مجلة جامعة دمشق للعلوم الهندسية
المجلد 42 العدد (2) :272-292

Damascus University Journal for Engineering Sciences
V42 No(2): 272-292

تقدير فعَّاليّة تقنية التشويش الواعي للبروتوكول مع رسالة ملاحة على منظومات الملاحة على متن الطائرات من دون طيار

عبده بللوق[*1] محمد خالد شاهين[2] محمد الحريري[3]

[*1]. طالب دراسات عليا، دكتوراه هندسة اتصالات متقدّمة، كلية الهندسة الميكانيكيّة والكهربائيّة، جامعة دمشق.
e.abdo @damascusuniversity.edu.sy

[2]. دكتور، أستاذ مساعد، في قسم هندسة الإلكترونيات والاتصالات في كلية الهندسة الميكانيكيّة والكهربائيّة بجامعة دمشق.
mk.chahine@damascusuniversity.edu.sy

[3]. دكتور، باحث رئيسي في المعهد العالي للعلوم التطبيقية والتكنولوجيا.
mohamad.alhariri@hiast.edu.sy

الملخص:

تشكل الطائرات من دون طيار UAVs أخطاراً أمنية على المنشآت الحيوية؛ إذ يمكن أن ينجم عن الاستخدام غير المرخص لتلك الطائرات وقوع حوادث، أو شن هجمات أو مراقبات غير قانونية. لذا ينبغي منعها من التحليق فوق المرافق المهمّة. ويشكل مستقبِل المنظومة الشاملة لتحديد المواقع GPS قلب منظومة الملاحة الخاصة بالطائرة من دون طيار، والتي من دونها يصعب السيطرة على الطائرة وتوجيهها. نقترح في هذه الورقة البحثية تصميماً لمنظومة تشويش على مستقبلات المنظومة الشاملة لتحديد المواقع GPS وتنفيذها باستخدام تقنية التشويش الواعي للبروتوكول والمتضمن لرسالة الملاحة. كما نعرض نتائج محاكاة منفذة بالاعتماد على برمجية ماتلاب MATLAB لتوليد إشارة تشويش واعية لبروتوكول تشكيل إشارات سواتل المنظومة الشاملة لتحديد المواقع.

إضافةً إلى ذلك، قمنا بالاعتماد على منصات الراديو المعرّف برمجياً وأدوات برمجية أخرى بتوليد إشارات مطابقة لإشارات الاستخدام المدني لثلاثة عشر ساتلاً من سواتل المنظومة الشاملة لتحديد المواقع عند التردد L1 (1.575.42 ميغا هرتز)، والتي تتضمن رِماز التحصيل الخشن C/A، وباستطاعة إرسال إجمالية -3.5 ديسيبل ميلي واط، مع إمكانية تعديل التوقيت في رسالة الملاحة بغرض تحديد موقع مزيف، وقد اختبرنا المنظومة المقترحة على عدد من الطائرات من دون طيار الصغيرة. وقد أظهرت النتائج نجاح تقنية التشويش الواعي للبروتوكول في حجب إشارات المنظومة الشاملة لتحديد المواقع الحقيقية عن المستقبل، وجعله يستقبل إشارات مزيفة؛ ومن ثمَّ تغيير موقع الطائرة الحقيقي إلى موقع مزيف مختار مسبقاً.

الكلمات المفتاحية: تقنيات التشويش، المنظومة الشاملة لتحديد المواقع، الطائرات من دون طيار، التشويش الواعي للبروتوكول، منظومات الملاحة الساتلية الشاملة.

تاريخ الإيداع: 2023/8/16
تاريخ القبول: 2023/11/7

حقوق النشر: جامعة دمشق – سورية، يحتفظ المؤلفون بحقوق النشر بموجب CC BY-NC-SA

Estimating the Effectiveness of Protocol-Aware Jamming Technique with a Navigation Message on Navigation Systems Onboard UAVs

Abdo Ballouk*[1] Mohamed Khaled Chahine[2] Mohamed Alhariri[3]

*[1]. Higher Education Student – Advanced Communications Engineering Ph.D. - Faculty of Mechanical and Electrical Engineering – Damascus University.
e.abdo @damascusuniversity.edu.sy

[2]. Dr, Associate Professor – Department of Electronics and Communication Engineering – Faculty of Mechanical and Electrical Engineering – Damascus University.
mk.chahine@damascusuniversity.edu.sy

[3]. Dr, Major Researcher, Higher Institute of Applied Sciences and Technology.
mohamad.alhariri@hiast.edu.sy

Received: 16/8/2023
Accepted: 7/11/2023

Copyright:Damascus University-Syria,The authors retain the copyright under a CC BY- NC-SA

Abstract:

Unmanned Aerial Vehicles (UAVs) present security threats to vital facilities, as the unauthorized use of these drones could cause accidents or carry at tacks or illegal surveillance. Thus, it is necessary to prohibited drones from flying over important facilities. Global Positioning System (GPS) receiver forms the heart of the navigation system of UAV, and without it, it is difficult to control and direct the aircraft. In this paper, we propose a design of a jamming system for GPS receivers and its implementation using the protocol-aware jamming technique, which includes a navigation message. We also present the results of a simulation done using MATLAB to generate a jamming signal conforming to the GPS satellite signal-shaping protocol. In addition, using software-defined radio platforms and other software tools we generated signals identical to the civilian use signals broadcasted by 13 GPS satellites on the L1 frequency (1575.42 MHz) which currently contains the coarse/acquisition (C/A) code, with a transmission power of -3.5 dBm; with the possibility of adjusting the timing in the navigation message to locate a fake location.

The proposed system was tested using several small UAVs, and the results showed the success of the protocol-aware jamming technique in blinding the receiver from the real GPS satellite signals, making it receive fake signals; thus changing the real aircraft location to a pre-selected fake location.

Keywords: Jamming techniques, GPS, UAVs, Protocol-Aware Jamming, and Global Navigation Satellite Systems.

المقدمة:

شاع في السنوات الأخيرة استخدام الطائرات من دون طيار Unmanned Aerial Vehicles (UAVs) الصغيرة في تطبيقات عسكرية ومدنية؛ إلا أن هذه الطائرات تطرح إشكاليات في كلا المجالين نظراً لأن التطبيق يمكنه مراقبة خصوصية الأفراد والمؤسسات، وجمع معطيات، أو حتى تنفيذ هجمات (Kim, 2021).

وتعتمد الطائرة من دون طيار في عملها بشكل رئيسي على المنظومة الشاملة لتحديد المواقع Global Positioning System (GPS)؛ حيث تقوم عادة بإرسال موقعها إلى متحكم أرضي وتلقي الأوامر منه. في حين تعتمد بعض الطائرات من دون طيار على ذاتها في عمليات التوجيه والطيران، وذلك بمساعدة طيار آلي يتبع مسار طيران جرت برمجته مسبقاً وتخزينه. ويقوم الطيار الآلي بمقارنة الموقع الحالي المحدد بوساطة مستقبل GPS مع الموقع المخزن لديه، وإعطاء أوامر للزعانف والمراوح للوصول إلى الموقع المطلوب. إن معظم هذه التجهيزات متوافرة للعامة ورخيصة الثمن، وهي تعتمد بشكل كلي على مستقبل GPS، لذا جرى تطوير تقنيات تشويش تسمح بتحييد عمل المستقبلات GPS الموجودة على متن الطائرات من دون طيار (Sathyamoorthy, 2020).

وتشير الأبحاث الخاصة بأداء تقنيات التشويش المختلفة ضد منظومات الاتصالات اللاسلكية عموماً إلى أنه من أجل التشويش على قناة تحكم الطائرة من دون طيار بكفاءة، فمن المستحسن استخدام تقنية التشويش الواعي للبروتوكول protocol-aware jamming (Poisel, 2011). إذ تأخذ هذه التقنية بالحسبان خصائص الإشارة اللاسلكية المرسلة بوساطة جهاز التحكم عن بعد، وتستخدم إشارة تشويش مشابهة للإشارة المرسلة للإخلال بعمل الطائرات من دون طيار. وتجدر الإشارة إلى توافر تقنيات تشويش أخرى منها التشويش السدّي barrage jamming والتشويش بالنغمات tone jamming والتشويش المسحي sweep jamming وهي أقل تعقيداً، لكنها لا تأخذ بالحسبان جميع خصائص الإشارة المستهدفة. وقد جرى اقتراح استخدام تقنيات تعلّم الآلة والتعلّم العميق في إجرائيات التشويش على الطائرات من دون طيار وتضليلها (Simon, 2022).

