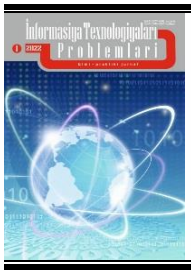


Available online at www.jpit.az

13 (1)
2022

Development of a method for detecting GPS spoofing attacks on unmanned aerial vehicles

Fargana J. Abdullayeva[a], Orkhan V. Valikhanli[b]

[a,b]Institute of Information Technology, Azerbaijan National Academy of Sciences, B. Vahabzade str., 9A, AZ1141 Baku, Azerbaijan

[a] a_farqana@mail.ru; [b] orkhanvalikhanli@gmail.com

ARTICLE INFO

http://doi.org/10.25045/jpit.v13.i1.01

Article history:
Received 15 September 2021
Received in revised form 23 November 2021
Accepted 21 January 2022

Key words:
UAV
GPS spoofing
CNN
Intrusion detection system

ABSTRACT

As in other vehicles, unmanned aerial vehicles (UAV) mainly use GPS (Global Positioning System) for the provision of navigation. Non-execution of necessary measures on UAV, availability of the devices used in the process of attack may cause GPS spoofing attack on UAV. The quick detection of the attack plays an important role in obtaining safety precautions. The use of artificial neural networks in the detection of such attacks is very convenient. Therefore, in the article new approach based on convolutional neural network (CNN) method is proposed in order to detect GPS spoofing attack. The new approach has been developed for two different types of UAVs. As a result of conducted experiments, high-accuracy detection of GPS spoofing attack has been provided.

Pilotsuz uçuş aparatlarına qarşı olan GPS spufinq hücumlarının aşkarlanması metodunun işlənməsi

Açar sözlər:
PUA
GPS spufinq
CNN
Müdaxilənin aşkarlanması sistemi

Pilotsuz uçuş aparatları (PUA) digər vasitələrdə olduğu kimi naviqasiyanın təmin olunması üçün əsasən GPS-dən (*Global Positioning System* – Qlobal Mövqetəyinetmə Sistemi) istifadə edir. PUA-larda zəruri tədbirlərin alınmaması, hücum prosesində istifadə edilən cihazların asanlıqla əlçatan olması PUA-ların GPS spufinq (*GPS spoofing*) hücumuna məruz qalmasına səbəb ola bilər. Hücumun tez bir zamanda aşkarlanması isə təhlükəsizlik tədbirlərinin alınmasında böyük rol oynayır. Bu cür hücumların aşkarlanmasında isə süni neyron şəbəkələrindən istifadə edilməsi olduqca əlverişlidir. Bunları nəzərə alaraq, məqalədə GPS spufinq hücumunun aşkarlanması üçün konvalyusiya neyron şəbəkə (*Convolutional Neural Network, CNN*) metoduna əsaslanan yeni yanaşma təklif edilmişdir. Yeni yanaşma iki fərqli tip pilotsuz uçuş aparatı üçün işlənib hazırlanmışdır. Aparılmış eksperimentlər nəticəsində GPS spufinq hücumunun yüksək dəqiqliklə aşkarlanması təmin olunmuşdur.

Разработка метода обнаружения GPS спуфинг атак на беспилотные летательные аппараты

Ключевые слова:
БПЛА
Спуфинг GPS
CNN
Система обнаружения вторжений

Беспилотные летательные аппараты (БПЛА) в основном используют GPS (Global Positioning System - Глобальная Позиционирующая Система) для навигации, как и другие транспортные средства. Несоблюдение необходимых мер предосторожности в отношении БПЛА и простота доступа к устройствам, используемым в процессе атаки, могут привести к подверганию БПЛА к GPS спуфинг атакам. Своевременное обнаружение атаки играет важную роль в соблюдении мер предосторожности. Использование искусственных нейронных сетей при обнаружении таких атак очень удобно. Следовательно, в статье предлагается новый подход, основанный на методе сверточной нейронной сети (*Convolutional Neural Network, CNN*) для обнаружения GPS спуфинг атак. Новый подход был разработан для двух разных типов БПЛА. В результате экспериментов было обеспечено высокоточное обнаружение GPS спуфинг атак.

