EURASIAN JOURNAL OF ACADEMIC RESEARCH
Innovative Academy Research Support Center
UIF = 8.1 | SJIF = 5.685 www.in-academy.uz


# IOTDA ALOQA PROTOKOLLARI. PROTOKOLLAR FARQI VA TAHLILI

**Sharifboyeva Ro'za Bahodirovna**
sharifboyeva9887@mail.ru Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Urganch filiali II-bosqich magistranti

https://www.doi.org/10.5281/zenodo.7890838

**ARTICLE INFO**

Received: 26th April 2023
Accepted: 02nd May 2023
Online: 03rd May 2023

**KEY WORDS**

*IoT, protokol, IoT arxitekturasi, Sensorlar Interneti, LoWPAN, LoRaWAN, Sigfox, NB-IoT, Wi-Fi HaLowTM, WPAN, LPWAN.*

**ABSTRACT**

*Ushbu maqolada biz IoT arxitekturasining asoslarini ko'rib chiqamiz va IoT texnologiyasi uchun ixtiro qilingan protokollar taqdim etamiz va tahlil qilamiz. Bundan tashqari, biz umumiy amaliyot muammolari va IoT rivojlanishidan eng ko'p foyda ko'rishi mumkin bo'lgan bir nechta sektorlarni ko'rib chiqamiz.*

*Ushbu izlanish va protokollarni tahlil qilish natijasida amaliyotda yuzaga kelayotgan muommolar va ularni yechimlari bilan tanishamiz. Qo'llanilish sohasiga mos bo'lgan optimal protokollarni va ularning xavfsizligini o'rganamiz.*

**Kirish.**

Bir necha o'n yillar oldin, Internet ulanish orqali bizning dunyomizni inqilob qildi real vaqtda bir vaqtning o'zida butun dunyo bo'ylab foydalanuvchilar internet tarmog'iga ulana boshladi. IoT deb qisqartirilgan "Internet of Things" atamasi butun dunyo bo'ylab ulanishi mumkin bo'lgan son-sanoqsiz moddiy qurilmalar Interneti deb tushunish ham mumkin. Ushbu qurilmalarning barchasi ma'lumotlarni to'playdi va bir-biri bilan almashadi. Kompyuterning paydo bo'lishi tufayli juda arzon narxlardagi chiplar, simsiz tarmoqlar paydo bo'ldi va qo'shimcha ravishda ko'plab texnologiyalarning mashina - o'rganish, katta ma'lumotlarni tahlil qilish, aqlli sensorlar va ayniqsa 5G rivojlanishiga turtki bo'ldi. Chunki IoT kichik chipdan tortib katta shaharlar uchun ham qo'llanilishi mumkin.

Garchi ko'plab qurilmalar Internetga ulanishi mumkin bo'lsa-da, IoT qurilmalarini odatda Internetga kirish imkoniga ega bo'ladilar, masalan, maishiy texnika, sog'liqni saqlash nazorati qurilmalari yoki har qanday turdagi uskunalar va shu bilan birga, inson ishtirokisiz bir-biri bilan muloqot qilish qobiliyatiga ega. Keyinchalik, noutbuk ham, smartfon ham sensorlarni olib yurishidan va Internet orqali muloqot qilishidan qat'i nazar, IoT qurilmalari hisoblanmaydi. Biroq, aqlli soatlar yoki fitnes-trekerlar kabi taqiladigan moslamalar sifatida qaralishi mumkin. Shunga qaramay, shaxsiy kompyuter yoki smartfon IoT tarmog'i bilan o'zaro aloqada bo'lishi mumkin [2, 3].

Noyob aniqlanishi mumkin bo'lgan barcha bu turli xil ob'ektlarni ulash va sensorlarni ulash ularni raqamli aqlli qurilmalarga aylantiradi. Natijada, ular real vaqt rejimida ma'lumotlarni uzatishga qodir bo'ladi, keyinchalik ularning samaradorligi va aniqligini

oshiradi va bizni o'rab turgan muhitni yanada aqlli va tezkor javob beradi, raqamli va jismoniy dunyoning uyg'unligini amalga oshiradi [4].

