PUA-larda KRİPTOQRAFİK PROTOKOLLAR SAHƏSİNDƏ MÖVCUD YANAŞMALARIN ANALİZİ

İlahə Həsən qızı Qəhrəmanova
Azərbaycan Texniki Universiteti, Bakı, Azərbaycan

ANALYSIS OF EXISTING APPROACHES IN THE FIELD OF CRYPTOGRAPHIC PROTOCOLS IN UAVs

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

Abstract. The rapidly increasing use of unmanned aerial vehicles has made the cybersecurity of their communication and control systems a critical issue. Since UAVs are widely used in military, industrial, logistics, and civilian fields, ensuring their secure communication channels is of strategic importance. There is a need to develop energy-efficient and computationally lightweight authentication protocols, as well as reliable cryptographic key exchange protocols, which are the basis of secure communication. Therefore, the scientific study of functional architecture and data exchange models plays a key role in ensuring the reliability, scalability, and cybersecurity of the system. This review article analyzes the role of existing authentication and encryption protocols, as well as lightweight cryptography, PUF-based authentication, and blockchain technologies in UAV security. Future research directions - post-quantum cryptography and security mechanisms integrated with artificial intelligence - are also discussed.

Keywords: *UAV, Elliptic Curve Cryptography, lightweight cryptographic protocols, post-quantum cryptography, blockchain technologies.*

Giriş. PUA -ların Ümumi Təhlükəsizlik Problemləri

Pilotsuz uçuş aparatları (PUA) və ya dronlar, əşyaların interneti (İoT) ekosisteminin ağıllı maşınları kimi çoxsaylı sahələrdə geniş tətbiq tapmışdır. Onlar ağıllı nəqliyyat sistemlərindən tutmuş, hərbi tətbiqlərə, təcili xilasetmədən ətraf mühitin monitorinqinə qədər çoxsaylı real vaxt xidmətləri göstərir [1]. Bu cihazların aşağı qiyməti və çevik əməliyyat qabiliyyəti onların populyarlığının əsas səbəbidir [8]. Lakin, məlumatların ictimai rabitə kanalları vasitəsilə mübadiləsi [10, 11, 12] və PUA -ların tez-tez təhlükəli və ya nəzarətsiz bölgələrdə yerləşdirilməsi [3, 18] onları bir sıra təhlükəsizlik hücumlarına qarşı müdafiəsiz edir (Cədvəl).

Təhlükəsizlik problemləri əsasən növbəti kateqoriyalara ayrılır: 1) **Şəbəkə əsaslı hücumlar:** PUA, PUA-lar arasında və ya PUA ilə yer stansiyası arasında ötürülən mesajlar təqlid, sessiya açarının açıqlanması, mesajın təkrarlanması, ortada adam (MitM) hücumları, izləmə və dinləmə hücumlarına məruz qalır [4, 13, 14]. 2) **Fiziki ələ keçirmə hücumları:** PUA-nın fiziki olaraq ələ keçirilməsi halında, onun yaddaşında saxlanılan məxfi təhlükəsizlik parametrləri oğurlana bilər. Bu da bütün sistem üçün məxfilik və təhlükəsizlik pozuntularına səbəb olur [3, 15, 16].

PUA sistemlərində təhlükəsizlik tələbləri

PUA sistemi real vaxtlı koordinasiya tələb edən çoxqatlı arxitektura üzərində qurulmuşdur. Bu sistemlərdə əsas təhlükəsizlik tələbləri aşağıdakılardır:

- **Autentifikasiya və identifikasiya** – PUA və yer stansiyası arasında qarşılıqlı tanınma.
- **Məxfilik və məlumatın gizliliyi** – uçuş koordinatları, sensor məlumatları, komanda paketlərinin şifrlənməsi.
- **Bütövlük** – məlumatın dəyişdirilməsinin qarşısının alınması.
- **Yüngülçəki hesablama** – məhdud enerji və prosessor gücünə uyğun kriptoqrafiya.
- **Fiziki təhlükəsizlik** – cihazın ələ keçirilməsi və reverse engineering hücumlarına davamlılıq

Bu tələblər müxtəlif protokolların əsas dizayn motivlərini formalaşdırır.

