

O'ZBEKISTON RESPUBLIKASI

OLIY TA'LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

FARG'ONA DAVLAT UNIVERSITETI

**FarDU.
ILMIY
XABARLAR**

1995-yildan nashr etiladi
Yilda 6 marta chiqadi

6-2025
ANIQ FANLAR

**НАУЧНЫЙ
ВЕСТНИК.
ФерГУ**

Издаётся с 1995 года
Выходит 6 раз в год

MATEMATIKA

Sh.T.Nishonova, M.S.Sodiqova

Elliptiko-giperbolik tipdagi tenglama uchun bir chegaraviy masalaning
bir qiymatli yechimi..... 4

N.S.Ikramova, M.T.Yunusalieva

Solvability of a mixed problem for a degenerate sub-diffusion
equation in a rectangular domain 12

INFORMATIKA

B.A.Umarov

IoT qurilmalarini tarmoqqa ulashdagi protokollar tahlili 25

B.A.Umarov, Sh.M.Kimsanboyeva

Tarmoq energiya samaradorligini oshirish strategiyalari..... 29

FIZIKA-TEXNIKA

G.Q.Muxamadaliyeva, M.R.Akbaraliyeva

Tabiiy va sun'iy tolalarni o'quvchilarga o'rgatishda steam va
smart metodlari orqali o'qitish samaradorligini oshirish..... 32

M.F.Solijonova

Texnologik ta'lim yo'nalishi talabalariga zamonaviy innovatsion pedagogik
texnologiyalardan foydalanib 'metallarning xossalarini o'qitish 36

J.R.Bobojonova

Umumta'lim maktablarida ta'lim samaradorligini oshirishda interfaol
usullarining roli 40

Sh.Sh.Shuxratov, S.A.Ismoilova

Alohida ta'lim ehtiyojlariga ega o'quvchilar uchun interfaol
pedagogik yondashuvlar 44

C.M.Отажонов, P.H.Эргашев, K.A.Ботиров, Д.Х.Нажмиддинова

Оптические свойство и рентгеноструктурный анализ тонких
пленок сdte с глубокими примесными уровнями 49

M.X.Рахмонкулов

Цели и методы изучения радиационных дефектов в полупроводниках 57

I.V.Xoldarova, Sh.A.Ibragimova

Mehnatsevarlik tushunchasining asosiy sotsiomadaniy
va tarbiyaviy kontsepsiyalari 61

ILMIY AXBOROT

G.X.Ismoilova

Xalq hunarmandchiligi va milliy qadriyatlarni umumiy o'rta ta'lim
maktablarida smart usulidan foydalanib o'qitish samaradorligi 67

F.R.Muxitdinova

Magnit maydondagi p-n o'tish kuchlanishining turli temperaturalarda o'zgarishi 671



UO'K: 004.738.5:004.773

IOT QURILMALARINI TARMOQQA ULASHDAGI PROTOKOLLAR TAHLILI

АНАЛИЗ ПРОТОКОЛОВ ПОДКЛЮЧЕНИЯ УСТРОЙСТВ IOT К СЕТИ

ANALYSIS OF PROTOCOLS IN CONNECTING IOT DEVICES TO THE NETWORK

Umarov Bekzod Azizovich 

Farg'ona davlat universiteti amaliy matematika va informatika kafedrası dotsenti p.f.f.d(PhD).

Annotatsiya

Ushbu maqola Internet of Things (IoT) qurilmalarini tarmoqqa ulashda keng qo'llaniladigan protokollarni tizimli tahlil qiladi. Ishda yengil vaznli va cheklangan resurslarga moslashgan transport va ilova qatlam protokollari — MQTT, CoAP, LwM2M kabi yechimlar, shuningdek past quvvatli keng hududli tarmoqlar uchun LoRaWAN va NB-IoT singari LPWAN texnologiyalari ko'rib chiqiladi. Maqolada protokollarning arxitektura xususiyatlari, qurilma resurslariga ta'siri, xavfsizlik mexanizmlari va amaliy joriy etishdagi cheklovlar solishtiriladi. Tahlil natijalari bir qancha qo'llanmali tavsiyalar va protokollarni tanlashda hisobga olinishi lozim bo'lgan mezonlarni beradi.