Bu tushuncha qo'llanilishi mumkin bo'lgan sohalarni ko'paytirdi, bu esa o'z navbatida mavjud vositalardan ilgari hech qachon o'ylamagan usullardan foydalanish orqali umumiy natijani oshirishi mumkin va u kelajakdagi texnologiyaning eng muhim sohalaridan biri hisoblanadi. bu ko'plab sohalarda mashhur bo'lib bormoqda [5]. Samaradorlik va aniqlikdan tashqari, IoT qurilmalarining o'zaro bog'lanishi muhim tizimlarga ulanishi mumkin bo'lgan foydalanuvchilarga bir qator xavfsizlik tahdidlarini [6] ochadi [7].

Ulangan qurilmalarning IoT texnologiyasi prognozi 2020-yildagi 8,7 milliard qurilmadan 2030-yilda 25 milliarddan ortiq IoT qurilmalariga qariyb 300 foizga oshishi kutilmoqda. 2020-yilda Xitoy 3 milliarddan ortiq qurilmalar bilan IoT ilovalari poygasida yetakchilik qilmoqda. Mavjud IoT qurilmalari har bir sanoat sohasida va chakana savdo bozorida mavjud. Xususan, chakana savdo bozori 2020-yilda IoT qurilmalari umumiy sonining qariyb 60% ni tashkil qiladi. Bu taqsimot kelgusi o‘n yil ichida o‘zgarmasligicha qoladi [8].

Ushbu maqolaning quyidagilarni tahlil qilamiz.

- Umumiy IoT arxitekturasini;
- Ilova, transport, tarmoq va jismoniy qatlamda qo'llaniladigan asosiy aloqa protokollarini;
- IoTda mavjud xavfsizlik tahdidlari;
- Mavjud muammolarni ko'rib chiqadi va mumkin bo'lgan yechimlar va kelajakdagi yo'nalishlar;

2018-04-22 _ Tegishli so'rovlar

1-jadvalda IoT ilovasi xavfsizligi bo'yicha tegishli tadqiqotlar keltirilgan [9]. IoT xavfsizligi sohasidagi mavjud tadqiqotlarni chuqur o'rganish orqali IoT xavfsizligining ilg'or zaifliklari va tahdidlariga e'tibor qaratdi. Tadqiqot aloqa, arxitektura va dastur kontekstidagi mavjud xavfsizlik tahdidlarining to'liq ko'rinishini taqdim etadi. Ushbu tadqiqot, shuningdek, IoTdagi potentsial xavfsizlik muammolarini taqqoslashni ham ta'minlaydi. Bundan tashqari, tadqiqot joriy IoT-ga asoslangan xavfsizlik muhitini muhokama qilish bilan bir qatorda potentsial tahdidlar haqida umumiy ma'lumot beradi. Qolgan davom etayotgan tadqiqot muammolari va IoT xavfsizligida xavfsizlikni joylashtirish muammolari ham taqdim etilgan [10]. IoT tizimi doirasidagi muhim uchta asosiy qatlam nuqtai nazaridan taksonomiyani ko'rib chiqishni taqdim etdi: 1) dastur darajalari; 2) transport; va 3) idrok etish [11].

1-jadval . Narsalar interneti ilovasining xavfsizligi bo'yicha tegishli tadqiqotlar.

| **IoT arxitekturasi** | **Aloqa protokollari** | **Xavfsizlik masalalari** | **IoT ilovalari** | **Qiyinchilikari** | **Maqolaga havola** |
|---|---|---|---|---|---|
| Qisman | Qisman | Ha | Qisman | Ha | [11] |
| Yo’q | Yo’q | Ha | Qisman | Qisman | [12] |
| Ha | Qisman | Qisman | Qisman | Ha | [13] |
| Qisman | Qisman | Qisman | Qisman | Qisman | [14] |
| Qisman | Qisman | Ha | Qisman | Ha | [15] |
| Qisman | Qisman | Ha | Qisman | Ha | [16] |
| Qisman | Yo’q | Qisman | Yo’q | Qisman | [17] |
| Ha | Qisman | Qisman | Qisman | Qisman | [18] |

| | | | | | |
|---|---|---|---|---|---|
| Qisman | Qisman | Qisman | Yo’q | Qisman | [19] |
| Yo’q | Yo’q | Qisman | Yo’q | Yo’q | [20] |
| Ha | Qisman | Ha | Yo’q | Ha | [21] |

IoT ilovasi uchun autentifikatsiya texnologiyalarini keng qamrovli o'rganish Ref tomonidan taqdim etilgan [12]. Xususan, IoT muhitida amalga oshirilgan yoki o'rnatilgan qirqdan ortiq autentifikatsiya protokollari aniqlanib, chuqur ko'rib chiqiladi. Protokollar maxsus IoT maqsadli sozlamalariga ko'ra tasniflanadi: Sensorlar Interneti (IoS), Energiya Interneti (IoE), Avtotransport Interneti va Mashinadan Mashinaga Aloqa (M2M).