PUA təhlükəsizlik protokollarının mövcud yanaşmaları

ECC (Elliptic Curve Cryptography) PUA şəbəkələrində ən geniş istifadə olunan asimmetrik kriptoqrafiya mexanizmidir, çünki qısa açarla yüksək təhlükəsizlik təmin edir. [1]-də ECC və simmetrik açar əsaslı protokol təqdim olunur. ECC-nin seçimi, Rivest-Shamir-Adleman (RSA) alqoritmi kimi digər asimmetrik şifrələmə alqoritmləri ilə müqayisədə nisbətən daha qısa açar ölçüləri ilə müəyyən edilmişdir. [5]-də uğurlu identifikasiyadan sonra hər iki tərəf təhlükəsiz rabitə üçün gizli sessiya açarı yaradılmasına baxılır. PUA sistemindəki bu vacib problemi həll etmək üçün TCALAS adlanan yeni bir zaman etimadnaməsinə əsaslanan anonim yüngül istifadəçi identifikasiyası mexanizmi hazırlamışdır. Daha az vaxt və resurs sərfiyyatı ilə [6]-da təhlükəsizlik problemlərinin öhdəsindən gəlmək üçün [5]-də təklif edilmiş dron şəbəkələri üçün müvəqqəti etimadnaməyə əsaslanan anonim yüngül identifikasiya sxemi (TCALAS) izlənilə bilənliyə və oğurlanmış doğrulayıcı hücumlarına qarşı zəif olduğundan, həmçinin miqyaslana bilmədiyindən təkmilləşdirilmişdir. [6]-da yüngül simmetrik açar primitivlərindən və müvəqqəti etimadnamələrdən istifadə edərək təkmilləşdirilmiş sxem (iTCALAS) təklif olunur. Təklif olunan sxem yüngüllüyü qoruyub saxlayaraq izləmə və oğurlanmış doğrulayıcı da daxil olmaqla bir çox məlum hücumlara qarşı təhlükəsizlik təmin edir. iTCALAS miqyaslanmanı genişləndirir və IoD (dronların interneti) mühitində bir neçə uçuş zonası/klaster olduqda işləyə bilir. [4]-də IoD tətbiqlərindəki bu problemləri həll etmək üçün serverin köməyi ilə istifadəçi ilə giriş əldə edilmiş PUA arasında yeni bir autentifikasiya və açar razılaşma sxemi təqdim edilir. İstifadəçi ilə PUA arasında uğurlu qarşılıqlı autentifikasiyadan sonra qurulan sessiya açarı, onlara müxtəlif məlum hücumların düşmən tərəfindən qarşısının alınması üçün təhlükəsiz şəkildə əlaqə qurmağa kömək edir. [7]-də IoD mühitində etibarlı rabitəni təmin etmək üçün səmərəli Doğrulanmış Sessiya Açarının Qurulması (ASKE) yanaşmasını tələb edir. Məqalədə IoD üçün Məxfiliyi Qoruyan ASKE sxemi (PASKE-IoD) təqdim edilir. PASKE-IoD, ASKE mərhələsini yerinə yetirmək üçün Doğrulanmış Şifrələmə ibtidai "ASCON" və heş funksiyasından "ASCON-heş" istifadə edir.

[8]-də məlumatların mobil cihaz vasitəsilə toplana biləcəyi müəyyən nöqtələrə quraşdırılmış sensorları olan nəzarətsiz bir mühit nəzərdən keçirilir. Bu cihaz əslində PUA-dır. Əvvəlcə bunun üçün uyğun bir arxitektura, həmçinin yerini dəyişə bilən dron vasitəsilə cihazlar və bulud arasında təhlükəsiz rabitə qurmaq üçün yüngül bir protokol hazırlanmışdır. Protokol həmçinin mesajı rabitədə şifrələmək üçün istifadə edilən Fiziki Klonlanmayan Funksiyanın (PUF) üstünlüklərindən istifadə edir.

[9]-da İKT və İnternetin artan populyarlığı, PUA Nəqliyyat Vasitələrinin Ad-hoc Şəbəkəsinə (VANET) əlverişli kömək təklif etməsinə və yoldakı əlaqəsiz seqmentlər arasında ötürmə qovşağının rolunu həyata keçirməsinə imkan yaratmışdır. Bu ssenaridə, rabitə nəqliyyat vasitələri arasında PUA-larla (V2U) həyata keçirilir və sonradan PUA ilə dəstəklənən VANET-ə çevrilir. PUA ilə dəstəklənən VANET istifadəçilərə real vaxt məlumatlarına, xüsusən də mövcud mobil şəbəkələrdən istifadə edən ağıllı şəhərlərdə monitorinq məlumatlarına daxil olmağa imkan verir. Buna baxmayaraq, rabitə infrastrukturunun açıq təbiətinə görə, nəqliyyat vasitələrinin yüksək hərəkətliliyi, təhlükəsizlik və məxfilik məhdudiyyətləri PUA ilə dəstəklənən VANET-in əsas narahatlıqlarıdır. Bu ssenarilərdə Dərin Öyrənmə Alqoritmləri (DLA) PUA ilə dəstəklənən VANET-in təhlükəsizliyi, məxfiliyi və marşrutlaşdırma məsələlərində təsirli rol oynaya bilər. Bunu nəzərə alaraq, PUA ilə dəstəklənən VANET üçün DLA əsaslı açar mübadiləsi protokolu hazırlamışlar.

