Informatics

PUA-LARIN KİBERTƏHLÜKƏSİZLİYİ HAQQINDA

İlahə Həsən qızı Qəhrəmanova
Azərbaycan Texniki Universiteti, Bakı, Azərbaycan

ABOUT UAV CYBER SECURITY

Ilaha Hasan Gahramanova
Azerbaijan Technical University, Baku, Azerbaijan: ilaha.qahramanova@aztu.edu.az
https://orcid.org/0009-0007-9761-1922

Abstract. Currently, unmanned aerial vehicles (UAVs) are widely used in civil and military fields. Due to this development, their security also becomes an important aspect. Problems related to the safety of UAVs also arise. Here, not only hacking, but also protection against radio-electronic interference devices are very serious problems. Based on a number of real security incidents, it can be argued that cyber security for UAVs and other unmanned vehicles is of exceptional importance. Various methods and main components neutralization are presented. Examples of real-life security incidents involving UAVs are presented in different years and in several sample countries. UAV system discusses certain methods for preventing and detecting cyber-attacks, anomalous behavior, identifying intrusion attempts and responding in real-time. Cryptography is invaluable in preventing some cyber attacks. Data encryption protects its privacy and prevents interception. This article examines the cybersecurity challenges of UAVs. The integration of artificial intelligence (AI) and machine learning (ML) into wireless network technologies can enable solutions to various security challenges. AI is being researched in a wide range of applications in automated systems and aviation.

Keywords: *drones, UAV, GPS, cyber attack, incident, Artificial İntelligence, Machine Learning.*

Giriş

Nikola Tesla 1898-ci ildə ilk pilotsuz, uzaqdan idarə olunan "tele-avtomobil"i nümayiş etdirmişdi. Bu sıçrayışdan sonra bir əsr ərzində pilotsuz sistemlər ilk növbədə ordu tərəfindən kəşfiyyat missiyaları üçün istifadə edildi. Texnologiyada irəliləyişlər daha sərfəli olduqca, pilotsuz uçuş aparatları (PUA) hərbi sahədən kənara çıxdı, mülki istifadələri genişləndi. Hazırda PUA-lar hərbi sahədən başqa, getdikcə daha çox müşahidə, tədqiqat və xəritəçəkmə, məkan məlumatlarının əldə edilməsi, geofiziki kəşfiyyat da daxil olmaqla geniş spektrli tətbiqlərdə istifadə olunur.

Lakin br çox halda PUA-ların təhlükəsizliyi ilə əlaqəli problemlər də meydana çıxır. Burada təkcə hakinq (hekləmələr) deyil, radioelektron maneə qurğularından müdafiə də çox ciddi problemlərdir. Bir sıra real təhlükəsizlik insidentlərindən çıxış edərək iddia etmək olar ki, PUA-lar və digər pilotsuz nəqliyyat vasitələri üçün kibertəhlükəsizlik müstəsna əhəmiyyətə malikdir [1].

PUA-nın əsas komponentləri

PUA-nın əsas komponentlərinə propellerlər, mühərriklər, çərçivə, sensorlar, sürət tənzimləyiciləri, uçuş kontrolleri, qəbuledici və batareya paketi daxildir. PUA ilə yanaşı, yerüstü stansiya və rabitə üçün lazım olan vasitəçilər də mühüm rol oynayır.

PUA operatordan əmrləri radio, Wi-Fi və Zigbee kimi müxtəlif texnologiyalar üzərində işləyən ötürücü və qəbuledici vasitəsilə qəbul edir. Radioötürücüdən siqnal qəbul etdikdən sonra radioqəbuledici onları PWM (Pulse Width Modulation) və ya PPM (Pulse Position Modulation) formatında elektrik siqnallarına çevirir. Bu siqnallar uçuş kontrolleri tərəfindən interpretasiya olunur, əmrlər PUA-nın idarə edilməsi üçün xüsusi hərəkətlərə çevrilir. Rotor əsaslı PUA-larda ESC (Electronic Speed Controller, elektron sürət nəzarətçisi) uçuş kontrollerindən siqnal və batareyadan enerji alır, uçuşa nəzarət etmək üçün mühərriklərin sürətini tənzimləyir. Sabit qanadlı PUA-larda qanadların bucağını dəqiq idarə etmək üçün servomühərriklərdən istifadə olunur, bu da öz növbəsində uçuşa nəzarət edir. Əmrlərdən başqa, telemetriya adlanan yerüstü stansiyasına batareya gərginliyinin oxunması və radio siqnalının gücü kimi mühüm məlumatları ötürən əlavə ötürücü-qəbuledici cütü də mövcuddur. Yerüstü stansiya PUA-ların insan idarəsini asanlaşdıran idarəetmə mərkəzidir [1].

