군 사 과 학 연 구 지
제16권 제2호(2023년 12월)

합성전장훈련체계를 위한 GPS 전파교란 모의 논리 연구

A Study on Simulation Logic of GPS Signal Jamming for the Synthetic Battlefield Training System

윤지영[1] · 강동수[2]
Jiyoung Yoon · Dongsu Kang

ABSTRACT

The weapon systems currently heavily rely on GPS(Global Positioning System), but there is a lack of practical training scenarios that assume GPS system is restricted by cyber attack. This paper proposes a simulation logic of GPS signal jamming for the synthetic battlefield training system. GPS signal jamming is categorized into three types: ground-to-air jamming, ground-to-ground jamming, and spoofing. We calculates jamming distance based on GPS jammer, GPS receiver, and signal strength. In addition, we figure out the signal strength of the GPS jammer and provide applicable jamming distances for the Korean peninsula. This simulation logic will contribute to providing a realistic environment of military training.

Key Words : GPS Jamming, GPS Spoofing, Simulation Logic, Synthetic Battlefield Training System, Modeling and Simulation(M&S)

논문접수일 : 2023년 11월 17일, 심사일 : 2023년 11월 27일, 게재확정일 : 2023년 12월 3일

본 연구는 2023년도 ㈜심네트의 육군합성전장체계(Build-I) 체계개발 위탁과제(2023MNS03-3) 지원을 받아 수행되었습니다.

1) 국방대학교 컴퓨터공학전공 석사과정
2) 국방대학교 컴퓨터공학전공 교수 / 교신저자(Corresponding author)

1. 서론

현대전에서 사이버 위협은 국가안보에 주요한 현실적인 위협으로 다루어지며 군사작전 영역인 MDO(Multi-Domain Operations) 환경에서 사이버 작전은 작전적 전술적 관점에서 전쟁 승리를 위해 수행해야 한다.[1-3] 이를 위해 사이버 작전을 통합 연습하고 훈련하는 환경이 필요하다. 대한민국 국군의 다수 무기체계는 GPS에 많은 부분 의존하고 있으나, GPS 시스템이 사이버 공격을 받았을 때를 가정한 훈련을 실질적으로 수행하는 경우는 없으며, 훈련할 수 있는 여건도 부족하다.

본 논문에서는 다수 무기체계에 사용되고 북한의 공격이 예상되는 사이버 전자전 분야의 대표적인 장비인 GPS(Global Positioning System) 재밍을 연구한다. GPS 전파 교란을 지대공 재밍, 지대지 재밍, 스푸핑으로 세 가지로 나누고. GPS 재머와 GPS 수신기와의 거리, GPS 재머의 신호강도에 따른 방해 거리를 두 가지 방법으로 산출한다.

이를 통해 한반도 환경에서 적용할 수 있는 GPS 전파교란 방해 거리를 나타내어, 육군의 합성전장훈련체계를 위한 GPS 전파교란 모의 논리[4]를 제안한다.

논문의 구성은 다음과 같다. 2장에서 GPS 기본 이론과 GPS 전파 교란에 대해 살펴보고, 3장에서는 성능 검사와 전파항법 공식을 이용하여 GPS 전파교란 방해 거리를 산출한다. 이후 4장에서는 GPS 전파교란 모의 논리를 제안하고, 마지막으로 5장에서 마무리한다.

2. 기존 연구

2.1 GPS 시스템

GPS는 지구 전역을 대상으로 위성을 통해 위치와 시각 정보를 제공하는 지구 위성항법시스템으로 지구 대기권 밖에 있는 24개 이상의 GPS 위성 중에서 최소한 4개 이상의 위성항법 신호를 수신하여 위치를 계산하는 원리이다. 각각의 GPS 위성에서 발사되는 신호가 지상 수신기에 도달할 때까지 걸리는 시간을 측정한 후, 이 값에 전파의 속도를 곱해 각 위성과 수신기와의 거리를 계산함으로써 GPS를 이용한 위치측정이 이루어진다.

