# AVTONOM G‘ILDIRAKLI ROBOT GALALARIDA AI GA ASOSLANGAN MARSHRUTLASH PROTOKOLLARINING KIBERHUJUMLARGA VA MANIPULYATSIYALARGA BARDOSHLILIGI

**Axmedov Jasur Rajab o‘g‘li.**
ISMA universiteti Magistranti ( Riga, Latvia)

**Annotatsiya:** Ushbu maqolada avtonom g‘ildirakli robot galalarida sun’iy intellektga asoslangan marshrutlash protokollarining kiberhujumlar, yolg‘on ma’lumotlar va adversarial manipulyatsiyalarga bardoshliligini ta’minlash masalasi tadqiq etiladi. Tadqiqotda robotlararo tarmoqning dinamik xususiyatlari hisobga olinib, tahdid modeli, AI-marshrutlash mexanizmi va uning xavfsizligini oshirishga qaratilgan ko‘p bosqichli himoya yondashuvi taklif qilinadi.

**Kalit so‘zlar:** avtonom robotlar, robot galasi, sun’iy intellekt, marshrutlash protokoli, kiberxavfsizlik, adversarial hujum, mashinali o‘qitish, tarmoq bardoshliligi.

So‘nggi yillarda avtonom robotik tizimlarning rivojlanishi bir nechta robotlarning yagona maqsad sari markazlashmagan holda hamkorlik qilishi imkonini beruvchi robot galalariga bo‘lgan ilmiy qiziqishni sezilarli darajada oshirdi. Robot galasining samarali ishlashi nafaqat alohida robotning harakatlanish qobiliyatiga, balki robotlar o‘rtasidagi axborot almashinuvi, tarmoqning barqarorligi va marshrutlash mexanizmlarining ishonchliligiga ham bog‘liq. Swarm tizimlarida aloqa va marshrutlash protokollari koordinatsiya hamda ma’lumot almashinuvi uchun fundamental komponent sifatida qaraladi.

Robotlarning tarmoqqa ulanganligi, shu bilan birga ularning fizik muhitda real harakatni amalga oshirishi kiberxavfsizlik muammosini an’anaviy kompyuter tarmoqlariga nisbatan yanada murakkablashtiradi. Robotik tizimlarda zaifliklar tarmoq, dasturiy ta’minot, ma’lumotlar va apparat komponentlari darajasida yuzaga kelishi mumkin; amaliy tadqiqotlarda DoS, MITM va robot dasturiy muhitiga qaratilgan hujumlar keng muhokama qilingan.[1,34-b]

Sun’iy intellekt asosidagi marshrutlash protokollarining joriy etilishi ushbu muammoning yangi qatlamini yuzaga keltiradi. Bir tomondan, AI dinamik tarmoq holatini tahlil qilish, optimal yo‘nalishni tanlash va o‘zgaruvchan sharoitga moslashish imkonini beradi. Ikkinchi tomondan, AI modeli o‘zi ham adversarial manipulyatsiyalarning nishoniga aylanishi mumkin. NIST tomonidan 2025-yilda e’lon qilingan adversarial machine learning taksonomiyasida evasion, poisoning va boshqa hujumlar AI tizimlarining hayotiy sikli bilan bog‘liq muhim xavflar sifatida tasniflangan.[2,13-b]

Shu sababli avtonom g‘ildirakli robot galalarida marshrutlash masalasini faqat tarmoq samaradorligi nuqtayi nazaridan emas, balki xavfsizlik, ishonchlilik va adversarial bardoshlilik nuqtayi nazaridan ham ko‘rib chiqish zarur.

*Muammoning qo‘yilishi*. Robot galasi (G=(V,E)) ko‘rinishidagi dinamik graf sifatida ifodalanadi. Bunda (V={v_1,v_2,\ldots,v_n}) robotlar to‘plamini, (E) esa ular orasidagi mavjud aloqa kanallarini bildiradi. Har bir robot tarmoq holati, qo‘shni robotlar, signal sifati, kechikish va paket yo‘qolishi kabi parametrlar asosida marshrutlash qarorini shakllantiradi.

