청-응답을 사용하므로 모든 노드들이 동일한 보안 시드를 가짐으로써 권한 없는 노드가 손쉽게 요청-응답 쌍을 취득하여 중요 서비스에 접근을 할 수 있다는 문제가 발생함.

- 이러한 문제를 해결하기 위해 접근제어에 사용하는 보안 시드의 하드코딩을 지양하고 노드별로 서로 다른 보안 시드를 갖도록 주기적으로 변형해주는 일이 필요함.

(다) 도로통신 네트워크 통합관계 SW - 결과물: 도로통신 네트워크 통합관계SW 설계서

① 표현 대상 오브젝트

	분 류	내 용	특이사항
1	도로	영동, 경부 고속도로	디테일한 도로를 구현하려면 새로 모델링 해야함.
2	도로중앙 분리대	현재 모델링 된 도로에 중앙 분리대	도로구간에 맞게 모델링이 되어야 함.
3	도로사이드 가드레일	현재 모델링 된 도로에 가드레일	"
4	지형	고속도로 주변의 산, 언덕 등	도로주변과 터널 상단 부분
5	건물	고속도로 주변의 건물	건물 단순 or 디테일 여부를 알고 모델링 되어야 함.
6	표지판	구간별 표지판	구간별 표지판 배치 여부를 알아야 모델링 가능.
7	차량	자율주행 자동차	자율주행 차종에 맞고 디테일 여부에 따라 모델링이 되어야 함.
8	3D UI	3D 위치상에 보여지는 UI	각종 이벤트 발생을 3D 위치에 표현 여부
9	2D UI	각종 정보창, 이벤트 패널 등	새로운 UI 구성 여부에 따라 디자인

② 모델링



그림 30 도로 전체 조감도



그림 31 자동차 모델링



그림 32 신갈 JC

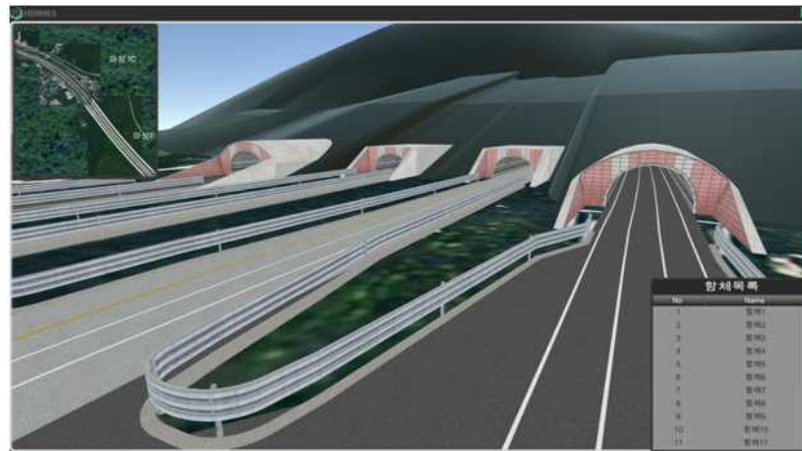


그림 33 마성 터널



그림 34 용인 휴게소



그림 35 도로 표지판 및 과속 단속 장비



그림 36 합체 및 내부 장비



그림 37 네트워크 원격 제어

(라) 2차년도 보완 사항

수정·보완요구사항		반영내용 요약
1	미달성 성과(특허 등록 및 출원 각 1건)를 달성하기 위한 노력이 필요하며, 당해 연도 목표 미달성시 차 년도 목표로 설정 필요	특허 등록 1건 및 출원 1건 연차 내 달성 완료
2	연구 성과 검증을 위한 공인성적서 제출 필요	3차 년도 수행 결과 검증 목표에 공인시험성적서 명시
3	요청한 성과지표 변경(신기술→GS인증)은 사업화 목적에 부합하지 않아 불필요할 것으로 판단됨	KAIA의 확인에 따라, GS인증이 아닌 조달우수제품 등록으로 신기술인증 달성
4	시범운용을 ‘시연/외부전문가 평가’로 성과검증 방법 변경 필요	3차 년도 시범운용 검증 방법을 동영상에서 시연/외부전문가 평가로 변경
5	한국도로공사 ‘시범운영’ 보고서를 성과지표로 제시 필요	3차 년도 양적 목표에 시범운영 보고서 추가
6	’19년도 종료과제로서 소요금액의 100%(413백만원)를 차 년도 정부출연금 기준 금액으로 함	예산 반영 완료
7	아래 연구비 검토의견을 반영하여 405백 만 원으로 연구비 조정	제어기 서버 및 노트북은 범용성 장비로 판단되어 구입 필요성이 낮 으므로 감액
		위탁연구기관 연구비 재검토 필요
		특허출원 관련 연구비 책정 필요
8	전담기관의 요청에 따른 차년도 양적 목표 추가	3차 년도 양적 목표에 SW등록 2건 추가

(3) 3차 년도(2019)

(가) 시범도로 운영 및 검증 (경부선/영동선 전구간 설치 완료)

① 시범 운영 개요

SDN 스위치만으로 구성된 테스트베드를 실 도로상에 구축하여 다음과 같은 테스트를 수행한다.

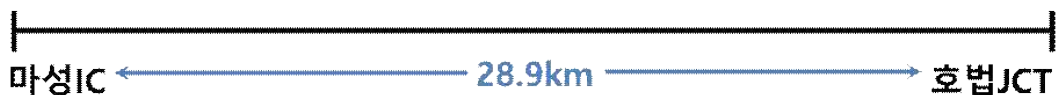
- 단말, 스위치, 회선, 센터 장비 장애 테스트
- 서비스 장애 유발 공격에 대한 방어 테스트
- 과부하 트래픽 발생 테스트
- 다양한 종류의 서비스 동시 발생 테스트
- 차량 에뮬레이션을 통한 시나리오 테스트

② 시범 운영 규모

5월 31일 경부선 10대, 영동선 8대를 추가 설치하여 경부/영동선 전 구간에 걸쳐 총 50대의 SDN 스위치를 설치 완료하여 운영하고 있다.



[경부선 시범도로]



[영동선 시범도로]

그림 38 시범도로 개요

③ 장비 운영 보고서

매달 작성하여 한국도로공사에 보고하고 있으며 아래는 장비 운영보고서의 일부분을 발췌하였다.

「SDN 기반 도로통신 네트워크 시스템 개발」 7월 운영 보고서

2019. 8

주관연구기관 / 아토리서치(주)

I 운영 현황

□ 장비 운영 현황

(기준일: 2019.7.31. / 단위 : 대)

구 분	계	경부선	영동선	궁내동
SDN 컨트롤러	1	0	0	1
산업용 SDN ¹⁾ 스위치	16	9	7	0
SDN 스위치	34	0	34	0

□ 장비 세부 사양

사 진	구 분	내 용
	장비명	컨트롤러 서버
	사양	CPU : Xeon E5-2630 Memory : 64GB / SSD : 480GB
	기능	SDN 스위치를 제어하는 SDN 컨트롤러가 설치되는 서버
	장비명 (모델명)	산업용 SDN 스위치 (ATT0-S1GF-8T8X4C)
	사 양	1G 8포트 / 10G 8포트 1G/10G 공용 포트 각 4포트 OpenFlow1.3.x 지원
	기 능	네트워크 통신 산업 환경이나 야외의 혹독하고 위험한 환경에서 사용

II 가동률 분석 및 장애 처리 현황

□ 장비별 가동률

(기간 : 2019.7.1. ~ 2019.7.31.)

노 선	이 정	방 향	DPID ²⁾	가동률 ³⁾
경부선	402.2k	서울	*****227	84.1442%
경부선	401.1k	서울	*****226	86.7334%
경부선	400.1k	서울	*****225	85.6745%
경부선	399.8k	부산	*****229	85.2179%
경부선	399.3k	서울	*****224	85.6744%
경부선	398.1k	서울	*****223	85.6742%
경부선	397.1k	서울	*****222	86.7394%
경부선	396.2k	서울	*****221	85.7129%
경부선	396.1k	부산	*****228	85.4120%
영동선	42.6k	강릉	*****211	85.4119%
영동선	43k	강릉	*****212	84.8388%
영동선	43.3k	강릉	*****213	84.8391%
영동선	44.4k	강릉	*****214	79.8955%
영동선	45.3k	강릉	*****215	79.3217%
영동선	46.6k	강릉	*****217	78.3736%
영동선	47.6k	강릉	*****218	78.4126%
영동선	50.2k	인천	*****219	80.8309%
영동선	51.0k	인천	*****220	79.2712%
영동선	51.9k	인천	*****221	80.8309%
영동선	52.06k	인천	*****244	78.3614%
영동선	52.2k	인천	*****210	78.4006%
영동선	52.47k	인천	*****245	78.3618%
영동선	52.9k	인천	*****222	80.7920%
영동선	53.8k	인천	*****223	80.8307%
영동선	54.80k	인천	*****224	79.2705%
영동선	55.23k	인천	*****246	75.9522%
영동선	54.6k	인천	*****209	75.0287%
영동선	55.70k	강릉	*****235	77.6306%
영동선	55.99k	인천	*****247	77.6310%
영동선	56.70k	강릉	*****225	76.7300%
영동선	57.70k	인천	*****236	76.6909%
영동선	58.30k	강릉	*****226	77.9013%
영동선	59.90k	강릉	*****227	83.3982%
영동선	60.16k	강릉	*****248	79.3847%
영동선	60.90k	강릉	*****249	80.2943%
영동선	61.70k	인천	*****237	79.3846%
영동선	62.1k	강릉	*****228	82.6792%
영동선	62.60k	인천	*****238	82.7177%

□ 월별 평균 가동률

월	1	2	3	4	5	6
가동률	99.9953%	99.7595%	94.3617%	99.7401%	97.6937%	73.7060%
월	7	8	9	10	11	12
가동률	81.5270%					

□ 장애 처리

일 시	구 분	내 용
2019.07.17.	전원 장애	6월에 장애 났던 사항 - 한일에서 영동선 55.9k 복구 - 전체 서비스 정상

그림 39 도로공사 월별 장비 운영 보고서

(나) 조달청 우수 제품 등록

① GS인증 획득(9월16일) - 결과물 : 인증서(1등급)

㉔ 인증 개요

조달청 우수 제품 등록을 원활하게 추진하기 위해 먼저 “TTA 한국정보통신기술협회”에서 심사하여 발급하는 GS인증은 아래와 같이 획득함

인증번호	회사명	제품명
19-0311	아토리서치(주) ATTO RESEARCH Inc.	아토 액세스 v1.0 ATTO ACCESS v1.0

㉕ 평가 항목

ISO/IEC 25023:2016(소프트웨어 제품 품질 측정에 관한 국제표준) 및 ISO/IEC 25051:2014(소프트웨어 제품 품질 요구사항과 시험에 관한 국제표준)에 따라 시험대상 제품(실행 소프트웨어, 사용자취급설명서 및 제품설명서)에 대해 품질 시험을 수행함