Umumiy IoT arxitekturasi

Nazariy jihatdan, IoT atamasi odatda unga kiritilgan qurilmalar ichidagi ma'lumotlar ma'lumotlarini muvaffaqiyatli boshqaradigan tarmoqni loyihalash va amalga oshirishni tavsiflash uchun ishlatiladi. Amalda, bu tarmoq Internet bo'lgani uchun, bu juda qiyin narsa, chunki unda ishtirok etayotgan barcha qurilmalar (Aqlli sensorlar, ma'lumotlar markazlari va boshqalar) bir-biri bilan to'g'ridan-to'g'ri yoki bilvosita (ya'ni, shlyuzlar) muammosiz aloqa qila olishi kerak.), xavfsiz tarzda. Natijada, Internetning barcha qurilmalarini moslashtirish aloqa uchun maxsus protokollarni, standart tuzilmani, ilovalarning muvofiqligini, ilg'or ma'lumotlarni qayta ishlashni talab qiladigan narsadir.. Muayyan amalga oshirishda ularning murakkabligiga qaramasdan, ularning elementar ishlashi juda oddiy [13].

Aqlli ob'ekt sensorlari (jismoniy dunyo) tomonidan to'plangan ma'lumotlarni ma'lumotlar markaziga (mahalliy yoki bulutga asoslangan) yoki hatto boshqa aqlli ob'ektga oraliq (shlyuz) orqali uzatadi. Shlyuzdan foydalanish majburiy emas, chunki aqlli ob'ekt shlyuz sifatida ham ishlashi mumkin. Keyin, "boshqa tomonda" olingan ma'lumotlar qayta ishlanadi va bir nechta harakatlar boshlanishi mumkin. Bu harakatlar amalga oshirishni murakkablashtiradigan harakatlardir, chunki avtonom avtomashinani boshqarish yoki kuzatish uchun, masalan, ma'lum darajada isitgichni yoqish uchun ko'proq o'zaro muvofiqlik talab qilinadi.

IoT texnologiyasi juda ko'p sohalarga taalluqli bo'lsa-da va hech qanday tarzda standartlashtirilmagan bo'lsa-da, biz asosiy arxitekturani va ushbu texnologiya uchun ixtiro qilingan eng keng tarqalgan protokollarni ko'rib chiqish orqali oddiy yondashuvni ko'rib chiqamiz [23] .

Joriy xususiyatlarni va kelajakdagi kengaytmalarni qo'llab-quvvatlaydigan mos yozuvlar arxitekturasini aniqlash uchun miqyoslilik, o'zaro ishlash, ma'lumotlarni taqsimlash, hisoblash quvvati va, albatta, xavfsizlik, me'moriy standartlashtirish bilan bog'liq ba'zi fundamental omillarni hisobga olish kerak, chunki adabiyotda bir nechta model arxitekturalari tasvirlangan [24] .

Aloqa protokollari

Ko'pgina protokollar IoTni amalga oshirishga hissa qo'shadi, ammo aloqa protokollari IoT tarmoqlari uchun majburiydir. Yuqorida aytib o'tilganidek, IoT qurilmalari bulut orqali ulangan jismoniy ob'ektlar o'rtasidagi aloqani ta'minlash uchun tarmoq standartlari va protokollaridan foydalanadi. Tarmoq protokollari va standartlari - bu turli xil tarmoq qurilmalari o'rtasidagi aloqa tilini belgilaydigan muayyan qoidalarni o'z ichiga olgan.

Har bir qurilma odatda Internetga Internet protokoli (IP) yordamida ulanadi, lekin mahalliy ravishda blacktooth, NFC (yaqin maydon aloqasi) va boshqalar orqali ulanishi mumkin. Ikkala turdagi ulanishlar o'rtasidagi farqlardan ba'zilari quvvat, diapazon va CPU quvvati ishlatiladi. IP-ulanishlar murakkab va ko'proq quvvat va xotira talab qiladi, ammo diapazonda cheklovlar yo'q. Blacktooth ulanishlari esa oddiy va kamroq quvvat va xotira talab qiladi, lekin diapazon cheklangan.

