

IOT-DAGI ALOQA MODELLARI YORDAMIDA QURILMALAR O'RTASIDA MA'LUMOTLARNI UZATISH VA QABUL QILISH

Maxkamov Farxod Aloviddin o'g'li

**“Tashkent International University of Education” (TIUE) universitetida Axborot
texnologiyalari kafedrasi o'qituvchisi.**

E-mail: makhkamovfarkhod@gmail.com

<https://doi.org/10.5281/zenodo.13762671>

Annotatsiya. Ushbu tezisda Internet of Things (IoT) tizimlarida aloqa modellari yordamida qurilmalar o'rtasida ma'lumotlarni yuborish va qabul qilish jarayonlari o'rganiladi. IoT (Internet of Things) texnologiyasi kundalik hayotimizda turli qurilmalar va tizimlar o'rtasida ma'lumotlar uzatish va qabul qilish imkonini beradi. Ushbu texnologiyaning muhim jihati – qurilmalar o'rtasida samarali va xavfsiz aloqa o'rnatishdir. IoT-dagi aloqa modellari, asosan, qurilmalar orasidagi ma'lumot almashinuvi usullarini ta'minlaydi. Bunda turli xil tarmoqlar va protokollar yordamida qurilmalar bir-biri bilan bog'lanadi va real vaqt rejimida ma'lumotlarni almashadi. IoT-da foydalaniladigan asosiy aloqa modellariga markazlashtirilgan, distribyutsiyalangan va aralash modellari kiradi. Markazlashtirilgan modelda barcha ma'lumotlar bir markaziy server orqali boshqariladi. Distribyutsiyalangan modelda esa qurilmalar o'zaro bevosita ma'lumot almashadi. Aralash model esa ikki yondashuvning kombinatsiyasi bo'lib, moslashuvchan va kengaytirilgan tizimlar yaratishga imkon beradi. Shuningdek, IoT tizimlarida turli tarmoqlar (Wi-Fi, Bluetooth, Zigbee) va protokollar (MQTT, CoAP) yordamida aloqa amalga oshiriladi. IoT-dagi aloqa modellari qurilmalarning samarali hamkorligini, ma'lumotlarning tez va ishonchli yetkazilishini hamda xavfsizlikni ta'minlashda muhim rol o'ynaydi. IoT qurilmalari o'rtasidagi samarali va xavfsiz aloqa, ularning funktsionalligini oshirishda muhim ahamiyatga ega. Tezisdagi tahlil aloqa protokollari, arxitektura, ma'lumot almashinuvi mexanizmlari va xavfsizlik masalalarini o'z ichiga oladi. Asosiy maqsad, IoT qurilmalarining ma'lumot almashinuvi jarayonlarini optimallashtirish uchun eng samarali aloqa modellarini aniqlashdir. Ushbu tadqiqot natijalari IoT tizimlarining rivojlanishi va keng qo'llanilishi uchun yangi yo'nalishlar ochishi kutilmoqda.

Kalit so'zlar: IoT (Internet of Things), Aloqa modellari, MQTT, CoAP, Klient-server modeli, Peer-to-peer modeli, Publish-subscribe modeli, IoT xavfsizligi.

DATA TRANSMISSION AND RECEPTION BETWEEN DEVICES USING COMMUNICATION MODELS IN IOT

Farkhod Aloviddinovich Makhkamov

**Teacher at the Department of Information Technologies at “Tashkent International
University of Education” (TIUE).**

E-mail: makhkamovfarkhod@gmail.com

Abstract. This thesis studies the processes of sending and receiving data between devices using communication models in Internet of Things (IoT) systems. IoT (Internet of Things) technology enables the transmission and reception of data between various devices and systems in our daily life. An important aspect of this technology is effective and secure communication between devices. Communication models in IoT mainly provide methods of data exchange between devices. Devices connect to each other and exchange data in real time