Müxtəlif rejimlərdə işləyən PUA-lar naviqasiya üçün müxtəlif prinsiplərdən istifadə edirlər. Əllə idarə olunan PUA-lar, adətən, operatordan, qismən avtonom olan operatordan, GNSS (Global Navigation Satellite System) sistemindən və sensorlardan siqnal alır, tam avtonom olanlar isə operatorun müdaxiləsi olmadan uçuş qabiliyyətinə malikdirlər.

Uzaqdan idarəetmə üçün radio rabitə metodunda PUA-nın uçuş yolunu idarə etmək üçün radio ötürücü/qəbuledici, smartfon, planşet və ya kompüter istifadə edilir. Bu tip rabitədən istifadə edən PUA-lar yalnız operatorun baxış xəttində uça bilir və qısa məsafələr üçün nəzərdə tutulur

Peyk naviqasiyası PUA-ların GNSS sistemi ilə əlaqə saxlamasını əhatə edir. Ən çox yayılmış GNSS sistemi GPS-dir. GPS (Global Positioning System) naviqasiyası yer ətrafında sabit orbitlərdə fırlanan 30-dan çox peykdən istifadə etməklə təmin edilir. Hər bir peyk digərləri ilə sinxronlaşdırılan sabit atom saatına və yerə nisbətən vaxtı yeniləyən baza stansiyasına malikdir. Mövqeyi dəqiq bilmək üçün ən azı 4 peykdən siqnal qəbul etmək lazımdır [4].

Ultrasəs, LIDAR və kameralar kimi müxtəlif sensorlar ətrafdakı obyektlərdən məsafəni təyin etmək üçün istifadə olunur. PUA-nın uçuş hündürlüyünü izləmək üçün barometrlər də istifadə olunur. Bu sensorlar sabit uçuş təminatında uçuş kontrollerinə məlumat vermək üçün birlikdə istifadə olunurlar. Əsasən bu tip sensorlar SLAM (Simultaneous Localization and Mapping – sinxron lokallaşdırma və xəritəçəkmə) alqoritmləri və ya dərin öyrənmə yanaşmaları vasitəsilə lokalizasiyanı həyata keçirmək məqsədi daşıyırlar [2].

PUA-lara hücumların növləri

PUA-ların iş rejimlərindən (tam və qismən avtonom) asılı olaraq, müxtəlif zərərsizləşdirmə yanaşmaları tətbiq edilə bilər. Tam və ya qismən avtonom PUA üçün yer stansiyası ilə radio rabitəsi (RF) sabit paket strukturu ilə müxtəlif protokollar üzərindən baş verir. Paket arxitekturası ələ keçirilə, deşifrlənə bilər. Radio dalğa tıxacları, PUA-ya yönələn enerji miqdarı da rabitəni pozmaq üçün istifadə edilə və müxtəlif növ təhlükələr yarada bilər ki, bu da təhlükəsiz eniş etmək, əvvəlcədən təyin edilmiş baza yerinə qayıtmaq və ya təsadüfən uçmaq, qəza etmək kimi problemlərə səbəb olur [5]. Avtonom PUA-larda sensor qiymətləri saxtalaşdırıla, pozula, GNSS siqnalları saxtalaşdırıla bilər. Proqram təminatı da saxtalaşdırıla və ya troyanlarla müdaxilə edilir. Əlavə olaraq, bəzi digər hücum növləri də mövcuddur (yüksək güclü mikrodalğalar, yüksək enerjili lazerlər, raketlər və s).

PUA-ların neytrallaşdırılmasının müxtəlif üsulları məlumdur:

Küy müdaxiləsi: PUA yerüstü idarəetməsində radio rabitəsindən istifadə edilir. Küy müdaxiləsi genişzolaqlı modullaşdırılmış siqnalın kiçik bir hissəsinə və ya bütün spektrinə tətbiq olunduğu ən sadə müdaxilədir. Müdaxilənin bu forması sistemin kanal tutumuna birbaşa təsir edir və onu azaldır . Pilot və ya peyk sistemlərindən gələn siqnallar onlardan asılı olan mexaniki və avtonom PUA-ların işini pozmaq üçün küy müdaxiləsinə məruz qala bilirlər. Bununla belə, sensorlarla işləyən bəzi PUA-lar küy müdaxiləsinə qarşı qorunma vasitələri ilə təchiz edilmişdir.

GNSS müdaxilə: Demək olar ki, bütün PUA proqramlarında avtopilot funksiyası var, yəni, onlar öz iş rejimində qismən, ya da tam avtonomdurlar. Avtopilot funksiyaları PUA-nın oriyentasiya, yer və sürətlənmə kimi cari xassələrini qiymətləndirmək üçün çoxsaylı sensorlar və bort aparatları ilə təchiz edilmişdir. Bunlardan biri lokalizasiya üçün siqnalları təmin edən GPS kimi GNSS moduludur. GPS zəif siqnal gücünə görə ümumiyyətlə küy və kənar müdaxilələrə çox həssasdırlar.

