ETRI Insight
Insight Report 2019-22

국가지능화 특집

# 국가 지능화를 위한 초신뢰 네트워크

신용희 ● syong@etri.re.kr
기술정책연구본부

최근 제4차 산업혁명이 진전됨에 따라 국가 지능화에 대한 관심이 높아지고 있다. 제4차 산업혁명에서 가치창출 메카니즘은 초연결 기반 지능의 학습과 진화, 적용에 기인한다. 인간의 삶 속에 내재화된 초연결은 혁신의 속도, 범위와 깊이, 시스템 영향력 측면에서 과거의 연결성과는 궤를 달리한다. 따라서, 초연결 네트워크의 신뢰성 담보는 인프라의 전제조건이자, 새로운 혁명을 향한 첫걸음이어야 한다. 기존의 네트워크에서 신뢰 관련 담론은 주로 보안과 안전의 개념에 국한하여 논의되어 왔으나, 향후에는 다차원적 네트워크 속성의 최적 조합에 의한 미션 완결성에 중심을 두어야 한다. 따라서, 본 고에서는 '안정성, 서비스성, 생존성, 안전성'을 하위 신뢰 속성으로 보고, 초신뢰(hyper trust)의 개념을 제안하였다. 초신뢰 개념을 바탕으로 네트워크 자체 고도화를 위한 Intelligence for Hyper-Trusted Network 방향성과 고도화된 초신뢰 네트워크가 국가 지능화의 초석이 되기 위한 Hyper-Trusted Network for Intelligence의 양상을 주요 서비스 사용 시나리오를 통해 제시하였다. 초신뢰 네트워크가 국가 지능화 인프라로서 건실한 기반을 제공하기 위해서는 초신뢰에 대한 공감대를 바탕으로 통신사업자와 국가의 합목적적 협력에 의해 인프라를 구축 및 운영해야 하고, R&D 및 산업정책 또한 개별 네트워크 속성과 관련한 분절적 접근이 아닌 초신뢰 보장을 중심으로 한 총괄적 접근으로 재편해야 한다.

## 1 제4차 산업혁명을 위한 신뢰 기반 초연결

제4차 산업혁명을 견인할 범용기술(GPT; General Purpose Technology)로는 데이터의 초연결성과 정보의 초지능성을 들 수 있다. 제4차 산업혁명에서 가치창출 메카니즘은 '데이터 획득(수집) ↔ 지능 생성(분석) ↔ 최적 결정(통제)'의 지속적 반복과정이라고 할 수 있는데, 모든 절차와 단계는 물론 적용 분야(verticals)에서 기본적으로 전제되어야 하는 것이 바로 초연결이다. 초연결은 기존의 연결방식(인간↔인간, 사물↔사물, 인간↔사물)에서 지능이 적극적으로 개입된 실제(physical, real)와 가상(cyber, virtual)의 양방향 연결 양상으로 진화하면서, 기존과는 격이 다른 '혁신의 속도(speed), 적용상 범위·깊이(scope·depth), 시스템 영향력(impact)'을 보여주고 있다.

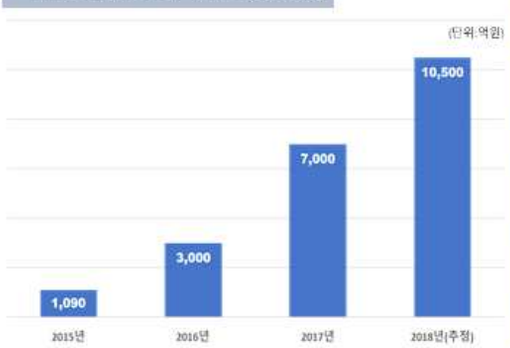
이러한 혁신의 흐름 속에서 네트워크 실패는 단순한 서비스 실패를 넘어 생명을 좌우할 정도로 심각하기 때문에 신뢰 기반 초연결은 선택이 아닌 필수전제조건이며, 초연결의 신뢰성이 담보되지 않는 한, 국가 지능화를 통한 제4차 산업혁명으로의 진전을 기대할 수 없을 것이다.

