

미래 군 작전 수행을 위한 군 비지상 네트워크의 구조, 요구조건, 핵심기술

조은정, 전해림, 백호기

경북대학교

cheu03@knu.ac.kr, jhr020528@knu.ac.kr, neloyou@knu.ac.kr

Architecture, Requirements, and Key Technologies of Military Non-Terrestrial Network for Performing Future Military Operations

Eunjeong Jo, Hyerim Jeon, Hoki Baek(Corresponding author)

Kyungpook National Univ.

요약

현대 전장은 더 이상 지상 영역에 국한되지 않으며, 육·해·공·우주·사이버를 아우르는 다영역(Multi-Domain) 환경으로 확장되고 있고, 네트워크 중심 작전 환경(NCOE, Network-Centric Operational Environments)으로 변화하고 있다. 또한, MUM-T(Manned-Unmanned Teaming)와 같이 유무인 복합 체계까지 작전에 참여하면서 이전과 다르게 고도로 동적이고 복잡한 전장 환경이 구성되고 있다. 이러한 환경에서 네트워크에 참여한 모든 유무인 체계들은 자신의 위치, 상태, 타겟 정보 등 전술 정보를 지휘부로 보고하여 전장의 상황 인지를 돕고, 지휘관은 정확하고 신속한 지휘통제를 하여 정밀 타격체계를 통해 적을 완벽하게 제압할 수 있다. 그러나 기존의 지상 기반 통신망만으로는 안정적이고 연속적인 연결성을 보장하기 어렵고 더욱 다양한 플랫폼이 참여할 미래 군 작전 환경을 제대로 지원할 수 없다. 이에 따라 미래 군사 작전을 효과적으로 수행하기 위한 핵심 인프라로서 비지상 네트워크(NTN, Non-Terrestrial Network)에 대한 관심이 증대되고 있다. 그러나 군사 통신은 도청이나 재밍 공격과 같은 위협이 직면하는 경우가 많고, 상용 네트워크와 다르게 요구조건이 매우 엄격하며, 이를 만족하기 위해서는 별도의 기술들이 필요하다. 본 논문에서는 미래 군 작전 수행을 위한 군 비지상 네트워크(M-NTN, Military NTN)의 구조, 요구조건, 핵심기술을 소개한다.

1. 서론

현대 전장은 더 이상 지상 영역에 국한되지 않으며, 육·해·공·우주·사이버를 아우르는 다영역(Multi-Domain) 환경으로 확장되고 있으며, MUM-T(Manned-Unmanned Teaming)와 같이 유무인 복합 체계까지 작전에 참여하는 형태로 진화하고 있다. 이렇게 고도로 동적이고 예측 불가능한 전장 환경에서 기존의 지상 기반 통신 네트워크만으로는 안정적이고 연속적인 연결성을 보장하기 어렵다. 이에 따라 미래 군사 작전을 효과적으로 수행하기 위한 핵심 인프라로서 비지상 네트워크(Non-Terrestrial Network, NTN)에 대한 관심이 급증하고 있다.

NTN은 저궤도/중궤도/정지궤도 위성, HAP(High altitude platform), UAV(Unmanned aerial vehicle) 등과 같은 우주 및 공중 플랫폼을 활용하여 지상 노드들을 연결하여 통신 서비스를 제공한다. NTN은 지상 인프라에 대한 의존도를 낮춤으로써 통신 커버리지 확장, 신속한 전개, 높은 생존성의 강점을 가지며, 지상 통신망이 파괴되거나 교란된 상황에서도 통신 능력을 유지할 수 있다. 이러한 특성 덕분에 동적이고 열악한 전장 환경에서도 지속적으로 군사 작전을 수행할 수 있다.