Sensor saxtalşdırılması: PUA avto-pilot tətbiqi lokalizasiya və naviqasiya üçün LIDAR, SONAR və optik axın sensorları kimi bortda olan sensorlardan çox istifadə edilir. Bu sensorlar ətraf mühitlə qarşılıqlı əlaqədə olur və avtonom pilotsuz uçan aparat sistemini optimal şəkildə idarə etmək üçün avtomatik pilot kompüter üçün dəyərli məlumatlar təqdim edir. Sensor saxtakarlığı hücumunda təcavüzkar uçuş nəzarətçisinə faktiki dəyərlərdən fərqli olaraq saxta sensor ölçülər ötürür. Saxta ölçüləri düzəltmək üçün PUA sabitləşməyə yönəldiyindən və çox sensorları işə salmaq üçün məlumatlar paylaşdığından, bu, hətta sistem üzərində nəzarətin tamamilə itirilməsinə səbəb ola bilər.

Bu cür hücumların sayını azaltmaq üçün sistemə qəbul edilən vəziyyətlə faktiki vəziyyət arasındakı fərqləri aşkarlaya bilən nəzarət vasitələri tətbiq edilir. Məsələn, GPS və optik axın

sensorlarının məlumatları bu cür hücumları aşkar etmək və uyğunsuzluqları təyin etmək üçün digər sensor məlumatları ilə müqayisə üçün istifadə edilə bilər.

Siqnal saxtalaşdırılması: Qəbuledicini küy saxtalaşdırılmasından fərqli olaraq, orijinal qanuni siqnal olduğuna inandırmaq üçün kifayət qədər gücə malik ağlabatan saxta giriş siqnallarının yaradılmasını nəzərdə tutur. Saxta GNSS siqnalı həmin ərazidə PUA-nın başqa bir mövqedə yerləşdiyi kimi qəbul edilməsinə səbəb ola və PUA-nın virtual idarəsini saxtakara ötürə bilər.

Proqram təminatının saxtalaşdırılması: Məsələn, qlobal şəbəkədə yerləşdirilmiş kitabxanalarda, yaxud PUA kamerası üçün nəzərdə tutulan obyekt müəyyənləşdirmə proqramında zərərli kod yerləşdirilə bilər.

GPS saxtakarlığı hücumu. Son zamanlar daha çox GPS saxtakarlığı hücumuna məruz qalması hallarına rast gəlinir. GPS saxtakarlığı hücumu zamanı hücumçu saxta siqnallar ötürərək qəbuledicini yanıltmağa çalışır. Bu isə öz növbəsində PUA-ların qaçırılmasına və ya qəsdən qəzaya uğradılmasına səbəb ola bilər. Bu növ hücum yalnız PUA-lara qarşı deyil, həm də GPS qəbuledicisindən istifadə edən digər vasitələrə də tətbiq edilə bilər.

GPS saxtakarlığı zamanı zərərli GPS siqnalları qanuni GPS siqnallarından bir qədər yüksək güclə göndərilir ki, qəbuledici əsas siqnalları deyil, saxta siqnalları emal etsin. Zərərli siqnal kodları kompüterlərdə yaradıla, qlobal şəbəkələrdə yerləşdirilə və ya qanuni GPS siqnallarının sonradan yenilənən proqram təminatlarında qeydə alına bilər. GPS saxtakarlığı hücumları GPS üçün əsas təhdidlərdən biridir və daha çox zərərli təsirlərə malikdir, çünki qəbul edən PUA tutula, yanlış istiqamətə yönəldilə və yaxud digər hədəflər, obyektlərlə toqquşmağa yönəldilə bilər [3].

PUA-larla əlaqəli real təhlükəsizlik insidentləri

2009-cu ildə İran dəstəkli qruplar SkuGrabber adlı onlayn proqram təminatından istifadə edərək Predator pilotsuz təyyarəsinin canlı yayımını sındırmışdılar. Bu, onlara şifrlənmiş məlumatlara çıxış əldə etməyə imkan vermişdi.

2014-cü ildə Texas Universiteti (Ostin) radionaviqasiya laboratoriyasında PUA-nın uğurlu spufinqi həyata keçirilmişdi. Hazırda PUA-lar üçün spufinq texnologiyaları kifayət qədər inkişaf etmişdir. Anti-spufinqin yayılmış metodları heç də həmişə dayanıqlı və etibarlı deyil. Təkcə GPS-vericilər deyil, görmə sensorları və infraqırmızı şüalanma sensorları da spufinqə qalırlar. Nəticədə PUA-nın lazımi uçuş trayektoriyası dəyişdirilir.

