

IoT TIZIMLARIDA MA'LUMOT UZATISH ISHONCHLILIGI: PROTOKOLLAR IMKONIYATLARI VA TIZIMLI CHEKLOVLAR TAHLILI

Abdujapparova Mubarak Baltabayevna

Muhammad al-Xorazmiy nomidagi TATU

“Telekommunikatsiya injiniringi” kafedrası mudiri PhD, dotsent

mubarakabd846@gmail.com

Muradova Alevtina Aleksandrovna

Muhammad al-Xorazmiy nomidagi TATU

“Telekommunikatsiya injiniringi” kafedrası PhD, dotsent

a.muradova1982@inbox.ru

Qobilov Tolmas Yusup o'g'li

Muhammad al-Xorazmiy nomidagi TATU, “Telekommunikatsiya injiniringi”

kafedrası 2-bosqich magistranti

dantes6699@gmail.com

Annotatsiya. Ushbu maqolada Internet of Things (IoT) tizimlarida ma'lumotlarni uzatish ishonchliligini ta'minlashning ilmiy-texnik muammolari tadqiq etilgan. Tadqiqot doirasida IoT qurilmalari o'rtasidagi muloqot protokollarining (MQTT, CoAP, 6LoWPAN, LoRaWAN) imkoniyatlari hamda tizimning hayotiyiligini belgilovchi energiya samaradorligi, spektral tirbandlik va heterogenlik kabi tizimli cheklovlar qiyosiy tahlil qilingan. Maqolada resursi cheklangan qurilmalarda ma'lumotlar butunligini ta'minlash va kechikishlarni minimallashtirish bo'yicha takliflar ilgari surilgan.

Kalit so'zlar: IoT, MQTT, 6LoWPAN, ishonchlilik, energiya samaradorligi, QoS, spektral tirbandlik, heterogenlik, Edge Computing.

Abstract. This article examines the scientific and technical problems of ensuring the reliability of data transmission in Internet of Things (IoT) systems. The research provides a comparative analysis of the capabilities of communication

protocols between IoT devices (MQTT, CoAP, 6LoWPAN, LoRaWAN) and the systemic constraints that determine the viability of the system, such as energy efficiency, spectral congestion, and heterogeneity. The article presents proposals for ensuring data integrity and minimizing delays in resource-constrained devices.

Keywords: IoT, MQTT, 6LoWPAN, reliability, energy efficiency, QoS, spectral congestion, heterogeneity, Edge Computing.

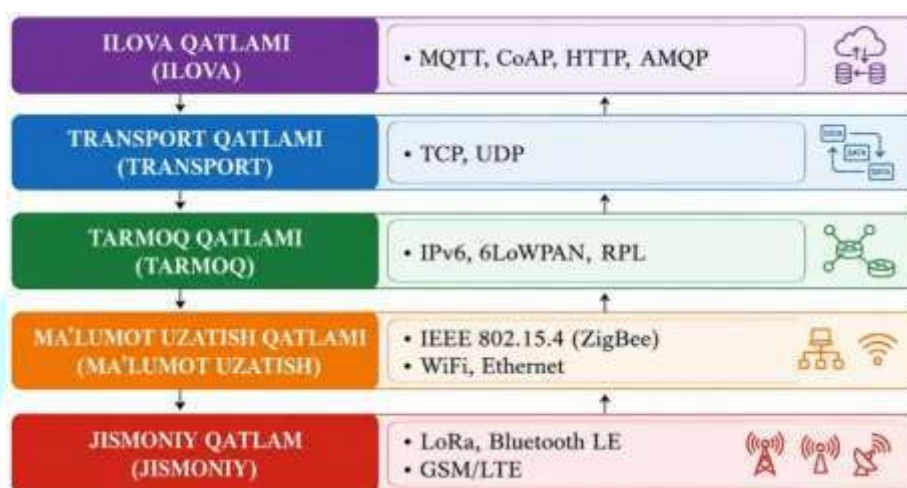
Аннотация. В данной статье рассматриваются научно-технические проблемы обеспечения надежности передачи данных в системах Интернета вещей (IoT). В рамках исследования проводится сравнительный анализ возможностей протоколов связи между устройствами IoT (MQTT, CoAP, 6LoWPAN, LoRaWAN) и системных ограничений, определяющих работоспособность системы, таких как энергоэффективность, перегрузка спектра и гетерогенность. В статье предлагаются решения для обеспечения целостности данных и минимизации задержек в устройствах с ограниченными ресурсами.

Ключевые слова: IoT, MQTT, 6LoWPAN, надежность, энергоэффективность, QoS, перегрузка спектра, гетерогенность, граничные вычисления.