그림 40 GS 인증 시험 평가 항목

- 기능 적합성: 지정된 조건에서 요구되는 기능을 제공하는 정도
- 성능 효율성 : 지정된 조건에서 사용되는 자원의 양에 따라 제공되는 성능의 정도
- 호환성 : 동일한 하드웨어 및 소프트웨어 환경을 공유하는 동안 타 소프트웨어와 정보를 교환하거나, 소프트웨어가 요구되는 기능을 수행할 수 있는 정도
- 사용성 : 지정된 사용 상황에서 효과성, 효율성 및 만족도를 가지고 지정된 목표를 달성하기 위해 사용자가 소프트웨어를 사용할 수 있는 정도
- 신뢰성 : 지정된 기간 동안 정해진 조건에서 소프트웨어가 요구되는 기능을 수행할 수 있는 정도
- 보안성 : 사용자 또는 타 소프트웨어에 허용된 권한의 종류 및 수준에 적합하게 데이터에 접근할 수 있도록 소프트웨어가 정보와 데이터를 보호하는 정도
- 유지보수성 : 유지 보수 자가 소프트웨어를 변경할 수 있는 효과성과 효율성의 정도
- 이식성 : 소프트웨어가 다른 하드웨어, 소프트웨어 등의 환경으로 옮겨질 수 있는 효과

성 및 효율성의 정도

－ 일반적 요구사항 : 제품 식별 및 표시 정보, 품질 특성별 정보 등을 제공하는 정도

㉔ 인증서



그림 41 소프트웨어품질인증서

② 조달청 우수 제품등록 완료



우수제품지정증서

지정번호 2019242

제 품 명 : 아토 액세스
업 체 명 : 아토리서치(주)
대표자명 : 정 재 용
지정기간 : 2019. 12. 30 ~ 2022. 12. 29
지정범위 : ATTO ACCESS v1.0

위 제품을 조달사업에관한법률
제9조의2 및 동법시행령 제18조에 따라
위와 같이 우수제품으로 지정합니다

2019년 12월 30일



조 달 청



그림 42 우수제품지정증서

(다) ETRI 시험인증

① 시험개요

과 제 명	SDN 기반 도로통신 네트워크 시스템 개발		
제 조 회 사	아토리서치(주)		
소프트웨어 버전	Obelle 2.4 + SDFAN		
하드웨어	SDN 제어기	OS : Ubuntu 16.04 12 Core CPU 64GB Memory	1대
	SDN 스위치	OpenFlow 1.3 지원 Model : ATTO-S1GF-8T8X4C Manufacturer: CENTEC L2 Industrial Switch	10대
시험기관	한국전자통신연구원, 박상길(042-860-5336)		
도입기관	한국도로공사		
적용 규격	과제 제안서 정량적 요구 사항		
비고	최초시험		

표 9 ETRI 인증시험 개요

② 주요 시험환경

㉠ SDN 스마트 네트워크 시험 환경

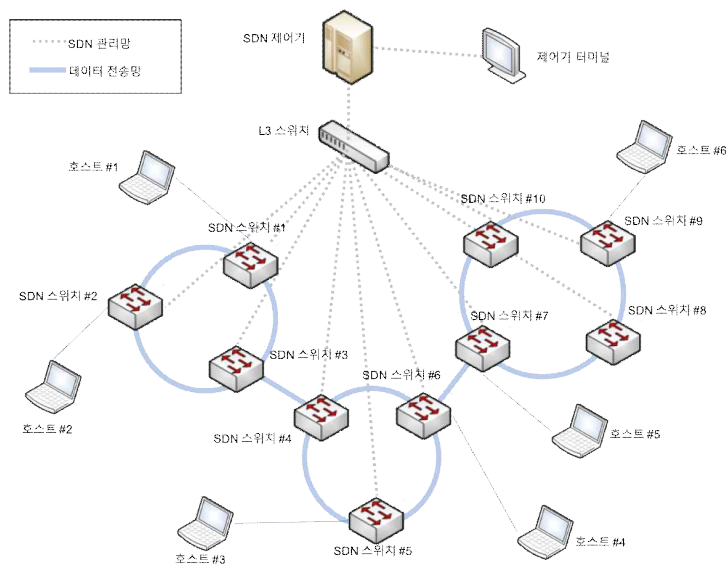


그림 43 인증 시험 환경 (스마트 네트워크)

장비 사양

장비명	규격	수량
SDN 제어기	Software : Obelle 2.4 + SDFAN OS : Ubuntu 16.04 12 Core CPU 64GB Memory	1
SDN 스위치	OpenFlow1.3 지원 Model :ATTO-S1GF-8T8X4C Manufacturer: CENTEC L2 Industrial Switch	10
L3 스위치	Model : ATTO-S1G-48T4X Manufacturer : CENTEC Switching Capacity : 176Gbps 1G-T Port : 48개 1/10G SFP+ Port : 4개	1
시험용 호스트 (호스트 #1 ~ 호스트 #5)	Raspberry PI 3B+ OS : Raspbian 4 Core CPU 1GB Memory	5
측정용 호스트 호스트 #6	MacBookPro OS : macOS Mojave 10.14.4 8 Core 2.8 GHz CPU 16GB Memory	1

표 10 인증 시험 장비 사양 (스마트 네트워크)

시험용/측정용 호스트 IP주소

장비명	IP 주소
시험용 호스트 #1	172.240250.101
시험용 호스트 #2	172.240250.102
시험용 호스트 #3	172.240250.103
시험용 호스트 #4	172.240250.104
시험용 호스트 #5	172.240250.105
측정용 호스트 #6	172.240250.106

표 11 시험 장비 IP 주소 목록 (스마트 네트워크)

㉠ 도로 통신 네트워크 보안 기술 시험 환경

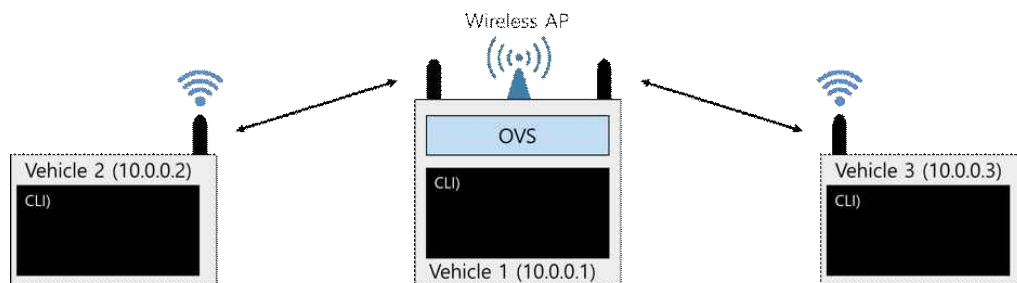


그림 44 도로 통신 네트워크 보안 기술 시험 환경

장비 사양

장비명	규격	수량
오드로이드 xu3		3
오드로이드 와이파이 모듈		3

표 12 도로 통신 네트워크 보안 기술 시험 장비 사양

③ 시험항목

연구 성과	단위성과	시험 항목	질적 성과지표	목표치	측정 방법
SDN기반 테스트베드	테스트 베드망 구축	지리적 거리 확인	지리적 거리	10km	iperf
	단말-관제 센터간 SDN통신	통신 지연 시간 측정 시험	지연시간	10ms	iperf
		대역폭 측정 시험	대역폭	900Mbps	iperf
SDN기반 트래픽 최적화 SW	트래픽 최적화 우선순위 지정 개수 대역폭 제한 단위	트래픽 최적화 우선 순위 시험	우선순위 개수	5개	iperf
		대역폭 제한 단위 시험	제한 단위	1Mbps	iperf
	트래픽 차단	차단 조건 개수		5개	아래 참조
		Destination MAC 주소 차단 시험	트래픽 차단 여부	차단	
		Source MAC 주소 차단 시험	트래픽 차단 여부	차단	
		Destination IP 주소 차단 시험	트래픽 차단 여부	차단	
		Source IP 주소 차단 시험	트래픽 차단 여부	차단	
		스위치 Port별 차단 시험	트래픽 차단 여부	차단	
도로통신 네트워크 보안기술	도로통신 네트워크 방어 전략	공격 종류 개수		5개	아래 참조
		도청 공격에 대한 방어 시험	공격에 대한 방어 여부	공격 무효화	
		블랙홀 공격에 대한 방어 시험	공격에 대한 방어 여부	공격 무효화	
		접근제어 시스템 오류 공격에 대한 방어 시험	공격에 대한 방어 여부	공격 무효화	
		서비스 거부 공격에 대한 방어 시험	공격에 대한 방어 여부	공격 무효화	
		브로드캐스트 이슈 공격에 대한 방어 시험	공격에 대한 방어 여부	공격 무효화	
도로통신 네트워크	네트워크 장애 발견	네트워크 장애 발견 시간 측정 시험	네트워크 장애 발견 시간 측정 시험	1초	로그파일 시간 차감
통합관제 SW	네트워크 장애 긴급 대응	네트워크 장애 대응 시간 측정 시험	네트워크 장애 대응 시간 측정 시험	1초	로그파일 시간 차감

표 13 인증 시험 항목

④ 시험 절차

㉔ 트래픽 최적화 우선순위 지정 개수

시험용 호스트 5대에 IPERF를 사용하여 최대치의 트래픽을 발생 시킨 후 트래픽 최적화 설정 후 트래픽 변화를 측정하여 설정한 대로 통신대역이 변하는지 시험함

- 시험용 호스트 5대의 터미널 (iperf 서버 실행)

```
attodev@sddc-test2:~$ iperf -s
-----
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
-----
```

그림 45 iperf 서버 실행 화면

- 측정용 호스트에 5개의 터미널을 띄우고 시험용 호스트 5대에 iperf 클라이언트로 접속

```
iperf -c 172.24.250.101 -i 1 -t 1000
-----
Client connecting to 172.25.255.102, TCP port 5001
TCP window size: 85.0 KByte (default)
-----
[ 3] local 172.24.250.106 port 43700 connected with 172.24.250.101 port 5001
[ ID] Interval      Transfer    Bandwidth
[ 3] 0.0- 1.0 sec   211 MBytes  1.77 Gbits/sec
[ 3] 1.0- 2.0 sec   242 MBytes  2.03 Gbits/sec
[ 3] 2.0- 3.0 sec   252 MBytes  2.11 Gbits/sec
[ 3] 3.0- 4.0 sec   185 MBytes  1.56 Gbits/sec
[ 3] 4.0- 5.0 sec   206 MBytes  1.73 Gbits/sec
[ 3] 5.0- 6.0 sec   204 MBytes  1.71 Gbits/sec
[ 3] 6.0- 7.0 sec   207 MBytes  1.74 Gbits/sec
[ 3] 7.0- 8.0 sec   220 MBytes  1.85 Gbits/sec
[ 3] 8.0- 9.0 sec   210 MBytes  1.76 Gbits/sec
[ 3] 9.0-10.0 sec   200 MBytes  1.68 Gbits/sec

iperf -c 172.24.250.102 -i 1 -t 1000
iperf -c 172.24.250.103 -i 1 -t 1000
iperf -c 172.24.250.104 -i 1 -t 1000
iperf -c 172.24.250.105 -i 1 -t 1000
```

그림 46 iperf 클라이언트 실행 화면

SDN 컨트롤러에서 호스트 5대에 대한 트래픽 우선순위를 아래와 같이 지정한 후 설정한 대로 대역폭이 변하는지 iperf를 이용하여 측정

순위	대상	IP 주소	할당 대역대
1순위	호스트 #1	172.24.250.101	100 Mbps
2순위	호스트 #2	172.24.250.102	10 Mbps
3순위	호스트 #3	172.24.250.103	1 Mbps
4순위	호스트 #4	172.24.250.104	100 Kbps
5순위	호스트 #5	172.24.250.105	10 Kbps

표 14 트래픽 우선순위 설정 내역

㉕ 대역폭 제한 단위

시험용 호스트 1대와 측정용 호스트 1대에 각각 iperf 서버와 iperf 클라이언트를 실행한다.

