Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Hálózati Rendszerek és Szolgáltatások Tanszék

Összefonódás-csere alapú útvonaltervezés kvantumműholdas rendszerekhez

TDK dolgozat

Készítette:

Mihály András

Konzulens:

Dr. Bacsárdi László

Budapest, 2022

Tartalomjegyzék

Absztrakt **i**

Abstract **ii**

1. Bevezető **1**

2. Kvantumkommunikációs bevezető **3**

2.1. Kvantumbit 4

2.2. Kvantumkapuk 4

2.3. Kvantumösszefonódás 4

2.4. Kvantumösszefonódás-csere 5

2.5. Kvantumismétlő 6

3. Műholdas rendszerek **7**

3.1. Műholdpályák 7

3.2. Műholdpálya propagátorok 8

3.2.1. Poliastro 9

3.2.2. Orekit 10

4. Műholdas kvantumkommunikáció napjainkban **11**

4.1. Műholdas kvantumkommunikációs architektúrák 11

5. REBSAN algoritmus **13**

5.1. Idővariáns gráfok 13

5.2. REBSAN algoritmus 14

5.2.1. A REBSAN algoritmus mögötti ötlet és működése 15

6. Az elkészült szimulátor **18**

6.1. Műholdas kvantumismétlő felépítése 19

6.2. Felhasznált műhold rendszerek 19

6.2.1. RETRO műholdas architektúra 21

6.2.2. CROSS műholdas architektúra 21

7. Eredmények **22**

7.1. RETRO architektúra 22
7.1.1. LOW konstelláció 23
7.1.2. LOWMID1 konstelláció 23
7.1.3. LOWMID2 konstelláció 24
7.1.4. MID konstelláció 25
7.2. CROSS architektúra 27
7.2.1. LOW konstelláció 27
7.2.2. LOWMID1 konstelláció 27
7.2.3. LOWMID2 konstelláció 28
7.2.4. MID konstelláció 29

8. Konklúzió **30**

Felhasznált irodalom **33**

Absztrakt

A kvantumszámítógépeknek nemcsak a kriptográfia, hanem az anyagtudomány és az orvostudomány területén is egyre nagyobb jelentősége van a kvantumalgoritmusok fejlődésének köszönhetően. A kvantumkommunikáció emiatt is egy kritikus terület, hiszen nemcsak egy biztonságos kommunikációs csatornát biztosít, hanem lehetővé teszi a világ különböző részein lévő kvantum számítógépek számára az együttműködést. Kvantuminformáció megosztására a legtöbb esetben fotonokat használunk. A fotonokat két féle közegen tudjuk közvetíteni: üvegszálon vagy szabadtéren keresztül. A szabadtéri kvantumkommunikáció eseténen műholdak bevonásával nagyobb területet is le lehet fedni, mint üvegszál használatával.

Az elmúlt években a legtöbb kutatásban, amely kvantumműholdas hálózattokat használt, mint közvetítő hálózat, két dolog volt közös. Először is az optikai átvitel maximalizálása érdekében alacsony pályájú műholdakat használtak, másrészt a földi állomások között pedig folytonos kapcsolatot biztosítottak. Az alacsony pályamagasság és a folytonos kapcsolat fenntartása érdekében több száz műholdra vagy speciális, magasabb pályán keringő támogató műholdakra van szükség. A szükséges technológia kifejlesztésének költségeit nem számítva az egyik legnagyobb költséget egy ilyen rendszer esetén a műholdak felküldése és fenntartása jelentené. Ezért fontos ezen műholdak számának minimalizálása, viszont azzal csökken az átviteli ablakok száma is, így egy folytonos kapcsolat már nem fentartható.

A kutatásunk során létrehoztunk egy új útvonalkereső algoritmust mely segítségével minimális számú műholdakkal is elérhető a teljes lefedettség. A kvantumösszefonódás-csere tulajdonságainak köszönhetően nem kellet időben egymást követniük a különböző útvonal részeknek. Az egyik fő célunk egy olyan algoritmus létrehozása volt mely segítségével lecsökken a teljes lefedettséghez szükséges műholdak száma.

Abstract

Quantum computing has growing importance not only in the field of cryptography but in material science, medicine, and many more thanks to the advancements in quantum algorithms. Quantum communication provides several solutions including secret key exchange and connectivity between quantum computers all around the world. Photons are one of the most used mediums for transmitting quantum information. There are two main mediums for transmitting photons, fiber and free-space based. Free-space quantum communication is possible to provide higher coverage with the use of satellites than the optical fiber.

In recent years, most research works that coined satellite networks as a medium for quantum communication had two things in common. First, the satellites should be in Low Earth Orbit, increasing the maximal optical throughput of the earth-satellite links. Second, the system should provide a continuous communication channel between the end nodes. Not considering the cost of technology development which is needed for high reliability satellite-based quantum system, one of the highest drivers of cost for these networks is the cost of launching and maintaining satellites. By decreasing the number of satellites needed for a functioning network, one can decrease the cost of that system.

In our research, we created a routing protocol for scarce quantum satellite systems. The main idea behind our algorithm was the utilization of entanglement swapping. By utilizing quantum entanglement swapping, we eliminated the need for the resulting routes to be time consecutive. Our main goal was to create an algorithm that would enable scarce quantum satellite networks.

1. - Bevezető

A kvantuminformatika folyamatos fejlődésének köszönhetően több ízben is meg fog változni a ma ismert informatikai világunk. Shor [1] algoritmusának felhasználásával a ma egyik leggyakrabban használt publikus kulcsú titkosítást rövid időn belül vissza lehet majd fejteni. Ezt felhasználva akár ma küldött üzenetek is feltörhetőek lehetnek, ha azokat egy rosszindulatú csoport elmenti. Kvantum algoritmusok segítségével nem csak a titkosítás visszafejtése gyorsítható fel, hanem olyan ma használt műveletek is melyek klasszikus számítógépen óriási számítási kapacitást igényelnek. Ilyen például a fehérje-hajtogatás [2] mely kritikus a része a modern gyógyászati kutatásnak. Az orvostudomány mellett az anyagtudományban is óriási előrelépést tudd elősegíteni a kvantuminformatika. Az anyagtudomány esetében anyagok tulajdonságainak szimulációját lehet felgyorsítani [3] [4] kvantum algoritmusok segítségével. Mint látható a kvantumszámítógépek kritikus részt fognak játszani a modern világ fejlődésében, ezért is fontos a kvantumkommunikáció. Kvantumkommunikáció segítségével nemcsak biztonságos kommunikációs médiumot tudunk majd létrehozni, hanem lehetővé teszi egymástól földrajzilag távol lévő kvantumszámítógépek közötti együttműködést is.

Kvantumkommunikáció során a kvantuminformációt legtöbb esetben fotonokon keresztül közvetítjük. Az optikai kvantumkommunikációt a közvetítésre felhasznált médium alapján két további részre oszthatjuk, melyek az üvegszálas és a szabadtéri kvantumkommunikáció. Az üvegszállas kvantumkommunikáció esetén egy kontrolált médiumon (az üvegszálon) keresztül küldjük a fotonokat. Az üvegszál alapú rendszernek az egyik legnagyobb előnye, hogy a küldési közeg a kontrollunk alatt van, viszont kötve vagyunk az infrastruktúrához, nem tudjuk szabadon változtatni az útvonalainkat. Szabadtéri kvantumkommunikáció esetében a közvetítő közeg a két kommunikációs állomás közötti tér. Mivel szabadtéri kvantumkommunikáció során nincs egy előre kiépített csatorna, a kommunikáció során kell számolni különféle kaotikus zavarokkal, viszont nincs kötve az előre kiépített infrastruktúrához így sokkal nagyobb lefedettséget is el lehet érni. A szabadtéri kvantumkommunikáció előnyeit többszörösen fel lehet erősíteni műholdas köztes csomópontok bevonásával. Műholdak segítségével akár egy az egész földet lefedő hálózatott létre lehet hozni.

Kvantumösszefonódás alapú hálózatok segítségével nemcsak biztonságos kommunikációt, hanem világ egymástól távoli pontjain lévő kvantumszámítógépek együttműködését lehet elő-

gíteni. A kvantumkommunikációt támogató tulajdonságai miatt kutatásunk során összefonódás alapú műholdas hálózatokkal dolgoztunk. Célunk egy minimális teljes földet lefedő műholdas kvantumhálózat költségeinek csökkentése egy olyan útvonalkereső algoritmus segítségével, mely kis elemszámú hálózatokban képes egy minimális optmiális rátát biztosítani.

A TDK dolgozat felépítése a következő. A második és harmadik fejezetekben röviden ismertetjük a szükséges kvantumkommunikációs és műholdas alapkoncepciókat. Utána a negyedik fejezeben a műholdas kvantumkommunikációs architektúrák mai állását mutatjuk be. Majd az ötödik fejezeben bemutatjuk az általunk fejlesztett REBSAN (Routing in entanglement-based satellite networks) algoritmust. A hatodik fejezetben az elkészült szimulátort ismertetjük. Végül az hetedik és nyolcadik fejezedben a szimulációs eredményeinket prezentáljuk.

2. - Kvantumkommunikációs bevezető

Munkánk során a kvantumösszefonódás-csere egyik tulajdonságát használtuk ki az algoritmusunk létrehozásához. A kvantumösszefonódás-csere megértéséhez szükség van pár kvantumkommunikációs fogalom tisztázására, ezek a kvantumbit, a szuperpozíció, a kvantumkapuk és a kvantumösszefonódás. Fontos még megismerni a bra-ket jelölést is, melyet az angol származású Paul Dirac hozott létre 1939-ben. Ahogy a neve is sejteti a bra-ket két új jelölést vezet be. A $|v\rangle$ (Ket v) egy V komplex vektortérben elhelyezkedő vektort jelent. Ez kvantum mechanikán belül az adott rendszer állapotát jelöli. A bra jelölés a $\langle f|$ formátumot követi. Itt f egy olyan funkciót jelöl mely a komplex vektor térhez egy-egy komplex számot rendel. A $\langle f|v\rangle \in \mathbb{C}$ egy lineáris funkció a v komplex vektoron.

I. Zárt fizikai rendszer állapota egy olyan egységnyi $|\phi\rangle \in H$ állapotvektorral írható le mely komplex együtthatókkal rendelkezik.

II. A rendszer időbeli változásai leírhatók unitér transzformációkkal amennyiben ismerjük a kezdő és végső állapotot.

III. Legyen X a mérés lehetséges eredményeinek halmaza. Egy mérés felírható a mérési operátorok halmazával azaz: $M = M_X, x \in X, M_X \in H$. Ha a rendszer állapota := $|\phi\rangle$ akkor $P(x|\,|\phi\rangle) = \langle\phi|\, M_X^T M_X\, |\phi\rangle$ és a mérés utáni állapota a rendszernek pedig: $|\phi\rangle = \frac{M_X|\phi\rangle}{\sqrt{p}_x}$

IV. Egy W kompozit rendszer állapotát meghatározható az őt felépítő V és Y rendszerek állapotából az az: $w = x \otimes y$ ahol $w \in W$ és $y \in Y$.

Az egyes posztulátumoknak meg lehet feleltetni egy-egy kvantumszámítógéphez szükséges fogalmat:

- Első posztulátum – Kvantumbit
- Második posztulátum – Kvantumlogikai kapuk
- Harmadik posztulátum – Kvantum állapotok mérése
- Negyedik posztulátum – Kvantumregiszterek

2.1. Kvantumbit

A kvantumbit a bit kvantuminformatikai megfelelője. A kvantumbit ábrázolható egy $|\phi\rangle$ vektorral. A vektor felírható a két vektor komplex amplitúdójú szorzatával: $|\phi\rangle = \alpha\binom{1}{0} + \beta\binom{0}{1}$, ahol $\alpha, \beta \in \mathbb{C}$ valószínűségi változók és $|\alpha|^2 + |\beta|^2 = 1$ valószínűségi eloszlás. Ez az ábrázolás látványosabb és elégséges az egyszerűbb rendszerek ábrázolásához. A rendszer dimenziószámának emelkedésével kevésbé lesz követhető ez a jelölés. Ennek következtében a bra-ket jelölést fogom a továbbiakban használni így $|0\rangle = \binom{1}{0}$ és $|1\rangle = \binom{0}{1}$. Az eredeti egyenletünk pedig az új alakban $|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ lesz. Amennyiben egyik valószínűségi változó sem 0, a kvantumbit egy úgynevezett szuperpozícióban van. Szuperpozíció során a kvantum állapotok összeadódnak, hasonlóan a hullámokhoz a klasszikus fizikában. Egy szuperpozícióban lévő kvantumbit mérésének eredményét a teljes rendszer állapotának ismeretében sem lehet megjósolni.