NTN 플랫폼은 이미 전장에서 사용된 사례가 있다. 예를 들어, 러시아-우크라이나 전쟁에서 Starlink가 제공하는 인터넷 서비스는 지상 네트워크가 심각하게 파괴된 군사적 상황에서 LEO 통신 위성의 실용성을 입증했다. 우크라이나 군은 Starlink를 사용하여 UAV를 제어하고 해당 UAV가 촬영한 공중 영상을 공유하는 GIS Arta 시스템을 운영했다[1]. 이 시스템은 적군 부대의 위치 좌표를 전달하고 아군 포병 부대에 화력 임무를 할당하기 위해 운영되었다. 또한, SpaceX의 Starshield는 상용 Starlink 서비스의 군용 버전인 위성 통신 서비스와 함께 원격 감지 및 표적 추적과 같은 맞춤형 서비스를 제공해 오고 있다.

그러나 NTN의 역할이 증대되에도 불구하고 NTN의 군사적 적용에는 여러 위협이 존재한다. 이러한 위협에는 도청, 재밍 공격[2], 스푸핑 공격

[3] 등이 포함되며, 이는 전술 통신에 중대한 도전 과제를 제기한다. 전술 통신을 지원하기 위해서는 지휘 통제(C2, command and control) 및 상황 인식(SA, Situational Awareness)과 같은 중요한 기능과 관련된 전술 데이터에 대해 통신 보안(COMSEC, communication security)이 보장되어야 한다. COMSEC이 보장되지 않으면 전술 데이터에 대한 도청이나 재밍 공격이 군사 작전의 실패로 이어질 수 있기 때문이다. SATCOM 시스템에 대한 도청이나 의도적인 재밍 공격 사례가 다수 있었다. 2009년 이라크에서는 SkyGrabber라는 도청 도구가 위성 방송 링크를 도청하여 미국의 MQ-1 Predator UAV의 비디오 피드를 기록하는 데 사용되었다 [3]. 2024년 5월에는 Starlink 신호에 대한 정교한 재밍 공격으로 인한 피해가 우크라이나에 의해 보고되었다. 또한, UAV와 지상 노드를 향한 위성 항법 시스템(GNSS, Global Navigation Satellite System) 재밍 또는 GNSS 스푸핑 공격 역시 상당한 피해를 초래할 수 있다. 앞서 언급한 공격들이 결합한 예시로, 2011년 이란군에 의해 포획된 미국의 RQ-170 Sentinel UAV 사례 등이 있다[4].

기존 NTN 기술이 전장의 만연한 위협 속에서 군사 통신을 지원하는 것은 비현실적이다. [2], [4], [5]에서는 이러한 문제들을 해결하기 위해 네트워크 중심 작전 환경을 만족시키기 위한 요구사항을 정의하였다. 제시한 요구사항의 세 가지 공통점은 다음과 같다. 첫째, COMSEC을 보장하기 위해 모든 플랫폼에 주파수 도약(FH, Frequency hopping)이 적용되어야 한다. 둘째, 여러 군사 작전을 동시에 지원하기 위해 각 플랫폼에 고유한 주파수 도약 패턴(FHPs, Frequency hopping patterns)이 할당되어야 한다. 마지막으로, FH는 넓은 대역폭 필요하므로 스펙트럼 공유가 가능해야 한다. 그러나 [2], [4], [5]의 가이드라인에는 몇 가지 한계가 있다. [4]와 [5]에서 제시된 스펙트럼 공유 방법은 고정 위성 서비스와 UAV 전술 데이터 링크(TDLs, tactical data links)만을 위한 것이며, 위성 링크에는 FH가 적용되지 않았고 재밍 탐지 방법도 다루어지지 않았다. [4]와 [5]에

서 제시된 스펙트럼 공유 방법은 고정 위성 서비스와 UAV TDLs만을 위한 것이며, 위성 링크에 FH가 적용되지 않았고 재밍 탐지 방법도 다루어지지 않았다. [2]에서는 FH 시스템이 LEO 위성, HAPs, 그리고 UAVs에 적용되는 새로운 스펙트럼 공유 방법이 제안되었다. 비록 이 접근 방식이 도청 및 재밍 공격에 대한 전송 데이터 보호를 만족시키지만, GNSS 재밍 및 GNSS 스푸핑, 높은 이동성으로 인한 상호 간섭, 그리고 재밍 공격의 탐지 및 복구와 같은 해결되지 않은 과제들이 남아 있다.