- 시험용 호스트

```
iperf -s
```

- 측정용 호스트

```
iperf -c 172.24.250.101 -i 1 -t 1000
```

SDN 컨트롤러에서 시험용 호스트에 대한 대역폭 제한을 1Mbps단위까지 단계적으로 조정해 나갈 때 iperf를 사용하여 실제 대역폭이 그대로 변하는지 측정함
1Gbps -> 2Mbps -> 1Mbps

㉔ 트래픽 차단 조건 개수

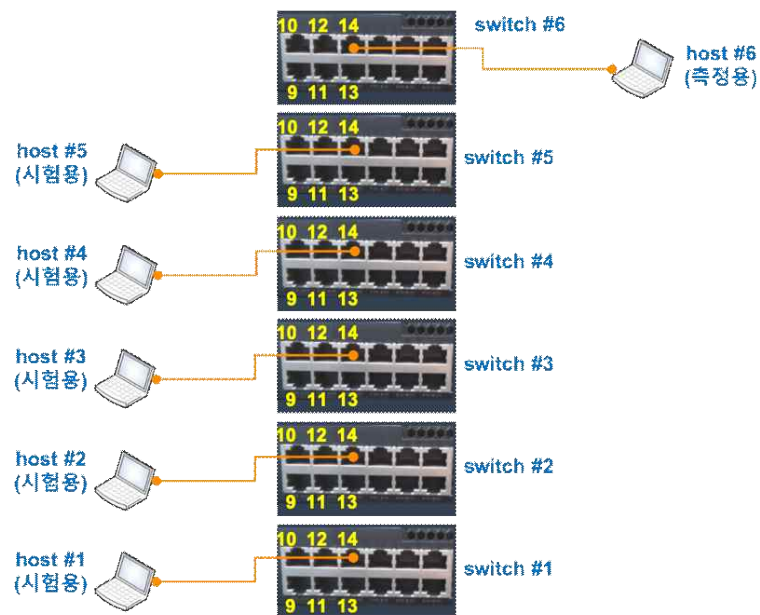


그림 47 시험환경 호스트 연결 상태

위의 그림처럼 시험환경에 시험용 호스트 5대를 연결한 후 아래의 순서대로 5가지 인증요소에 대해서 순차적인 트래픽 차단을 설정한다.

시험차수	차단용 인증요소	차단조건	차단대상
1차	Destination MAC주소	Destination MAC주소가 b8:27:eb:f7:39:e1인 호스트	시험용 호스트 #1
2차	Source MAC주소	Source MAC주소가 b8:27:eb:f7:39:e1인 호스트	시험용 호스트 #2
3차	Destination IP주소	Destination IP주소가 172.24.250.103인 호스트	시험용 호스트 #3
4차	Source IP주소	Source IP주소가 172.24.250.104인 호스트	시험용 호스트 #4
5차	특정 스위치 포트	5번 스위치의 14번 포트	시험용 호스트 #5

표 15 대역폭 제한 내역

차단을 설정한대로 해당 호스트의 트래픽이 차단되었는지는 iperf를 사용하여 대역대가 0이 되었는지 확인한다.

㉔ 네트워크 공격 및 방어 전략 개수

아래와 같이 차량 3대를 나타내는 3대의 오드로이드를 설치한다. 이 중에서 2대의 차량의 통신을 중계해주는 중계 차량에는 OVS가 추가로 설치되어 있다.

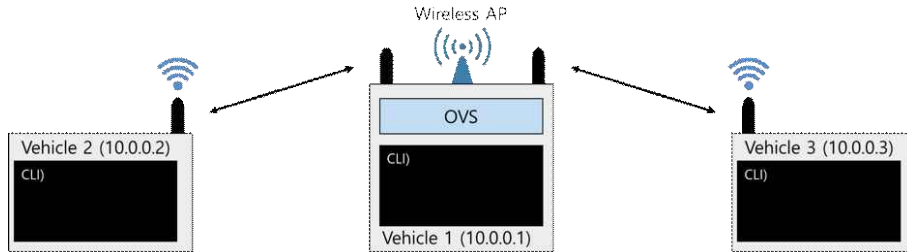


그림 48 네트워크 공격 및 방어 시험 환경

5가지 유형의 공격에 대해서 방어 전략이 없는 상태와 방어 전략을 가동한 상태가 아래와 같음을 확인한다.

공격 종류	방어 전략이 없는 상태	방어 전략을 가동한 상태
도청 공격	차량1에서 tcpdump로 차량2와 차량3이 주고받는 메시지를 원문의 형태로 볼 수 있음	차량2와 차량3이 주고받는 메시지가 암호화되어 내용을 알 수 없음
블랙홀 공격	차량2의 OVS에 잘못된 플로우 룰이 삽입되어 차량1과 차량2 사이의 통신이 단절됨	timeout으로 통신 단절이 감지되면 새로운 경로 설정으로 통신이 재개됨
접근제어 시스템 오류 공격	공격자인 차량2가 차량1에 접근하여 잘못된 플로우 룰을 설치함	공격자인 차량2가 차량1에 접근하려고 할 때 액세스 테이블을 참조하여 접근을 차단함
서비스 거부 공격	차량3이 차량2에 반복적인 메시지를 전송하여 차량2에서 이에 응답하기 위해 많은 자원 사용	차량1의 OVS가 특정 값 이상의 트래픽 감지시 소스(차량3)를 차단함
브로드캐스트 이슈 공격	차량 상호간의 패킷이 제3자에 의해서 그대로 보여짐	차량 상호간의 패킷이 암호화되어 제3자에 의해서 확인이 어려움

㉕ 네트워크 장애 발견 시간

- SDN 스위치 5번을 SDN 컨트롤러에 시간 동기화 시킨다(시험환경에서 SDN 컨트롤러의 IP는 172.18.192.73).

```
ntp server 172.18.192.73
```

- 스위치 4번과 스위치 5번 사이의 연결 케이블을 제거하여 장애 상황을 만듦

- 화면 프로그램에서 장애 발견 메시지가 발생하는 시간과 스위치 5번의 로그상의 네트워크 단절 시간이 1초 이내인지 확인

㉖ 네트워크 장애 대응 시간

- SDN 스위치 6번을 SDN 컨트롤러에 시간 동기화시킴

```
ntp server 172.18.192.73
```

- 아래와 같이 6대의 호스트의 IP를 설정하고 SDN 스위치에 연결함

호스트 명	호스트 IP	상위 스위치
호스트 1	172.24.250.101	스위치 1
호스트 2	172.24.250.102	스위치 2
호스트 3	172.24.250.103	스위치 3
호스트 4	172.24.250.104	스위치 4
호스트 5	172.24.250.105	스위치 5
호스트 6	미설정	스위치 6

- ifconfig명령으로 호스트 6번은 호스트 4번과 동일한 172.24.250.104로 바꾸어 IP 충돌 장애 상황을 만듦

- 화면 프로그램에서 문제해결 명령을 보내는 시간과 스위치 6번에 호스트 6번 차단 rule을 보내는 시간(스위치 로그에서 확인)이 1초 이내임을 확인

⑤ 시험 결과

- 시험성적서 발급 완료.
- 전항목 만족.

시 험 성 적 서							
한국전자통신연구원 34129 대전광역시 유성구 가정로 218 Tel : 042-860-6114 Fax : 042-860-5083	성적서 번호 : ETRI-2019-3000-181 페이지(1)/(총 3) 한국전자통신연구원 Electronic and Telecommunications Research Institute						
1. 의뢰자 ○ 기 관 명 : 아토리체시㈜ ○ 주 소 : 경기도 성남시 분당구 대왕판교역로 225-18							
2. 시험성적서의 용도 ○ 과제연구결과물 관리기관 제출							
3. 시험대상품목/물질/시료 설명 : ○ SDN제어기, L3스위치, SDN스위치, 시험용 호스트, 측정용 호스트, 오드로이드-XU3							
4. 시험기간 : 2019. 11. 11. ~ 11. 12.							
5. 시험방법 : SDN 기반 도로통신 네트워크 시스템 개발 시험절차서 (NSQT-19-RNDT-0089)							
6. 시험결과 : 시험 요약서, 시험 결과 요약서 및 시험 결과서 참조							
이 성적서는 의뢰자가 제시한 시료 및 시료명에만 한정되며, 용도 이외의 사용을 금합니다.							
확 인	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">시험자</th> <th style="width: 50%;">승인자</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;"> 성 명 : 박 상 길 (서명) </td> <td style="padding: 5px;"> 직 위 : 센터장 </td> </tr> <tr> <td style="padding: 5px;"></td> <td style="padding: 5px;"> 성 명 : 남 기 동 (서명) </td> </tr> </tbody> </table>	시험자	승인자	성 명 : 박 상 길 (서명)	직 위 : 센터장		성 명 : 남 기 동 (서명)
시험자	승인자						
성 명 : 박 상 길 (서명)	직 위 : 센터장						
	성 명 : 남 기 동 (서명)						
한국전자통신연구원장 2019 년 11 월 21 일 (관인)							

(나) 시연/외부 전문가 평가 (안)

① 시연용 테스트 베드 - 구축 완료

㉔ 시연 환경 개요도

현재 경부/영동선 고속도로에 SDN 네트워크로 구현된 테스트 베드가 운용 중임. 궁내동 센터에 전체 네트워크를 제어하는 SDN 컨트롤러가 설치되어 있고 고속도로를 따라 SDN 스위치들이 설치되어 네트워크를 구성하고 있음. 시연은 궁내동 센터 주변 SDN 스위치들과 무선 AP를 통하여 시연용 차량/단말기들을 연결하여 진행 예정.