2.2. Kvantumkapuk

A kvantumkapuk unitér operátorok melyek segítségével kvantumbiteken hajtunk végre változtatásokat. Többféle kvantumkaput ismerünk melyek egy vagy több elemű kvantumbit rendszereken hajtanak végre módosításokat. Míg a kvantumbiteket vektorokkal, a kvantumkapukat mátrixokkal jelöljük, így a kvantumkapuk hatásait mátrix műveletként jellemezhetjük. Kvantumkapuk esetén fontos kitétel, hogy kötelezően unitér transzformációk kell legyenek, azaz minden N kvantumkapura igaz, hogy $NN = I$ ahol I egy N-nel megegyező dimenziójú identitás mátrix.

2.3. Kvantumösszefonódás

A kvantumösszefonódás a kvantumhálózatok egy fontos építőköve. Egy kvantum rendszer összefonódott állapotban van, ha rendszer elemeinek állapotai nem írhatóak le egymástól függetlenül. Másnéven a rendszer egy részhalmazának megmérésével következtetni lehet a teljes rendszer mérési eredményére. Például vegyünk két szuperpozícióban lévő kvantumbitet. Ha a két kvantumbit összefonódott állapotban van akkor az egyik kvantumbit mérési eredményéből ki tudjuk következtetni bizonyossággal a másik kvantumbit mérési eredményét anélkül, hogy azt elvégeznénk. Többféle összefonódási állapot is létezik, ezek közül a Bell-állapotokat (EPR-párok) használják legtöbb esetben, mivel ezek egymásra ortogonálisok és így könnyen megkülönböztethetőek. Ezek sorrendben:

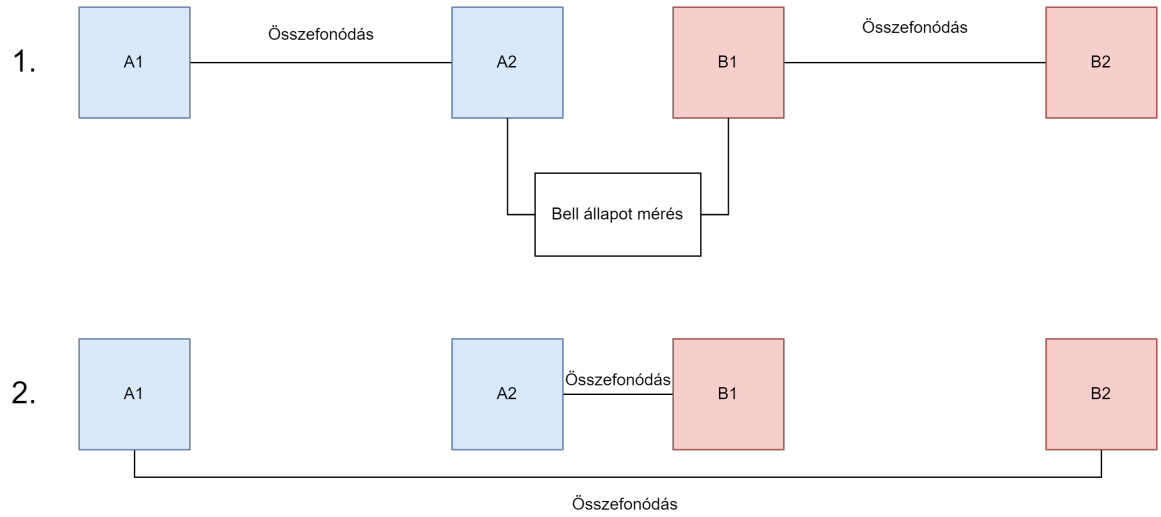
$$\beta_{00} = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad \beta_{01} = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$
$$\beta_{10} = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \quad \beta_{11} = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

2.1. ábra. A 4 darab Bell pár felírása bra-ket jelöléssel.

Amikor kvantum összefonódásról beszélünk, általában a fentebb említett párok egyikét használjuk. Ezek a kvantum összefonódás párok több modern kvantumkulcsszétosztó rendszer alapját is képezik. Ezek az algoritmusok lehetnek pont-pont kapcsolati rendszerek mint az E91 protokoll [5], vagy modern többszereplős rendszer mint [6] és [7].

2.4. Kvantumösszefonódás-csere

A kvantumösszefonódás-csere felfedezése egy fontos lépés volt a kvantumkommunikáció fejlődésében. Először a Genfi egyetemen [8] hajtották végre, egymástól független összefonódott fotonpáron. A kvantumösszefonódás működése a 2.2. ábrán látható. Az ábrán található kezdő állapot két összefonódott kvantumbit párból áll, $A_1 - A_2$ és $B_1 - B_2$. Ezen a két kvantumbit páron hajtjuk végre a Bell állapot mérést (Bell state measurment – BSM).

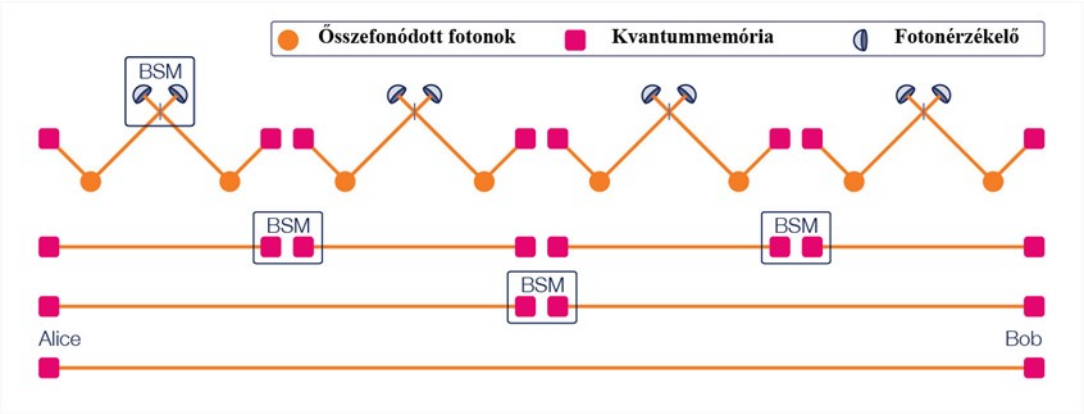


2.2. ábra. Kvantumösszefonódás-csere BSM által. Az ábra tetején a két összefonódott foton pár található, míg az ábra alján a megcserélt összefonogassuak.

A BSM hatására létrejön a 2.2 ábra alsó részén látható állapot. Az A_2 és B_1 kvantumbitek melyeken a Bell állapot mérést hajtottuk végre, összefonódott állapotba kerülnek és emellett az $A_1 - B_2$ kvantumbitek is összefonódnak. Az utóbbi az egyik legfontosabb tulajdonsága a kvantumösszefonódás-cserének, mivel az $A_1 - B_1$ kvantumbit pár úgy került összefonódott állapotba, hogy azok nem kerültek fizikai interakcióba.

2.5. Kvantumismétlő

A kvantumismétlők bár felépítésben és működésben is különböznek klasszikus párjuktól hasonló funkciót töltenek be. Üvegszál alapú kvantumkommunikáció esetén fő feladatuk a jelerősítés, hiszen pár száz kilométer után nagyon megnő a csillapítása az üvegszálnak. Szabadtéri kvantumkommunikáció esetén a köztes kvantumismétlő csomópontoknak nem csak a jel erősítése, hanem annak irányának változása is feladata. Fontos megjegyezni, hogy bár a kvantumismétlőkre mint egy egyszerű újrajátszó állomás hivatkozunk, korán sem ez a helyzet. A kvantumbiteket nem lehetséges másolni annak klónozhatatlansági tulajdonságai [9] miatt, így más megoldáshoz kell folyamodni, hogy egy kvantumhálózatot hozzunk létre.



2.3. ábra. Kvantumösszefonódás propagálása Alice és Bob között összefonódás-csere segítségével.

A fent említett klónozhatatlansági problémára egy megoldás a 2.3 ábrán látható rendszer. A kvantumösszefonódás-csere többszörös egymás utáni használatával egymástól távoli pontok között is meg lehet osztani kvantumösszefonódást. A létrejött összefonódott kvantumbitpárt fel lehet használni további kvantum információ küldésére [10].

3. - Műholdas rendszerek

Napjainkban a nagy méretű alacsony pályás műholdas konstellációk már-már mindennapossá váltak. Ma már lehetőség van arra, hogy egy civil lakos hozzáférjen az egyik legnagyobb alacsony pályás műholdas konstellációhoz egy párszázezer forintos ár megfizetése után [11]. A műholdashálózatok nemcsak a klasszikus, hanem a kvantum kommunikációban is megjelentek. Szabadtéri kvantumkommunikációban a zavar legnagyobb része a két pont közötti térben keletkezik a légkörben található molekuláknak köszönhetően. Ezek a molekulák nemcsak elnyelik a fotonokat, hanem szórják is azokat ezzel növelve a csatorna zavarrátáját. A zavarráta arányosan csökken a levegőben található molekulák számával, így egy két műhold közötti kapcsolat hibaaránya jóval alacsonyabb, mint egy hasonló távolságú földi csomópontok közötti kapcsolaté. Az alacsony hibaarány és nagyobb lefedettségnek köszönhetően a műholdas rendszereken alapuló kvantumkommunikáció egy fontos sarokköve lesz a jövő kvantumhálózatainak.

3.1. Műholdpályák

Műholdas hálózattokat és rendszereket rendszerint az őket alkotó műholdak pályái alapján kategorizáljuk. Egy műhold pályája az adott égitest körüli folyamatos mozgását írja le. Az adott pályát lehet csoportosítani annak magassága vagy középpontja szerint is. A műholdak föld körüli pályáinak több kategorizációja is létezik ezek közül a legismertebbek a következőek.

Az alacsony pályán keringő (Low Earth Orbit - LEO) műholdak maximális távolsága a föld felszínétől nem haladja meg az 1000 kilométert. A LEO pálya földhöz való közelsége több szempontból is előnyös tudd lenni űrmissziók során. A felszín közelségének köszönhetően műholdas képalkotásra és optikai kommunikációra is gyakran használják. A nemzetközi űrállomás is LEO pályán kering a föld körül mivel az alacsony (408 km) pályának köszönhetően a hasznos terheket kisebb távolságon keresztül kell szállítani.

A közepes föld körüli pályák (Medium Earth Orbit - MEO) határai a 2000-36000km melyek közül a leggyakoribb a 20000 kilométerre található a föld felszínétől. Ezt a pályát nagyon gyakran használják a navigációs műholdak, például az európai Galileo rendszer. A Galileo biztosítja a navigációs kommunikációt Európa-szerte, és számos navigációs célra használják, mint például

okostelefonos tájékozódás vagy különböző eszközök követése. A Galileo egy több műholdból álló konstellációt használ, hogy egyszerre a világ legtöbb részére kiterjedő lefedettséget biztosítson.

A Geoszinkron (Geosynchronous Earth Orbit - GEO) egy speciális a föld felszínétől 35786 kilométerre található pálya. A GEO pályán keringő műholdak a felszín egy adott pontjáról, egy adott pillanatban mindig ugyanott látszanak. A legtöbb műholdas TV adást biztosító műhold GEO pályán található ezért nincs szükség az antennák folyamatos mozgatására.