GPS는 지구상으로부터 약 2만km 상공에서 25W의 신호 세기로 신호를 송신한다. 지상에서 GPS 수신기의 평균 수신신호 세기는 약 -160dBW로 휴대전화의 1/300 수준이기 때문에 수신감도가 미약하여 간섭에 취약하다. 각각의 GPS 위성은 위성에 탑재된 시계의 시각 및 오차와 위성의 상태정보, 모든 위성과 관련된 궤도 정보와 상태 등이 포함된 항법 메시지를 전송한다. GPS 위성에서 발사되는 신호는 반송파, PRN 코드, 항법메시지 세 가지 종류의 신호로 구성되어 있다.

각 인공위성에서는 신호를 보낼 때 표준측위를 위한 반송파인 L1 대역과 고 정확도 측위를 위한 반송파인 L2 대역, L5 대역이 있다. PRN(Pseudo-Random Noise) 코드는 위성마다 유일한 값을 갖도록 하는 이진부호로 구성된다.

PRN 코드는 용도에 따라 C/A(Coarse Acquisition) 코드와 P(Precision) 코드로 구분된다. C/A 코드는 민간에 개방되어있어 누구나 사용 할 수 있으며, P 코드는 암호화가 되어 있어 군용으로 활용된다. C/A 코드는 L1 반송파를 통해 표준위치측정 서비스를 제공한다. P 코드는 L1, L2 대역에 모두 전송되며, 정밀한 위치와 정확한 속도, 시간 등을 제공한다.

P 코드는 기만 방지(Anti-Spoofing) 기능이 있어 적의 GPS 공격을 차단한다. AS는 P 코드를 암호화하여 Y 코드를 만든다. 수신기는 Y 코드를 수신하기 위해 AS 모듈이 있어야 하며, AS 암호키를 규칙적으로 변경하여 사용한다.

GPS 네비게이션 메시지 신호에는 위성의 시각 보정 정보와 궤도 정보 이외에 다른 위성들에 대한 대략의 궤도 정보가 포함된다. 반송파별 중심주파수와 코드는 <표 1>과 같다.

<표 1> 반송파별 중심주파수와 코드

반송파	중심주파수	코드
L1	1575.42 MHz	C/A, P(Y), M
L2	1227.60 MHz	C/A, P(Y), M
L5	1176.45 MHz	P

2.2 GPS 전파교란

GPS 신호를 교란, 위조하여 정해진 경로를 이탈하게 하거나 GPS 관제시스템의 정상적인 통제를 불가능하게 할 수 있다. 이러한 GPS 전파교란은 크게 3가지로 구분된다. GPS 재밍은 GPS 주파수 대역에 큰 신호 전력을 송신하여 GPS 수신기가 GPS 위성 신호를 수신하지 못하게 하는 공격이다. GPS 재방송(Repeat-back Jamming)공격은 위성 신호의 수신시간 지연으로 거리오차를 발생시키는 공격이다.

GPS 스푸핑은 GPS 위성 신호보다 약간 높은 신호로 GPS 신호와 비슷한 위조된 정보를 방송하여 GPS 수신기가 잘못된 위치와 시각을 계산하도록 하는 공격이다. 상용 GPS의 경우에는 주파수, 코드 및 신호 구조가 노출되어 있어 교란이 상대적으로 용이하다.

북한으로부터 GPS 전파교란을 받은 사례는 여러 차례 있었다.[4] 북한은 2020년도부터 2021년까지 전파방해로 여러 차례 교란작전을 수행하고 있다. 이러한 교란작전은 GPS 위성에 대한 높은 의존도를 가진 우리 무기체계에 대해 포격 타격, 유도무기 등에 심각한 손상을 입힐 수 있다.

