

빅데이터 분석을 활용한 GPS 전파교란 대응방안

Big Data Analytics for Countermeasure System Against GPS Jamming

최영동¹ · 한경석^{2*}

¹송실대학교 IT정책경영학과

²송실대학교 경영학부

Young-Dong Choi¹ · Kyeong-Seok Han^{2*}

¹Department of IT Policy Management, Soongsil University, Seoul, 06978, Korea

²Department of IT Policy Management, Soongsil University, Seoul, 06978, Korea

[요 약]

인공지능은 우리 실생활과 밀접하게 연관되어 다양한 분야에서 혁신을 주도하고 있다. 특히 인공지능을 보유한 이동수단으로서, 자율무인이동체의 연구가 활발하게 이루어지고 곧 실용화를 앞두고 있다. 자율자동차와 무인기 등이 스스로 경로를 설정하고 목적지까지 이동하기 위해서는 정확한 위치정보를 제공하는 항법장비가 필수적이다. 현재 운용되고 있는 이동수단들의 항법은 대부분 GPS에 의존하고 있다. 그러나 GPS는 외부 교란에 취약하다. 지난 2010년부터 북한은 수차례 GPS 교란을 감행하여 우리 측에 이동통신, 항공기 운항 등에 심각한 장애를 유발했다. 따라서 자율무인이동체의 안전성을 보장하고 교란으로 인한 피해를 방지하기 위해서는 신속한 상황판단과 대응이 요구된다. 본 논문에서는 빅데이터, 머신러닝 기술을 기반으로 John Boyd의 OODA LOOP Cycle(탐지-방향설정-결심-행동)을 적용한 조치방안 도출과 결심을 지원하는 GPS 전파교란 대응체계를 제시하였다.

[Abstract]

Artificial intelligence is closely linked to our real lives, leading innovation in various fields. Especially, as a means of transportation possessing artificial intelligence, autonomous unmanned vehicles are actively researched and are expected to be put into practical use soon. Autonomous cars and autonomous unmanned aerial vehicles are required to equip accurate navigation system so that they can find out their present position and move to their destination. At present, the navigation of transportation that we operate is mostly dependent on GPS. However, GPS is vulnerable to external interference. In fact, since 2010, North Korea has jammed GPS several times, causing serious disruptions to mobile communications and aircraft operations. Therefore, in order to ensure safety in the operation of the autonomous unmanned vehicles and to prevent serious accidents caused by the interference, rapid situation judgment and countermeasure are required. In this paper, based on big data and machine learning technology, we propose a countermeasure system for GPS interference that supports decision making by applying John Boyd's OODA loop cycle (detection - direction setting - determination - action).

Key word : GPS, Electromagnetic Interference, OODA LOOP, Autonomous System, Machine Learning.

<https://doi.org/10.12673/jant.2019.23.4.296>



This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

Received 10 August 2019; Revised 11 August 2019

Accepted (Publication) 23 August 2019 (30 August 2019)

*Corresponding Author; Kyeong-Seok Han

Tel: +82-2-8954-7137

E-mail: kshan@soongsil.ac.kr

I. 서론

IT 대표 리서치 기관인 가트너(Gartner)는 2019년 전략기술 추세를 발표했다. 그 중 첫번째로 제시된 것은 자율화 사물(autonomous things)이다. 가트너의 부사장 데이비드 설리는 ‘자율화 사물이 확산되면서 독립적인 지능형 사물이 아니라 여러가지 장비들과 함께 작동하는 지능형 사물이 도입될 것’이라 언급하였다. 그 예로 그는 넓은 발의 수확을 위한 자율 무인기와 수확기계의 협업, 그리고 자율주행차량과 무인기를 이용한 소포 배송 아이디어를 제시하였다[1]. 이렇듯 자율 자동차와 자율 무인기는 최근 자율화 기술을 대표하는 연구분야이다. 자율자동차 분야에서는 테슬라, 구글, GM 등의 여러 업체들이 이미 개발 경쟁을 통해 상당한 자율화 기술수준을 달성하고 있다. 보잉, 에어버스 등은 소형 자율 무인기 택시가 도심지역에서의 운송체계에 혁신을 가져올 것으로 판단하고 이에 대한 개발을 시작했다. 최근 보잉에서는 자율무인택시의 첫 비행을 성공하였으며, 2020년대 초반에 상용을 목표로 연구가 진행중이다. 군에서도 ‘드론봇 전투단’이라는 개념으로 드론을 활용한 정찰 임무, 3D 영상정보 생성, 표적 타격임무, 집단운용 등의 기술을 활용하여 민간분야보다 좀 더 진보된 무인기술의 적용을 연구하고 있다. 이렇듯 향후 무인 자율이동체의 활용이 다양화, 보편화 될 것이고, 인구감소 등의 사회적 추세를 감안해볼 때 무인 자율 이동체의 활용은 지금보다 더욱 가속화 될 것이다. 이러한 자율 이동체에는 최적의 이동경로, 상호 충돌방지 등을 위해 GPS (global positioning system)로 부터 수신되는 정확한 위치정보를 활용한다. 자율이동체의 이동에는 항법장비인 GPS가 가장 핵심적인 역할을 한다. GPS 외에도 INS (Inertial Navigation System) 또한 항법장비로서의 역할을 수행할 수 있지만 자체 발생오차로 인해 GPS보다 정확도가 상대적으로 떨어진다. 따라서 현재까지는 정확한 위치정보를 수신하기 위해서 GPS에 전적으로 의존할 수밖에 없는 실정이다.