Kirish. Bugungi kunda raqamli transformatsiya jarayonlarining eng muhim bo'g'ini Internet of Things (IoT) hisoblanadi. IoT konseptual jihatdan milliardlab avtonom qurilmalarni global tarmoqqa birlashtirishni nazarda tutadi [1]. Ushbu tizimlarning samaradorligi nafaqat qurilmalar soni, balki ular o'rtasida ma'lumotlarning qanchalik ishonchli va o'z vaqtida yetkazib berilishi bilan o'lchanadi. Telekommunikatsiya sohasida IoT protokollari mashinalararo (M2M) aloqani osonlashtiruvchi standartlar to'plami bo'lib, ular tizimning ishonchlilik darajasini belgilovchi asosiy "til" hisoblanadi. Mazkur maqolada Internet of Things (IoT) tarmoqlarida ma'lumot uzatishdagi muammolar va ularni bartaraf tahlil qilinadi.

Asosiy qism. IoT tarmoq protokollari axborot almashinuvi va mashinadan mashinaga (M2M) aloqasini osonlashtiradigan standartlar va qoidalar to'plamidir.

IoT platformalari sanoat muhitida avtomatlashtirish va unumdorlikni oshirishdan yangi boshqaruv modellarini yaratishgacha bo‘lgan ko‘plab afzalliklarni taqdim etadi. Ularning ishlashi uchun IoT tarmoqlarida qo‘llaniladigan ma‘lumotlar protokollari besh qatlamli modelga asoslanadi: ilova, tarmoq, transport, jismoniy va ma‘lumotlar havolasi qatlamlari [1].



1-rasm. IoT protokollarining iyerarxik stek modeli (TCP/IP stack)

Ilova va seans darajasidagi protokollar. 1. MQTT (Message Queuing Telemetry Transport): ushbu protokol “Publisher-Subscriber” (ma‘lumot uzatuvchi va qabul qiluvchi) modeli asosida ishlaydi. U ochiq standart bo‘lib, o‘zaro ishlash, va energiya samaradorligi yuqori. 2. CoAP (Constrained Application Protocol): cheklangan tugunlar uchun mo‘ljallangan bo‘lib, UDP protokoli ustida ishlaydi va past kechikish vaqtini ta‘minlaydi.

Tarmoq va inkapsulyatsiya protokollari. Past quvvatli qurilmalar uchun.

1. 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) texnologiyasi muhim ahamiyatga ega. U IPv6 ning siqilgan versiyasi bo‘lib, har bir IoT qurilmasiga o‘z IP-manziliga ega bo‘lish imkonini beradi, bu esa tizim masshtablanuvchanligini oshiradi.

2. LPWAN texnologiyalari: uzoq masofali aloqa uchun LoRaWAN protokoli ajralib turadi. Uning kuchi qishloq sharoitida 30 km gacha ma‘lumot uzatish imkoniyatidadir. Bu “aqlli shahar” loyihalari uchun ishonchli aloqa kanalini yaratadi

[3].

Ushbu qatlamlarda ishlovchi asosiy protokollarning texnik imkoniyatlarini, ularning ma'lumotlarni uzatish tezligi, ishonchlilik ko'rsatkichlari hamda resurs tejamlilik xususiyatlarini tizimli ravishda yanada chuqurroq va kengroq tahlil qilish maqsadida quyidagi 1-jadvalda keltirilgan qiyosiy ma'lumotlarni ko'rib chiqishimiz maqsadga muvofiqdir.

1-jadval

Internet of Things (IoT) tarmoq protokollarining qiyosiy texnik tavsiflari.

Protokol	Asosiy model	Ma'lumot uzatish turi	Quvvat sarfi	Masofa	Qo'llash sohasi
MQTT	Publish/Subscriber	TCP/IP	Past	Global (Internet orqali)	Bulutli aloqa, telemetriya
CoAP	Client/Server	UDP	Juda past	Global (Internet orqali)	Sensor tarmoqlari
6LoWPAN	IPv6 integratsiyasi	IP/UDP	Juda past	Qisqa masofa (100–500 m)	Aqlli binolar, uylarni avtomatlashtirish
LoRaWAN	Yulduzsimon (Star)	RF (LPWAN)	Juda past	Uzoq masofa (15–30 km gacha)	Smart city, qishloq xo'jaligi

Internet of Things (IoT) tarmoqlarida ishonchlilik faqat texnik sozlamalariga emas, tarmoqning arxitekturaviy cheklovlari va resurslar balansiga ham bog'liq.