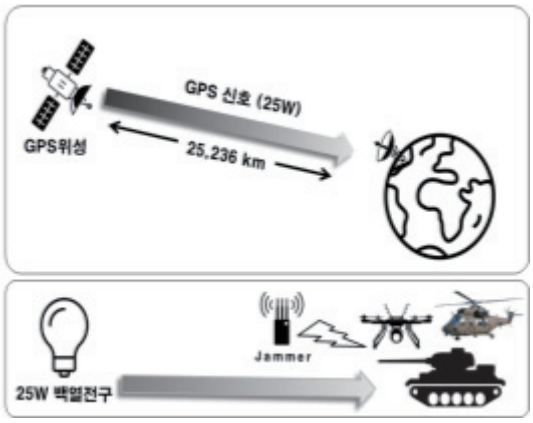
GPS 전파교란은 전파신호를 방해하여 GPS 수신기의 오작동을 일으킬 수 있다. 이러한 방해효과는 재밍 신호의 발생 위치와 GPS 수신기의 위치, 노출시간, 재밍 신호의 강도와 특성 등에 따라 달라진다. 이에 따라 무기체계에 미치는 방해효과도 달라질 수 있다. 또한 재밍 신호의 발생 위치와 강도에 따라 방해 범위가 달라진다. 일반적으로 재밍 신호의 강도가 높을수록 방해 범위가 넓어지며, GPS 수신기와 재밍 신호의 거리가 가까울수록 방해효과가 크다. 따라서 재밍 신호를 사용하여 GPS 수신기를 방해하려는 공격자는 GPS 수신기와 가까운 거리에서 재밍 신호를 발생시키는 것보다 효과적일 수 있다.[5]

GPS 재머가 전파교란 공격을 시도할 때, 각 재머의 신호가 영향을 미칠 수 있는 거리를 산출하기 위해 중앙전파관리소의 무선국 및 전파응용설비의 검사업무 처리기준의 성능검사 공식과 최신전파항법 공식을 참조한다. 지대지 재밍 공격은 이상적인 자유공간에서의 전파 감쇠만 고려했으며 지대공 재밍의 경우에는 대기의 강우감쇠에 따른 전파 손실값을 추가로 적용하여 거리를 산출한다.

2.3 GPS 재머의 재밍 효과

GPS 전파교란 원리는 GPS 신호가 약 25,200km 상공에서 25W의 출력으로 송신되어 지상에서의 수신전력이 극히 미약하여 혼신에 취약하다. GPS 신호 혼신은 <그림 1>과 같이 약 25,200km 상공의 위성에 설치된 25W 백열전구를 지상에서 관찰하는 상황과 유사하여 공격자가 이보다 강한 빛을 비추면 백열전구 불빛을 식별할 수 없게 되는 원리이다.

재밍 신호의 강도가 높을수록 GPS 수신기의 성능에 미치는 영향이 크게 된다. GPS 수신기는 신호 강도에 따라 GPS 신호를 구별하고 위치를 결정한다. 재밍 신호가 강하면 GPS 수신기가 GPS 신호를 감지하지 못할 수 있다. 따라서 재밍 신호가 강할수록 비행체의 GPS 수신기의 성능이 크게 저하된다.



<그림 2> GPS 재밍 원리

그리고, GPS 신호는 무인항공기(UAV)의 비행 경로, 위치 및 속도를 제어하는 데 필수적이며, GPS 재밍은 UAV가 올바른 위치를 식별하지 못하게 하여 비행 경로 및 위치를 제어하는 능력을 무력화한다. 이는 무인항공기가 제어 불능 상태가 되거나 완전히 통제 불능의 영역에 빠질 수 있다.

GPS 재머는 GPS 신호를 방해하거나 차단하여 GPS 수신기가 잘못된 정보를 받거나 아예 신호를 수신하지 못할 수 있으므로, GPS 재밍은 효과적으로 무기체계를 방해할 수 있다.

3. 전파교란 거리 분석

3.1 성능기준 전파교란 거리

전파교란 영향분석을 위해 위성 수신 코드별 J/S(Jamming per Signal Ratio) 성능값과 자유공간경로 손실 수식을 사용하여 재밍 가능 거리를 산출한다.[6] GPS 항재밍 성능은 재머 출력값과 자유공간손실을 고려한 값이 GPS 수신레벨(-130dBm[3]) 보다 큰 값을 가질 경우 재밍이 가능한 것으로 계산한다. GPS 수신레벨은 민간용 25W GPS위성신호(C/A)의 수신 세기가 약 -160dBW(-130dBm)이기 때문에 GPS 수신레벨은 -130dBm으로 산정하였다.