Smartfonlar va shaxsiy kompyuterlar kabi yagona qurilmalar aloqa uchun tarmoq protokollaridan foydalanadi, ammo bu qurilmalar tomonidan ishlatiladigan umumiy protokollar tarmoqli kengligi, kechikish va IoT-ga asoslangan yechimlarni qamrab olish masofasi kabi maxsus talablarga javob bermasligi mumkin. IoT qurilmalarini joylashtirish oson bo'lsa-da, ularning aloqa protokollari mavjud internet infratuzilmasi bilan ishlash quvvati, diapazoni va ishonchliligi yetishmasligini to'ldirishi kerak. Mavjud protokollar IoTni joriy qilish mezonlariga javob bermaganligi sababli (Wi-Fi 802.11 a/b/g/n/ac va boshqalar), biz IoT ilovasi talablari uchun yaratilgan ba’zi yangi IoT protokollarini ko‘rib chiqamiz.

IoT tarmoqlarini loyihalashda energiya iste'moli muhim omil bo'lgani uchun kam quvvatli simsiz tarmoq texnologiyalari afzalroqdir. Ushbu texnologiyalar odatda ikki guruhga bo'linadi.

- Bir necha kilometrgacha kengaytirilgan diapazonni ta'minlovchi, lekin ko'pchilik uchun cheklangan ma'lumotlar tezligi (masalan, LoWPAN, LoRaWAN, Sigfox, NB-IoT, Wi-Fi HaLowTM);
- Wireless Personal Area Networking (WPAN) texnologiyalari, 100 m gacha diapazon va Zigbee uchun 250 kbps gacha ma’lumot uzatish tezligi va blacktooth Low Energy uchun 3 Mbit/s gacha.

LPWAN

LPWAN (past quvvatli keng tarmoqli tarmoqlar) qisqa masofali aloqa uchun ishlab chiqilgan protokollar toifasidir. Garchi "an'anaviy" uyali aloqa tarmoqlari keng tarmoqli aloqa tarmoqlarini qo'llab-quvvatlashga qodir bo'lsa- da, ularning kamchiliklari, masalan, murakkab infratuzilma (antennalar, kuchaytirgichlar va boshqalar) va yuqori quvvat iste'moli talablari IoT ilovalarini ko'rib chiqishda ularni kamroq qulay yechimga aylantiradi. Boshqa tomondan, LPWAN protokollari oddiy, kam quvvatli, past protsessor imkoniyatlari tomonidan qo'llanilishi kerak, bu esa arzon batareyalarga asoslangan shlyuzlarga investitsiya qilmasdan datchiklarni joylashtirish imkonini beradi va bu protokollardan farqli o'laroq uni yanada qulayroq variantga aylantiradi.

Kam talab qilinadigan apparat qobiliyatini hisobga olgan holda, LPWAN texnologiyasi atrof-muhit va to'siqlarga qarab 10 km dan ortiq masofada ishlashi mumkin va ma'lumotlar uzatish tezligi har bir kanal uchun 0,3 kbit / s dan 50 kbit / s gacha. Bundan tashqari, quvvat iste'moli va ma'lumotlar tezligi LPWAN uchun katta qiyinchiliklar bo'lsa-da, LPWAN protokolini tanlashda xizmat ko'rsatish sifati (QoS) va kengayishi muhim omillardir. 6LoWPAN protokoli IPv6 va LoWPAN texnologiyalarini birlashtirgan LPWAN protokoliga misol bo‘lib, juda ko‘p afzalliklarga ega, jumladan, istisnoli ulanish, oldingi arxitekturalar bilan moslik, kam energiya sarfi va o‘z-o‘zini tashkil qilish.

WPAN

WPAN - bu tarmoqli topologiyada tashkil etilgan qurilmalarning mahalliy tarmoq tarmog'i bo'lib, unda har bir qurilma tarmoqning boshqa qurilmalari bilan to'g'ridan-to'g'ri (shlyuzsiz) ulanadi va ushbu tarmoq ichidagi oxirgi qabul qiluvchiga yetguncha bir-biri o'rtasida ma'lumotlarni uzatadi . Ushbu tuzilma tarmoqning mustahkamligini ta'minlaydi, amalga oshirish oson va uni o'rnatish boshqa tarmoqlarga qaraganda kamroq xarajat qiladi, ayniqsa qo'shimcha uskunalar (ya'ni, shlyuzlar) yo'qligi sababli katta maydonlarda.

