MỘT PHƯƠNG PHÁP NÂNG CAO HIỆU QUẢ CHẾ ÁP PHƯƠNG TIỆN BAY KHÔNG NGƯỜI LÁI SIÊU NHẸ BẰNG TẠO NHIỄU GIẢ TÍN HIỆU GPS

Nguyễn Văn Cường[1*], Phạm Trọng Hoan[1], Nguyễn Lê Cường[2], Nguyễn Huy Hoàng[3]

Tóm tắt: *Bài báo này trình bày một phương pháp tạo ra tín hiệu giống với tín hiệu GPS nhưng không chứa các thông tin cần thiết cho việc tính toán vị trí hoặc chứa thông tin sai lệch, làm cho máy thu không thể hoặc nhầm lẫn trong việc tính toán chính xác vị trí của mình, để nâng cao hiệu quả chế áp đối với bộ thu GPS trên các phương tiện bay không người lái siêu nhẹ (PTBKNLSN). Nền tảng phần cứng vô tuyến cấu hình mềm (SDR) được sử dụng để tạo ra tín hiệu này. Kết quả lý thuyết và thực nghiệm cho thấy hiệu quả của phương pháp được đề xuất.*

Từ khóa: Chế áp; GPS; SDR.

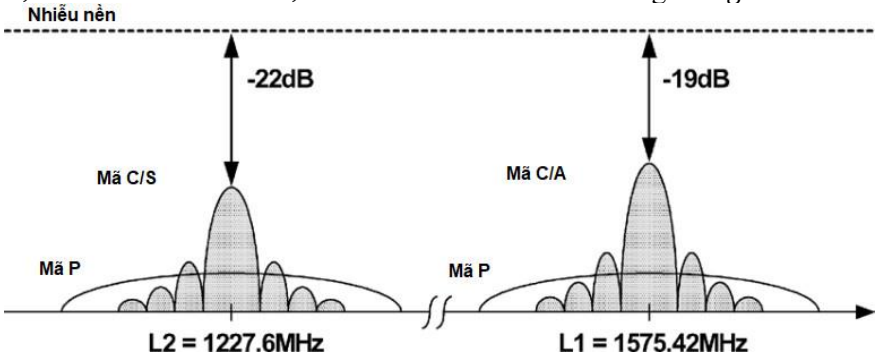
1. ĐẶT VẤN ĐỀ

Trong thời gian gần đây, các phương tiện bay không người lái siêu nhẹ (PTBKNLSN) ngày càng phổ biến được sử dụng vào nhiều mục đích khác nhau. Mặc dù đã có các quy định nhưng vẫn có nhiều vụ việc đáng tiếc xảy ra nguyên nhân xuất phát từ các hoạt động bay trái phép. Để giúp giảm thiểu vấn đề này, có nhiều cách tiếp cận khác nhau trong đó chế áp là một trong những cách đem lại hiệu quả. Trong các loại tín hiệu được sử dụng trên các PTBKNLSN Flycam thì GPS rất quan trọng được dùng để ổn định vị trí, lái tự động và điều hướng. Hiệu quả của việc gây nhiễu đối với từng loại tín hiệu phụ thuộc rất nhiều vào dạng của nhiễu hay loại nhiễu được tạo ra [1]. Trong bài báo này, chúng tôi khảo sát một số dạng nhiễu khác nhau đối với tín hiệu GPS và đề xuất một phương pháp nâng cao hiệu quả chế áp bằng tạo nhiễu giả tín hiệu GPS. Các dạng nhiễu này được tạo ra dựa trên nền tảng vô tuyến cấu hình mềm và thử nghiệm trên thực tế để đánh giá hiệu quả gây nhiễu đối với bộ thu GPS của Flycam.