أما في ورقتنا البحثية فلن نقوم بدراسة التشويش الواعي للبروتوكول التقليدي الشائع الاستخدام في الأدبيات، والذي يعتمد على توليد إشارة مشابهة طيفياً للإشارة الحقيقية التي يعمل عندها المستقبل المستهدف، بل سوف نقوم بالاعتماد على الهندسة العكسية بتوليد إشارة تقنية التشويش الواعي للبروتوكول، كما سنقوم بتوليد الإشارات الحقيقية لعدد من سواتل الملاحة الخاصة بالمنظومة الشاملة لتحديد المواقع GPS متضمنة رسائل الملاحة. وقد قمنا بالاعتماد على البيئة البرمجية ماتلاب MATLAB بمحاكاة توليد إشارة تشويش وفق تقنية التشويش الواعي للبروتوكول للتشويش على مستقبل منظومة GPS، وذلك بتوليد إشارة مطابقة لمواصفات الإشارة المرسلة من سواتل المنظومة GPS. بعدها قمنا بالاعتماد على منصة راديو معرَّف برمجياً Software-Defined Radio (SDR) من طراز HackRF وأدوات برمجية أخرى بتوليد إشارات تشويش مطابقة للإشارة المرسلة من 13 ساتل من سواتل المنظومة GPS، قابلة لتغيير في التوقيت بغية تحديد موقع مزيف يمكن اختياره؛ بهدف جعل الطائرات من دون طيار الصغيرة التجارية تنحرف عن أهدافها. كما قمنا بتصميم برنامج تحكم مدعوم بالخرائط بالاعتماد على اللغة البرمجية C# مما يسهل عملية تحديد الموقع المزيف والتحكم بإرسال إشارات التشويش. سوف نستعرض أولاً بنية الإشارة L1 (ذات التردد 1.575.42 ميغا هرتز) التي ترسلها المنظومة الشاملة لتحديد المواقع GPS، ونقدم دراسة تحليلية سريعة لبعض تقنيات

http://journal.damascusuniversity.edu.sy/index.php/index/index
ISSN (online): 2789-6854

التشويش، ثم نستعرض نتائج المحاكاة المنفذة، وأخيراً التنفيذ العملي العتادي والنتائج التي حصلنا عليها، ونقدم بعض التوصيات.

1- الدراسات المرجعية:

درس لي وزملاؤه تأثير فعالية التشويش على قناة تحكم طائرة من دون طيار تعتمد مبدأ القفز الترددي Frequency Hopping (FH)؛ حيث قام الباحثون بالاعتماد على الأداة Simulink المتضمنة في MATLAB بإجراء محاكاة لقناة اتصال تعتمد على القفز الترددي بمعدل 100 قفزة في الثانية، وجرى توليد إشارة تشويش ذات ضجيج أبيض غاوصي. كما قاموا بحساب معدل خطأ البت BER بوجود إشارة التشويش، ووجدوا أنها تزداد بزيادة نسبة استطاعة المشوش إلى الإشارة Jammer-to-Signal Ratio (JSR)، لكنها تتعلق بشكل أكبر بنسبة التداخل إلى الاضطراب، والتي تساوي مدة بقاء إشارة التشويش على مدة بقاء إشارة القفاز، وجد أن أفضل نسبة هي 50%، أي يجب أن تبقى إشارة التشويش نصف مدة بقاء إشارة قفاز الإشارة المستهدفة.

(Li., 2023) وقام سونغ وزملاؤه بدراسة تأثير عرض نبضة تشويش مِكروية واستطاعتها على قناة اتصال قفز ترددي لطائرة من دون طيار من طراز Phantom 4 pro، حيث قاموا بتوليد نبضة مربعة دورية وفق شرطين هما: أن تغطي إشارة التشويش كامل عرض مجال قناة الاتصال، وأن تكون كثافة استطاعة إشارة التشويش من مستوى أعلى من dBm/MHz 70-، لكي تعدّ الطائرة من دون طيار خاضعة للتشويش؛ كما يجب أن لا يتجاوز عرض نبضة إشارة التشويش عرض مجال قناة الاتصال، ووجد الباحثون أنه عند زيادة دور النبضة يضيق عرض النبضة، لكن عندما يكون عرض النبضة ثابت فإن متوسط الاستطاعة المطلوبة للتشويش يزداد ببطء مع زيادة دور النبضة. (Song et al., 2023).

في حين قام هايوانغ Haiwang وزميله بدراسة تقنيات التشويش على الطائرات من دون طيار، حيث اعتمدا على استقبال إشارة منظومة GPS حقيقية، وإجراء انحراف زمني على بتات رسالة الملاحة مما تسبب بحدوث خطأ في حساب موقع الطائرة.

(Haiwang, Z. & Jing, W. 2022)

كما اقترح فيريرا Ferreira وزملاؤه تصميماً لمنظومة تشويش محمولة على الطائرات من دون طيار بالاعتماد على منصة راديو معرف برمجياً من طراز BladeRF x40، حيث قاموا باختبار عدة تقنيات تشويش، ووجدوا أن أفضل تقنية للتشويش على مستقبلات GPS هي تقنية التشويش الواعي للبروتوكول protocol-aware jamming، وأن أفضل تقنية للتشويش على قناة تحكم الطائرة هي تقنية التشويش السدي barrage jamming. (Ferreira et al., 2022)

قدم نورهاشم Norhashim وزملاؤه عام دراسة لأثر التشويش على الطائرات من دون طيار المعتمدة على المنظومة الشاملة لتحديد المواقع GPS استناداً إلى الأزمنة المتغيرة وزوايا الدوران عبر استهداف التردد الحامل للمنظومة GPS. وأجروا الاختبارات في غرفة عديمة الصدى anechoic، وأظهرت النتائج أن فعالية التشويش تتعلق باستطاعة إشارة التشويش وزمن إجراء التجربة بسبب تغير هندسة السواتل (موقع السواتل التي تغطي منطقة المستقبل وعددها)؛ كما تتعلق كفاءة التشويش بزاوية ورود إشارة التشويش بالنسبة للطائرة من دون طيار. (Norhashim et al., 2022)

وقام تشيبر Chiper وزملاؤه باقتراح منظومة دفاع ضد الطائرات من دون طيار معتمدة على منصات راديو معرّف برمجياً SDR طراز USRP E312 محمولة بوساطة طائرة من دون طيار صديقة. تعتمد هذه المنظومة على مبدأ التعرّف على وجود طائرة من دون طيار بالكشف عن الإشارات الراديوية المتبادلة بين الطائرة الهدف والمشغل الأرضي، وباستخدام خوارزميات تحسس الطيف في التنفيذ، إلى جانب تحديد الاتجاه النسبي للطائرة المستهدفة مع عدّ الطائرة من دون طيار

تقدير فعَّاليّة تقنية التشويش الواعي للبروتوكول مع رسالة ملاحة على منظومات الد

الصديقة مرجعاً، وذلك باستخدام خوارزميات الكشف عن زاوية الوصول Angle-of-Arrival (AoA). ويعتمد مبدأ التشويش على إرسال إشارة التشويش على نفس المجال الترددي المستخدم للاتصال من قبل الطائرة الهدف.

(Chiper et al., 2022)

3- الأسس النظرية:

3-1- بنية إشارات المنظومة GPS: تبث سواتل المنظومة الشاملة لتحديد المواقع GPS إشاراتها على ثلاث موجات حاملة هي:

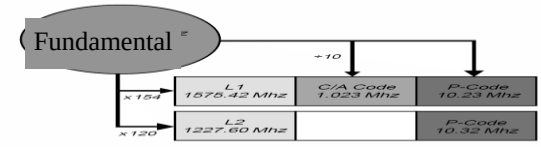
الحامل L1 المستخدمة لملاحقة موضع ساتل المنظومة GPS، وتُبث على التردد 1575.42 ميغاهرتز.

الحامل L2 المستخدمة لملاحقة صحة health سواتل المنظومة GPS، وتُبث على التردد 1227.60 ميغاهرتز.

الحامل L5 المستخدمة لتحسين الضبط accuracy من أجل بعض الاستخدامات المدنية مثل توجيه الطائرات بدقة عند اقترابها من المطارات، وتُبث على التردد 1176 ميغاهرتز.

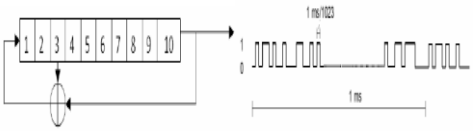
(Egido, 2014)

وتستقبل مستقبلات المنظومة GPS المدنية التردد L1، والذي يحوي رِمازين مُعدِلين هما: رِماز التحصيل الخشن Coarse Acquisition (C/A) code المتاح مجاناً للعموم المرسل على التردد 1.023 ميغا هرتز، والرِماز الدقيق Precision (P) code المقيد الاستخدام والمخصص عادةً للتطبيقات العسكرية المرسل على التردد 10.23 ميغاهرتز. أما الحامل L2 والذي يستخدم للتطبيقات العسكرية فيحوي رمازاً مُعدِلاً واحد فقط: الرِماز الدقيق P عند التردد 10.23 ميغاهرتز. وثمة رِماز آخر هو الرِماز P(Y) وهو حالة خاصة من الرِماز P (Kaplan & Hegarty, 2017). ويُبيّن الشكل (1) الترددات المستخدمة في المنظومة GPS.