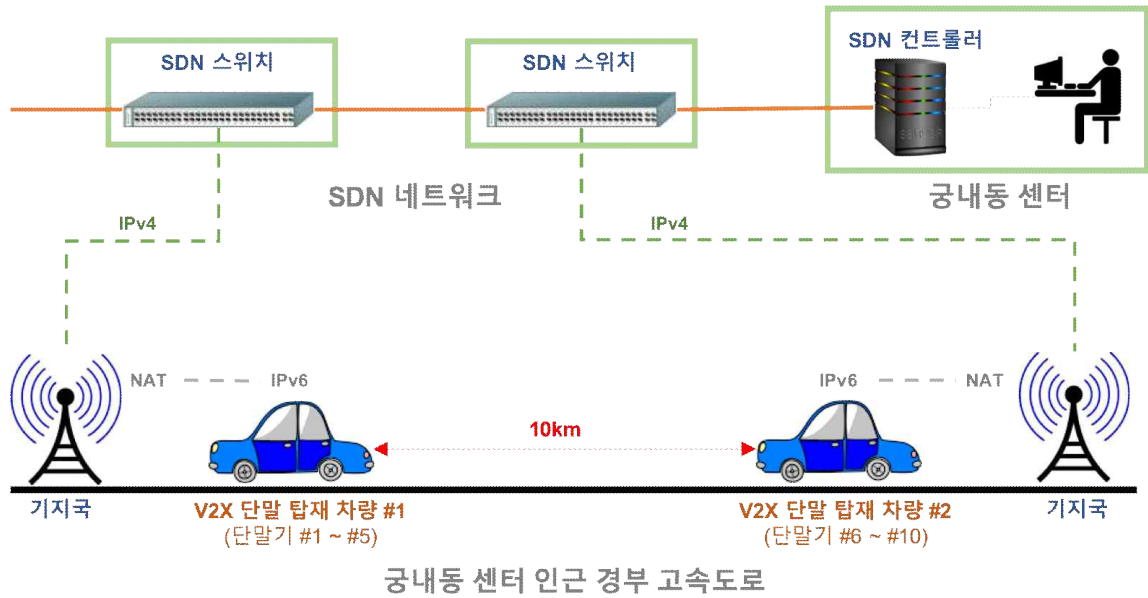


그림 49 외부 전문가 평가 시험 환경

㉠ 시연용 장비 내역

기존에 구축된 경부/영동선 SDN 네트워크 테스트베드(컨트롤러 1대, SDN 스위치 50대) 이외에 아래와 같은 시연 장비가 필요함

장비명	규격	수량
실험용 차량	무관	2
V2X 무선통신 단말기		10

② 시연 내용

시연 항목	시연 세부 내용	목표치	시연 장소
단말기 접속 시험	차량/단말기 동시 접속 수량 시험	10대	공내동 센터
통신 지연 시간 시험	네트워크 내 통신 지연 시간 확인	100ms	공내동 센터
지리적 거리 시험	차량 간 통신이 가능한 지리적 거리에 대한 시험	10km	공내동 센터
트래픽 차단 시험	보안상 문제를 발생시키는 차량에 대한 차단 시험	차단 여부	공내동 센터

③ 시연 방법

㉡ 단말기 접속 시험

위의 시연 환경 개요도에서와 같이 단말기 5대씩 탑재된 차량 총 2대(단말기는 총 10대)를 공내동 센터 인근 경부 고속도로에서 주행시킴. 단말기들이 기지국에 접속이 되면 공내동 센터에서 LDM 서버의 GUI상에서 차량 10대로 보이는지 확인



그림 50 LDM 서버 GUI 화면

㉔ 통신 지연 시간 시험

궁내동 센터에서 SDN 컨트롤러에 터미널로 접속하여 각 단말기가 접속한 기지국들에 ping 테스트를 실시함. 5회 실시 후 ping 응답 시간의 평균값이 100ms이하로 측정되는지 확인함(실제 시연환경에서는 기지국의 IP가 아래와 다를 수 있음)

기지국 #1

```
64 bytes from 172.24.250.101: icmp_seq=63011 ttl=64 time=0.417 ms
64 bytes from 172.24.250.101: icmp_seq=63012 ttl=64 time=0.367 ms
64 bytes from 172.24.250.101: icmp_seq=63013 ttl=64 time=0.393 ms
64 bytes from 172.24.250.101: icmp_seq=63014 ttl=64 time=0.379 ms
64 bytes from 172.24.250.101: icmp_seq=63015 ttl=64 time=0.395 ms
```

기지국 #2

```
64 bytes from 172.24.250.102: icmp_seq=63525 ttl=64 time=0.388 ms
64 bytes from 172.24.250.102: icmp_seq=63526 ttl=64 time=0.349 ms
64 bytes from 172.24.250.102: icmp_seq=63527 ttl=64 time=0.354 ms
64 bytes from 172.24.250.102: icmp_seq=63528 ttl=64 time=0.354 ms
64 bytes from 172.24.250.102: icmp_seq=63529 ttl=64 time=0.385 ms
```

그림 51 무선 기지국 ping 테스트 화면

㉕ 지리적 거리 시험

2대의 차량에서 탑승자가 스마트폰/노트북 등을 사용하여 구글맵(maps.google.co.kr)에 접속한 후 마우스 오른쪽을 클릭하여 “What’s here?” 메뉴를 선택하여 각각의 차량 GPS 좌표를 얻어옴. 두 차량의 좌표를 구글맵의 검색 창에 각각 입력하고 “Measure distance”와 “Distance to here”메뉴를 선택하여 두 차량의 거리가 10km이상임을 확인한다.

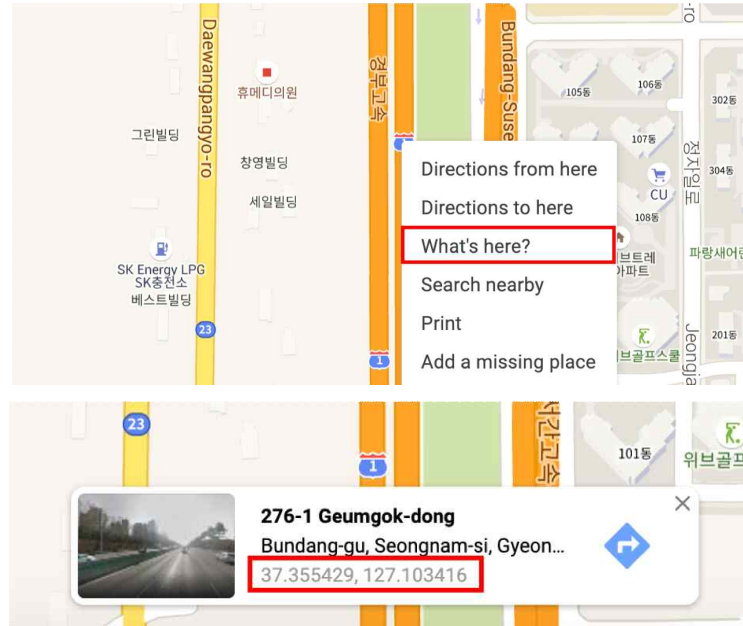


그림 52 차량 간 거리 측정 방법

㉔ 트래픽 차단 시험

단말기 10대 중 한 대를 공격자로 가정하고 컨트롤러에서 해당 단말기가 연결된 기지국의 트래픽을 차단한다. 컨트롤러의 단말기에서 차단하고자하는 기지국에 ping 테스트를 하면서 차단 설정 후 ping이 도달하지 않음을 확인함(실제 시연환경에서는 기지국의 IP가 아래와 다를 수 있음)

```

64 bytes from 172.24.250.101: icmp_seq=61930 ttl=64 time=0.377 ms
64 bytes from 172.24.250.101: icmp_seq=61931 ttl=64 time=0.411 ms
64 bytes from 172.24.250.101: icmp_seq=61932 ttl=64 time=0.532 ms
64 bytes from 172.24.250.101: icmp_seq=61933 ttl=64 time=0.420 ms
64 bytes from 172.24.250.101: icmp_seq=61934 ttl=64 time=0.515 ms
64 bytes from 172.24.250.101: icmp_seq=61935 ttl=64 time=0.501 ms
64 bytes from 172.24.250.101: icmp_seq=61936 ttl=64 time=0.468 ms
64 bytes from 172.24.250.101: icmp_seq=61937 ttl=64 time=0.478 ms
64 bytes from 172.24.250.101: icmp_seq=61938 ttl=64 time=0.543 ms
64 bytes from 172.24.250.101: icmp_seq=61939 ttl=64 time=0.495 ms
64 bytes from 172.24.250.101: icmp_seq=61940 ttl=64 time=0.395 ms
64 bytes from 172.24.250.101: icmp_seq=61941 ttl=64 time=0.447 ms
64 bytes from 172.24.250.101: icmp_seq=61942 ttl=64 time=0.368 ms
64 bytes from 172.24.250.101: icmp_seq=61943 ttl=64 time=0.366 ms
no answer yet for icmp_seq=61944
no answer yet for icmp_seq=61945
no answer yet for icmp_seq=61946
no answer yet for icmp_seq=61947

```

트래픽 차단 후

그림 53 트래픽 차단 ping 테스트 화면

④ 외부 전문가 평가서

외부 전문가에게 아래의 양식으로 연구개발의 성과를 평가하도록 함. 외부전문가 평가서는 별도로 첨부.

㉠ 평가지표

평가 항목	평가지표	배 점	평가 점수	평가 등급	평가지표 설명
연구 개발 수행	연구의 배경 및 목적	10			• 연구의 배경 및 필요성, 목적 및 범위가 사업 방향과 일치하는지를 평가
	기존 기술과의 차별성 및 우수성 확보 여부	10			• 기존 네트워크 기술과 차별화 되는 기술인지 평가
	연구성과물의 활용 및 사업화 가능성	10			• 과제 완료 후에 사업화하여 매출 발생 가능성이 있는가를 평가
연구 개발 성과 (시연)	다수 차량/단말 운영성	20			• 10대의 단말이 동시 운영 가능한지 평가
	다양한 종류의 서비스 지원 여부	15			• 실제 도로에 구축된 SDN 기반 네트워크에서 다양한 서비스 트래픽을 지원하는지 평가
	장비 장애에 대한 가용성	10			• 장비 장애에도 전체 시스템이 운영 가능한지 평가
	네트워크 공격에 대한 방어 기능	15			• 장애 유발 공격에 대한 원격 방어가 가능한지 평가
	과부하 트래픽 제어	10			• 과부하 트래픽에 대한 제어가 가능한지 평가
합 계		100			

*등급: S(100-91), A(90-81), B(80-71), C(70-61), D(60-0)

㉠ 평가진행 세부사항

- 일시: 2019. 12. 12.
- 장소: 자율협력주행 통합운영센터 (궁내동)
- 참석인원: 연구책임자 및 참여연구원 (5명), 네트워크/IT 전문가 평가위원 (3명)
- 시간대별 진행내용

시간	내용
13:00-13:05	인사말
13:05-13:15	과제개요 및 평가절차 설명
13:15-13:35	과제 성과 발표 및 질의응답
13:35-13:45	coffee break
13:45-14:15	현장 시연
14:15-14:30	평가표 작성
14:30-14:50	최종 평가의견
14:50-15:00	평가결과 정리 및 종료

- 평가위원 약력 (가나다 순)

No	성명	약력
1	백송기	KT IP 운용센터 부장 대한민국산업현장교수 정보통신기술사 공주대학교 대학원 박사과정
2	이승준	(주) 가교통신기술 대표이사 강원도립대학 겸임교수 대한민국산업현장교수 정보통신기술사 (사) 정보통신기술사회 부회장
3	황인준	고려대학교 전기전자공학부 교수

㉔ 평가결과

평가 항목	평가지표	배 점	위원1	위원2	위원3	평균	등급
연구 개발 수행	연구의 배경 및 목적	10	97	95	93	95	S
	기존 기술과의 차별성 및 우수성 확보 여부	10	95	95	88	93	S
	연구성과물의 활용 및 사업화 가능성	10	95	90	87	91	S
연구 개발 성과 (시연)	다수 차량/단말 운영성	20	91	90	94	92	S
	다양한 종류의 서비스 지원 여부	15	92	90	89	90	A
	장비 장애에 대한 가용성	10	95	90	87	91	S
	네트워크 공격에 대한 방어 기능	15	95	89	92	92	S
	과부하 트래픽 제어	10	95	95	86	92	S
합 계		100					S

*등급: S(100-91), A(90-81), B(80-71), C(70-61), D(60-0)