An’anaviy marshrutlash mexanizmlarida yo‘l tanlash masofaga, ulanishga yoki boshqa oldindan belgilangan metrikalarga asoslangan bo‘lishi mumkin. AI asosidagi yondashuvda esa qarorlar tarmoqning joriy holatidan o‘rganilgan bog‘lanishlar asosida shakllantiriladi. Natijada tizim dinamik muhitga moslasha oladi, biroq noto‘g‘ri yoki manipulyatsiya qilingan kirish ma’lumotlari marshrutlash qarorining buzilishiga olib kelishi mumkin.

Mazkur tadqiqotda asosiy muammo quyidagicha ifodalanadi: tarmoqdagi dushman tomonning yolg‘on, buzilgan yoki ataylab o‘zgartirilgan ma’lumotlari mavjud bo‘lgan sharoitda AI asosidagi marshrutlash protokoli robotlar o‘rtasidagi ishonchli aloqa va optimal marshrutlashni qanday saqlab qolishi mumkin?

Mazkur savol robot galasi uchun alohida ahamiyatga ega, chunki bitta robotning noto‘g‘ri marshrutlash qarori boshqa robotlarning qarorlariga ham ta’sir qilishi va tizim bo‘yicha xatolarni kuchaytirishi mumkin. Swarm robotikasi bo‘yicha zamonaviy tadqiqotlarda aloqa, xavfsizlik va real vaqt talablari bir-biri bilan uzviy bog‘liq masalalar sifatida qayd etilgan. [4,56-b]

*Mavzuning ilmiy-nazariy asoslari.* Adversarial machine learning AI modellarining maxsus tayyorlangan yoki o‘zgartirilgan ma’lumotlar orqali xato qaror qabul qilishiga olib keluvchi hujumlarni o‘rganadi. NIST 2025-yilgi taksonomiyasida hujumchi maqsadi, bilim darajasi, hujum bosqichi va foydalanilayotgan mashinali o‘qitish usuli asosida adversarial tahdidlarni tizimlashtirish taklif etilgan.

Robot galasi kontekstida bunday hujumlar quyidagi ko‘rinishlarda namoyon bo‘lishi mumkin.

*False Data Injection hujumi.* Hujumchi robotga yoki uning marshrutlash moduliga soxta signal sifati, masofa, qo‘shni robot holati yoki kanal yuklamasi haqidagi ma’lumotni yuboradi. AI ushbu ma’lumotni haqiqiy deb qabul qilsa, xavfsiz bo‘lmagan yoki samarasiz yo‘lni tanlashi mumkin.

*Data Poisoning hujumi.* AI modeli o‘qitilishi vaqtida foydalaniladigan ma’lumotlar to‘plamiga zararli yoki noto‘g‘ri namunalar kiritiladi. Natijada model normal sharoitda ham noto‘g‘ri umumlashtirishga moyil bo‘lib qoladi. Data poisoning adversarial machine learning doirasidagi asosiy hujum turlaridan biri sifatida ko‘rsatilgan.

*Evasion hujumi.* Model ishga tushirilganidan so‘ng uning kirish ma’lumotlari modelning noto‘g‘ri klassifikatsiya yoki noto‘g‘ri qaror chiqarishiga sabab bo‘ladigan tarzda o‘zgartiriladi. Bunday yondashuv AI asosidagi xavfsizlik mexanizmlariga ham qo‘llanishi mumkin.

*DoS va DDoS hujumlari.* Tarmoq resurslarini haddan tashqari band qilish natijasida robotlar orasidagi aloqa kechikadi yoki uziladi. Robotlar uchun bu faqat ma’lumot yetkazish sifatining pasayishi emas, balki koordinatsiya va harakat boshqaruvida ham salbiy oqibatlar keltirib chiqarishi mumkin. Robot kiberxavfsizligi bo‘yicha sharhlarda DoS va DDoS hujumlari muhim tarmoq tahdidlari sifatida qayd etilgan.

*Sybil hujumi.* Bitta zararli qurilma tarmoqda bir nechta soxta robot identifikatorlari bilan namoyon bo‘lishi mumkin. Natijada marshrutlash algoritmi mavjud tugunlar va ularning ishonchliligi haqida noto‘g‘ri tasavvur hosil qiladi. Bu, ayniqsa, markazlashmagan robot galalarida tugunlar haqidagi qarorlarni faqat lokal ma’lumotlar asosida qabul qilish holatlarida xavfli hisoblanadi.