الشكل (1) الترددات المستخدمة في المنظومة GPS (Zogg, 2009)

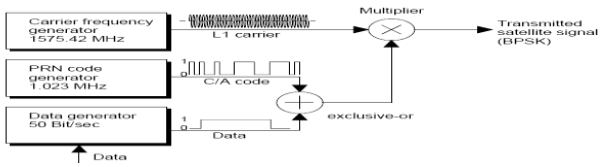
تتألف هذه الرِمازات من سلاسل ضجيج شبه عشوائي Pseudo Random Noise (PRN) مولَّدة بوساطة سجلات إزاحة ذات تغذية خلفية خطية linear-feedback shift register (LFSR)، كما هو مبيّن في الشكل (2).



الشكل (2) سجل إزاحة ذا تغذية خلفية خطية LFSR (Zogg, 2009)

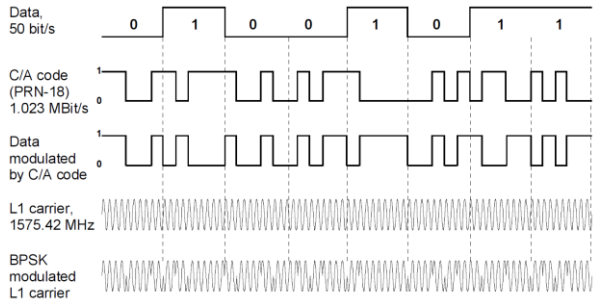
تسمح السلاسل شبه العشوائية بالتمييز بين السواتل المختلفة؛ حتى وإن كانت تبث على نفس المجال الترددي L، بفضل تقانة النفاذ المتعدد بتقسيم الرِماز Code Division Multiple Access (CDMA) (Kaplan & Hegarty, 2017).

تُعدّل المعطيات بالرِماز C/A أو الرِماز P، ويُعّدل الناتج بدوره بوساطة الحامل L1 أو L2 باستخدام التعديل الرقمي بإزاحة الطور الاثناني Binary Phase Shift Keying (BPSK)، كما هو مبيّن في الشكل (3).



الشكل (3) المخطط الصندوقي لمولِّد إشارة الساتل (Zogg, 2009)9

ومع كل تغير في المعطيات المُعدّلة ثمة تغير °180 في طور الحامل L1 أو L2 (Wildemeersch, 2010)، كما هو مبيّن في الشكل (4).



الشكل (4) المخطط الزمني لإشارات سواتل منظومة GPS

(Zogg, 2009)

3-2- توصيف إشارات التشوّيش:

تعرَف إشارات التشوّيش عادةً على أنها إشارات تداخل راديوي Radio Frequency Interference (RFI)، ويمكن أن تكون هذه الإشارات مستمرة أو نبضية.

يرتبط أداء التشويش بنسبة استطاعة التشويش إلى استطاعة الإشارة Jamming-to-Signal Ratio (JSR) عند دخل المستقبل، والتي تُعطى بالعلاقة (1) (Parlin et al., 2017) ويمكن عدّ النسبة JSR مقلوب نسبة استطاعة الإشارة إلى استطاعة الضجيج Signal-to-Noise Ratio (SNR).

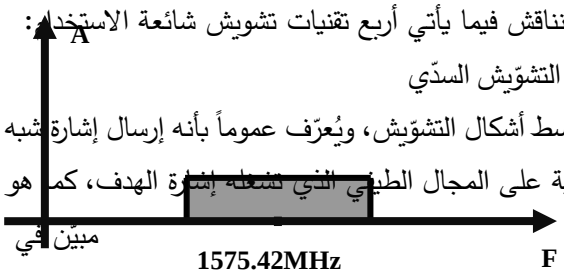
$$JSR_{dB} = 10 * \log_{10}\left(\frac{P_{jammer}+P_{noise}}{P_{signal}}\right) \qquad (1)$$

3-3- تقنيات التشويش الرئيسية:

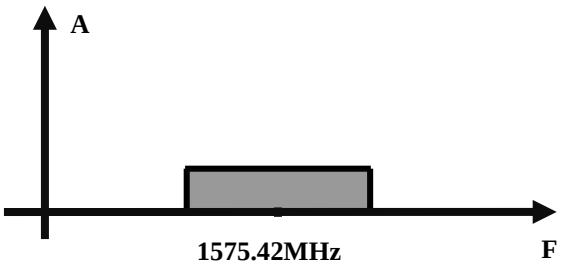
سوف نناقش فيما يأتي أربع تقنيات تشويش شائعة الاستخدام:

أ- التشوّيش السدّي

وهو أبسط أشكال التشوّيش، ويُعرّف عموماً بأنه إرسال إشارة شبه عشوائية على المجال الطيفي الذي تشغله إشارة الهدف، كما هو مبيّن في



الشكل (5)، بهدف زيادة مستوى الضجيج عند جهاز الاستقبال، مما يُصعّب التشغيل الصحيح للمنظومة (Pärlin, 2017).



الشكل (5) طيف إشارة التشويش السدّي (Ferreira et al., 2022)

ب- **التشوّيش المسحي sweep jamming:**

وهي تقنية تشبه كثيراً تقنية التشويش السدّي، لأنها تعمل على كامل المجال الترددي المطلوب. ويتمثل الفرق بين هاتين التقنيتين في أن التشويش المسحي لا يصدر إشارة ذات تردد ثابت أو ذات عرض مجال ترددي ثابت.

وتقنية التشويش المسحي أكثر فاعلية فيما يتعلق بالكثافة الطيفية للاستطاعة، لأنها تُرسل إشارة ضيقة المجال وتمسح الترددات من أجل تغطية كامل عرض المجال الترددي للإشارة المراد التأثير عليها، كما هو مبيّن في الشكل (6). وتُعطى إشارة التشويش المسحي بالعلاقة (2)(Alam et al., 2017).

$$J(t) = P_J \cos(2\pi f(t)t + \varphi) \qquad (2)$$

وفيها يمثل P_J استطاعة التشويش، و φ طور الإشارة، و $f(t)$ التردد الآني والذي يُعطى بالعلاقة (3)(Alam et al., 2017) .

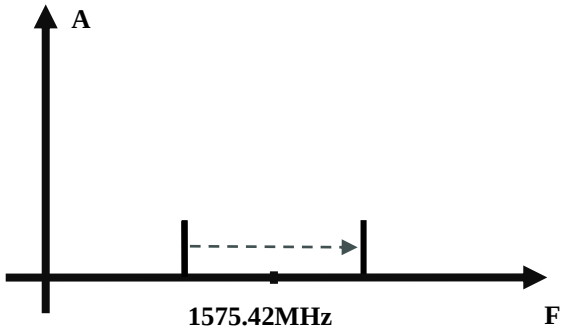
$$f(t) = f_0 + kt \qquad (3)$$

ويعطى المعامل k بالعلاقة (4).

$$k = \frac{f_1 - f_0}{T_{sweep}} \quad (4)$$

وفيها يمثل f_0 التردد الأولي، وf_1 التردد النهائي، وT_{sweep} دور مسح كامل المجال.

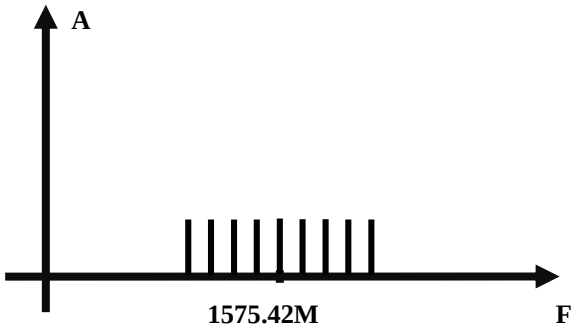
ويبيّن الشكل (6) مبدأ التشويش المسحي.



الشكل (6) مبدأ التشويش المسحي (Ferreiraet al., 2022)

ج- التشويش بالنبضات المتتالية: successive pulses jamming

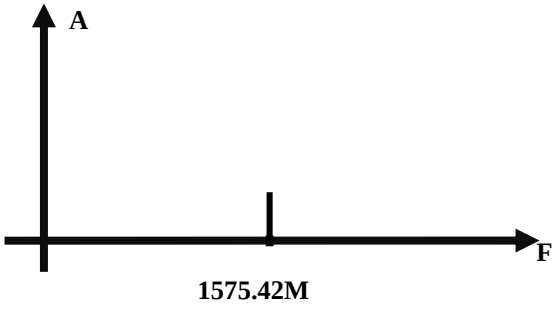
يعتمد هذا النهج على إرسال سلسلة من النبضات ذات دورة تشغيل duty cycle منخفضة على إشارة المنظومة GPS. وباستخدام هذه التقنية، يمكن تحقيق التشوّيش على تردد الموجة الحاملة وذلك بسبب الطيف الناتج عن إشارة التداخل. ويبيّن الشكل (7) طيف إشارة التشويش بالنبضات المتتالية.