1-Resurslar cheklanganligi va energiya samaradorligi. IoT tugunida energiya sarfining 70-80% qismi ma'lumot uzatish (Communication) jarayoniga to'g'ri keladi. Signal masofasi (d) va zarur bo'lgan nurlanish quvvati (P) o'rtasidagi bog'liqlik quyidagi formula bilan ifodalanadi:

$$P \propto d^n, (2 \leq n \leq 4), \quad (1)$$

bu yerda: P - signalni uzatish uchun sarflanadigan quvvat; d - uzatish masofasi; n - muhitning so'nish koeffitsiyenti (ochiq joyda 2 ga, to'siqlar mavjud joyda 4 ga yaqin).

Ushbu ziddiyat (trade-off) ishonchlilikka bevosita ta'sir qiladi. Energiya tejash maqsadida paketlarni qayta jo'natish sonining cheklanishi ma'lumot yo'qolishi ehtimolini oshiradi.

2-Spektral zichlik va tarmoq tirbandligi. Millionlab qurilmalar litsenziyalanmagan ISM diapazonlarida (2.4 GHz) ishlaydi. ALOHA- asosli tasodifiy kirish tamoyili qurilmalar zichligi ortgan sharoitda paketlar to'qnashuvini keltirib chiqaradi. Bu esa signal-shovqin nisbatining (SNR) pasayishiga va signallarning "ifloslanishi"ga (spectral noise) olib keladi. Interferensiya sharoitida signalning ishonchliligini baholashda SNR (Signal-to-Noise Ratio) ko'rsatkichi muhim ahamiyatga ega:

$$SRN = \frac{P_{signal}}{P_{shovqin}}, \quad (2)$$

Interferensiya natijasida SNR ko'rsatkichi pasayadi, bu esa qabul qiluvchi qurilmaning signalni foydali ma'lumot sifatida taniy olmasligiga sabab bo'ladi. Ko'pgina IoT protokollari ALOHA-asosli tasodifiy kirish tamoyiliga tayanganligi sababli, muvaffaqiyatli uzatish ehtimoli (S) tarmoq yuklamasiga bog'liq holda quyidagicha aniqlanadi:

$$S = G \cdot e^{-2G}, \quad (3)$$

G - ma'lum bir vaqt birligi ichida tarmoqdagi barcha qurilmalar tomonidan yuborishga harakat qilingan jami paketlar soni.

3-Kechikishlar (Latency) va xizmat ko'rsatish sifati (QoS). Kritik tizimlarda (tibbiyot, transport) umumiy kechikish (End-to-End Latency) bir necha bosqichli jarayonlardan, jumladan ishlov berish, navbat kutish va uzatish kechikishlaridan iborat. "Best-effort" tamoyili asosida ishlovchi an'anaviy protokollar yetkazib berish vaqtini kafolatlay olmaydi, bu esa deterministik tizimlar uchun hayotiy xavf tug'diradi. Umumiy kechikish (End-to-End Latency) quyidagi komponentlardan iborat:

1. Ishlov berish kechikishi (Processing Delay).
2. Navbat kutish kechikishi (Queuing Delay).

3. Uzatish kechikishi (Transmission Delay).

$$T_{jami} = T_{ishlov} + T_{navbat} + T_{uzat} + T_{tarqat}, \quad (4)$$

T_{jami} - ma'lumot uzatishdagi umumiy kechikish (End-to-End Latency); T_{ishlov} - ishlov berish kechikishi (paketlash va shifrlash vaqti); T_{navbat} - navbat kutish kechikishi (tugun buferidagi vaqt); T_{uzat} - uzatish kechikishi (ma'lumot hajmi va kanal tezligiga bog'liq vaqt); T_{tarqat} - tarqalish kechikishi (signalning fizik muhitda bosib o'tgan masofasiga bog'liq vaqt).

Yuqorida qayd etilgan deterministik kechikishlarni minimallashtirish va adaptiv marshrutlashni ta'minlash uchun Q-learning algoritmi asosidagi intellektual tizimlarni joriy etish taklif etiladi. Ushbu algoritmi IoT tugunlariga o'zgaruvchan tarmoq muhitida eng maqbul yo'lni mustaqil tanlash imkonini beradi [4]. Agent (tugun) har bir muvaffaqiyatli uzatilgan paket uchun "mukofot" olishi quyidagi Bellman tenglamasi orqali ifodalanadi:

$$Q_{s,a} \leftarrow Q_{s,a} + \alpha \left[R + \gamma \max_{a'} Q_{(s',a')} - Q_{(s,a)} \right], \quad (5)$$

Bu yerda: $Q(s,a)$ - joriy holat (s) va tanlangan harakat (a) uchun kutilayotgan foyda; (α) - o'qish tezligi (learning rate); (R) - olingan mukofot (masalan, paket muvaffaqiyatli yetib borgandagi ko'rsatkich); (γ) - diskontlash koeffitsiyenti (kelajakdagi mukofotlarning ahamiyati).

