ETRI

초연결 신뢰 네트워크 기술

Hyper-connected Trust Network Technology

정부금 (B.G. Jung) 네트워크연구본부 책임연구원
이형규 (H.G. Lee) 네트워크연구본부 책임연구원
박혜숙 (H.S. Park) 네트워크연구본부 PL
박종대 (J.D. Park) 네트워크연구본부 PL

* 본 연구는 미래창조과학부 '범부처 Giga KOREA 사업[GK16P0100, Giga Media 기반 Tele-Experience 서비스 SW플랫폼 기술 개발]'과 'ICT R&D 바우처사업[R7317-16-0038, 차량용 모바일 단말과 클라우드 간의 가상사설망 보안서비스 기술 개발]'의 지원을 받아 수행하였음.

모든 사회 생활 및 경제 활동이 인터넷을 통해 이루어지며 IoT, 빅데이터, 모바일, 클라우드가 연결되는 초연결 시대를 대비하기 위하여 신뢰성이 담보된 차세대 네트워킹 기술이 요구되고 있다. 신뢰성 있는 IP네트워킹 기술은 속도와 기능 및 성능의 고도화를 넘어서 새로운 환경에 적응이 가능한 유연한 구조와 다양한 상황에 대응하는 지능적 처리 방식으로 혁신되어야 하며 안전한 초연결 서비스를 위해서 프라이버시와 보안이 핵심으로 제공되어야 한다. 본고에서는 최근의 IP 네트워크 기술 동향을 살펴보고 이를 기반으로 초연결 세상을 구현하기 위한 중심에 있는 신뢰 네트워크에 대한 개념을 새로이 정의하며, 필수적인 요구사항들과 기능들을 분석하고 이를 기반으로 적용 가능한 다양한 응용 분야를 도출하며, 지속적인 향후 연구방향에 대해서도 살펴보고자 한다.

Ⅰ. 서론

우리가 아침에 눈을 떠서 잠자리에 들 때까지, 어떤 사람들은 잠자리에 들어서도 항상 손에서 놓지 않는 것이 있다. 바로 스마트폰이다. 왜일까? 스마트폰은 항상 인터넷 통신이 가능하여 나와 세상과 연결해주는 장치이기 때문이다. 앞으로 주변의 모든 사물과 장치가 항상 인터넷에 연결되면 어떤 일이 벌어질까? 사람과 사물, 여기서 창출되는 데이터나 프로세스까지 모든 것이 연결되는 초연결 세상에서 우리의 삶과 비즈니스의 방식은 예상을 초월할 정도로 다양하게 변모될 것이다. 정보통신기술(ICT) 산업뿐만 아니라 공공, 제조, 의료 등 전통적인 산업과 주거환경, 도시, 국가까지도 큰 변화가 나타날 것이다. 2020년에는 250억개의 사물이 네트워크에 연결되는 초연결 시대가 본격 도래할 것으로 예측된다[1]. 온라인, 오프라인을 포함한 무수한 연결과 폭발적인 데이터와 멀티미디어 콘텐츠가 실시간으로 사용되고 효율적으로 활용되어 또 다른 가치를 창출하는 초연결의 가장 중심에는 빠르고 안전하고 믿을 수 있는 네트워크가 있어야 한다. 이에 본고에서는 초연결을 위한 신뢰 네트워크의 필요성 및 역할에 대하여 논의한다. 제 Ⅱ장에서는 기술 현황으로 주요 산업체 동향, 신뢰 네트워크 기술 동향과 표준화 동향을 살펴보고 이를 기반으로 제 Ⅲ장에서 초연결 신뢰 네트워크 기술의 개념과 주요 기능을 정의하며 Ⅳ장에서는 응용 분야의 예를 기술하고 Ⅴ장에서 결론을 맺는다.

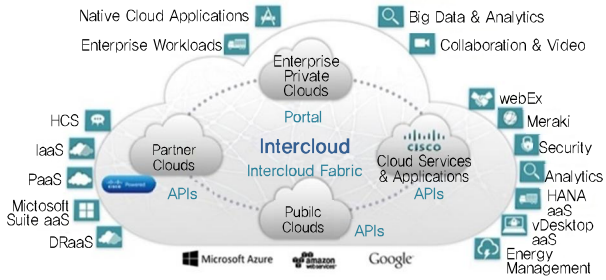
Ⅱ. 초연결 신뢰 네트워크 기술 현황

컴퓨터와 컴퓨터를 연결하기 위해 시작된 네트워크 기술은 속도와 기능과 성능이 고도화되면서 진화되어 왔다. 그러나 최근에는 연결의 수가 기하급수적으로 늘어나고 생성되는 데이터에 대한 지능적인 처리를 통한 연결이 필요하게 되어 근본적인 네트워크의 구조 및 방식에 있어 혁신적 변화를 필요로 하게 되었다. 소프트웨어 정의 네트워킹(SDN), 네트워크 기능가상화(NFV), 클라우드가 대표적인 새로운 개념이다. 이같은 변화를 이끄는 핵심 동력은 바로 초연결 시대의 진입에 있다. 본 장에서는 이러한 초연결 시대를 맞이하기 위하여 준비하는 산업계 동향과 기술의 동향 및 표준화 동향에 대해서 알아본다.