ZigBee IoTda ishlatiladigan eng mashhur protokoli hisoblanadi. U qisqa masofaga ega, lekin minimal quvvat sarflaydi, bu esa bir nechta IoT qurilmalari orqali aloqani kengaytirishi mumkin. LPWAN protokollari bilan taqqoslaganda, ZigBee bir vaqtning o'zida yuqori ma'lumotlarni uzatish tezligini ta'minlay oladi, ammo tarmoqli topologiyasi tufayli ko'proq quvvat samaradorligi bilan. Biroq, ularning qisqa jismoniy diapazoni tufayli, ZigBee va boshqa har qanday tarmoq protokoli aqlli uy tarmoqlari kabi kichik va o'rta diapazonli ilovalar uchun eng mos keladi [23].

IoT texnologiyalaridagi aloqa simli va simsiz ulanishlarni qamrab oladi . Ulanish turiga qarab, 4 qatlamli tarmoqdagi aloqa protokollari keyingi bosqichda har bir qatlam uchun tavsiflanadi.

Ilova qatlami

Quyida dastur qatlami uchun besh xil protokol tasvirlangan; MQTT, CoAP , REST , XMPP va AMQP. Xavfsizlik bilan bog'liq bo'lgan xususiyatlar va muammolar ham muhokama qilinadi.

MQTT

Message Queuing Telemetry Transport (MQTT) protokoli juda oddiy mijoz/server modelida ishlaydigan va TCP/IP yoki boshqa protokollar orqali ishlaydigan nashr qilish va obuna bo'lish uchun xabar almashish protokoli. Bu IoT kabi cheklangan muhitlar uchun ko'proq mos keladi, chunki u ochiq, engil va oson amalga oshirilishi mumkin. MQTT ilovalarida bajarilishi kerak bo'lgan xavfsizlik talablari autentifikatsiya, avtorizatsiya va xavfsiz aloqadir. Muhim infratuzilmalar va maxfiy ma'lumotlarga ega ilovalarda MQTT tavsiya etilgan xususiyatlardan foydalangan holda ilg'or xavfsizlik xizmatlarini taklif qilishi va ishlashi mumkin.

CoAP

Cheklangan ilovalar protokoli (CoAP) RFC 7252 da ixtisoslashtirilgan veb-uzatuv protokoli sifatida belgilangan. Bu cheklangan tugunlar va cheklangan tarmoqlar bilan foydalanish uchun tavsiya etilgan, past uzatish tezligiga ega yengil protokol va uning nomi shu bilan belgilanadi. Dizayn ta'minot zanjirini boshqarish va energiya sarfini kuzatish uchun aqlli hisoblagichlar kabi mashinadan mashinaga (M2M) ilovalar uchun mos keladi . U HTTP bilan juda yaxshi interfeysga kirishi mumkin, bu esa Internet bilan integratsiyani osonlashtiradi. Ammo CoAP xavfsiz protokol emas va bu jiddiy kamchilik. Xavfsizlikka Ref.da belgilangan Datagram Transport Layer Security (DTLS) yordamida erishiladi . [31]; Bu, afsuski, IoT-da keng qo'llanilmaydi.

REST

Representational State Transfer (REST) - bu Fielding tomonidan Ref. [25]. U ma'lum cheklovlar bilan dastur yaratish uchun dasturiy ta'minot muhandisligining rahbarlik tamoyillarini tavsiflovchi qoidalar to'plamini o'z ichiga oladi. U RESTful deb ham ataladigan veb-xizmatlarni qurish uchun ishlatiladi. REST quyidagilarni o'z ichiga oladi: a) mijoz-server

cheklovi, b) ko'rinish, ishonchlilik va miqyoslilikka erishadigan fuqaroligi bo'lmagan cheklov, c) tarmoq samaradorligini oshiradigan kesh cheklovi, d) komponentlar orasidagi yagona interfeys uchun to'rtta cheklovlar to'plami, e) qatlamli tizim cheklovlari va f) talab bo'yicha kod bo'yicha ixtiyoriy cheklash.