Аннотация

В данной статье проводится системный анализ протоколов, широко применяемых при подключении устройств Интернета вещей (IoT) к сети. Рассматриваются легковесные и адаптированные к ограниченным ресурсам транспортные и прикладные протоколы, такие как MQTT, CoAP, LwM2M, а также технологии LPWAN для сетей с низким энергопотреблением и широким покрытием, включая LoRaWAN и NB-IoT. В статье сопоставляются архитектурные особенности протоколов, их влияние на ресурсы устройств, механизмы безопасности и ограничения при практическом внедрении. Результаты анализа предоставляют ряд практических рекомендаций и критериев, которые следует учитывать при выборе протоколов.

Abstract

This article presents a systematic analysis of protocols commonly used for connecting Internet of Things (IoT) devices to networks. The study examines lightweight and resource-constrained transport and application layer protocols such as MQTT, CoAP, and LwM2M, as well as LPWAN technologies designed for low-power wide-area networks, including LoRaWAN and NB-IoT. The paper compares the architectural features of the protocols, their impact on device resources, security mechanisms, and limitations in practical implementation. The analysis results provide a set of practical recommendations and criteria that should be considered when selecting appropriate protocols.

Kalit so'zlar: IoT, MQTT, CoAP, LwM2M, LoRaWAN, NB-IoT, 6LoWPAN, protokollar tahlili, xavfsizlik, resurs cheklovlari.

Ключевые слова: IoT, MQTT, CoAP, LwM2M, LoRaWAN, NB-IoT, 6LoWPAN, анализ протоколов, безопасность, ограниченные ресурсы.

Key words: IoT, MQTT, CoAP, LwM2M, LoRaWAN, NB-IoT, 6LoWPAN, protocol analysis, security, resource constraints.

KIRISH (ВВЕДЕНИЕ/INTRODUCTION)

IoT ekotizimi ko'plab turdagi qurilmalardan tashkil topadi: oddiy sensordan tortib murakkab aktuatorgacha bo'lgan qurilmalar tarmoqqa ulangan holda ma'lumot uzatadi va qabul qiladi. Bu qurilmalar ko'pincha hisoblash quvvati, xotira va energiyaga cheklovlarga ega bo'lib, an'anaviy veb-protokollar bilan to'g'ridan-to'g'ri ishlashi noqulay yoki samarasiz bo'lishi mumkin. Shu sababli IoT uchun maxsus mo'ljallangan protokollar va standartlar paydo bo'ldi: ular cheklangan resurslarga moslashgan, tarmoqqa va energiyaga samarali, hamda xavfsizlik va boshqaruv imkoniyatlarini inobatga olgan. Ushbu maqola ularning arxitekturaviy xususiyatlarini, afzallik va kamchiliklarini, shuningdek real dunyo ssenariylarida qo'llanish omillarini tahlil qiladi.

ADABIYOTLAR TAHLILI VA METODOLOGIYA (LITERATURA I METODOLOGIYA /METHODS)

IoT protokollari bo'yicha adabiyotlarda ikki katta yo'nalish ajraladi: ilova/transport qatlam protokollari va tarmoq/qatlam protokollari hamda nazorat va boshqaruv mexanizmlari.