## 2 네트워크 실패에 따른 부담의 확대

인공지능과 IoT를 기반으로 한 제4차 산업혁명은 정보 및 네트워크 보안이 담보되지 않으면 한계에 부딪힐 수밖에 없다. 랜섬웨어 확산, 가상통화와 IP 카메라 해킹은 물론 IoT 기술이 접목된 디바이스가 늘어나면서 사이버공간이 확장되고, 보호 대상 역시 기하급수적으로 증가하고 있는 상황이다. 랜섬웨어, 가상화폐 탈취 등과 같은 경제적 목적의 해킹으로 인한 개인과 기업의 피해도 증가하고 있지만, IoT 디바이스, 드론, 자율주행차, 원격수술 등에 대한 위협은 기존 정보 유출 및 시스템 파괴에서 비롯되는 경제적 피해는 물론 생명까지 좌지우지할 수 있는 위협으로 심화되고 있는 양상이다.

그림 1 국내 랜섬웨어 피해 규모 및 IoT 분야별 보안 위협 시나리오

국내 랜섬웨어 피해 규모(신고기준)




IoT 분야별 보안 위협 시나리오

| 분야 | 주요 내용 |
|---|---|
| 스마트 TV | 스마트 TV에 탑재된 카메라 해킹으로 사생활 영상 유출 |
| 스마트 가전 | 로봇 청소기 원격조정 애플리케이션 해킹으로 탑재 카메라 실시간 모니터링 |
| 공유기 | 수십만대 인터넷 공유기 해킹하여 DDos 공격 창구로 활용 |
| 스마트카 | 차량 네트워크에 침투하여 고속주행, 브레이크 조작, 방향 변경 등 가능 |
| 의료기기 | 인슐린 펌프 조작으로 약물 치사량 주입가능, 처방 내용 임의 변경 등 |

※ 출처: (좌) 한국랜섬웨어침해대응센터(2018), (우) KISTEP(2016), IoT 분야별 보안 위협 시나리오

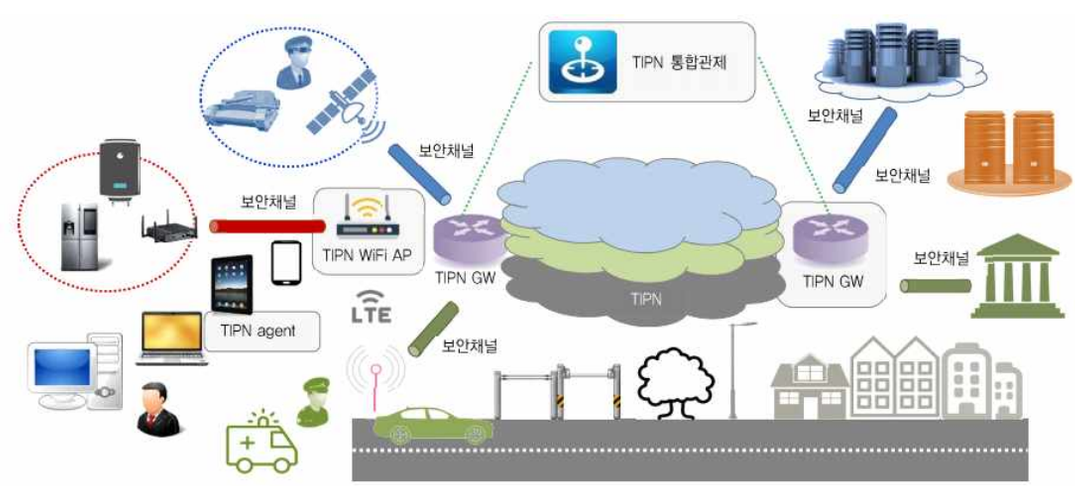
2018년 11월 발생한 서울 KT 아현국사 화재 사고로 서울 5개 구와 경기 고양시 일대 통신 장애가 발생하였다. 이 화재로 인하여 발생한 피해는 인터넷 서비스 및 카드 결제 단말기가 중단되었고, 유무 전화 단절 및 응급 전화 장애 등의 막대한 피해가 발생하였으며, 보상액은 요금 감면 약 350억 원에 소상공인에 대해서는 별도의 피해 보상이 진행 중이다. 이처럼 어떠한 환경에서도 끊김 없이 작동하는 네트워크는 막대한 경제적 손실의 예방은 물론 나아가 제4차 산업혁명 시대 핵심 인프라로서 필수적인 사항이다. 제4차 산업혁명 시대에는 모든 국가 시스템이 지능으로 제어되고, 제어는 네트워크로 연결되는 만큼 연결 인프라인 네트워크의 실패는 개인 생명, 기업 생산, 사회 혼란, 국가 안보 위협 등 그 피해 속도와 규모는 거의 재난에 달하는 수준이 될 것으로 전망된다.