	평가의견	평가의견 반영방향
1	SDN 기반 지능형 도로 제어 네트워크 구현 및 관제 네트워크 사업화 성과가 우수함. 국내/국외 기술특허 를 획득하고, GS인증, 조달평가 인증을 수행하는 등 사업화 및 프로젝트 성과가 우수함. 향후 도로 네트 워크 통합 및 신기술과의 접목 시 성과가 기대됨	

2	사업화 가능성 및 미래 활용 가능성이 높은 개발과 제임. 다양한 도로이용 장비의 예측을 고려한 보안 및 예상 상황을 조금 더 고려하시면 상당히 훌륭한 성과물이 되리라고 예상함.	
3	시연에서 개발한 관제 기능은 제대로 작동되는 것을 확인했으나 시연 시나리오가 다소 단순하여 성능확인을 위한 좀 더 다양한 시나리오 구상 필요.	더 복잡한 시나리오로 관계자 및 전문가 피드백 기회 마련 예정

3. 목표 달성도 및 관련 분야 기여도

가. 목표

(1) 최종 성과별 점검기준

구분	핵심성과 (level1)		단위성과 (level2)		최종 성과점검기준					해당 기관	예산 (백만원)	양적 성과목표
					질적 성과지표	목표치	측정방 법	검증방 법	기준 치			
총괄	A	SDN기반 테스트베 드	A-1	테스트베드망 구 축	① 차질거리	10km	지도 서비스	보고서	2	아토리 서치		
			A-2	단말-관제센터간 SDN통신	① 지연시간	100ms	ping	보고서	1			
					② 대역폭	900M bps	iperf	보고서	1			
	B	SDN기반 트래픽 최 적화 SW	B-1	우선순위 지정	① 우선순위 개수	5개	iperf	동영상	1	아토리 서치		특허: 출원 2 건 시제품: 1 건 SW: 3 건
			B-2	대역폭 제한	① 제한 단위	1Mbps	iperf	동영상	2			
			B-3	트래픽 차단	① 차단 조건 개 수	5개	iperf	동영상	2			
	C	도로통신 네트워크 보안 기술	C-1	도로통신 네트워크 공격 발굴 및 방어 전략	① 공격 종류 개 수	5개	직접 공격	동영상	2	아토리 서치		특허: 출원 1 건 특허: 등록 1 건
	D	도로통신 네트워크 통합관제 S W	D-1	네트워크 장애 발 견	① 발견 시간	1초	장애 발생 및 발견 시각 측정	시제품 시연	2	아토리 서치		특허: 출원 1 건 시제품: 1 건 SW: 1 건
			D-2	네트워크 장애 긴 급 대응	① 대응 시간	1초	대응 명령 입력 후 실행 시각 측정	시제품 시연	2			
	E	신기술 인 증	E-1	시범운용	① 다수 차량/단 말 동시 운용	10대	정상 관제 확인	평가서	1	아토리 서치		특허: 출원 1 건 특허: 등록 1 건 기타 시범운영보고서 1건 기타 시험성적서 1건 기타 신기술인증 1 건
			E-2	공인인증 기관 시 험	① 공인인증 기관 의 시험 검증	1건	시험성 적서	시험성 적서	2			
			E-3	신기술 인증	① 신기술 인증	1건	인증서	인증서	2			
계									20			특허: 출원 5 건 특허: 등록 2 건 시제품: 2 건 SW: 4 건 기타 시범운영보고서 1건 기타 시험성적서 1건 기타 신기술인증 1건

나. 목표 달성여부

(가) 연구개발 수행 결과

본 연구개발의 3차년도 까지 최종성과점검기준표에서 질적 성과지표 중 A항목(SDN기반 테스트 베드)의 전부와 E-2(공인인증 기관 시험), E-3(신기술 인증) 항목을 만족하였음. 또한 B항목(SDN기반 트래픽 최적화 SW), C항목(도로통신 네트워크 보안 기술), D항목(도로통신 네트워크 통합관제 SW)은 ETRI 인증시험을 통해, E-1항목(시험운용)은 외부 전문가 시험 및 평가를 통해 검증하였음.

양적 성과목표와 관련해서는 특허 5건을 출원하여 3건은 등록되었으며, S/W 저작권은 4건 등록하였음.

구분	핵심연구 과 (level1)	단위 성과 (level2)	최종 성과점검기준						해당 기관	장량목표	결과		
			질적 성과지표	목표치	측정방법	검증방법	가중치						
총괄	A	반 테스트 베드	A-1	테스트베드망 구축	①	지리적 거리	10km	지도서비스	보고서	2	아토 리서 치	10km	13.25km 이상
				단말-관제센터	①	지연시간	100ms	ping	보고서	1		100ms	1.5ms
			A-2	터간 SDN통신	②	대역폭	900Mbps	iperf	보고서	1		900Mbps	910Mbps
	B	반 트래픽 최적화 SW	B-1	우선순위 지정	①	우선순위 개수	5개	iperf	동영상	1	아토 리서 치	5개	5개
			B-2	대역폭 제한	①	제한 단위	1Mbps	iperf	동영상	2		1Mbps	1Mbps
			B-3	트래픽 차단	①	차단 조건 개수	5개	iperf	동영상	2		5개	5개
	C	도로통신 네트워크 보안 기술	C-1	도로통신 네트워크 방어 전략	①	공격 종류 개수	5개	직접 공격	동영상	2	아토 리서 치	5개	5개
	D	도로통신 네트워크 통합관제 SW	D-1	네트워크 장애 발견	①	발견 시간	1초	장애 발생 및 발견 시각 측정	시제품 시연	2	아토 리서 치	1초	0.525초
			D-2	네트워크 장애 긴급 대응	①	대응 시간	1초	대응 명령 입력 후 실행 시각 측정	시제품 시연	2		1초	0.22초
	E	신기술 인증	E-1	시험운용	①	다수 차량/단말 동시 운용	10대	정상관제확인	동영상	1	아토 리서 치	10대	10대
			E-2	공인인증 기관 시험	①	공인인증 기관의 시험 검증	1건	시험성적서	시험성적서	2		1건	1건
			E-3	신기술 인증	①	신기술 인증	1건	신기술 인증	인증서	2		1건	1건
	계									20		특허: 출원 5 건 특허: 등록 2 건 시제품: 2 건 SW: 4 건 기타: 시험운용보고서 1건 기타: 시험성적서 1건 기타: 신기술인증 1건	특허: 출원 5 건 특허: 등록 3 건 시제품: 2 건 SW: 4 건 기타: 시험운용보고서 1건 기타: 시험성적서 1건 기타: 신기술인증 1건

상세 추진일정에 따라 세부추진개발이 이루어졌으며, Activity별 문서산출물도 모두 완료했음

① 1차 년도 추진일정

구분	연구과제명 (연구수행기관)	세부추진내용 (연구수행 Activity)	Activity별 산출물	1차년도			
				1/4	2/4	3/4	4/4
주관	아토리서치(주)	ITS네트워크 문제점 파악	ITS네트워크 분석 보고서				
		네트워크 요구사항 도출					
		SDN 테스트베드 구축 계획 수립	SDN기반 테스트베드				
		SDN 테스트베드 구축					
공동 위탁	한국도로공사 한국과학기술원	SDN 지연시간 검증	SDN 망 테스트 결과서				
		SDN 대역폭 검증					
		네트워크 요구사항 분석					
		도로통신 네트워크 공격 정보 수집 및 분석	도로통신 네트워크 공격 분석 보고서				
		도로통신 네트워크 공격 도출					

② 2차 년도 추진일정

구분	연구과제명 (연구수행기관)	세부추진내용 (연구수행 Activity)	Activity별 산출물	2차년도			
				1/4	2/4	3/4	4/4
주관	아토리서치(주)	서비스 별 우선순위 설계	SDN기반 트래픽 최적화 SW				
		SDN 대역폭 제한 단위 검증					
		서비스 별 대역폭 제한 개발					
		트래픽 차단 조건 선정					
		트래픽 차단 기능 개발					
		트래픽 최적화 테스트	도로통신 네트워크 방어 시스템				
		도로통신 네트워크 방어 시스템 개발					
		도로통신 네트워크 공격 실증 테스트					
		네트워크 관제 GUI 개발					
		네트워크 관제 이벤트 연동					
공동 위탁	한국도로공사 한국과학기술원	네트워크 장애 테스트	도로통신 네트워크 통합관제 SW				
		네트워크 장애 긴급 대응 기능 개발					
		네트워크 장애 긴급 대응 테스트					
		네트워크 서비스 분류					
		네트워크 관제 UX 요구사항 분석					
		도로통신 네트워크 방어 연구	도로통신 네트워크 방어 연구 보고서				
		도로통신 네트워크 방어 시스템 개발					

③ 3차 년도 추진일정

구분	연구과제명 (연구수행기관)	세부추진내용 (연구수행 Activity)	Activity별 산출물	3차년도			
				1/4	2/4	3/4	4/4
주관	아토리서치(주)	시범도로 확대 운영	월간 운영 보고서				
		GS 인증 시험 진행	GS 인증서				
		조달청 우수제품 등록	우수제품지정증서				
		ETRI 인증 시험 진행	ETRI 시험 성적서				
		외부 전문가 평가 진행	외부 전문가 평가서				
공동 위탁	한국도로공사 한국과학기술원	시범도로 운영	월간 회의록				
		ETRI 인증 시험 진행	ETRI 시험 성적서				

(나)연구 목표 달성도

세부 연구 목표 (연구계획서의 목표)	비중 (%)	달성도 (%)	자체평가
SDN기반 테스트베드	20	100	이미 구축되어 있는 Legacy 스위치 망과 함께, SDN 스위치 및 SDN 제어기로 구성된 SDN 기반 도로통신 네트워크를 성공적으로 구축 - 경부/영동선 고속도로에 적용 완료 - 외부 전문가 입회하에 V2X 단말기 탑재 차량 운용으로 성능 및 안정성 테스트 완료
SDN 기반 트래픽 최적화 SW	25	100	- 우선순위 기능 구현 완료 - 대역폭 제한 구현 완료 - 트래픽 차단 구현 완료 - 영동 고속도로 실제 망에 적용 및 테스트 완료 자율협력주행 사업에서 사용할 네트워크 인프라를 SDN망으로 완벽히 대체하여, 실제 도로 네트워크 트래픽을 SDN으로 운영
도로통신 네트워크 보안 기술	10	100	- 5가지 공격 및 방어 전략 도출 완료 (Broadcast, DoS, 블랙홀, 도청, 접근제어 오류 - 보안이 강화된 새로운 도로통신 네트워크 제안 (가상화, 인증, 제어 센터) 도로통신 네트워크 공격에 대한 보안 방안을 제시 완료
도로통신 네트워크 통합 관제 SW	20	100	- 영동 고속도로 구간 모델링 완료 - 도로 장비 정보 수집 시스템 구현 완료 - 도로 장비 장애 대응 시스템 구현 완료 영동/여주 구간 자율협력주행 네트워크 및 장비를 실시간 모니터링 가능한 시스템 구축 완료.
신기술 인증	25	100	- 특허 출원 및 등록 목표 달성 - S/W 저작권 등록 4건 완료 - GS 인증 획득 완료 - 조달청 우수제품 지정 획득
합계	100점		