using various networks and protocols. The main communication models used in IoT include centralized, distributed, and hybrid models. In the centralized model, all data is managed through one central server. In the distributed model, devices exchange information directly with each other. A mixed model is a combination of two approaches, which allows to create flexible and scalable systems. Also, IoT systems communicate using various networks (Wi-Fi, Bluetooth, Zigbee) and protocols (MQTT, CoAP). Communication models in IoT play an important role in ensuring effective collaboration of devices, fast and reliable data delivery, and security. Effective and secure communication between IoT devices is important to improve their functionality. The analysis in the thesis includes communication protocols, architecture, information exchange mechanisms and security issues. The main goal is to determine the most effective communication models to optimize the data exchange processes of IoT devices. The results of this research are expected to open new directions for the development and widespread use of IoT systems.

Key words: IoT (Internet of Things), Communication models, MQTT, CoAP, Client-server model, Peer-to-peer model, Publish-subscribe model, IoT security.

Kirish. IoT (Internet of Things) texnologiyasi kundalik hayotimizda va sanoat tarmoqlarida tobora keng qo'llanilmoqda. IoT texnologiyalari orqali turli qurilmalar bir-biri bilan bevosita aloqa qilishlari, ma'lumot almashishlari va bu jarayonni boshqarishlari mumkin. Ushbu texnologiya zamonaviy jamiyatda avtomatlashtirish va raqamlashtirishga muhim hissa qo'shmoqda. Ushbu maqolada IoT (Internet of Things) texnologiyalarida qo'llaniladigan aloqa modellari va ularning asosiy xususiyatlari tahlil qilinadi.

IoT dagi aloqa modellari

IoT tizimida qurilmalar o'rtasida ma'lumotlarni uzatish va qabul qilish jarayonlari turli aloqa modellariga asoslanadi. Aloqa modellari IoT tizimlarining samaradorligini ta'minlash uchun muhim omil hisoblanadi. Quyida IoT qurilmalari o'rtasida keng qo'llaniladigan asosiy aloqa modellari keltirilgan:

❖ **Klient-server modeli**

○ IoT tarmog'ida keng qo'llaniladigan ushbu modelda qurilma (klient) ma'lumotlarni serverdan so'rab oladi yoki unga uzatadi. Ushbu model katta hajmdagi ma'lumotlarni uzatish uchun qulay bo'lib, ma'lumotlarni markazlashgan tarzda boshqarishni ta'minlaydi. Bu model an'anaviy kompyuter tarmoqlarida ham keng qo'llaniladi.

❖ **Peer-to-peer (P2P) modeli**

○ Ushbu modelda qurilmalar bir-biriga teng huquqli bo'lib, ma'lumotlarni bevosita almashadi. P2P modeli markaziy serverga ehtiyoj sezmasdan to'g'ridan-to'g'ri ulanishlarni amalga oshiradi, bu esa kechikish va tarmoqning markaziy qismida yuklamani kamaytirishga yordam beradi.

❖ **Publish-subscribe modeli**

○ Ushbu modelda ma'lumotlarni yuboruvchi qurilmalar (publisher) va qabul qiluvchi qurilmalar (subscriber) mavjud bo'lib, ularning har biri ma'lum bir mavzuga (topic) asoslangan holda aloqa o'rnatadi. Qurilmalar bir-birlari bilan to'g'ridan-to'g'ri aloqaga kirishmaydi, balki ma'lumotlar almashinuvini boshqaruvchi broker orqali bog'lanadi. Bu model real vaqtda monitoring qilish tizimlari uchun juda qulaydir.

❖ **MQTT (Message Queuing Telemetry Transport)**

○ MQTT IoT tarmoqlarida keng qo'llaniladigan va kam quvvat sarflaydigan protokollardan biri bo'lib, u publish-subscribe modeliga asoslanadi. Ushbu protokol kichik o'lchamdagi ma'lumotlarni tez uzatish imkonini beradi va ayniqsa past kechikish talab qilinadigan tarmoqlar uchun mos keladi.