1. 초연결 네트워크 산업계 동향

가. 시스코

시스코는 초연결(IoE: Internet of Everything) 시대를 위하여 새로운 인프라 기술을 개발하고 있다[2]. 사물과 그 사물이 생성하는 데이터, 데이터 처리 프로세스, 사람이 모두 연결되는 초연결 환경에서는 현재의 인프라만으로는 부족하기 때문이다. 이에 시스코는 포그 컴퓨팅(Fog Computing) 아키텍처와 개방형 연동 클라우드 서비스인 인터클라우드(InterCloud) 기술을 제시하였다. 구름보다 땅에 가까이 있는 안개를 의미하는 포그 컴퓨팅 아키텍처는 컴퓨터, 스토리지, 네트워크 각 요소가 있는 에지에 센서와 가까운 별도의 레이어를 추가해 데이터 프로세싱을 분산 처리하는 방식으로 포그 레이어에서 특정 지역에서 발생한 데이터 애널리틱스를 가까이에서 수행하고 중요한 것만 선별적으로 클라우드에 올리는 것이다. 이를 위해 네트워크 에지단의 네트워크 장비(라우터)에서 컴퓨팅 기능을 추가해 제공하고 있다. 이와 함께 네트워크 에지단에서 애플리케이션 개발·적용을 쉽게 할 수 있도록 IOx 플랫폼을 새로이 개발하였다. 시스코의 기존 네트워크 장비 플랫폼인 IOS에 리눅스를 추가해 애플리케이션 개발 환경을 지원하는 것이다. 또한, 초연결 시대의 도래에 대비하기 위하여 산재된 여러 클라우드를 상호 연결하기 위해 전 세계적으로 연결된 클라우드 네트워크인 인터클라우드를 구축하고 있다. 인터클라우드는 (그림 1)과 같이 전 세계적으

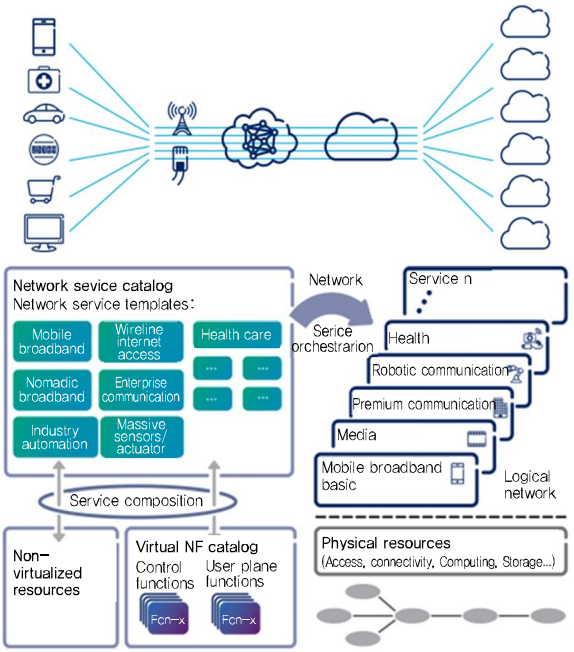


(그림 1) 시스코 인터클라우드[2]

로 안전한 클라우드 플랫폼을 구축하여 전 세계 모든 곳에 안전한 클라우드 서비스를 제공하기 위한 것이다. 이러한 인터클라우드로 만물인터넷(IoE)으로부터 요청되는 초연결 네트워크의 수요를 충족시키고, 고부가가치의 애플리케이션 워크로드는 물론 실시간 분석, 무한에 가까운 고확장성을 지원하고자 하는 것이다. 더불어 개방적인 클라우드 서비스 제공, 로컬 호스팅 및 로컬 서비스 제공 업체의 참여를 허용해 고객이 데이터 주권 문제를 해결할 수 있도록 돕고, 컴플라이언스와 통제력을 갖춘 서비스들의 선택권을 제공하기 위한 기술을 개발하고 있다.

나. 에릭슨

에릭슨의 홈페이지는 'One Network for a million needs'라는 슬로건으로 장식되어 있을 정도로 초연결 사회를 위해서 네트워크의 중요성을 강조하고 있으며 앞으로의 비즈니스의 혁신은 바로 네트워크의 혁신에서 시작됨을 강조하고 있다[3]. 이를 위하여 에릭슨은 미래 네트워크 환경에서는 하나의(One) 공통된 네트워크 플랫폼을 바탕으로 다양한 산업 요구에 맞춰 유연하고 안전한 방식으로 네트워크를 슬라이스해서 제공할 수 있는 기술을 개발하고 있다. 이를 가능하게 하려면 클라우드화는 필수다. 전 세계가 초연결 네트워크 사회로 전환되면서 그 근간이 되는 네트워크 자체가 수평적인 네트워크로 변모하여야 하며, 하드웨어와 소프트웨어가 분리되고 가상화가 구현돼, 모든 기기가 하나의 네트워크

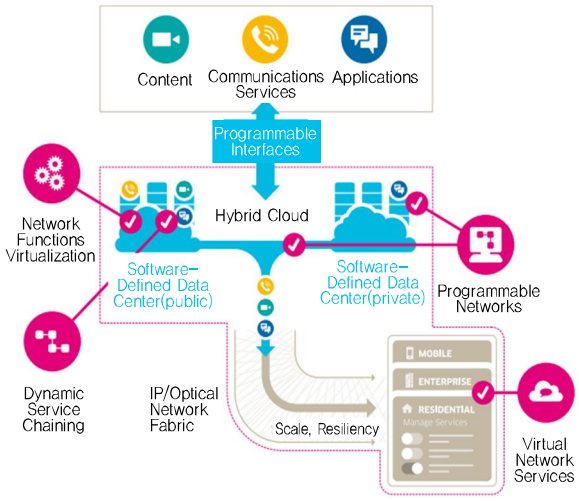


(그림 2) 에릭슨 원네트워크(One Network) & 네트워크 슬라이싱[3]

(One Network)상에서 클라우드와 연결된다는 것이다. 이러한 '원네트워크'를 통해 모든 것을 연결하며, 하나의 네트워크를 슬라이스, 클라우드와 연결해 밀리세컨드 네트워크를 제공하고 안전하게 연결된 다양한 디바이스로 서비스를 제공하는 기술을 개발하고 있다[(그림 2) 참조].