그런데 GPS는 외부의 교란에 취약성을 지닌다. 먼저, 국제적인 대표 사례로는 미국의 RQ-170 가 이란에 포획된 사건을 들 수 있다. 2011년 12월 4일, 미국의 스텔스 무인기 RQ-170 sentinel 이 이란군에 의해 포획되었다. 이란은 극비의 임무를 수행중이던 이 무인기를 포획 즉시 공개하였다. 미국 정부는 이 사항이 공개되었을 당시에는 무인기의 포획사실을 부인하였으나 나중에는 이를 인정하였다[2]. 이란은 GPS spoofing 교란으로 미국의 무인기를 탈취한 것으로 알려졌다[3]. 국내 사례로는 수년 전 북한의 GPS 교란에 의한 장애 발생을 대표적 예로 들 수 있다. 북한은 2010년부터 지금까지 4회에 걸쳐 GPS 교란행위를 감행했으며, 그로인해 우리측의 민간 이동통신, 선박, 항공기 등에 비정상적인 작동을 유발하였다. 2012년 5월 10일에는 한국 해군의 정찰/통신 중계 목적의 S-100 회전익 무인항공기(오스트리아 Schiebel 사 제작)가 시험비행 중에 추락하여 원격조종사 1명이 사망하고 시험비행 지원요원 2명이 부상을 당하는 사고가 있었다. 이 사고는 북한으로 추정되는 GPS 교란

에 의해 무인기의 GPS가 수신불능으로 추락한 것이었다[4].

위에서 살펴본대로, 무인이동체계의 활용이 가속화 될 수록 GPS 전파교란에 대한 대비가 필요하며, 이에 적절히 대처하지 못 할 경우 심각한 국가재난으로 확대될 수 있다. 물론 각 이동체별 GPS 교란에 대응할 수 있는 능력을 구비한 수신장비를 구비하는 것도 하나의 대비방안이 될 수 있겠지만 이는 실제 고가의 군용장비에 주로 국한되어 있으며 대중화, 보편화된 체계에 장착된 상용 GPS는 교란에 취약할 수밖에 없다.

GPS 교란 상황이 발생했을 시에는 무엇보다 가장 먼저 탐지하고 사용자들에게 신속하게 전파하는 것이 중요하다. GPS 교란은 이동체계 뿐만 아니라 금융, 에너지 등 사회기반체계에 단시간에 심대한 영향을 주어 막대한 피해를 가져올 수 있기 때문이다.

본 논문에서는 GPS 전파혼신이 발생할 수 있는 여러 상황에서 우리에게 가장 위협이 되고 발생가능성이 높은 북한의 의도적 교란에 의한 장애발생 사례만을 가정한다. 그리고 이러한 상황에서 신속하게 파악하고 대응할 수 있도록 빅데이터(big data), 머신러닝(machine learning) 등 제4차산업혁명의 핵심기술을 적용한 GPS 전파교란 대응방안을 제안하고자 한다.