1. Giriş

Pilotsuz uçuş aparatları (PUA) artıq həyatımızın ayrılmaz bir hissəsinə çevrilmişdir. Onların tətbiqini son zamanlar bir çox sahədə müşahidə etmək mümkündür. Xüsusilə süni intellektin PUA-lara tətbiqi onların artıq tam avtonom rejimdə işləməsini mümkün etmişdir. Bu isə insan əməyinin sayını azaltmaqla yanaşı görüləcək işin tez bir zamanda yerinə yetirilməsini təmin etməkdədir. Statistikaya əsasən yaxın 5-10 il ərzində PUA-ların bazar dəyəri milyardlarla dollar olacaqdır. Artıq PUA-lardan, nəinki yer kürəsində, hətta digər planetlərdə istifadə edilməyə başlanılmışdır. Buna cari ildə NASA (National Aeronautics and Space Administration) tərəfindən mars planetinə göndərilmiş "Ingenuity" adlı tək-fırlancaqlı PUA-nı misal göstərmək olar.

PUA-ların qısa zamanda geniş tətbiq edilməsi öz növbəsində bəzi problemləri də aktual edir. Bu problemlərdən ən vacibi onların kibertəhlükəsizliyidir. Təhlükəsizlik təkcə kommersiya və şəxsi tipli deyil, hətta hərbi PUA-larda belə ciddi bir problem kimi qalmaqdadır. Kiberhücumların vaxtında aşkarlanmaması ciddi fəsadlara gətirib çıxarır. Belə hallardan biri 5 dekabr 2011-ci ildə baş vermişdir. Belə ki, Amerikaya məxsus "Lockheed Martin RQ-170 Sentinel" adlı PUA İran İslam Respublikasının silahlı qüvvələri tərəfindən GPS spufinq hücumu edilərək ələ keçirilmişdir (Yağdereli et al., 2015). Daha sonra ələ keçirilən PUA-nın üzərində geriyə mühəndislik (*reverse engineering*) əməliyyatları aparılmış və ona oxşarı düzəldilərək istifadəyə verilmişdir.

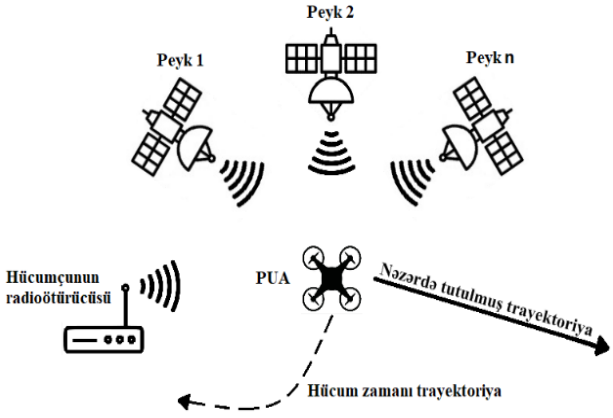
Ümumi nəzər yetirdikdə PUA-ları hədəf alan bir çox hücum növü mövcuddur. Bunlara zərərli proqram inyeksiyasını (*malware injection*), əngəlləməni (*jamming*), xidmətdən imtinanı (*Denial-of-service, DoS*), ortada adam hücumunu (*Man-in-the-middle attack*) və GPS spufinqi misal göstərmək olar. Lakin sadalanan kiberhücumlardan ən geniş yayılmışı GPS spufinq hücumudur. Baş vermiş insidentlərə nəzər salındıqda GPS spufinq hücumunun ilk sıralarda olduğu müşahidə olunmuşdur. Həmçinin GPS spufinq hücumu təkcə PUA-lara deyil, GPS qəbuledicisindən istifadə edən bütün cihaz və vasitələrə, o cümlədən gəmilərə, maşınlara və s. qarşı istifadə edilə bilər. Məhz bunları nəzərə alaraq məqalədə GPS spufinq hücumunun aşkarlanması məsələsinə baxılmışdır.

GPS spufinq hücumunun aşkar olunması üçün maşın və dərin təlimə əsaslanan bir çox metod təklif edilmişdir. Mövcud metodlarda əsasən, CNN, RNN (recurrent neural network), MLP (multilayer perceptron) və LSTM (Long short-term memory) istifadə edilmişdir. Təlim prosesində uçuş loq-fayllarından, müxtəlif siqnal parametrlərindən və spektroqramlardan istifadə edilmişdir. Mövcud metodların analizi haqqında daha ətraflı məlumat əlaqəli işlər bölməsində verilmişdir.