Ilova va transport qatlamida eng keng tarqalgan yechimlardan biri — MQTT bo'lib, u publish/subscribe (nashr/obuna) paradigmaga asoslangan yengil vaznli tashuv protokoli sifatida ishlab chiqilgan. MQTT masofaviy, cheklangan resursli qurilmalar bilan kam band kengliklarda ishonchli ikki tomonlama muloqot o'rnatish imkonini beradi va ko'plab sanoat amaliyotlarida keng qo'llaniladi. MQTTga oid standart va so'nggi versiyalar OASIS tomonidan rasmiylashtirilgan va unga xos xabar yetkazib berish kafolat darajalari (QoS) hamda ulanish holatini boshqarish mexanizmlari mavjud. Resurslari qattiq cheklangan qurilmalar uchun CoAP (Constrained Application Protocol) kabi HTTP-ga mos, ammo yengil vaznli protokollar taklif etilgan. CoAP RESTful tamoyillarga mos keladi, UDP ustida ishlaydi va kichik paketlar hamda kontekstga mos qayta jo'natish mexanizmlari orqali yuqori samaradorlikni ta'minlaydi. CoAP bilan yonma-yon ishlaydigan DTLS tashqi xavfsizlik qatlamini berishi mumkin, bu esa UDP asosidagi ilova qatlamining xavfsizligini ta'minlash uchun qo'llanadi. Boshqaruv va qurilma menejmenti nuqtai nazaridan LwM2M (Lightweight M2M) kabi spetsifikatsiyalar uzoq muddatli masofadan monitoring, konfiguratsiya va firmware yangilash samarali mexanizmlarini taqdim etadi. Bunday protokollar tarmoq boshqaruvi va qattiq xavfsizlik talablarini qondirishga mo'ljallangan. Tarmoq qatlamida esa LPWAN texnologiyalari — LoRaWAN va mobil operatorlar uchun NB-IoT — uzoq masofali va past energiya xarajatli ulanish talab qilinadigan ssenariylar uchun keng qo'llaniladi. LoRaWAN o'zining spektral samaradorligi va keng qamrov imkoniyati bilan kichik paketlar uchun ideal bo'lsa, NB-IoT mobil operator infratuzilmasiga integratsiyalashgan holda keng qamrov va ishonchlilik kafolatlarini beradi.

Adabiyotlarda shuningdek IPv6-ning cheklangan simli/wireless tarmoqlarda ishlatilishini ta'minlovchi 6LoWPAN kabi texnikalar (IPv6 header compressiyasi, fragmentatsiya va manzilaviy optimizatsiya) muhim o'rin egallaydi. Bu texnikalar zamonaviy IoT tarmoqlarining Internet bilan to'liq mosligini ta'minlashga yordam beradi. Umuman olganda, adabiyotlar tarmoq sharoitlari, energiya cheklavlari, kechikish talablari va xavfsizlik talablariga qarab protokollar to'plamini tanlash kerakligini ta'kidlaydi. Har bir protokolning o'z domeni va ssenariylari mavjud bo'lib, ular orasidagi tanlovni amalga oshirish uchun ko'p mezonli baholash zarur.

NATIJALAR (РЕЗУЛЬТАТЫ/RESULTS)

Maqolada protokollarni tahlil qilish uchun quyidagi metodologik yondashuv qo'llandi. Avvalo, protokollar arxitekturasini formali jihatdan taqqoslandi: qatlamlar (transport/ilova), ishlash paradigmasi (publish/subscribe vs request/response), xavfsizlik imkoniyatlari, uskunalar va tarmoq resurslariga bo'lgan talablar, energiya xarajatlari va kengaytirilish (scalability) mezonlari ko'rsatildi.

Ikkinchi bosqich sifatida amaliy ssenariylar ishlab chiqildi. Har bir protokol turli IoT ssenariylarga mosligi jihatidan baholandi. Ssenariylar quyidagilarni o'z ichiga oladi: uy-joy aqlli qurilmalari (smart home), sanoat monitoring (industrial telemetry), chekka joylarda sensor tarmoqlari (environmental sensing), va mobil ob'ektlarga o'rnatilgan qurilmalar (asset tracking). Har bir ssenariy uchun mos keluvchi protokol yoki protokollar guruhi aniqlanib, ular uchun quyidagi parametrlar baholandi: o'rnatish murakkabligi, energiya/bit ko'rsatkichi, kechikish va ishonchlilik, xavfsizlik darajasi va qo'llab-quvvatlanish (ecosystem) holati.

Uchinchi bosqich — xavfsizlik va boshqaruv talablari bo'yicha solishtirish. Bu yerda autentifikatsiya mexanizmlari, ma'lumot shifrlash, sertifikat/kalit boshqaruvi, firmware yangilash imkoniyatlari va xujumlarga (replay, MITM, DOS) chidamlilik o'rganildi.