2. TÍN HIỆU GPS

GPS là hệ thống vệ tinh dẫn đường toàn cầu sử dụng phổ biến nhất hiện nay được ứng dụng với các mục đích khác nhau trong đời sống như bản đồ, điều hướng, giao thông, xây dựng, các PTBKNLSN,… GPS cung cấp vị trí và thời gian chính xác với 24 vệ tinh nằm trong sáu mặt phẳng quỹ đạo. Mỗi vệ tinh GPS truyền đi hai tín hiệu trải phổ trên băng tần L tại hai tần số: L1 với tần số 1.575,420 MHz và L2 với tần số 1.227,600 MHz. Hai tần số tạo ra từ tần số cơ bản 10,23 MHz, được nhân với 154 và 120, tương ứng. Như vậy, tần số (L) và bước sóng (λ) của L1 và L2 là:

+ L1 = 10,23 MHz × 154 = 1575,42 MHz và λ = 19 cm với băng thông 15,345 MHz;
+ L2 = 10,23 MHz × 120 = 1227,60 MHz và λ = 24 cm với băng thông 11 MHz.



Hình 1. *Mô tả tín hiệu GPS và nhiễu nền.*

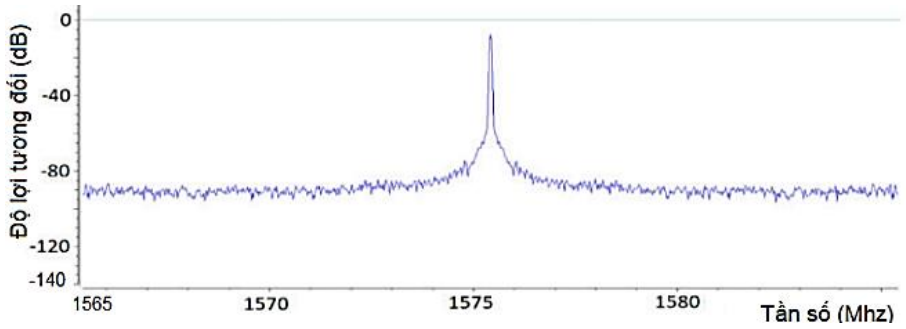
Tín hiệu L1 sử dụng loại điều chế BPSK với hai chuỗi mã giả ngẫu nhiên theo dạng cầu phương là mã C/A và mã P. Các dịch vụ định vị tiêu chuẩn [10] như trên các PTBKNLSN Flycam thu mã C/A trên băng L1 để xác định vệ tinh từ đó tính ra tọa độ. Vì vậy, trong bài báo này, tín hiệu nhiễu giả GPS cũng mô phỏng lại tín hiệu mã C/A từ các vệ tinh trên băng L1.

3. CÁC PHƯƠNG PHÁP CHẾ ÁP TÍN HIỆU GPS

Bộ gây nhiễu là một thiết bị có khả năng ngăn chặn việc tiếp nhận các tín hiệu, chẳng hạn như các tín hiệu được sử dụng trong hệ thống GNSS, hệ thống thông tin di động, Wi-Fi, v.v. Để tạo ra một thiết bị gây nhiễu tín hiệu GPS, chúng ta có thể áp dụng các kỹ thuật được dùng để làm nhiễu các loại tín hiệu khác. Bài báo này sẽ tập trung vào 5 phương pháp gây nhiễu GPS được trình bày sau đây.

3.1. Chế áp tín hiệu GPS sử dụng nhiễu ngắm

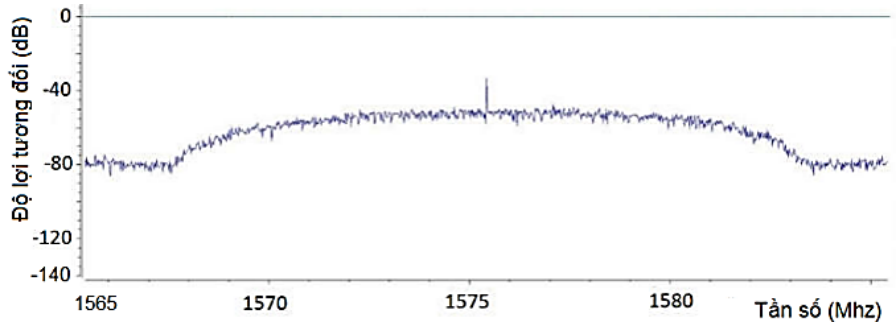
Nhiễu ngắm là gây nhiễu băng hẹp. Trong kỹ thuật này, chỉ một hình sin được truyền đi trên cùng tần số với sóng mang của tín hiệu [7], tất cả năng lượng được tập trung tại tần số trung tâm, thể hiện ở hình 2, phù hợp với mục tiêu có băng thông thấp và biết chính xác tần số. Đây chính là nhược điểm của kỹ thuật trong việc chế áp tín hiệu trải phổ của GPS dẫn đến hiệu quả chế áp thấp [8].