الشكل (7) طيف إشارة التشويش بالنبضات المتتالية (Ferreira et al., 2022)

ويجب أن تشغل هذه النبضات الترددية كامل المجال الترددي للإشارة المراد التشويش عليها؛ لذا يطرح توليد هذه النبضات الترددية صعوبة تقنية كبيرة، بالإضافة إلى التكلفة العالية التي تتعلق بعدد هذه الترددات وعرض مجال الإشارة المستهدفة.

د- التشوّيش بالنغمات: tone jamming



الشكل (8) طيف إشارة التشويش بالنغمات (Ferreira et al., 2022)

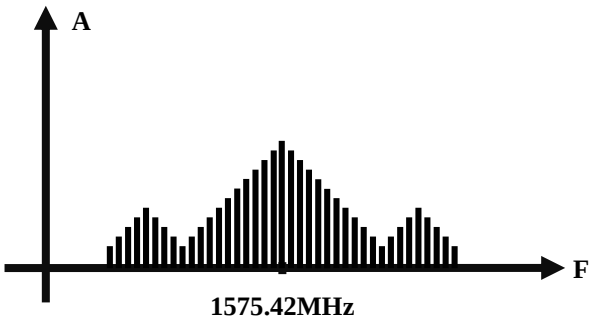
في هذه التقنية يجري إرسال إشارة جيبية لها تردد يساوي تردد الحامل الترددي لإشارة المنظومة GPS، لذا يكون التداخل فقط مع التردد المركزي، وليس مع كامل عرض المجال. وباستخدام

هذه التقنية، يجري تطبيق كامل الاستطاعة المرسلة على التردد المركزي للحامل. وتعطى إشارة التشويش بالنغمات بالعلاقة (5) (Alam et el., 2017).

$$J(t) = \sqrt{\frac{2P_J}{N_J}} \sum_{i=1}^{N_j} \cos(2\pi f_i + \varphi_i) \qquad (5)$$

وفيها تمثل P_J استطاعة التشويش، و N_J عدد النغمات، وf_i تردد النغمة i، و φ_i طور النغمة i. ويبيّن الشكل (8) طيف إشارة التشويش بالنغمات.

هـ- التشوّيش الواعي للبروتوكول:

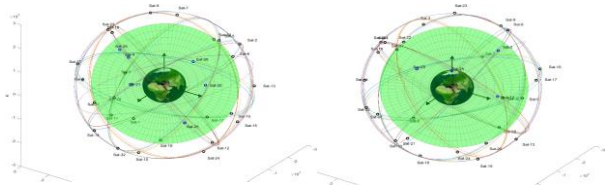


الشكل (9) طيف إشارة تشويش واعٍ للبروتوكول (Ferreira et al., 2022)

تعتمد هذه التقنية على أخذ معاملات parameters الإشارة المستهدفة بالحسبان أثناء تشكيل إشارة التشويش، وتشتمل هذه المعاملات على نوع التعديل ومعدل المعطيات وعرض مجال القناة. وفي حال استخدام تقنية الطيف المنثور بالقفز الترددي Frequency-Hopping Spread Spectrum (FHSS)، فيجب معرفة ترددات القناة وأنماط القفز ومعدل القفز؛ أما في حال استخدام تقنية الطيف المنثور بالسلسلة المباشرة (DSSS) Direct-Sequence Spread Spectrum فيجب معرفة الرِماز شبه الضجيجي Pseudo Noise (PN) المستخدم لنثر الطيف. إن القدرة على مزامنة شكل موجة التشويش مع إشارة الهدف مطلوبة أيضاً في التشويش الواعي للبروتوكول. ويبيّن الشكل (9) مثالاً على طيف إشارة تشويش واعٍ للبروتوكول.

4- النتائج والمناقشة:

4-1 التنفيذ العملي البرمجي:



الشكل (10) السواتل الواقعة في مجال رؤية المستقبل في الموضع المختار

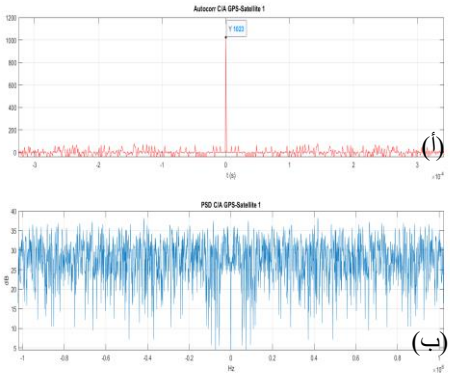
تعتمد آلية التشويش على المنظومة GPS باستخدام تقنية التشويش الواعي للبروتوكول Protocol-Aware Jamming على توليد إشارة مشابهة لإشارة المنظومة GPS الحقيقية. وقد استخدمنا برمجية ماتلاب MATLAB الإصدار R2019A في محاكاة توليد إشارة المنظومة GPS الصادرة عن ساتل واحد بوجود معطيات رسالة الملاحة؛ وذلك بغرض تحديد موقع مزيف لخداع المستقبل؛ مما يتطلب تعديل التوقيت في رسالة

الملاحة، ومعرفة السواتل الواقعة في مجال رؤية المستقبل في ذلك التوقيت. قمنا بالاعتماد على المعطيات المقدمة من موقع إدارة الطيران والفضاء الوطنية (ناسا) NASA الأمريكية، والتي تحتوي على التقويم الفلكي لسواتل المنظومة GPS، بحساب موقع السواتل فوق مدينة دمشق بتاريخ 10-4-2023 عند الساعة 17:00. ويظهر الشكل (10-أ) إمكانية الاستقبال بمستوى إشارة قوية نسبياً من أربع سواتل، في حين يظهر الشكل (10-ب) عند الساعة 19:00 مساءً توافر ستة سواتل.

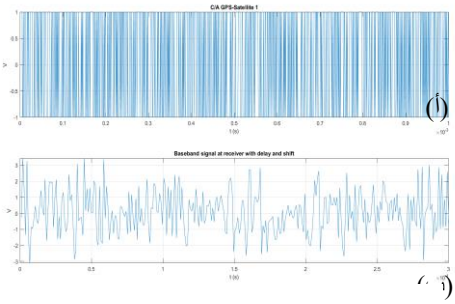
قمنا بتوليد الرِماز C/A للساتل رقم 1 وحساب الترابط الذاتي autocorrelation له، والترابط المتقاطع cross-correlation بين الرِماز C/A للساتل رقم 1 والساتل رقم 2. ويبيّن الشكل (11-أ) قيم الترابط الذاتي للرِماز C/A بقيمة عظمى 1023؛ أي إن جميع رموز الرِماز مترابطة ذاتياً على كامل طول السلسلة، في حين يبيّن الشكل (11-ب) الكثافة الطيفية لاستطاعة الرِماز C/A للساتل رقم 1.

يبيّن الشكل (12-أ) الرِماز C/A للساتل رقم 1، ويبيّن الشكل (12-ب) الإشارة عند المستقبل بالمجال الرئيسي مع إضافة التأخير الناتج عن الانتشار وانزياح دوبلر.

ويبيّن الشكل (13) الترابط المتقاطع بين الرِماز C/A للساتل رقم 1 ونظيره الساتل رقم 2.

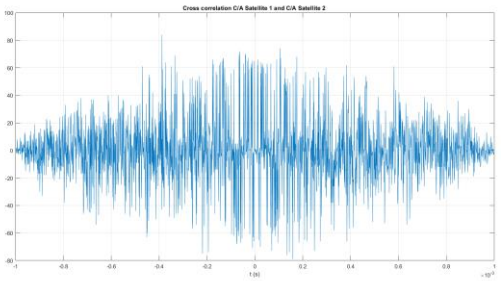


الشكل (11) (أ) الترابط الذاتي لرماز C/A، (ب) الكثافة



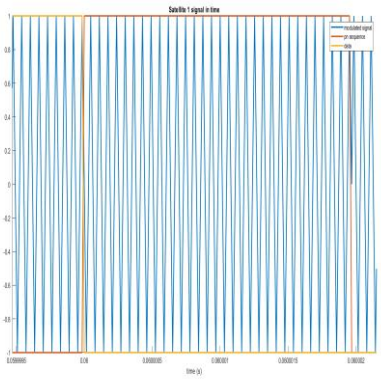
الشكل (12): الرِماز C/A للساتل رقم 1

قمنا بإجراء عملية الخيار المقصور XOR بين رسالة الملاحة وبين الرِماز C/A للساتل رقم 1 ليعطي سلسلة شبه ضجيجية PN Sequence، ثم تعديل هذه الإشارة تعديلاً رقمياً بإزاحة الطور الاثناني بوساطة إشارة التردد الحامل عند التردد 1575.42 ميغا هرتز. ويبيّن الشكل (14) كلاً من رسالة المعطيات والسلسلة شبه العشوائية والإشارة المعدَلة.