## 3 신뢰 네트워크에 대한 기존의 접근 방향

통상적으로 신뢰 네트워크란 신뢰할 수 있는 사람-사물-데이터가 시간과 장소에 관계 없이 높은 신뢰성을 가지고 연결, 유통되어 정보의 신뢰성을 보장할 수 있는 네트워크를 의미한다. 이러한 통상적인 신뢰 네트워크는 '①접근 신뢰성 보장'과 '②신뢰 영역(trust zone) 형성'이라는 두 가지 접근법이 사용된다.

**접근 신뢰성 보장**은 사용자가 사전에 인가받은 정당한 사용자인지, 접근에 사용되는 단말은 허용된 단말이며 허용된 보안수준을 준수하는지를 판별하는 사전인가 절차라 할 수 있다. 한편 **신뢰영역 형성**은 보안이 강화된 네트워크 노드와 물리적 네트워크의 오버레이를 구성하는 네트워크 가상화, 그리고 단말-네트워크-서버-서비스의 전역적 통합제어를 통해 형성되는데, 신뢰영역에서는 접근이 인가된 사용자 및 단말기에 대해서 안전한 연결성을 보장하게 된다.

그림 2 신뢰네트워크에 대한 통상적인 개념




* TIPN : Trust IP Network

※ 출처: 정부금 외(2017), 초연결 신뢰 네트워크 기술, 전자통신동향분석 41p

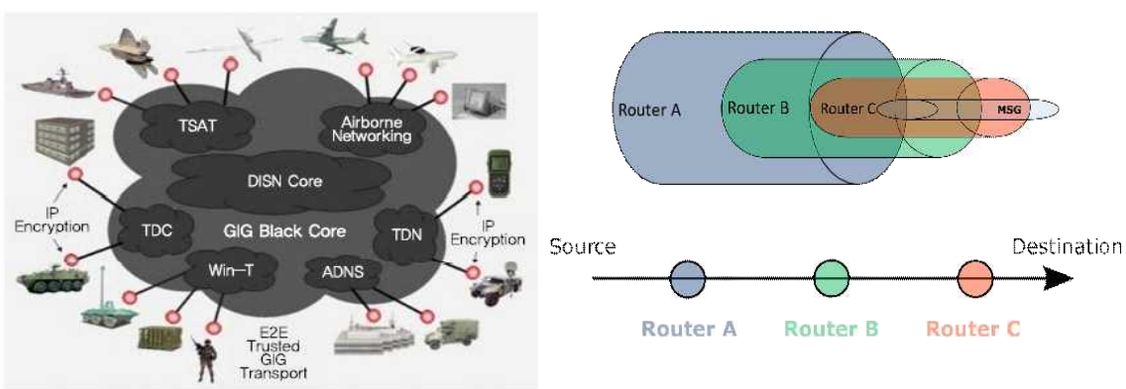
이러한 신뢰 네트워크 구현을 위해 다양한 관점에서 기술이 개발되고 있는데, Zero Trust Security Model, Black Core Network, TOR, 양자암호통신 등이 대표적 사례이다.