(다) 정량적 연구 성과 목표 및 달성도

구분		목표	달성도(%)	비고
국외 논문 게재	SCI			
	비SCI			
	계			
국내 논문 게재	SCI			
	비SCI			
	계			
특허 출원	국내	5	100%	
	국외			
	계	5	100%	
특허 등록	국내	3	150%	
	국외			
	계	3	150%	
인력 양성	석사			
	박사			
	계			
기술 이전	계약 건수			
	계약액			
	징수액			
국제 표준화	기고서 제출			
	기고서 채택			
	표준안 채택			
국내 표준화	기고서 제출			
	기고서 채택			
	표준안 채택			
등록·기탁 대상 성과물	보고서 원문			
	연구시설·장비			
	기술요약정보			
	생명자원	생명정보		
		생물자원		
		신품종		
	소프트웨어		4	100%
기타	화학물			
	시제품		2	100%
	성과 홍보			
	일자리 창출			

(라) 연구개발성과

(1) 지식재산권(특허, 실용신안, 의장, 디자인, 상표, 규격, 신품종, 프로그램)

번호	지식재산권 등 명칭 (건별 각각 기재)	국명	출원			등록		기 여 율
			출원인	출원일	출원번호	등록일	등록번호	
1	소프트웨어 정의 네트워크에서 호스트 상태 정보를 확인하는 방법, 장치 및 컴퓨터 프로그램	대한민국	김지원 황인옥 송용주	2017-09-13	10-2017-0117103	2018-12-14	10-1931139	100%
2	SDN 및 NFV를 이용한 도로 교통 네트워크의 보안 서비스 제공 시스템 및 그 방법	대한민국	신승원 우승원 김연근	2018-04-02	10-2018-0038069			100%
3	소프트웨어 정의 네트워크에서 패킷의 경로를 설정하는 방법, 장치 및 컴퓨터 프로그램	대한민국	신규식 황인옥 손우진 박현우 송용주	2018-09-06	10-2018-0106280	2019-09-17	10-2023901	100%
4	소프트웨어 정의 네트워크에서 네트워크 장비를 인식하는 방법, 장치 및 컴퓨터 프로그램	대한민국	박현우 송용주 황인옥	2018-11-06	10-2018-0135037	등록결정	등록결정	100%
5	소프트웨어 정의 네트워크에서 가상 네트워크를 제공하는 방법, 장치 및 컴퓨터 프로그램	대한민국	신규식 황인옥	2019-10-04	10-2019-0122865			100%

(2) 저작권(소프트웨어, 서적 등)

번호	저작권명	창작일	저작자명	등록일	등록 번호	저작권자명	기여율
1	3D 도로공사 자율주행자동차 관제 클라이언트	2018-09-30	아토리서치 주식회사	2018-10-18	C-2018-027847	아토리서치 주식회사	100%
2	SDN(소프트웨어 정의 네트워킹)기반 도로망 L2스위칭 어플리케이션	2018-08-30	아토리서치 주식회사	2018-10-18	C-2018-027848	아토리서치 주식회사	100%
3	네트워크 응답 지연시간 측정 어플리케이션	2019-09-23	아토리서치 주식회사	2019-09-27	C-2019-026625	아토리서치 주식회사	100%
4	SDN 로그 기반 네트워크 상태 분석 어플리케이션	2019-09-23	아토리서치 주식회사	2019-09-27	C-2019-026626	아토리서치 주식회사	100%

4. 연구개발성과의 활용 계획 등

가. 사업화 전략

(1) 시장 전망

- 4차 산업혁명으로 대표되는 신기술/산업 패러다임 - 5G, IoT, 가상현실/증강현실, UHD/4K, 인공지능, 머신 러닝, Bio, Big Data -는 기존의 네트워크상에서는 서비스 제공이 불가하며 SDN/NFV와 같은 새로운 네트워크 구조가 필수임
- 도로교통에서도 자율주행, 자율도로, 차량 간 통신(V2V) 등 새로운 기술이 등장하였으며, 특히 현재 추진 중인 C-ITS는 차량의 상태 정보 공유(1단계), 차량에서 수집된 정보 공유(2단계), 차량 운전자의 의도 공유(3단계)를 실현하는 고도의 기술로서 단계가 진화할수록 대용량의 정보 처리를 요구함
- 이번 연구를 통해 SDN/NFV 기반의 네트워크 시스템이 시험도로에 적용이 완료되면 고속도로 전체 및 일반도로까지 확산하는 것을 목표로 함.
- 도로교통의 지능화/고도화는 Smart City와도 밀접한 관련이 있는데, SDN 기반 도로통신 네트워크 시스템은 Smart City 환경에 필수적인 네트워크 인프라 및 보안 기능을 제공하기 때문임.
- 국내 Smart City는 현재 정부에서 추진 중인 U-City (유비쿼터스 시티) 조성 사업이 있으며 본격적으로 Smart City 시장이 열리는 2020년까지 시장에 선 진입하여 경쟁력 확보에 유리함. 세종시, IFEZ(인천자유경제구역), 안양시, 대전시가 지자체로서 U-City를 구축한 대표 사례이며, 하기와 같은 조성 사업이 진행 중.

국내 U-City 현황

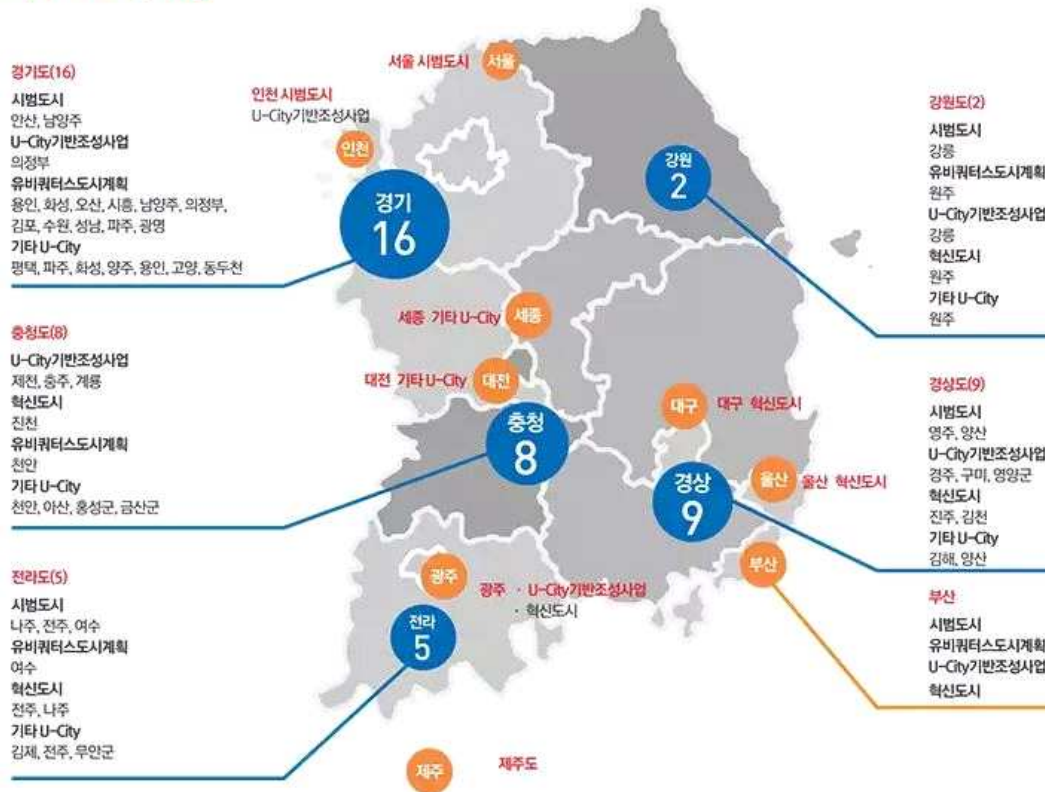


그림 54 국내 U-City 현황

출처: http://www.u-city.or.kr/kr/mp07_ucity/trend.php

- SDN 기반 도로통신 네트워크 시스템은 C-ITS, Smart City를 넘어 IoT 환경에서도 기존 Legacy 방식에 비해 기술적, 경제적으로 월등한 효과가 전망되고 있으며, 특히 국제 인터넷 표준화 기구(IETF, Internet Engineering Task Force)는 IoT 망에서 수용될 수많은 이 기종 디바이스의 end-to-end 연동에 대해 SDN/NFV를 권고함
- Smart City, IoT 환경에서는 수집될 정보의 양, 디바이스/프로토콜의 종류가 폭발적으로 증가하며 보안 위협도 증대됨. 기존의 Legacy 네트워크에서는 이에 대한 효과적인 대응이 불가함
- Smart City와 밀접하게 연관되는 IoT(사물인터넷)은 시장규모가 2022년까지 국내에서만 약 23조원까지 성장할 것으로 예상됨



◇ (자료=미래부)

그림 55 국내 사물인터넷 시장 규모 전망

(2) 단계별 사업화 전략



그림 56 단계별 사업화 전략

- 본 사업의 연구기간인 2017년~2019년은 개발기로서 SDN 기반 도로통신 네트워크 시스템을 개발하고 실증하여 신기술 인증까지 획득하는 전략으로 상용화 준비를 충실히 마칩
- 본 사업이 종료된 2020년~2023년은 C-ITS 및 자율협력주행 인프라가 본격적으로 확산되는 시기. 국토교통부에서도 2030년까지 완전 자율협력주행을 실현하기 위해서 도로 인프라를 확충하는 상태.
- 경부/영동 자율협력주행 테스트베드와 대전-세종 C-ITS시험 사업 구간에서의 실증 실적을 바탕으로, 2023년까지는 고속도로에 '신규'로 구축되는 도로통신 네트워크를 모두 SDN화 하는 것을 목표로 함. 고속도로 인프라의 확충은 본 사업의 참여기관 이며 수요기관인 한국도로공사가 담당하기 때문에 가능한 목표

- 2024년 부터는 고속도로 인프라 실적을 바탕으로 스마트 시티와 같은 일반 도로 시스템에도 본격적으로 진출. 자율협력주행 표준 인프라 가이드라인에 SDN을 필수로 명시함으로써 시장 확대를 추진. 당사가 모든 시장을 가져갈 수는 없겠지만, 최소한 자율협력주행을 위한 네트워크 인프라는 SDN기술로 구성되도록 사업화 전략을 구성

(3) 도로통신 네트워크 시스템의 제품화

(가) 개발기술의 생산특성

- ① 생산형태 : 완제품
- ② 제품명 : SDN 기반 도로통신 네트워크 시스템
- ③ 제품 구성

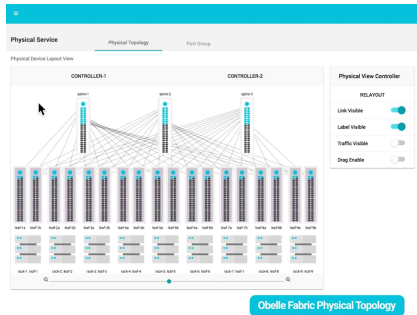
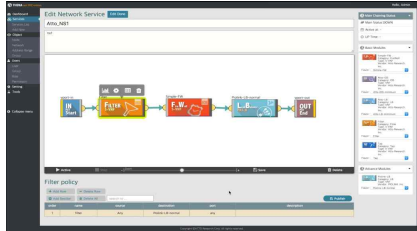
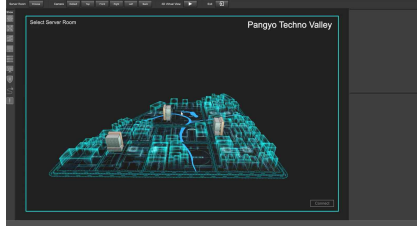
제품 구성		용도	예상 가격 (천원)	제품 형상(예시)
SDN 네트 워크	SDN기반 트래픽 최적화 SW	SDN 스위치를 중앙 관리/제어	100,000	
	SDN 스위치	도로교통정보를 SDN으로 전달	4,000/대	
보안	도로통신 네트워크 보안 시스템	NFV 기반 보안 기능 제공	50,000/대	
통합 관리	도로통신 네트워크 통합 관제 SW	네트워크 통합 관리/시각화	200,000	