Təklif edilmiş metod digər maşın və dərin təlim metodları ilə müqayisədə daha yüksək aşkarlama dəqiqliyinə malikdir. Həmçinin digər fərqli yanaşmalar ilə (məsələn, siqnalın gəliş istiqaməti) müqayisədə hər hansı bir aparat təminatını tələb etmir. Aparata ehtiyac olmaması isə öz növbəsində PUA-nın enerjisinə, çəkisinə və s. qənaət olunması deməkdir.

2. GPS spufinq hücumları

GPS spufinq hücumu prosesində hücumçu GPS peyki tərəfindən ötürülənə bənzər lakin gücü daha yüksək və saxta olan siqnal göndərir (Borhani-Darian et al., 2020). Göndərilən saxta siqnallar PUA-nı yanıldaraq onun öz trayektoriyasından çıxıb qəsdən qəzaya uğradılmasına və ya qaçırılmasına səbəb ola bilər. GPS spufinq hücumu prosesi şəkil 1-də təsvir edilmişdir.



Şəkil 1. GPS spufinq hücumu prosesi

GPS spufinq hücumunun yerinə yetirilməsi üçün xüsusi cihazlardan istifadə olunur. Belə

cihazlar proqramla müəyyənləşdirilmiş radio (*software-defined radio*) adlanır. Proqramla müəyyənləşdirilmiş radiocihazlar, aparatda istifadə olunan komponentlərin əvəzinə bunun bir proqram vasitəsi ilə tətbiq olunduğu radiorabitə sistemidir. Bu növ cihazlara HackRF, BladeRF, USRP və s. misal göstərmək olar (Semanjski et al., 2020).

GPS spufinq hücumunun aşkar edilməsi təkcə maşın və dərin təlim metodları ilə məhdudlaşmır. Aşağıda digər aşkarlama metodları haqqında məlumat verilmişdir. Bu metodlara həm proqram, həm də aparat təminatı tələb edənlər daxildir.

- Maşın və dərin təlim metodları
- Siqnalın gəliş istiqamətinə əsaslanan metod
- Siqnal emalına əsaslanan metod
- Hibrid metod

Maşın və dərin təlimə əsaslanan metodlarda müxtəlif alqoritmlər tətbiq edilir. Bu alqoritmlər qəbul olunmuş GPS siqnalında və ya toplanmış digər məlumatlarda olan anomaliyaların aşkarlanması üçün istifadə olunur (Riahi Manesh et al., 2019). Siqnalın gəliş istiqamətinə əsaslanan metodda PUA-ya bir neçə antena bərkidilir və xüsusi hesablamalar aparılır (Riahi Manesh et al., 2019; Psiaki et al., 2016). Məqsəd isə GPS siqnalının gəliş istiqamətini müəyyən etməkdir. Çünki GPS spufinq hücumu zamanı çox vaxt saxta siqnallar bir mənbədən göndərilir. Normal siqnallar isə GPS peyki tərəfindən və fərqli istiqamətlərdən göndərilir. Siqnal emalına əsaslanan metod hücum zamanı yaranan pozulmanın analizinə əsaslanır (Psiaki et al., 2016). Belə ki, GPS spufinq hücumu zamanı saxta siqnal həqiqi siqnalla uyğunlaşdırılır. Bu zaman müəyyən vaxt intervalında ani dəyişikliklər baş verir. Bu dəyişikliklərin daim monitorinqinin aparılması hücumun aşkar olunmasını mümkün edir. Hibrid əsaslı metod dedikdə yuxarıda qeyd edilənlərin bir neçəsinin eyni anda tətbiqi başa düşülür (Riahi Manesh et al., 2019). Beləliklə, bir metod səmərəsiz olduqda digəri hücumun qarşısının alınmasında vacib rol oynaya bilər.