**Zero Trust Security Model**은 2010년 Forrester Research Inc.에서 고안한 보안모델로, 기존 IT보안이 네트워크 외부로부터의 진입은 어렵지만 인가를 받은 사용자의 네트워크 연결과 접속이 자유로운 성-해자(castle-moat) 모델 접근법을 사용하는 것을 감안하여 내부자 위험에 주목한 모델이다. 즉, Zero Trust Security Model은 네트워크 외부자뿐만 아니라 내부자에 의해서도 공격이나 정보 유출이 발생할 수 있다는 개념에서 출발한 것으로 네트워크 자원에 접근하려는 모든 사람에 대하여 확인하고, 단계적 혹은 차등적인 접근 권한을 부여하게 된다. 이러한 Zero Trust Security 모델의 대표적인 사례는 Google의 BeyondCorp가 있는데, 액세스 제어 기능을 네트워크 에지에서 개별 기기로 이전하여 직원들이 전통적인 VPN을 사용하지 않고도 장소에 상관없이 안전한 업무를 수행할 수 있도록 하고 있다. 최근 기업 비즈니스 환경이 공공 혹은 사설 클라우드 기반으로 구현되어 내부 이용자의 IT자원에 대한 접근이 빈번해지면서, 이러한 Zero Trust Security Model은 기업의 신뢰네트워크 구현을 위한 유용한 방법으로 평가받고 있다.

**Black Core Network 기술**은 2020년 미국 국방인터넷의 고도화를 위해 미국 국방성을 중심으로 개발되고 있는 신뢰 네트워크 기술로, 데이터의 신뢰성을 보장하기 위해 암호화 프로토콜을 사용하여 데이터를 암호화한다. 그리고 암호화 프로토콜(HAIPE)이 탑재된 라우터의 주소를 수시로 변경하여 네트워크를 음영화함으로써 데이터 자체의 보안성과 end-to-end 데이터 전달의 신뢰성을 제고한다.

이와 유사한 기술로는 미 해군연구소가 개발한 TOR기술이 있는데, **TOR기술**은 네트워크 노드를 거칠 때마다 마치 양파처럼 데이터를 계속 암호화하여 전송하고, 트래픽 추적을 회피하기 위해 중계서버를 이용하며 패킷에는 최종목적지에 대한 정보 없이 다음에 전송할 중계서버에 대한 정보만 기록되어 네트워크 경로를 은닉하는 방법이다.

**그림 3** Black Core Network(좌)와 TOR(우) 개념도




※ 출처: Black Core Network 이미지(전자통신동향분석, 2017) 및 TOR 이미지(www.wikipedia.org)

**양자암호통신**은 에너지 최소 단위인 양자의 복제불가능한 특성을 이용한 통신 암호화 기술로, 전송구간에서는 현존하는 어떠한 해킹기술로도 침입이나 정보탈취가 불가능한 보안체계를 구축할 수 있다는 점에서 주목을 받고 있으며, 국내에서는 SK텔레콤이 전용 중계장치를 국내기술로 개발하여 상용망에 적용하고 있다.

이러한 기술 외에 새롭게 등장한 신뢰 네트워크 기술로는 **블록체인 기술**이 세간의 주목을 받고 있다. 기존 신뢰 네트워크가 중앙집중식 보안 관리 및 제어를 통해 외부의 사이버 공격이나 내부의 정보유출로부터 IT자원을 보호하는데 비해, 블록체인은 관련 사업영역에 참여하는 모든 대상자가 분산원장을 통해 자료(정보)를 공유하고, 이를 서로 상호대조하는 합의에 의해 상호 인증함으로써 데이터 및 정보의 신뢰를 보장하게 된다. 블록체인은 데이터 분산저장과 더불어, 상호비교 및 합의를 통해 데이터의 정합성과 투명성이 보장되기 때문에 지능사회에서 발생하는 다양한 비즈니스 거래 및 응용 서비스 영역에서 폭넓게 활용될 수 있다.

