



IOT VA TELEKOMMUNIKATSIYA INTEGRATSIYASI. IoT QURILMALARI UCHUN AI ASOSIDAGI AQLLI TARMOQ BOSHQARUV TIZIMI

U.A. Saparova¹

N.S.Shamuratova²

M.N.Jalgashova²

¹assistent, Nukus davlat texnika universiteti

²talaba, Nukus davlat texnika universiteti

Annotatsiya: Ushbu maqolada IoT va telekommunikatsiya tarmoqlari integratsiyasi sharoitida AI asosidagi aqlli tarmoq boshqaruv tizimini ishlab chiqish masalasi yoritilgan. Ishda IoT arxitekturasini, 5G/MEC imkoniyatlari, MQTT va CoAP kabi protokollar, telemetriya yig'ish, anomaliya aniqlash, trafik prognozi, resurslarni optimallashtirish hamda kiberxavfsizlik talablari tahlil qilinadi. Taklif etilgan model IoT qurilmalaridan kelayotgan ma'lumotlarni real vaqtga yaqin yig'ish, AI modeli orqali tahlil qilish va tarmoq siyosatini avtomatik yoki yarim avtomatik tarzda tanlashga asoslanadi.

Kalit so'zlar: IoT, telekommunikatsiya integratsiyasi, AI (sun'iy intellekt), aqlli tarmoq boshqaruv tizimi, IoT me'morchiligi, 5G/MEC, MQTT, CoAP, telemetriya, anomaliya aniqlash, trafik prognozi, resurslarni optimallashtirish, kiberxavfsizlik.

Kirish

So'nggi yillarda raqamli iqtisodiyot, aqlli shahar, sanoat avtomatizatsiyasi, transport, sog'liqni saqlash va kommunal xizmatlar sohalarida IoT qurilmalaridan foydalanish keskin kengaymoqda. Sensorlar, aktuatorlar, aqlli hisoblagichlar, kuzatuv kameralari, sanoat kontrollerlari va mobil terminal qurilmalari doimiy ma'lumot oqimini hosil qiladi. Bu oqimni barqaror uzatish, qayta ishlash va boshqarish telekommunikatsiya infratuzilmasiga bog'liq. Shuning uchun IoT va telekommunikatsiya integratsiyasi zamonaviy axborot-kommunikatsiya tizimlarining eng muhim yo'nalishlaridan biri hisoblanadi.

IoT qurilmalari sonining ortishi tarmoq boshqaruvini murakkablashtiradi. An'anaviy monitoring tizimlari ko'pincha hodisa sodir bo'lgandan keyin xabar beradi, ya'ni ular reaktiv ishlaydi. Biroq katta hajmdagi IoT trafikida bunday yondashuv yetarli emas. Tizim yuklama oshishini oldindan bilishi, anomaliyani erta aniqlashi, resurslarni avtomatik taqsimlashi va operatorga asoslangan tavsiya berishi lozim. AI texnologiyalari aynan shu vazifalarni bajarishda qo'llanilishi mumkin.

Ushbu maqsadga erishish uchun quyidagi vazifalar belgilandi: IoT va telekommunikatsiya integratsiyasining nazariy asoslarini tahlil qilish; IoT protokollari, 5G/MEC, telemetriya va kiberxavfsizlik talablarini o'rganish; AI asosidagi boshqaruv tizimining funksional talablarini shakllantirish; ma'lumotlar oqimi va modullar arxitekturasini ishlab chiqish; anomaliya aniqlash,



trafik prognozi va optimallashtirish algoritmlarini tavsiflash; prototip sinovi uchun metodika va samaradorlik ko'rsatkichlarini ishlab chiqish.

Tadqiqot metodlari sifatida tizimli tahlil, arxitektura modellashtirish, taqqoslash, algoritmik loyihalash, telemetriya metrikalarini tahlil qilish, statistik baholash va konseptual prototiplash usullaridan foydalanildi. Ishda xalqaro standartlar va tavsiyalar, xususan IoT referens modeli, 5G tizim arxitekturasi, MEC, MQTT, CoAP, tarmoq telemetriyasi va AI risklarini boshqarish bo'yicha manbalarga tayanildi.

IoT tushunchasi, tarkibi va referens modeli. Ushbu maqolaning markaziy masalalaridan biri bo'lib, amaliy telekommunikatsiya muhitida IoT qurilmalarini yagona boshqaruv konturiga ulashni nazarda tutadi. IoT ekotizimida fizik obyekt, sensor, aktuator, identifikatsiya, gateway va bulutli xizmatlar o'zaro bog'lanadi.