2016-cı ildə Rusiyada keçirilən Praktiki Təhlükəsizlik üzrə Beynəlxalq Forumda PUA-ların qaçırılmasının mümkünlüyü nümayiş etdirilmişdi. Ələkeçirmə üçün Arduino Nano, PUA idarəetmə modulu BK2423, həmçinin HackRF və BladeRF kimi proqram təminatı ilə müəyyən edilmiş radio (SDR) cihazları istifadə edilib [6].

İcazəsiz girişin qarşısını almaq üçün yalnız hərbi GPS siqnalları şifrlənir, mülki GPS siqnalları isə açıq siqnallar kimi yayımlanır. Mülki GPS siqnallarının bu xüsusiyyəti hər kəsə GPS siqnallarına giriş imkanı verir ki, bu da olduqca populyar mülki GPS hücumlarına səbəb olur.

Snoopy bədniyyətli proqram təminatını [5] dronlarda quraşdırmaqla şəxsləri Wi-Fi olan smartfonlarını izləmək və onların fərdi məlumatlarını toplamaq olar. Snoopy vasitəsi ilə RFID (Radio Frequency IDentification), Bluetooth və 802.15 standartlı şəbəkələrini də izləmək olar.

Snoopy əvvəlcə qurbanın telefonu tərəfindən yayılan siqnalı seçir və bu cihaza artıq məlum olan və etibar edilən şəbəkəni müəyyən edir. Sonra Snoopy müəyyən edilmiş şəbəkəni təqlid edərək smartfonu ona qoşulmaq üçün aldadır. Bundan sonra Snoopy bu maskalanmış şəbəkədən bütün məlumatları, o cümlədən telefonu real vaxt rejimində izləmək üçün istifadə edilən smartfonun MAC ünvanını da toplaya bilər.

DJI Phantom 4 Pro və Parrot Bebop 2 dronlarının bir sıra hücumlara həssas olmaları [6]-da analiz edilmişdir. GPS-spufinq hücumu LabSat3 GPS simulyatoru vasitəsilə saxtakarlığın aşkarlanması üçün qurğu olmadan PUA-da həyata keçirilə bilər [6]. Açıq WiFi və de-avtorizasiya daxil olmaqla üç xüsusi Bebop 2 hücumu da var.

PUA sistemində kiberhücumların qarşısının alınması və aşkarlanması

Ümumilikdə PUA sistemində hücumların qarşısının alınması əks tədbirləri aşağıdakı üç üsulla işləyir:

• Sistemə ciddi giriş nəzarəti tətbiq edilməlidir ki, yalnız səlahiyyətli şəxslər və proqram agenti PUA ilə əlaqə yarada bilsin.

• Məlumatın məxfiliyi, bütövlüyü və həqiqiliyi elə qorunmalıdır ki, heç bir saxta və ya səhv məlumat, əmr qəbul edilməsin.

• Yalnız etibarlı mənbələrdən əldə edilmiş sistem proqram təminatı və proqram komponentlərindən istifadə olunsun.

Sensor hücumuna qarşı əks tədbir olaraq, müəyyən əməliyyat diapazonunda yalnız məqbul xarakteristikaya malik sensorlar PUA-da istifadə edilməlidir. Xüsusilə, tipik iş diapazonunda ətrafdakı akustik küydən təsirlənməyən uyğun bir giroskop seçilməlidir. Nəzərə almaq lazımdır ki, belə bir əks tədbir digər hücumlar üçün faydalı deyil.

Eyni sinif daxilində qruplaşdırılmış olmasına baxmayaraq, müxtəlif qarşısının alınması əks tədbirləri əhəmiyyətli dərəcədə fərqli həyata keçirir. Məlumatın silinməsinin və virus hücumlarının qarşısını almaq üçün giriş nəzarəti ümumi simsiz bağlantılar üzərindən bəzi şifrə əsaslı node identifikasiyası sxemləri vardır.

De-autentifikasiya hücumunda olduğu kimi simsiz əlaqə Wi-Fi olduqda, girişə nəzarət yalnız əvvəlcədən qeydiyyatdan keçmiş MAC ünvanları olan cihazların PUA ilə əlaqə yaratmasına icazə vermək şəklində həyata keçirilir və Wi-Fi giriş nöqtəsidir. Bu, etibarlı əks tədbirdir, çünki MAC ünvanı hər bir Wi-Fi interfeys kartına təyin edilmiş unikal aparat identifikatorudur. MAC ünvanını yoxlayaraq, PUA düşməni dəqiq şəkildə süzgəcdən keçirir və saxta de-autentifikasiya siqnalı təqdim etmək cəhdini rədd edir. MAC ünvan filtri ilə giriş nəzarətinə əlavə olaraq, PUA-nın giriş nöqtəsi identifikatorunu yayımlamaqla deyil, gizlətməklə de-autentifikasiya hücumlarının qarşısını almaq mümkündür. Həmçinin, defolt olaraq açıq mətnlə ötürülən autentifikasiya mesajları hücumdan əvvəl olan simsiz sniffing – in qarşısını almaq üçün şifrələnməlidir.