[10]-da müstəqil olaraq həssas məlumat toplayan PUA mühiti üçün S-IoD çərçivəsi təqdim olunur. Doğrulama protokolunun hesablama xərclərini azaltmaq üçün yüngül məxfiliyi qoruyan sxem (L-PPS) təqdim olunur. Təklif olunan L-PPS, etibarlı identifikasiya müddəti ilə IoT cihazları arasında möhkəmlik təmin etmək üçün konstruktivdir.

[11]-də PMAP adlı yüngül və məxfiliyi qoruyan qarşılıqlı identifikasiya və açar razılaşma protokolu təklif edilir. Sonuncu, qarşılıqlı identifikasiyanı dəstəkləmək və IoD sistemindəki rabitə qurumları arasında təhlükəsiz sessiya açarı yaratmaq üçün fiziki klonlanmayan funksiyadan və xaotik sistemdən istifadə edir. PMAP iki sxemdən ibarətdir: 1) PMAPD2Z (dron və zona xidmət təminatçısını qarşılıqlı olaraq təsdiqləyən və təhlükəsiz sessiya açarlarını yaradan) və 2) PMAPD2D (dronları qarşılıqlı olaraq təsdiqləyən və təhlükəsiz sessiya açarlarını yaradan).

[12]-də xüsusən də hərbi şəraitdə PUA rabitə protokolunun təhlükəsizlik şərtləri araşdırılmışdır. Daha da əhəmiyyətlisi, PUA-lar arasında və PUA ilə Yerüstü İdarəetmə Stansiyası (YİS) arasında rabitənin təhlükəsizliyini təmin edən təhlükəsizlik protokolu (iki alt protokolla) təklif olunur. Bu protokol, ümumi təhlükəsizlik tələblərindən əlavə, təhlükəsiz hərbi rabitə üçün vacib olan mükəmməl irəli məxfilik və rədd edilməmə prinsiplərinə nail olur.

[13]-də təklif olunan protokol, kriptoqrafik XOR, təhlükəsiz rabitə üçün heş funksiyası və unikal cihazdan asılı identifikasiya generasiyası üçün fiziki olaraq klonlanmayan funksiyadan (PUF) və fiziki hücumların qarşısını almaq üçün yüngül təhlükəsizlik həllindən istifadə edir. Bu müstəqil protokol əlavə rabitə və hesablama resursları tələb etmədən cihazdan cihaza və cihazdan serverə identifikasiyanı həyata keçirə bilər və bu da fərqli protokollara olan ehtiyacı aradan qaldırır.

[14]-də blokçeyn texnologiyasının tətbiqi və yüngül kriptoqrafik alqoritmlərin kombinasiyasının IoT şəbəkələrində təhlükəsizliyi artırmaq üçün istifadə edilə biləcəyini müəyyən etməyi hədəfləyir. IoT cihazı məhdud emal və enerji tutumuna malik olduğundan təhlükəsiz məlumatların ötürülməsində problem yaşamayacaq. Mövcud ədəbiyyat vasitəsilə məxfilik və identifikasiyanı təmin etmək üçün IoT tətbiqləri üçün uyğun simmetrik şifrələmə və heş funksiyaları da daxil olmaqla bir neçə yüngül şifrələmə üsulu müzakirə olunur. Bundan əlavə, məqalədə blokçeyndə ağıllı müqavilələrin tətbiqinin təhdidlərə vaxtında reaksiya verən və kiberhücumların qarşısını alan avtomatlaşdırma üçün təhlükəsizlik siyasətlərinin təmin edilməsinə necə imkan verdiyi nəzərdən keçirilir. Bu texnologiyalar birlikdə problemlərə qarşı güclü müdafiə mexanizmi təmin edir ki, bu da IoT-nu daha qorunmuş və istifadə üçün təhlükəsiz edir. Təklif olunan həllin miqyaslılığı, səmərəliliyi və mümkünlüyü də bu məqalədə təqdim edilmişdir və beləliklə, təqdim olunan həllin effektivliyi potensial real dünya IoT sistemləri kimi xidmət etmək üçün araşdırılmışdır.

