OSI 참조 모델에 의한 사이버전자전 개념 분석

이민우[1] · 이종관[2,*]

[1]아주대학교 · [2]육군사관학교

Conceptual Analysis of Cyber Electronic Warfare by OSI Reference Model

Minwoo Lee[1] · Jongkwan Lee[2,*]

[1]Ajou University · [2]Korea Military Academy

E-mail : iminu@ajou.ac.kr / jklee64@kma.ac.kr

요 약

제5의 전장인 사이버 공간은 전자기 스펙트럼을 이용하여 사이버 공간과 물리 공간 사이에서 다영역 기동에 활용될 수 있다. 이것은 사이버전과 전자전의 특징을 융합하는 사이버전자전의 주요 개념이 된다. 본 연구에서는 OSI 참조 모델을 활용하고, 2계층 데이터링크 계층의 위협 요소를 살펴봄으로써, 사이버전자전 개념을 분석한다.

ABSTRACT

The cyberspace, which is the fifth battle field, should be utilized for multi-domain maneuvering between the cyberspace and the physical space using an electromagnetic spectrum. This becomes a major concept of cyber electronic warfare that combines the characteristics of cyber warfare and electronic warfare. In this study, the concept of cyber electronic warfare is analyzed by using the OSI reference model and examining the threats of the two-layer data link layer.

키워드

Cyber Electronic Warfare, OSI Reference Model, Datalink Layer

Ⅰ. 서 론

정보통신기술(ICT: Information Communication Technology)의 발전에 따라 정보기술(IT: Information Technology)과 운영기술(OT: Operation Technology)은 네트워크 기술에 깊이 접목되고 있다.

이러한 모습은 미래 전장에 대비하기 위한 미래 전력을 개발하고 획득하는 국방분야에서는 더욱 적극적으로 나타나고 있다. 예를 들어 게임 체인저(game changer)로써 무인체계를 이용하기 위해 5G 기반의 지휘통신체계를 구축을 추진하는데 이는 앞서 언급한 기술의 발전 방향을 따르는 것이다.

국방분야에서는 사이버 공간(CS: Cyber Space)을 제5의 전장으로 인식하면서 새로운 작전 개념으로 사이버전(CW: Cyber Warfare)을 정립하고 있다. 사이버 공간은 전자기 스펙트럼(EMS: Electromagnetic Spectrum)을 이용하여 사이버 공간과 사이버 공간, 사이버 공간과 물리 공간을 다영역 기동(multi-domain maneuver) 할 수 있다.

그래서 최근에는 사이버전과 기존의 전자전(EW: Electronic Warfare)을 함께 다루는 사이버전자전(CEW: Cyber - Electromagntic Warfare)에 대한 연구가 이뤄지고 있다.

본 논문에서는 사이버전자전의 개념을 가시적으로 이해하기 위해, OSI(Open Systems Interconnection) 참조 모델 중 2계층인 데이터링크 계층의 관점으로 사이버전자전의 특징을 살펴본다.

II. 데이터링크 계층의 특징

OSI 참모 모델은 1970년대 인터넷의 탄생과 함께 만들어졌다. 각 계층에서는 네트워크 연결에 필요한 독립된 기능이 수행된다.

계층별 기능을 고려하여 심층 방어(defense in depth) 기법에서는 각 계층별로 적절한 보안통제를 적용한다. 하지만 네트워크의 물리적 접점과 논리적

* corresponding author

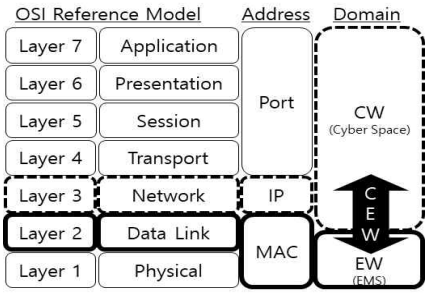

그림 1. OSI 참조 모델과 사이버전자전 위상

접점을 관여하는 2계층(데이터링크 계층)이 침해된 경우에는 3계층~7계층에 적용된 보안통제가 무력화 될 수 있다. 이것은 데이터링크 계층이 다음과 같은 기능을 수행하기 때문이다.

첫째, 데이터링크 계층은 3계층(네트워크 계층)과 1계층의 중간 연결 기능을 수행한다. 예를 들어 IEEE 802.2 표준에서는 LLC(Logical Link Control) 하위 계층을 정의하고 있다. 상위에 있는 네트워크 계층의 소프트웨어를 하위 계층의 장치 하드웨어 사이에서 통신을 담당한다.