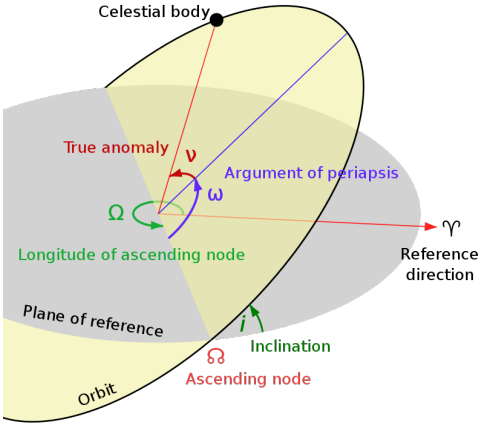
3.2. Műholdpálya propagátorok

A pálya propagátorok segítségével ki lehet számítani egy adott űreszköz helyzetét egy adott időpontban. Ahhoz, hogy egy műhold későbbi helyzetét ki tudjuk számítani szükséges nemcsak a pozícióját megadni, hanem mozgásának valamilyen leíróját is. Több műholdpályaleíró rendszer is létezik az egyik leghíresebb a TLE (Two Line Element set) mely a kepleri pályaleíróknak egy kiterjesztését használja. A TLE alapját Max Lane 1860-as űrbéli ellenállással kapcsolatos kutatása képezte [12]. Max Lane kutatását továbbfejlesztve hozta létre a ma ismert TLE-t a NORAD (North American Aerospace Defense Command), mely eredetileg lyukkártyákra lett tervezve. A TLE egy mai napig használt leírója különböző űrben található tárgyak (űrállomások, műholdak, űrszemét) pályáinak. Mint ahogy az a 3.1 ábrán is látható a TLE két sorában található információkat két kategóriába lehet osztani. Az ábrán pirosan jelölve az adott rendszer azonosítására szolgáló információk találhatóak, míg zölden a rendszer pályáját befolyásoló információk találhatóak.

```
ISS (ZARYA)
1 25544U 98067A   08264.51782528 -.00002182  00000-0 -11606-4 0  2927
2 25544  51.6416 247.4627 0006703 130.5360 325.0288 15.72125391563537
```

3.1. ábra. Nemzetközi űrállomás TLE adatai, az ábrán pirossal vannak jelölve az azonosításra használt elemek, zölddel pedig a pályaelemeket tartalmazók mezők.

A Kepleri pályaleíró nevét alkotója Johannes Kepler után kapta. A Kepleri pályaleíró a TLE-nél egy egyszerűbb rendszert feltételez, ennek következtében pontatlanabb hosszútávon. A hosszútávú pontatlansága nem volt kritikus számomra hisz az általam végzett szimulációk nem voltak hosszabbak négy óránál. A 3.2 ábrán a különböző pályaelemek láthatóak, míg a 3.1 táblázaton a különböző elemek magyarázata és jelölése.



3.2. ábra. Kepleri pálya rendszer vizuális bemutatása, a változókhoz tartozó részletes magyarázatok a 3.1. táblázatban találhatók.

Semimajor axis (a) - a pálya földtől felvett legnagyobb távolsága

Inclination (i) - pálya egyenlítővvel bezárt szöge

Eccentricity (e) - a tökéletes körtől való eltérése a pályának

Longitude of the ascending node (Ω) - pálya referencia ponttal bezárt szöge

Argument of periapsis (ω) - a pálya legmagasabb pontja és a referencia pont által bezárt szög

True anomaly (ν) - a test hol helyezkedik el a pályán annak legmagasabb pontjához képest.

3.1. táblázat. A Kelperi pályarendszer elemeinek részletes leírása

3.2.1. Poliastro

A Poliastro [13] egy python alapú pályapropagátor és vizualizáló alkalmazás. A főként Juan Luis Cano Rodríguez által fejlesztett szimulátor munkám kezdetekor még gyerekcipőben járt ezért nem esett rá a választásom. Viszont az utóbbi időben nagy fejlődésen ment keresztül, ami látható a dokumentációs oldalán is [14]. A teljesség igénye nélkül néhány a funkciói közül: atmoszféra adatainak modellezése vizualizációja; pálya vizualizáció Celsium [15] segítségével; műholdak földi nyomvonalainak bemutatása; manőverek és azok pályára való hatásainak vizualizálása

Mint látható, a Poliastro egy részletes és funkciógazdag szimulátor, ami mellett támogat több vizualizációs technikát is. Két okból nem esett rá a választásom. Amikor először rátaláltam dokumentációja, funkciói is hiányosak voltak ezért nem volt alkalmas számomra, emellett az optikai áteresztés számolásához használt QSCS [16] kódja Java-ban íródott. A Java python keresztbe hívások pedig megnehezítették volna a szimulátor létrehozását.

3.2.2. Orekit

Az Orekit egy alacsony szintű űrdinamikai szimulációs könyvtár, mely 2008 óta open-source [17]. A könyvtárat a világ minden táján használják: a Svéd Űrtársaságtól (SSC) kezdve egészen az Amerikai haditengerészeti kutatólaboratóriumig (NRL). A könyvtár funkcionalitásai a Poliastrohoz képest sokkal alacsonyabb szintűek. Ezek, a teljesesség igénye nélkül, a következőek: lézer alapú mérések alapján a pálya meghatározása; különböző manőverek szimulációja; egy, két vagy több test alapú propagáció és forgó test követése az orbitális pályán.

Természetesen az előbb felsorolt szimulátorok mindegyike képes a legtöbb orbitális pályarendszer mentén progagálni a műholdakat. Választásom végül azért esett az Orekit-re mivel ez a szimulátor egy működő kiadott verzió volt (általam használt verzió: 10.3), java-ban íródott és sok változatos helyen használják, ezért a kijelölt fórumán [18] és weboldalán [19] könnyedén lehetett segítséget kapni.

4. - Műholdas kvantumkommunikáció napjainkban

Hét évvel ezelőtt, 2015-ben kezdtek felbukkanni a műholdas kvantumkommunikáció megvalósíthatóságának első jelei. Az első kvantumösszefonódást demonstráló SpooQy-1 [20] nanoműholdat 2019 áprilisába állították pályára. Bár a szingapúri kutató csapat csak 2020-ra tudta publikálni kutatását, az előkészületeket már 2015-ben megkezdték.

2017-ben a kínai Micius kvantumműhold segítségével hoztak létre összefonódást Delingdha és Lijiang között. A kísérlet elött a legnagyobb távolság, amin keresztül kvantumösszefonódást tudtak létrehozni pár száz kilométer volt. Ezzel szemben a kínai kutatók két egymástól 1200 kilométerre található pont között hozták létre az összefonódást [21]. Ennek segítségével végül 2020-ban összefonódás alapú kulcsszétosztást is végrehajtottak [22].

A Micius kvantumműhold segítségével a kínai kutatók 2018-ban világon elsőként hoztak létre kvantumcsatornán keresztül kulcsokat kontinensek között. A kísérlet során a kutatók Ausztria és Kína között osztottak meg biztonságos kommunikációhoz szükséges kulcsokat. A megosztott kulcsok segítségével ezután klasszikus csatornán keresztül osztottak meg képeket egymás között a kutató csoportok [23].

4.1. Műholdas kvantumkommunikációs architektúrák

Kvantumműholdas architektúrák tervezésével foglalkozó kutatások egyre gyakoribbak, hiszen műholdak segítségével a szabadtéri kvantumkommunikáció előnyeit még jobban ki lehet használni. Műholdak segítségével nagyobb területek fedhetőek le akár kisebb zavarrátával. Az alacsony zavarráta annak köszönhető hogy bár a földi légtér tele van olyan részecskékkel melyek szórják és/vagy elnyelik a fényt, ezen részecskék koncentrációja csökken a tengerszint feletti magasság növekedésével [24][25].

A műholdas architektúráknak két fő alfaját különböztetjük meg a felhasznált műholdpályák alapján. Az egyrétegű konstellációk csak egy pályamagasságot használnak, az az minden műhold pályája LEO, MEO vagy GEO. Kvantumkommunikációs egyrétegű műholdas architektúrák az alacsony pályás LEO műholdakat használják, mert bár az űrben ritkább az olyan anyagok előfordulása melyek a fényt szórják vagy elnyelik, a távolság növekedésével a fotonnyaláb ke-

resztmetszete is megnövekszik. A nyaláb növekedésével pedig megnőnek a fotonvesztés esélyei is. Az alacsony pályás műholdak használatával a teljes lefedettséghez szükséges műholdak száma felhasznált magasságtól függően több százra nőhet [26].

A többrétegű műholdas architektúrák szintén egy alacsony LEO pályás réteget használnak a földi csomópontokkal való kommunikációra. Az egyrétegű konstellációkkal szemben bevezetnek egy támogató műhold réteget is a közép és/vagy magas Föld körüli pályákon. A támogató rétegek feladata az alacsony pályás műholdak kommunikációjának támogatása, így lecsökkentve a teljes lefedettséghez szükséges műholdak akár számát száz alá. A műholdak számának csökkentésese mellett viszont megnő a rendszer komplexitása, késleltetése és zavarrátája is [27] [28].

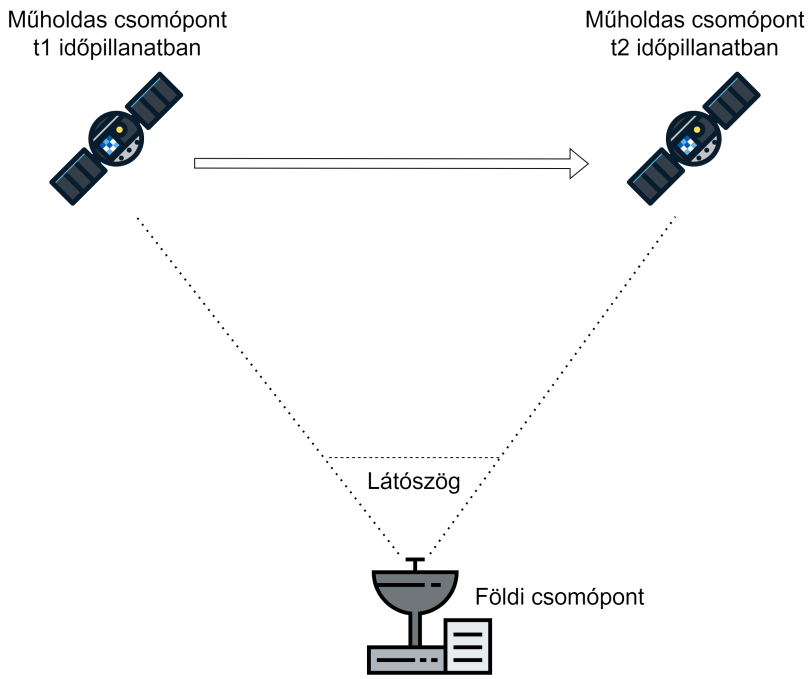
5. - REBSAN algoritmus

Kutatásunk során egy olyan algoritmust próbáltunk létrehozni mely segítségével az előbb felvázolt műholdas architektúráknál alacsonyabb számú műholdak segítségével is egy teljes földet lefedő kommunikációs hálózatott lehet létrehozni. Algoritmusunk tervezése során a már ismert rendszerekkel szemben két fő változást vezettünk be. A földi csomópontok között nem egy folytonos kommunikációs csatornát hoztunk létre, az az voltak időpillanatok amikor két csomópont között nem volt érvényes kommunikációs csatorna. A folytonosság elhagyása nem csak a földi csomópontok közötti kommunikációra volt igaz. Műholdjaink közötti kommunikációt egy tárolás-és-továbbítás (Store-And-Forward) technikára cseréltük. A Store-And-Forward kapcsolatok esetén a kvantumműholdak nem folytonos átjátszást hajtottak végre, hanem a létrehozott kvantumösszefonódásokat kvantummemóriájukban tárolták egészan addig míg a REBSAN algoritmus szerinti optimális küldési idő és cél nem került be a látóterükbe.

5.1. Idővariáns gráfok

Algoritmusunkban a műholdak egymás közötti láthatósági intervallumainak a modellezésére Idővariáns gráfokat (Time-Varying graph) [29] használtunk. Az idővariáns gráfok segítségével statikusan lehet ábrázolni időben változó gráfokat. Ehhez a statikus gráf éleit azok dinamikus megfelelőinek előfordulási pillanataival címkézzük. Idővariáns gráfok segítségével könnyedén lehet gyorsan változó rendszereket átláthatóan modellezni. Modellezési tulajdonságait több területen is használják mesterséges intelligencia kutatástól kezdődően [30], ütemezési algoritmusokon [31] keresztül egészen Műholdas rendszerekben való útvonaltervezésig[32].

