

KO'P QATLAMLI IOT TIZIMLARIDA NOSOZLIK XAVFINI BAHOLASH VA XAVFSIZ TIKLASHGA ASOSLANGAN O'Z-O'ZINI DIAGNOSTIKALASH

E.S. Babadjanov¹, O.K. Ataboyev¹, M.N. Jumaniyozov^{1*}

¹Nukus davlat texnika universiteti, Nukus, O'zbekiston

E-mail: elmurbes@gmail.com, muzrobjumaniyozov653@gmail.com

Annotatsiya. Ko'p qatlamli IoT tizimida sensor, hisoblash va aloqa qismlaridagi nosozliklar tashqi tomondan o'xshash belgilarni yuzaga keltirishi mumkin. Ushbu tezisda qatlamlar holatini birgalikda baholash, umumiy xavf ko'rsatkichini hisoblash, ehtimoliy nosozlik manbasini aniqlash va mos xavfsiz tiklash chorasi bajarilgandan keyin tizim holatini qayta tekshirish tamoyili bayon etildi. Yondashuv energiya holatini ham hisobga olgan holda diagnostika jadalligini o'zgartiradi. Miqdoriy natijalar imitatsion tajribaga tegishli bo'lib, tiklash mexanizmlarining apparat samaradorligi keyingi tajribalarda tekshirilishi kerak.

Kalit so'zlar: ko'p qatlamli IoT, o'z-o'zini diagnostikalash, nosozlik xavfi, sensor, edge tugun, aloqa, xavfsiz tiklash.

Kirish

Avtonom IoT tizimida ma'lumot kelmay qolishi yoki noto'g'ri bo'lishi har doim ham sensorning ishdan chiqishini anglatmaydi. Muammo sensorning o'zida, ma'lumotlarni qayta ishlovchi edge tugunda yoki aloqa kanalida yuzaga kelishi mumkin. Agar tizim faqat anomaliya mavjudligini aniqlasa-yu, uning qaysi qismdan kelib chiqqanini farqlamasa, noto'g'ri tiklash chorasi tanlanishi mumkin. Bu esa qo'shimcha energiya sarfi, ma'lumot yo'qotilishi yoki xizmatning vaqtincha to'xtashiga olib keladi.

Shuning uchun o'z-o'zini diagnostikalash jarayoni uchta ketma-ket vazifani bajarishi kerak: nosozlik belgisini aniqlash, ehtimoliy manbani lokalizatsiya qilish va bajarilgan tiklash chorasidan keyin tizim holatini qayta tekshirish. Mazkur tezisning maqsadi sensor, edge va aloqa qismlaridan olinadigan holat ko'rsatkichlarini birlashtirib, xavfga mos diagnostika va yopiq qayta tekshirish tamoyilini shakllantirishdan iborat.

Ko'p qatlamli diagnostika modeli

Taklif etilgan tuzilma sensor, edge tugun, aloqa, shlyuz va bulut/operator qismlaridan tashkil topadi [6]. Sensor obyekt haqidagi ma'lumotlarni yig'adi, edge tugun ularni mahalliy tahlil qiladi, aloqa qatlami esa zarur ma'lumotlarni shlyuzga uzatadi. Murakkabroq tahlil yoki modelni yangilash vazifalari shlyuz yoki bulutda

bajarilishi mumkin. Qurilmalar o'rtasidagi ma'lumot almashinuvi MQTT protokoli orqali tashkil etiladi [5].

Tugunning holati $E(t)$, $H_s(t)$, $H_e(t)$, $C(t)$, $L(t)$ va $A(t)$ parametrlaridan tuzilgan $x(t)$ holat vektori bilan ifodalanadi. Har bir qatlamda haqiqiy qiymat kutilayotgan qiymat bilan solishtirilib, $r_i(t)$ farq hosil qilinadi [1–4]. Kutilayotgan qiymat EWMA yoki sodda prognoz modeli orqali aniqlanishi mumkin. Farqning ortishi tegishli qatlamdagi nosozlik ehtimoli oshganini bildiradi.

$$R(t) = \sum w_i \cdot \min(1, |r_i(t)|/\tau_i) + w_q \cdot Q(t).$$

$R(t)$ umumiy xavf darajasini ifodalaydi. $Q(t)$ aloqa holatini paket yo'qolishi, qayta uzatish va signal sifati orqali baholaydi. w_i koeffitsiyentlari esa har bir qatlamdagi o'zgarishning umumiy xavfga ta'sirini belgilaydi. Shu tarzda tizim faqat bitta sensor ko'rsatkichiga emas, bir nechta qatlamdan kelayotgan belgilar majmuasiga tayangan holda qaror qabul qiladi.

Nosozlikni aniqlash va xavfsiz tiklash ketma-ketligi

Algoritmda dastlab sensor ko'rsatkichlari, batareya holati, aloqa sifati va qurilma yuklamasi yig'iladi. Keyin sensor, hisoblash va aloqa qismlaridagi haqiqiy qiymatlar kutilayotgan qiymatlar bilan solishtiriladi. Aniqlangan farqlar asosida anomaliya mavjudligi tekshiriladi va uning ehtimoliy manbasi aniqlanadi. Nosozlik turi yetarli ishonch bilan aniqlangandan so'ng unga mos xavfsiz chora tanlanadi.