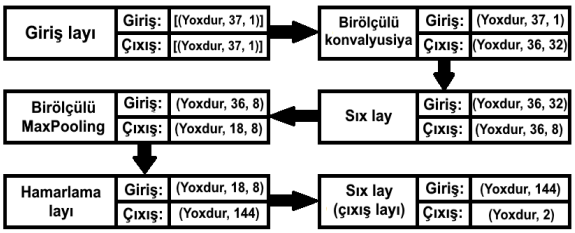
3. Əlaqəli işlər

(Borhani-Darian et al., 2020) məqaləsində GPS spufinq hücumunun aşkarlanması üçün dərin təlim metodlarından istifadə edilmişdir. Bu təlim metodlarından MLP, sadə CNN və VGG (Visual Geometry Group) 16-nın strukturuna bənzər olan kompleks CNN əsas götürülmüşdür. Sadə CNN-in strukturu 3 konvalyusiya layı və 3 tam birləşmiş əlaqəli lay vasitəsi ilə təyin edilmişdir. Kompleks CNN-in strukturu 13 konvalyusiya layı və 3 tam əlaqəli layla müəyyən edilmişdir. Hər üç metod üçün ReLU aktivləşmə funksiyasından istifadə edilmişdir. İstifadə olunan metodlarda optimizator kimi SGDM (Stochastic Gradient Descent with Momentum) və Adam (adaptive moment estimation) götürülmüşdür. Təlim zamanı süni şəkildə yaradılmış 10000 nümunədən istifadə olunmuşdur. Eksperimentlər nəticəsində kompleks CNN daha yaxşı nəticə göstərmişdir. Həmçinin hər bir metod üzrə Adam optimizatorunun dəqiqliyi daha yüksək olmuşdur. Ən zəif nəticə isə MLP-dən istifadə zamanı qeydə alınmışdır. (Manesh et al., 2019) məqaləsində neyron şəbəkəsindən istifadə edilmişdir. Tədqiqat zamanı beş əlamət götürülmüşdür. Bu əlamətlər arasında kombinasiya aparılmış və dəqiqlik hesablanmışdır. Bu əlamətlərdən üçü – siqnal-uğultu nisbəti, psevdo məsafəsi və dopler sürüşməsi əsas olaraq götürülmüşdür. Təlim zamanı 2000 nümunədən istifadə olunmuşdur. Neyron şəbəkə üçün bir və daha sonra iki gizli lay (*hidden layer*) müəyyən edilmişdir. Hər bir gizli lay üçün 1-25 diapazonunda neyron təyin edilmişdir. Burada iki gizli laydan ibarət olan neyron şəbəkə (hər birində 3 neyron olmaqla) daha yaxşı nəticə vermişdir. (Shafiee et al., 2017) məqaləsində MLP neyron şəbəkəsi ilə yanaşı KNN (k-nearest neighbors) və Naive Bayes təsnifat alqoritmləri də istifadə edilmişdir. MLP-dən istifadə daha yüksək nəticələr vermişdir. MLP-nin strukturu 3-2-1 kimi müəyyən edilmişdir. 3 giriş, 2 gizli, 1 isə çıxış layında olan neyronların sayı kimi təyin edilmişdir. Neyron şəbəkəsində siqnal səviyyəsi, delta və erkən-gec faza (radianlardakı normallaşmış faza) əsas əlamətlər kimi götürülmüşdür. (Xiao et al., 2019) məqaləsində sadə RNN, LSTM-RNN və GRU-RNN (gated recurrent unit-recurrent neural network) neyron şəbəkələri istifadə edilmişdir. Təlim zamanı dəqiqliyi təmin etmək üçün gəliş istiqaməti (*direction of arrival*) qiymətləndirmə alqoritmindən istifadə olunmuşdur. Ümumilikdə 30000 nümunə götürülmüşdür. 20000 nümunə təlim, 10000 nümunə isə test üçün istifadə

olunmuşdur. Layların sayı 3-4, neyronların sayı isə 16 və 32 olaraq təyin edilmişdir. Burada sadə RNN və LSTM-RNN daha yaxşı nəticə vermişdir. (Park et al., 2020) məqaləsində supervizorsuz (*unsupervised learning*) maşın təliminin bir növü olan avtoenkoderdən (*autoencoder*) istifadə olunmuşdur. Təlim zamanı yalnız zərərsiz uçuş məlumatlarından istifadə olunmuşdur. Metodun optimallaşma funksiyası Adam, aktivləşmə funksiyası ReLU-dur.

4. Təklif edilmiş metod

Məqalədə GPS spufinq hücumunun aşkarlanması üçün CNN-ə əsaslanan metod təklif edilmişdir. Təklif edilmiş metod uçuş zamanı PUA tərəfindən qeydə alınan loq-faylların analiz olunmasına əsaslanır. CNN süni neyron şəbəkəsinin bir növü olub müxtəlif sahələrə tətbiq edilmişdir. Verilənlər bazasında istifadə olunan siniflər (GPS spufinq hücumunun mövcud olduğu və olmadığı) məlum olduğundan metod öyrədilən maşın təliminə əsaslandırılmışdır. Metodda aktivləşmə funksiyası kimi ReLU və Sigmoid, optimizator kimi isə Adam istifadə edilmişdir. Təklif edilmiş metodun strukturu şəkil 2-də təsvir edilmişdir.



