국방 5G 운영을 위한 보안정책과 단계별 구축에 대한 고찰

송원석[1] · 조준하[1] · 강성문[1] · 이민우[2,*]

[1]안보지원사령부 국방보안연구소 · [2]아주대학교

A Review of Security Policy and 3-Steps for Defense 5G

Won-Seok Song[1] · Jun-Ha Cho[1] · Seong-Moon Kang[1] · MinWoo Lee[2,*]

[1]Defense Security Support Command · [2]Ajou University

E-mail : s506439@dssc.mil.kr / wearegoodman@naver.com / smkang111@korea.com / iminu@ajou.ac.kr

요 약

5G 기술은 국방분야에서 게임 체인처(game changer)에 관련된 다양한 기술에 접목될 것이다. 또한 모바일 업무 환경 구축도 활용될 것이다. 5G는 이전 기술과 다른 주요 기술로 인해 새로운 위협이 등장하였다. 그리고 5G 기술로 인해 모바일 기술을 국방분야에 적용하려는 요구가 증가하고 있다. 본 논문에서는 국방 5G 운영을 위한 보안정책과 3개로 구성된 단계별 구축 방안을 살펴본다.

ABSTRACT

5G technology will be applied to various technologies related to game changers in the defense field. In addition, the establishment of a mobile work environment will be utilized. 5G has emerged as a new threat due to major technologies different from previous technologies. And due to 5G technology, there is an increasing demand to apply mobile technology to the defense sector. In this paper, we look at the security policy for defense 5G operation and the step-by-step construction plan consisting of three.

키워드

Military 5G, Security Poligy, Mobile Network

Ⅰ. 서 론

최근 5G(Fifth Generation) 이동통신 기술은 사물인터넷(IoT: Inter of Things), 인공지능(AI: Artificial Intelligence), 차량 통신(V2X: Vehicle to Everything), 확장 현실(XR: eXtended Reality)을 구현하는 데 사용되고 있다.

5G 기술을 국방분야에서 활용하기 위한 다양한 계획이 만들어지고 있다. 미 국방부는 5G 기술을 이용하는 차세대 시스템 개발에 투자를 강화하고, 무기체계 네트워크를 통해 모든 전투 기능을 지원할 계획을 추진 중이다.

우리 국방부는 국방분야의 이동통신 기술 구축 전략이나 획득을 위한 지침을 구체화하는 단계에 있다. 미래 전장에서 게임 체인저 운영에 필요한 기반체계로서 5G를 이용하는 방안이 검토되고 있다. 그리고 5G 기술 기반의 이동통신체계를 구축하여 언제, 어디서나 정보를 활용할 수 있도록, 비공개 업무자료와 비밀자료를 유통할 수 있는 보안대책 수립도 추진 중이다.

본 논문에서는 국방분야에 5G 기술을 도입하는데 있어서 5G 기술의 보안이슈와 대책을 살펴본다. 그리고 사설 5G(Private 5G) 체계를 중심으로 5G 구축을 위한 단계별 방안을 제시한다.

Ⅱ. 국내외 국방분야 5G 구축 동향

2.1 미 국방부 동향

미 국방부는 모바일 업무환경 구축 전략으로 ① 모방일 기기 지원을 위한 무선 인프라 확충 ② 정책과 표준 마련 및 관리 시스템 구축 ③ 개발 프레임워크 수립 및 인증 절차 정립을 추진하고 있다.

또한 모바일 환경에서의 데이터 보안 등급을

* corresponding author

DMUC(DoD Mobility Unclassified Capability), DMCC-S(DoD Mobility Classified Capability-Secret, DMCC-TS(DMCC-Top Secret)으로 구분하여 5G 기반체계에서 데이터 보호정책을 구체화하고 있다.

실제로 미 육군은 5G 기술을 이용하는 증강 및 가상현실 고글(gogle) 실험을 추진하였고, 미 해군은 군수 작전에 5G 망을 적용하는 시험을 진행 중이다. 미 공군은 유타 주 힐 공군기지와 넬리스 공군기지에서 5G 기반의 지휘통제체계 생존성 향상을 위한 실험을 추진 중에 있다.

2.2 우리 군 동향

국방부는 국방분야에 군 스마트 폰 활용을 위해 단말 보안통제 강화, 음성과 문자 데이터의 암호화, 정보보호체계의 간접연동에 대한 보안대책 마련을 추진 중에 있다.