Hình 2. *Phổ nhiễu ngắm.*

3.2. Chế áp tín hiệu GPS sử dụng nhiễu chặn

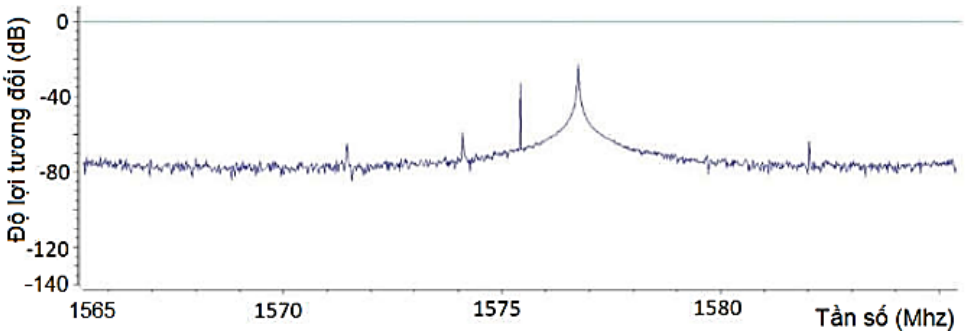
Nhiễu chặn gây nhiễu đến một dải tần cụ thể cho toàn bộ phổ mục tiêu [8], hiệu quả sử dụng năng lượng thấp, phù hợp trong trường hợp mục tiêu có băng thông rộng hoặc có khả năng nhảy tần. Ứng dụng kỹ thuật này vào gây nhiễu tín hiệu GPS đạt hiệu quả [8] với mục tiêu chế áp là dải tần L1 tần số 1575.42 Mhz và băng thông 15,4 Mhz.



Hình 3. *Phổ nhiễu chặn.*

3.3. Chế áp tín hiệu GPS sử dụng nhiễu quét

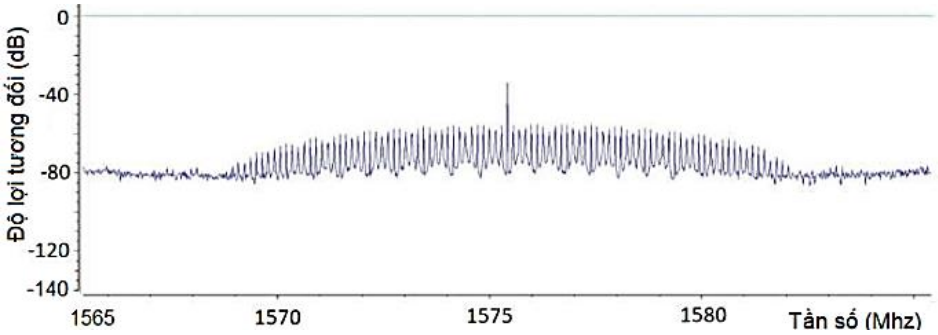
Nhiễu quét là sự kết hợp của kỹ thuật gây nhiễu chặn và gây nhiễu ngắm [7], cũng gây nhiễu trên toàn bộ phổ tần mục tiêu nhưng khác ở điểm, nhiễu chặn phát ra tín hiệu tĩnh còn nhiễu quét thay đổi các tần số trên toàn băng thông đó. Ưu điểm của kỹ thuật này là mật độ phổ công suất tập trung cao, gây nhiễu được trên băng thông lớn, hiệu quả cao với chế áp tín hiệu GPS [8].