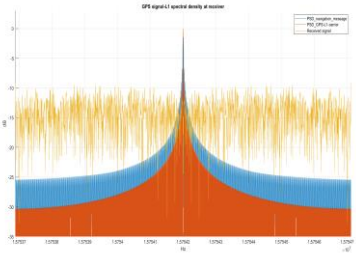


الشكل (13): الترابط المتقاطع بين الرِماز C/A

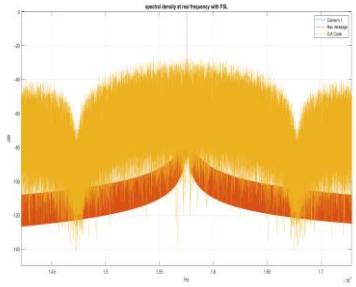
يبيّن الشكل (15-أ) الكثافة الطيفية لإشارة التشويش الواعي للبروتوكول، والتي تشبه إشارة الحامل L1 التي ترسلها المنظومة الشاملة لتحديد المواقع GPS، كما يبيّن الشكل (15-ب) الكثافة الطيفية للإشارة عند دخل المستقبل، مع الأخذ بالحسبان فقد مسار الفضاء الحر Free Space Path Loss (FSPL).



الشكل (14): إشارة الساتل رقم 1 قبل



(أ)



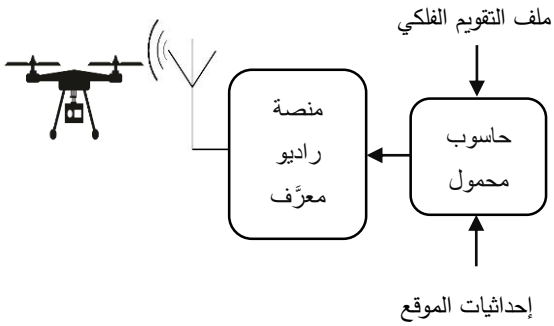
(ب)

الشكل (15) الكثافة الطيفية لاستطاعة الإشارة عند دخل المستقبل

4-2- التنفيذ العملي العتادي:

بالاعتماد على تقنية التشويش الواعي للبروتوكول، يتوجب بناء إشارة مشابهة للإشارة المرسلة من سواتل المنظومة GPS وتوليدها. قمنا بتوليد تلك الإشارات بالاعتماد على منصات

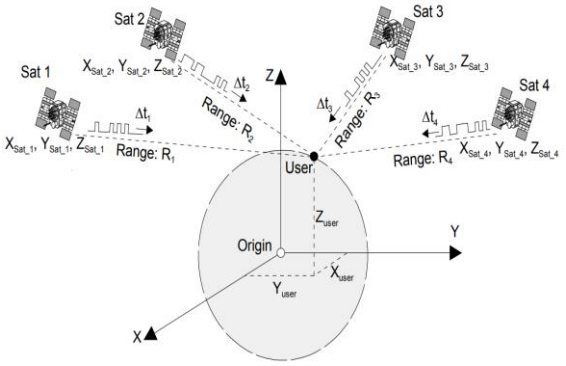
الراديو المعرَّف برمجياً من طراز BladeRF XA9 و Hakerf One، وبرمجيات مصممة باللغة C. يبيّن الشكل (16) المخطط العام للمشوش المقترح. وقد قمنا بتحميل ملف التقويم الفلكي من موقع ناسا؛ وهو يحوي جميع المعلومات الخاصة بسواتل المنظومة GPS، وقمنا بتضمين هذا الملف في برنامج قمنا بتصميمه خصيصاً باللغة C# يستعرض خرائط متعددة الطبقات. يمكن بوساطة هذا البرنامج تحديد الموقع المزيف المطلوب توليد رسائل الملاحة الخاصة به.



الشكل (16) المخطط العام للمشوش بالاعتماد على تقنية التشويش الواعي للبروتوكول

يتحدد عدد إشارات السواتل المرسلة وأرقام السواتل التي يجب توليد إشارتها بحسب الموقع المزيف الذي نرغب أن يتلقاه المستقبل، وهو يتعلق بالتقويم الفلكي للسواتل وهندسة السواتل التي تغطي الموقع المزيف بالتوقيت المحلي.

يبيّن الشكل (17) سواتل الملاحة وموقع المستخدم وفق الإحداثيات ثلاثية الأبعاد.



الشكل (17) سواتل الملاحة وموقع المستخدم وفق الإحداثيات ثلاثية الأبعاد

إن سواتل الملاحة متزامنة مع بعضها بدقة عالية بسبب استخدامها لساعات ذرية، لذا فإن التوقيت الذي يجري فيه إرسال إشارة الساتل معرّف بدقة كبيرة. يجري ضبط أو مزامنة جميع ساعات السواتل مع بعضها البعض وبالتوقيت العالمي المنسق Coordinated Universal Time (UTC). ترسل سواتل الملاحة اللحظة الزمنية التي يجري فيها الإرسال في رسالة الملاحة الخاصة بكل ساتل، ولا تجري مزامنة ساعة المستقبِل مع التوقيت العالمي المنسق (UTC)، ومن ثمَّ فهي أبطئ أو أسرع بمقدار Δt_0. تكون Δt_0 موجبة عندما تكون ساعة المستخدم أسرع. يسبب انحراف الوقت Δt_0 في خفض دقة قياس زمن انتشار الإشارة والمسافة R. نتيجة لذلك، يجري

قيـاس مسـافة غيـر صـحيحة تُعـرف باسـم المـدى الزائـف PSeudoRange (PSR)؛ وتجري الاستفادة من هذا المبدأ لجعل المستقبل يخطأ في حساب زمن الانتشار والمسافة R كما هو مبيّن في الشكل (17)، حيث قمنا بتعديل زمن الإرسال في رسالة الملاحة. ويُعطى المدى الزائف بالعلاقة (6).(Zogg, J-M, 2009)

$$PSR = \Delta t_{meas} \times c \qquad (6)$$

وفيها تمثل c سرعة الضوء في الخلاء وΔt_{meas} وقت القياس، والذي يعطى بالعلاقة (7) (Zogg, J-M, 2009).

$$\blacksquare(\sqrt{((X_sat(i) - X_Drone)\hat{}2 + (Y_sat(i) - Y_Drone)\hat{}2 + (Z_sat(i) - Z_Drone)\hat{}2} = (\Delta t - [\![\Delta t]\!]_meas) \times c \&\ \&(11))$$

$$\Delta t_{meas} = \Delta t + \Delta t_0 \qquad (7)$$

وفيها تمثل Δt وقت الإرسال، وΔt_0 الفرق بين ساعة المرسل وساعة المستقبل، وبتعويض العلاقة (7) في العلاقة (6) نحصل على العلاقة (8).

$$PSR = (\Delta t + \Delta t_0) \times C = R + \Delta t_0 \times C \qquad (8)$$

وفيها تمثل R المسافة الحقيقية بين الساتل والمستقبل؛ وبتعويض المسافة بالإحداثيات ثلاثية الأبعاد نحصل على