하지만 작전관련 영상 데이터에 대한 보안 등급 지정의 모호함과 상용망에서의 보안이슈 등으로 인해 일반 자료에 한해 사용하도록 제한하고 있다.

육군은 모바일 업무수행체계를 구축하기 위해 보안 장비 개발, 군 전용 주파수 확보 등 자체적으로 실증 방안을 모색 중이다. 해군은 함정 내에서 일반 정보와 승조원 건강 관리, 함정 안전 관리 등에 LTE 기술을 활용하고 있다. 공군은 기존 LTE 체계를 5G로 전환하기 위한 정보화전략계획(ISP: Information Strategy Plan)을 추진할 예정이다.

III. 5G 핵심기술의 보안이슈와 대책

3.1 SDN/SDMN 위협 보안대책

소프트웨어 기반의 네트워크 기능 구현으로 개발 속도가 향상됨에 따라 보안 위협 역시 증가하고 있다. 또한 기존 시스템과 연결 접점이 다양해지므로 이들 연동 구간에서 취약점 발생 가능성이 증가한다.

따라서 안전한 암호기술을 이용하는 인증체계를 기반으로, 신속한 보안 패치와 업그레이드 관리가 필요하며, 보안정책 기반의 통신체계, 빅데이터 기반의 보안 관리 체계를 함께 구축해야 한다.

3.2 NFV 위협 보안대책

코어망을 구성하는 네트워크 장비들이 범용서버와 가상화 기술을 이용함으로써 구축 비용이 절감되고 독립적이고 유연한 개발이 가능해진다.

가상화 구현과 다양한 범용 기술을 적용에 따른 공급망 위험 관리가 중요하며, NFV 응용체계의 공통자원에 대한 접근통제와 보안관리 프레임워크 적용이 필요하다.

3.3 MEC와 클라우드 위협 보안대책

MEC는 트래픽의 전송지연을 감소 시키기 위해 네트워크의 에지(edge)에서 처리능력을 갖추는 기술이다. 따라서 기존 이동통신 기반체계에 비해 에지 단에 데이터 전송 경로가 집중되고 코어망 접속과 사용자 데이터 접근이 증가하게 된다.

우선적으로 에지 단에 있는 장비에 대한 물리적 보안이 강화되어야 하고, 대용량 데이터 유출을 통제하는 보안기술이 적용되어야 한다. 또한 신뢰 기반의 모바일 클라우드 컴퓨팅 보안 프로토콜을 사용해야 한다.

3.4 네트워크 슬라이싱 위협 보안대책

네트워크 슬라이싱 기술은 전용 네트워크에서 다양한 서비스를 독립적으로 제공하기 위해 논리적으로 네트워크를 분리한다.

위협으로는 네트워크 슬라이스 관리를 방해하거나 네트워크 자원의 사용을 방해하는 서비스 거부 공격, 다른 네트워크 슬라이스에 대한 부채널 공격이 대표적이다.

대책으로는 네트워크 슬라이스 운영에 필요한 보안 정책의 일관성 있는 관리, 다양한 네트워크 슬라이스에 대한 보안 수준에 맞는 권한 분리와 구획을 적용해야 한다.

IV. 단계적 5G 구축 방안

4.1 1단계 (X-4년 ~ X-3년): 실증 시험

X-4년부터 1년간 민간 이통사 상용망을 임차하여 비공개 업무자료와 일반군사자료를 소통하는 실증 시험을 진행한다. 네트워크는 이통사의 5G 망을 이용하되 네트워크 슬라이싱 기술을 이용하여 논리적으로 네트워크를 구분한다.

비화망 운영을 위해 암호모듈검증(K-CMVP: Korea- Cryptographic Module Validation Program) 인증을 획득한 암호모듈을 탑재한 장비로 체계를 구성한다. 국방망과 상용망(인터넷)은 망분리 상태를 유지하며, 이동성과 보안을 강화하기 위해 UPF(User Plane Function)과 EMG (Enterprise Mobile Gateway)를 구현한다. 개인 단말은 Dual USIM (Universal Subscriber Identify Module) 기술을 사용하여 업무용과 비밀용으로 구분한다.