## 4 초신뢰 네트워크에 대한 새로운 시각

기존의 신뢰 네트워크 논의는 보안의 개념에만 국한시켜 왔으나, 원래 신뢰란 다차원적인 속성을 지니고 있으므로 신뢰 확보를 위한 다양한 네트워크 속성을 논의해 보고자 한다.

**신뢰성(reliability)** : 오류가 없다는 뜻으로 일정 기간 동안 고장이나 실패없이 주어진 기능을 올바르게 수행할 수 있는 능력을 의미하며, 일반적으로 신뢰성은 오류 발생까지의 작동 시간, 즉 실질 가동시간인 MTBF[1]로 평가

**가용성(availability)** : 시스템에서 자원(장비)을 필요로 할 때 언제든지 요구사항을 만족시킬 수 있는 능력을 의미하는 것으로, 일반적으로 신뢰성을 가늠하는 MTBF와 함께 평균 오류복구시간(MTTR)을 도입하여, 총가동시간 대비 실질가동시간의 비율[2]로 측정

**표 1** 가용성 수준별(1~6 Nine) 오류 시간 허용치와 적용 가능 분야

| 수준 | 가용성 | 오류 시간/년 (최대) | 적용 가능 분야(예시) |
|---|---|---|---|
| 1 | 90% | 36D 12H | personal clients, experimental systems |
| 2 | 99% | 87H 36M | entry-level business systems |
| 3 | 99.9% | 8H 46M | top ISP, mainstream business systems |
| 4 | 99.99% | 52M 33S | high-end business systems, data centers |
| 5 | 99.999% | 5M 15S | carrier telephony, health systems, banking |
| 6 | 99.9999% | 31.5S | military defense systems |

※ 출처: Bradley Mitchell(2019), Availability Concepts for Networks and Systems

1) 평균오류간격(Mean Time Between Failures)으로 오류 복구에서 그 다음 오류 발생 시점까지의 평균적인 가동시간을 의미하고, '총가동시간/총오류회수'로 측정
2) 평균오류복구시간(Mean Time To Repair)은 오류를 복구하는데 걸리는 평균적인 시간을 의미하고, 가용성은 '(MTBF)/(MTBF+MTTR) = (실질가동시간)/(총가동시간)'으로 측정

**생존성(survivability)** : 시스템 차원의 속성으로 시스템내 자원(장비)의 실패나 예상치 못한 사고 발생시에도 주어진 요구사항에 부합하여 지속적으로 서비스를 제공할 수 있는 시스템적 능력

**서비스가능성(serviceability)** : 서비스 시나리오별로 매우 다양하고 상이한 네트워크 속성 혹은 성능 요구사항에 대해 맞춤형으로 조합하여 원하는 수준의 서비스를 만족스럽게 제공할 수 있는 능력[3)]

**안전성(security)** : 물리적인 또는 소프트웨어 방어 도구를 이용해 기반 네트워크 인프라를 승인되지 않은 액세스나 오용, 오동작, 수정, 파괴, 부적절한 노출 등 내·외부로부터 네트워크를 보호하는 능력[4)]

앞에서 언급한 바와 같이 신뢰(trust)란 보안 및 안정성이라는 단일한 속성만으로만 이뤄진 것이 아니라, 서비스 완결과 관련한 다양한 속성의 다차원적 조합에 의해서 확보될 수 있다. 따라서, 본 고에서는 기존 신뢰 네트워크와 구별하기 위하여 다차원적 신뢰 속성의 최적 조합에 의해 획득되는 신뢰 기반 네트워크를 **'초신뢰 네트워크(hyper-trusted network)'**라고 정의하고자 한다.