Kriptoqrafiya bəzi kiberhücumların qarşısının alınmasında əvəzsizdir. Məlumatın şifrələnməsi onun məxfiliyini qoruyur və ələ keçirilməsinin qarşısı alır. Asimmetrik kriptoqrafiya ilə müqayisədə simmetrik kriptoqrafiya daha az hesablama tələb edir və buna görə də bort resursları məhdud olan aşağı qiymətli PUA-lar üçün daha uyğundur. Simmetrik şifrələmənin həyata keçirilməsində problem gizli açar paylanmasıdır. Adətən radio idarəetmə kanalında mübadilənin həyata keçirilməsi üçün simmetrik açar paylama sxemi təklif edilir. Sxem o mənada unikaldır ki, ümumi mövcud radio modullarında həyata keçirilir və hər hansı hardware modifikasiyası tələb etmir [7].

PUA-nın hərəkətliliyindən istifadə etməklə onun trayektoriyasını optimallaşdırmaq və ötürməklə, yerdəki dinləyiciyə məxfilik dərəcəsini maksimuma çatdırmaqla məlumatı ötürmək mümkündür. Fiziki səviyyənin təhlükəsizlik texnikaları perspektivli olsa da, dinləyici yerüstü idarəetmə stansiyası və ya PUA ötürücüyə yaxın olduqda, rabitə üçün kifayət qədər yüksək məlumat məxfilik dərəcəsinə nail olmaqla bağlı problemlər hələ də aktualdır .

Man-in-the-middle hücumu şəklində görünən nəzarət siqnalının saxtalaşdırılmasının qarşısını almaq üçün şifrələmə mütləqdir. Başqa bir misal, naviqasiya siqnalının saxtalaşdırılmasında bütün yayım məlumatlarını şifrələməklə hücumun qarşısının alınması mümkündür. Şifrələmə üsulları adətən baha başa gəldiyindən yalnız nəzərdə tutulan qəbuledicilərin vacib bildiyi hərbi əməliyyatlar üçün edilir.

Siqnalın məxfiliyi pozulduqda, şifrələmə məlumatın bütövlüyünü yoxlamaq imkanı ilə məlumatın saxtalaşdırılmasının qarşısını almaq üçün ikinci müdafiə xətti təklif edə bilər. Kriptoqrafik şifrələmə məlumatın həqiqətən də qanuni göndəricidən ötürüldüyünü yoxlaya bilən mesajın autentikfikasiyası vasitəsilə mesaj inyeksiya hücumunun qarşısını almaqda faydalıdır. Mesajların şifrələnməsi ilə yanaşı, kriptoqrafiya həm də Blockchain texnologiyasının əsasını təşkil edir. Birtərəfli hash funksiyasından çox asılı olan Blockchain, PUA-ların təhlükəsiz rabitə ilə təmin edilməsi üçündür. Göndərən PUA əvvəlcə birdəfəlik simmetrik şifrələmə açarından istifadə edərək məlumatını

şifrələməli, şifrələnmiş paketi Blockchain qrupundakı bütün PUA-lara ötürməli və mesajın bütövlüyünü təsdiqləmək üçün qrupdan konsensus əldə etməlidir. Təsdiq konsensusa əsaslanır və sadə səs çoxluğu ilə həyata keçirilir. Yalnız belə bir təsdiqdən sonra göndərən PUA məlumatı başqa PUA və ya yerüstü idarəetmə stansiyası ola biləcək nəzərdə tutulan qəbulediciyə çatdıracaq. Məlumatın məxfiliyi simmetrik şifrələmə vasitəsilə əldə edilir [7].

Kor inyeksiya nəticəsində daxil olan məlumatların və ya xidmət sorğularının sayı birdən-birə yüksələ bilər. Kor inyeksiya paketlərin sayının statistik xarakteristikalarının və paket gecikməsinin yoxlanılması ilə aşkar edilir. Xüsusi hücum tipini hədəf almadan, müxtəlif maşın öyrətmə alqoritmlərindən istifadə edərək şəbəkə trafikində anomaliyaların aşkar edilməsi mümkündür. Alqoritm girişləri müxtəlif şəbəkə trafiki xüsusiyyətləridir, bunlara axın müddəti, paketlərin sayı, maksimum və minimum paket ölçüləri, orta və ümumi paket ölçüləri, paket ölçülərinin standart kənarlaşması və s. daxildir [7].