다. 알카텔 루슨트

알카텔루슨트 벨연구소는 2020년 미래 네트워크는 공통의 융합화된 네트워크로, 동적이며 프로그램 가능한 네트워크 형태가 될 것으로 전망하며, 이 같은 변화를 견인하는 3대 핵심 동력으로 가상화와 SW중심, 클라우드를 지목한다[4]. 벨연구소는 보다 구체적으로 IP와 광 코어가 다계층 SDN 제어를 통해 함께 최적화되고 클라우드화가 네트워크 전반에서 이루어지며, 특히 지능화된 분석과 최적화를 위한 다양한 에지 클라우드 및 IP와 광의 융합·최적화 및 동적 연결이 가능하도록 하기 위한 기술을 구현하고 있다[(그림 3) 참조][5].

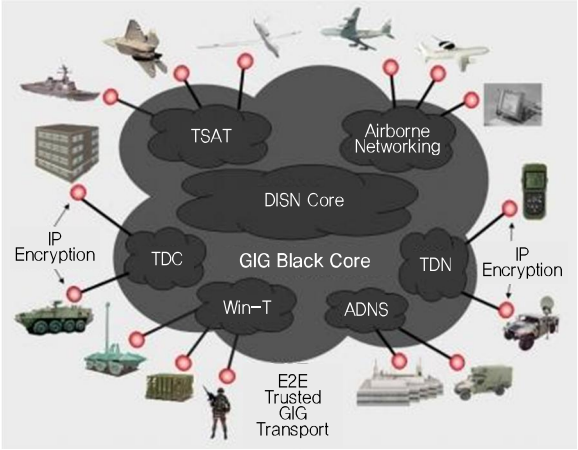


(그림 3) 동적 서비스를 위한 SDN/NFV 기반의 동적 네트워크[5]

2. 신뢰 네트워크 기술 동향

가. Black Core Network 기술

Black Core Network 기술은 미 국방성을 중심으로 개발되고 있는 신뢰 네트워크 기술로 (그림 4)와 같이 네트워크를 음영화하여 사이버 테러에 대한 안전성 보장을 위한 것으로 이를 기반으로 2020년까지 국방인터넷의 고도화를 추진 중이다[6]. 기존 네트워크상에서 오버레이 방식으로 보안성을 요구하는 연결에 네트워크 자원의 배타적 할당과 암호화를 통한 폐쇄적 연결 서비스를 제공하는 것으로, 데이터의 신뢰성 보장을 위하여, 개방된 퍼블릭망을 경유하는 트래픽의 경우, HAIPE (High Assurance Internet Protocol Encryption) 프로토콜을 사용하여 데이터를 암호화하며, HAIPE가 탑재된 에지 라우터 주소의 수시변경을 통하여 코어망 전체를 보호하는 기술이다. Black Core는 HAIPE IKE를 이용한 동적 보안 연결(SA: Security Association)과 SA복구, SA기반 통계, 다중 보안 정책에 따른 SA구성을 요구한다. 특히 CT(cipher text) IP 주소와 PT(plain text) IP 주소를 구분하여 PEPT(Peer Enclave Prefix Table)을 구성한다. 즉, GIG Black Core 연결 네트워크 전체

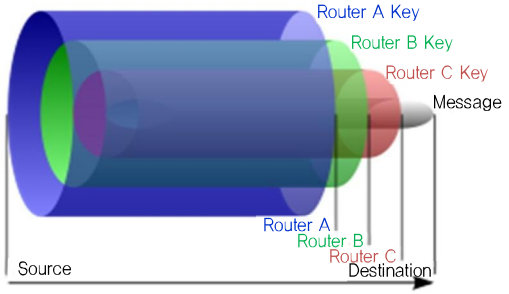


(그림 4) E2E Trusted GIG Transport[6]

를 음영화하여 단말과 단말간의 암호화된 신뢰 전달을 보장할 수 있는 기술이다.

나. TOR 기술

TOR(The Onion Routing)은 (그림 5)와 같이 네트워크 노드를 거칠 때마다 마치 양파처럼 데이터를 계속 암호화하여 전송하는 것으로, 트래픽 추적을 불가능하게 하여 네트워크상에서 익명성을 보장할 수 있는 기술로 미국 해군 연구소에서 시작하여 현재는 EFF에서 관리되고 있는 Free Software 프로젝트이다[7]. 초기에는 내전 중이거나 인터넷에 대한 규제가 엄격한 국가의 사용자들이 감시를 받지 않고 네트워크를 자유로이 사용하기 위해서 활용되었다. 토르 네트워크(Tor Network)는 어니언 라우터(Onion Router)라고 하는 중계서버로 구성되어 있고 트래픽은 목적지까지 바로 전달되지 않고



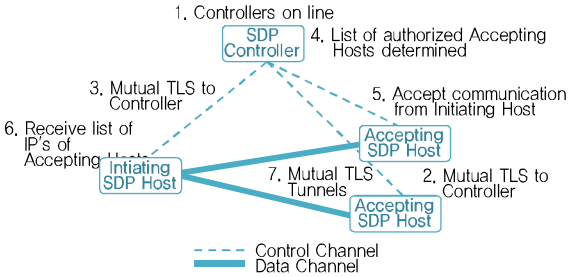
(그림 5) 토르 네트워크—어니언 라우팅[7]

중계서버를 통해 전송된다. 각 중계 서버는 패킷이 어디서 출발했는지를 알 수 없으며, 최종목적지가 어디인지도 알 수 없고 오직 다음 중계 서버의 주소만을 알 수 있을 뿐이다. 따라서 토르 네트워크를 사용하게 되면 IP 추적이 되지 않고 익명성이 보장되는 것이다. 그러나 출발점도 도착지도 알 수 없는 이러한 네트워크 환경은 악성코드를 유포하는 채널로 악용될 수 있는 문제점을 내포하고 있다.

