

GPS 재밍을 고려한 해상교통관제 시스템 설계

† 이병길 · 김병두 · 나중찬 · 조현숙
 † 한국전자통신연구원

요 약 : 최근 국내에서는 북한의 사이버 테러로 추정되는 전산망 해킹(APT공격)사건과 더불어 하나의 전자전으로서 GPS 재밍 사건들이 인천 등 서해에서 다수 발생되어 왔다. 즉, 이러한 GPS 재밍은 러시아 등에서 유출되는 간단한 장비에서부터 치명적인 대규모 전과공격까지 다양한 형태가 발생할 수 있다. 특히 GPS 정보를 사용하는 선박의 AIS 정보는 다수의 선박으로부터 전송되는 정보로서 재밍 대응 가능한 고가의 장비를 선박측에서 탑재하기 어려우며, 송신지가 인근 북한의 경우 국내에서 근원지를 탐지하더라도 대응이 어려운 실정이다. 따라서 본 논문에서는 GPS 교란의 지능화된 여러 공격 형태를 파악하고, 해상교통관제 시스템에서 자체적으로 실시간 대응할 수 있는 방안을 검토하여 시스템 설계에 반영 하고, 관제사의 실시간 인지를 통한 혼란을 방지하며, 선박에 해당 교란 정보를 제공함으로써 능동적인 관제 방안을 제시한다. 실제적으로 재밍에 대응하는 시스템 설계가 관제에 효율적인 방안인지 확인되어야 하며, 국가적으로도 VTS 서비스의 안전성을 보장하는 기술개발로 진화가 고려되어야 한다.

핵심용어 : VTS, GPS 재밍, 보안

Contents ETRI

- 1 배경 및 목적
- 2 GPS 재밍 등 전자전 현황 분석
- 3 VTS에서 재밍 대응 구조설계 및 시나리오
- 4 탐지 시스템 연동을 통한 검증(융합 관제)
- 5 맺음말

IT R&D Global Leader

배경 및 목적 ETRI

1) 배경

- 최근 북한의 사이버테러, GPS교란 등은 전자전 성격의 형태
- 실시간 선박 AIS 송신정보는 해상교통관제 시스템에서 국가적으로 보안에 민감한 정보로서 국내 환경에서는 특히 GPS 교란을 통한 테러 등 역기능에 대한 우려가 있어 안전한 정보처리 및 신속한 대응은 필수적임
- 따라서 국가적 보안 정책에 의해 GPS 교란 탐지 가능한 해상교통관제(VTS) 시스템에서 재밍 대응 보안 프로토콜 설계와 이를 통한 안전한 데이터 융합처리는 반드시 필요한 상황임
- 실시간 재밍 탐지고려한 관제 외에도 좀더 세부적인 재밍 영역 선박 목표 정보관리 및 타 선박에 주의를 전달하기 위한 추가적 속성 정보의 등 보완될 요소가 존재함

2) 목적

- 국가적 차원에서 좀더 안전한 VTS 정보를 자체적으로 관리하고, GPS교란 유사시 실시간 대응하는 관제로서 해상의 안전을 높이고자 함

IT R&D Global Leader

GPS 재밍 등 전자전 현황 분석 ETRI

최근의 사이버테러 위협

"3.20 사이버 테러는 북한 소행... 해킹 수법 일치"

북 소행 증거(1)

북 내부에서 국내 공력경유지에 침투, 장기간 공격 운위

<3.20 사이버 테러-발표> <관련 자료>

IT R&D Global Leader

GPS 재밍 등 전자전 현황 분석 ETRI

GPS 개요

- GPS는 최소 3개의 GPS위성(고도 2만Km, 24개위성)으로부터 전파를 수신하여 삼각 측량법에 의해 위치를 결정
- GPS 오차율은 군사용 3m, 민간용 15m → DGPS 사용시 오차 5m이내(1m이내) 축소
- GPS 송출전력은 개방장소에서 약 -160dBW로 낮아 전파간섭 영향이 큼
- GPS와 유사 항법 시스템은 러시아의 GLONASS, 중국의 COMPASS, 유럽의 Galileo 등 존재

시스템 명칭	GPS	GLONASS	COMPASS	Galileo
운용 국가	미국	러시아	중국	유럽
주파수(GHz)	1.5754 (L1신호) 1.2276 (L2신호)	~1.602 (SP) ~1.246 (SP)	1.561098 (B1) 1.589742 (B1-2) 1.20714 (B2) 1.269852 (B3)	1.164 - 1.215 (E5a & E5b) 1.260 - 1.300 (E6) 1.559 - 1.592 (E2-L1-E11)
위성 고도(km)	20,180	19,130	21,150	23,220
위성 갯수	최소 24개	31개	5개(잠지), 30개(IMEO)	2개(시험 중) 최종 22개
운용 현황	운용 중	운용 중	10개만 운용 중	준비 중