Maqolada ilmiy tahlil nazariy asoslarda va soha yetakchi spetsifikatsiyalariga (RFC va konsorsium hujjatlari) tayangan holda o'tkazildi; zarur joylarda amaliy misollar va dizayn tavsiyalari keltirildi. Muqobil yoki yangi yechimlar bilan bog'liq g'oyalar — maqolada taklif qilingan tavsiyalar — muallifning tajribaviy va nazariy tahlil natijasidir.

Tahlil natijalari protokollar orasidagi farqlar va har bir yondashuvning amaliy cheklavlari hamda afzalliklarini yanada chuqurroq ochib berdi. Ilova va transport qatlamida ko'rib chiqilgan protokollar turli operatsion muhitlar va qurilma resurslari sharoitida turlicha xatti-harakat ko'rsatdi. Broker asosidagi publish/subscribe modeli bilan ishlaydigan protokollar o'zining markazlashtirilgan boshqaruv qobiliyati va asinxron xabar almashinuvi bilan ajralib turadi; bu yondashuv monitor qilish va telemetriya yig'ishda qulaylik yaratadi va qurilmalar soni ko'payganda ham tizimni boshqarishni soddalashtiradi. Shu bilan birga, markaziy broker nuqtasining yukini va uning xavfsizlik talablarini hisobga olish zarurati paydo bo'ladi, shuningdek, provayder tomonida yuqori ishonchlilikni

INFORMATIKA

ta'minlash uchun qo'shimcha mexanizmlar joriy etilishi lozim. So'nggi tahlillar shuni ko'rsatdiki, request/response paradigmasini qo'llovchi yengil vaznli protokollar UDP ustida ishlaganda paket uzatishning samaradorligi va tarmoq resurslaridan tejimli foydalanish imkoniyatini beradi. Bunday protokollar RESTful interfeys orqali mavjud veb-ekotizimlarga integratsiyani yengillashtiradi va cheklangan resursli qurilmalar uchun moslashuvchanlik taklif qiladi. Biroq UDP ustida ishlash xavfsizlik nuqtai nazaridan qo'shimcha qatlamlarni talab qiladi, chunki shifrlash va autentifikatsiya mexanizmlari UDP xususiyatlariga mos ravishda amalga oshirilishi lozim. Shu tariqa, ilova darajasidagi samaradorlik bilan xavfsizlik va ishonchlilik talablari o'rtasida muvozanatni ta'minlash muhim ahamiyat kasb etadi. Radio va tarmoq qatlamida olib borilgan baholashdan ko'rinib turibdiki, past energiya va uzoq qamrov talab qilinadigan ssenariylar uchun mo'ljallangan tarmoqlar butunlay boshqacha kompromisslarni talab qiladi. Keng maydonni qamrab olish va batareya umrini maksimal darajada oshirish imkoniyatini beruvchi texnologiyalar kichik paketlar va past bitrateni qo'llab-quvvatlash orqali chekka joylardagi sensorlar uchun ideal yechimni taklif etadi. Bunday tarmoqlarda real-vaqt talab qilinadigan xizmatlar ishlatilganda kechikish va bosqichma-bosqich yetkazib berish mexanizmlari bilan bog'liq muammolar yuzaga keladi; shuning uchun ilova talablari tarmoq tanlovida asosiy yumshatish nuqtasi bo'lishi kerak.

Mobil operator infratuzilmasiga moslashgan texnologiyalar esa tarmoq qamrovi va ishonchlilikini oshirish hamda operator tomonidan taqdim etiladigan qo'llab-quvvatlash xizmatlaridan foydalanish imkonini beradi. Bunday yechimlar yordamida qurilmalar tarmoq tomonidan boshqariladigan xavfsizlik va sifat xususiyatlariga ega bo'lib, keng qamrov va tarmoq xizmatlariga munosib ulanishni ta'minlaydi. Shu bilan birga, ushbu platformalarning xarajat tuzilmasi va operatorga bog'liqligi loyihaning moliyaviy va boshqaruv jihatlariga ta'sir etadi.