II. GPS에 대한 이해

2-1 GPS 운영현황

GPS는 24개의 위성으로 구성되어 6개의 12시간짜리 궤도를 움직인다. NAVSTAR(NAVigation by satellite timing and ranging)로도 일컬어지는 GPS 위성은 미 국방부의 의해 운영되고 있으며, 전천후 24시간 위치정보를 제공하고 있다. 각각의 GPS 궤도에는 4개의 위성이 20,200 km의 고도에서 이동하고 있다. GPS위성은 4개의 원자시계를 장착하여 매우 정확한 시간을 측정할 수 있다. 위성에서는 L1, L2밴드 (L1=1575.42 MHz, L2=1227.60 MHz)의 두가지 신호가 송출된다. L1 신호는 course/acquisition (C/A)와 precision(P) 코드로 구성되어 있는 반면, L2 신호는 P코드만으로 이루어져 있다. 민간에서는 일반적인 위치정보를 제공하는 것으로 알려진 L1신호의 C/A 코드만이 사용 가능하며, 군 또는 특정 인가된 사용자는 좀 더 정확한 위치정보를 제공하는 L1, L2 신호를 사용할 수 있다.

2-2 GPS 위치측정방식

GPS 수신기는 GPS 위성으로부터 정보를 받으면서 위성으로부터 수신기까지 라디오 신호가 도달하는데 까지 필요한 시간을 계산한다. 수신기는 이렇게 계산된 시간과 라디오 신호의 속도(300,000 km/s)를 곱해서 위성까지의 거리를 산출한다. 그림 1과 같이 최소 3개 이상 위성까지의 거리를 알 수 있다면 삼

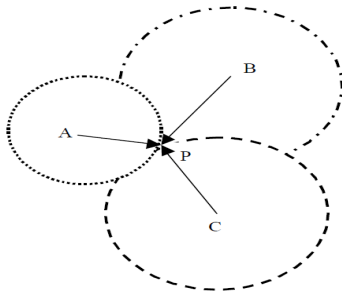


그림 1. 삼각측량법을 이용한 위치 계산[5]
 Fig. 1. Calculation unknown position using triangulation[5]

각측량법을 이용하여 지구상의 수신기 위치를 계산할 수 있다. 그러나 수신기의 시계가 위성의 원자시계만큼 정확하지 않아 시간 측정의 차이로 인해 시간오차가 발생하게 된다. 이러한 오차를 줄이기 위해 수신기는 추가로 네 번째 위성의 정보를 필요로 한다.

2-3 교란 취약성

GPS 위성으로부터 송신되는 신호가 지상 수신기에 도달할 때는 -160 dBW ($1 \times 10^{-16} \text{ W}$)로 수신레벨이 극히 낮아진다. 이렇게 수신신호가 미약한 특성으로 인해 GPS는 외부의 교란 행위에 취약해질 수밖에 없다.

GPS 전파교란 원리는 다음과 같다. 약 20,200 km 상공에서 비행중인 위성에 25 W 백열전구가 설치되고 여기에서 발생시키는 빛을 지상에서 관찰하는 상황을 가정하면, 지구에서 빛을 수신하는 수신자는 위성으로부터 오는 미약한 불빛을 확인할 수 있을 것이다. 그러나 수신자 근처에서 공격자가 관찰을 방해할 목적으로 강한 써치라이트를 비추게 되면, 희미하게 보이던 백열전구의 불빛을 더 이상 인식할 수 없게 된다[6]. 이런 방식으로 GPS 교란장비들은 GPS 신호 수신기에 GPS 신호와 동일한 주파수의 강한 신호를 송출하여 수신부가 정상적인 GPS 신호를 수신하지 못하여 정확한 위치파악을 할 수 없도록 한다.

III. 북한의 GPS 전파혼신 사례

북한에 의한 전파교란은 현재까지 총 4차례에 걸쳐 이루어졌으며 2010년부터 시작되었다. 당시 개성에서 발원된 교란신호는 4일간 지속되었으며 -70 dBm ~ -60 dBm 의 세기로 남측에 영향을 주어 수도권 서북구 지역에 영향을 주었다.

2011, 2012년에는 수도권 지역 및 강원 동북부까지 영향을 미쳐 2010년에 비해 교란에 의한 민간분야의 장애접수가 증가되었다. 그림 2에서처럼 2016년에는 교란 발신지가 이전에 비해 다양해지고 교란범위가 넓어졌으며, 그에 따라 장애접수가 급격히 증가하였다[7].