초신뢰 네트워크를 구성하는 다차원 하위 신뢰 속성을 도출하기 위하여 네트워크가 수행해야 할 요구 조건을 미션 수행 완결성 측면에서 재구성해보면 '**안정 신뢰성**(Stability : reliability, availability), **서비스 신뢰성**(Serviceability : eMBB, LLC, mMTC), **생존 신뢰성**(survivability), **안전 신뢰성**(security)'으로 유형화 할 수 있다.

**표 2** 초신뢰 네트워크를 구성하는 다차원 하위 속성

| 초신뢰 네트워크 속성 | 구성 요소 | 개념 |
|---|---|---|
| Stability | Reliability | 자원(장비)의 무결성 및 가용성에 기반한 **네트워크 안정성** |
| | Availability | |
| Serviceability | eMBB | 네트워크 자원의 최적 조합으로 사용 시나리오별 요구사항을 만족시키는 **네트워크 서비스 제공성** |
| | LLC[5)] | |
| | mMTC | |
| Survivability | - | 어떠한 상황에도 주어진 미션을 중단없이 수행하는 **네트워크 생존성** |
| Security | - | 내외부 공격·위협으로부터 완벽하게 시스템을 방어하는 **네트워크 안전성** |

3) ITU의 IMT Vision 문서는 지능화 시대 인프라인 5G 서비스가능성을 위해 8개의 주요 성능 파라미터를 제시하였고, 이를 서비스 요구별로 8개 주요 성능지표를 조합하여 3대 사용 시나리오인 eMBB(enhanced Mobile BroadBand), URLLC(Ultra-Reliable and Low Latency Communications), mMTC(massive Machine Type Communications)를 구성

4) ITWorld(2018), 네트워크 보안의 이해; 정의, 방법론, 일자리

5) URLLC에서 네트워크 안정성(stability)에 reliability가 있으므로, UR(ultra-reliable) 제외

## 5 국가 지능화 연결 인프라로서 초신뢰 네트워크

국가 지능화는 수많은 인적·물적 자원이 상호연결되어 생성되는 수많은 데이터를 기반으로 구현된다. 따라서 네트워크는 전달과 소통이라는 단순한 연결(connectivity)의 개념에서 탈피하여, 국가 생태계의 지속가능성을 담보한 '신뢰할 수 있는 지능'을 구현하는 인프라로서 역할을 부여받고 있다. 신뢰성 있는 지능 인프라를 구현하기 위해 통상적인 개념인 '보안'에 중점을 둔 '안전 신뢰성'과 더불어 '안정 신뢰성', '서비스 신뢰성', '생존 신뢰성'이 더해진 초신뢰 네트워크로 발전하고 있는데, 이렇게 확장된 초신뢰 네트워크는 인공지능이 가미된 자율 네트워크 기술을 사용하여 구현될 수 있다.

지능화를 통한 초신뢰 네트워크의 구현은 소프트웨어 중심의 네트워크 기술이 발전으로 가능하게 되었다. 대표적으로 SDN[6]기술, NFV[7]기술, 그리고 인공지능 기반 자율네트워크 기술을 들 수 있다. SDN과 NFV 기술은 다양한 공공·산업분야에서 필요로 하는 네트워크 서비스 속성을 달리하여 수요 맞춤형(on demand)으로 제공하는 네트워크 슬라이싱(slicing) 서비스[8]를 가능케 함으로써 '서비스 신뢰성'을 제고할 수 있게 한다.

하지만, 이러한 SDN과 NFV 기술도 결국에는 사람에 의한 작업을 동반하므로, 더욱 복잡해지고 어려워지는 미래 네트워크 서비스 환경을 위해서는 인공지능을 통한 네트워크 지능화 기술이 필요하다. 궁극적으로는 인공지능에 의해 네트워크 구성, 최적화, 복구, 운영 등이 가능한 자율네트워크(Autonomous Network)로 발전하여 인간의 개입 없이도 최적의 서비스와 운영이 가능한 네트워크 서비스 환경이 구현될 것으로 예상되고 있다.