Qurilmalarni masofadan boshqarish va kuzatish nuqtai nazaridan ko'rilgan protokollar boshqaruv, konfiguratsiya va firmware yangilash kabi funksiyalarni ta'minlash jarayonida o'zlarini samarali namoyon etdi. Bunday mexanizmlar tizimning xizmat ko'rsatish muddatini uzaytiradi va texnik xizmat ko'rsatish xarajatlarini kamaytiradi, biroq ular ham tarmoq cheklovlari va xavfsizlik talablarini inobatga olgan holda loyihalashtirilishi lozim. Firmware yangilash kabi og'ir jarayonlar past bitrateli tarmoqlarda murakkablik tug'diradi va bu holat xavfsizlik siyosatlarini loyihalashda maxsus yechimlar talab qilinishiga olib keladi.

Xavfsizlikka oid tahlillar ko'rsatdiki, autentifikatsiya va shifrlash mexanizmlarining mavjudligi va ularning boshqaruv usullari protokollar tanlovida muhim rol o'ynaydi. Ilovalar real dunyoda turli turdagi hujumlarga duch kelishi mumkinligi sababli kalitlarni boshqarish, sertifikat aylanishi va kerak bo'lganda kalitlarni yangilash imkoniyatlari tizim barqarorligi uchun zarur hisoblanadi. Shuningdek, ba'zi protokollar o'z ichiga xavfsizlik funksiyalarini nazorat darajasi bilan integratsiyalashgan bo'lsa-da, cheklangan resursga ega qurilmalarda bu funksiyalarni amalga oshirish qo'shimcha dizayn choralari talab qiladi.

Tahlil natijalari shuni ham ko'rsatadiki, protokollarni bir-biri bilan kombinatsiyalash yondashuvi ko'pincha eng maqbul natijani beradi. Masalan, uzoq muddat ishlash va past energiya talabi bo'lgan qurilmalar uchun radio qatlamida energiya tejankor texnologiyani tanlab, ilova qatlamida yengil vaznli protokollar va boshqaruv darajasida masofadan yangilash imkoniyatini ta'minlovchi standartlarni joriy etish samarali yechimdir. Bunday kombinatsiyalar tizimning umumiy ishlash samaradorligini oshiradi, tarmoq resurslaridan oqilona foydalanishni ta'minlaydi va xavfsizlikni muvofiqlashtirish imkonini beradi.

Umuman olganda, olingan natijalar protokollar tanlovining kontekstga bog'liqligini mustahkamladi. Loyihaning maqsadi, qurilma cheklovlari, tarmoq muhitining xususiyatlari va xavfsizlik bo'yicha talablar e'tiborga olinmagan holda yagona protokol yoki standartga tayangan yechim real amaliyotda o'zini samarali ko'rsatmasligi mumkin. Shu sababli protokollarni tanlash jarayonida tizim darajasida chuqur baholash, turli kombinatsiyalarni pilot rejimda sinab ko'rish va xavfsizlik hamda boshqaruvga alohida e'tibor berish tavsiya etiladi.

MUHOKAMA (ОБСУЖДЕНИЕ/DISCUSSION)

Tahlil ko'rsatdiki, protokollar orasida universal «eng yaxshi» tanlov mavjud emas; protokol tanlovi ilovaning talablari, qurilma imkoniyatlari va tarmoq muhitiga bog'liq bo'ladi. Masalan, energiya tejash va uzoq muddat ishlash talab qilinadigan chekka sensorlar uchun LoRaWAN afzal bo'lsa, operator infratuzilmasiga moslashgan qurilmalar uchun NB-IoT afzalliklar beradi. MQTT va

CoAP esa ilova darajasida turli kompromisslarni taklif qiladi: MQTT broker — markazlashtirilgan boshqaruv va asinxronlikni yaxshilaydi, CoAP esa RESTful arxitektura orqali mavjud veb xizmatlar bilan integratsiyani osonlashtiradi.

Xavfsizlik sohasida esa o'ziga xos muammolar mavjud. Resinli xabarlar (QoS 2 yoki DTLS bilan) haqiqiy dunyoda qo'llanilganda ham, kalitlarni xavfsiz saqlash va yangilash mexanizmini ta'minlash qiyinchiliklari ko'p hollarda hal qilinishi kerak. Shuningdek, LPWAN tarmoqlaridagi cheklangan paket hajmi va past bitrate firmware yangilashni murakkablashtiradi, bu esa xavfsizlikni oshirish bo'yicha qo'shimcha dizayn qarorlarini talab qiladi.