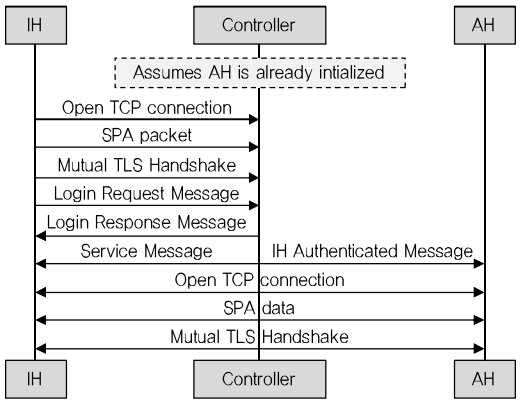
다. SDP 기술

SDP는 Cloud Security Alliance에서 개발하고 있는 Software Defined Perimeter의 약자이다[8]. 인터넷상에 흩어져 있는 자원(예, 서비스 혹은 데이터)을 보호하기 위해 경계기반 보안 메커니즘을 제공한다. SDP는 기존 보안 프로토콜의 취약성이 Connection-oriented protocol이라는 점에 기인하고 있다고 판단한다. 따라서 실제 서비스에 접속을 요구하는 단말과 서버 사이의 연결을 데이터 채널과 제어 채널로 분리하고, 인증받지 못한 단말에 대해 어떠한 서비스 연결 정보도 얻지 못하도록 하고 있다. 이러한 설계 개념에 의해 기존의 서버 탐침, 크레덴셜 탈취, 세션 하이재킹과 같은 보안 위협들에 대한 해결책을 제시하고 있다. 또한, 채널 분리에 의해 실제 서비스 서버에 대한 분산서비스거부공격(DDoS)을 줄이기 위한 방법도 제공하고 있다.

다음 (그림 6)과 (그림 7)에서 보이는 바와 같이 단말과 서버 사이의 데이터 채널(혹은 서비스 채널)은 SDP 컨트롤러와 단말 및 SDP 컨트롤러와 게이트웨이 간의 제어채널을 통한 시그널링에 의해 안전하게 구축될 수 있다. 제어 채널 역시 초기 접속 인증을 위한 방법이 요구되는데 이를 위해 SDP 스펙 1.0에서는 일회용 패스워드 인증 방식과 결합된 형태의 mTLS(상호인증 TLS)를 사용하고 있다. 위의 데이터 채널 구축과 관계된 안전한 시그널을 통해 데이터 채널 역시 일회용 패스워드



(그림 6) Software Defined Perimeter 구조[8]



(그림 7) IH-CH-AH 연결 프로토콜[8]

인증과 mTLS의 결합된 방식을 사용하거나 상호인증을 통한 IKE/IPsec 방식을 사용하게 된다.

SDP는 다양한 인터넷 환경에 보안 터널을 설정할 수 있도록 하는 동적인 특성을 가진다. 따라서, 클라이언트-게이트웨이, 클라이언트-서버, 서버-서버를 비롯한 다양한 네트워크 서비스 환경에 적용될 수 있다. 따라서, IaaS/PaaS/SaaS와 같은 클라우드 서비스나 클라우드 기반 VDI, IoT 플랫폼과 결합하여 중요한 자원을 권한없는 사용자로부터 격리시키고 더 나아가 실질적인 탐지 불가 기능을 제공하여 보다 강하고 효율적 안전성을 제공하기 위한 기술이다.

라. 5G 기술

2020년 상용화될 것으로 전망되는 5세대(G) 이동통신 기술은 초연결 시대 네트워크 미래상에 가장 부합된 개념이다. 5G는 현재의 이동통신 환경보다 1000배에서

(그림 8) 5세대 네트워크 기술[9]

1만배 가량의 트래픽을 수용할 수 있는 고용량과, 1~10Gbps의 초고속 데이터 처리속도, 1밀리초(msec) 이하의 저지연, 품질 안정성과, 수많은 디바이스의 다중 연결성, 10년간의 저전력 배터리 수명과 뛰어난 에너지 효율성, 확장·운용·진화가 용이한 유연성, 저비용의 경제성, 보안성 등이 제공되는 기술이다[9]. 5G 환경에서는 언제 어디서나 원하는 서비스 경험을 전달할 수 있는 고용량의 광대역 네트워크가 더욱 확장되는 동시에 특화된 초연결 서비스를 지원하기 위한 저지연, 저전력 네트워크도 지원될 것으로 예상되고 있다. 가장 두드러진 5G 네트워크의 특징은 '융합'이다. 현재 사용되는 이동통신 기술인 3G와 4G 롱텀에볼루션(LTE) 진화 기술뿐만 아니라 스몰셀, 와이파이(WiFi) 등 다양한 유무선 네트워크가 결합·최적화되고, 가상화·클라우드 기술까지 접목될 것이란 점에서다. 5G 환경이 구현되면서부터 네트워크의 구조나 운영, 서비스 제공방식이 획기적으로 변화되고, 이른바 초연결 서비스가 구현될 수 있는 환경이 갖춰지게 될 것이다[(그림 8) 참조].