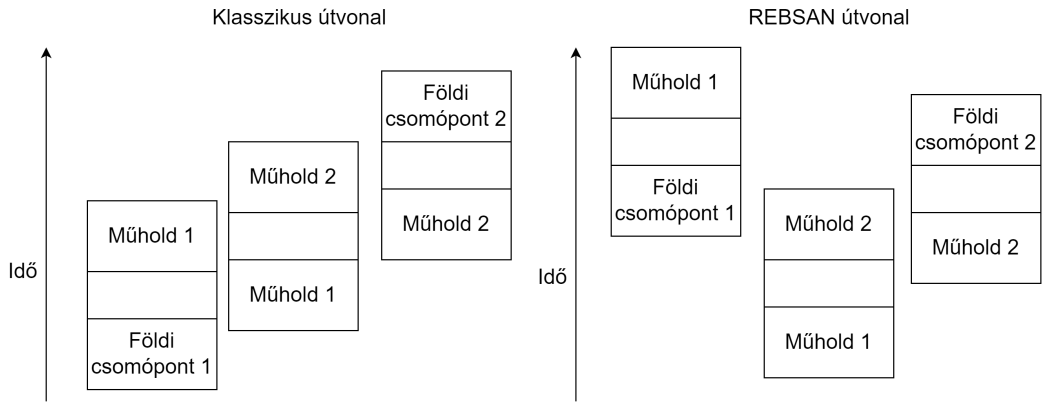
Kutatásunk során az idővariáns gráfok egy módosított verzióját használtuk. A gráfban a csomópontok egy-egy műholdas vagy földi csomópontot jelöltek. Két csomópont közötti élen nemcsak az időintervallumokat címkéztük, hanem az adott időintervallumban a két csomópont közötti optikai-transzmittanciát is. Például ha az 5.1 ábrán található rendszert vesszük alapul a földi és a műholdas csomópontok között egy $\overset{[t_1,t_2]\ \mu[...]}{\longrightarrow}$ él lesz, ahol a t1 és t2 az időintervallum kezdetét és végét jelölik és μ pedig az optikai-transzmittanciát.



5.1. ábra. Az adatértelmezést segítő ábra. Az ábrán található két csomópont (egy földi és egy műholdas) közötti láthatósági intervallum látható. A két csomópont közötti láthatóság szerint hozzuk létre a címkézést az idővariáns gráfon belűl.

5.2. REBSAN algoritmus

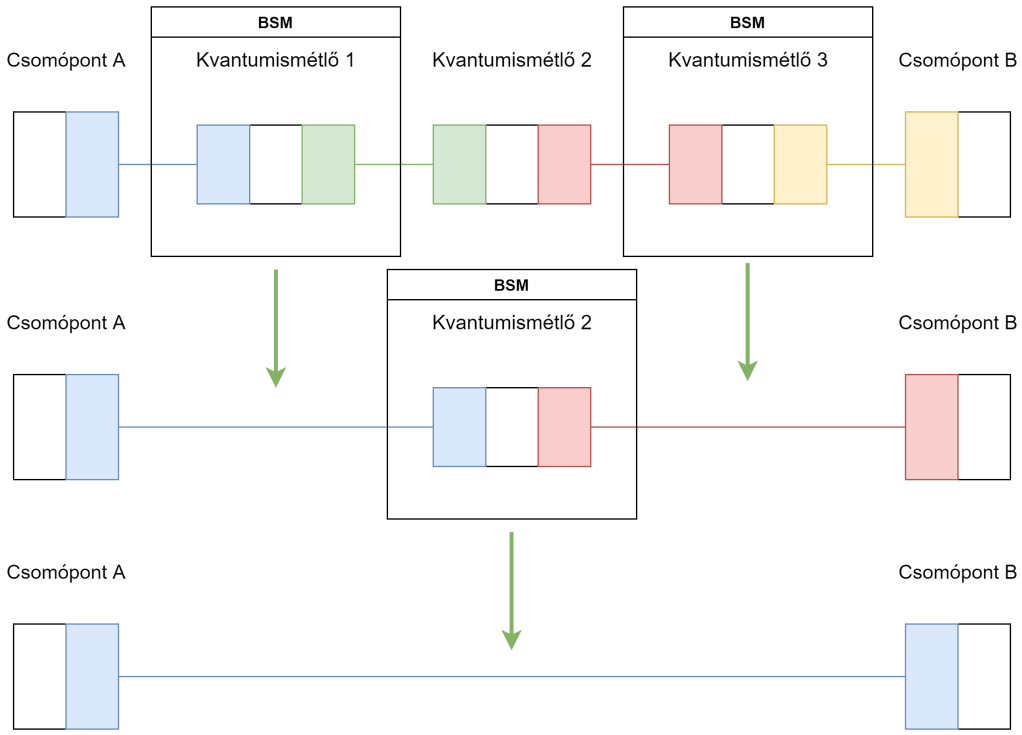
Miután a dinamikusan változó műholdas hálózattokat átalakítottuk egy statikus idővariáns gráffá, már csak a földi csomópontokat összekötő útvonalakat kellet megtalálni. Az általunk létrehozott REBSAN algoritmus egyik legnagyobb előnye és újdonsága az általa generált utak időbeli szabadsága. Az útvonalak éleinek nem szükséges időben egymás követniük, mint az ahogy az 5.2 ábrán is látható. Az ábra bal oldalán a klasszikus útvonal időintervallumait láthatjuk. Az ábra jobb oldalán pedig az új útvonaltervező algoritmusunk egy útvonala található melyen látható, hogy a REBSAN algoritmus sokkal szélesebb választékból tudja kiválogatni útvonalaihoz a láthatósági időintervallumokat.



5.2. ábra. A klasszikus és a REBSAN által létrehozott útvonalak összehasonlítása. Függőlegesen tengelyen az idő található. A vízszintesen tengelyen pedig az útvonalon belüli sorrend látható.

5.2.1. A REBSAN algoritmus mögötti ötlet és működése

Mint azt előbb említettük a REBSAN algoritmus több lehetséges útvonalat tudd találni időbeli flexibilitásának köszönhetően. Az időbeli szabadságát két kulcs elemének köszönheti. A store-and-forward technikának köszönhetően a műholdak mindig az optimális cél csomópontokkal tudják létrehozni az összefonódott kvantumbiteket. A kvantumösszefonódás csere tulajdonságainak köszönhetően pedig nem szükséges, hogy időben egymás után legyenek a végső útvonal időintervallumai, elég létrehozni az útvonalban egymás mellett szereplő csomópontok között az összefonódást. Az így létrehozott összefonódásokat az 5.3 ábrán is látható módszer szerint az kvantumösszefonódás-csere többszörös alkalmazásával tovább lehet propagálni. A végeredmény egy összefonódottkvantumbit pár az A és B csomópont között.

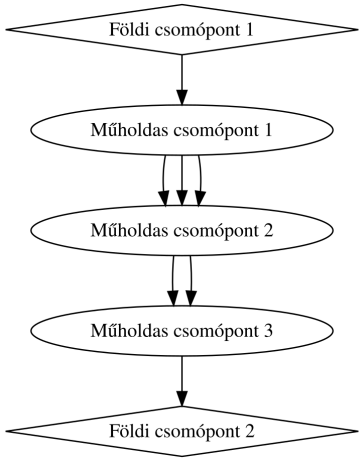


5.3. ábra. Példa az összefonódás-cserén alapuló architektúrára. Az ábrán egy 5 csomópontból álló rendszer működése látható, ahogyan a két fő csomópont között a köztes csomópontok segítségével létrejön az összefonódás.

Az algoritmus működése fő két részre osztható, ezek az útvonalak keresése és azok optimalizálása. Mivel az idővariáns gráfban található élek több időintervallumot is tartalmazhatnak az útvonal keresés során speciális szélességi keresést használtunk. A szélességi keresés nem állt meg abban az esetben, ha talált egy útvonalat a cél csomóponthoz, hanem tovább folytatta míg egy bizonyos előre megszabott mélységet el nem ért. A megállási feltétel módosítására azért volt szükség mert könnyen megtörténhet, az idővariáns gráf tulajdonságainak köszönhetően, hogy a legkevesebb lépésből álló út nem lesz a legkedvezőbb átvitelű. Az így keletkező útvonalak élei az összes csomópontok közötti láthatósági időintervallumot tartalmazzák. Az optimalizálás során ezen útvonalak időintervallumai közül válogattuk ki a legoptimálisabbakat.

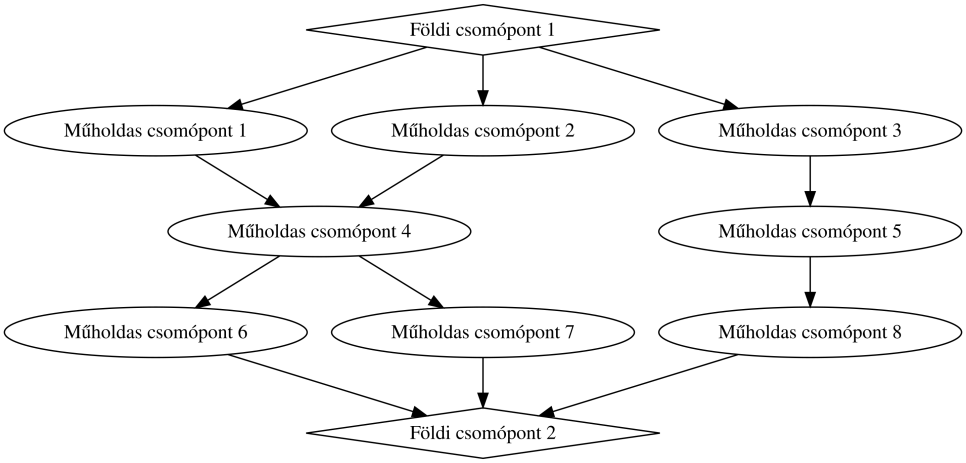
Az optimalizálás bemenete egy útvonal két földi csomópont között. A bemeneti útvonalak mint az ahogy az az 5.4 ábrán is látható, az összes csomópontok közötti láthatósági időintervallumot tartalmazzák. Az optimalizálás során az egyik földi csomópontból kiindulva iteratívan végig vesszük az összes láthatósági intervallum kombinációját. Minden újabb iteráció során ellenőrizzük, hogy az adott időintervallum hozzáadása során létrejövő időintervallum-útvonal belefér-e az algoritmusnak előre megszabott konstans időkorlátba. Az időkorlátra kvantummemória helyi és időbeli tárolókapacitásának végessége miatt volt szükség. Legfőbb ok a kettő közül az idő-

beli tárolókapacitás volt, hiszen hosszútávon a tárolt kvantumbitek elvesztik koherenciájukat, aminek következtében nem lehet őket összefonódás-cserére felhasználni.



5.4. ábra. Példa útvonal az idővariáns gráfban két földi csomópont között.

A teljes optimalizálás lefutása után eredményként egy sor időintervallum útvonalat kaptunk a két csomópont között. Kihasználva a tényt hogy egy műholdas optikai hálózat optikai áteresztése a földi állomásokat tartalmazó linkjein a legalacsonabb [33] , le tudjuk egyszerűsíteni az optimális útvonalak megtalálását a két csomópont között, anélkül hogy a linkek terhelését figyelmen kívül kéne hagyjuk. Az útvonal listákat összevonva egy maximális párosítási feladatot kapunk, ahol a két csomópont halmaz a földi csomópontok időintervallumainak végződései, az időintervallum útvonalak optikai áteresztése pedig az élek súlyozása. Az így kapott maximális párosítási problémát pedig könnyedén megoldhatjuk a Magyar módszer [34] felhasználásával. A REBSAN algoritmus kimenete egy az 5.5 ábrán is látható gráfhoz hasonló útvonal rendszer minden csomópont párhoz.



5.5. ábra. Példa kimeneti időintervallumútvonalgráf két földi csomópont között.

6. - Az elkészült szimulátor

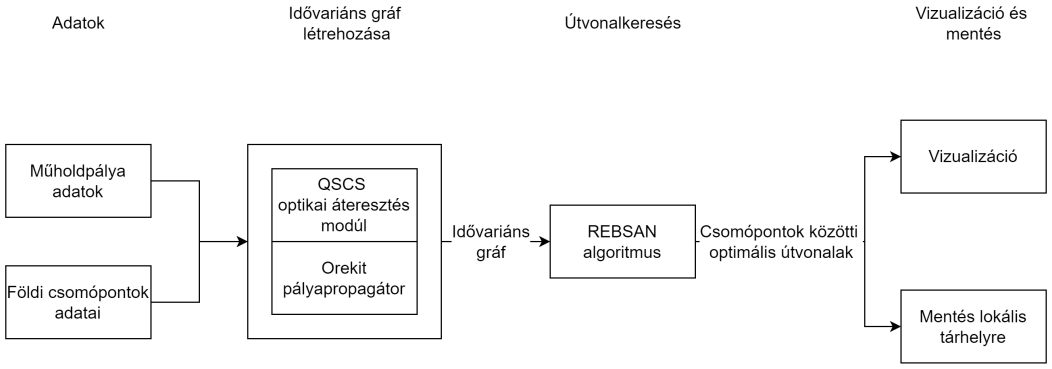
Az állatunk készített szimulátor az előző fejezetekben bemutatott rendszerekből és a QSCS [16] optikai áteresztést szimuláló moduljából állt. Az idővariáns gráf létrehozásához szükséges dinamikus láthatósági gráfokat az Orekit pályaszimulátor felhasználásával hoztuk létre. Az elkészült szimulátor négy logikai részre osztható, melyek interakciója a 6.1 ábrán látható. Az elemek, mint ahogy az az ábrán is látható, balról jobbra sorrendben hajtják végre feladataikat. Az elemek futási sorrendben a következőek:

1. Adatok: A műholdrendszerek Kepleri pályaadatait és a földi csomópontok földrajzi koordináta-rendszeri adatait tartalmazzák. Összesen 6 műholdas rendszert használtunk fel kutatásunk során, ezek részletes leírása a 6.2 fejezetben található.