Hình 4. *Phổ nhiễu quét.*

3.4. Chế áp tín hiệu GPS sử dụng nhiễu xung

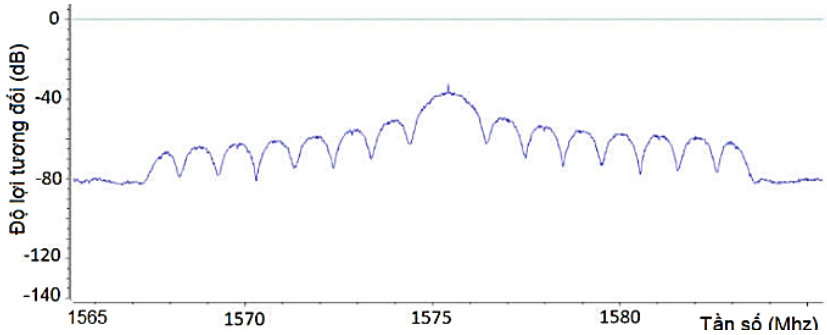
Nhiễu xung tạo tín hiệu gây nhiễu theo chu kỳ với khoảng thời gian được thiết lập tùy thuộc vào mục tiêu [8]. Kỹ thuật này có thể gây nhiễu từ dải hẹp đến dải rộng bằng cách sử dụng một hoặc nhiều nhiễu điểm, tiết kệm năng lượng nguồn phát. Tuy nhiên, vì nhiễu có tính chu kỳ nên có thời gian để tín hiệu kết nối lại, đây cũng là nhược điểm lớn của kỹ thuật. Hiệu quả chế áp đối với tín hiệu GPS là thấp [8].



Hình 5. *Phổ nhiễu xung.*

3.5. Chế áp tín hiệu GPS sử dụng nhiễu giao thức

Nhiễu giao thức là một kỹ thuật gây nhiễu bắt chước các tham số, giao thức của tín hiệu [8], từ đó tạo ra một phổ tương tự trộn lẫn với tín hiệu mục tiêu, để phá hủy thông tin của chúng hoặc không tiếp nhận được ở máy thu. Kỹ thuật này tiết kiệm năng lượng nguồn phát và cho mật độ phổ công suất ở mức trung bình, tuy nhiên lại đem lại hiệu quả chế áp cao đối với tín hiệu GPS [8].



Hình 6. *Phổ nhiễu giao thức.*

Dựa trên phổ tần gây nhiễu đối với tín hiệu GPS chia 5 phương pháp trên thành 2 loại:

+ Gây nhiễu băng hẹp: Nhiễu điểm;

+ Gây nhiễu băng rộng: Nhiễu chặn, nhiễu quét, nhiễu xung và nhiễu giao thức.

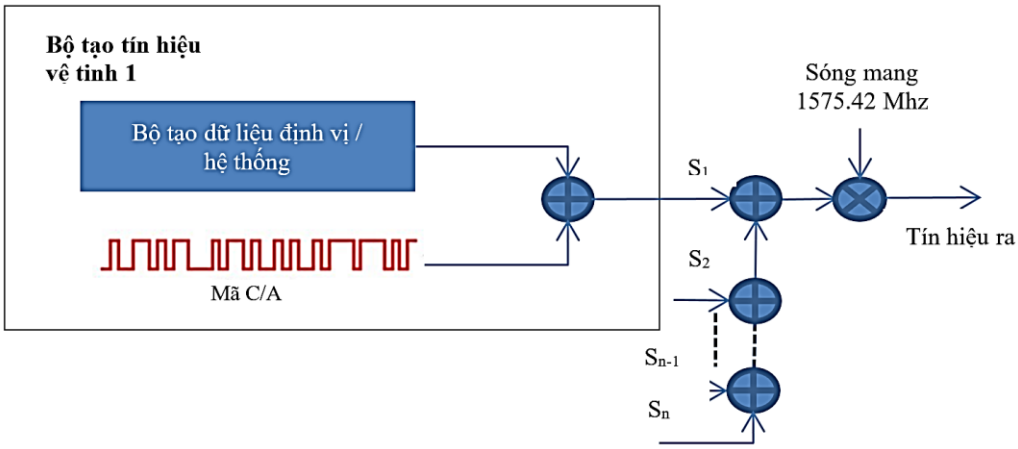
Với 5 phương pháp gây nhiễu được trình bày ở trên theo kết quả tại [8] các phương pháp gây nhiễu chặn, nhiễu quét và nhiễu giao thức đem lại hiệu quả chế áp hơn hẳn nhiễu ngắm và nhiễu xung. Các kết quả trình bày tại [2, 8] cho thấy, để chế áp hiệu quả tín hiệu GPS thì tín hiệu gây nhiễu phải bao phủ toàn bộ băng thông của mã C/A và mật độ phổ công suất phải tập trung tại tần số trung tâm.