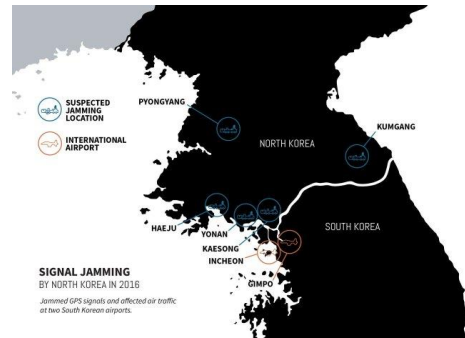


그림 2. 2016년 북한의 GPS 교란행위[7]
 Fig. 2. Jamming conducted by nK in 2016[7]

2016년 국토부 국정감사 자료에 따르면 2010년 부터 2011년과 2012년, 그리고 2016년 등 4차례에 걸쳐 이루어진 북한의 전파교란 기간에 실제 GPS가 교란된 것으로 신고된 항공기는 총 2143대였다. 2010년에는 항공기 14대, 2011년에는 106대, 2012년에는 1016대의 항공기의 GPS가 교란되었다. 2012년 교란상황 때에는 미군기 또한 교란대상에 포함되었으며 민간항공기 4대가 비상착륙하기도 하였다. 2016년으로 갈수록 북한의 전파교란 강도가 심각해졌으며, 하루에 평균적으로 피해를 입은 항공기가 2010년 4.6대, 2011년 10.6대, 2012년 63.5대에서 2016년 167.8대로 대폭 증가하였다[8]. 국토부 자료에 따르면 북한의 교란신호 발신지역이 2010~2012년에 1~2곳에서 2016년 5곳으로 증가하였다. 또한 과거에는 북한이 특정 지역에서 국지적 교란행위를 시도했으나, 2016년 이후에는 강한 신호를 여러 곳에서 지속적으로 발생시켰던 것으로 추정하였다.

이상의 내용을 종합해 볼 때, 제4차산업혁명 시대를 대표하는 자율 무인기와 자율자동차 또한 북한의 GPS 교란 대상에서 제외가 될 수는 없으며, 지대한 영향을 받을 것으로 예상된다. 따라서 그에 따른 대응책이 시급히 마련되어야 한다.

IV. GPS 전파혼신 탐지 및 전파체계

표 1. 북한의 GPS 교란 현황[9]

Table 1. North Korea GPS jamming summary[9]

Dates	Jammer Locations	Affected Areas	Disruptions
2010, Aug 23-26 (4 days)	Kaesong	Gimpo, Paju, etc.	Testing Equipment for...? 15 airplanes 1 Battleship
2011, Mar 4 - 14 (11 days)	Kaesong Mtn, Kungang	Gimpo, Paju, Gangwon etc	145 cell towers 106 airplanes 10 ships
2012, Apr 28 - May 13 (16 days)	Kaesong	Gimpo, Paju, etc.	1,016 airplanes 254 ships
2016, Mar 31 - ongoing	Mt. Geumgang Haeju	Easter Gagnwon Seoul	962 airplanes 700 ships 1,786 cell towers

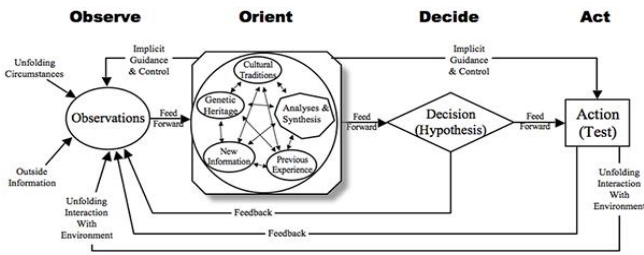


그림 3. OODA LOOP Cycle[10]
Fig. 3. OODA LOOP Cycle[10]

4-1 의사결정모델 OODA LOOP

앞에서 언급했듯이, 자율무인기와 자율자동차 등의 자율 이동체계는 GPS 신호를 활용하며 계획된 경로를 비교적 빠른 속도로 이동한다. 따라서 GPS 교란 발생 시에는 무엇보다 중요한 것이 무인 자율체계의 항법체계 혼란에서 오는 피해 최소화를 위한 신속한 상황파악과 의사결정이다. 이러한 일련의 조치를 통합적으로 수행하기 위해서는 GPS 교란 탐지 및 전파체계의 구축이 필요하며, 교란상황 발생 시 신속 의사결정 도구로서 OODA LOOP를 적용해 볼 수 있다. 발생한 교란 수준에 따라 OODA LOOP 모델에서 제시한 의사결정단계를 적용한다면 단 시간에 효과적인 대응방안을 모색할 수 있다.