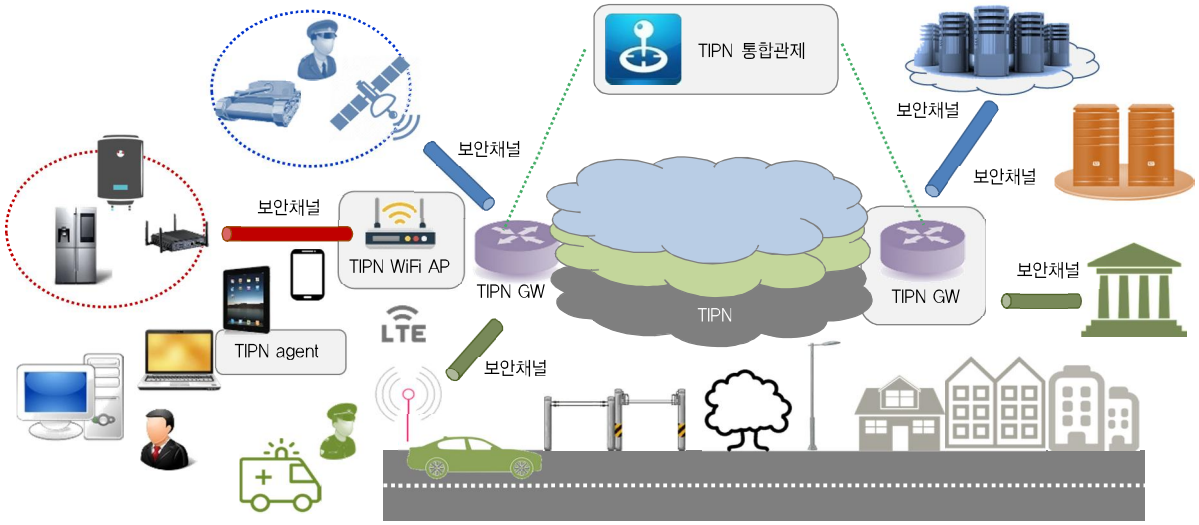
3. 표준화 동향

IETF에서는 클라우드 데이터센터 내에서의 브리지간 라우팅 기술인 TRILL[10] 표준 기술과 데이터센터간 오버레이 네트워킹 기술로서 VxLAN[11], NVGRE[12], STT[13], eVPN[14] 등의 표준기술이 개발 중이며, 데이터센터간에 응용 계층 기반의 전달망에서의 트래픽 최적화를 위한 ALTO[15] 기술 표준화 진행하고 있다. OPNFV[16]는 ETSI(European Telecommunication Standards Institute)가 규정하고 있는 NFV 구현에 필요한 다양한 요소들을 사전 검증을 거쳐 통합된 형태로 제공하기 위해 시작된 오픈 소스 프로젝트로서 최근 결과물인 Arno를 발표, 캐리어급 NFV 플랫폼의 오픈소스 개발을 지속적으로 추진하고 있다. ODL[17]은 여러 제조업체의 네트워크 장비 구성 상태에 SDN 구축을 위한 고가용성, 모듈성, 확장성을 갖춘 다중 프로토콜 컨트롤러 인프라를 지원하기 위한 오픈소스 프로젝트이며 최근 보안과 자동화 기술이 보강된 새로운 버전인 Lithium 발표하였다. ONOS[18]는 선도적인 글로벌 통신사들과 장비업체들이 주도하고 있는 오픈소스 SDN 제어 플랫폼으로, 높은 성과, 신뢰성, 보안성 및 확장성과 같은 통신사들의 네트워크 및 서비스 요구사항에 초점을 두고 이를 반영한 아키텍처에 기반한 오픈 소스 개발에 주력하고 있다. 단말의 인증 분야에서는 ITU-T에서 OTP 기반 부인방지 프레임워크 표준 X.1156[19]을 제정하고, 모바일기기를 사용한 다중요소 인증 메커니즘(Multi-factor authentication mechanisms using a mobile device) 표준 X.1158을 제정하였다. FIDO Alliance[20]에서는 FIDO Universal Authentication Framework(UAF)와 Universal Second Factor(U2F) 1.0 산업표준을 제정하였다.

Ⅲ. 초연결 신뢰 네트워크 기술

1. 기술 개념

초연결 신뢰 네트워크(TIPN: Trust IP Network)란 신뢰할 수 있는 사람-사물-데이터(클라우드)가 실시간, 온-디맨드로 연결되는 네트워크로, 모든 사물의 연결로 인한 디바이스(사람)-네트워크-클라우드에 대해 언제 어디서나 고신뢰 연결성 제공과 유통되는 정보에 대한

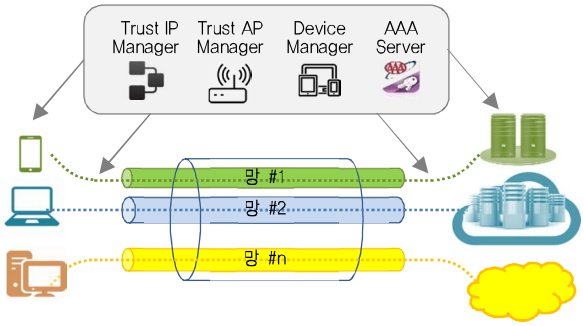


(그림 9) 초연결 신뢰 네트워크 기술 개념

신뢰성을 보장할 수 있는 네트워크 기술을 의미한다. 최상의 보안 및 신뢰 솔루션은 믿을 수 있는 사물만 연결하고 인프라의 모든 접촉 지점에 지능을 부여하여 정책을 기반으로 제어할 수 있는 솔루션을 제공하는 것이다. 이를 위해서는 인터넷 속에 신뢰 존(zone)을 만들고, 이 신뢰 존은 허가된 사용자/디바이스 만이 안전하게 접속할 수 있도록 하며, 접속에 대해서는 접속 전에 보안 상태를 사전에 점검하여 인증된 사용자만이 접속이 가능하도록 관리해야 한다. 이를 위해서는 하나의 물리 네트워크를 가상화하여 안전한 오버레이 네트워크를 구성할 수 있는 네트워크 가상화, 신뢰할 수 있는 사용자에 대해 자원 접근 전에 인증하는 사전 인증 제어가 필요하며, 또한 신뢰 단말, 신뢰 네트워크 노드, 단말-네트워크-서버-서비스 전 영역의 통합 관제가 제공되어야 한다[(그림 9) 참조].