재머 출력값은 GPS 수신기가 신호를 수신하지 못할 때 재머장비의 출력값을 의미한다. 지대공 재밍일 경우 대기편광손실을 고려하여 아래와 같은 식을 적용한다.

J/S = 재머 수신레벨 - GPS 수신레벨
= {재머 출력값 + 대기편광손실
+ 자유공간경로손실(L)} - GPS 수신레벨

L = 32.45 + 20logf(MHz) + 20logd(km)
f = 측정주파수
d = 송신안테나와 수신 안테나 간의 거리

공간손실값은 중앙전파관리소 무선국 및 전파응용설비의 검사업무 처리기준을 참조하여 송신안테나와 수신 안테나 간의 거리는 아래와 같이 표현할 수 있다.

$$d = 10^{\frac{L-32.45-20\log f}{20}}$$

L(dB) 자유공간경로손실

f=1,575.42MHz (GPS 주파수)

GPS 수신레벨 = -130.83dBm

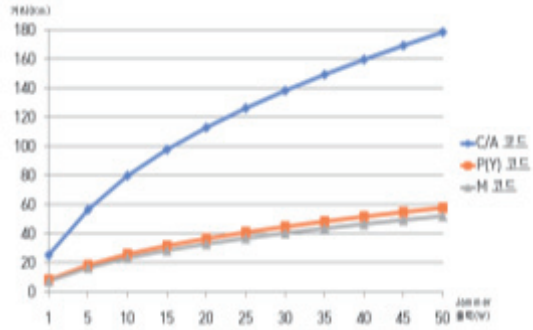
J/S 값(dB)이 높을수록 항 재밍 성능이 우수하며, 계산하면 <표 2>와 같다.

<표 2> 코드별 J/S 값[7]

구분	C/A 코드	P(Y) 코드	M 코드
J/S 값	36.4	46.2	47.1

3) dBm은 GPS 수신감도에 사용되는 단위로 mW를 기준으로 한 전력 측정값으로 mW 단위의 전력을 dB스케일로 나타낸 단위이다.

상용 주파수를 쓰는 L1 C/A의 경우 1W에서 25.21km에서 50W출력의 경우 178.28km로 계산된다. 재머 출력값과 코드를 고려하여 재머가 방해할 수 있는 거리는 <그림 2>와 같다.



<그림 3> GPS 재밍 거리

3.2 전파항법 전파교란 거리

GPS 항재밍 성능 값(J/S)은 대기편광손실과 자유공간경로손실을 반영하여 계산한다.[8] 송신안테나와 수신 안테나 간의 거리는 아래와 같이 나타낼 수 있다.

$$d = 10^{\frac{-L}{20} - \log\left(\frac{4\pi}{\lambda}\right)}$$

L(dB) = GPS 수신레벨 - {재머출력값 + 대기편광손실} + J/S

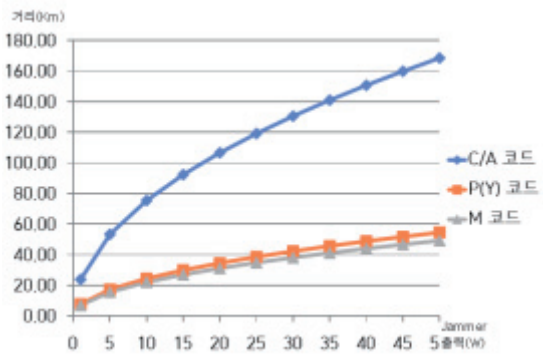
$\lambda = \frac{c}{f}$ *(f=GPS 주파수, c=3×108m/s)*

f = 1,575.42MHz (GPS 주파수)

c = 3×108m/s

대기 및 편광 손실값 = -0.5dB

상용 주파수를 쓰는 C/A 코드의 경우 1W에서 23.84km에서 50W출력의 경우 168.55km로 계산된다. 재머 출력값과 코드를 고려하여 재머가 방해할 수 있는 거리는 <그림 3>과 같다.