표 16 판매 제품 구성 및 가격

④ 예상 핵심 원재료 및 특성

형태	원재료명	가격(천원)	조달 특성
서버	X86 서버	10,000/대	- 범용 x86 서버 - OS: Linux Cent OS 7 - 사양: xeon E5, 2 socket - 조달기간: 국내 재고(1주 이내) - 조달용이성: 용이(양산품)
스위치	SDN 스위치	4,000/대	- Open Flow를 지원하는 White Box 스위치 - 사양: 1Gbps SFP 24 port 이상 - 조달기간: 국내 재고(1주 이내) - 조달용이성: 용이(양산품)

표 17 핵심 원재료 및 특성

⑤ 생산 규모 및 예상 Lead-Time

- 생산규모 : 소규모
- 예상 제품 조달 기간 : 2주 이내
 - . 원재료 조달 기간 : 7일 이내
 - . 아토리서치 소프트웨어 설치 : 3일 이내
 - . QA 검증 : 4일 이내

(나) 기존 사업아이템을 R&D과제에 활용할 수 있는 연관정도

- ① 기존 생산라인(설비포함) 예상 활용정도(90 %) 및 근거
- ② 원재료 및 개발설비 공용화정도(80 %) 및 근거

- 아토리서치(주)는 SDN/NFV의 선도 기업으로써 스탠포드 연구소 (Stanford Research Institute), KAIST, 서울대학교 차세대 융합기술원, 오키나와 오픈 랩 (Okinawa Open Laboratory), 한국전자통신연구원 (ETRI)등 국내외 유수의 연구 기관과 기술 연구 실적을 진행한 바 있음
- 아토리서치(주)는 자체 개발한 SDN 컨트롤러와 NFV 기반 보안 서비스, 3D 관제와 같은 핵심기술을 기 보유하고 있으며 다양한 사업 레퍼린스를 확보/확장 중

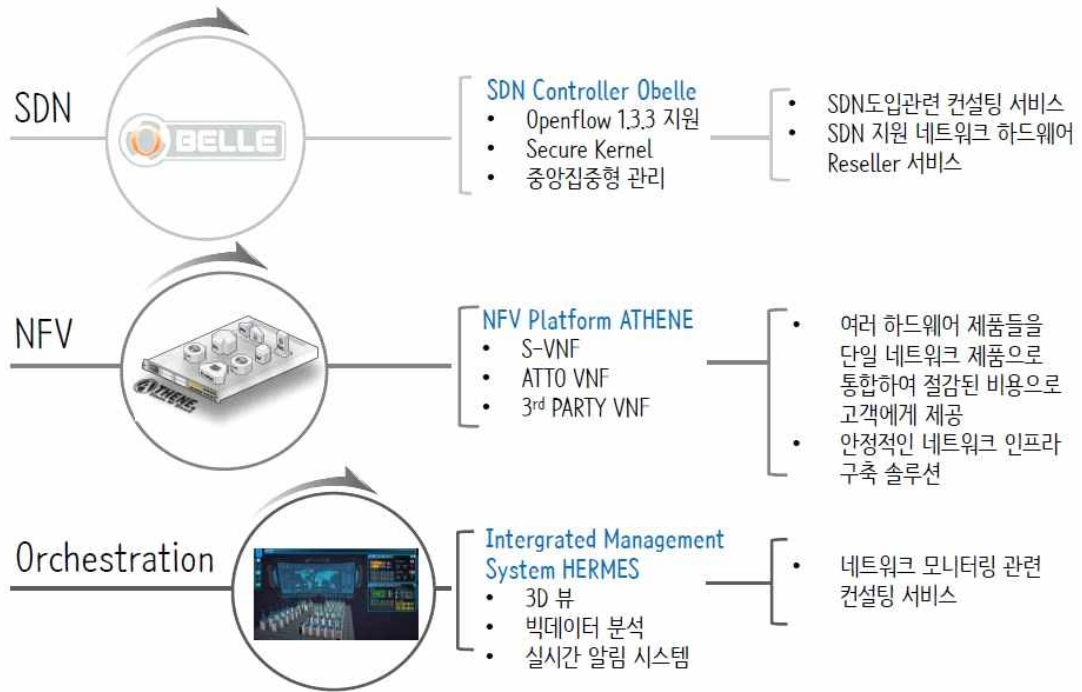


그림 57 SDN과 NFV와의 관계

- 4차 산업혁명으로 대표되는 신기술/산업 패러다임 - 5G, IoT, 가상현실/증강현실, UHD/4K, 인공지능, 머신 러닝, Bio, Big Data -는 기존의 네트워크상에서는 서비스 제공이 불가하며 SDN/NFV와 같은 새로운 네트워크 구조가 필수임
- 도로교통에서도 자율주행, 자율도로, 차량 간 통신(V2V) 등 새로운 기술이 등장함. 특히 현재 추진 중인 C-ITS는 차량의 상태 정보 공유(1단계), 차량에서 수집된 정보 공유(2단계), 차량 운전자의 의도 공유(3단계)를 실현하는 고도의 기술로서 단계가 진화할수록 대용량의 정보 처리를 요구함
- 추후 Smart City로의 진화를 고려하면 차량/도로 뿐 아니라 도로가 위치한 지형 및 도로 시설물의 정보까지 처리를 하게 되므로, 대용량 정보 처리와 다수의 보안 취약점 증가에 대한 대비가 필요함.
- SDN/NFV는 Smart City의 네트워크 인프라 구축에 필수적인 기술로서 고려됨. 차량이나 도로 네트워크만을 위한 전용 기술이 아니라 네트워크 전반에 사용되는 범용 기술이므로 다소의 차이점은 존재함
- 따라서 기존 사업아이템과 본 사업에서 개발되는 기술과의 연관 정도는 90% 이상임
- 또한 기 보유하고 있는 개발 시스템, 검증 시스템, 연구 인력 등은 본 사업에서 그대로 활용이 가능함(100%)
- 원재료 측면에서는 SDN 제어기와 NFV 보안 박스, 통합 관리 모두 x86서버에 소프트웨어를 탑재하는 형태가 그대로 유지되므로 공용화가 가능함. 소프트웨어 개발 인력을 개발 설비로 대입한다면, 도로교통 네트워크 용 추가 개발 인력을 제외한 기존 인력의 공용화 정도는 80%로 추산

(3) 사업화 모델(Business Model)의 제시
(가) 최종 목표

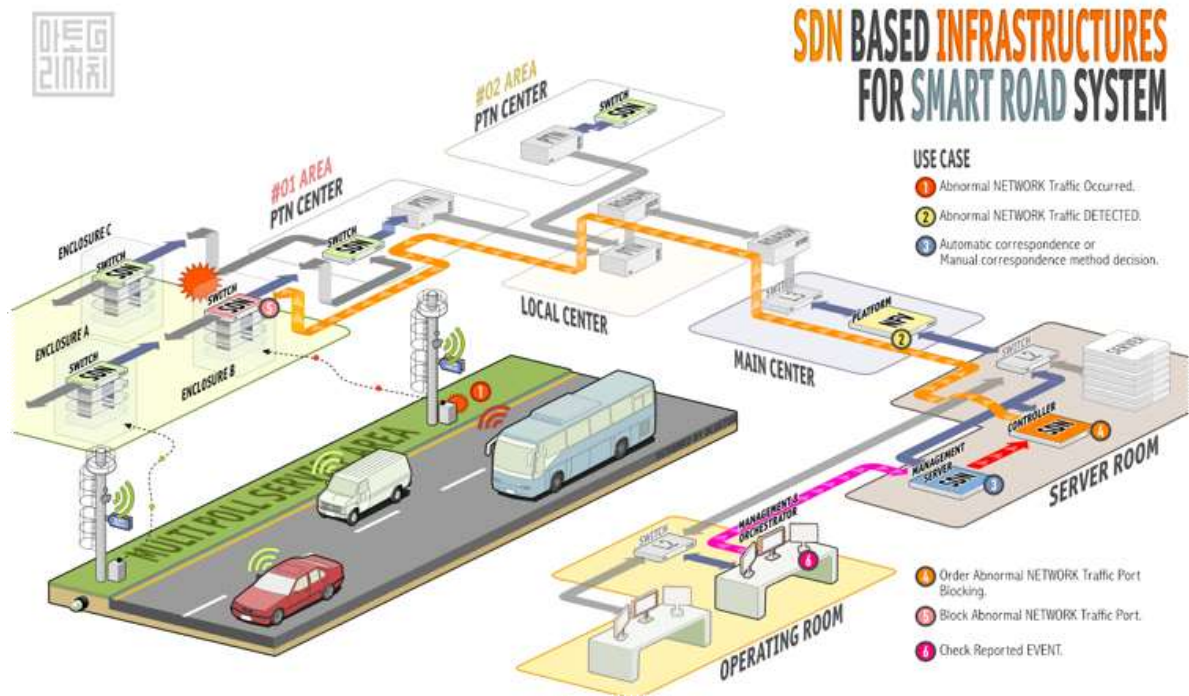


그림 58 사업화 모델 최종 목표

(나) 사업화 모델의 경쟁력

現 도로통신 N/W		SDN 도로통신 N/W
장비 추가시 물리장비 증설 필수	설치	가상망 활용 자원 효율화 통해 네트워크 장비 증설 최소화
- 네트워크 구성 및 설정 변경시 현장 장비별 인력 투입	관리	- 네트워크 구성 및 설정 변경시 관제센터에서 자동 설정
- 설정된 경로로만 데이터 전송		- 상황변동에 따른 자동 경로설정
장애 발생시 인력 출동 정비	재난	장애발생시 우회 등 실시간 우선 대응
디도스 공격 등 사후 대응중심	보안	빅데이터 기반 AI 엔진 활용해 즉시 대응및 보안 조치
설치-유지보수 외주 등 H/W, 인력중심 과다 도입 및 운영 비용 소요	비용	화이트 박스 등 H/W 절감 + S/W 확장성 소프트웨어 통해 비전문가 유지관리 가능 도입비용 뿐만 아니라 운영비용까지 절감

그림 59 사업화 모델의 경쟁력

(다) 목표 시장의 구조

① 경쟁 기업 현황

- Big Switch Network: 스탠포드 대학에서 OpenFlow 1.0을 개발한 팀들이 주축으로 2010년도에 설립하였으며, 2011년4월에 1,400만 달러를 투자받으면서 주목 받음. 현재는 Big Cloud Fabric, Big Tap의 두 가지 솔루션으로 데이터센터 시장을 공략중

