논문 16-41-12-15 The Journal of Korean Institute of Communications and Information Sciences '16-12 Vol.41 No.12
https://doi.org/10.7840/kics.2016.41.12.1759

수신기 수평적 위치의 표본 분산에 따른 GPS 재방송 재밍 신호 검출 기법

최 영 은◆, 김 선 용°

A GPS Repeat-Back Jamming Signal Detection Scheme Based on the Sample Variance of Horizontal Location of a Receiver

Young Eun Choe◆, Sun Yong Kim°

요 약

본 논문에서는 항법을 위해 가장 많이 사용하는 GPS 민간용 신호의 재방송 재밍에 의한 영향 분석을 바탕으로 수평 위치해의 표본분산에 따른 GPS 재방송 재밍신호 검출 기법을 제안하고, 그 성능을 분석한다.

Key Words : Global Positioning System, Repeat-back Jamming, Meaconing, Horizontal Location Solution, Sample Variance

ABSTRACT

In this letter, we propose a GPS repeat-back jamming signal detection scheme based on the sample variance of the horizontal location of a receiver and evaluate the detection performance using real positioning data of the GPS receiver.

Ⅰ. 서 론

GPS (global positioning system)는 TDoA (time difference of arrival)를 이용해 사용자의 항법해인 위치, 속도, 시간을 얻을 수 있는 전파항법체계 가운데 하나이다. GPS는 발전소와 가정의 효과적인 전력관리를 위한 차세대 전력망, 자동인출기, 주식시장, 인터넷 뱅킹 등 스마트 금융, 무선 인터넷, 지리정보접속, 응급구조체계, 선박 및 기차 의 항행을 위한 필수 체계로 사용되고 있으며, 날로 그 필요성이 증대되고 있다[1].

GPS 신호는 지상으로부터 약 2만 킬로미터 상공에 위치한 위성들에서 송신되며, 지상에 도달한 신호는 상온에서의 열잡은 수준 이하로 매우 미약하다. 현재 주로 사용되는 GPS 민간용 신호인 L1 대역의 C/A(coarse/acquisition) 신호는 이를 극복하기 위해 DS/SS(direct sequence/spread spectrum) 체계를 통신 물리계층으로 사용한다. 그럼에도 불구하고 GPS L1 C/A 신호 사양이 모두 공개되어 있어 이에 대한 의도적 전파방해인 재밍(jamming) 위협은 날로 증가하고 있다. 재밍은 태양풍이나 전리층 산란, 인접대역 통신 시스템의 간섭과는 다른 의도가 분명한 인위적 전파방해이며, 재밍 신호의 형태에 따라 단순 재밍, 재방송 재밍, 기만 재밍으로 구분한다. 단순 재밍은 협대역 연속파(continuous wave, 보통 CW로 부름)나 광대역 백색잡음을 사용한 재밍으로서 GPS 수신기의 정상적인 수신을 방해한다. 재방송 재밍은 GPS 수신기 근처에 위치한 재방송 재밍기가 정상적인 GPS 신호를 수신한 후 GPS 수신기로 재방송해 수신기의 위치를 재방송 재밍기의 위치 또는 그 사이로 위치로 GPS 수신기의 위치를 혼동시킨다. 기만 재밍은 GPS 수신기가 공격자가 의도한 위치를 정상적인 위치해로 착각하도록 기만한다. 이 가운데 단순 재밍은 재밍기의 구현난이도가 낮고, 가격이 저렴한 반면, 피해 수준이 낮고, 쉽게 검출할 수 있다. 반면 기만 재밍은 재밍기의 구현 난이도가 상당히 높은 반면 기만이 성공한 경우 GPS 수신기를 탑재한 항체를 포획하거나 다른 의도로 활용할 수 있어 전술적 피해를 극대화할 수 있다. 재방송 재밍은 구현 난이도가 평이하고, 가격이 크게 비싸지 않으면서도 GPS 수신기를 탑재한 항체에 일정수준 이상의 피해를 야기할 수 있다[1-3]. 본 논문에서는 단순 재밍, 재방송 재밍, 기만 재밍 가운데 향후 발생 가능성이 비교적 높은 재방송 재밍에 초점을 맞춘다.