*AI asosidagi xavfsiz marshrutlash modeli.* Taklif etilayotgan yondashuvda robotlar tarmog‘ining holatini aks ettiruvchi xususiyatlar vektori quyidagicha ifodalanadi:[5,67-b]

[X_i=[d_i,r_i,l_i,p_i,e_i,t_i]]

bu yerda:

- (d_i) — qo‘shni robotgacha bo‘lgan masofa;
- (r_i) — aloqa signalining sifati;
- (l_i) — kanal yuklamasi;
- (p_i) — paketlarning yo‘qolish darajasi;
- (e_i) — robotning energiya holati;
- (t_i) — kechikish ko‘rsatkichi.

AI modeli ushbu parametrlar asosida har bir ehtimoliy marshrut uchun xavfsizlik va samaradorlik qiymatini hisoblaydi. Umumiy marshrut bahosi quyidagi ko‘rinishda berilishi mumkin:

[S(R)=\alpha Q(R)+\beta C(R)-\gamma L(R)-\delta A(R)] bu yerda (Q(R)) — aloqa sifati, (C(R)) — marshrutning ishonchlilik ko‘rsatkichi, (L(R)) — kechikish va resurs xarajati, (A(R)) esa aniqlangan xavf darajasini bildiradi.

Mazkur modelning muhim jihati shundan iboratki, marshrutlash qarori faqat tezkor va qisqa yo‘lni emas, balki xavfsiz va barqaror yo‘lni tanlashga yo‘naltiriladi.

*Taklif etilayotgan himoya mexanizmi*. AI asosidagi marshrutlash protokolining adversarial bardoshliligini oshirish uchun ko‘p bosqichli himoya arxitekturasidan foydalanish maqsadga muvofiq.

Birinchi bosqichda ma’lumotlarni tekshirish amalga oshiriladi. Robotdan kelgan ma’lumotlar vaqt tamg‘asi, manba identifikatori, qiymatning fizik jihatdan mumkinligi va qo‘shni tugunlar ma’lumotlari bilan solishtiriladi.

Ikkinchi bosqichda anomaliyalarni aniqlash modeli ishlaydi. Ushbu modul normal tarmoq holatini o‘rganib, keskin o‘zgarishlar, takrorlanuvchi g‘ayritabiiy qiymatlar yoki bir-biriga zid xabarlarni aniqlaydi.

Uchinchi bosqichda adversarial robust AI modeli ishlatiladi. Modelni o‘qitish jarayonida oddiy ma’lumotlar bilan bir qatorda manipulyatsiya qilingan namunalar ham qo‘llanib, modelning hujumlarga nisbatan barqarorligi oshiriladi. Adversarial training va anomaliyalarni aniqlash kabi himoya mexanizmlari AI-ga asoslangan robot tizimlari xavfsizligini kuchaytiruvchi istiqbolli choralar sifatida ilmiy adabiyotlarda muhokama qilingan.[3,49-b]

To‘rtinchi bosqichda ishonchlilikka asoslangan marshrut tanlash amalga oshiriladi. Har bir robot yoki aloqa kanali uchun dinamik trust score shakllantirilib, ishonchlilik darajasi past bo‘lgan tugunlar marshrut tanlash jarayonida cheklanadi.

Beshinchi bosqichda xavfsiz qayta marshrutlash mexanizmi ishga tushiriladi. Asosiy marshrutda tahdid aniqlanganda, tizim avtomatik ravishda xavfi past bo‘lgan muqobil marshrutni tanlaydi.

*Modelning algoritmik ishlash prinsipi.* Taklif qilinayotgan algoritmni quyidagi ketma-ketlikda tashkil etish mumkin:

1. Robotlar tarmoq holati haqida lokal ma’lumotlarni yig‘adi.
2. Ma’lumotlar dastlabki verifikatsiyadan o‘tkaziladi.
3. AI modeli tarmoqdagi marshrutlar uchun samaradorlik va xavfsizlik ko‘rsatkichlarini hisoblaydi.
4. Anomaliya aniqlash moduli shubhali tugun yoki ulanishlarni belgilaydi.
5. Ishonchlilik ko‘rsatkichi asosida marshrutlar qayta baholanadi.
6. Eng maqbul va xavfsiz marshrut tanlanadi.
7. Tarmoq holati o‘zgarganda qaror qayta hisoblanadi.