[15]-də IoT arxitekturasının hər bir məntiqi təbəqəsi üçün mümkün bir həll təklif edilir. Bundan əlavə, şifrələmə mexanizmini, məxfiliyin mərkəzləşdirilməməsini, təhlükəsiz rabitəni, yüngül kriptoqrafik protokolu və bütün təhlükəsizlik təhdidlərinə qarşı həll yollarının nümayişi hazırlanmışdır.

Məqalələrdə istifadə edilən tədqiqat mövzuları və texnologiyalar

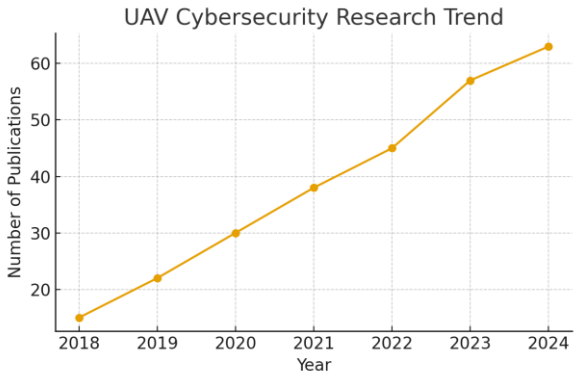
Mövzu / Texnologiya	**Təsvir**	**Əlaqədar İstinadlar**
Autentifikasiya və Ümumi Təhlükəsizlik	PUA-lar, yerüstü idarəetmə stansiyaları və digər IoT qurğuları arasında rabitənin geniş yayılmış kibertəhlükələrə qarşı qorunması.	[1-16]
Post-Kvant Kriptoqrafiya (PQC)	Həm klassik, həm də kvant kompüter hücumlarına qarşı davamlı olması üçün nəzərdə tutulmuş kriptoqrafik alqoritmlər.	[2, 4, 9]
Blokçeyn Texnologiyası	PUA şəbəkələrində təhlükəsizliyin və məlumat bütövlüyünün artırılması məqsədilə mərkəzləşdirilməmiş və saxtalaşdırılması çətin reyestrlərdən istifadə.	[3, 7, 10]
Aparat Səviyyəli Təhlükəsizlik (PUF-lar)	Yüngül və klonlanması çətin autentifikasiya mexanizmləri üçün fiziki klonlanmayan funksiyalardan istifadə.	[10]
Hibrid və Kvant Autentifikasiyası	Gələcəkdə davamlı təhlükəsizliyin təmin edilməsi üçün kvant davamlı mexanizmlərin (məsələn, QKD) klassik sistemlərlə inteqrasiyası.	[10]

[16]-da Kvant hesablamasının ortaya çıxması IoT-nə əsaslanan istehlakçı elektronikası cihazlarında köhnə kriptoqrafik protokolların təhlükəsizliyini ciddi şəkildə təhdid edir. Bunlar sənaye idarəetmə sistemləri, ağıllı şəbəkələr və səhiyyə kimi vacib infrastrukturların əsas komponentləridir. Xüsusilə, bu iş dərin öyrənmə metodlarını post-kvant kriptoqrafiyası (PQC) ilə birləşdirməklə IoT-nin klassik və kvant əsaslı kiberhücumlara qarşı müqavimətini necə gücləndirməyi araşdırır. IoT istehlakçı cihazlarında açar mübadiləsi, şifrələmə və identifikasiya proseslərini qorumaq üçün biz qəfəs əsaslı, heş əsaslı və kod əsaslı kriptoqrafiya da daxil olmaqla kvanta davamlı kriptoqrafik alqoritmlərdən istifadə etməyə davam ediləcəkdir. Real vaxt rejimində anomaliya aşkarlanması və cavablandırma imkanlarını təmin etmək üçün PQC-ni dərin öyrənməyə əsaslanan müdaxilə aşkarlama sistemləri ilə birləşdirən hibrid təhlükəsizlik çərçivəsi təklif edilir. Metodologiya gələcəkdə IoT

sistemləri daxilində kvant hücumları ilə əlaqəli təhlükəsiz rabitə və məlumat mübadiləsini təmin edir və Müdaxilə Aşkarlama Sistemi (IDS) modellərinin yeni hücum vektorlarına uyğunlaşmasına imkan vermək üçün zamanla davamlı öyrənmədən istifadə edir. PQC tətbiqinin çətin olacağı resursla məhdud olan IoT vəziyyətlərini nəzərə alaraq, kənar hesablama qovşaqlarında və Əşyaların İnterneti cihazlarında yerləşdirmək üçün yüngül və uyğun olan PQC həlləri üçün optimallaşdırılmış alqoritmlər təklif edilir.