2. Idővariáns gráf létrehozása: Az Orekit műholdpropagációs moduljának segítségével a bemeneti adatokból kiszámoljuk a földi és műholdas csomópontok közötti láthatósági időintervallumokat. A generált időintervallumok alapján pedig létrehozzuk az idővariáns gráfot.

3. Útvonalkeresés: Az előző fejezetben is bemutatott REBSAN algoritmus segítségével minden földi csomópont között megkeressük az optimális útvonal rendszereket.

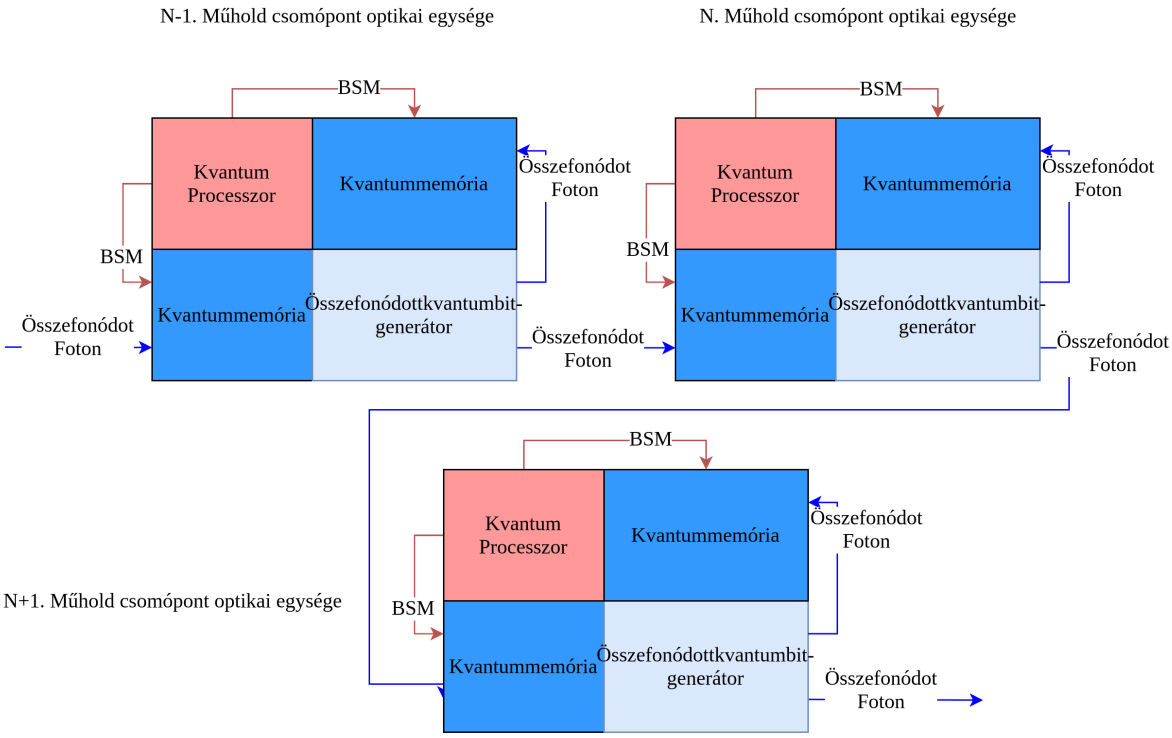
4. Vizualizáció és mentés: Ebben a fázisban a már elkészült útvonal rendszereket elmentjük és az adatokat vizualizáljuk.



6.1. ábra. A szimulátor felépítése mely négy fő logikai részből és a hozzájuk tartozó modulokból áll. A logikai modulok a következőek: Adatok, Idővariáns gráf létrehozása, Útvonalkeresés és a Vizualizáció.

6.1. Műholdas kvantumismétlő felépítése

A szimulációhoz felhasznált műholdas kvantumismétlők részletes bemutatása a 6.2 ábrán látható. Az N. műhold a generál egy összefonódott kvantumbitpárt. A pár első tagját elmenti a saját kvantummemóriájába míg a másodikat a következő $N+1$. műhold kvantummemóriájába küldi. Az $N-1$. műhold hasonlóan, az N. műholdnak a kvantummemóriájába is küld egy kvantumbitet. Eredménykép az N. műhold két kvantummemóriájában az $N-1$. és $N+1$. műholdakkal összefonódott kvantumbitek találhatóak. Az N. műhold alkalmazza a két kvantummemóriájában található kvantumbiteken a BSM mérést, aminek hatására az $N-1$. és $N+1$. műholdak kvantummemóriájában maradt kvantumbitek összefonódnak egymással. Az előbb bemutatott műveletnek az ismételt használatával létre lehet hozni összefonódott kvantumbitpárokat egymástól távol lévő földi csomópontok között.

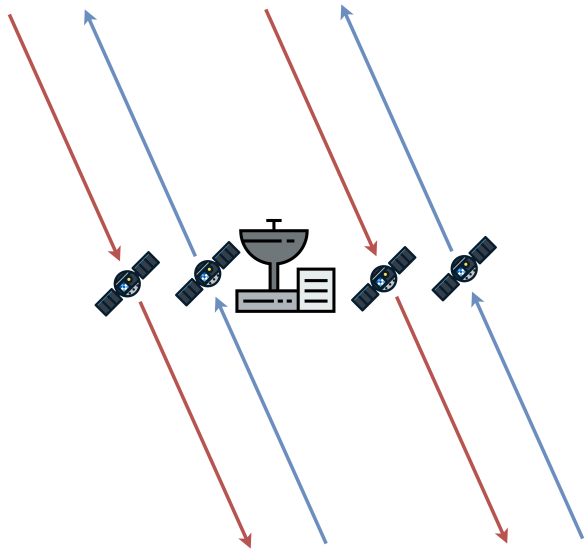


6.2. ábra. A műholdas kvantumismétlő felépítése, sötétkéken a két kvantummemória, pirosan a kvantumprocesszor és az általa végrehajtott BSM, míg világoskéken a összefonódottkvantumbit-generátor látható.

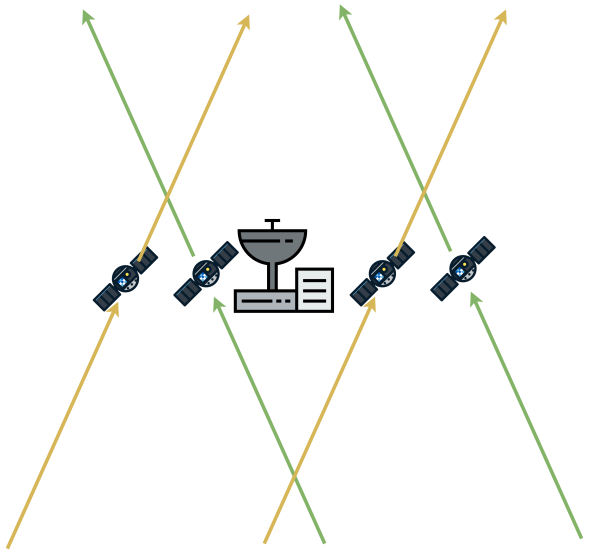
6.2. Felhasznált műhold rendszerek

Munkánk során többféle műholdas konstellációt használtunk, hogy többféle, más-más csomópont számosságú műholdas architektúra mentén is tudjuk az algoritmusunkat tesztelni. A felhasznált konstellációkat két fő architektúra mentén hoztuk létre, melyek különböző műholdak

közötti láthatósági intervallumokkal dolgoztak. Az első ilyen architektúra a retrográd (továbbá RETRO), mely rövidebb láthatósági intervallumokat használt nagyobb gyakorisággal. A láthatósági intervallumok lerövidítését, mint ahogy az a 6.3 ábrán is látható, minden második műholdaspálya inklinációjának 180° fokos eltolásával értük el. A második felhasznált pályaarchitektúra a keresztező (továbbá CROSS), ahol hosszabb, de alacsonyabb gyakoriságú láthatósági intervallumokat hoztunk létre. Az architektúra fő különbsége a RETRO architektúrával szemben, hogy mint az a 6.4 ábrán is látható, minden második műhold az előzőre merőleges pályát követ.



6.3. ábra. Retrográd műholdas architektúra vázlatos bemutatása.



6.4. ábra. Keresztező műholdas architektúra vázlatos bemutatása.

6.2.1. RETRO műholdas architektúra

Összesen négy RETRO architektúrájú műholdaskonstellációt hoztunk létre. Amint az a 6.1 táblázatban is látható a létrehozott rendszerek csomópontjainak mennyisége 16-tól egészen 64-ig terjed. A műholdpályákat egy már létező STARLINK műhold pályaadataiból származtattuk. Az architektúra célja, a REBSAN algoritmus tesztelése volt különböző méretű rövid láthatósági intervallumos konstellációkon.

	LOW	LOWMID1	LOWMID2	MID
Műholdak [db]	16	32	32	64
Ω intervallum [°]	0 - 180	0 - 180	0 - 360	0 - 360
ω intervallum [°]	0 - 180	0 - 360	0 - 180	0 - 360
i értékek [°]	56.0568 / 236.0568			

6.1. táblázat. A négy műholdkonstelláció pályaadatai.

6.2.2. CROSS műholdas architektúra

A CROSS műholdas architektúrához, mint a RETRO-hoz is, négy műholdas konstellációt hoztunk létre. A CROSS architektúra célja a REBSAN algoritmus tesztelése volt ritkább, de hosszabb láthatósági időintervallumokon. Mint az a 6.2 táblázatban is látható a RETRO architektúrához hasonlóan a konstellációkat alkotó műholdak száma 16-tól 64-ig terjed.

	LOW	LOWMID1	LOWMID2	MID
Műholdak [db]	16	32	32	64
Ω intervallum [°]	0 - 180	0 - 180	0 - 360	0 - 360
ω intervallum [°]	0 - 180	0 - 360	0 - 180	0 - 360
i értékek [°]	56.0568 / 146.0568			

6.2. táblázat. A négy műholdkonstelláció pályaadatai.