Shuningdek, IoT hajmi va heterojenligi tizim integratsiyasi va boshqaruvni murakkablashtiradi. Shu sababli protokollarni tanlashdan oldin tizim darajasida to'liq baholash (energy budget, latency budget, security requirements, maintenance plan) amalga oshirilishi lozim.

XULOSA

Ushbu maqolada IoT qurilmalarini tarmoqqa ulashdagi asosiy protokollar — MQTT, CoAP, LwM2M, LoRaWAN, NB-IoT va ularning tarmoq arxitekturasini, xavfsizlik va resurs talablariga ta'siri tahlil qilindi. Har bir protokol o'ziga xos kuchli va zaif tomonlarga ega bo'lib, amaliy tanlov ilovaning konkret talablari, qurilma cheklavlari va mavjud tarmoq infratuzilmasiga bog'liq. Tavsiya qilinadi: IoT loyihasini boshlashdan avval talablarni (energiya, kechikish, xavfsizlik, kengaytirilish) aniq belgilab, protokollar orasidan bir nechta kombinatsiyani pilot loyihada sinab ko'rish. Kelajak tadqiqotlari protokollar o'rtasidagi dinamik gatewaylar, avtomatik protokol tanlash mexanizmlari va xavfsiz, energiya samarador boshqaruv tizimlarini ishlab chiqishga qaratilishi lozim.

ADABIYOTLAR RO'YXATI

1. OASIS. MQTT — The Standard for IoT Messaging. mqtt.org+1
2. IETF. RFC 7252 — The Constrained Application Protocol (CoAP). datatracker.ietf.org
3. LoRa Alliance. LoRaWAN® Specification v1.1. resources.lora-alliance.org
4. 3GPP. NB-IoT standardization (Release announcement). [3GPP](https://www.3gpp.org)
5. Open Mobile Alliance. Lightweight M2M (LwM2M) specification. openmobilealliance.org
6. IETF. RFC 4944 / 6LoWPAN resources. datatracker.ietf.org+1
7. IETF. RFC 6347 — Datagram Transport Layer Security (DTLS)
8. Umarov B. RAQAMLI TEXNOLOGIYALAR VOSITASIDA PEDAGOGLARNING PROFESSIONAL KOMPETENTLIGINI RIVOJLANTIRISH TAMOIYILLARI //Farg'ona davlat universiteti. – 2023. – №. 3. – C. 5-5.
9. Azizovich U. B. THE DEVELOPMENT OF PROFESSIONAL COMPETENCY OF TEACHERS IN EDUCATIONAL TECHNOLOGY BASED ON DIGITAL TECHNOLOGIES //Eurasian Journal of Mathematical Theory and Computer Sciences. – 2024. – T. 4. – №. 7. – C. 11-14.
10. Azizovich U. B. PEDAGOGICAL-PSYCHOLOGICAL PRINCIPLES OF THE FORMATION OF PROFESSIONAL COMPETENCE //Confrencea. – 2023. – T. 6. – №. 6. – C. 204-212.
11. Umarov B. THE ROLE OF THE PRINCIPLES OF DECENTRALIZATION IN THE CONCEPT OF PUBLIC ADMINISTRATION //The American Journal of Political Science Law and Criminology. – 2023. – T. 5. – №. 02. – C. 62-68.
12. Umarov B. THEORETICAL FOUNDATIONS OF THE ORGANIZATION OF PROFESSIONAL PRACTICE THAT DEVELOPS PROFESSIONAL COMPETENCE BY MEANS OF DIGITAL TECHNOLOGIES //Science and innovation. – 2024. – T. 3. – №. B8. – C. 107-109.
13. Azizovich U. B. THE DEVELOPMENT OF PROFESSIONAL COMPETENCY OF TEACHERS IN EDUCATIONAL TECHNOLOGY BASED ON DIGITAL TECHNOLOGIES //Eurasian Journal of Mathematical Theory and Computer Sciences. – 2024. – T. 4. – №. 7. – C. 11-14.