Mazkur yondashuvda identifikatsiya, sensor ma'lumoti va aktuator buyrug'i o'zaro bog'langan jarayonlar sifatida qaraladi. Standartlarda IoT faqat alohida sensorlar majmui emas, balki identifikatsiya, aloqa, qayta ishlash va xizmat ko'rsatish qatlamlaridan iborat tizim sifatida tavsiflanadi. Shuning uchun integratsiya loyihasida qurilma, tarmoq, platforma va foydalanuvchi ilovasi bir-biridan ajratilmagan holda baholanadi.

Amaliy jihatdan IoT tushunchasi, tarkibi va referens modeli bo'yicha asosiy talablar uch guruhga ajratiladi: funksional talablar, sifat ko'rsatkichlari va ekspluatatsion talablar. Funksional talablar qurilmani ro'yxatdan o'tkazish, ma'lumot yuborish, buyruq qabul qilish, holatni monitoring qilish va nosozlikka javob berishni qamrab oladi. Sifat ko'rsatkichlari esa kechikish, paket yo'qotilishi, tarmoqqa ulanish barqarorligi, ma'lumotning butunligi hamda xizmat uzluksizligi bilan o'lchanadi. Ekspluatatsion talablar konfiguratsiyani masofadan yangilash, audit jurnalini yuritish, operatorga qulay dashboard berish va tarmoq holatini tushunarli ko'rinishda aks ettirishdan iborat.

IoT qurilmalari ko'p hollarda quvvat, protsessor va xotira bo'yicha cheklangan bo'ladi. Shu sababli identifikatsiya va sensor ma'lumoti kabi komponentlar keraksiz trafikni kamaytirishi, paketlarni guruhlashi va faqat kerakli metrikalarni yuqori qatlamlarga uzatishi zarur. Telekommunikatsiya tarmog'i esa ushbu trafikni mintaq, servis turi va ustuvorlik bo'yicha boshqaradi. Agar qurilma soni minglab yoki millionlab bo'lsa, oddiy qo'lda konfiguratsiya qilish usuli yetarli bo'lmaydi. Bunday sharoitda avtomatlashtirilgan monitoring, AI asosida prognozlash va siyosatga asoslangan boshqaruv muhim ahamiyat kasb etadi. Xavfsizlik nuqtai nazaridan IoT tushunchasi, tarkibi va referens modeli faqat parol yoki kanalni shifrlash bilan cheklanmaydi. Qurilma identifikatsiyasi, sertifikatlar, kalitlarni boshqarish, OTA yangilanishlar, firmware butunligini tekshirish, audit jurnali va kirish huquqlarini chegaralash birgalikda ishlashi kerak.

AI asosidagi boshqaruvning ustunligi shundaki, u tarmoq holatini faqat joriy qiymatlar bilan emas, tarixiy tendensiya va ehtimoliy kelajak yuklamasi bilan birga baholaydi. Model soatlik, kunlik va mavsumiy trafik o'zgarishini o'rganadi; favqulodda keskin sakrashlarni aniqlaydi; operatorga oldindan ogohlantirish yuboradi. Biroq AI qarori to'liq nazoratsiz qoldirilmasligi kerak. Muhim

o'zgarishlar auditdan o'tishi, izohlanadigan metrikalar bilan asoslanishi va kerak bo'lganda inson operatori tomonidan tasdiqlanishi lozim.

Ushbu ishda taklif qilinadigan konsepsiyada aktuator buyrug'i, edge gateway va bulutli platforma asosiy tayanch komponentlar hisoblanadi. Birinchi komponent qurilmalardan kelayotgan oqimni yig'adi, ikkinchisi ma'lumotni tahlil qiladi, uchinchisi esa boshqaruv buyruqlarini tarmoq elementlariga uzatadi. Modullar orasidagi interfeyslar ochiq API tamoyiliga yaqin loyihalansa, tizim keyinchalik yangi qurilmalar, yangi protokollar va yangi AI modellarini qo'shishga tayyor bo'ladi.

Baholash mezonlari sifatida o'rtacha kechikish, 95-percentil kechikish, paket yo'qotilishi, aniqlik, yolg'on ogohlantirishlar ulushi, resurs sarfi va operator reaksiyasi vaqti tanlanadi. Har bir mezon bo'yicha boshlang'ich holat va AI yordamidagi holat solishtiriladi. Natija real tarmoqda olinmagan bo'lsa ham, laboratoriya yoki emulyatsiya muhiti orqali tizimning prinsipial afzalliklarini ko'rsatish mumkin. Eng muhim talab – sinov shartlarini aniq yozish, cheklovlarni ochiq ko'rsatish va natijalarni haddan tashqari bo'rttirmaslikdir.