7. - Eredmények

Munkánk során a REBSAN algoritmust próbáltuk ki több műholdas konstelláció mentén. Két fő architektúrát használtunk, melyekhez négy-négy konstellációt hoztunk létre. A REBSAN algoritmus hatásfokának mérése érdekében több, az egész bolygót lefedő földi állomást szimuláltunk. Minden konstelláció esetén kiválasztottunk egy kezdő földi csomópontot, ahonnan megmértük az optikai átviteli rátát az összes többi földi csomópont irányába. Az eredményeink számszerűsítésének érdekében, a kapott optikai átvitelekre kiszámoltuk, egy már létező összefonódott kvantumbitgenerátor [35] kimenete alapján, a megosztható összefonódott-kvantumbitek számát. A REBSAN algoritmus ismertetésében már említett maximális útvonal hosszt pedig a pekingi egyetem kutatói munkája alapján [36] egy órában maximalizáltuk. A könnyebb összehasonlítás érdekében az átlagos óránkénti összefonódott kvantumbitekkel (average entangled quantum bits per hour – AEQ/h) számoltunk. Szimulációnkat a következő bemeneti adatokkal futtattuk:

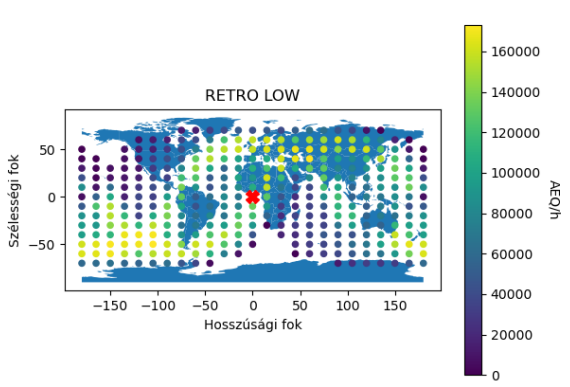
- **Alap STARLINK műhold Kepleri pályája:** a: 1000 [km], e: 0.0002090, i: 56.0568°, Ω: 0°, ω: 0°, θ: 0°
- **Maximális útvonal hossz:** 3600 [mp] [36]
- **Szimulált földi állomások:** Egy csomópont minden 10° széleségi fokra és 15° hosszúsági fokra.
- **Kezdő földi csomópont:** Hosszúság: 0°, szélesség: 0°
- **Az összefonódottkvantumbit-generátor hatékonysága:** 3.5 [kHz] [36]
- **Felhasznált lézer hullámhossza:** 860nm
- **Szimuláció hossza:** 14400 [mp]

7.1. RETRO architektúra

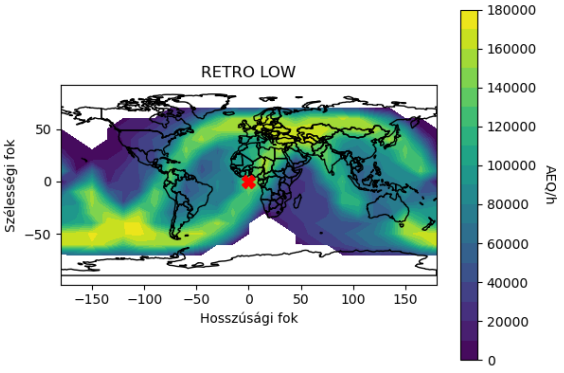
Mint az ahogy az előző fejezetben is taglaltuk a retrográd konstellációk kulcs eleme a páronként egymással retrográd pályát leíró műholdak. Ennek hatására a rendszer láthatósági intervallumai gyakoribbak és rövidebbek lettek.

7.1.1. LOW konstelláció

A LOW konstelláció rendelkezik a legkevesebb műholdas csomóponttal a RETRO architektúrán belűl. Mint az ahogy a 7.1 ábrán is látható, 16 műhold segítségével nem lehet elérni teljes lefedettséget a kezdeti földi csomópontból. A 7.2 ábrán látható hogy a legnagyobb átviteli ráta a kezdeti csomópontból az 56° inklináció vonalán volt mérhető. Bár ez a konstelláció nem tudott teljes lefedettséget nyújtani a 7.1 és 7.2 ábrákon megfigyelhető, hogy a legtöbb földi csomópont felé 80000 AEQ/h nagyságú átviteli rátát tudott biztosítani.



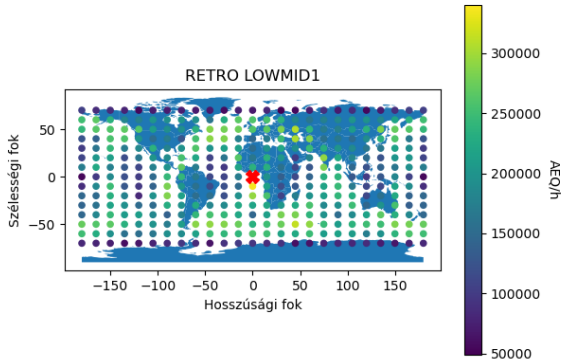
7.1. ábra. Az AEQ/h értéke minden földi csomópontnak a kezdeti pontból számítva. Vízszintes tengelyen a hosszanti koordináták míg a függőleges tengelyen a szelességi koordináták találhatóak. A piros X-el jelölt kezdő földi csomópontból induló útvonalak AEQ/h áteresztőképességét az adott csomópontok színezése jelöli.



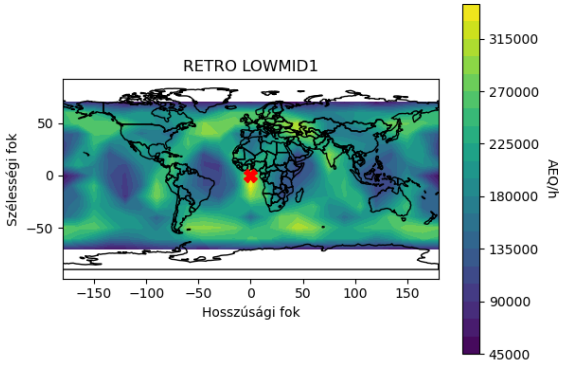
7.2. ábra. Az AEQ/h értéke minden földi csomópontnak a kezdeti pontból számítva kontúros ábrázolással. Vízszintes tengelyen a hosszanti koordináták míg a függőleges tengelyen a szelességi koordináták találhatóak. A piros X-el jelölt kezdő földi csomópontból induló útvonalak AEQ/h áteresztőképességét az adott csomópontok színezése jelöli.

7.1.2. LOWMID1 konstelláció

A 7.3 és 7.4 ábrákat megfigyelve látható hogy a LOWMID1 konstelláció teljes lefedettséget tudd biztosítani mindössze 32 műhold felhasználásával. Érdekességként még látható a 7.4 ábrán egy erősebb dupla spirál alakú vételi sáv.



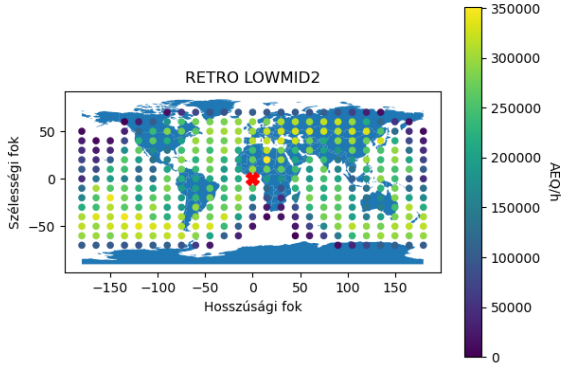
7.3. ábra. Az AEQ/h értéke minden földi csomópontnak a kezdeti pontból számítva. Vízszintes tengelyen a hosszanti koordináták míg a függőleges tengelyen a szelességi koordináták találhatóak. A piros X-el jelölt kezdő földi csomópontból induló útvonalak AEQ/h áteresztőképességét az adott csomópontok színezése jelöli.



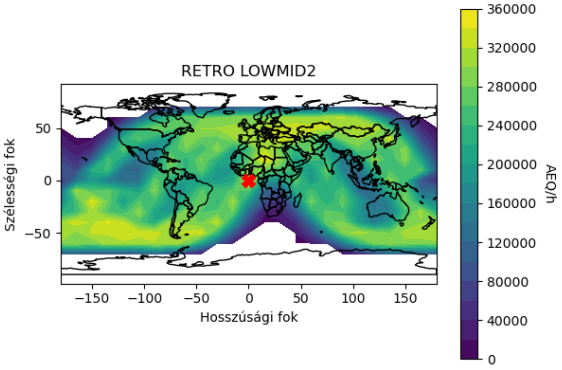
7.4. ábra. Az AEQ/h értéke minden földi csomópontnak a kezdeti pontból számítva kontúros ábrázolással. Vízszintes tengelyen a hosszanti koordináták míg a függőleges tengelyen a szelességi koordináták találhatóak. A piros X-el jelölt kezdő földi csomópontból induló útvonalak AEQ/h áteresztőképességét az adott csomópontok színezése jelöli.

7.1.3. LOWMID2 konstelláció

A LOWMID2 konstelláció esetén, mint ahogy az a 7.5 és 7.6 ábrákon látható, egy hasonló mintázatot figyelhetünk meg, mint a LOW konstelláció esetén. Bár ez a konstelláció nem tudd egy teljes globális lefedettséget biztosítani, sokkal magasabb AEQ/h rátát tudd biztosítani az érintett területeken, mint a LOWMID1 pályarendszer.



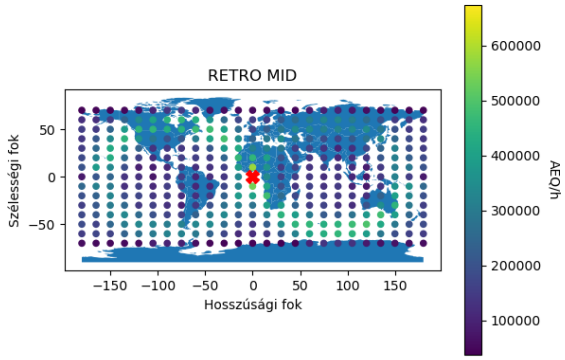
7.5. ábra. Az AEQ/h értéke minden földi csomópontnak a kezdeti pontból számítva. Vízszintes tengelyen a hosszanti koordináták míg a függőleges tengelyen a szelességi koordináták találhatóak. A piros X-el jelölt kezdő földi csomópontból induló útvonalak AEQ/h áteresztőképességét az adott csomópontok színezése jelöli.



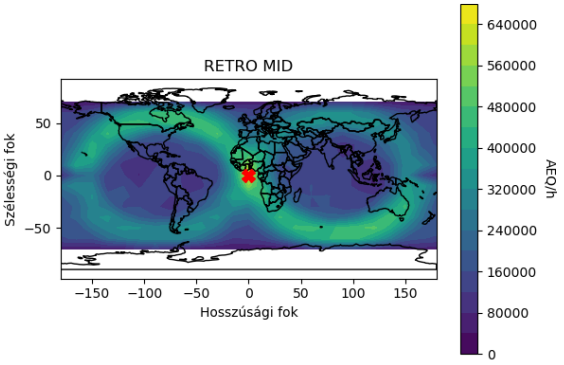
7.6. ábra. Az AEQ/h értéke minden földi csomópontnak a kezdeti pontból számítva kontúros ábrázolással. Vízszintes tengelyen a hosszanti koordináták míg a függőleges tengelyen a szelességi koordináták találhatóak. A piros X-el jelölt kezdő földi csomópontból induló útvonalak AEQ/h áteresztőképességét az adott csomópontok színezése jelöli.

7.1.4. MID konstelláció

Az összesen 64 műholdból álló MID konstelláció a legnagyobb a RETRO architektúrán belül. Ahogy az a 7.7 és 7.8 ábrákon is látható, mint a LOWMID1 ez a konstelláció is teljes lefedettséget biztosít egy jóval nagyobb AEQ/h rátával. A 7.8 ábrán még észre lehet venni egy elfordított nyolcas alakzatú erőteljesebb átviteli rátát.



7.7. ábra. Az AEQ/h értéke minden földi csomópontnak a kezdeti pontból számítva. Vízszintes tengelyen a hosszanti koordináták míg a függőleges tengelyen a szelességi koordináták találhatóak. A piros X-el jelölt kezdő földi csomópontból induló útvonalak AEQ/h áteresztőképességét az adott csomópontok színezése jelöli.



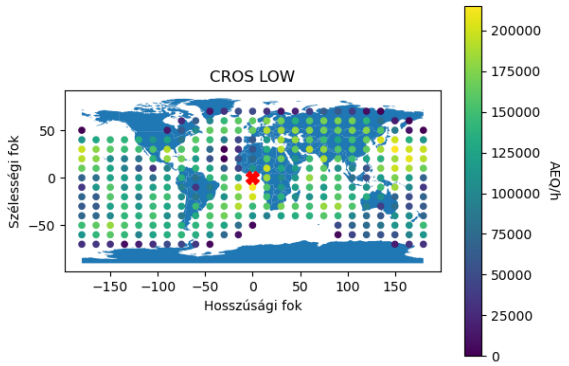
7.8. ábra. Az AEQ/h értéke minden földi csomópontnak a kezdeti pontból számítva kontúros ábrázolással. Vízszintes tengelyen a hosszanti koordináták míg a függőleges tengelyen a szelességi koordináták találhatóak. A piros X-el jelölt kezdő földi csomópontból induló útvonalak AEQ/h áteresztőképességét az adott csomópontok színezése jelöli.