Şəkil 2. Təklif edilmiş metodun strukturu

Şəkil 2-dən göründüyü kimi metodun strukturu 1 giriş, 4 gizli və 1 çıxış layından ibarətdir. Hər bir layın girişi və çıxışı vardır. Neyronların sayı isə layın çıxışındakı formaların ölçüsü ilə təyin olunur. Məsələn, şəkildəki birölçülü konvalyusiya gizli layına nəzər yetirək. Layın çıxışındakı formalar 36*32 kimi müəyyən olunub. Bu isə laydakı neyronların sayının 1152 olması deməkdir. Digər laylardakı neyronları hesabladıqda və nəticələri topladıqda ümumi rəqəm 1728-ə bərabər olur. Qeyd etmək lazımdır ki, bəzi mənbələrdə giriş və çıxış laylarındakı neyronların sayı nəzərə alınır, bəzilərində isə alınmır. Burada qeyd edilən laylardakı neyronların sayı nəzərə alınmamışdır.

Təklif edilmiş metodun tətbiqi üçün iki hal mümkündür. Birincisi, PUA-nın uçuş zamanı qeydə aldığı loq-faylların sonradan analizidir. İkincisi isə metodun uçuş zamanı müdaxilənin aşkarlanması sistemində (*Intrusion Detection System, IDS*) istifadə edilməsidir. Müdaxilənin aşkarlanması sistemi zərərli davranışı aşkarlamaq üçün cihaz və ya proqram təminatıdır. Uçuş prosesində baş vermiş GPS spufinq hücumu zamanı müdaxilənin aşkarlanması sistemi dərhal bu haqda həyəcan siqnalı verəcəkdir.

5. Təklif olunmuş metodun eksperimental tədqiqi

Eksperimentlərin aparılması üçün "UAV attack dataset" adlı verilənlər bazalarından istifadə edilmişdir (Whelan et al., 2020). Verilənlər bazalarından biri kvadrokopter (*quadcopter*) tipli PUA-nın uçuş məlumatlarını özündə əks etdirir və 3247 sətir nümunədən ibarətdir. Digər seçilmiş verilənlər bazası isə quyruq üstündə dayanan (*tailsitter*) tipli PUA-nın uçuş məlumatlarını özündə əks etdirir və 1209 sətir nümunədən ibarətdir. Hər bir verilənlər bazası normal və GPS spufinq hücumunun olmasına görə iki sinfə bölünür. Hücumsuz normal uçuş "0", hücumun olduğu isə "1" ilə etiketlənmişdir. Verilənlər bazası etiketlə birlikdə 89 əlamətdən ibarətdir. Bu əlamətlərdən bəziləri dəyişməz və yararsız olduğundan təlim prosesində onlardan istifadə olunmamışdır. Beləliklə istifadə üçün yararlı 37 əlamət seçilmişdir. Alınacaq nəticənin daha yüksək olması üçün verilənlər bazası üzərində standartlaşdırma əməliyyatı aparılmışdır.

Təklif olunmuş metodun effektivliyini qiymətləndirmək üçün müxtəlif parametrlərdən istifadə olunmuşdur. Bu parametrlərdə qeyd edilən əmsallar belə izah olunur: Həqiqi pozitiv (*true positive, TP*) - düzgün proqnoz edilmiş müsbət nümunələrdir, həqiqi neqativ (*true negative, TN*) - düzgün proqnoz edilmiş mənfi nümunələrdir, yanlış pozitiv (*false positive, FP*) - səhv proqnoz edilmiş müsbət nümunələrdir, yanlış neqativ (*false negative, FN*) - səhv proqnoz edilmiş mənfi nümunələrdir. Qeyd edilən əmsallardan istifadə edərək dürüstlük (*precision*), tamlıq (*recall*), F-ölçü (*F-measure*) və dəqiqlik

(*accuracy*) parametrləri aşağıdakı kimi hesablanır.