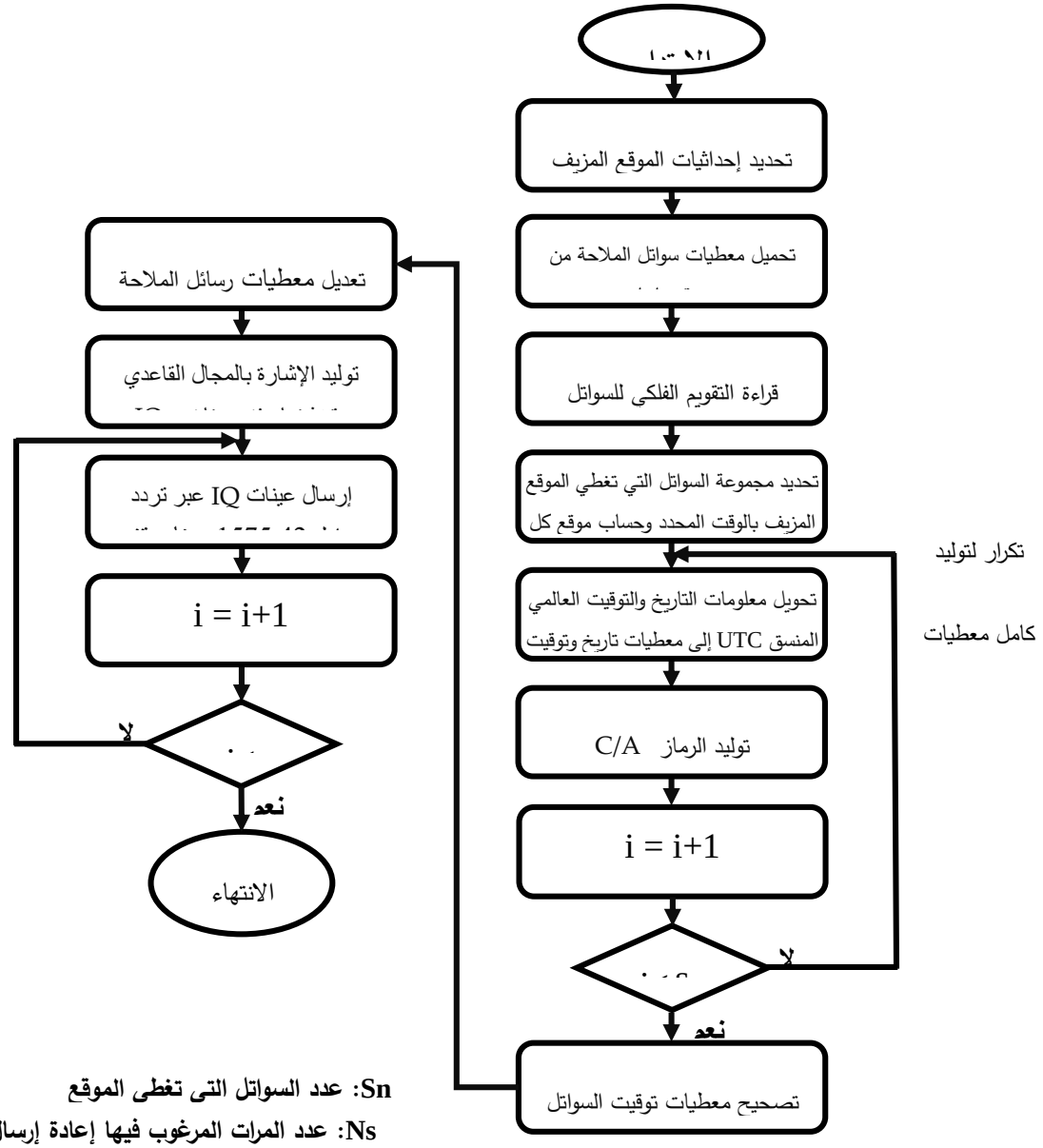
$$\blacksquare(PSR = \sqrt{((X_sat - X_Drone)\hat{}2 + (Y_sat - Y_Drone)\hat{}2 + (Z_sat - Z_Drone)\hat{}2} + [\![\Delta t]\!]_0 \times c \&\ \&(9))$$ الصيغة المكافئة المعطاة بالعلاقة (9) (Zogg, J-M, 2009)

وبافتراض أن كل من المستقبل والمرسل "المشوش" يعملان بنفس التوقيت المحلي، يمكن إهمال المدى الزائف وعدّه معدوماً، ومن ثمَّ الحصول على العلاقة (10).

وحيث أننا افترضنا في بحثنا أن زمن إرسال جميع السواتل موحد، لذا يمكن كتابة إحداثيات المستقبل بالعلاقة (11).

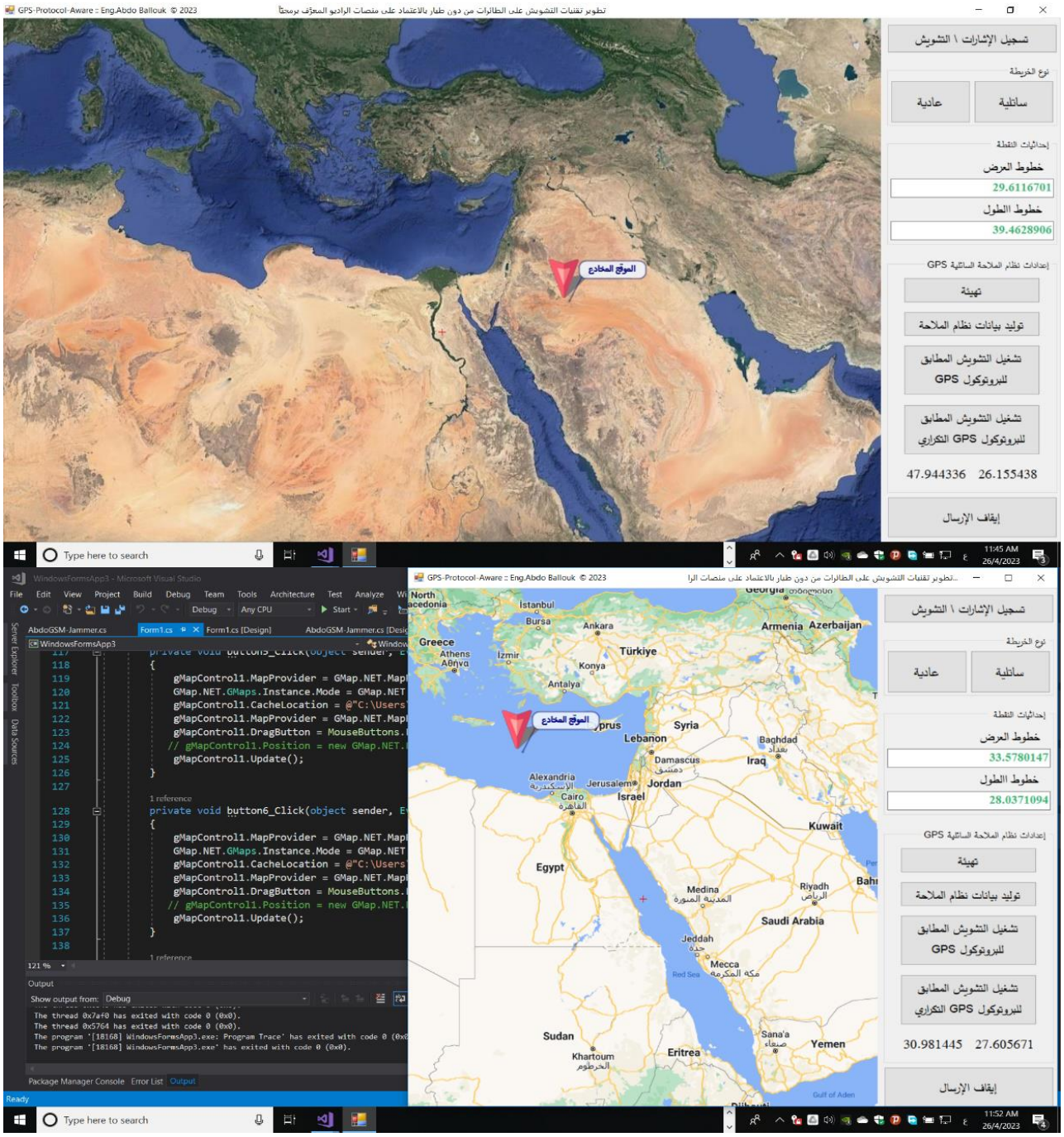
بناءً على ما سبق نحن بحاجة ليس فقط لتعديل زمن الإرسال Δt، بل وتحديد قائمة السواتل التي تغطي الموقع المزيف في اللحظة Δt أيضاً. يبيّن الشكل (18) المخطط التدفقي للخوارزمية المقترحة لتوليد إشارة التشويش الواعي للبروتوكول، التي تشبه الإشارة الحقيقية للمنظومة GPS.

$$\blacksquare(\sqrt{((X_sat - X_Drone)\hat{}2 + (Y_sat - Y_Drone)\hat{}2 + (Z_sat - Z_Drone)\hat{}2} = [\![\Delta t]\!]_0 \times c \&\ \&(10))$$



Sn: عدد السواتل التى تغطى الموقع
Ns: عدد المرات المرغوب فيها إعادة إرسال عينات

الشكل (18) المخطط التدفقي لخوارزمية توليد إشارة التشويش الواعي للبروتوكول



الشكل (19) برنامج توليد معطيات الملاحة والتحكم بمنصة الراديو المعرّف برمجياً

قمنا بتصميم برنامج يسمح بعرض خرائط متعددة المستويات

بالاعتماد على لغة C# والمبيّن في الشكل (19). يتيح هذا

البرنامج باختيار إحداثيات الموقع المزيف من على الخريطة، وتوليد معطيات منظومة الملاحة وفق الخوارزمية المعطاة بالشكل (18)، كما يقوم البرنامج بالتحكم بمنصة الراديو المعرّف برمجياً SDR بوساطة تهيئتها، وذلك بتحديد معدل معطيات الإرسال والتردد الحامل ومستوى استطاعة الإرسال والتحكم بتشغيل المرسل وإطفاؤه.

3-4 الأدوات المستخدمة في تنفيذ الاختبارات:

قمنا بتجهيز منصة اختبار لتقدير فعالية التشويش الواعي للبروتوكول على المنظومة GPS؛

وتضم هذه المنصة التجهيزات والأدوات والبرمجيات المبيّنة في الجدول (1).