Xulosa va amaliy tavsiyalar

Xulosa sifatida, IoT tushunchasi, tarkibi va referens modeli IoT qurilmalarini telekommunikatsiya tarmog'iga ulashdan ko'ra kengroq masalani anglatadi. Bu yerda qurilma hayotiy sikli, ma'lumotlar oqimi, tarmoq resurslari, xavfsizlik, AI modeli va operator qarori yagona tizim sifatida qaraladi. Shunday yondashuvgina aqlli shahar, sanoat IoT, logistika, tibbiyot va kommunal xizmatlar kabi sohalarda ishonchli raqamli infratuzilma yaratishga imkon beradi. Keyingi boblarda aynan shu asosda AI asosidagi aqlli tarmoq boshqaruv tizimi loyihalanadi.

Nazariy tahlilda IoT qurilmalarini uch darajada ko'rish maqsadga muvofiq: qurilma darajasi, aloqa darajasi va xizmat darajasi. Qurilma darajasida sensor o'lchaydi, aktuator esa tashqi muhitga ta'sir ko'rsatadi. Aloqa darajasida ma'lumot qisqa paketlarga ajratiladi, tarmoq orqali uzatiladi va protokol qoidalari asosida qayta yig'iladi. Xizmat darajasida esa foydalanuvchi uchun qiymat yaratiladi: monitoring, masofadan boshqarish, analitika yoki avtomatik ogohlantirish. Diplom ishida shu uch daraja o'rtasidagi bog'lanish alohida yoritiladi.

IoT va telekommunikatsiya integratsiyasi faqat texnologik masala emas, balki tashkiliy masala hamdir. Operator tarmog'i, korxona axborot tizimi, qurilma ishlab chiqaruvchisi va xizmat provayderi turli mas'uliyat zonalariga ega. Ma'lumot kimga tegishli, kim uni qayta ishlaydi, kim xavfsizlik uchun javob beradi va kim nosozlik paytida qaror qabul qiladi degan savollar oldindan belgilanmasa, yaxshi texnik yechim ham amalda qiyinchilik tug'diradi. Shu sababli loyiha boshida rol va javobgarliklar matritsasi tuzilishi kerak.

IoT qurilmalari ko'p hollarda quvvat, protsessor va xotira bo'yicha cheklangan bo'ladi. Shu sababli 4G/5G va NB-IoT kabi komponentlar keraksiz trafikni kamaytirishi, paketlarni guruhlashi va faqat kerakli metrikalarni yuqori qatlamlarga uzatishi zarur. Telekommunikatsiya tarmog'i esa ushbu trafikni mintaqa, servis turi va ustuvorlik bo'yicha boshqaradi. Agar qurilma soni minglab yoki millionlab bo'lsa, oddiy qo'lda konfiguratsiya qilish usuli yetarli bo'lmaydi.

Bunday sharoitda avtomatlashtirilgan monitoring, AI asosida prognozlash va siyosatga asoslangan boshqaruv muhim ahamiyat kasb etadi.

Telekommunikatsiya tarmoqlarining evolyutsiyasi va IoT ehtiyojlari uchun ma'lumotlar sifati alohida rol o'ynaydi. AI modeli noto'g'ri, kechikkan yoki to'liq bo'lmagan ma'lumotga tayansa, boshqaruv qarori ham noto'g'ri bo'lishi mumkin. Shuning uchun telemetriya oqimida vaqt tamg'asi, qurilma identifikatori, lokatsiya, signal darajasi, paketlar soni, xatolik kodi va servis turi kabi belgilar saqlanishi lozim. Ma'lumotlarni normalizatsiya qilish, keskin chetlanishlarni filtrlash va dublikat yozuvlarni olib tashlash modelning barqarorligini oshiradi.

Foydalanilgan adabiyotlar

1. ITU-T Recommendation Y.4000/Y.2060. Overview of the Internet of Things. International Telecommunication Union, 2012.
2. 3GPP TS 23.501. System architecture for the 5G System (5GS). 3rd Generation Partnership Project.
3. 3GPP TS 23.288. Architecture enhancements for 5G System to support network data analytics services.
4. ETSI GS MEC 003. Multi-access Edge Computing (MEC); Framework and Reference Architecture.
5. OASIS Standard. MQTT Version 5.0. Message Queuing Telemetry Transport Technical Committee, 2019.
6. IETF RFC 7252. The Constrained Application Protocol (CoAP). Internet Engineering Task Force, 2014.
7. NISTIR 8259A. IoT Device Cybersecurity Capability Core Baseline. National Institute of Standards and Technology, 2020.
8. NIST AI 100-1. Artificial Intelligence Risk Management Framework (AI RMF 1.0). National Institute of Standards and Technology, 2023.
9. IETF RFC 9232. Network Telemetry Framework. Internet Engineering Task Force, 2022.
10. IETF RFC 9019. A Firmware Update Architecture for Internet of Things Devices. Internet Engineering Task Force, 2021.