XMPP

Extensible Messaging and Presence Protocol (XMPP) real vaqt rejimida muloqot qilish uchun ochiq XML texnologiyasidir. U tezkor xabar almashish , mavjudligi va hamkorlik qilish uchun ishlatiladi . Presence ob'ekt xabar almashish uchun tayyor ekanligini bildiradi. Xabarlar real vaqt rejimida ishlash imkoniyatini ta'minlaydigan samarali surish mexanizmidan foydalanadi. XMPP ning ochiq dizayni o'zgarishlarni osonlashtiradi va uning IoT joriy etilishiga mos keladigan kengaytiriladigan xususiyatiga imkon beradi. Yaqinda NIST tomonidan yuritiladigan NVD ma'lumotlar bazalariga XMPP ning ma'lum zaifliklari bilan bog'liq bo'lgan CVE kodlarining katta qismi qo'shildi, ular qator hujumlarni amalga oshirishga imkon beradi.

MQP

Advanced Message Queuing Protocol (AMQP) turli tashkilotlar va platformalarda asinxron tarzda ishlaydigan ilovalar o‘rtasida biznes xabar almashish uchun mos bo‘lgan ochiq standartdir. Bu ishonchli biznes xabarlarini yuborish imkonini beruvchi simli darajadagi protokol. AMQP dizayniga kiritilgan ba'zi asosiy xususiyatlar xavfsizlik, ishonchlilik va o'zaro muvofiqlikni ta'minlashga qaratilgan. U 2014 yilda ISO va IEC xalqaro standarti sifatida chiqarish uchun tasdiqlangan va u bir necha qatlamlardan iborat. Eng past daraja ikki jarayon o'rtasida xabarlarni tashish uchun mo'ljallangan va xabarlar darajasi har bir xabarda bo'lishi kerak bo'lgan standart kodlash formatini belgilaydi.

Tarmoq qatlami

Ilova qatlami uchun beshta tarmoq protokoli taqdim etiladi; WiFi, blacktooth, ZigBee, Z-Wave va LoRaWAN va xavfsizlik bilan bog'liq xususiyatlar va muammolar ham muhokama qilinadi.

Wi-fi

WiFi Elektr va elektronika muhandislari instituti (IEEE) 802.11 simsiz aloqa standartiga asoslangan eng ko'p ishlatiladigan va taniqli aloqa texnologiyasidir . U tez, kamroq kechikish bilan va bir nechta turli qurilmalarga mos keladi. WiFi avlodiga qarab, xavfsizlik autentifikatsiya ma’lumotlarining maxfiyligi va WIFi ulanishlarini ta’minlovchi mavjudlik talablariga javob berish uchun kuchaytiriladi . Qurilmalar 100 m masofada signallarni yuborish orqali simsiz ulanadi, lekin aslida bu ancha qisqaroq.

Blacktooth

Blacktooth Low Energy (LE) radiosi IoTni amalga oshirish uchun afzalroq, chunki u juda kam quvvatda ishlashga mo'ljallangan. U ma'lumotlarni ko'p sonli kanallar bo'ylab uzatishga qodir bo'lib, bir nechta turli xil aloqa topologiyalarida, nuqtadan nuqtaga va to'rli topologiyalarda va keng ko'lamli simsiz qurilmalar tarmoqlari yonida amalga oshirilishi uchun zarur bo'lgan ochiqlikni ta'minlaydi. Bundan tashqari, u yuqori aniqlik bilan qurilma joylashuvini aniqlash xizmatlarini taqdim etadi. U keng qo'llaniladi, chunki u butun dunyo bo'ylab tarqalgan taqiladigan va smartfonlar kabi eng zamonaviy mobil qurilmalar uchun juda mos keladi.

ZigBee

ZigBee - bu IoT infratuzilmalarida blacktooth kabi muhim foydalanishga ega protokol. U kam quvvat iste'moli , past ma'lumot diapazoni va 200 m gacha bo'lgan aloqa diapazoni bilan ilg'or xavfsizlik talablarini qamrab oladi , bu mos keladigan blacktooth bilan solishtirganda ikki baravar uzun. Bir nechta cheklovlarga ega bo'lgan sensorlar va qurilmalar uchun mos keladi, u ko'p sonli tugunlarga ega bo'lgan yirik IoT modellarini qurishni osonlashtiradi.