본 논문에서는 기존 NTN의 한계를 극복하기 위해 미래 군 작전 수행을 위한 M-NTN의 구조와 새로운 요구사항들을 상세히 설명한다. 그리고 이러한 요구사항을 만족할 수 있는 핵심기술들을 소개한다.

II. M-NTN의 구조, 요구조건, 핵심기술

M-NTN은 군용 NTN으로서 저궤도/중궤도/정지궤도 위성, HAPs, UAVs, 그리고 지상 노드들로 구성된다. 저궤도 위성, HAP, UAV는 지상 노드에 통신 셀을 제공하고, 작전 그룹으로 구분된다. 저궤도 위성 등 위성망은 전략 자산으로 군 전체의 통신 인프라 역할을 수행한다. 반면에, HAP이나 UAV 부대에서 운용하며 고도와 커버리지에 따라 운용 부대의 규모가 달라질 수 있다. 예를 들면, HAP은 군단이나 사단급 이상으로 운용하고, UAV는 사단 이하 부대에서 운용 가능하다. 그리고 각 부대에서는 작전 그룹을 정의하고 참여 노드를 정의하여 작전을 수행한다. 이때, 위성자산은 누구나 접근할 수 있고, HAP이나 UAV는 해당 부대의 작전 그룹에 귀속되어 작전을 수행한다. 따라서 전송 정보 교환은 기존 지상망, HAP이나 UAV 망, 또는 위성망을 통해서 하게 된다.

미래 군 작전 수행을 위한 M-NTN의 요구조건은 다음과 같다. 첫째, 전송 네트워크 핵심 요구조건인 COMSEC을 보장해야 한다. 즉, 모든 전송 데이터는 메시지 암호화인 MSEC(Message security)과 전송 암호화인 TSEC(Transmission security)이 적용되어야 한다. 일반적으로 메시지 암호화와 FH를 사용하여 COMSEC을 보장한다. 둘째, 각 작전 그룹에 참여하는 플랫폼은 고유한 FHP가 할당되어야 하며, 타 작전 그룹이 사용하는 FHP와의 간섭을 고려하여 통신이 가능해야 한다. 셋째, FH는 넓은 대역폭이 필요하기 때문에 별도 대역 확보보다는 스펙트럼 공유 기술이 필요하며, SUs(Secondary users)는 PUs(Primary users)에게 간섭을 일으켜서는 안 된다. 넷째, 통신 링크 재밍이나 도청의 위협을 극복할 수 있는 기술이 필요하다. 다섯째, 전송 정보 QoS(Quality of services)를 보장하는 자원할당 기술이 필요하다. 마지막으로 여섯째, GNSS 재밍이나 불능 환경에서도 플랫폼의 위치 정보를 획득할 수 있어야 한다.

이러한 요구조건들을 만족시킬 수 있는 M-NTN의 핵심기술은 다음과 같다. 첫째, 저궤도 위성의 스펙트럼을 공유하는 FH 기술이다. 저궤도 위성 통신 대역을 UAV나 HAP 기반의 통신 셀이 공유해서 사용하고, 이때 저궤도 위성 통신 빔이 사용하는 주파수를 피해서 FH를 할 수 있도록 FHP를 설계한다. 기존 연구에서는 저궤도 위성의 군용 빔은 SFH(slow frequency hopping)을 사용하고, UAV나 HAP은 FFH(fast frequency hopping)을 사용하도록 설계한 사례가 있다[2]. 둘째, 도청 방지를 위한 secure communication 기술이다. 전송 노드의 존재 자체를 감추는 covert communication이나 도청이 불가능한 PLS(Physical-Layer Security) 방식으로 전송하는 방식이다. 셋째, GNSS 재밍 또는 불능 환경에서도 위치 정보를 획득하는 GNSS-free localization 기술과 통신을 하면서 타겟의 위치를 찾을 수 있는 ISAC(Integrated sensing and communication) 기술이다. 넷째, LEO 위성 통신 시 지상국의 전송 정보 QoS를 고려한 핸드오버 기술이다. 지상국은 대체로 여러 노드들로부터 다양한 전송 정보를 수집한 뒤, 위성으로 통해 전달할 가능성이 높아, 다양한 QoS가 혼재된 데이