※ 본 논문은 2015년도 정부(교육부)의 재원으로 한국연구재단의 기본연구지원사업의 지원을 받아 수행되었음(2015R1D1A1A01059492).
◆ First Author : Konkuk University Department of Electronics Engineering,choe4375@konkuk.ac.kr, 학생회원
° Corresponding Author : Konkuk University Department of Electronics Engineering, kimsy@konkuk.ac.kr, 종신회원
논문번호 : KICS2016-11-340, Received November 7, 2016; Revised December 6, 2016; Accepted December 6, 2016

Ⅱ. 실험 모형

[4]처럼 일부 제한된 환경에서 GPS L1 신호의 재방송 재밍에 의한 전파방해 영향이 분석된 바 있다. 본 논문에서도 그림 1처럼 [4]와 동일한 사양으로 재방송 재밍기를 구성하였다.

GPS 수신기는 독일 IFEN사의 GPS SDR(software defined radio) SX-NSR을 사용하였으며, 안정적 분석을 위한 GPS 신호 저장 및 재생을 위해 영국 RaceLogic사의 LabSat3를 사용하였다.

GPS 수신기는 위도 북위 37.544015도, 경도 동경 37.544015도에 안테나의 중심이 천정을 향하도록 지상에서 약 1m 위에 고정시켰으며, 이를 기준으로 같은 높이에 재방송 재밍기를 50m 동남동쪽 방향으로 이격시켜 배치했다. 실험시작 시점은 1,897 GPS 주이고, 주차 내 시각은 304,400초였다. 일반적인 재방송 재밍 공격은 정상적인 GPS 수신기 가동 중 야기되는 것을 고려해 5분간 정상 수신 후 5분간 재방송 재밍 공격을 진행하고, 다시 5분간 정상 수신을 진행하였다. 측위결과는 1초마다 1개의 위치를 특정하도록 설정하였다. 실험시각에 해당 위치에서의 가시 위성은 모두 8개였다. 실험에 따른 측위결과는 그림 2와 같다.

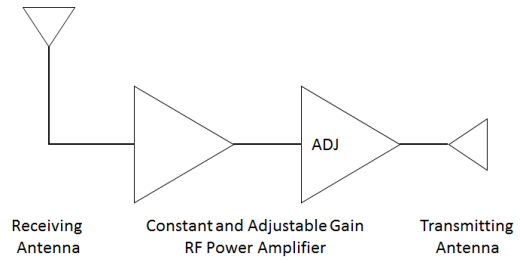

그림 1. 재방송 재밍기 구성도 [4]
Fig. 1. Configuration of meacon

그림 2처럼 정상적인 GPS 수신이 가능한 경우 지름 10m 이내의 원 안에 측위결과나 나타나는 것을 확인할 수 있으며, 재방송 재밍 공격이 진행되는 경우 GPS 수신기로부터 동남동쪽 방향에 위치한 재방송 재밍기의 위치를 기준으로 동남동 방향으로 길게 측위오차가 나타나는 것을 확인할 수 있다.

Ⅲ. 제안한 기법 및 결론

앞서 살펴본 것처럼 재방송 재밍에 의해 GPS 수신기를 기준으로 재방송 재밍기의 위치 방향으로 측위오차가 발생하는 것을 확인할 수 있다. 만약 실험처럼 GPS 수신기와 재방송 재밍기 모두 고정되어 있다면 수신기의 위치해의 표본분산을 통해 재방송 재밍에 의한 이상 여부를 판단할 수 있다. GPS 수신기가 이동하는 경우 [1]에서 언급한 것처럼 수신기의 운동성을 파악할 수 있는 관성항법센서로부터 부가적인 정보를 얻고, 이를 측위오차의 표본분산을 얻을 때 고려한다면 고정 상태와 유사한 결과를 얻을 수 있다.

i 표본시간에서 위치 해의 오차는 다음과 같다.