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \quad (1)$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \quad (2)$$

$$\text{F} - \text{measure} = 2 * \frac{\text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}} \quad (3)$$

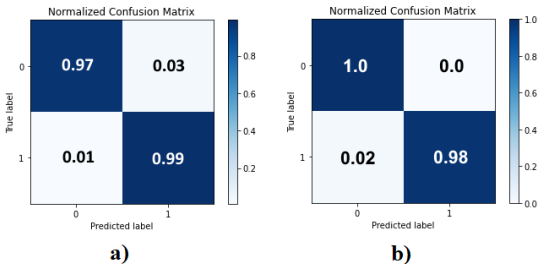
$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \quad (4)$$

Metodun eksperimental yoxlanması zamanı alınmış nəticələr Cədvəl 1-də təsvir edilmişdir. Dəqiqlik hər iki verilənlər bazası üzrə 0.99-dur. Bu isə GPS spufinq hücumunun aşkarlanması üçün olduqca yaxşı nəticədir.

Cədvəl 1. Təklif olunmuş metoddan alınmış nəticələr

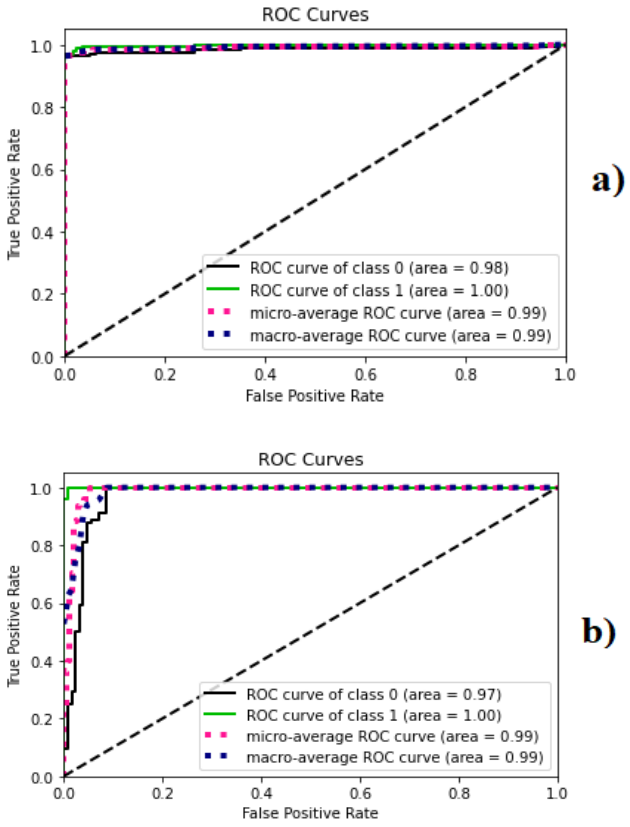
Verilən-lər bazası	Siniflər	Accuracy (Dəqiq-lik)	Precision (Dürüst-lük)	Recall (Tam-lıq)	F1-score (F-ölçü)
Kvadro-kopter tipli PUA	Normal (0)	0.99	0.99	0.97	0.98
	GPS spufinq (1)		0.97	0.99	0.98
Quyruq üstündə dayanan tipli PUA	Normal (0)	0.99	0.97	1	0.99
	GPS spufinq (1)		1	0.98	0.99

Eksperimentlər zamanı xətalar matrisindən də istifadə olunmuşdur. Xətalar matrisi təsnifat alqoritminin effektivliyinin xülasəsidir (Brownlee, 2016). Şəkil 3-də hər iki verilənlər bazası üçün alınmış xətalar matrisi təsvir olunmuşdur.



Şəkil 3. Xətalar matrisi (a-kvadrokopter PUA, b-quyruq üstündə dayanan PUA)

Digər bir qiymətləndirmə metodu isə qəbuledicinin fəaliyyət xarakteristikası (*receiver operating characteristic, ROC*) əyrisindən istifadədir. ROC – effektivliyinə görə təsnifatlandırıcıları vizuallaşdırmaq, qurmaq və seçmək üçün bir üsuldur (Fawcett, 2006). Şəkil 4-də hər iki verilənlər bazası üçün ROC qrafiki verilmişdir.