2. 계층적 다중 네트워크 가상화 기술

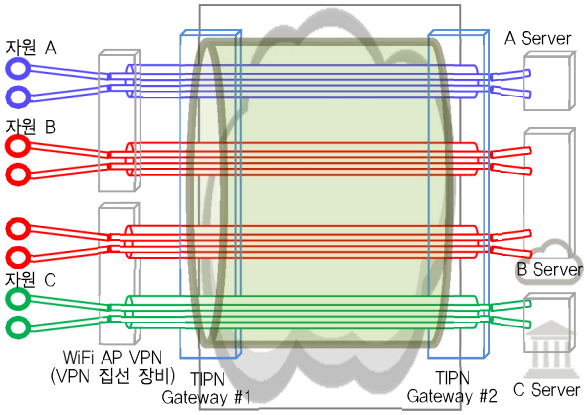
네트워크 가상화 기술은 하나의 물리 네트워크상에서 다수개의 가상 네트워크를 생성할 수 있는 기술로 생성된 가상 네트워크는 마치 자신만의 물리 네트워크를 소유하여 사용하는 것처럼 각각 독립적으로 운용된다. 즉,



(그림 10) 네트워크 가상화 개념

다음의 (그림 10)에서 보는 바와 같이 하나의 물리 네트워크를 사용하여 다수개의 논리 네트워크(가상 네트워크)를 생성하고 독립적으로 각각의 자원에 접근이 가능한 것이다. 각 가상 네트워크에는 고유한 아이디가 부여되어 서로 다른 가상 네트워크에서의 접근이 불가능하며, 하나의 물리 라우터로 N개의 Virtual Router 기능 제공이 가능한 기술이다.

이러한 네트워크 가상화 기술을 기반으로 초연결 신뢰 네트워킹을 위해서는 계층적 다중 터널링 (TLS/SSL, IP/GRE, IP-in-IP, IP/MPLS 등)(그림 11)에 대한 정책 기반 라우팅과 자원 관리(QoS)가 가능해야 한다. 즉, 기관별, 기관 내에서도 조직별, 사용자 그룹별로 소유의 분리가 되어야 하며, 정보보호를 위해서 관제 정보의 격



(그림 11) 다계층 터널링 개념

〈표 1〉 VPN과 TIPN의 가상화 기능 요구사항 비교

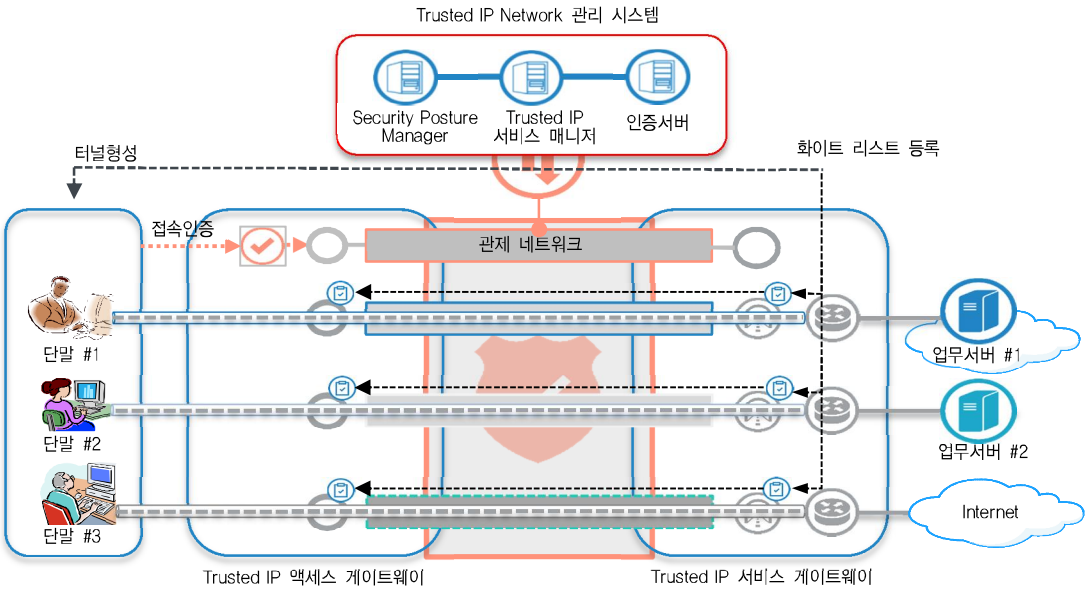
논리적 분리 기능		VPN	TIPN
소유	기관/사용자 그룹별 독립네트워크	미비	제공
관제	관리 제어정보의 격리된 관리 및 운영	無	제공
경로	다중 라우팅 도메인 접속 서비스	미비	제공
주소	물리주소(가변)와 논리주소(고유) 사용	미비	제공
서버	Virtual Private Cloud 접속 서비스	無	제공
단말	서로 다른 VPN의 동시 접속 지원	無	제공
대역	End-to-End 네트워크 대역 품질보장	無	제공

리 운용, 정보 접근 경로의 분리, 주소 은닉을 위한 주소의 분리, 서버 은닉을 위한 서버 분리, 하나의 단말에서 서로 다른 VPN의 동시 접속 및 접속하는 대역에 대한 보장 기능이 요구된다. 이러한 기존 VPN과 초연결 신뢰 네트워크(TIPN)를 위한 네트워크 가상화 기능을 비교하면 〈표 1〉과 같다.