<그림 4> GPS 재밍 거리

4. GPS 전파교란 모의 논리

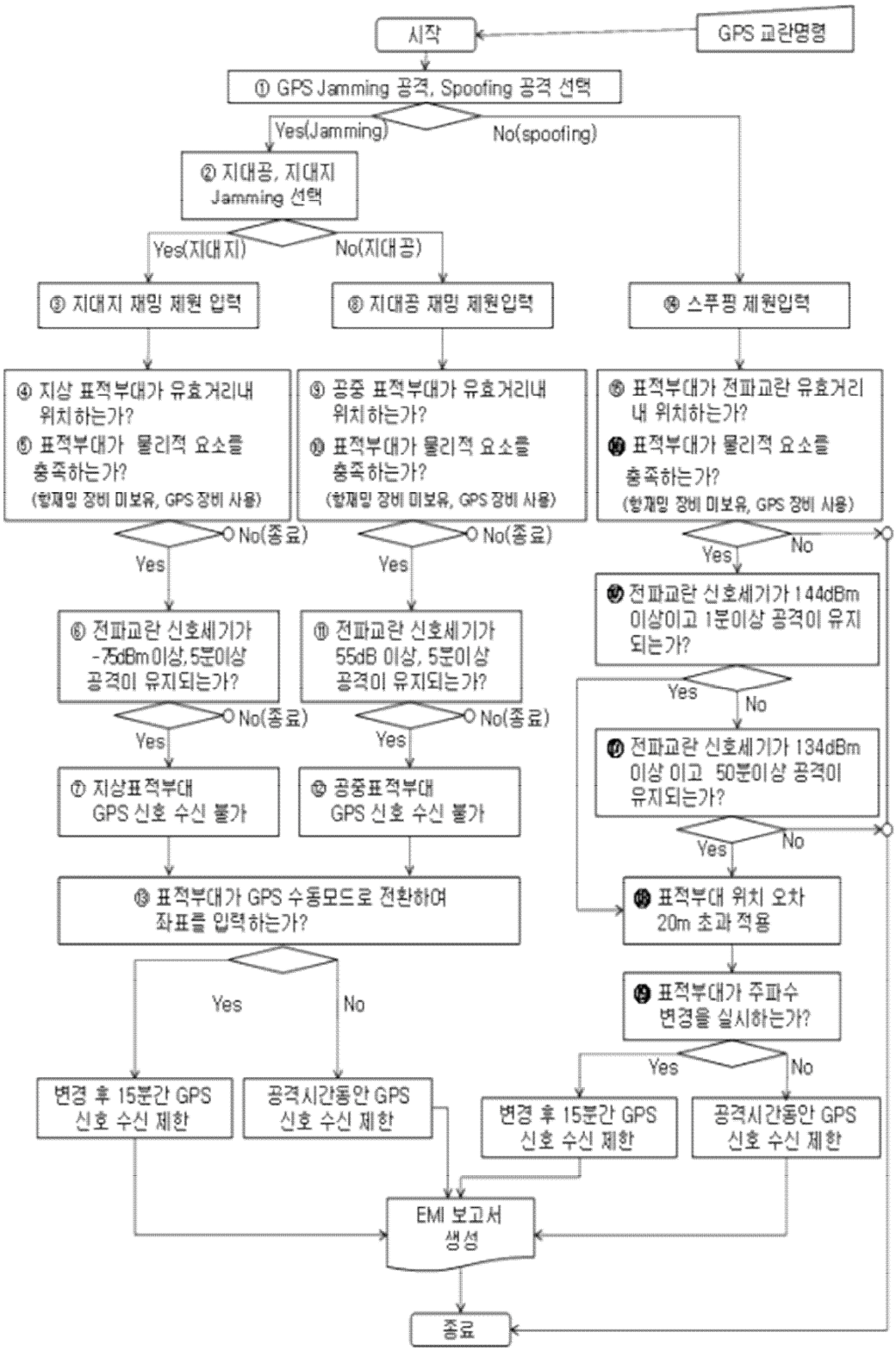
성능검사 공식을 적용한 거리는 지대지, 지대공 GPS 재밍에 적용하고, GPS 스푸핑 공격 간에는 성능 기준과 전파항법 공식을 적용하여 지대공 재밍, 지대지 재밍, GPS 스푸핑 모의 논리를 제안한다. 재머 출력값, 운용부대, 표적부대와의 거리, 사용주파수, 전파교란 지속시간을 고려하여 나타낸 GPS 전파교란 모의 논리는 <그림4>와 같다.