<글로벌 항법 시스템 종류>

IT R&D Global Leader

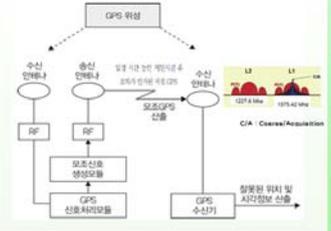
GPS 교란관련 기술동향

- 1) 2003년 이라크 전쟁시 미국에서 사용
- 2) GPS 재머의 기술이 인터넷에 공개되며, 러시아 등 에서 다양한 GPS 재머의 형태로서 발전함
- 3) 미국은 GPS 교란 대응 기술과 더불어 GPS 신호 위기관리 체계 수립 및 운용 (국토안보부, 연방항공국, IDM(Interference Detection and Mitigation))
미국은 1400개 CORS(교란신호 상시감시) 지구국 운영
- 4) 미국 NavCOM Tech.사 및 HAVSYS사는 항공관제 및 항공기 장비의 위성항법 수신교란 신호 대응 기법연구를 통한 대응(해당기술 보유)
- 5) 영국은 정부의 GAARDIAN 프로젝트 수행, 독일 GIMOS 시스템을 운용하며, 호주는 CORSnet통해 감시운용

지능화된 GPS 교란 동향

최근에는 아래와 같은 다양한 방법의 스마트 재밍 기법으로 발전, 지속적 개발

- 1) 단순히 GPS 신호보다 높은 신호 송출형태의 주파수 재밍을 통한 교란(기존방법)
- 2) 잘못된 위치 및 시각 정보를 산출하게 하는 기만(Spoofing) 재밍에 의한 형태로 발전
- 3) 오차 모조신호를 만들어 높은 신호로 송출하는 스마트 재밍으로 발전
- 4) 일정시간 지연시킨 후 수신기에 재송신하는 방법



최근 국내에서의 GPS 재밍 피해 사례

구분	발생시기	피해지역	피해사례
1차 전파교란	2010년 8월 23~26일 (4일간)	인천공항 등 경기 서북부	기지국, 선박, 항공기 GPS 수신 장애, VTS 포함
2차 전파교란	2011년 3월 4~14일 (11일간)	인천공항 등 경기 서북부	기지국, 선박, 항공기 GPS 수신 장애, VTS 포함
3차 전파교란	2012년 4월 28일~ 5월 13일(16일간)	인천공항 등 경기 서북부	기지국, 선박, 항공기 GPS 수신 장애, VTS 포함



목적 : 선박 또는 항공기의 충돌을 통한 혼란 GPS 사용 군사 장비의 무력화

GPS 재밍 대응 기술(현실적 대안 절실)

- 1) 재밍 발생 근원지 실시간 탐지/대응 기술
-> 복원이 근원지인 경우
-> 선박 고비용
- 2) 재밍 대응 안테나/송수신 모듈 개발
-> 선박 고비용
- 3) GPS 재머 방향의 전파 신호 차단 장치 부가
-> 선박 고비용
- 4) 실시간 탐지 가능한 감시 시스템 상시 운용 및 전파
-> VTS의 관제 시스템과 연계요
- 5) 재밍 위협에 강한 위성통신/대체항법 개발
의사위성, E-LORAN, 신항법기술
-> Prototype 개발, 기술적 성숙요
- 6) GPS 신호 인증 -> 자체 위성요



<재밍 감시시스템 예>
→ 재밍 탐지는 여러 방법으로 구현
1) 신호전력 크기/변화를 감시
2) 코드와 반송파 변화를 비교 등

VTS에서의 재밍 대응

→ 국내에서도 전파 교란에 대한 감시 장비를 두고 신호감시체계를 운용중에 있지만, 실제 관제 환경에서 교란신호에 대한 정보를 받기는 시간적인 지연이 존재하므로 실시간 대응이 어렵고, 교란이 있다는 단순 정보로만 알려주므로 관제에 혼선이 발생가능



→ 해당 피해 영역 정보까지 필요

따라서 근본적으로 VTS에서 실시간 탐지 가능한 구조로 설계하고 재밍 영역 판단하여 융합처리 시스템이 해당 정보를 필터링하는 것이 필요함