3. 협업형 통합관제 기술

IP 네트워크 업체들은 자사의 장비를 관리하기 위한 네트워크 관제 시스템을 각각 고유하게 보유하고 있으며, 이러한 관제 시스템을 바탕으로 QoS 정책 설정 및 네트워크 관리 기능을 수행하고 있다[21]. 즉, 해당 장비의 관제 시스템은 해당 회사의 네트워크 장비에만 적용이 가능하며 보안 기술과 관련된 제어는 별도의 관제 시스템을 이용해야만 한다. 또한, 보안 장비 업체들은 자사의 보안 장비를 관리하기 위한 보안 관제 시스템을 보유하고 있으며, 이러한 관제 시스템을 이용해서 방화벽, IDS, IPS 등과 같은 장비들을 통합적으로 관리하고 있다. 이러한 관제 시스템은 해당 회사의 보안 장비에만 적용이 가능하며 네트워크를 제어하기 위해서는 별도의 관제 시스템을 이용해야만 한다. 기기 인증 또는 사용자 인증을 통한 네트워크 접속 인증 절차와 특정 서비스를 제공받기 위한 서비스 인증 절차가 개별적으로 진행되는 인증 메커니즘을 제공하고 있으며, 접속 인증을 통과하면 서비스 권한이 없는 사용자도 특정 서비스 서버에 인증을 요구할 수 있으므로 접속 인증과 서비스 인증을 동시에 처리하는 기술이 보안성 측면에서 우수하다. 한번의 인증으로 제공받을 서비스, QoS 정책, 보안 정책까지 결정되는 통합된 인증 기능이 필요하다.

이처럼, 네트워크 관제나 보안 관제 솔루션 및 인증 기능을 제공하는 업체들이 존재하지만 전역적으로 End-to-End에 대해서 보안 및 QoS 정책을 제어하기 위한 솔루션이 없으며 그에 대한 연구도 미비한 상태로, 초연결 시대에 대비하기 위해서는 네트워크-보안-인증 기능이 모두 협업된 통합형 관제 시스템이 필요하다. 통합형 관제 시스템에서는 우선, 한번의 다중 인증을 통해 보안 등급, 서비스를 인지하여 네트워크 구성, 트래픽 및 서비스에 대한 동적이고 전역적인 고신뢰 네트워킹을 제어하여야 한다. 또한, 액세스 네트워크 기기 인증 및 제어 기능은 고신뢰 네트워크에 수용되는 단말 인증, 무선 인터넷 장치 제어 및 이동성 제어 기능 수행해야 한다. 고신뢰 네트워크 제어 관리 기능은 코어 네트워크 영역을 제어 관리하는 기능으로 인가된 트래픽에 대한 고품질 서비스를 보장하고 비인가 트래픽에 대해 네트워크 접근을 제어하고, 트래픽 모니터링을 통해 DDoS와 같은 네트워크 위협을 사전에 차단하고, 서비스 연속성을 위한 장애관리, 서비스 품질 제어를 위하여, 네트워크를 관리해야 한다. 아울러 네트워크 주소 노출로 인한 네트워크 공격 차단을 목적으로 하는 네트워크 은닉 제어, 인증된 사용자별로 인가된 터널을 맵핑



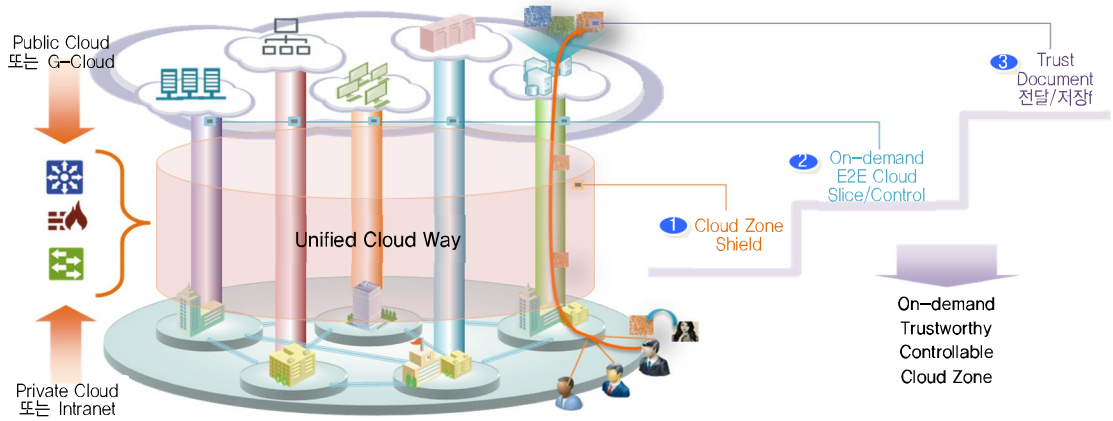
(그림 12) 협업형 통합관제 기술 개념

하도록 제어하는 계층적 터널링 제어, 사용자의 다양한 액세스 네트워크에 대한 이동성 제어 및 계층적으로 구성된 터널에 대한 QoS 제어를 수행해야 한다[(그림 12) 참조].

Ⅳ. 초연결 신뢰 네트워크 기술의 응용

1. 신뢰성있는 클라우드 서비스

클라우드 발전법[22] 시행과 민간 클라우드를 활용한 정부 클라우드(G-Cloud) 서비스 전환 가속화로 개인, 기관 또는 정부부처의 안전한 클라우드 인프라 및 서비스 수요 증가로 정부, 조직 및 기관 차원에서 안전하고 편리한 클라우드 사용을 위한 인프라 간 신뢰성 있는 연결기술을 필요로 한다. 즉, 클라우드 환경에서는 개인 및 조직의 자원과 서비스가 클라우드로 이동함에 따라 인증기반의 등급별 자원 및 서비스 접근제어를 위한 일원화된 수단이 필요한 것이다. 따라서 초연결 신뢰 네트워크 기술을 적용하여 클라우드 공간에 대한 안전한 연결성과 클라우드 자원의 제어뿐만 아니라 클라우드의 자료전달 및 저장까지를 안전하게 제공해야 한다. 이를

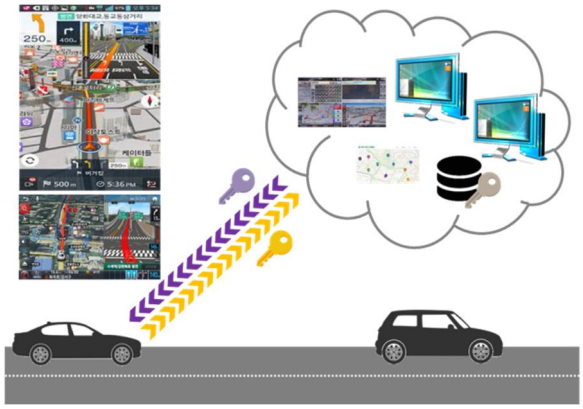


(그림 13) 신뢰내재형 클라우드 존 제공서비스 예시

통해 데이터 주권 실현을 가능하게 한다[(그림 13) 참조].