Tədqiqat yeniliklərinin analizi

Son illərdə PUA sənaye, hökumət və akademiya tərəfindən əhəmiyyətli dərəcədə diqqət və populyarlıq qazanmışdır. Sürətli inkişafı və mülki hava məkanına yerləşdirilməsi ilə PUA-lar malların çatdırılması, axtarış-xilasetmə və nəqliyyatın monitorinqi daxil olmaqla müxtəlif tətbiqlərdə mühüm rol oynayır. Uğurlu və etibarlı uçuş missiyası üçün PUA-ların identifikasiya modelləri vasitəsilə təhlükəsiz rabitə təmin etmək vacibdir. Bu cür tələbləri ödəmək üçün ədəbiyyatlarda çoxsaylı identifikasiya mexanizmləri təklif edilmişdir. On altı fərqli məqalədən istifadə edərək PUA identifikasiyası işinin təhlükəsizliyi təhlil edilir. Təhlil göstəririk ki, PUA identifikasiyası sxemlərinin əksəriyyəti rabitə xərcləri baxımından yüngüldür. Lakin, saxlama xərci və ya enerji istehlakı bir çox identifikasiya tədqiqatları tərəfindən bildirilmir. Daha sonra, təhlükəsizlik təhlilində geniş istifadə olunan formal modelləri (yəni, riyazi model vasitəsilə identifikasiya protokolunun mücərrəd təsvirləri) aşkar edilir, halbuki tədqiqatların əksəriyyətində PUA sistemlərini hədəf ala biləcək bir çox hücumlar əhatə olunmur. Həmçinin, təhlükəsiz və etibarlı PUA identifikasiya sxemlərinin hazırlanması və tətbiqi üçün həll edilməli olan çətinliklər vurğulanır. Nəhayət, gələcək tədqiqatlar üçün perspektivli istiqamətləri motivasiya etmək üçün PUA-ların identifikasiya strategiyaları üzrə əldə edilən dərslər ümumiləşdilir.



2018-2024-cü illərdə PUA-ların kibertəhlükəsizliyi ilə əlaqəli nəşrlər

Şəkildən göründüyü kimi, son yeddi ildə PUA-ların kibertəhlükəsizliyinin tədqiqatına diqqət nəzərəçarpacaq dərəcədə yüksəlmişdir. 2018 və 2019 illər arasında artım on faiz təşkil etsə də, yeddi il ərzində inkişaf altmış faizə qədər yüksəlmişdir. Artım inkişafda olan sahəyə gələcəkdə daha çox tədqiqatçıların diqqətini yönəldəcəyini və mövcud boşluqların aradan qaldırılmasına ehtiyac olduğunu göstərir.

PUA sistemlərinin təhlükə modeli

PUA kommunikasiya kanalları bir neçə hücuma məruz qala bilər:

- **Replay attack** – köhnə kadrlardan istifadə edərək sistemin aldadılması
- **MITM (Man-in-the-Middle)** – PUA sisteminə aid olan elementlər arasında rabitə kanallarına qoşularaq məlumatın dəyişdirilməsi
- **GPS spoofing / jamming** – naviqasiyanın pozulması
- **Key extraction attacks** – kriptoqrafik açarlarının oğurlanması

- **Firmware injection** – zərərli proqram təminatının yüklənməsi

PUA -lar üçün təhlükə modelinin fərqi odur ki:

- **Kompрometasiya real fiziki insidentlərə gətirə bilər.**
- **Resurs məhdudluğu** (CPU, enerji) klassik kripto protokolları tətbiqini çətinləşdirir.
- **Hərəkətli node-lar** geriyə-qaytarılan gecikməyə həssasdır.

Kriptoqrafik müdafiə mexanizmləri

Tədqiqatçılar, qeyd olunan təhlükəsizlik problemlərini həll etmək və resursları məhdud olan dronlar üçün uyğun həllər təklif etmək məqsədilə müxtəlif yüngül təhlükəsizlik protokolları hazırlamışlar. Bu protokollar əsasən aşağıdakı texnologiyalara əsaslanır:

Simmetrik və Elliptik Əyrilər Əsaslı Şifrələmə

PUA rabitəsində ən çox tətbiq olunan üsullardan biri simmetrik açar və Elliptic Curve Cryptography (ECC) birləşməsidir. [1]-də təklif edilən protokol, simmetrik açarın ECC vasitəsilə təhlükəsiz mübadiləsini təmin etməklə hesablama yükünü azaldır və yüksək sürətli məlumat ötürməsini qoruyur. Bu yanaşma həm də uçuş zamanı real vaxt rejimində şifrələnmiş məlumat ötürülməsi üçün uyğundur [1, 10].