LoRaWAN

LoRaWAN - bu IoT ilovalarida batareyaga asoslangan qurilmalarni simsiz ulash uchun ishlatiladigan kam quvvatli, keng maydon (LPWA) tarmoq protokoli. U ikki tomonlama aloqa va oxirigacha xavfsizlikning muhim talablariga javob beradi [26].

Jismoniy qatlam

IEEE 802.15.4 - bu jismoniy qatlam va MAC qatlami uchun mo'ljallangan protokol bo'lib, u quvvat cheklovlari va sensorlar orqali xizmatlarni taqdim etish uchun ma'lum talablarga ega qurilmalar o'rtasidagi aloqani ta'minlaydi. Arzon va qisqa masofali aloqa qo'llab-quvvatlanadi va qurilmalar ko'p tarmoqli marshrutlashni osonlashtirish va diapazonni kengaytirish uchun hamkorlik qiladi. U past tarifli simsiz shaxsiy tarmoq (LR-WPAN) uchun tavsiflarni o'z ichiga oladi.

4 qatlamli ISO arxitekturasida IoT uchun aloqa protokollari: ijobiy va salbiy tomonlari.

| **Protokol** | **Afzalliklari** | **Kamchiliklari** |
|---|---|---|
| **AMQP** | Ishonchlilik xavfsizligi, minimal harakat bilan kengaytirilishi | Og'ir xotira talablari, Sekin ma'lumotlarni uzatish |
| **MQTT** | Kam quvvat sarfi Kam tarmoqli kengligidan foydalanish | Cheklangan o'zaro hamkorlik, o'ziga xos xavfsizlik cheklovlari, zaif kengaytirilish |
| **ZigBee** | Yuqori darajada xavfsiz, kam quvvat iste'moli, uzoq aloqa oralig'i | aralashuvga moyil, qimmat |
| **Z to'lqini** | Kam kechikish, kam quvvat iste'moli, oqilona qamrov | Past ma'lumot uzatish tezligi, Premium narxlar |
| **Wi-fi** | Qulay va oson o'rnatish, Yuqori ma'lumotlarni uzatish tezligi | Yuqori quvvat sarfi, o'lchash qiyin |
| **LoraWan** | Masshtablilik, keng qamrovli, kam quvvat sarfi | Past ma'lumot uzatish tezligi, Custom LoRa shlyuzi |

Xulosa.

Internet texnologiyalari rivojlanib borayotgan paytda ma'lumotlarni uzatish va qabul qilishga bo'lgan ehtiyoj ham ko'payib borayotgan. Ma'lumot uzatishda ma'lumotni uzatish tezligi, ma'lumot hajmi, ma'lumot turi, uzatish uzoqligi ahamiyatga ega. Protokollarni esa yuqoridaki sifatlardan kelib chiqqan holda tanlagan maqul. Yuqoridagi maqolada protokollarni tahlil qilish orqali har qanday protokollarni hususiyatlari bilan tanishtirdik.

Bulutli xizmatlar, katta ma'lumotlarning rivojlanishi bilan texnologiyalar jumladan tahliliy va mobil texnologiyalar, kichik o'lchamli jismoniy tarmoqni tashkil etuvchi qurilmalar odamsiz ma'lumotlarni to'plashi va almashishi ham rivojlanib bormoqda. Ushbu giperbog'langan muhitda har bir tugun bog'langan narsalar orasidagi har bir shovqinni yozib

olishi, kuzatishi va sozlashi mumkin. Ushbu istiqbolli texnologiyalar foydalanuvchilarning maxfiyligi va xavfsizligiga 100 foiz javob bera olmaydi.

IoT tarmoqlari Internet atamasini yaratuvchi an'anaviy tarmoqlar sifatida qaraladi.