터 묶음을 효과적으로 저궤도 위성을 통해 전달할 수 있어야 한다. 다섯째, 정책에 따른 스펙트럼 관리가 필요하다. SFH와 FFH 전용 채널을 어디까지 허용할 것이며, 고정주파수(FF, Fixed frequency) 방식으로 멀티 채널은 몇 개까지 운용할 것인지를 결정해야 한다. 여섯째, 멀티넷을 지원해야 한다. 멀티넷은 여러 FHPs이 동시에 사용될 수 있는 구조로서 여러 미션 그룹이 각자 FHP를 사용하여 작전을 수행할 수 있도록 해야 한다. 마지막으로, 재밍 공격에 대응하여 안정적으로 전송 정보 교환이 가능한 jamming resilience 기술이 필요하다.

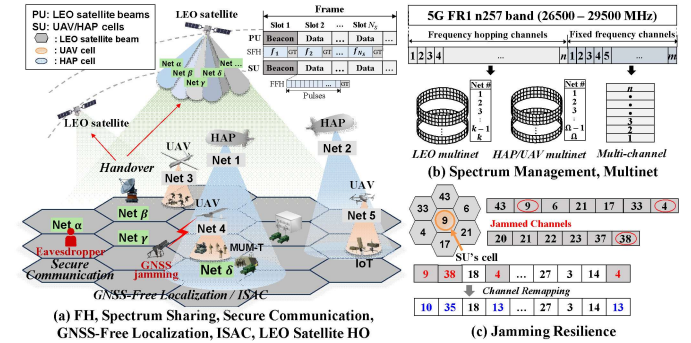


그림 1. M-NTN 구조 및 핵심기술

III. 결론

본 논문에서는 미래 군 작전 수행을 위한 M-NTN의 구조, 요구조건, 핵심기술을 소개하였다. 요구조건은 기존 전송 네트워크의 요구조건에 근거하여 미래 전에서 요구되는 새로운 요소를 도출하였으며, 핵심기술은 요구조건을 만족하는데 필요한 기술로 구성하였다. 핵심기술로는 스펙트럼 공유 기반 FH 기술, 도청 방지를 위한 secure communication 기술, GNSS-free localization 및 ISAC 기술, LEO 위성 핸드오버 기술, 스펙트럼 관리, 멀티넷, jamming resilience 기술을 소개하였다. 본 연구의 결과가 미래 군 작전 수행을 위한 M-NTN 구조의 초석이 되길 기대한다.

ACKNOWLEDGMENT

이 논문은 정부(중소벤처기업부)의 중소기업기술혁신개발사업(시장대응형), 2026년도 경북대 지역산업연계 대학 Open-lab 육성지원사업, 정부(과학기술정보통신부)의 정보통신기획평가원-지역지능화혁신인재양성사업(IITP-2026-RS-2022-00156389)의 지원을 받아 수행된 연구임.

참고 문헌

- [1] S. Wiedemar, "The New Frontier of Space Militarization," CSS Analyses in Security Policy, no. 333, Dec. 2023.
- [2] H. Jeon and H. Baek, "Military Non-Terrestrial Networks Architecture and Spectrum Sharing Method for Mitigating Jamming Attacks and Multiple Access Interference," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 5, pp. 1465-1474, May 2024.
- [3] S. Salim, N. Moustafa, and M. Reisslein, "Cybersecurity of Satellite Communications Systems: A Comprehensive Survey of the Space, Ground, and Links Segments," *IEEE Commun. Surveys Tuts.*, vol. 27, no. 1, pp. 372-425, Feb. 2024.
- [4] H. Baek and J. Lim, "Design of Future UAV-Relay Tactical Data Link for Reliable UAV Control and Situational Awareness," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 144-150, Oct. 2018.
- [5] H. Baek and J. Lim, "Spectrum Sharing for Coexistence of Fixed Satellite Services and Frequency Hopping Tactical Data Link," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 10, pp. 2642-2649, May 2016.