Nəzarət siqnalının saxtalaşdırılması PUA-nın qaçırıcının diktə etdiyi kimi gözlənilmədən hərəkət etməsinə səbəb ola bilər. Digər tərəfdən, naviqasiya siqnalının saxtalaşdırılması PUA-nın istiqamətini itirməsinə səbəb olur. Beləliklə, PUA-nın uçuş davranışları və statistikasında anomaliyaları tapmaqla həm nəzarət, həm də naviqasiya mesajı saxtakarlığını aşkar etmə mümkündür.

Məlumat yeridilməsi forması olaraq, video axınında ətraf mühitə uyğunsuzluq tapmaqla aşkar edilə bilər. Məsələn, PUA-nın günəş kölgəsi PUA-nın yerindən, günəşin mövqeyindən və cari vaxtdan asılıdır. Müəyyən bir vaxtda gözlənilən günəş kölgəsi və PUA-nın yeri müəyyən edilə bilər (analemmatik günəş saatı modeli vasitəsi ilə). Video görüntüdə kölgələr varsa, video təkrar hücumu təsbit edilir və videoda gözlənilən kölgəyə uyğun gəlmir. Bu tip video analitik yanaşma GPS naviqasiya siqnalının saxtalaşdırılmasını aşkar etmək üçün istifadə edilə bilər. Çünki, günəş kölgəsindəki uyğunsuzluq, eyni zamanda yerləşmənin uyğunsuzluğunu da bildirir. Xüsusilə, qəbul edilmiş videodakı günəş kölgəsi naviqasiya siqnallarından hesablanan PUA məkanında gözlənilən kölgəyə uyğun gəlmirsə, GPS saxtakarlığı aşkar edilir.

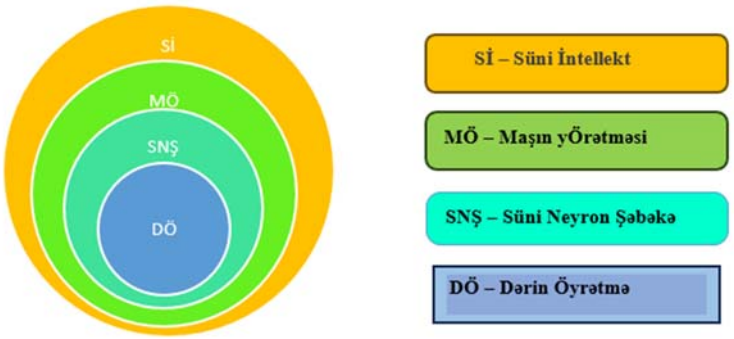
Günəş kölgəsindən başqa, GPS saxtakarlığının aşkarlanması üçün yer ardıcıllığı digər ətraf mühit xüsusiyyətlərindən istifadə etməklə də yoxlanılır. Daha dəqiq desək, PUA-nın ətraf mühiti, alınan naviqasiya mesajlarından istifadə etməklə əldə edilən yerə uyğun olmalıdır. Məsələn, GPS siqnalları PUA-nın dəniz üzərində uçduğunu müəyyən edərsə, PUA-dan çəkilmiş bir şəkil onun meşənin üstündə uçduğunu göstərməməlidir.

Kamera və ərazi hündürlük xəritəsindən istifadə etməklə GPS saxtakarlığını aşkar etmək üçün bir üsul da vardır. GPS siqnallarından əldə edilən PUA-nın mövqeyinə əsaslanaraq gözlənilən video görüntüsünü müəyyən edir və həmin görüntünü kamera tərəfindən çəkilmiş faktiki görüntü ilə müqayisə edir.

Yuxarıda təsvir edilən vizual əsaslı məkan ardıcıllığı metoduna əlavə olaraq, GPS-in radio siqnal xüsusiyyətlərindəki anomaliyaları yoxlamaq mümkündür. GPS saxtakarlığının aşkarlanmasına dair digər məlumat, anomaliyalar qeyri-adi güclü qəbul edilmiş siqnal gücü və həddindən artıq aşağı küy səviyyələri şəklində olur. Qeyri-normal dəyərlər GPS qəbuledicilərinin siqnallarının gəliş bucağında, siqnal fazasının gecikməsində və s. müşahidə olunur.