Yüngül Autentifikasiya və Açar Mübadiləsi Protokolları

[4]-də IoD mühitində uzaqdan istifadəçi autentifikasiyası və açar razılaşması üçün yüngül sxem təklif etmişdir. Bu protokol hesablama xərclərini minimuma endirir və qarşılıqlı autentifikasiyanı təmin edir. Eyni istiqamətdə müvəqqəti etimadnamələrə əsaslanan anonim autentifikasiya (TCALAS) sistemi ilə şəxsiyyətin məxfiliyini qorumağa nail olmuşlar [5]. [7]-də PASKE-IoD adlı protokolu isə həm məxfilik, həm də autentifikasiyanı birləşdirərək məlumat mübadiləsini daha etibarlı edir.

PUF Əsaslı Təhlükəsizlik

PUF texnologiyası son illərdə PUA təhlükəsizliyində effektiv yanaşma kimi formalaşır. PUF, yarımkeçirici cihazların fiziki xüsusiyyətlərindən istifadə edərək hər bir cihaz üçün unikal və klonlanması çətin olan "rəqəmsal barmaq izi" yaradır. [8]-də CoMSeC++ protokolunda PUF-lərdən istifadə etməklə unikal cihaz identifikasiyasını təmin etmiş və hücuma davamlı autentifikasiya sistemi təqdim etmişlər. Eyni prinsiplər PLAKE protokolunda da tətbiq olunaraq [13], açar mübadiləsinin saxtalaşdırılmasının qarşısını almışdır. [8, 10, 13]-də təklif olunan protokollar PUF-dan istifadə edərək, hətta fiziki ələ keçirmə halında belə, məxfi açarların sızdırılmasının qarşısını alır və möhkəm müdafiə təmin edir.

Blokçeyn və Paylanmış Etibar Mexanizmləri

Blokçeyn əsaslı yanaşmalar, xüsusilə təhlükəsiz məlumat ötürülməsi və şəffaf autentifikasiya üçün perspektivli sayılır. [15] göstərir ki, yüngül blokçeyn modelləri ilə kriptoqrafik əməliyyatlar arasında tarazlıq saxlanıla bilər. Bu yanaşma dronların idarəetməsində mərkəzsizləşmiş etibar sistemlərinin tətbiqinə imkan yaradır. [14, 15]-də qeyd olunduğu kimi, blokcheyn dron şəbəkələrində məlumatın bütövlüyünü qorumaq, təhlükəsiz açarların mübadiləsini asanlaşdırmaq və qərarların izlənilməsi üçün istifadə edilir.

Süni İntellekt və Dərin Öyrənmə Əsaslı Təhlükəsizlik

Yeni tədqiqatlarda dərin öyrənmə modelləri ilə post-kvant kriptoqrafiyasının birləşməsi dronların gələcək müdafiə sistemləri üçün ümidverici istiqamət sayılır [16]. Bu yanaşma real vaxtda hücum aşkarlanması və adaptiv cavab mexanizmlərinin inkişafına şərait yaradır.

Tədqiqat boşluqları və inkişaf istiqamətləri

Mövcud məsələlər müəyyən təhlükəsizlik problemlərini həll etsə də, texnologiyanın inkişafı ilə yeni təhdidlər ortaya çıxır. Bunlardan ən kritiki, kvant hesablamanın təhlükəsizlik üçün təhdidid ir. Güclü kvant kompüterləri hazırda İoD şəbəkələrinin təhlükəsizliyinin əsasını təşkil edən bir çox ənənəvi kriptoqrafik alqoritmi, o cümlədən ECC sındıra bilər . Bu, bütün müdafiə olunan məlumatların məxfiliyinin və bütövlüyünün təhlükə altına qoyulması potensialına malikdir.

Kvant-Sonrası Kriptoqrafiya (PQC): Kvant hücumlarına qarşı davamlı olan kriptoqrafik alqoritmlər üzərində işlər davam edir. [16]-da qeyd olunduğu kimi, PQC-nin İoT cihazları ilə inteqrasiyası, o cümlədən PUA -lar, onların təhlükəsizliyini gələcək təhdidlər qarşısında qorumaq üçün vacib bir addımdır. Bu, Dronların Kvant İnterneti (İoQD) kimi yeni anlayışların yaranmasına səbəb olur.