3.6. Chế áp tín hiệu GPS sử dụng phương pháp tạo nhiễu giả tín hiệu GPS

Nhiễu giao thức cho phổ tín hiệu gây nhiễu rất giống với phổ tín hiệu GPS là loại nhiễu đem lại hiệu quả chế áp cao. Bài báo đề xuất một phương pháp nâng cao hiệu quả chế áp PTBKNLSN cụ thể là Flycam [12], bằng tạo nhiễu giả tín hiệu GPS được phát triển trên phương pháp tạo nhiễu giao thức thuộc nhóm gây nhiễu băng rộng. Đánh giá hiệu quả khi so sánh với phương pháp tạo nhiễu ngắm thuộc nhóm gây nhiễu băng hẹp.

Các bộ tạo giả tín hiệu GPS được ứng dụng trong cả dân dụng và quốc phòng. Trong dân dụng các thiết bị tạo giả tín hiệu GPS thường dùng phục vụ mục đích kiểm thử thiết bị thu như sản phẩm của LabSat[14], hệ thống mô phỏng tín hiệu NAVISIM của trung tâm NAVIS-Đại học Bach Khoa Hà Nội [15],... Trong quốc phòng, tạo giả tín hiệu GPS nhằm đánh lừa các bộ thu GPS, khiến nó tính toán ra một vị trí khác với vị trí thực của nó hoặc một thời điểm khác được ứng dụng để bảo vệ hoặc đánh lừa mục tiêu [16],... Tuy nhiên, cũng là tín hiệu giả GPS nhưng khi không mang thông tin hoặc thông tin không đúng lại trở thành tín hiệu gây nhiễu với bộ thu.

Trước tiên, bài báo xây dựng mô hình tạo nhiễu giả tín hiệu GPS.

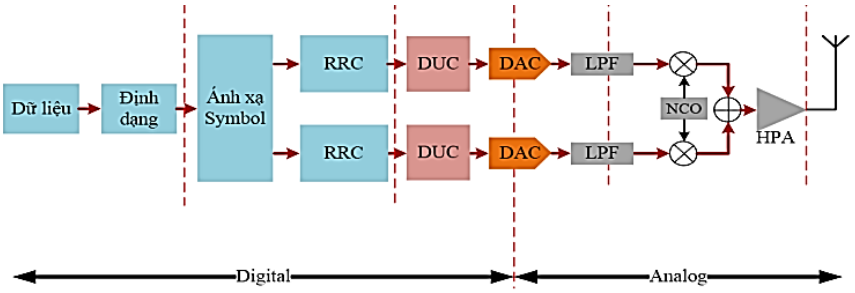


Hình 7. *Mô hình bộ tạo nhiễu giả tín hiệu GPS.*

Các bộ tạo tín hiệu vệ tinh: Sử dụng các dữ liệu là thông tin thiên văn của vệ tinh trong hệ tọa độ ECEF và tọa độ muốn tạo giả tổng hợp thành bản tin gửi đi với mã C/A. Để đảm bảo giống với tín hiệu GPS thật phải có ít nhất 4 bộ tạo tín hiệu vệ tinh trong luồng dữ liệu cuối. Luồng dữ liệu cuối sau đó đẩy lên cao tần với sóng mang băng L1 tần số 1575.42 Mhz để truyền đi.

Mô hình tạo nhiễu giả trên khi triển khai trên nền tảng phần cứng vô tuyến cấu hình mềm (SDR) sẽ được ánh xạ và vào khối chức năng như mô tả ở hình 8. Bộ tạo tín hiệu vệ tinh được thực hiện bằng máy tính, đầu ra sẽ là luồng dữ liệu thể hiện là khối "Dữ liệu" trên hình 8. Luồng dữ liệu chuyển xuống phần cứng SDR tại đây với FPGA dung lượng lớn thực hiện việc điều chế số BPSK tạo ra đúng dạng sóng của tín hiệu GPS, trên sơ đồ hình 8 cả quá trình này là phần "Digital".