Mazkur yondashuvning afzalligi shundaki, marshrutlash va xavfsizlik alohida modullar sifatida emas, balki yagona qaror qabul qilish mexanizmi sifatida qaraladi.

*Tadqiqotni eksperimental baholash metodikasi.* Maqolada taklif qilinayotgan modelni eksperimental tasdiqlash uchun robotlar galasini simulyatsiya qiluvchi muhit yaratish mumkin. Simulyatsiyada robotlar soni, aloqa radiusi, harakat tezligi, paket uzatish chastotasi, tarmoq zichligi va hujumchilar soni kabi parametrlar o‘zgartiriladi.

Model samaradorligini baholashda quyidagi ko‘rsatkichlardan foydalanish maqsadga muvofiq:

[PDR=\frac{N_{received}}{N_{sent}}\times100%] bu yerda (PDR) — paketlarni yetkazib berish darajasi.

Shuningdek, o‘rtacha end-to-end kechikish, marshrutning barqarorligi, hujumni aniqlash aniqligi, false positive rate, false negative rate, qayta marshrutlash vaqti va robotning energiya sarfi ham baholanishi lozim.

AI modelining xavfsizlik ko‘rsatkichlarini oddiy marshrutlash algoritmi bilan taqqoslash ayniqsa muhim. Bunda asosiy savol faqat “model qanchalik tez marshrut topadi?” emas, balki “hujum sharoitida model o‘z funksiyasini qanchalik yaxshi saqlab qoladi?” degan masala bo‘lishi kerak.

*Muhokama.* Robotlar kiberxavfsizligi bo‘yicha mavjud ilmiy ishlar xavfsizlik muammosi robotning fizik qismi bilan cheklanmasligini, balki tarmoq, dasturiy ta’minot va ma’lumotlar

qatlamlarini ham qamrab olishini ko‘rsatadi. AI texnologiyalarining robotik tizimlarga chuqurroq integratsiyalashuvi esa xavfsizlik masalasiga modelning o‘zini himoya qilish talabini ham qo‘shadi. 2024-yildagi IEEE tadqiqoti robotika va avtonom tizimlarda AI yordamida kiberxavfsizlikni rivojlantirish bilan bog‘liq ilmiy bo‘shliqlar mavjudligini qayd etadi.

Shu nuqtayi nazardan, avtonom g‘ildirakli robot galalarida marshrutlash protokolini faqat klassik tarmoq parametrlari asosida optimallashtirish yetarli emas. Marshrutning xavfsizlik qiymati, tugunning ishonchliligi va AI modeliga berilgan ma’lumotlarning yaxlitligi ham qaror funksiyasiga kiritilishi lozim.

Taklif etilayotgan yondashuvda uchta maqsad bir vaqtning o‘zida optimallashtiriladi: tarmoq samaradorligi, hujumlarga bardoshlilik va tizimning uzluksiz ishlashi. Biroq ushbu maqsadlar o‘rtasida muvozanat mavjud. Haddan tashqari qat’iy xavfsizlik tekshiruvlari tarmoq kechikishini oshirishi, juda tezkor qaror qabul qilish esa xavfsizlik darajasini pasaytirishi mumkin. Swarm robotik tizimlari bo‘yicha zamonaviy sharhlarda aynan real vaqt talablari bilan xavfsizlik va samaradorlik o‘rtasidagi muvozanat muhim ochiq masala sifatida ko‘rsatilgan.

*Ilmiy yangilik.* Mazkur maqolaning asosiy ilmiy yangiligi avtonom g‘ildirakli robot galalari uchun AI asosidagi marshrutlashni xavfsizlik metrikasi bilan birlashtirgan holda ko‘rib chiqishdan iborat.