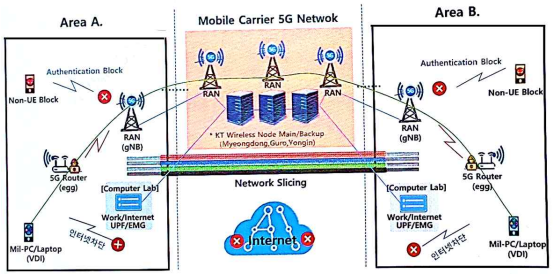

그림 1. 1단계 (X-4년 ~ X-3년): 실증 시험

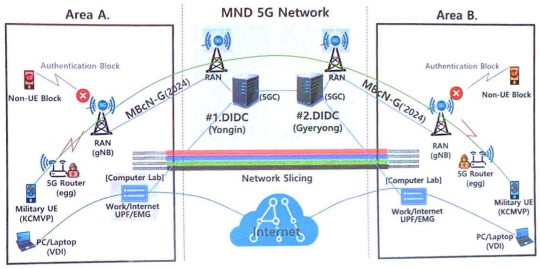

그림 2. 2단계 (X-3년 ~ X-2년): 국방 5G 기반 구축

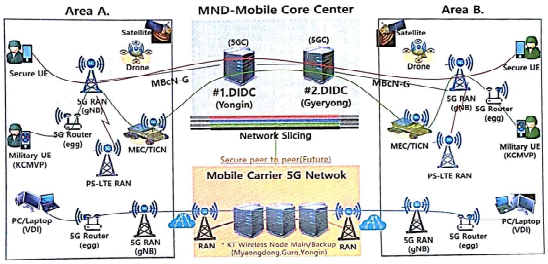

그림 3. 3단계(X-1년 ~ X년): 국방 모바일 코어 센터 구축

4.2 2단계 (X-3년 ~ X-2년): 국방 5G 기반 구축

1단계 실증 시험 후 앞서 임차했던 상용 코어(core) 장비들은 2단계에서는 국방 전용 코어 장비로 교체된다. 국방 5G 기반체계는 2곳의 국방데이터센터에 설치되어 2중화 된다. 2024년에 구축이 완료되는 차기 MBcN 망을 활용하여 국방 5G 기반이 구축하여 시범 운영을 추진한다.

비화망 운영과 UPF/EMG, 그리고 Dual USIM은 동일하게 사용된다.

4.3 3단계(X-1년 ~ X년): 국방 모바일 코어 센터 구축

2단계 시범 운영중 식별된 개선사항을 보완하고, 체계를 전력화하는 단계이다.

상용 이통사의 기지국(RAN)을 제외하고 국방 모바일 코어 센터를 중심으로 군 전용망을 구축한다.

군사 비밀은 비화폰을 사용하여 전송하고, 비공개 업무자료와 일반 군사자료는 실증 시험과 시범 운영중 검증된 비화망 기술을 사용한다.

이동형 MEC와 보안용 망 연동장비 개발을 통해 인터넷과 전장망, 재난안전통신망(PS-LTE: Public Safety-Long Term Evolution)과의 연동을 추진한다.

V. 결 론

본 논문에서는 5G 기술을 국방분야에 적용하는데 필요한 구축방안과 보안위협에 대한 대책방안을 살펴보았다.

본 논문에서 제시한 3단계 구축방안은 미래 국방 이동통신 기술 구축 추진전략과 획득사업 추진 시 보안대책 마련을 위한 포괄적인 안내가 될 것이다.

References

[1] J. G. Park, et al. “Security Trend of Super-Connected Intelligence Infrastructure,” *E-Trend,* ETRI, 2019.

[2] J. G. Park, “5G Edge Security on MEC”, NetSec-Korea, 2020.

[3] H. K. Kim, et al. “Considerations for Security Issues and Cyber Measurement of 5G Network,” IITP, 2019.

[4] NGMN, 2016. (ngmn.org)

[5] R. Khan, et al. “A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions.“ *IEEE Communications Surveys & Tutorials*, 2019.

[6] A. Nieto, et al., “Crowdsourcing analysis in 5G IoT: Cybersecurity threats and mitigation,” *Mobile Networks and Applications*, 2019.

[7] S. M. Park, “5G NSA/SA Threat Trend and Measurement Analaysis,” KISA, 2020.