Luồng dữ liệu số sau điều chế đẩy vào DAC để ra tín hiệu tương tự. Bộ dao động nội NCO tạo sóng mang cao tần tại tần số 1575.42Mhz ghép với tín hiệu sau bộ lọc thông thấp LPF cho ta tín hiệu nhiễu giả GPS, bộ HPA khuếch đại tín hiệu để đưa ra ăng-ten, tất cả các khối chức năng này được gộp chung vào phần "Analog" trên hình 8.



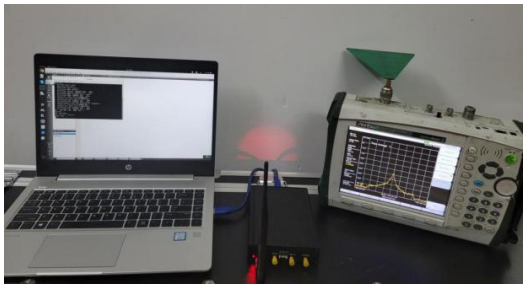
Hình 8. *Sơ đồ khối bộ tạo nhiễu giả tín hiệu GPS.*

Tín hiệu nhiễu giả GPS phát ra tại ăng-ten là tín hiệu chế áp đối với các bộ thu GPS trên PTBKNL Flycam.

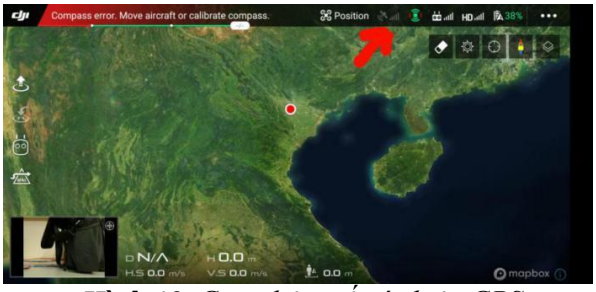
4. ĐÁNH GIÁ THỬ NGHIỆM

4.1. Thử nghiệm tạo nhiễu giả tín hiệu GPS

Quá trình tạo nhiễu giả tín hiệu GPS bằng cách sử máy tính chạy hệ điều hành Ubuntu 18.04 tạo ra luồng dữ liệu tín hiệu băng cơ sở GPS, sau đó, đẩy xuống nền tảng phần cứng vô tuyến cấu hình mềm (SDR) B210 của Ettus chuyển thành tín hiệu RF tại tần số 1575.42 Mhz với công suất -7.4 dBm (mức TxGain = 60 dB).



Hình 9. *Thử nghiệm thiết bị.*



Hình 10. *Giao diện mất tín hiệu GPS trên DJI app.*

Với nhiễu giả tín hiệu GPS, phần mềm được biên dịch với việc loại bỏ các thông tin thiên văn tại tệp dữ liệu BRDC được cung cấp miễn phí từ NASA, hoặc cung cấp một tọa độ sai không tồn tại trên Trái đất. Tham số không mang thông tin hoặc thông tin sai lệch này làm cho tín hiệu giả GPS trở thành tín hiệu nhiễu đối với máy thu.

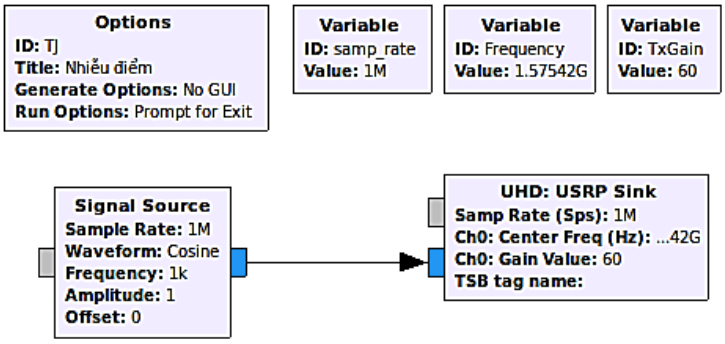
```
1     2             NAVIGATION DATA                     RINEX VERSION / TYPE
2 CCRINEXN V1.6.0 UX  CDDIS               05-JUL-21 06:42     PGM / RUN BY / DATE
3 IGS BROADCAST EPHEMERIS FILE                            COMMENT
4     0.7451D-08  0.2235D-07 -0.5960D-07 -0.1192D-06          ION ALPHA
5     0.9216D+05  0.1311D+06 -0.6554D+05 -0.5243D+06          ION BETA
6     0.186264514923D-08 0.444089209850D-14   319488     2165 DELTA-UTC: A0,A1,T,W
7     18                                                    LEAP SECONDS
8                                                           END OF HEADER        (1)
```

gps-sdr-sim -e brdc1640.21n -l 8888.888888,9999.999999 (2)