자율네트워크가 구현되면 네트워크 장비의 이상 상태를 사전에 탐지하여 네트워크 실패를 방지할 수 있을 뿐만 아니라, 네트워크 실패가 발생하더라도 down time을 최소화하여 '안정 신뢰성'을 높일 수 있게 된다. 또한, 응급 상황이나 예측치 못한 이벤트 발생시 최적 경로나 우회경로를 신속하게 자동 설정함으로써 '생존 신뢰성'이 강화될 수 있다. 그리고 외부로부터 사이버 공격 혹은 내부 정보 유출 감지와 자동화된 방어체계 가동으로 기존보다 강화된 보안체계의 구축이 가능해진다. 자율네트워크는 초신뢰 네트워크를 실질적으로 구현해 줄 뿐만 아니라, 초신뢰 네트워크의 기능을 보다 강화시켜 주는 것이다. 아울러, 인공지능과 연계된 자율네트워크는 초신뢰의 4가지 특성(안정신뢰성, 서비스 신뢰성, 생존 신뢰성, 안전 신뢰성)을 이용자의 수요에 맞게 차별적으로 제공하는 트러스트 슬라이싱(trust slicing)을 가능하게 할 것이다.

---

6) Software Defined Network(SDN)은 노드간 패킷의 이동과 관련된 전송부(data plane)과 어떠한 flow로 패킷을 전송할지는 결정하는 제어부(control plane)을 이원화하고, 제어부를 프로그래머블 콘트롤러로 구현하는 기술로, 네트워크 시스템의 일괄제어·통합제어를 가능케 하는 소프트웨어 중심 제어·관제 기술

7) 네트워크 기능 가상화(NFV) 기술은 일반 서버의 가상화 기술을 이용하여 가상머신(Virtual Machine)상에서 네트워크 기능을 소프트웨어를 통한 네트워크 기능 구현 기술

8) 네트워크 슬라이싱은 수요 맞춤형 서비스를 제공하기 위해 필요한 논리적 가상네트워크를 생성 및 이전하고, 즉각적이면서 복잡한 대응을 소프트웨어로 제어·관제함으로써 '서비스 신뢰성'을 보장

초신뢰 네트워크는 트러스트 슬라이싱을 통해 서비스 사용 시나리오별(service use case)로 요구하는 네트워크 속성을 자율적으로 제공할 수 있어야 한다. 사용 시나리오는 우선 민간(private)과 공공(public)으로 대별하고, 민간의 경우는 1차, 2차, 3차 산업을 대표하는 분야를 선정하여 속성별 요구 수준을 분석하였고, 공공의 경우는 파급효과가 큰 국방, 에너지 등을 중심으로 속성별 요구 수준을 분석하였으며, 결과는 아래의 표와 같다.

**표 3** 서비스 사용 시나리오별 네트워크 속성 요구 : 네트워크 속성 이퀄라이저

| Sector | Stability | | Serviceability | | | Survivability | Security |
|---|---|---|---|---|---|---|---|
| | Reliability | Availability | eMBB | mMTC | LLC | | |
| Aagriculture, Forestry, Fising | | | | | | | |
| Mining | | | | | | | |
| Automotive | | | | | | | |
| Manufacturing | | | | | | | |
| Construction | | | | | | | |
| Financial, Insurance | | | | | | | |
| Healthcare | | | | | | | |
| Hospitality | | | | | | | |
| Transport | | | | | | | |
| Logistics | | | | | | | |
| Arts, Entertainment | | | | | | | |
| Information Communications | | | | | | | |
| Professional services | | | | | | | |
| Real estate activities | | | | | | | |
| Wholesale, Retail | | | | | | | |
| Defense | | | | | | | |
| Energy | | | | | | | |
| Utillities | | | | | | | |
| Education | | | | | | | |
| Public service | | | | | | | |

사용 시나리오별 네트워크 속성 수준은 각 네트워크 속성에 대한 통신사 및 제조사, 기존 문헌에서 제시하는 수준을 우선 설정하고, 네트워크 관련 경제, 경영, 정책 및 기술 전문가 합의에 의해 결정하였다. 먼저 안정성의 경우 전게서(Bradley Mitchell, 2019)의 적용 분야를, 서비스가능성의 경우 에릭슨, 삼성, 노키아, 화웨이에서 발표한 시나리오 및 5G 백서를, 생존성 및 안전성은 영향력과 필수성 등을 참조하여 속성 수준의 범위와 기준을 1차적으로 설정하였고, 이어 전문가 회의를 통한 합의 방식에 의해 사용 시나리오별 네트워크 속성 요구 수준을 최종 결정하였다.