الجدول (1) الأدوات المستخدمة في التنفيذ العملي للاختبارات على المنظومة المطورة

م	الأداة	الغرض
1	جهاز محلل طيف Rohde & Schwarz	لعرض طيف إشارة التشويش وكثافة استطاعتها
2	راسم إشارةTektronix	
3	كبل RF-SMA	
4	منصة راديو معرّف برمجياً Hackrf One SDR	لتوليد إشارة التشويش
5	طائرات من دون طيار من طراز: - DJI Phantom 3Pro - DJI Phantom 4Pro - DJI Mavic Pro - DJI Matrice 600 pro	إجراء اختبارات التشويش
6	حاسوب لوحي Ipad Air 2	لتشغيل بالطائرات من دون طيار والتحكم وعرض
7	هاتف محمول عدد 2 لديه إمكانية استقبال إشارات	إجراء اختبارات التشويش
8	هوائي غير موجه عدد 2	هوائي للإرسال وهوائي للاستقبال
9	تطبيق أندرويد GPS Test	عرض معلومات سواتل الملاحة والموقع ومستوى
10	تطبيق DJI GO	برنامج للتحكم بالطائرة من دون طيار طراز Phantom 3Pro وعرض معطياتها.
11	تطبيق DJI GO 4	برنامج للتحكم بالطائرة من دون طيار ذات الطراز ما فوق Phantom 3Pro
12	البرنامج المصمم GPS-Protocol Aware	لتوليد إشارة التشويش والتحكم بمنصة SDR

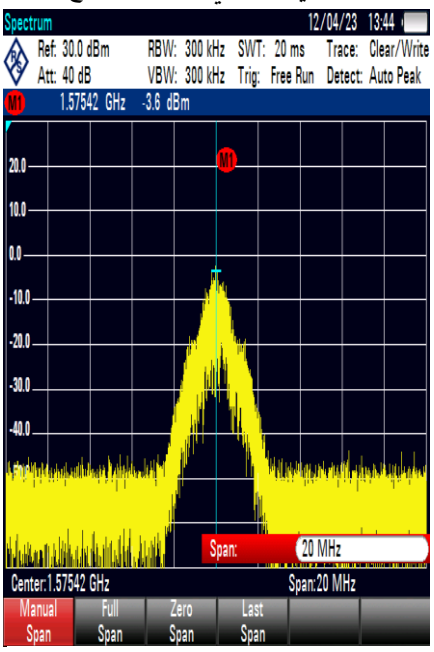
ويبـــيّن الشـــكل (20) منصـــة الاختبـــار المنفـــذة.

الشكل (20) منصة اختبار التشويش الواعي للبروتوكول

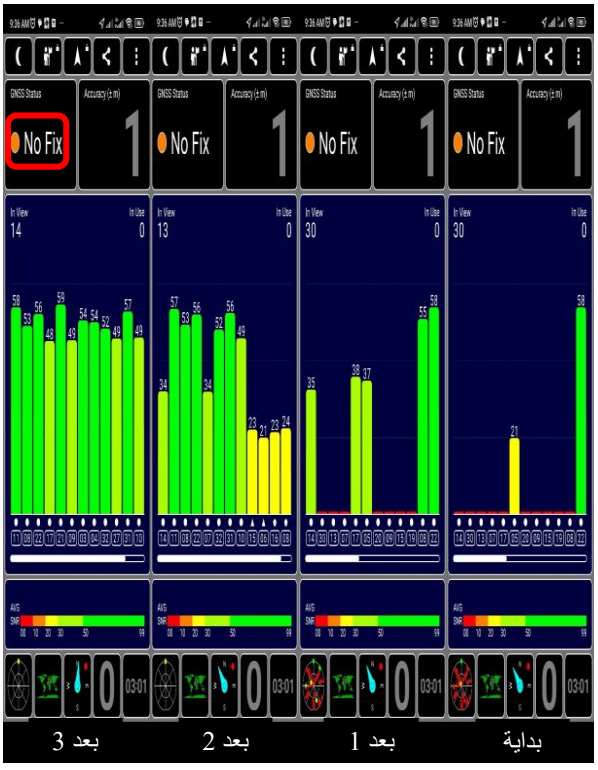
4-4 نتائج الاختبارات العملية وتحليلها:

قمنا بتوليد إشارة الملاحة بعد تحديد الموقع الزائف في منطقة فـــي صـــحراء الســـعودية عنـــد إحـــداثيات خطـــوط العـــرض 26.8524769 وخطـــوط الطـــول 41.3146484، وإرســـالها باستخدام هوائي غير موجه باستطاعة إرسال تساوي 3.5- ديسيبل ميلـي واط تقريبـاً. يبـيّن الشـكل (21) طيـف إشـارة التشويش الواعي لبروتوكول المنظومة الشاملة لتحديد المواقع GPS، والذي يتضمن رسالة ملاحة. قمنا بإجراء التجارب في مكان يسمح نوعاً ما باستقبال إشارات المنظومة GPS. عند إرسال إشارة التشويش بدأت تظهر إشارات السواتل المزيفة على تطبيق GPS Test ويزداد عددها واستطاعتها بشكل تدريجي كما هو مبيّن في الشكل (22). في البداية كان المستقبل قادراً على التقاط إشارة حوالي 29 ساتل من سواتل منظومات الملاحة الساتلية الشاملة GNSS من بينها غاليليو Galileo وغلوناس GLONASS و جي بي إس GPS. مع استقبال إشارات السواتل المزيفة بدأت إشارة سواتل المنظومات GNSS بالاختفاء تدريجياً لتختفي بالكامل بعد حوالي 4 ثانية من الإرسال، وذلك نظراً لأن استطاعات إشارات السواتل المزيفة أعلى من استطاعات الإشارات الحقيقة، وقد بلغ عدد السواتل الزائفة 14 ساتل، وراوحت نسبة استطاعة الإشارة إلى استطاعة الضجيج SNR بين 49 ديسيبل و 59 ديسيبل.

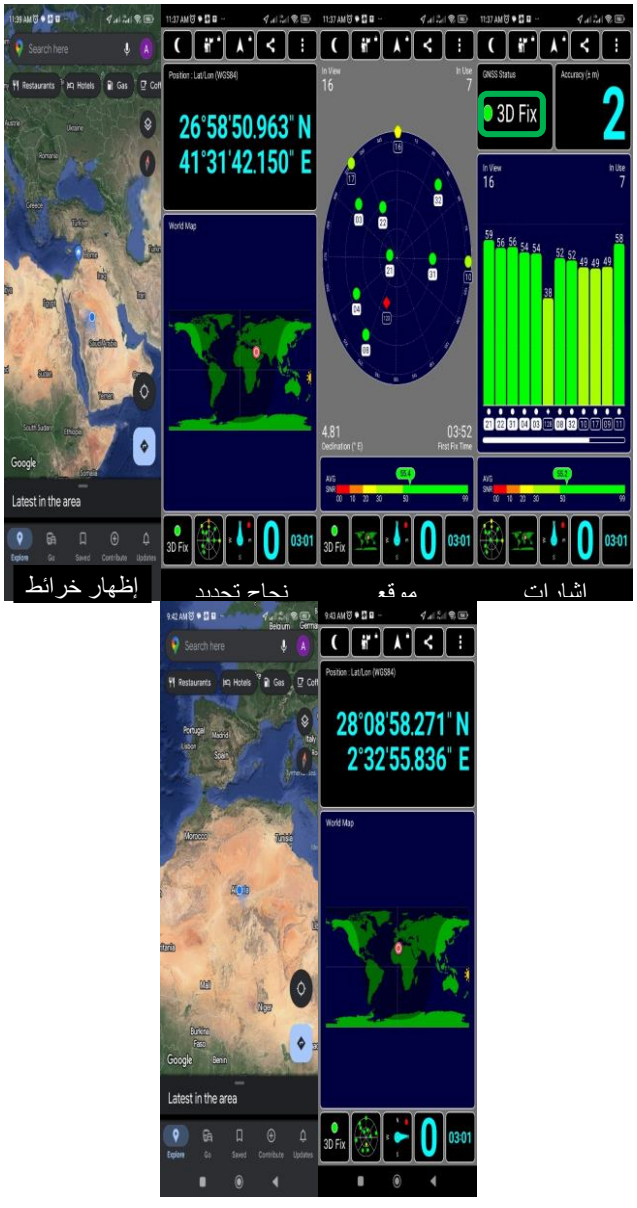
5- الاستنتاجات والتوصيات:



الشكل (21) طيف إشارة التشويش الواعي لبروتوكول المنظومة GPS



الشكل (22) إشارات السواتل المزيفة المستقبلة



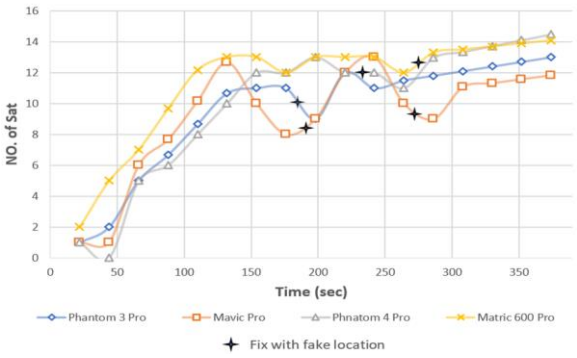
الشكل (23): إشارات السواتل المزيفة المستقبلة والموقع المزيف