Taklif qilinayotgan modelda:

- marshrutning tarmoq samaradorligi;
- tugunning ishonchlilik darajasi;
- ma’lumotlar anomaliyasi;
- adversarial xavf;
- qayta marshrutlash zarurati yagona qaror qabul qilish jarayonida hisobga olinadi.[7,85-b]

Shuningdek, modelning o‘zini himoyalashga qaratilgan adversarial training, anomaliya aniqlash va trust-based routing mexanizmlarini birlashtirish robot galasining kiberhujumlarga chidamliligini oshirish uchun istiqbolli konseptual asos sifatida qaraladi. Bunday yo‘nalish adversarial machine learning bo‘yicha xalqaro taksonomiyalar bilan hamohangdir.

*Xulosa.* Avtonom g‘ildirakli robot galalari kelajakdagi aqlli transport, monitoring, qidiruv-qutqaruv, logistika va boshqa ko‘plab avtonom tizimlarning muhim tarkibiy qismiga aylanishi mumkin. Biroq bunday tizimlarning samaradorligi faqat avtonom qaror qabul qilish imkoniyati bilan emas, balki tarmoq va AI komponentlarining kiberxavfsizligi bilan ham belgilanadi.

Tadqiqotda AI asosidagi marshrutlash protokollarini adversarial hujumlar, ma’lumotlarni manipulyatsiya qilish, soxta ma’lumot kiritish va tarmoq xizmatlarini izdan chiqarishga urinishlardan himoyalash uchun ko‘p bosqichli yondashuv taklif qilindi. Ushbu yondashuv ma’lumotlarni verifikatsiya qilish, anomaliyalarni aniqlash, adversarial jihatdan bardoshli AI modeli, tugunlar ishonchliligini baholash va xavfsiz qayta marshrutlash mexanizmlarini yagona tizimga birlashtiradi.

Kelgusidagi tadqiqotlarda ushbu modelni ROS 2 yoki boshqa robototexnika simulyatsiya muhitida amalga oshirish, turli robotlar soni va tarmoq zichligi uchun sinash, adversarial hujumlarning bir nechta ssenariylarini shakllantirish hamda himoyalangan va himoyalanmagan marshrutlash algoritmlarini statistik jihatdan taqqoslash zarur. Aynan empirik sinovlar orqali taklif etilgan modelning xavfsizlik, kechikish, paket yetkazib berish va energiya samaradorligi bo‘yicha ustunliklarini miqdoriy asoslash mumkin.

**Foydalanilgan adabiyotlar**

1. Vassilev, A., Oprea, A., Fordyce, A., Anderson, H., Davies, X., & Hamin, M. (2025). *Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations*. NIST AI 100-

2e2025. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-2e2025. (NIST Computer Security Resource Center)

2. Santoso, F., & Finn, A. (2024). An in-depth examination of artificial intelligence-enhanced cybersecurity in robotics, autonomous systems, and critical infrastructures. *IEEE Transactions on Services Computing, 17*(3), 1293–1310. https://doi.org/10.1109/TSC.2023.3331083. (Digital Library Adelaide)
3. Yan, Y., Xie, Y., Tang, J., Li, Y., & Jin, Y. (2025). Reliability and security: from swarm robots to AI agents. *Journal of Reliability Science and Engineering, 1*, 032001. https://doi.org/10.1088/3050-2454/adea7a. (DOI)
4. Macas, M., Wu, C., & Fuertes, W. (2024). Adversarial examples: A survey of attacks and defenses in deep learning-enabled cybersecurity systems. *Expert Systems with Applications, 238*, 122223. (ScienceDirect)
5. Chen, X., Tang, J., & Lao, S. (2020). Review of unmanned aerial vehicle swarm communication architectures and routing protocols. *Applied Sciences, 10*(10), 3661. https://doi.org/10.3390/app10103661. (MDPI)
6. Grigorescu, S., Trasnea, B., Cocias, T., & Macesanu, G. (2021). Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security, 20*, 819–838. https://doi.org/10.1007/s10207-021-00545-8. (PubMed)
7. Diab, A., et al. (2023). Cyber security of robots: A comprehensive survey. *Intelligent Systems with Applications, 18*, 200237. https://doi.org/10.1016/j.iswa.2023.200237. (DOI)
8. Altun, V. C., Ata, B., & Canbay, Y. (2026). Threats, vulnerabilities and measures in robot communication security: A review. *Kahramanmaraş Sütçü İmam Üniversitesi Mühendislik Bilimleri Dergisi, 29*(1). (jes.ksu.edu.tr)