OODA LOOP는 군사 전략가였던 미 공군대령 John Boyd가 고안한 의사결정 모델이다. 이론에 따르면, 관찰(observe)-방향 설정(orient)-결심(decide)-행동(act)의 각 단계를 중첩하면서 이루어지는 순환을 빠르게 유지해야 급변하는 상황 속에서 최적의 방안을 신속하게 도출할 수 있다. GPS 교란 상황에서 OODA LOOP에서 제시한 개념을 GPS 교란 탐지 및 대응체계에 적용하면 신속하고 적절한 대응을 위한 결심지원체계로서의 역할을 수행할 것이다. 더욱이, 빅데이터 또는 머신러닝과 같은 첨단기술이 접목되면 OODA LOOP 모델 활용의 궁극적 이점인 민첩성(agility)이 더욱 극대화 될 것이다.

4-2 GPS 교란신호 탐지

OODA LOOP Cycle에서의 첫 단계는 ‘관찰’이다. 이 단계는 주변 환경과의 상호작용 및 감지 등을 통해 정보를 습득하는 과정이다. 정부에서는 GPS 교란발생을 탐지할 수 있도록 전파감시 안테나를 서해와 동해안 접경지역에 구축하여 24시간 모니터링을 하고 있다[11]. 전파감시 안테나를 통해 수집되었던 그

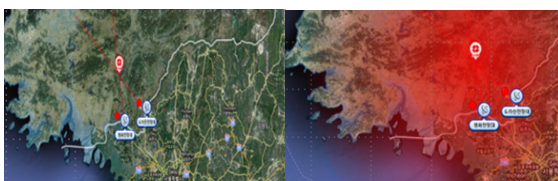


그림 4. 교란원점 위치파악[13]
Fig. 4. Locating jamming source[13]

동안의 실제 교란 신호들과 식별되었던 발신원의 정보들을 빅데이터 처리를 거쳐 머신러닝이 적용된 시스템을 구현하면 교란 발생 시 대응시간을 단축할 수 있다.

기존에는 교란원점을 식별하기 위해서 그림 4와 같이 2대 이상의 탐지안테나에서 탐지된 신호의 세기, 방향 등을 바탕으로 분석이 이루어졌다. 빅데이터를 활용한 기존 사례들과의 비교 분석, 탐지전파의 특성분석이 머신러닝으로 구현된다면 교란원점의 위치를 찾아내는데 소요되는 시간이 기존보다 단축되고 보다 정확한 식별이 이루어 질 수 있다. 이를 위해, 그동안 접경지역에 구축된 다수의 감시안테나에 탐지되었던 각각의 교란신호 세기, 방향, 방사 특성(지향성) 등과 북한의 주요 교란 지점과의 연계성을 빅데이터 분석을 거쳐 정형화하고 이러한 패턴을 적용한 머신러닝을 구현하면 실제 교란발생 시 초기 탐지범위를 최소화할 수 있고, 이에 따라 이전 방식보다 더욱 정확하고 신속한 교란원점 탐지가 가능하게 된다. 지난 2010년 8월에 있었던 북한의 GPS 교란상황에서 한국군은 교란장비의 위치를 명확하게 파악하지 못했는데, 이는 교란상황이 10분 이내 단속적으로 이루어졌기 때문이었던 것으로 알려졌다[12]. 머신러닝을 적용한 탐지체계를 활용하면 지난 2016년 사례와 같은 북한의 동시 다발적인 교란상황에서도 신속하게 교란신호의 원점을 파악할 수 있다.