PUA təhlükəsizliyinin təmin edilməsi üçün Maşın Öyrətməsi

Simsiz şəbəkə texnologiyalarına süni intellekt (SI) və maşın öyrətməsi (ML)-nin inteqrasiyası müxtəlif təhlükəsizlik problemlərinin həlli şərait yarada bilər. SI adətən avtomatlaşdırılmış sistemlərdə istifadə olunur və aviasiyadan tutmuş səhiyyəyə qədər geniş tətbiq sahəsinə malikdir (şəkil). Konvolyusiya neyron şəbəkələri (CNN) təsnifata əsaslanan tapşırıqları yerinə yetirmək üçün birbaşa mətnlərdən, şəkillərdən, səslərdən və ya videolardan öyrəndiyi dərin öyrənmə (DL) üsullarından biridir. CNN üz tanıma və özü idarə olunan aparatlara tətbiq edililir. Nəticədə, müxtəlif sahələrdə, tətbiqlərdə və şəbəkə səviyyələrində SI/ML və PUA-nın birləşməsi səmərəli olur.



Süni intellekt və alt sahələri

PUA-ların avtonom işləməsi üçün MÖ getdikcə daha vacib olan SI yanaşmasına çevrilir. Qabaqcıl MÖ alqoritmlərinin istifadəsi (məsələn, dərin öyrətmə (DL) alqoritmləri) PUA sisteminə daha düzgün qərarlar qəbul etməyə yardımçı olur [8].

SI/MÖ texnologiyalarında son inkişaflar, mürəkkəb və dinamik sistemlərdə təhlükəsizliyi qorumaq və insan xətalarını azaltmaqla yanaşı, tam avtonom PUA əməliyyatlarının inkişafı sayəsində PUA əsaslı tətbiqlər üçün yeni imkanlar yaradıb. PUA-lara əsaslanan multimedia sistemləri üçün şəxsiyyətlərini dəyişdirərək PUA-ların ötürülməsini pozmaq, xüsusən də çoxlu sayda PUA olan şəbəkələrdə ciddi təsir göstərə bilər.

Tək PUA-larla müqayisədə koordinasiya edilmiş PUA-lar dəstəsi vacib missiyaları yerinə yetirir. Uçuş zamanı bir-biri ilə qarşılıqlı əlaqədə olan PUA-lar xüsusi tapşırıqları üzrə razılığa gəlir və buna görə də dəyişən şəraitə avtonom reaksiya verə bilirlər. PUA-lar qrupu arasında məlumat mübadiləsinin bu sxemi, adətən, təcavüzkarın dəstəyə daxil ola biləcəyi və onların paylaşılan məlumatlarını dəyişdirə biləcəyi, qeyri-ahəng hərəkətlər və toqquşmalarla nəticələnən rəqib hücumlarına qarşı həssasdır.

MÖ zənciri idarə etmək üçün blockchain daxilində real vaxtda qərar vermək üçün böyük məlumatlarla (BD) çalışmaq qabiliyyətinə malikdir. Bu səbəbdən, paylaşılan məlumatları təşviq edən blokçeynin qeyri-mərkəzləşdirilmiş təbiəti vasitəsilə təhlükəsizlik gücləndirilə və daha yaxşı modellər yarada bilər. PUA-ları avtonom şəkildə idarə etmək üçün MÖ daha düzgün qərarlar qəbul etməkdə əsas rol oynayır. Sürətli dronlarla əməkdaşlıq üçün, missiya zamanı toqquşmaya səbəb ola biləcək şəbəkə qırılmalarının qarşısını almaq üçün mərkəzsizləşdirmə tələb olunur. Şəbəkədə dəyişikliklərin proqnozlaşdırılması, daha təhlükəsiz əməliyyatları təmin etmək üçün optimallaşdırmadan istifadə olunur. İstənilən real dünya tətbiqində və naməlum mühitdə dronlarla əməkdaşlıq üçün tələb olunan tapşırıqları yerinə yetirmək çətin məsələdir.

Məsələn, bir PUA qrupdan hər hansı məqsəd üçün ayrıldıqda və ya nasaz vəziyyətə gəldikdə Blokçeyn bu dronu müəyyən etmək və digərləri arasında əlaqəni yüksək autentifikasiyada və təhlükəsiz saxlamaq üçün əsas texnologiyadır. Toplanmış məlumatlardakı küy böyük bir problemdir və qrup dronları ilə əlaqədə səhv qərarların qəbul edilməsinə səbəb ola bilər. Blockchain texnologiya şəbəkəsində qonşu dronların paylaşılan məlumatlarına əsaslanan dəqiq məlumatlarla küy arasındakı fərqi müəyyən etmək üçün təsnifat üsulları kimi MÖ texnikaları tələb olunur [8].