Đoạn dữ liệu (1) là một phần trong tệp dữ liệu thiên văn BRDC cần loại bỏ. Dãy số gạch chân ở (2) là tọa độ không tồn tại trên Trái đất. Kết quả đo được tại đầu ra của bộ phát tín hiệu cho ta dạng phổ tương tự với tín hiệu GPS chuẩn nhưng khi phát ra ăng-ten lại làm cho Flycam thử nghiệm không định vị được vị trí, kết quả cũng tương tự khi ta xoá toàn bộ thông tin thiên văn trong tệp dữ liệu brdc1640.21n. Hình 10 là phần mềm điều khiển Flycam của DJI cho ta thấy kết quả của thử nghiệm. Như vậy, việc tạo nhiễu giả đã mang lại kết quả chế áp đối với tín hiệu GPS.

4.2. Đánh giá hiệu quả chế áp của nhiễu giả tín hiệu GPS và nhiễu điểm

Bài báo cũng tạo ra một tín hiệu gây nhiễu điểm bằng việc sử dụng phần mềm GNU Radio kết hợp cùng phần cứng SDR.



Hình 11. *Sơ đồ phần mềm tạo nhiễu điểm thực hiện trên GNU Radio.*

Đánh hiệu quả chế áp cho hai kỹ thuật gây nhiễu là nhiễu điểm và nhiễu giao thức với phương pháp tạo giả tín hiệu GPS tại cũng mức TxGain = 60 dB ở bộ phát B210, ăng-ten phát vô hướng omni độ lợi 3 dBi đặt cao 2 m, các vật mẫu thử nghiệm đặt dưới đất. Thử nghiệm được tiến hành với Flycam DJI Mavic 2 Pro và DJI Phantom 3 cho ra kết quả chỉ ra ở 2 bảng sau.

Bảng 1. *Kết quả thử nghiệm đối với Flycam DJI Mavic 2 Pro*

Khoảng cách / Loại nhiễu	10m	20m	30m	35m	40m
Nhiễu điểm	✓	✓	X	X	X
Nhiễu từ tạo giả tín hiệu GPS	✓	✓	✓	✓	X

✓:Flycam nhận được vị trí. X: Flycam không định vị được vị trí.

Bảng 2. *Kết quả thử nghiệm đối với Flycam DJI Phantom 3.*

Khoảng cách / Loại nhiễu	10m	20m	30m	35m	40m
Nhiễu điểm	✓	✓	✓	X	X
Nhiễu từ tạo giả tín hiệu GPS	✓	✓	✓	✓	✓

✓:Flycam nhận được vị trí. X: Flycam không định vị được vị trí.

Từ bảng trên cho thấy, nhiễu giả tín hiệu GPS cho cự ly chế áp hơn hẳn nhiễu điểm trên các vật mẫu thử và hiệu quả chế áp không giống nhau trên các mẫu thử khác nhau.

5. KẾT LUẬN

Bài báo này đánh giá phương pháp tạo ra nhiễu giả tín hiệu GPS đã nâng cao hiệu quả chế áp, dẫn đến mất khả năng định vị và điều hướng của PTBKNLSN Flycam. Thiết bị tạo ra tín hiệu tương tự như GPS chuẩn, tín hiệu này trộn lẫn hiệu quả với tín hiệu GPS thật vì dạng phổ giống hệt nhau, tuy nhiên, do không mang thông tin hoặc mang thông tin không đúng khiến tại các máy thu không thể nhận được dữ liệu định vị từ các vệ tinh thật, vì vậy, chúng được xem như đã bị chế áp. Phương pháp thực hiện tương đối phức tạp vì phải kết hợp giữa phần mềm chạy trên máy tính và phần cứng SDR, tuy nhiên, hiệu quả chế áp lại rất tốt.