İoQD və Hibrid Autentifikasiya Modelləri: İoQD, kvant rabitəsi (məsələn, kvant açarı paylanması - QKD) kimi kvant texnologiyaları ilə təchiz edilmiş PUA şəbəkələrini ifadə edir. Əsas çətinlik, klassik PUA-larla kvant PUA-larının birgə işləyə biləcəyi hibrid autentifikasiya modellərinin yaradılmasıdır. Bu, iki fərqli texnologiyanı birləşdirən və təhlükəsiz şəkildə qarşılıqlı əlaqəni təmin edən yeni protokolların işlənib hazırlanmasını tələb edir.

Enerji optimizasiyası baxımından PUA-ların çoxunun batareya ehtiyatı məhduddur. Bu səbəblə kriptoqrafik əməliyyatların enerji optimizasiyası hələ də açıq qalan problemdir. 6G və massiv IoT ilə inteqrasiya gələcək PUA-lar 6G şəbəkələri ilə birlikdə işləyəcək və aşağı gecikməli çoxsaylı bağlantılar tələb edəcək. Həmçinin, süni intellekt əsaslı hücumlardan müdafiə PUA-ların kiberfiziki təbiəti onların Maşın Öyrənməsi-əsaslı hücumlardan qorunmasını tələb edir

Nəticə

PUA-lar üçün təhlükəsizlik protokolları sürətlə inkişaf edən tədqiqat sahəsidir. İoD geniş imkanlar təqdim etsə də, ictimai rabitə kanalları və fiziki hücumlar kimi mürəkkəb təhlükəsizlik problemləri ilə üzləşir. Hazırkı yanaşmalar müəyyən səviyyədə təhlükəsizlik təmin etsə də, formal doğrulama, enerji optimizasiyası və post-kvant kriptoqrafiyanın tətbiqi hələ də araşdırma tələb edir. Bu icmal müasir protokolları sistemli şəkildə müqayisə edir və gələcək tədqiqat istiqamətlərini müəyyən edir. Tədqiqatçılar, ECC, PUF və blokcheyn kimi yüngül kriptoqrafiya və autentifikasiya protokolları ilə bu problemlərə qismən həll tapmışlar. Lakin, kvant hesablamanın yüksəlişi, mövcud kriptoqrafik sistemlər üçün yeni təhdid yaradır. Buna görə də, gələcək tədqiqatlar PQC tətbiqinə, klassik və kvant dron şəbəkələri arasında təhlükəsiz əlaqəni təmin edəcək hibrid autentifikasiya modellərinin işlənib hazırlanmasına yönəldilməlidir. Bu yanaşma, İoD sistemlərinin uzunmüddətli təhlükəsizliyini və davamlılığını təmin edəcəkdir.

ƏDƏBİYYAT

1. Nyangaresi V.O., Jasim H.M., Mutlaq K.A.-A., Abduljabbar Z.A., Ma J., Abduljaleel I.Q., Honi D. G. A Symmetric Key and Elliptic Curve Cryptography-Based Protocol for Message Encryption in Unmanned Aerial Vehicles. *Electronics*, 2023, 12(17), 3688.
2. Yahuza M., Idris M.Y.I., Wahab A.W.A., Nandy T., Ahmedy I.B., Ramli R. An Edge Assisted Secure Lightweight Authentication Technique for Safe Communication on the Internet of Drones Network. In *IEEE Access*, vol. 9, pp. 31420-31440, 2021.
3. Tian C., Ma J., Li T., Zhang J., Ma C., Xi N. Provably and Physically Secure UAV-Assisted Authentication Protocol for IoT Devices in Unattended Settings. In IEEE Transactions on Information Forensics and Security, vol. 19, pp. 4448-4463, 2024.
4. Wazid M., Das A.K., Kumar N., Vasilakos A.V., Rodrigues J.J.P.C. Design and Analysis of Secure Lightweight Remote User Authentication and Key Agreement Scheme in Internet of Drones Deployment. In IEEE Internet of Things Journal, vol. 6, no. 2, pp. 3572-3584, April 2019, doi: 10.1109/JIOT.2018.2888821.
5. Srinivas J., Das A.K., Kumar N., Rodrigues J.J.P.C. TCALAS: Temporal Credential-Based Anonymous Lightweight Authentication Scheme for Internet of Drones Environment. In *IEEE Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 6903-6916, July 2019.
6. Ali Z., Chaudhry S.A., Ramzan M.S., Al-Turjman F. Securing Smart City Surveillance: A Lightweight Authentication Mechanism for Unmanned Vehicles. In *IEEE Access*, vol. 8, pp. 43711-43724, 2020.
7. Tanveer M., Khan A.U., Shah H., Chaudhry S.A., Naushad A. PASKE-IoD: Privacy-Protecting Authenticated Key Establishment for Internet of Drones. In IEEE Access, vol. 9, pp. 145683-145698, 2021.
8. Mall, Priyanka, et al. "CoMSeC++: PUF-based secured light-weight mutual authentication protocol for Drone-enabled WSN." *Computer Networks* 199 (2021).
9. Akram M.W. et al. A Secure and Lightweight Drones-Access Protocol for Smart City Surveillance. In IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 10, pp. 19634-19643, Oct. 2022.
10. Deebak, Bakkiam David, Fadi Al-Turjman. A smart lightweight privacy preservation scheme for IoT-based UAV communication systems. *Computer Communications* 162 (2020): 102-117.