## 6 전략적 시사점 : R&D 및 정책 관점

지금까지 초연결 지능사회에서 신뢰의 필요성과 중요성에 대해서 논의하였고, 신뢰 네트워크에 대한 전통적인 접근과 함께 주요 기술을 살펴보았으며, 네트워크에서 신뢰성의 관점을 보안 및 안전 중심에서 다차원 신뢰 속성을 만족시킬 수 있는 네트워크 미션 완결성 중심으로 확대해야 한다는 초신뢰(hyper-trust)의 개념을 제안하였다. 이어서, 이러한 초신뢰의 개념이 네트워크에 내재화 되기 위한 Intelligence for Hyper-Trusted Network의 방향성과 제4차 산업혁명의 초석이 되는 국가 지능화를 위한 Hyper-Trusted Network for Intelligence의 양상을 주요 서비스 사용 시나리오를 통해 제시하였다.

국가 지능화를 위한 인프라로서 초신뢰 네트워크를 구축하기 위해서는 우선, 신뢰에 대한 기존의 관점을 확장한 초신뢰에 대한 공감대를 형성해야 하고, 이를 바탕으로 과거 분절적인 접근보다는 네트워크에 대한 총체적 접근이 필요하다.

우선, 신뢰 네트워크 구축 및 운영 주체 측면에서, 국가 지능화는 국가 안보, 산업 경쟁력, 공공서비스 등 국민의 삶과 직결되는 것이므로, 이를 위한 인프라인 초신뢰 네트워크의 구축과 운영 의무가 통신사업자만의 역할은 아니다. 예를 들어, 생존 신뢰성 극대화를 위한 네트워크 이원화, 재난·재해를 대비한 예비망, 산업용 네트워크(IIoT)를 위한 투자 등 시장성·경제성에 부합하지 않는 경우 국가가 개입하여 사업자에 대한 산업적 유인책을 제시하거나, 국가 주도형으로 신뢰 네트워크 구축을 진행할 필요도 있다.

또한, 네트워크 관련 정부 정책 측면에서, 기존의 R&D 혹은 산업 정책은 초고속·광대역, 지능화, 보안, 소재·부품·장비 국산화 등 네트워크 속성의 고도화, 또는 5G, 기가인터넷, 재난통신 등 네트워크 서비스의 고도화를 중심으로 추진해왔다. 그러나, 국가 지능화를 위한 첫걸음은 이러한 네트워크의 다차원 하위 속성을 모두 결합하여 신뢰성이 담보되는 초연결 인프라 구축부터 시작되어야 한다. 국가 지능화가 진전될수록 신뢰성이 결여된 연결 인프라의 폐해는 상상을 초월하는 재난을 초래할 수 있기 때문이다. 따라서, 네트워크 R&D 및 산업정책은 어떤 상황에서도 신뢰를 담보할 수 있는 초신뢰 네트워크를 중심으로 재편되어 국가 지능화, 나아가 제4차 산업혁명을 위한 건실한 초석을 다져야 한다.

www.etri.re.kr

본 보고서는 ETRI 기술정책연구본부 주요사업인 "ICT R&D 경쟁력 제고를 위한 기술경제 및 표준화 연구"를 통해 작성된 결과물입니다.



ETRI Electronics and Telecommunications Research Institute

34129 대전광역시 유성구 가정로 218
TEL. (042) 860-6114 FAX. (042) 860-6504