$$\varepsilon_i = \sqrt{(x_i - x_{i-1})^2 + (y_i - y_{i-1})^2} \quad (1)$$

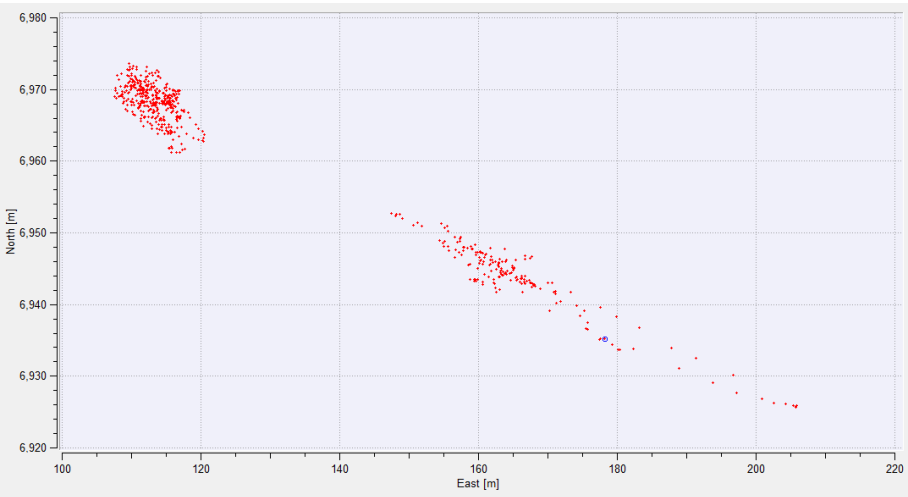

그림 2. GPS 수신기의 측위결과 [4]
Fig. 2. Positioning result of the GPS receiver [4]

이로부터 다음과 같은 표본분산을 얻을 수 있다.

$$\sigma_{\varepsilon}^{2} = \frac{1}{N-1}\sum_{i=1}^{N}(\varepsilon_i - \mu)^2 \quad (2)$$

여기서 N은 연산을 위해 사용하는 표본 수, μ는 다음과 같은 수평 위치에 대한 측위오차의 표본평균이다.

$$\mu = \frac{1}{N}\sum_{i=1}^{N}\varepsilon_i \quad (3)$$

이로부터 다음과 같은 재방송 재밍 검출 기법을 제안한다.

$$\sigma_{\varepsilon}^{2} > \gamma \quad (4)$$

여기서 γ는 문턱값이다.

제안한 기법의 성능을 확인하기 위해 그림 2의 측위 데이터를 활용했으며, $N=10$으로 설정했다. $\gamma=25$로 설정한 경우, 실험 결과 재방송 재밍 신호가 송신된 동안 약 93%는 재방송 재밍 공격으로 판정하였다. 그러나 동일한 설정에서 재방송 재밍 신호가 송신되지 않았음에도 약 18%를 재방송 재밍 공격으로 오판정하였다. $\gamma=15$로 설정한 경우, 실험 결과 재방송 재밍 신호가 송신된 동안 약 99%를 재방송 재밍 공격으로 판정하였으나 동일한 설정에서 재방송 재밍 신호가 송신되지 않았음에도 약 41%를 재방송 재밍 공격으로 오판정하였다.

본 논문에서는 항법을 위해 가장 많이 사용하는 GPS 민간용 신호의 재방송 재밍에 의한 영향 분석을 바탕으로 수평 위치해의 표본분산에 따른 GPS 재방송 재밍신호 검출 기법을 제안하고, 그 성능을 분석하였다. GPS 수신기의 위치해는 재방송 재밍기에 의해 GPS 수신기를 기준으로 재방송 재밍기의 위치 방향으로 측위오차가 크게 나타나는 것을 확인할 수 있다. 따라서 이를 기준으로 재방송 재밍 공격 여부를 판단할 수 있었으며, 설정한 값에 따른 재방송 재밍 검출 성능을 확인하였다. 본 논문에서는 임의로 설정한 문턱 값을 사용해 검출과 오판정 성능을 얻었다. 추후에는 이론적 분석을 통해 오경보 확률에 따른 검출확률을 분석할 예정이다. 또한 본 논문에서는 단순한 측위해의 오차만을 고려하였으나 방향 등을 추가적으로 고려해 세부적인 실험과 분석을 수행한다면 재방송 재밍 공격에 따른 효과적인 공격 여부 판단 및 방향 추정 기법을 고안할 수 있을 것으로 예상된다. 추후에는 이에 대한 세부 연구를 수행할 예정이다.

References

[1] R. T. Ioannides, T. Pany, and G. Gibbons, “Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques,” in *Proc. IEEE*, vol. 106, no. 6, pp. 1-21, Jun. 2016.

[2] F. Dovis, *GNSS Interference Threats and Countermeasures*, Artech House, Norwood, MA, 2015.

[3] I.-S. Lee, S.-J. Oh, and J.-H. Han, “Narrow-band jamming signal cancellation algorithm for GPS receivers,” *J. KICS*, vol. 41, no. 08, pp. 859-867, Aug. 2016.

[4] H. Kim, Y. E. Choe, S. Yoo, G.-I. Jee, D.-J. Yeom, and S. Y. Kim, “A study on the repeat-back jamming effects of GPS L1 C/A signal through a field experiments,” in *Proc. KICS Int. Conf. Commun.,* pp. 283-284, Jeju, Korea, Jun. 2016.