GPS 전파교란 모의 수행은 재밍과 스푸핑으로 나누어 실행되며, 수집된 적 부대지역에 대해 전파 교란을 시행함으로써 방해받은 부대가 일정 시간 동안 표적 확인, 위치보고, 감시자산에 대한 시간 오차 등을 적용하여 수행한다.

먼저 GPS 재밍 또는 스푸핑 공격 여부를 선택하고, 지대지 공격 또는 지대공 공격 여부를 선택한다. 공중에 있는 무기체계들에 대해서는 공역 사용 수단별 운용고도를 감안하여 공격부대와 표적부대 간 측정된 거리를 고려한다.

GPS 재머의 출력값에 따른 교란 가능 거리와, 운용부대와 지상 표적부대와의 거리를 비교한다. GPS 재머의 교란 가능 거리는 표적부대가 사용하는 주파수에 따라 J/S 값 및 교란 가능 거리가 변경된다.

지상 표적부대가 GPS 수신기를 사용하는지



<그림 5> GPS 전파교란 모의 논리

또는 항재밍 장비를 보유하고 있는지 확인한다. 항재밍 능력이 있으면 지대지 재밍 공격을 실패 처리하고 모의를 종료한다. 육군의 일부 무기체계는 패키지 형태로 항재밍 능력이 향상되어 운용되고 있기 때문이다.

재머의 출력값이 -75dBm 이상, 전파교란 지속시간이 5분 이상[9]인지 확인한다. 출력값에 따른 교란 가능 거리 내 지상에 위치한 부대는 GPS 신호 및 좌표값을 사용할 수 없게 된다.

공중표적부대가 GPS 수신기를 사용하는지 또는 항재밍 장비를 보유하고 있는지 확인한다. 항재밍 능력이 있으면 지대지 재밍 공격을 실패 처리하고 모의를 종료한다. 육군 일부 무기체계는 패키지 형태로 항재밍 능력이 향상되어 운용되고 있기 때문이다.

재머의 출력값이 55dB 이상, 전파교란 지속시간이 5분 이상[9]인지 확인한다. 출력값에 따른 교란 가능 거리 내 공중에 위치한 표적은 GPS 신호 및 좌표값을 사용할 수 없게 된다. 재밍 공격을 받은 표적 부대가 운용 중인 GPS 장비를 GPS 수동모드로 전환하거나, 관성항법장치(INS) 사용으로 변경하는지 확인한다. 관성항법장치(INS)를 사용하는 장비들은 관성항법장치 사용으로 모드 변경을 하는지 확인한다. 운용 방법을 변경 할 경우 15분간 GPS 수신 제한하고, 운용 방법을 변경하지 않을 경우 공격 시간 동안 GPS 수신이 제한된다.

스푸핑 공격에 필요한 제원을 입력한다. 지상 표적 부대가 교란 가능 거리 내에 위치하는지 확인한다. 공중표적은 공역 사용 수단별 운용고도를 고려하여 공중 표적부대가 유효 거리 내에 위치하는지 확인한다.

표적부대가 GPS 수신기를 사용하는지 또는 항재밍 장비를 보유하고 있는지 확인한다. 항재밍 능력이 있으면 스푸핑 공격을 실패 처리하고 모의를 종료한다.