11. Pu C., Wall A., Choo K.-K.R., I.Ahmed, Lim S. A Lightweight and Privacy-Preserving Mutual Authentication and Key Agreement Protocol for Internet of Drones Environment. In IEEE Internet of Things Journal, vol. 9, no. 12, pp. 9918-9933, 15 June15, 2022.
12. Ko, Yongho et al. Drone secure communication protocol for future sensitive applications in military zone. *Sensors* 21.6 (2021): 2057.
13. Roy S., Das D., Mondal A., Mahalat M.H., Sen B., Sikdar B. PLAKE: PUF-Based Secure Lightweight Authentication and Key Exchange Protocol for IoT. In IEEE Internet of Things Journal, vol. 10, no. 10, pp. 8547-8559, 15 May15, 2023.
14. Naveen V., Narang S., Ramesh P.S., Ponmalar A., Sudha I. Secure Data Transmission in IoT Networks Using Blockchain and Lightweight Cryptography: Safeguarding the Connected Future. 2025 3rd International Conference on Communication, Security, and Artificial Intelligence (ICCSAI), Greater Noida, India, 2025.
15. Chowdhury N.J.K., Alam K.M.R., Islam M.M. Security and Privacy in IoT using Blockchain and Lightweight Cryptographic Protocol. 2022 IEEE 7th International conference for Convergence in Technology (I2CT), Mumbai, India, 2022.
16. Sharma A., Rani S. Post-Quantum Cryptography (PQC) for IoT-Consumer Electronics Devices Integrated With Deep Learning. In IEEE Transactions on Consumer Electronics, vol. 71, no. 2, pp. 4925-4933, May 2025.

PUA-larda KRİPTOQRAFİK PROTOKOLLAR SAHƏSİNDƏ MÖVCUD YANAŞMALARIN ANALİZİ

İ.H.Qəhrəmanova

Xülasə. Pilotsuz uçuş aparatlarının sürətlə artan istifadəsi onların rabitə və idarəetmə sistemlərinin kibertəhlükəsizliyini kritik məsələyə çevirmişdir. PUA-lar hərbi, sənaye, logistika, və mülki sahələrdə geniş tətbiq olunduğuna görə, onların təhlükəsiz rabitə kanallarının təmin edilməsi strateji əhəmiyyət daşıyır. Enerji-effektiv və hesablama baxımından yüngül autentifikasiya protokolu, həmçinin təhlükəsiz rabitənin təməli olan etibarlı kriptoqrafik açar mübadiləsi protokollarının işlənib hazırlanmasına tələbat vardır. Buna görə də funksional arxitektura və məlumat mübadiləsi modellərinin elmi əsaslarla öyrənilməsi sistemin etibarlılığı, miqyaslana bilməsi və kibertəhlükəsizliyinin təminatında əsas rol oynayır. Bu icmal məqalədə mövcud autentifikasiya və şifrələmə protokolları, eləcə də yüngül kriptoqrafiya, PUF əsaslı autentifikasiya və blokçeyn texnologiyalarının PUA təhlükəsizliyində rolu təhlil olunur. Həmçinin gələcək tədqiqat istiqamətləri – post-kvant kriptoqrafiyası və süni intellektlə inteqrasiya olunmuş təhlükəsizlik mexanizmləri müzakirə edilir.

Açar sözlər: *PUA, Elliptic Curve Cryptography, yüngül kriptoqrafik protokollar, post-kvant kriptoqrafiyası, blokçeyn texnologiyaları.*

Accepted: 18.12.2025