❖ **CoAP (Constrained Application Protocol)**

○ CoAP — past quvvatli qurilmalar uchun mo'ljallangan va RESTful modelga asoslangan engil protokoldir. Ushbu protokol kichik hajmdagi ma'lumotlar almashinuvini ta'minlab, IoT qurilmalarining samaradorligini oshiradi.

IoT-dagi aloqa modellarining har biri o'ziga xos afzalliklari va cheklovlariga ega:

❖ Klient-server modeli qulay va keng tarqalgan bo'lsa-da, markazlashgan arxitektura tarmoqdagi serverga katta yuklama tushirishi mumkin.

❖ P2P modeli markaziy serverga ehtiyoj sezmasdan, ma'lumotlarni tezkor almashishga imkon beradi, ammo bu modelda xavfsizlik masalalari ko'proq e'tiborni talab qiladi.

❖ Publish-subscribe modeli katta miqdordagi qurilmalar o'rtasida ma'lumotlarni samarali uzatish uchun qulay, biroq qo'shimcha broker tarmoqda kechikishlarni keltirib chiqarishi mumkin.

❖ MQTT va CoAP protokollari kichik va cheklangan quvvat manbalari bilan ishlaydigan IoT qurilmalar uchun ideal hisoblanadi, lekin katta hajmdagi ma'lumotlarni uzatishda ularning samaradorligi pasayishi mumkin.

IoT tarmoqlaridagi aloqa protokollari va xavfsizlik masalalari

IoT qurilmalari o'rtasida ma'lumotlarni uzatish jarayonida xavfsizlik katta ahamiyatga ega. Ushbu texnologiyalar osonlik bilan hujumga uchrashi mumkin, chunki aksariyat IoT qurilmalari past quvvat va resurs cheklovlariga ega bo'ladi. Shuning uchun, IoT tarmoqlarida quyidagi xavfsizlik choralari ko'rilishi lozim:

- Shifrlash texnologiyalari orqali ma'lumotlar almashinuvi xavfsizligini ta'minlash.
- Autentifikatsiya va avtorizatsiya mexanizmlarini joriy etish orqali har bir qurilma va foydalanuvchini tasdiqlash.
- Xavfsizlik protokollarini qo'llash orqali IoT tarmog'idagi zaifliklarni kamaytirish.

Xulosa

IoT texnologiyalari dunyo miqyosida turli sohalarda keng qo'llanilib, qurilmalar o'rtasida ma'lumot almashishni avtomatlashtiradi va optimallashtiradi. Ushbu texnologiyalarni qo'llash orqali tarmoqlarning samaradorligini oshirish, real vaqtda monitoring qilish va operatsiyalarni boshqarish jarayonlarini sezilarli darajada yaxshilash mumkin. Aloqa modellari esa IoT tizimlarining asosi bo'lib, ular qurilmalar o'rtasidagi ma'lumotlar uzatishning tezligi, ishonchliligi va xavfsizligini ta'minlaydi.

References:

1. Mohammed, A., & Ismail, A. (2021). *IoT Communication Protocols: A Comparative Study*. Journal of Internet Services and Information Security, 11(3), 65-80. doi:10.22667/jisis.2021.06.11.3.65.
2. Zhang, Q., & Li, S. (2020). *Security Challenges in IoT Systems: Attacks, Countermeasures, and Future Directions*. IEEE Internet of Things Journal, 7(9), 7631-7642. doi:10.1109/JIOT.2020.3001784.

3. Gupta, V., & Agrawal, A. (2022). *An Efficient IoT-Based Framework for Smart Cities Using MQTT Protocol*. IEEE Access, 10, 65402-65412. doi:10.1109/ACCESS.2022.3178790.
4. Boulos, M. N., & Zhang, P. (2020). *Smart Health IoT: Development, Applications, and Security Issues*. Future Generation Computer Systems, 105, 699-712. doi:10.1016/j.future.2019.12.003.
5. Patel, K., & Mehta, N. (2023). *Emerging Trends in IoT Communication Models and their Impact on Smart Systems*. IEEE Communications Surveys & Tutorials, 25(1), 324-342. doi:10.1109/COMST.2023.3214587.