Bu yondashuv an'anaviy statik protokollardan farqli o'laroq, tarmoq o'tkazuvchanligini 15-20% ga oshirish imkonini beradi [5].

Ma'lumotlar sintaksisi va semantikasi nomutanosibliklari tizimlararo moslashuvchanlikni (interoperability) cheklaydi. Yagona global standartning yo'qligi esa tizimni muayyan ishlab chiqaruvchi texnologiyasiga bog'lab qo'yadi (Vendor Lock-in). Ushbu to'siqlarni bartaraf etish uchun Middleware qatlami va ontologik modellarni joriy etish talab etiladi. Shu bilan birga, IoT tarmoqlarida aniqlangan kechikish (latency) muammosini tubdan hal qilish uchun Edge Computing (chekka hisoblashlar) arxitekturasini tatbiq etish strategik ahamiyatga ega. Bu ma'lumotlarni

markaziy serverga yubormasdan, manbaning o'zida qayta ishlash orqali kechikish vaqtini 30-40% gacha qisqartirish imkonini beradi. Tarmoq xavfsizligini ta'minlashda esa Blockchain (blokcheyn) texnologiyasiga asoslangan markazlashmagan modellarni joriy etish, resursi cheklangan qurilmalarda ma'lumotlar daxlsizligini kafolatlovchi eng samarali yechim hisoblanadi [6].

Xulosa. Tadqiqot natijalari shuni ko'rsatadiki, IoT tarmoqlarida ishonchlilikni oshirish uchun faqat texnik sozlamalar yetarli emas. Tizimli cheklovlarni bartaraf etish uchun Edge Computing texnologiyasini joriy etish orqali kechikishlarni kamaytirish, resursi cheklangan qurilmalarda yengil vaznli kriptografik algoritmlarni qo'llash va standartlararo moslashuvchanlikni ta'minlovchi ochiq API interfeyslarini tadbiq etish lozim. Shuningdek, resurslar tejamkorligi va ma'lumotlar daxlsizligi o'rtasidagi muvozanatni ta'minlash uchun adaptiv xatoliklarni tuzatish mexanizmlarini ishlab chiqish bugungi kunning dolzarb vazifasidir.

O'tkazilgan tahlillar va o'rganishlar shuni ko'rsatadiki, IoT ekotizimida ishonchlilikni yangi bosqichga olib chiqishda intellektual algoritmlari katta o'rin va ahamiyat kasb etadi. Xususan, Q-learning algoritmi asosidagi intellektual marshrutlash tizimlarini joriy etish orqali tarmoqning dinamik o'zgarishlarga moslashuvchanligini ta'minlash, energiya sarfini optimallashtirish bilan birga o'tkazuvchanlik qobiliyatini 15-20% ga oshirish imkonini beradi. IoT tizimlarining barqarorligini yanada oshirish uchun: ma'lumotlarni qayta ishlashda markazlashgan bulutli serverlardan Edge arxitekturasiga o'tish (bu RTT kechikishlarini minimallashtiradi); xavfsizlikni ta'minlashda resurs tejamkor Blockchain modellarini integratsiya qilish (bu ma'lumotlar daxlsizligini kafolatlaydi) strategik zarurat hisoblanadi.

Apparat va algoritmik yechimlarning kompleks birlashtirilishi - "Raqamli O'zbekiston" strategiyasi doirasidagi "aqlli" tizimlarning ishonchli ishlashi uchun ilmiy asos bo'lib xizmat qiladi.

Foydalanilgan adabiyotlar.

1. Al-Fuqaha A, et al. “Internet of Things: A Survey on Enablers, Protocols, and Applications”, IEEE Communications Surveys & Tutorials, 2015.
2. Aliev R.R. IoT tizimlari arxitekturasini va protokollari. Darslik. – Toshkent: “Fan va texnologiya”, 2022. – 210 b.
3. Dorri A., Kanhere S. S. “Blockchain for IoT Security and Privacy”, IEEE Communications Magazine, 2017.
4. Matchonov S., To‘rayev B. Raqamli texnologiyalar va sun‘iy intellekt asoslari. – Toshkent: “O‘zbekiston”, 2021. – 142 b.
5. Nie S, et al. “Intelligent Routing Protocol for IoT Networks Based on Reinforcement Learning”, IEEE Internet of Things Journal, vol. 7, pp. 6112–6123, 2020.
6. Sutton R. S., Barto A. G. Reinforcement Learning: An Introduction. – MIT Press, 2018.