

**DRONLAR TARMOG'IDA KIBERHUJUMLARNI ANIQLASH HAMDA
XAVFSIZLIK ARXITEKTURASINI TAKOMILLASHTIRISH**

Rivojiddinov Doniyor Baxtiyor o'g'li

Toshkent Kimyo xalqaro universiteti Namangan filiali, assistenti

Dolzarbligi: Uchuvchisiz uchish apparatlari (dronlar) tarmog'i fuqaro va harbiy sohalarda tobora keng ko'lamda qo'llanilmoqda. Biroq, dronlar tarmog'ida ma'lumotlar ochiq simsiz aloqa kanallari orqali uzatilishi hamda tugunlar (dronlar)ning apparat resurslari (protessor, xotira, energiya) cheklanganligi kiberhujumlarga nisbatan zaiflikni yuzaga keltirmoqda. An'anaviy xavfsizlik mexanizmlari dron tarmoqlarining dinamik strukturasi va cheklangan resurslariga mos kelmaydi. Shu sababli, dronlar tarmog'ida kiberhujumlarni o'z vaqtida aniqlash va unga moslashuvchan xavfsizlik arxitekturasini modelini takomillashtirish o'ta dolzarb ilmiy-amaliy vazifalardan biridir.

Tadqiqotning maqsadi: Dronlar tarmog'iga uyushtiriladigan kiberhujumlarni aniqlash samaradorligini oshirish va resurs tejovchi, ko'p bosqichli xavfsizlik arxitekturasini takomillashtirishdan iborat.

Tadqiqot vazifalari:

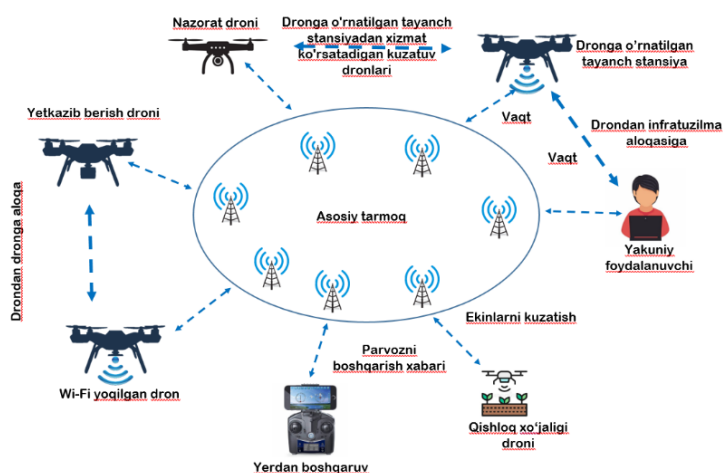
1. Dronlar tarmog'ida aloqa jarayoni va kiberhujumlarning tarqalish xususiyatlarini tahlil qilish ;
2. DoS/DDoS, Man-In-The-Middle, GPS-spoofing va Wormhole kabi xarakterli kiberhujumlarni aniqlash mezonlarini ishlab chiqish;
3. Dronlarning resurs cheklovlarini hisobga olgan holda takomillashtirilgan va moslashuvchan xavfsizlik arxitekturasini taklif etish .

Tadqiqot metodologiyasi va usullari: Tadqiqotda kiberhujumlarni modellashtirish, tarmoq anomaliyalarini tahlil qilish, kriptografik shifrlash tamoyillari hamda tizimli tahlil usullaridan foydalanildi [1-rasm]. Dron va yer usti boshqaruv stansiyasi hamda drondan dronga aloqa kanallaridagi axborot xavfsizligi darajasi baholandi.

ASOSIY MAZMUN VA TAKOMILLASHTIRILGAN ARXITEKTURA

Dron tarmoqlarida kibertahdidlarni barvaqt aniqlash uchun tarmoq trafiginini va tugunlar xatti-harakatini doimiy monitoring qilish talab etiladi. Dron apparat resurslari cheklanganligi sababli barcha hisoblash ishlarini dronda bajarish samarasizdir. Shuning uchun kiberhujumlarni aniqlash va himoyalash ikki bosqichda amalga oshiriladi:

- **Xizmatdan voz kechish (DoS/DDoS) va Jamming:** Tarmoq kanallarini to'sib qo'yish va soxta so'rovlar bilan yuklash hujumlari. Bularni aniqlash uchun paketlar chastotasi va signal-shovqin nisbati tahlil qilinadi.
- **Man-In-The-Middle (MITM) va Wormhole hujumlari:** Tranzit ma'lumotlarni tutib olish va yashirin tunnellash. Ularni aniqlash uchun tugunlararo masofa va kechikish vaqti (RTT) ko'rsatkichlari baholanadi.
- **GPS-spoofing:** Soxta geoma'lumotlar uzatish orqali dron yo'nalishini o'zgartirish. Buni aniqlash uchun qo'shni tugunlar va inertial navigatsiya ma'lumotlari solishtiriladi.



1-rasm.

XULOSA VA AMALIY TAVSIYALAR

Dronlar tarmog'ining xavfsizlik arxitekturasini takomillashtirish orqali kiberhujumlarni barvaqt aniqlash va ularning ta'sirini kamaytirishga erishiladi. Tadqiqot natijasida quyidagi amaliy va texnik tavsiyalar ilgari surildi:

1. **Resurs tejovchi shifrlash va autentifikatsiya:** Dronlar o'rtasida yengil siklli kriptografik algoritmlar hamda dinamik autentifikatsiya mexanizmlarini qo'llash.
2. **Anomaliyalarni intellektual aniqlash:** Yer usti boshqaruv stansiyasi va tayanch dronlarda tarmoq anomaliyalarini aniqlovchi intellektual algoritmlarni joriy etish.

**FAN, TA'LIM, TEXNOLOGIYA VA ISHLAB CHIQARISH
INTEGRATSIYASI ASOSIDA RIVOJLANISH ISTIQBOLLARI
RESPUBLIKA ILMIY-AMALIY KONFERENSIYASI
VOLUME-3, ISSUE-10**

3. Kiber-moslashuvchanlik va RTH rejimi: GPS-spoofing yoki Jamming aniqlanganda dronni avtomatik ravishda “Uyga qaytish” (RTH) va xavfsiz avtonom rejimga o‘tkazish.

4. Dasturiy ta’minot va kirish nazorati: Dron mikrodasturlarini xavfsiz yangilab borish va tayanch stansiyaga ulanuvchi qurilmalar sonini cheklash.

FOYDALANILGAN ADABIYOTLAR

1. Rivojiddinov D. B., Sattarov N. A., Umarov M. X., Tursunov B. A. Dronlarda axborot xavfsizligini ta'minlash muammolari va hujumlarning tahlili // Journal of Education, Ethics and Value. – 2025. – Vol. 4, No. 6. – PP. 82-83. ISSN: 2181-4392.
2. Ullah H., Nair N. G., Moore A., Nugent C., Muschamp P., Cuevas M. 5G communication: an overview of vehicle-to-everything, drones, and healthcare use-cases // IEEE Access. – 2019. – Vol. 7. – PP. 37251-37268.
3. Westerlund O., Asif R. Drone hacking with raspberry-pi 3 and wifi pineapple: Security and privacy threats for the internet-of-things // 2019 1st International Conference on Unmanned Vehicle Systems-Oman (UVS). – IEEE, 2019. – PP. 1-10.