둘째, 데이터링크 계층은 사이버 공간의 데이터와 물리 공간의 신호를 서로 변환하는 기능을 수행한다. 예를 들어 IEEE 802 표준에서는 물리공간의 매체에 따라 다양한 MAC(Medium Access Control) 하위 계층을 정의하고 있는데, 이더넷(ethernet)은 802.3, 무선랜은 802.11, 블루투스는 802.15가 대표적인 사례이다. MAC 하위 계층은 매체에 맞춰 데이터의 캡슐화(encapsulation)를 담당한다.

그림 1은 데이터링크 계층의 특징을 고려하여 사이버전자전의 위상을 OSI 참조 모델과 비교한 것이다. 이와 같이 사이버공간과 물리공간을 잇는 기동을 위해 사이버전자전의 기능은 데이터링크 계층에서 이뤄지는 것으로 볼 수 있다.

III. 사이버전자전과 무선 네트워크의 위협

OSI 참조 모델에서 사이버전자전의 위상을 보면, 데이터링크 계층의 위협이 사이버전자전에서 활용되는 공격 기술이 될 수 있음을 알 수 있다.

그림 1에서와 같이 사이버전자전은 사이버공간과 전자기 스펙트럼 공간을 모두 활용한다. 여기에서 전자기 스펙트럼은 곧 무선 기술을 의미한다. 따라서 데이터링크 계층이 무선 매체를 사용하는 무선 통신 기술의 위협이 곧 사이버전자전의 대상이 된다고 볼 수 있다.

표 1은 무선랜(WLAN: Wireless Local Area Network)의 주요 위협을 정리한 것이다. 그림 1과 표 1을 통해 알 수 있는 것은, 사이버전자전 기술을 이용하여 물리 공간에서 사이버 공간으로 다영역 기동하기 위해서는 데이터링크 계층의 역할이 매우

표 1. 무선 네트워크의 주요 위협

Attack Type	Measurement
Interception of data	Data Encryption
Wireless intruders	Access Control
Denial of Service (DoS)	Various
Rogue Access Point	Access Control

중요하다는 점이다. 예를 들어 가짜 접속점(Rogue Access Point)를 이용하려면 네트워크에 직접 접속하거나, 무선의 경우 정상 접속점으로 가장(spoofing) 할 수 있어야 한다. 이것은 네트워크에서 2계층 접속이 가능해야 함을 의미한다.

또한 서비스 거부 공격(DoS)은 전자전에서 전통적으로 수행하는 전자전 공격(EA: Electronic Attack)과 개념적으로 동일하다. 서비스 거부 공격은 다양한 방법으로 수행되기 때문에 이에 대한 대응책은 각각에 맞춰 이뤄져야 한다. 예를 들어, 주파수 무단 점유는 전파 분석기를 이용하여 간섭 주파수를 찾아 방사원을 제거해야 한다. 또 다른 예로는 CSMA/CA(Carrier Sense Multiple Access/Collision Avoidance)의 CTS(Clear to Send) 메시지의 악용에 의한 서비스 거부 공격을 들 수 있는데, 이러한 공격은 네트워크 가입시 인증(authentication) 절차와 단말에 대한 관리를 강화하지 않으면 대응하기가 매우 어렵다.

IV. 결론 및 향후 연구

본 논문에서는 사이버전자전 개념을 가시적으로 이해하기 위해 OSI 참조 모델을 활용하였다. 사이버전자전은 2계층인 데이터링크의 역할이 중요함을 알 수 있었다. 이러한 개념 분석을 바탕으로 사이버전자전에 대한 연구를 고도할 계획이다.

Acknowledgement

이 논문은 2019년 한국연구재단의 지원을 받아 수행하였음. (No. 2019R1G1A100303013)

References

[1] S. Y. Kim, S. P. Kim, B. J. Park, U. S. Jung, H. W. Chu, J. Yoon, J. Y. Kim, “Cyber Electronic Warfare Technologies and Development Directions,” *Journal of Korean Institute of Electromagnetic Engineering and Science* 32(2), 2021.2, 119-126.

[2] T. J. Son, “Cyber Electronic Warfare, Concept and Operational Direction,” *KIDA Defense Issues & Analyses*, vol. 1759, no. 19-20, 2019.