4-3 GPS 교란 영향 파악

‘방향설정’ 단계는 OODA Cycle에서 가장 핵심적인 단계로 관찰, 결심, 행동의 방향과 근거를 제시해준다. 방향설정단계에서는 습득된 정보를 바탕으로 현재 처한 상황에 대한 다방면의 분석이 이루어진다. GPS 교란신호가 탐지되면 이러한 신호분석을 통해 다음 대응방향을 설정해야 한다. 먼저, 탐지된 신호를 면밀히 분석하여 교란의 의도가 무엇인지를 파악한다. GPS 교란방식은 크게 두 가지로 나눌 수 있는데 스푸핑(spoofing)과 재밍(jamming)이다. 교란 행위자는 기만신호를 발생시켜 GPS 사용자들이 잘못된 정보를 수신하도록 하는 스푸핑을 통해 정상적인 경로가 아닌, 교란행위자가 의도하는 지역으로 사용자를 유도할 수 있다. 또는, 재밍을 통해서 사용자의 ‘눈’을 멀게 하여 혼란을 유도하고 그로인한 피해를 강요할 수도 있다. 이러한 교란의도가 파악되어야 그에 따른 적절한 조치방안을 통해 GPS 장비들의 피해를 최소화 할 수 있다. 이러한 체계를 구축하기 위해서는 모의 전파혼신 신호생성 장치와 같은 훈련장비를 통해 여러 시나리오를 적용한 모의 교란훈련을 반복하고 체계에 학습시켜 향후 교란 발생 시 탐지 신호에 대한 특성을 분석하고 의도를 파악하는 능력을 증대시킬 수 있다[13].

다음으로는, 교란에 따른 영향범위 분석이 이루어져야한다. 교란신호 탐지 시, 그에 따른 영향성을 파악하지 못한다면 불가피하게 모든 GPS 장비 사용자들은 장비 운용을 중지해야한다. 이런 비효율적인 상황을 피하기 위해서는 교란 신호의 영향이 어느정도의 범위까지 미치는지 확인하고 GPS 사용자들이 영향범위를 벗어날 수 있도록 조언해야 한다.

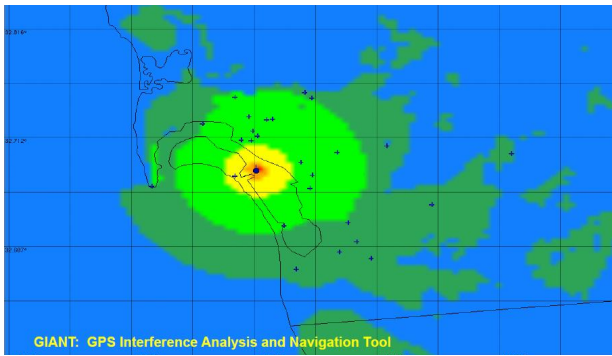


그림 5. GIANT를 통한 교란범위 시현[14]
 Fig. 5. Displaying the area affected by GPS jamming on GIANT[14]

GPS 교란에 대한 영향성을 예측하는 시뮬레이션 프로그램인 GIANT(GPS interference analysis navigation tool)는 미 공군, 육군 등 정부기관에서 사용중인 프로그램으로, GPS 운용에 필요한 여러 가지 산물을 생산할 수 있다. 특히 GPS 교란상황에서 GIANT를 통해 교란환경이 어떻게 형성되었는지를 지도에 시현할 수 있다. 교란신호를 방출하고 있는 교란 장비의 위치를 입력하면, 현재 운용중인 장비들에 미치는 영향을 시현해준다. 사용자들이 어느 지역에서 GPS를 정상적으로 사용할 수 있는지를 알려주는 것이다. 이를 참조하여 사용자는 교란신호를 회피할 수 있는 운행경로를 계획할 수 있다.

GPS 교란 탐지/대응체계에는 GIANT와 같은 분석능력이 반드시 구비되어야 하며 시뮬레이션이 아닌, 실시간 영향성 파악이 이루어져야 한다. 그러기 위해서는 실제 교란상황 발생 시마다 지상에 있는 교란신호 탐지소를 비롯하여 공중, 해상상의 GPS 운용장비에서 수집된 교란신호 탐지정보를 수집하여 DB를 구축할 필요가 있다. GIANT보다 신뢰성있는 영향성 분석결과를 제공받기 위해서는 지형, 교란신호 세기 등을 고려한 기존의 이론적인 분석과 더불어, 다양한 탐지원으로 부터 실제 수집된 다량의 데이터 축적을 바탕으로 한 빅데이터 분석이 이루어져야 한다.

4-4 GPS 교란 대응방안 결심 및 전파

결심 단계에서는 방향설정 단계에서 도출된 여러 가정사항들 중 적절한 대응방안에 대한 결심이 이루어진다.

GPS 교란상황이 발생하면 과기부에서는 자체 GPS 혼신 위기평가회의를 개최한다. 과기부는 평가회의를 통해 GPS 혼신 상황을 파악하고 위협수준에 따라 위기경보를 발령하게 되는데, 관심-주의-경계-심각 4단계로 이루어진다.