7.2. CROSS architektúra

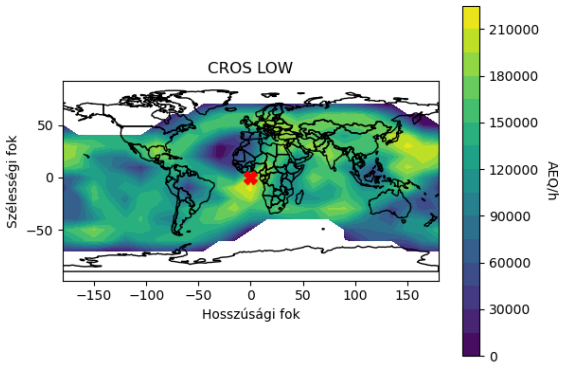
A CROSS architektúra alá tartozó konstellációk időben ritkább, de hosszabb láthatósági időintervallumokkal dolgoztak.

7.2.1. LOW konstelláció

Mint ahogy az a 7.9 és 7.10 ábrákon is észrevehető, a RETRO architektúrához tartozó társával szemben a LOW konstelláció kimenetén nem voltak megtalálhatóak ugyanannyira élesen az inklinációval megegyező irányú erősebb átviteli ráták. Viszont, mint az a 7.10 ábrán látható retrográd társánál jóval nagyobb 110000-es átlagos AEQ/h értéket tudott produkálni.



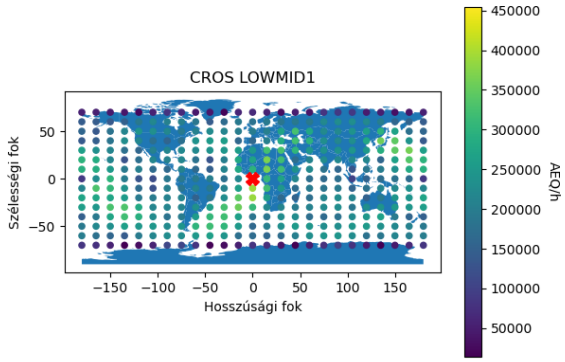
7.9. ábra. Az AEQ/h értéke minden földi csomópontnak a kezdeti pontból számítva. Vízszintes tengelyen a hosszanti koordináták míg a függőleges tengelyen a szelességi koordináták találhatóak. A piros X-el jelölt kezdő földi csomópontból induló útvonalak AEQ/h áteresztőképességét az adott csomópontok színezése jelöli.



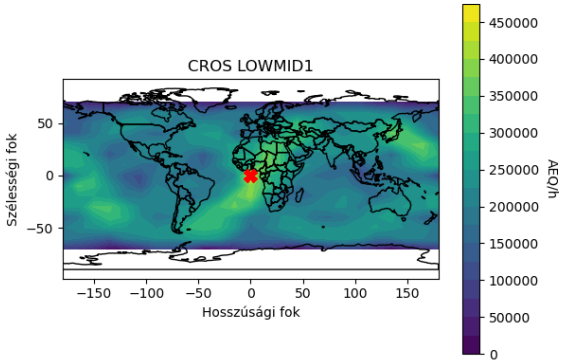
7.10. ábra. Az AEQ/h értéke minden földi csomópontnak a kezdeti pontból számítva kontúros ábrázolással. Vízszintes tengelyen a hosszanti koordináták míg a függőleges tengelyen a szelességi koordináták találhatóak. A piros X-el jelölt kezdő földi csomópontból induló útvonalak AEQ/h áteresztőképességét az adott csomópontok színezése jelöli.

7.2.2. LOWMID1 konstelláció

Mint az a 7.11 és 7.12 ábrákon látható, RETRO architektúrába tartozó társához hasonlóan a LOWMID1 konstelláció is egy teljes lefedettséget biztosít. Fontos még megemlíteni a 7.12 ábrán látható erősebb átviteli mintázatot hiszen az a 7.8 ábrán láthatóéhoz hasonlít nem a konstelláció RETRO architektúrás megfelelőére.



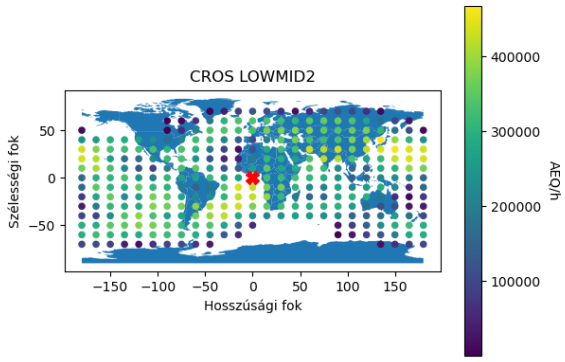
7.11. ábra. Az AEQ/h értéke minden földi csomópontnak a kezdeti pontból számítva. Vízszintes tengelyen a hosszanti koordináták míg a függőleges tengelyen a szelességi koordináták találhatóak. A piros X-el jelölt kezdő földi csomópontból induló útvonalak AEQ/h áteresztőképességét az adott csomópontok színezése jelöli.



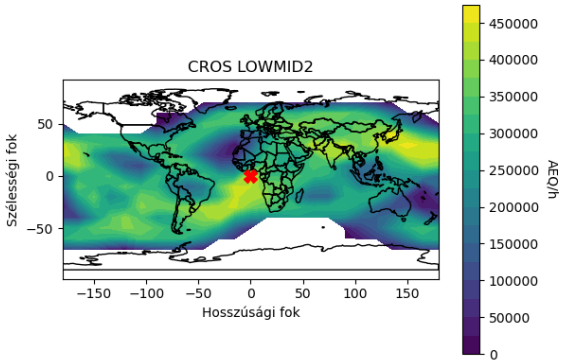
7.12. ábra. Az AEQ/h értéke minden földi csomópontnak a kezdeti pontból számítva kontúros ábrázolással. Vízszintes tengelyen a hosszanti koordináták míg a függőleges tengelyen a szelességi koordináták találhatóak. A piros X-el jelölt kezdő földi csomópontból induló útvonalak AEQ/h áteresztőképességét az adott csomópontok színezése jelöli.

7.2.3. LOWMID2 konstelláció

A 7.13 és 7.14 ábrákon található a LOWMID2 konstelláció szimulációs kimenete. A konstelláció a RETRO architektúrájú társához hasonlóan nem biztosít teljes lefedettséget viszont magasabb átlagos AEQ/h értéket produkál társánál.



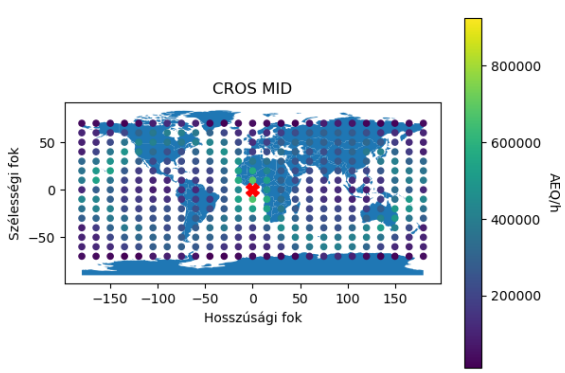
7.13. ábra. Az AEQ/h értéke minden földi csomópontnak a kezdeti pontból számítva. Vízszintes tengelyen a hosszanti koordináták míg a függőleges tengelyen a szelességi koordináták találhatóak. A piros X-el jelölt kezdő földi csomópontból induló útvonalak AEQ/h áteresztőképességét az adott csomópontok színezése jelöli.



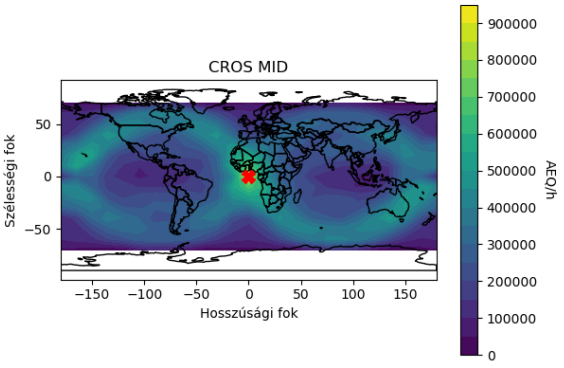
7.14. ábra. Az AEQ/h értéke minden földi csomópontnak a kezdeti pontból számítva kontúros ábrázolással. Vízszintes tengelyen a hosszanti koordináták míg a függőleges tengelyen a szelességi koordináták találhatóak. A piros X-el jelölt kezdő földi csomópontból induló útvonalak AEQ/h áteresztőképességét az adott csomópontok színezése jelöli.

7.2.4. MID konstelláció

A MID konstelláció biztosította az összes közül a legmagasabb átlagos AEQ/h értéket a teljes lefedettség mellett. A 7.15 és 7.16 ábrákon látható a már több előző pályarendszeren is megfigyelt elforgatott nyolcas alakzatú erősebb átviteli tartomány.



7.15. ábra. Az AEQ/h értéke minden földi csomópontnak a kezdeti pontból számítva. Vízszintes tengelyen a hosszanti koordináták míg a függőleges tengelyen a szelességi koordináták találhatóak. A piros X-el jelölt kezdő földi csomópontból induló útvonalak AEQ/h áteresztőképességét az adott csomópontok színezése jelöli.



7.16. ábra. Az AEQ/h értéke minden földi csomópontnak a kezdeti pontból számítva kontúros ábrázolással. Vízszintes tengelyen a hosszanti koordináták míg a függőleges tengelyen a szelességi koordináták találhatóak. A piros X-el jelölt kezdő földi csomópontból induló útvonalak AEQ/h áteresztőképességét az adott csomópontok színezése jelöli.

8. - Konklúzió

Mint az látható a 8.1 és 8.2 táblázatokon is, a műholdak számosságának növelésével az optikai áteresztés drasztikusan megnőt és mindkét architektúra esetén már 32 műhold segítségével is teljes lefedettséget lehetett elérni. A LOWMID1 konstelláció mind a RETRO és CROSS architektúrán belül az teljes lefedettséget tudott biztosítani mindössze 32 műhold segítségével. A REBSAN algoritmus segítségével a LOWMID1 konstelláción belű olyan kommunikációs hálózat tudtunk létrehozni melyen keresztül átlagosan másodpercenként 55 összefonódást tudunk megosztani a föld különböző pontjai között. Az összefonódásokat sokféleképen felhasználhatják a végfelhasználók. Kvantum teleportálás [37] segítségével küldhetnek kvantumbiteket, elosztott számításokat végezhetnek [38] vagy egyből felhasználhatják különböző kulcsszétosztó protokollokhoz [5].

Konstelláció	RETRO LOW	RETRO LOWMID1	RETRO LOWMID2	RETRO MID
Átlagos AEQ/h	82101	183151	204359	222428
Minimális AEQ/H	0	48746	0	37252
Maximális AEQ/h	173307	340536	351410	674053

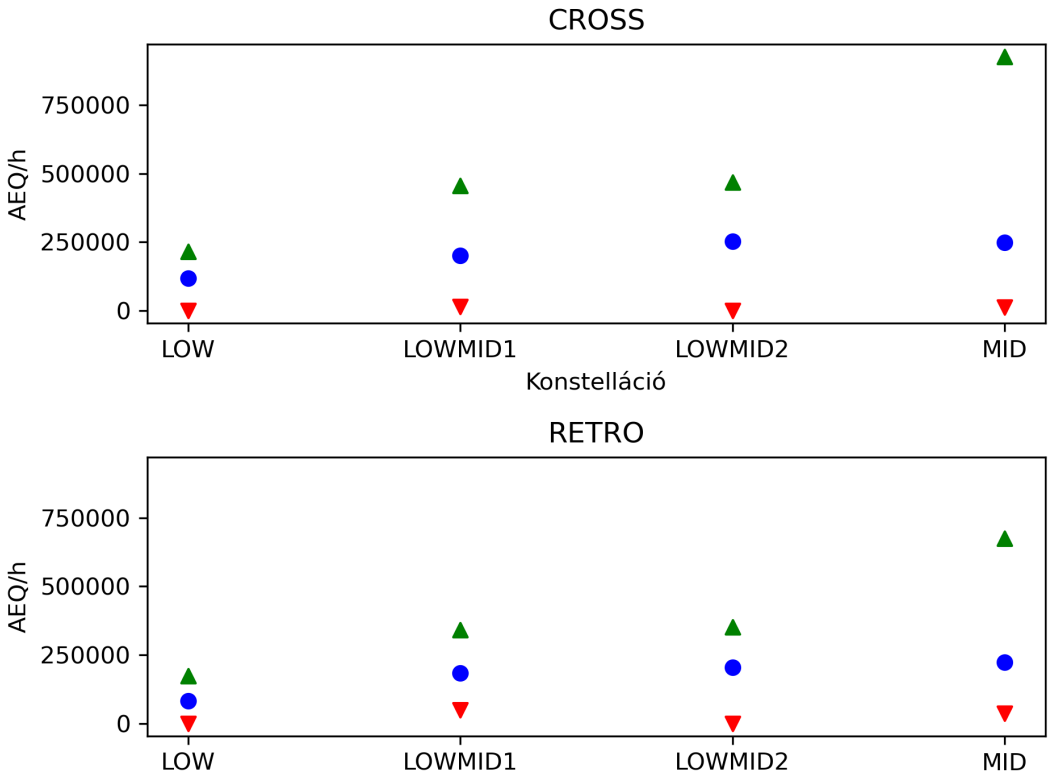
8.1. táblázat. A RETRO architektúra konstellációinak átlagos, minimális és maximális AEQ/h rátája.