في بداية الاختيار لم تتمكن مستقبلات المنظومة GPS الموجودة في الهواتف النقالة ولا حتى مستقبلات الملاحة على

متن الطائرات من دون طيار قراءة رسائل الملاحة للسواتل المزيفة، ولم تتمكن من إجراء حساباتها لتحديد الموقع، الشكل (22)؛ وذلك بسبب عدم تحقيق التزامن الأمثل بين إشارات السواتل والمستقبلات، نظراً لعدم دقة التردد الأساسي لمنصة HackRF one. وللتغلب على هذه المشكلة قمنا باستخدام منصة مساعدة من طراز Portapack H2 تحتوي على مهتز بلوريّ معوّض حرارياً (TCXO) Temperature Compensated Crystal Oscillator. وقد قمنا بربط هذه المنصة بالمنصة Hackrf one، وإعادة إرسال إشارة التشويش؛ فبدأت مستقبلات GPS الموجودة على متن الطائرات من دون طيار والهواتف النقالة باستقبال إشارات السواتل المزيفة، وبعد حوالي الدقيقة تمكنت المستقبلات من تحقيق التزامن مع السواتل المزيفة وقراءة رسائل الملاحة، لتقوم بحساب موقعها بناءً على المعلومات المستقبلة من السواتل المزيفة. قمنا بتكرار التجارب عدة مرات مع تغيّر الموقع المزيف، كما هو مبيّن في الشكل (23).

قمنا بإعادة التجارب على عدد من الطائرات من دون طيار من طراز Phantom 3 pro, Phantom 4 pro, Mavic pro, Matrice 600 pro، في حالة التقاط مستقبلات تحديد الموقع إشارات السواتل الحقيقة وقيامها بحساب الموقع الحقيقي؛ ثم عند تشغيل المشوش لم تظهر الطائرة استقبال سواتل جديدة، لأن المستقبل يقوم بإهمال معطيات الساتل الذي يقدم خطأ كبير في حساب الموقع، وينخفض مباشرة عدد السواتل الحقيقية المستقبلة بشكل تدريجي إلى الصفر، لأن نسبة استطاعة الإشارة إلى استطاعة الضجيج SNR للسواتل المزيفة أفضل من الإشارة الحقيقية إلى جانب الأخطاء الكبيرة بحساب الموقع الناتجة عن إشارة التشويش. بعدها يفقد المستقبل القدرة على التزامن مع مجموعة السواتل الحقيقية، ويبدأ المستقبل بالتزامن مع مجموعة السواتل المزيفة ليقوم بحساب الموقع الجديد وفق رسائل الملاحة للسواتل الزائفة. وتستغرق مستقبلات منظومة الملاحة للتزامن مع مجموعة السواتل المزيفة وحساب الموقع الزائف زمن أكثر من ثلاث دقائق يختلف تبعاً لنوع المستقبل ومستوى استطاعة إشارة التشويش كما هو مبيّن في الشكل (24). عند إطفاء التشويش لا يقوم المستقبل بالحساب وفقاً لإشارة السواتل الحقيقة مباشرة، بل يستغرق زمن بين الدقيقة والخمس دقائق حسب نوع المستقبل، حيث يقوم المستقبل بمسح سجلات معاملات الموقع القديم ليعيد حساب الموقع وفق المعاملات الحقيقية. عندما يكون المشوش بحال العمل

الاستباقي قبل تشغيل الطائرات من دون طيار تقوم مستقبلات منظومة الملاحة على متن الطائرات من دون طيار مباشرة باستقبال رسائل ملاحة السواتل المزيفة وقراءتها، ويستغرق حساب الموقع المزيف بضعة ثوان.



الشكل (24) عدد سواتل الملاحة المستقبلة من قبل الطائرات من دون طيار

6- الخاتمة والأعمال المستقبلية:

أثبت منظومة التشويش المقترحة القدرة على التشويش على استقبال إشارات السواتل الحقيقية للمنظومة الشاملة لتحديد المواقع GPS وبكفاءة عالية. كما أثبتت قدرتها على إيهام المستقبل بموقع زائف افتراضي يجري اختياره مسبقاً. وأظهرت التجارب الميدانية على عدد من الطائرات من دون طيار ضرورة أن يكون التشويش استباقي، قبل أن تتمكن مستقبلات الملاحة على متن الطائرات من طيار من المزامنة مع المنظومة GPS. في حين أن التشويش اللاحق يقوم بخداع المستقبل بشكل تدريجي ويحتاج زمن طويل نسبياً للتزامن مع مجموعة السواتل الزائفة. سوف نقوم لاحقاً بدراسة أثر زيادة مستوى استطاعة إشارة التشويش على سرعة استبعاد السواتل الحقيقية والمزامنة مع السواتل الزائفة، كما سوف نقوم بتحديد مسافة التشويش الفعالة وعلاقتها باستطاعة إشارة التشويش على عدد من الطائرات من دون طيار.

جدول المصطلحات والاختصارات:

الجدول (2) أهم المصطلحات والاختصارات العلمية

المصطلح الإنكليزي	الاختصار	المصطلح المعرّب
Barrage Jamming	BJ	التشويش السدّيّ
Electromagnetic Pulse	EMP	النبضة الكهرطيسية
Frequency Hopping Jamming	FHJ	التشويش بالقفز الترددي
Frequency-Hopping Spread Spectrum	FHSS	الطيف المنثور بالقفز الترددي
Global Navigation Satellite System	GNSS	المنظومة الشاملة للملاحة الساتلية
Global Positioning System	GPS	المنظومة الشاملة لتحديد المواقع
Quadrature Phase Shift Keying	QPSK	التعديل الرقمي التعامدي بإزاحة الطور
Software-Defined Radio	SDR	الراديو المعرّف برمجيّاً
Successive Pulses Jamming	SPJ	التشويش بالنبضات المتتالية
Sweep Jamming	SJ	التشويش المسحي
Tone Jamming	TJ	التشويش بالنغمات
Unmanned Aerial Vehicle	UAV	طائرة من دون طيار

التمويل: هذا البحث ممول من جامعة دمشق وفق رقم التمويل (501100020595).

References:

[1] Li, J., et al. (2023). Follower Jamming to UAV FH Communication System Based on Simulink. In 24th International Vacuum Electronics Conference (IVEC). IEEE Xplore, 1-2.

[2] Song, R., et al. (2023). Communication Jamming of High Power Microwave Pulse to UAV. In 24th International Vacuum Electronics Conference (IVEC). IEEE Xplore, 1-2.

[3] Zogg, J. M. (2009). GPS: Essentials of Satellite Navigation. U-Blox.

[4] Poisel, R. (2011). Modern Communications Jamming Principles and Techniques. Artech House.

[5] Haiwang, Z., & Jing, W. (2022). Design and Implementation of Anti-UAV System Based on Satellite Navigation Interference. IEEE 6th Information Technology and Mechatronics Engineering Conference (ITOEC), 1226 – 1230.

[6] Ferreira, R., et al. (2022). A Software Defined Radio Based Anti-UAV Mobile System with Jamming and Spoofing Capabilities. 22(4), 1487. 1-17.

[7] Norhashim, N., et al. (2022). The Effects of Jamming on Global Positioning System (GPS) Accuracy for Unmanned Aerial Vehicles (UAVs). International Conference on Computer and Drone Applications (IConDA). 18 – 22.

[8] Chiper, F.-L., et al. (2022). Aerial Drone Defense System based on Software Defined Radio Platforms. 14th International Conference on Communications (COMM). 1-4.

[9] Kaplan, E. D., & Hegarty, C. (2017). Understanding GPS/GNSS: Principles and Applications: Artech house.

[10] Wildemeersch, M., and Fortuny Guasch J., (2010). Radio Frequency Interference Impact Assessment on Global Navigation Satellite Systems. Publications Office of the European Union.

[11] Kim K et al. (2021). Variation in the Polarization Loss Factor in an Unmanned Aerial Vehicle Jamming Link Due to the Attitude Change. Applied Sciences, 11, 10725, 1-11.

[12] Pärlin, K. (2017). Jamming of Spread Spectrum Communications Used in UAV Remote Control Systems. Master Thesis. Tallinn University of Technology.

[13] Simon O. and Gotthans T. (2022). A Survey on the Use of Deep Learning Techniques for UAV Jamming and Deception. Electronics, 11(19), 1-32.

[14] Egido Egido, A. (2014). GNSS Reflectometry for Land Remote Sensing Applications. PhD Thesis. Polytechnic University of Catalonia.

[15] Sathyamoorthy D. et al. (2020). Evaluation of the Vulnerabilities of Unmanned Aerial Vehicles (UAVS) to Global Positioning (GPS) Jamming and Spoofing. Defence S and T Technical Bulletin, 13(2), 33

http://journal.damascusuniversity.edu.sy/index.php/index/index
ISSN (online): 2789-6854