‘관심’ 단계의 조건이 충족되면 GPS 혼신 비상대응팀이 운영된다. GPS 실제 교란이 30분 이내 또는 불연속적으로 발생하거나 항공기, 선박 1~2대 에서 GPS 미수신이 발생하면 ‘관심’ 단계가 발령된다. 이동통신기국, 항공기, 선박 등 3대 이상에서 GPS 미수신 시 또는 8시간 이내로 40~70 dB의 교란세기가

지속될 때에는 ‘주의’ 단계가 발령된다.

‘경계’ 단계는 교란피해가 국가핵심 기반분야로 확대되며 교란 세기가 8시간, 70 dB 이상 지속될 때 발령된다. ‘심각’ 단계는 교란으로 인해 국가 핵심 기반분야의 서비스가 중단되거나 피해 규모가 전국으로 확대되고 교란 세기가 8시간, 70 dB 이상 지속될 때 발령된다. 심각 단계에서는 국가차원의 각 부처별 공동대처방안을 모색하게 된다[15].

앞에서 이미 언급했듯이 GPS 교란에 대한 대응은 신속성이 가장 필요로 한다. 지난 2010년부터 북한의 GPS 교란사례를 거치면서 각 기관에서는 GPS 교란 발생 시 대처방안을 준비하고 있으며 위기경보 단계별로 매뉴얼화 되어있다. 위기경보 단계는 GPS 혼신 위기평가회의에서 현재의 위기상황이 각 등급별 조건을 충족하는 지에 대한 여부를 판단하고 경보 발령 또는 격상 여부를 결정한다. GPS 전파교란 대응체계가 빅데이터 및 머신러닝을 통해 교란 신호에 대한 ‘관찰’, ‘방향결정’ 에서 분석된 결과로 위기경보 단계별 조건 충족여부에 대한 판단을 비롯한 위기경보 발령을 위한 종합적인 평가를 도출할 수 있는 ‘결심’ 지원기능을 수행한다면, 대응체계 운영을 통해 GPS 교란상황을 통합적으로 관리할 수 있다. 또한 위기상황에 대한 신속한 조치가 가능하여 결심지연으로 인한 피해확대를 방지할 수 있다. 이를 위해서는 신뢰성 있는 평가를 도출할 수 있도록 조치 단계별 경보발령 조건의 구체화, 세분화가 필요하다.

V. 결 론

북한은 하노이 회담 결렬 이후 국면 전환 및 미국과의 협상에 유리한 위치를 점하기 위해 단거리 미사일 발사 등 저장도 도발을 지속할 것으로 보인다[16]. 중·저장도 도발에는 GPS 교란과 같은, 간접적이지만 영향력이 막대한 도발 또한 발생 가능성이 높다고 할 수 있다. 일부 전문가들은 그동안 북한의 GPS 교란이 수차례 이루어졌지만 이를 방지하거나 중단시킬 수 있는 확실한 방안이 있었던 것은 아니었던 것으로 평가하고 있다 [12]. 국제기구를 통한 항의는 북한의 GPS 교란을 중단시키고 방지하기 위한 실질적인 대책은 아니라는 것을 반증한다. GPS 교란 상황 발생 시에 무엇보다 중요한 것은 신속하게 상황을 파악하고 평가하는 것이다. 그리고 GPS장비 사용자들의 피해를 최소화하기 위해 빠르게 위기경보를 전파해야한다.

제4차산업혁명시대의 핵심인 빅데이터, 머신러닝 기술은 외부의 GPS교란에 대해 신속히 대응하기 위한 실질적인 해결방안을 제시한다. 빅데이터를 활용한 교란원점 식별과 영향성 파악이 이루어지면 머신러닝을 적용한 결심체계로 상황에 적합한 경보발령이 이루어진다. 이를 통해 GPS 교란에 의한 피해를 최소화하고 그에 따른 추가적인 조치를 이행하게 되며 이러한 제반 절차가 기존보다 빠르게 이루어질 수 있다. 향후, GPS에 대한 의존도가 높은 자율이동체계가 지금보다 더욱 보편화 되어 운용될 시기에는 교란상황에 대한 대응이 근 실시간에 이루어

어려야 하며 이는 국가적인 재난으로의 확대를 예방하기 위해 결코 지나치지 않다.