- VMware: 본래는 가상화 솔루션 전문 세계적인 회사이지만, 역시 세계적인 SDN전문 기업인 Nicira를 1조가 넘는 가격에 인수하면서 SDN시장에 뛰어듦. Nicira는 OpenFlow를 창시한 스탠포드 대학의 Nick McKeown, 버클리 대학의 Scott Shenker가 공동 창업한 회사로서, 클라우드 데이터센터를 위한 SDN기반의 네트워크 가상화 솔루션이 주력 사업임
- 쿨클라우드: 국내 SDN벤처 1세대. SDN 제어기 및 가상 라우터 솔루션을 가지고 있으며, 데이터센터와 통신사를 주로 타겟으로 사업 중

② 시장 진입 장벽

- 기존 벤더들은 데이터센터와 통신사 용 솔루션에 집중하고 있기 때문에 도로통신 네트워크 분야에 있어서는 최소 3년 이상의 기술 격차를 가질 수 있음
- 그와 함께, 최종 제품의 핵심 기술은 특허로 기술 장벽을 만들 예정

(라) 수익 확보 전략

① 주요 고객 군

- 1차 목표시장은 한국도로공사, 민자 고속도로, 지자체, 국토관리청 등 도로운영주체를 대상으로 함
- 2차 목표시장은 국토교통부, 지자체, 미래창조과학부 등 Smart City 추진 주체를 대상으로 함
- 3차 목표시장은 국내 적용(검증) 사례를 기반으로 해외 수요처를 대상으로 함

② 수요처별 마케팅 전략

수요처	주요 마케팅 전략
도로운영주체	- 자율협력주행 도로망 등 과제 개발 과정에서 확보된 레퍼런스 활용 - 한국도로공사 차세대 도로망 구축에 적극 활용.
스마트시티 추진 주체	- GS 인증 및 조달청 우수제품 지정을 기반으로 관련사업 적극 입찰
해외 수요처	- 각종 해외전시회 참석을 통한 수요업체 발굴

③ 사업화 모형(BM)을 통한 수익 창출 방안

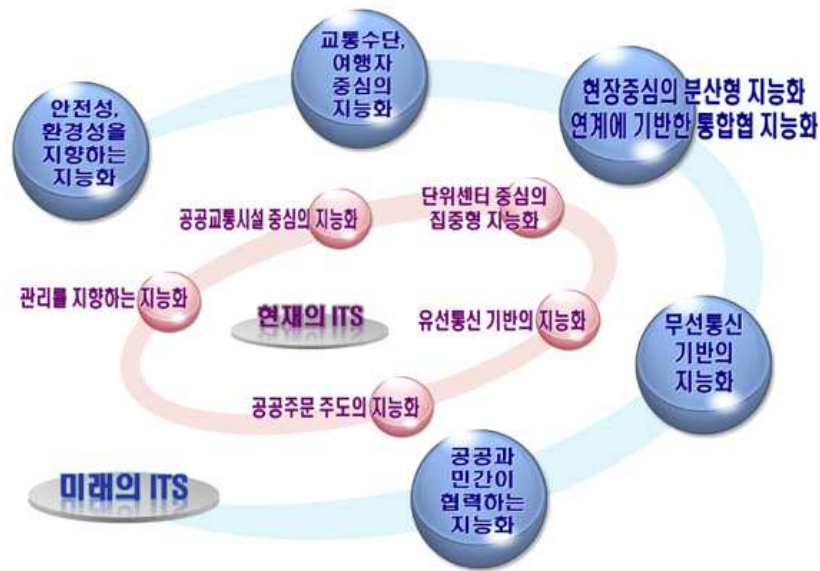


그림 60 사업화 모형의 수익 창출 방안

나. 성과물의 활용방안

- (1) 본 사업의 결과물인 도로교통 특화 네트워크 보안 기술이 적용된 트래픽 최적화 시스템 개발 및 네트워크 통합 관제 시스템 현장 적용 계획
 - 경수산업도로 왕복 6차선 27Km 구간 내 SDN망 구축 및 트래픽 최적화 시스템 적용.
 - 하이패스 등 통행료 무인수납 시스템망 내 도로교통 특화 네트워크 보안기술 적용.
 - 평택-시흥 간 고속도로와 제2 서해안고속도로 구간 네트워크 통합 관제 시스템 연계 적용.
 - 첨단 기술이 집약된 스마트시티 네트워크, 센서, CCTV, 지능형 교통체계 등 첨단 IT 기술을 집대성한 미래형 첨단 친환경 도시에 적용
- (2) 본 사업의 결과물중 도로교통 특화 네트워크 보안기술 실용화 및 제품화 방안
 - 2025년 완전 개통을 목표로 하고 있는 서울-세종 간 고속도 등 국가 운영 고속도로 대상
 - 지난 2016년 7월부터 시범운영하고 있는 세종-대전 고속도 87.8Km의 차세대 지능형 교통체계 시스템과 연계운영
 - 스마트시티 실증단지를 조성하여 미래 신산업을 발굴하고 도시 문제 해결과 동시에 지속적으로 수익 창출이 가능한 오픈 이노베이션 형태의 자생적 생태계 활성화
- (3) 본 사업의 미래원천 기술 확보 방안
 - 자율주행 자동차 주행 컨트롤 데이터 트래픽을 분리하여 V2C, V2V 통신 간 보안채널을 확보하고 악의적인 데이터 차단
 - 위치기반 안전 재난방지용 ITS 어댑티브 프로토콜 규격화 및 개발

(4) 본 사업의 신산업 창출 분야 및 활용방안

- 철도 및 항로 등 궤도에 의존하는 다양한 교통/운송설비의 지능화를 위한 신산업 창출기
대 - 차세대 철도 교통 설비 및 무인비행장치의 입체적 항공교통설비 기술 제휴
- 내비건트 연구기관에 따르면 비 OECD 국가의 경제 성장으로 인해 전 세계 인구 50%가 도시에 거주하고 전 세계 자원의 70~80%가 도시에서 소모되고 있음. 2050년에는 전 세계 70%의 인구가 도시에 거주할 예정. 급속화 도시화의 진전으로 인프라, 에너지 부족, 교통난 및 생활비용 증가 등 도시 효율성을 저해 하는 요인 확대. 과거에는 대규모 자원 투입을 통해 물리적으로 해결했지만 스마트시티는 기존의 도시 자원에 지능화된 ICT기술을 적용한 스마트 플랫폼으로 효율적인 해결 가능. 또한, 스마트시티는 신기술의 융합으로서 도시의 효율성을 제고하고 국가적으로 시간적, 경제적으로 새로운 가치 창출

상기와 같이 본 사업 성과물을 기반으로 한 사업화 방안은 1)국내 본 사업 수행경험을 바탕으로 여주 시범도로인 스마트 하이웨이와 유사한 해외ITS(미국, 유럽, 일본)의 진출을 꾀하고, 또한 2)스마트하이웨이 운항수단과 유사한 한국철도공사, 도시철도공사 등 교차시장에 진출하여 응용서비스 제공. 그 외에 3)무인비행장치인 무인항공기, 무인비행장치, 무인자유기구와 같은 드론의 운항고도에 따른 입체적 관제 실시. 본 사업의 성과를 체계와 하여 기술이전 및 후속연구 지원

다. 기대성과 및 파급효과

(1) 과학기술적 측면

(가) 기술의 확산효과

① 전방산업에 대한 기술적 파급효과

- 도로교통 분야 교통정보 품질 향상 및 차세대 ITS 활성화에 기여
- SDN/NFV 기술을 활용하여 실시간 교통상황, 돌발 상황, 교통류 제어상태 및 전방교통 정보등과 같은 트래픽을 분류 최적화하여 교통정보의 품질 향상
- 자율주행 자동차와 보안 통신을 위해 표준 인터페이스 제공하고 자율주행 자동차 간 운항정보, 교통정보, 상황별 자동제동 및 가속 시스템을 ITS와 연계하여 미래차 기술개발 방향성 제시

(나) 후방산업에 대한 기술적 파급효과

① 사물인터넷(IoT) 기술을 활용한 스마트시티 시장의 지배력 강화

- 유럽, 미국 등 해외 선진국은 기존도시의 재개발 중심으로 중동, 중국 등은 신규 도시 개발 중심으로 U-City의 개념과 유사한 스마트시티 건설이 활발하게 진행 중임. 전 세계적으로 첨단 IT기술을 적용한 신도시 개발이 성장성과 수익성 측면에서 성장할 가능성 매우 높음. 2011년 글로벌 스마트시장의 누적 규모는 530조 원가량임. 연평균 14% 성장해 2016년에는 1천 300조원을 형성할 것으로 전망

(2) 사회·경제적 측면

(가) 기술개발에 따른 경제적 효과

① 도로운영자(도로공사, 민자 고속도로, 지자체 등) ITS 구축비용 절감

- 전통적 방식의 네트워크 및 보안 기술대비 제품 가격의 경제성 확보는 물론 해외 제품 대비 경제성을 확보하여 수요처의 IS 시스템 구축비용 절감
- 침체된 ITS 시장의 변화 및 활성화 기여

(3) 정책적 측면

(가) 전문인력 양성 및 산업구조개선

- SDN/NFV 기반 솔루션의 제품개발 및 차세대 ITS 연계형 연구개발투자선행으로 전문 ITS 솔루션 개발 및 운영, 관제 인력을 양성하고 현 고속도로 운영 실정에 따른 노동집약적 인력구조를 소프트웨어 기반의 제 4차 산업혁명 산업시대로 고도화
- 도로 ITS 외 도로를 사용하는 차량 지능화에 따른 인명피해, 경제적 손실 감소 등 교통안전 개선으로 차량 전복, 추돌 사고 등을 방지하고 그에 따른 사회적, 경제적 손실 감소
- 교통안전 정보제공, 교통사고 예방체계 구축, 교통사고 사망자수 감소 기대

(나) 해외 수출로 인한 창조경제 활성화 기여 및 국가 경쟁력제고

- ITS의 도로교통 특화 네트워크는 국내뿐만 아니라, ITS 도입국인 미국, 유럽, 일본 등 해외 국가에 수출이 가능한 국가전략기술기반 솔루션으로 우리나라 ITS 기술의 해외수출에 따른 창조경제 활성화 및 국가 경쟁력 제고

[공인인증기관의 시험성적서 등 기술개발결과물의 객관적 증빙자료]

- 공인인증기관의 시험성적서, 결과서
- 시범운영보고서
- 신기술인증서
- 우수제품지정증서
- 외부평가계획안
- 외부전문가평가서
- 특허출원서
- SW 저작권 등록증

붙임. 참고문헌

- OpenFlow Switch Specification Version 1.3.3, Open Networking Foundation
- SDN 기반 도로 통신 네트워크 시스템 개발 연구개발 계획서

뒷면지

주 의

1. 이 보고서는 국토교통부에서 시행한 국토교통기술사업화지원 사업의 연구보고서입니다.
2. 이 보고서 내용을 발표하는 때에는 반드시 국토교통부에서 시행한 국토교통기술사업화지원 사업의 연구결과임을 밝혀야 합니다.
3. 국가과학기술 기밀 유지에 필요한 내용은 대외적으로 발표 또는 공개하여서는 안 됩니다.