2. 안전한 커넥티드-차량-클라우드 서비스

자동차에 인터넷을 연결함으로써 자동차는 움직이는 거대한 모바일 단말화 되어가고 있으며, 앞으로 디지털 비즈니스의 가장 큰 시장 중 하나로 떠오르고 있다. 2020년까지 80%의 차량이 네트워크에 연결될 것으로 전망되고 있으며[23], 자동차 해킹으로 인한 사고는 커넥티드 카의 보안성에 더욱 집중하여 연구개발 해야 함을 시사하고 있다. 초연결 신뢰 네트워크를 이용한 차량과 클라우드 센터의 안전한 실시간 연결 및 On-demand mobility 제공은 기존 자동차에 차별성을 부여하여 새로운 도전적인 비즈니스 모델이 될 것이다[(그림 14) 참조].



(그림 14) Connected-Vehicle-Cloud 서비스 예시

V. 결론

본고에서는 안전한 초연결 세상을 구현하기 위한 중심에 있는 신뢰 네트워크 기술에 대하여 살펴보았다. 초연결 세상은 모든 것이 네트워크로 연결되어 개인과의 커뮤니케이션뿐만 아니라 여론형성 과정과 정책 결정, 의사결정에도 많은 영향을 미칠 것이다. 이러한 상황에서 우리의 생활 공간 전체가 위험지대가 되고 있으며, 사이버 영토에서의 국민과 사회를 보호할 수 있는 안전한 인프라의 준비가 필요하다. 이러한 안전한 인프라를 기반으로 언제 어디서나 어떠한 통신 환경에서도 안전하게 모바일 연결로 인터넷 사용이 가능할 것이다. 초연결 신뢰 네트워크 기술은 기존 IP 네트워크를 기반으로 새로운 구조와 방식과 패러다임을 전환하여 새롭게 지능적인 처리를 추가하는 것으로 향후 새로운 세상을 대비하는 기반 기술이 될 것으로 지속적인 연구 개발이 필요한 분야이다.

용어해설

초연결 신뢰 네트워크 기술 모든 사물-사람-프로세스-클라우드가 연결되는 환경에서 어디서나 인가된 단말과 사용자는 안전하게 허용된 네트워크 자원에 접근이 가능하도록 제어 및 관리하는 단말-네트워크 노드-관제의 통합적 네트워크 솔루션 기술

G-Cloud 클라우드 활성화를 위하여 민간 클라우드를 활용하여 정부 클라우드 서비스를 제공하는 것으로 안전한 연결을 위한 신뢰 통신 기능 필요

커넥티드 카 IT 기술로 언제 어디서나 인터넷에 연결되는 자동차, 차량 내부 통신과 외부 통신을 연결하고 안전하게 클라우드와 자료를 송수신하는 기능 필요

약어 정리

IoT	Internet of Thing
IoE	Internet of Everything
TOR	The Onion Routing
SDP	Software Defined Perimeter
TLS	Transport Layer Security
IKE	Internet Key Exchange
DDoS	Distributed Denial of Service
VDI	Virtual Desktop Infrastructure
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
VPN	Virtual Private Network
TIPN	Trust IP Network

참고문헌

[1] Gartner, "The Internet of Things Revolution: Impact on Operational Technology Ecosystems," Aug. 2016.

[2] http://www.cisco.com/c/r/en/us/internet-of-everything-ioe/

tomorrow-starts-here/index.html
[3] https://www.ericsson.com
[4] http://success.alcatel-lucent.com/en/network-2020
[5] Phil Tilley, "Transforming Networks Through NFV & SDN," Ultra Broadband Symposium, Nov. 2014.
[6] 미국방성(US DoD), "GIG 3.0 Design Factors," Jan. 11th, 2011.
[7] https://www.torproject.org/
[8] Cloud Security Alliance, Software Defined Perimeter Working Group, "SDP Specification 1.0," Apr. 2014.
[9] https://en.wikipedia.org/wiki/5G
[10] https://datatracker.ietf.org/wg/trill/charter/
[11] https://tools.ietf.org/html/rfc7348
[12] https://tools.ietf.org/html/rfc7637
[13] https://tools.ietf.org/html/draft-davie-stt-04
[14] http://www.cisco.com/c/en/us/products/collateral/routers/asr-9000-series-aggregation-services-routers/whitepaper_c11-731864.html
[15] Application-Layer Traffic Optimization (ALTO), http://datatracker.ietf.org/wg/alto/
[16] https://www.opnfv.org/
[17] https://www.opendaylight.org/
[18] http://onosproject.org/
[19] https://www.itu.int/rec/T-REC-X.1156/en
[20] https://fidoalliance.org/
[21] 예병호, 박종대, "고신뢰 네트워킹 기술," 전자통신동향분석, 제31권 제1호, 2015. 2, pp. 77-86.
[22] 미래창조과학부, "클라우드컴퓨팅 발전 및 이용자 보호에 에 관한 법률," 법률 제13234호, 2015. 9.
[23] Gartner, "Predicts 2016: Automobiles Become Digital End Points in the Era of Smart Mobility," Nov. 2015.