Nəticə

PUA-lar tezliklə gündəlik həyatımızda geniş istifadə ediləcək və bu prosesi sürətləndirmək üçün onlarla əlaqəli təhlükəsizlik problemlərinin həllinə yönəlmiş tədqiqatlara ehtiyac var. Bu məqalədə PUA-lara yönəlik hücumların müxtəlif növləri analiz edilir. PUA-larda real təhlükəsizlik insidentləri təqdim edilir. Simsiz şəbəkə texnologiyalarına süni intellekt (SI) və maşın öyrətməsi (MÖ)-nin inteqrasiyası müxtəlif təhlükəsizlik problemlərinin həlli şərait yarada bilər. PUA-ları avtonom şəkildə idarə etmək üçün MÖ daha düzgün qərarlar qəbul etməkdə əsas rolunun tədqiqatı aparılır. Sistemə ciddi giriş nəzarəti tətbiq edilməsinin vacibliyi, yalnız səlahiyyətli şəxslərin PUA ilə

əlaqə yarada bilməsinin təminatı yolları üzə çıxarılır. Məlumatın məxfiliyi, bütövlüyü və həqiqiliyinin qorunması, saxta və ya səhv məlumat, əmr qəbul edilmə faktının aradan qaldırılması müzakirə edilir. Yalnız etibarlı mənbələrdən əldə edilmiş sistem proqram təminatı və proqram komponentlərindən istifadə olunmasının vacibliyi vurğulanır.

ƏDƏBİYYAT

1. Liu Y., Dai H.N., Wang Q., Shukla M.K., Imran M. Unmanned aerial vehicle for internet of everything: Opportunities and challenges. Computer Communications, 2020, vol. 155, pp. 66-83.
2. Ly B., Ly R. Cybersecurity in unmanned aerial vehicles (UAVs). Journal of Cyber Security Technology, 2021, vol. 5, no. 2, pp. 120-137.
3. Chamola V., Kotesh P., Agarwal A., Gupta N., Guizani M. A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques. Ad hoc networks, 2021, vol. 111, Article 102324.
4. Kerns A.J., Shepard D.P., Bhatti J.A., Humphreys T.E. Unmanned aircraft capture and control via GPS spoofing. Journal of field robotics, 2014, vol. 31(4), pp. 617-636.
5. https://github.com/sensepost/Snoopy.
6. Shafique A., Mehmood A., Elhadef M. Survey of security protocols and vulnerabilities in unmanned aerial vehicles. IEEE Access, 2021, vol. 9, pp. 46927-46948.
7. Kong, Peng-Yong. "A survey of cyberattack countermeasures for unmanned aerial vehicles." *IEEE Access* 9 (2021): 148244-148263.
8. Kurunathan H., Huang H., Li K., Ni W. and Hossain E. 2023. Machine learning-aided operations and communications of unmanned aerial vehicles: A contemporary survey. *IEEE Communications Surveys & Tutorials*.

PUA-LARIN KİBERTƏHLÜKƏSİZLİYİ HAQQINDA

İ.H.Qəhrəmanova

Xülasə. Hazırda pilotsuz uçuş aparatları (PUA-lar) mülki və hərbi sahələrdə geniş tətbiq edilməyə başlayır. Bu inkişafla əlaqədar olaraq, onların təhlükəsizliyi də mühüm aspektə çevrilir. PUA-ların təhlükəsizliyi ilə əlaqəli problemlər də meydana çıxır. Burada təkcə hakinq deyil, radioelektron maneə qurğularından müdafiə də çox ciddi problemlərdir. Bir sıra real təhlükəsizlik insidentlərindən çıxış edərək iddia etmək olar ki, PUA-lar və digər pilotsuz nəqliyyat vasitələri üçün kibertəhlükəsizlik müstəsna əhəmiyyətə malikdir. PUA-ların neytrallaşdırılmasının müxtəlif üsulları, əsas komponentləri təqdim edilir. PUA-larla əlaqəli real təhlükəsizlik insidentləri nümunələri müxtəlif illərdə və bir neçə ölkə nümunəsində əks olunur. PUA sistemində kiberhücumların qarşısının alınması və aşkarlanması, anomal davranış, icazəsiz giriş cəhdlərini müəyyən etmək və real vaxt rejimində cavab vermək üçün müəyyən metodlar müzakirə edilir. Kriptoqrafiya bəzi kiberhücumların qarşısının alınmasında əvəzsizdir. Məlumatın şifrələnməsi onun məxfiliyini qoruyur və ələ keçirilməsinin qarşısı alınır. Bu məqalədə PUA-ların kibertəhlükəsizliyi ilə bağlı problemlər araşdırılır. Simsiz şəbəkə texnologiyalarına süni intellekt (SI) və maşın öyrətməsi (MÖ)-nin inteqrasiyası müxtəlif təhlükəsizlik problemlərinin həlli şərait yarada bilər. SI-in avtomatlaşdırılmış sistemlərdə və aviasiyada geniş tətbiq sahələrinin tədqiqatı aparılır.

Açar sözlər: *pilotsuz uçuş aparatları, PUA, GPS, kiberhücum, insident, Süni intellekt, Maşın Öyrətməsi.*

Accepted: 05.04.2024