References

[1] D. P. Kim (2018, October), Top 10 Strategic Technology Trends for 2019 according to Gartner. iTNews [Internet]. Available : <http://www.itnews.or.kr/?p=29420>

[2] T. K. Park, Y. J. Kim, S. Y. Kim, S. Y. Lee, and J. H. Lee, “Unmanned aircraft cyber security incident case and security vulnerability,” *IT Technology Support Center*, Vol. 1716, pp. 1-11, Oct. 2015.

[3] D. H. Shin, Easy to hack Drone, Can it be hijacked by GPS jamming? [Internet]. Available : <https://news.joins.com/article/23177968>

[4] K. Y. Lee and K. S. Ryu, “Research for improving vulnerability of unmanned aircraft,” *Smart Media Journal*, Vol. 7, No. 3, p.65, Sep. 2018.

[5] S. K. Upadhyaya, G. S. Pettygrove, J. W. Oliveira, and B. R. Jahn An introduction – global positioning system [Internet]. Available : https://www.researchgate.net/publication/237370722_AN_INTRODUCTION_-_GLOBAL_POSITIONING_SYSTEM/download

[6] S. H. Hwang, “Recent GPS jamming characteristics and countermeasure technics,” *IITP Trends report*, Vol. 1853, No. 3, p.18, Jul. 2018

[7] Center for Strategic and International Studies. Signal jamming by North Korea in 2016 [Internet]. Available: <https://aerospace.csis.org/space-threat-2018-north-korea/>.

[8] “North Korean GPS disturbance attacked the US military aircraft and caused four commercial airline emergency landings,”[Internet]. Available : <https://blog.naver.com>

/jbrave119/221213395913

[9] RNT foundation. Summary of GPS jamming by North Korea. [Internet]Available : <https://rntfnd.org/wp-content/uploads/North-Korea-Jamming-summary.jpg>

[10] Dr. Donald A. MACCUISHE, “Orientation : the key to the ooda loop,” *Journal of Defense Resources Management*, Vol 2, Issue 2, pp. 29-36 Oct. 2011

[11] C. K. Yang. South Korea Government, North Korea GPS jamming countermeasure system [Internet]. Available : <http://www.etoday.co.kr/news/section/newsview.php?idxno=1311956>

[12] H. Todd, J. Kaitlyn, T.G. Roberts, Space threat assessment [Internet]. Available : <https://www.csis.org/analysis/space-threat-assessment-2019>

[13] S. W. Lee, “GPS jamming monitoring and response trend,” [Internet]. Available : http://www.kiees.or.kr/download.php?mode=board&board_idx=1828&file_idx=1759

[14] J. Merrill – Program Manager Patriot Watch vigilance safeguarding america DHS Position, Navigation & Timing (PNT) Program Management Office WSTS March 2012 [Internet]. Available : <https://www.gps.gov/multimedia/presentation/s/2012/03/WSTS/merrill.pdf>

[15] MSIT Official Blog. Confirmation of GPS interfering signals in some areas in the northwestern part of the metropolitan area [Internet]. Available : http://blog.naver.com/PostView.nhn?blogId=with_msip&logNo=220671198871&parentCategoryNo=&categoryNo=47&viewDate=&isShowPopularPosts=false&from=postView

[16] J. Y. Kim, North Korea requests withdrawal of nuclear abandonment First , Provocation could be followed. [Internet]. Available : <http://www.fnnews.com/news/201905191437127854>



최영동 (Young-Dong Choi)

2003년 : 공군사관학교 (이학사)
 2011년 : 美 공군대학원 (공학석사)
 2017년~현재 : 송실대학교 IT정책경영학과 경영학박사과정
 ※ 관심분야 : 인공지능(AI), 빅데이터(Big Data), 자율무인체계(Autonomous Vehicles) 등



한경석 (Kyeong-Seok Han)

1979년 : 서울대학교 문학사
 1983년 : 서울대학교 경영학과 (경영학 석사)
 1989년 : 미국 퍼듀대학교 대학원(경영정보시스템전공 박사) 1989년~1990년 : 미국 휴스턴대학교 조교수
 1993년~현재 : 송실대학교 경영학부 경영정보시스템 교수
 ※ 관심분야 : E-Business, ERP(Enterprise Resource Planning), PLM(Product Lifecycle Management), AIS, 중소기업 정보화, 디지털저작권 등