## References:

1. A. Rayes, S. Salam, Internet of Things from Hype to Reality, Springer, 2017
2. I. Lee, K. Lee, The internet of things (iot): applications, investments, and challenges for enterprises, Bus. Horiz. 58 (2015) 431–440
3. M.A. Ferrag, L. Maglaras, A. Derhab, Authentication and Authorization for Mobile Iot Devices Using Biofeatures: Recent Advances and Future Trends, Security and Communication Networks, 2019, 2019.
4. S. Khan, K.A. Shakil, M. Alam, Internet of Things (IoT): Concepts and Applications, Springer, 2020
5. J. Wang, M.K. Lim, C. Wang, M.L. Tseng, The evolution of the internet of things (iot) over the past 20 years, Comput. Ind. Eng. 155 (2021), 107174
6. M.A. Ferrag, L. Maglaras, A. Ahmim, M. Derdour, H. Janicke, Rdtids: rules and decision tree-based intrusion detection system for internet-of-things networks, Future Internet 12 (2020a) 44.
7. L. Maglaras, M.A. Ferrag, A. Derhab, M. Mukherjee, H. Janicke, S. Rallis, Threats, Protection and Attribution of Cyber Attacks on Critical Infrastructures, 2019 arXiv preprint arXiv:1901.03899
8. Al-Sarawi, M. Anbar, R. Abdullah, A.B. Al Hawari, Internet of things market analysis forecasts, 2020–2030, in: 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), IEEE, 2020, pp. 449–453
9. F.A. Alaba, M. Othman, I.A.T. Hashem, F. Alotaibi, Internet of things security: a survey, J. Netw. Comput. Appl. 88 (2017) 10–28.
10. M.A. Ferrag, L.A. Maglaras, H. Janicke, J. Jiang, L. Shu, Authentication Protocols for Internet of Things: a Comprehensive Survey. Security and Communication Networks 2017, 2017.
11. M. Frustaci, P. Pace, G. Aloi, G. Fortino, Evaluating critical security issues of the iot world: present and future challenges, IEEE Internet Things J. 5 (2017) 2483–2495
12. S. Vashi, J. Ram, J. Modi, S. Verma, C. Prakash, Internet of things (iot): a vision, architectural elements, and security issues, in: 2017 International Conference on ISMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), IEEE, 2017, pp. 492–496
13. M. Ammar, G. Russello, B. Crispo, Internet of things: a survey on the security of iot frameworks, J. Inf. Secur. Appl. 38 (2018) 8–27.
14. V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, B. Sikdar, A survey on iot security: application areas, security threats, and solution architectures, IEEE Access 7 (2019) 82721–82743.
15. N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, P. Faruki, Network intrusion detection for iot security based on learning techniques, IEEE Commun. Surv. Tutor. 21 (2019) 2671–2701.

16. M.A. Ferrag, L. Shu, X. Yang, A. Derhab, L. Maglaras, Security and privacy for green iot-based agriculture: review, blockchain solutions, and challenges, IEEE Access 8 (2020b) 32031–32053.
17. L. Da Xu, Y. Lu, L. Li, Embedding blockchain technology into iot for security: a survey, IEEE Internet Things J. 8 (2021) 10452–10473.
18. X. Yang, L. Shu, Y. Liu, G.P. Hancke, M.A. Ferrag, K. Huang, Physical security and safety of iot equipment: a survey of recent advances and opportunities, IEEE Trans. Ind. Inf. 18 (2022) 4319–4330.
19. A. Derhab, O. Cheikhrouhou, A. Allouch, A. Koubaa, B. Qureshi, M.A. Ferrag, L. Maglaras, F.A. Khan, Internet of drones security: taxonomies, open issues, and future directions, Veh. Commun. (2022), 100552
20. A. Chaudhary, S.K. Peddoju, K. Kadarla, Study of internet-of-things messaging protocols used for exchanging data with external sources, in: 2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), IEEE, 2017, pp. 666–671
21. D. Serpanos, M. Wolf, The iot landscape, in: Internet-of-Things (IoT) Systems, Springer, 2018, pp. 1–6.
22. B.B. Gupta, M. Quamara, An overview of internet of things (iot): architectural
23. aspects, challenges, and protocols, Concurrency Comput. Pract. Ex. 32 (2020), e4946.
24. I.B.F. de Almeida, L.L. Mendes, J.J. Rodrigues, M.A. da Cruz, 5g waveforms for iot applications, IEEE Commun. Surv. Tutor. 21 (2019) 2554–2567.
25. E. Rescorla, N. Modadugu, Rfc 6347: Datagram Transport Layer Security Version 1.2, Internet Engineering Task Force (IETF), 2012, p. 2070, 1721
26. R.T. Fielding, Rest: Architectural Styles and the Design of Network-Based Software Architectures, Doctoral dissertation, University of California, 2000.
27. J. de Carvalho Silva, J.J. Rodrigues, A.M. Alberti, P. Solic, A.L. Aquino, Lorawan—a low power wan protocol for internet of things: a review and opportunities, in: 2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech), IEEE, 2017, pp. 1–6.