Şəkil 4. ROC əyrisi qrafikləri (a-kvadrokopter PUA, b-quyruq üstündə dayanan PUA)

6. Nəticə

Məqalədə PUA-ların uçuş loq-fayllarının analizi əsasında GPS spufinq hücumunun aşkar olunması üçün metod təklif edilmişdir. Təklif olunmuş metodda yüksək dəqiqliyin əldə edilməsinə baxmayaraq, bəzən aşkarlama üçün bu kifayət etməyə bilər. Bunun səbəbi daim yeni növ GPS spufinq hücumlarının meydana gəlməsidir. Bu problemi aradan qaldırmaq üçün maşın və dərin təlim metodları ilə yanaşı, digər yanaşmaların da tətbiqi məqsədəuyğundur. Bu yolla bir metodun uğursuz olması hallarında digərlərinin aşkarlamanı təmin etməsi mümkün olacaqdır.

Ədəbiyyat

Borhani-Darian, P., Li, H., Wu, P., & Closas, P. (2020). Deep Neural Network Approach to Detect GNSS Spoofing Attacks. Proceedings Of The 33Rd International Technical Meeting Of The Satellite Division Of The Institute Of Navigation (ION GNSS+ 2020), Manassas, Virginia, USA, September 2020, (pp. 3241-3252). https://doi.org/10.33012/2020.17537

Brownlee, J. (2016). What is a confusion matrix in machine learning. Machine Learning Mastery. https://machinelearningmastery.com/confusion-matrix-machine-learning

Fawcett, T. (2006). An introduction to ROC analysis. Pattern Recognition Letters, 27(8), 861-874. https://doi.org/10.1016/j.patrec.2005.10.010

Manesh, M., Kenney, J., Hu, W., Devabhaktuni, V., & Kaabouch, N. (2019). Detection of GPS Spoofing Attacks on Unmanned Aerial Systems. 16Th IEEE Annual Consumer Communications & Networking Conference (CCNC), Piscataway, New Jersey, USA, January 2019 (pp. 1-6). https://doi.org/10.1109/ccnc.2019.8651804

Park, K., Park, E., & Kim, H. (2020). Unsupervised Intrusion Detection System for Unmanned Aerial Vehicle with Less Labeling Effort. Information Security Applications, 45-58. https://doi.org/10.1007/978-3-030-65299-9_4

Psiaki, M., & Humphreys, T. (2016). GNSS Spoofing and Detection. Proceedings Of The IEEE, 104(6), 1258-1270. https://doi.org/10.1109/jproc.2016.2526658

Riahi Manesh, M., & Kaabouch, N. (2019). Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions. Computers & Security, 85, 386-401. https://doi.org/10.1016/j.cose.2019.05.003

Semanjski, S., Semanjski, I., De Wilde, W., & Muls, A. (2020). Use of Supervised Machine Learning for GNSS Signal Spoofing Detection with Validation on Real-World Meaconing and Spoofing Data—Part I. Sensors, 20(4), 1171. https://doi.org/10.3390/s20041171

Shafiee, E., Mosavi, M., & Moazedi, M. (2017). Detection of Spoofing Attack using Machine Learning based on Multi-Layer Neural Network in Single-Frequency GPS Receivers. Journal Of Navigation, 71(1), 169-188. https://doi.org/10.1017/s0373463317000558

Whelan, J., Sangarapillai, T., Minawi, O., Almehmadi, A., & El-Khatib, K. (2020). UAV Attack Dataset. IEEE Dataport. https://dx.doi.org/10.21227/00dg-0d12

Xiao, K., Zhao, J., He, Y., Li, C., & Cheng, W. (2019). Abnormal Behavior Detection Scheme of UAV Using Recurrent Neural Networks. IEEE Access, 7, 110293-110305. https://doi.org/10.1109/access.2019.2934188

Yağdereli, E., Gemci, C., & Aktaş, A. (2015). A study on cyber-security of autonomous and unmanned vehicles. The Journal Of Defense Modeling And Simulation: Applications, Methodology, Technology, 12(4), 369-381. https://doi.org/10.1177/1548512915575803

Fərqanə C. Abdullayeva[a], Orxan V. Vəlixanlı[b]

[a,b]Azərbaycan Milli elmlər Akademiyası, İnformasiya Texnologiyaları İnstitutu, B. Vahabzadə küç., 9A, AZ1141 Bakı, Azərbaycan

Фаргана Дж. Абдуллаева [a], Орхан В. Валиханлы [b]

[a,b] Институт Информационных Технологий НАН Азербайджана. Азербайджан, г. Баку, AZ1141, ул. Б.Вахабзаде, 9А.

[a] 0000-0003-2288-6255; [b] 0000-0001-6966-5084;