Sensor qismidagi muammo uchun sensorni qayta sozlash, edge xizmatidagi xato uchun tegishli dasturni qayta ishga tushirish, aloqa muammosida kanalni almashtirish yoki ma'lumotlarni qayta uzatish, jiddiy holatda esa qurilmani xavfsiz ishlash rejimiga o'tkazish ko'zda tutiladi. Bajirilgan chora yakuniy natija sifatida qabul qilinmaydi. Ma'lum Δt vaqtdan keyin xavf darajasi qayta hisoblanadi. Agar $R(t+\Delta t)$ kamaymasa, muammo haqidagi ma'lumot shlyuz yoki operatorga yuboriladi. Shu sababli diagnostika jarayoni kuzatish–qaror–tiklash–qayta tekshirish yopiq ketma-ketligida ishlaydi.

Mazkur yondashuvdagi “o'z-o'zini tiklash” tushunchasi fizik shikastlangan detalni mustaqil ta'mirlashni anglatmaydi. U dasturiy qayta ishga tushirish, qayta sozlash, aloqa parametrlarini o'zgartirish yoki xavfsiz rejimga o'tish kabi boshqaruv choralari anglatadi.

Imitatsion baholash

Umumiy adaptiv diagnostika yondashuvi 100 ta mustaqil, 30 kunlik Monte-Karlo tajribasida baholandi. Har bir tajribaga 24 ta nosozlik epizodi kiritildi. Baholashda energiya sarfi, nosozliklarni aniqlash darajasi, aniqlash kechikishi va yolg'on ogohlantirishlar soni hisobga olindi. Adaptiv usulda energiya sarfi $6520,6 \pm 652,0$ mJ, recall $0,697 \pm 0,102$, aniqlash kechikishi $21,2 \pm 4,4$ minut va yolg'on ogohlantirishlar soni $9,5 \pm 2,5$ ni tashkil etdi.

Bu natijalar ko'p qatlamli xavfga mos diagnostika boshqaruvining umumiy ishlashini tavsiflaydi. Biroq aynan nosozlik manbasini sensor, edge yoki aloqa qatlamiga ajratish aniqligi hamda tanlangan tiklash choralarning muvaffaqiyat darajasi ushbu imitatsiyada alohida miqdoriy ko'rsatkich sifatida baholanmagan. Shuning uchun lokalizatsiya va tiklash qismini apparat tajribasi bilan tekshirish keyingi bosqichning muhim vazifasi hisoblanadi.

Amaliy tekshirish yo'nalishi

Keyingi bosqichda ESP32 yoki STM32 mikrokontrolleri, tok va kuchlanish o'lchagichi hamda MQTT shlyuzidan iborat prototip yaratish rejalashtiriladi. Tajribada sensor uzilishi, ko'rsatkichlarning asta-sekin og'ishi, paketlarning yo'qolishi va edge xizmatining to'xtashi kabi nosozliklar nazorat ostida sun'iy hosil qilinadi. Bunda faqat umumiy recall emas, balki nosozlik manbasini to'g'ri aniqlash ulushi, tiklash chorasining muvaffaqiyat darajasi, qayta tiklanish vaqti va tiklash uchun sarflangan energiyani ham alohida baholash maqsadga muvofiq.

Xulosa

Ko'p qatlamli IoT tizimida sensor, hisoblash va aloqa holatini birgalikda baholash nosozlikka faqat bitta ko'rsatkich asosida javob berishdan ko'ra tizimliroq diagnostika jarayonini tashkil etishga imkon beradi. Taklif etilgan ketma-ketlik anomaliyani aniqlash, ehtimoliy manbani ajratish, xavfsiz boshqaruv chorasini bajarish va natijani qayta tekshirish bosqichlarini birlashtiradi. Hozirgi natijalar imitatsion baholash bilan cheklangan; nosozlik lokalizatsiyasi va tiklash mexanizmlarining amaliy samaradorligi real prototipda alohida tasdiqlanishi lozim.

Foydalanilgan adabiyotlar:

1. Chandola V., Banerjee A., Kumar V. Anomaly Detection: A Survey. ACM Computing Surveys. 2009;41(3):1–58. <https://doi.org/10.1145/1541880.1541882>
2. Du M., Li F., Zheng G., Srikumar V. DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning. ACM CCS 2017. pp. 1285–1298. <https://doi.org/10.1145/3133956.3134015>
3. Meng W. et al. LogAnomaly: Unsupervised Detection of Sequential and Quantitative Anomalies in Unstructured Logs. IJCAI 2019. pp. 4739–4745. <https://doi.org/10.24963/ijcai.2019/658>
4. Carvalho T.P. et al. A Systematic Literature Review of Machine Learning Methods Applied to Predictive Maintenance. Computers & Industrial Engineering. 2019;137:106024. <https://doi.org/10.1016/j.cie.2019.106024>
5. OASIS. MQTT Version 5.0. OASIS Standard. 2019. <https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html>
6. ISO/IEC 30141:2018. Internet of Things Reference Architecture. <https://www.iso.org/standard/65695.html>