TÀI LIỆU THAM KHẢO

[1]. Richard Poisel. *"Modern Communications Jamming Principles and Techniques",* ARTECH HOUSE, pp.467-503.

[2]. H. Hu, N. Wei, *"A study of GPS jamming and anti-jamming"* Published in: 2009 2nd International Conference on Power Electronics and Intelligent Transportation System (PEITS).

[3]. K. Grover, A. Lim, Q. Yang, *"Jamming and anti-jamming techniques in wireless networks: a survey"* - International Journal of Ad Hoc and Ubiquitous Computing, 2014 Vol.17 No.4, pp.197 – 215.

[4]. J. Gaspar, R. Ferreira, P. Sebastião and N. Souto, *"Capture of UAVs Through GPS Spoofing,"* 2018 Global Wireless Summit (GWS), Chiang Rai, Thailand, 2018, pp. 21-26, doi:10.1109/GWS.2018.8686727.
[5]. What-when-how - In Depth Tutorials and Information, *"GNSS Antennas and Front Ends (GPS and Galileo Receiver) Part 1"*[Online]. Available: http://what-when-how.com/a-software-defined-gps-and-galileo-receiver/gnss-antennas-and-front-ends-gps-and-galileo-receiver-part-1/. [Accessed: 14-July-2018].
[6]. K. Pärlin, *"Jamming of Spread Spectrum Communications used in UAV Remote Control Systems",* Tallinn University of Technology, School of Information Technologies, Thomas Johann Seebeck Department of Electronics 2017.
[7]. Ahmad Danial Bin Abdul Rahman, *"Unmanned Aerial Vehicle (UAV) GPS Jamming Test by using Software Defined Radio (SDR) platform",* J. Phys.: Conf. Ser. 1793 012060.
[8]. R. Ferreira, J. Gaspar, P. Sebastião, and N. Souto, *"Effective GPS Jamming Techniques for UAVs Using Low-Cost SDR Platforms,"* Wireless Pers Commun (2020). doi.org/10.1007/s11277-020-07212-6.
[9]. Arslan, Hüseyin, and Joseph Mitola III. *"Cognitive radio, software-defined radio, and adaptive wireless systems."* Wireless Communications and Mobile Computing 7.9 (2007): 1033-1035.
[10]. http://www.csr.utexas.edu/texas_pwv/midterm/gabor/gps.html.
[11]. Software-Defined GPS Signal Simulator. https://github.com/osqzss/gps-sdr-sim.
[12]. Nguyễn Huy Hoàng, *"Ứng dụng phương pháp TDOA để xác định tọa độ phương tiện bay không người lái siêu nhẹ Flycam",* TC. Nghiên cứu KHCNQS, Số Đặc san Hội thảo Quốc gia FEE, tr.166.
[13]. Thang Xuan Pham, *"Apply Satellite Position Interpolation Algorithm in the Implementation of GPS signal Generator in Laboratory"* 19th International Conference on IT Applications and Management, 2018, pp.202-205.
[14]. https://www.labsat.co.uk/index.php/en/applications/receiver-sensitivity-testing.
[15]. https://soict.hust.edu.vn/bo-mon/bo-mon-trung-tam/trung-tam-navis.
[16]. https://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea.

ABSTRACT

A METHOD TO ENHANCE THE EFFICIENCY OF JAMMING ULTRA-LIGHT DRONES BY GENERATING FAKE GPS SIGNAL

This paper present a method of generating fake GPS signal that does not include information or incorrect location. This method improves jamming performence to GPS receiver signal on ultra-light drones. It was built using Software-defined radio hardware (SDR) to evaluate this method. The results of theory and experiment shows efficiency of this method.

Keywords: Jamming; Fake GPS; SDR.

Nhận bài ngày 30 tháng 6 năm 2021
Hoàn thiện ngày 30 tháng 7 năm 2021
Chấp nhận đăng ngày 02 tháng 8 năm 2021

Địa chỉ: [1]Công ty Cổ phần công nghệ Macrocom;
[2]Đại học Điện lực;
[3]Khoa Vô tuyến điện tử, Học viện Kỹ thuật quân sự.
*Email: cuongnvth@gmail.com.