Konstelláció	CROSS LOW	CROSS LOWMID1	CROSS LOWMID2	CROSS MID
Átlagos AEQ/h	116615	200842	251400	249062
Minimális AEQ/H	0	13729	0	11428
Maximális AEQ/h	215295	454791	467762	925660

8.2. táblázat. A CROSS architektúra konstellációinak átlagos, minimális és maximális AEQ/h rátája.

A két táblázaton és a 8.1 ábrán is látható, hogy a két felhasznált architektúra között kulcs különbségek vannak. A CROSS architektúra összes konstellációja nagyobb divergenciával és átlagos AEQ/h értékkel rendelkezett, mint a RETRO architektúra. A RETRO architektúra sokkal kisebb mértékben tért el az átlagtól és csak egy kevéssel volt kevesebb az kisebb AEQ/h értéke. Több konstellációnál is lehetett tapasztalni eltérő méretű és alakzatú erőteljesebb átviteli tartományokat. Ezen alakzatok egy érdekes kutatási irányt jelenthetnek, hiszen, ha irányíta-

ni tudnánk hol jelenjenek meg erősítőként tudnánk őket használni a nagyobb átvitel igénylő területeken.



8.1. ábra. A két fő konstellációs architektúrák adatai. A függőleges tengelyen az AEQ/h értékek, míg a vízszintesen az architektúrát használó konstellációk találhatóak. A piros háromszög a legkisebb, a kék kör az átlagos, míg a zöld háromszög a legnagyobb AEQ/h értéket jelöli az adott konstelláción belül.

A cikkben bemutattuk, hogy a REBSAN felhasználásával lehetséges 32 műholdas csomóponttal (szinte) teljes bolygót lefedni. Rendszerünk által másodpercenként megosztott összefonódások száma alacsonyabb, mint más, már meglévő [26] kvantumműholdas rendszerek esetén. Az alacsony átvitel betudható a felhasznált kvantumösszefonódás-generátor hatékonyságának, melynek növelésével egyenes arányosan nőne a megosztott összefonódások száma is. Az itt bemutatott rendszer képes akár klasszikus rendszerek biztonságának támogatására is, hiszen a CROSS MID hálózat használatával másodpercenként átlagosan 69 összefonódást tudunk megosztani két csomópont között. A megosztott összefonódások lehetővé tennék kvantumalgoritmusok elosztott kvantumrendszereken való fútatását [39].

Végül, de nem utolsósorban, szeretném megköszönni konzulensemnek Bacsárdi Lászlónak a sok éve tartó segítségét kvantumkommunikációs kutatásaimban.

A kutatást az Innovációs és Technológiai Minisztérium és a Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal támogatta a Kvantuminformatika Nemzeti Laboratórium keretében.

Felhasznált irodalom

[1] P.W. Shor. „Algorithms for quantum computation: discrete logarithms and factoring". *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994. nov., 124–134. old. DOI: 10.1109/SFCS.1994.365700.

[2] Anton Robert és tsai. „Resource-efficient quantum algorithm for protein folding". en. *npj Quantum Information* 7.1 (2021. febr.), 1–5. old. ISSN: 2056-6387. DOI: 10.1038/s41534-021-00368-4. URL: https://www.nature.com/articles/s41534-021-00368-4 (elérés dátuma 2022. 10. 06.).

[3] Bela Bauer és tsai. „Quantum Algorithms for Quantum Chemistry and Quantum Materials Science". *Chemical Reviews* 120.22 (2020). PMID: 33090772, 12685–12717. old. DOI: 10.1021/acs.chemrev.9b00829. eprint: https://doi.org/10.1021/acs.chemrev.9b00829. URL: https://doi.org/10.1021/acs.chemrev.9b00829.

[4] Panagiotis Kl Barkoutsos és tsai. „Quantum algorithm for alchemical optimization in material design". en. *Chemical Science* 12.12 (2021. ápr.), 4345–4352. old. ISSN: 2041-6539. DOI: 10.1039/D0SC05718E. URL: https://pubs.rsc.org/en/content/articlelanding/2021/sc/d0sc05718e (elérés dátuma 2022. 10. 06.).

[5] Artur K. Ekert. „Quantum cryptography based on Bell's theorem". *Physical Review Letters* 67.6 (1991. aug.), 661–663. old. DOI: 10.1103/PhysRevLett.67.661. URL: https://link.aps.org/doi/10.1103/PhysRevLett.67.661 (elérés dátuma 2021. 10. 21.).

[6] Xiyuan Ma és tsai. „Multi-Party Quantum Key Distribution Protocol with New Bell States Encoding Mode". en. *International Journal of Theoretical Physics* 60.4 (2021. ápr.), 1328–1338. old. ISSN: 0020-7748, 1572-9575. DOI: 10.1007/s10773-021-04758-4. URL: https://link.springer.com/10.1007/s10773-021-04758-4 (elérés dátuma 2022. 10. 08.).

[7] Ji-Zhong Wu és Lili Yan. „Quantum Key Distribution Protocol Based on GHZ Like State and Bell State". en. *Artificial Intelligence and Security*. Szerk. Xingming Sun, Jinwei Wang és Elisa Bertino. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2020, 298–306. old. ISBN: 9783030578817. DOI: 10.1007/978-3-030-57881-7_27.

[8] Matthäus Halder és tsai. „Entangling independent photons by time measurement". *Nature Physics* 3.10 (2007. aug.), 692–695. old. ISSN: 1745-2481. DOI: 10.1038/nphys700. URL: http://dx.doi.org/10.1038/nphys700.

[9] W. K. Wootters és W. H. Zurek. „A single quantum cannot be cloned”. en. *Nature* 299.5886 (1982. okt.), 802–803. old. ISSN: 0028-0836, 1476-4687. DOI: 10.1038/299802a0. URL: http://www.nature.com/articles/299802a0 (elérés dátuma 2022. 10. 08.).

[10] Sándor Imre és Laszlo Gyongyosi. *Advanced quantum communications: an engineering approach*. Undetermined. OCLC: 833855769. 2013. ISBN: 9781118337431 9781118337455 9781118337448 9781118002360 9781118337462. URL: http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=509506 (elérés dátuma 2021. 10. 25.).

[11] *Starlink*. URL: https://www.starlink.com (elérés dátuma 2022. 10. 16.).

[12] K. Cranford. „An improved analytical drag theory for the artificial satellite problem”. en. *Astrodynamics Conference*. Princeton,NJ,U.S.A.: American Institute of Aeronautics és Astronautics, 1969. aug. DOI: 10.2514/6.1969-925. URL: https://arc.aiaa.org/doi/10.2514/6.1969-925 (elérés dátuma 2021. 10. 02.).

[13] *poliastro/poliastro: poliastro 0.15.2 (astroquery edition)*. 2021. jún. DOI: 10.5281/ZENODO.5035326. URL: https://zenodo.org/record/5035326 (elérés dátuma 2021. 10. 03.).

[14] *Astrodynamics in python*. URL: https://docs.poliastro.space/en/v0.15.2/?badge=v0.15.2.

[15] *Cesium: The Platform for 3D Geospatial*. en-US. URL: https://www.cesium.com/ (elérés dátuma 2021. 10. 03.).

[16] *Quantum Satellite Communication Simulator*. URL: https://www.mcl.hu/quantum-old/simulator/ (elérés dátuma 2021. 10. 03.).

[17] Luc Maisonobe, Véronique Pommier és Pascal Parraud. „OREKIT: AN OPEN SOURCE LIBRARY FOR OPERATIONAL FLIGHT DYNAMICS APPLICATIONS”. 2010. ápr.

[18] *Orekit*. en. URL: https://forum.orekit.org/ (elérés dátuma 2021. 10. 03.).

[19] *About Orekit*. URL: http://orekit.org/ (elérés dátuma 2021. 10. 03.).

[20] Aitor Villar és tsai. „Entanglement demonstration on board a nano-satellite”. *Optica* (2020).

[21] Juan Yin és tsai. „Satellite-based entanglement distribution over 1200 kilometers”. *Science* 356 (2017), 1140–1144. old.

[22] Juan Yin és tsai. „Entanglement-based secure quantum cryptography over 1,120 kilometres”. *Nature* 582 (2020), 501–505. old.

[23] Shengkai Liao és tsai. „Satellite-Relayed Intercontinental Quantum Network.” *Physical review letters* 120 3 (2018), 30501. old.

[24] Hao Yang és tsai. „Atmospheric Optical Turbulence Profile Measurement and Model”. 2021.

[25] Yousef K. Chahine és tsai. „Beam propagation through atmospheric turbulence using an altitude-dependent structure profile with non-uniformly distributed phase screens”. *Free-Space Laser Communications XXXII* (2020).

[26] Sumeet Khatri és tsai. „Spooky action at a global distance: analysis of space-based entanglement distribution for the quantum internet”. *npj Quantum Information* 7.1 (2021. dec.). arXiv: 1912.06678, 4. old. ISSN: 2056-6387. DOI: 10.1038/s41534-020-00327-5. URL: http://arxiv.org/abs/1912.06678 (elérés dátuma 2021. 10. 04.).

[27] Donghai Huang és tsai. „Quantum Key Distribution Over Double-Layer Quantum Satellite Networks”. *IEEE Access* 8 (2020), 16087–16098. old.

[28] Laurent de Forges de Parny és tsai. „Satellite-based Quantum Information Networks: Use cases, Architecture, and Roadmap”. 2022.

[29] Yishu Wang és tsai. „Time-Dependent Graphs: Definitions, Applications, and Algorithms”. *Data Science and Engineering* 4 (2019), 352–366. old.

[30] Sergey Voronov és tsai. „AI Meets Real-Time: Addressing Real-World Complexities in Graph Response-Time Analysis”. *2021 IEEE Real-Time Systems Symposium (RTSS)* (2021), 82–96. old.

[31] Krishnendu Chatterjee és tsai. „Automated competitive analysis of real-time scheduling with graph games”. *Real-Time Systems* 54 (2017), 166–207. old.

[32] T. Zhang és tsai. „Application of Time-Varying Graph Theory over the Space Information Networks”. *IEEE Network* 34 (2020), 179–185. old.

[33] Dirk Giggenbach és Amita Shrestha. „Atmospheric absorption and scattering impact on optical satellite-ground links”. *International Journal of Satellite Communications and Networking* 40 (2022), 157–176. old.

[34] Harold W. Kuhn. „The Hungarian method for the assignment problem”. *Naval Research Logistics (NRL)* 52 (2010).

[35] Zichang Zhang és tsai. „High-performance quantum entanglement generation via cascaded second-order nonlinear processes”. en. *npj Quantum Information* 7.1 (2021. dec.), 123. old. ISSN: 2056-6387. DOI: 10.1038/s41534-021-00462-7. URL: https://www.nature.com/articles/s41534-021-00462-7 (elérés dátuma 2021. 10. 14.).

[36] Pengfei Wang és tsai. „Single ion qubit with estimated coherence time exceeding one hour”. *Nature Communications* 12 (2021).

[37] Dirk Bouwmeester és tsai. „Experimental quantum teleportation”. *Nature* 390 (1997), 575–579. old.

[38] Jehn-Ruey Jiang. „Quantum Entanglement with Self-stabilizing Token Ring for Fault-tolerant Distributed Quantum Computing System”. *ArXiv* abs/2209.11361 (2022).

[39] Daniele Cuomo, Marcello Caleffi és Angela Sara Cacciapuoti. „Towards a Distributed Quantum Computing Ecosystem”. *ArXiv* abs/2002.11808 (2020).