전파교란장비의 신호 세기가 144dBm이상, 전파교란장비 운용 시간이 1분 이상 인지 확인한다. 스푸핑 공격을 받은 표적에 대해 위치 오차 20m 초과를 적용한다. GPS 전파교란 감시체계 '기만' 경보와 같은 효과를 적용한다. 표적부대는 정상과 다른 신호를 수신하여 GPS 신호가 비정상적으로 수신됨을 인지할 수 있다.

스푸핑 공격을 받은 부대가 운용 중인 주파수를 변경하는지 확인한다. 주파수를 변경할 경우 15분간 GPS 수신 제한한다. 주파수를 변경하지 않을 경우 공격 시간 동안 GPS 수신 제한 한다. Spoofing 공격 후 EMI 보고서를 피해부대에 생성한다.

5. 결론

무선네트워크의 발전과 사용 증가로 사이버공간과 전자기스펙트럼의 교차영역이 확대되면서 사이버전과 전자전을 융합하여 시너지 효과를 창출하려는 사이버 전자전의 개념이 대두되었다. 이는 고출력 전자기스펙트럼과 멀웨어를 융합하여 사이버공간 및 시스템에 장애를 일으킬 수 있는 효과를 가져온다. 사이버 전자전에 관한 대부분의 무기체계에 주로 사용되는 GPS와 GPS 재밍은 특성상 다른 전투 형태에 비해 상대적으로 모의 논리 개발이 적었던 것이 사실이다.

본 연구에서는 육군 합성전장훈련체계의 전투지휘훈련모델에 적용가능한 GPS 재밍 모의를 연구하였다. GPS 재밍을 지대공 재밍, 지대지 재밍, GPS 스푸핑으로 구분하여 GPS 재머의 영향 거리에 따른 전파의 손실을 고려한 GPS 재밍 모의 논리를 제안하고, GPS 전파교란 모의 수행 절차를 바탕으로 하여 아군에 전파 교란을 시행하고, 이를 통해 방해받은 부대가 일정 시간 동안 표적 확인, 위치보고, 감시자산에 대한 시간 오차 등을 적용하여 GPS 신호가 제한되도록 모의하였다.

참 고 문 헌

[1] 강동수, 이민우, 현대전에서의 사이버전 위게임 연구, 국가안보문제연구소, 2020.
[2] 윤지영, 강동수, “합성전장훈련체계의 사이버 작전 모의를 위한 GPS 잡음 Jamming 유효거리 분석, 2023 국방경영분석 학술대회 논문집, pp.326~335, 2023.
[3] 김도현, 강동수, ”북한의 사이버전자전 능력 연구“, 한국소프트웨어종합학술대회 논문집, pp.37-39, 2021.
[4] 강동수, 이상준, 윤지영, “육군 합성전장훈련체계의 GPS Jamming 및 사이버작전 모의논리 연구,” 연구보고서, ㈜심네트, 2023.
[5] Joint Navigation Warfare Center, GPS Frequency Clearances and Reliability Prediction Model
[6] 중앙전파관리소, “무선국 및 전파응용설비의 검사업무 처리기준(고시 제2023-1호)”
[7] E. D. Kaplan, C. J. Hegarty, "Understanding GPS Principles and Applicagions," 2005.
[8] 해수부, 국토부, 과기정통부, “최신 전파항법 국제동향 파악 및 아국 대응전략 수립,” 2017.
[9] 국방부, GPS 전파혼신 재난 위기대응 실무매뉴얼, 2023.

저 자 소 개

윤지영(E-mail: yoonjy131@gmail.com)
2017 창원대학교 신소재공학 공학사
현재 국방대학교 컴퓨터공학 석사과정
관심분야 : 사이버 전자전, GPS 전파교란

강동수(E-mail: greatkoko@kndu.ac.kr)
2011 고려대학교 컴퓨터공학 박사
현재 국방대학교 국방과학과 학과장
관심분야 : SW보안 테스팅, 해사 사이버 보안, 무기체계 SW, 북한 SW, 국방M&S, 머신러닝, 국방획득