



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

# Útvonaltervezés összefonódás alapú műholdas kvantumkommunikációs hálózatokban

**TDK dolgozat**

Készítette:

Mihály András

Konzulens:

Dr. Bacsárdi László

Budapest, 2021

# Tartalomjegyzék

<b>Kivonat</b>	<b>i</b>
<b>Abstract</b>	<b>ii</b>
<b>1. Bevezetés</b>	<b>1</b>
<b>2. Kvantum hálózati alapok</b>	<b>3</b>
2.1. Kvantumbit . . . . .	3
2.2. Kvantumkapuk . . . . .	4
2.3. Kvantumösszefonódás . . . . .	4
2.4. Kvantumösszefonódás-csere . . . . .	5
2.5. Kvantumismétlő . . . . .	5
<b>3. Műholdpálya-propagátorok</b>	<b>7</b>
3.1. Poliastro . . . . .	8
3.2. Orekit . . . . .	8
<b>4. Optikai áteresztőképesség alapú útvonaltervező</b>	<b>10</b>
4.1. Időbélyegzett intervallumgráf . . . . .	10
4.2. Az algoritmus felépítése . . . . .	11
4.3. Az algoritmus működése . . . . .	13
<b>5. Az elkészült szimulátor</b>	<b>15</b>
5.1. Műholdas kvantumsimétlő felépítése . . . . .	15
5.2. Szimulátor felépítése . . . . .	16
5.3. Felhasznált műhold rendszerek . . . . .	18
5.4. Bemeneti adatok . . . . .	19
<b>6. Eredmények</b>	<b>20</b>
6.1. Retrográd műholdkonstelláció . . . . .	20
6.1.1. Kicsi műholdas-pályarendszer . . . . .	20
6.1.2. Közepes I. műholdas-pályarendszer . . . . .	22
6.1.3. Közepes II. műholdas-pályarendszer . . . . .	23

6.1.4.	Nagy műholdas-pályarendszer . . . . .	25
6.2.	Keresztpályás műholdas rendszer . . . . .	26
6.2.1.	Kicsi műholdas-pályarendszer . . . . .	26
6.2.2.	Közepes I. műholdas-pályarendszer . . . . .	29
6.2.3.	Közepes II. műholdas-pályarendszer . . . . .	30
6.2.4.	Nagy műholdas-pályarendszer . . . . .	32
<b>7.</b>	<b>Összefoglalás</b>	<b>34</b>
	<b>Felhasznált irodalom</b>	<b>36</b>

# Összefoglaló

A jelenkori kommunikációs világ egy lehetséges jövőbeli mozgatója a kvantumkriptográfia. Eddig az interneten való biztonságos kommunikációnak az egyik alappillére alkotta az a feltételezés, hogy a prímek faktorizációja egy nagyon nehéz és lassú folyamat. Ezt a műveletet – egy nagy ( $\sim 10^{30}$ ) szám esetén – a mai klasszikus számítógépekkel több ezer évbe kerülne végrehajtani, ez adja az RSA – és még sok más publikus kulcsú – titkosítás alapját. Peter W. Shor kvantumalgoritmusának köszönhetően viszont ezt a műveletet végre lehet hajtani az eredeti idő töredéke alatt. Éppen ezért már csak a kvantumhardverek fejlődésétől függ, hogy a ma használt publikus kulcsú titkosítások mikor lesznek feltörhetőek.

A kvantumtechnológia fejlődése nemcsak a kommunikációs világban fog nagy változásokat hozni, hanem sok ehhez egyáltalán nem köthető területen is, mint például az orvostudomány (fehérje hajtogatás) vagy az anyagtudomány (anyagok molekuláris tulajdonságának számolása). Emellett a kvantumtechnológia felhasználható biztonságos kommunikáció lebonyolításához is, erre már most több kulcsszétosztó protokoll is létezik, melyek a részecskék kvantumtulajdonságait használják ki. Ezek közül a legismertebbek a Charles Bennett és Gilles Brassard által létrehozott BB84 protokoll, mely a fotonok polarizációján alapul és az Artur Ekert alkotta E91 protokoll, mely kvantum-összefonódás segítségével hoz létre kulcsot a kommunikációt végző felek között.

Kvantumbitekét – a kvantuminformatika legkisebb információs építőelemeit – a legtöbb esetben fotonokon keresztül osztunk meg távoli pontokkal. Kvantumkommunikációt két fő közegen folytathatunk: optikai szálon vagy szabad optikai csatornán keresztül. Az optikai szál előnye, hogy a kommunikáció egy menedzselt környezetben keresztül történik, az az a külső zavarok nagy részétől megszabadulhatunk különböző óvintézkedések bevezetésével. Nagy hátrányai viszont, hogy költséges kiépíteni, fenntartani és alacsony lefedettséget biztosít. A szabadtéri kvantumkommunikációval ezzel szemben nagyobb lefedettséget tudunk elérni, viszont a csatornának sokkal nagyobb az entrópiája.

Munkám során egy lehetséges műhold alapú kvantumhálózat tulajdonságait vizsgáltam, az Orekit műholdpálya szimulátor segítségével. Létrehoztam egy saját, optikai áteresztőképességen alapuló útvonaltervező algoritmust. Ennek segítségével vizsgáltam összefonódás alapú kvantumhálózatokat változó sűrűségű műholdas rendszerek mentén. Tevékenységem fő motivációja egy Európát lefedő, kis méretű összefonódásos kvantumhálózat szimulációjának vizsgálata volt.

# Abstract

So far, one of the cornerstones of secure communication over the Internet has been the assumption that the process of prime factorization is a slow and tedious process. This operation - in the case of a large number ( $\sim 10^{30}$ ) - would take thousands of years with today's most advanced classic computers, this provides the basis for the RSA - and many other public key-based - encryption. Thanks to Peter W. Shor's quantum algorithm, however, this operation can be performed in a fraction of the original time. Because of this, the moment when public key-based encryption can be cracked only depends on the advancements of quantum hardware.

The development of quantum technology will bring about major changes, not only in the field of communication, but in many areas not related to it at all, such as medicine (protein folding) or material science (calculating the molecular properties of materials). In addition, quantum technology can be used to conduct secure communication, for which there are already several key distribution protocols that use the quantum properties of particles. The most well-known of these are the BB84 protocol created by Charles Bennett and Gilles Brassard, which is based on the effects of photon polarization, and the E91 protocol, made by Artur Ekert, which uses quantum entanglement to create keys between the communicating parties.

Quantum bits – the basic building blocks in quantum computing – are mostly transmitted to distant points through photons. Quantum communication can be carried out on two main media: fiber or free space. The advantage of fiber is that communication takes place through a managed environment and by controlling the said environment, we can dampen the effects of external disturbances over the channel. Its drawbacks are however that it is costly to build and upkeep and provides only point-point coverage. Free-space quantum communication on the other hand can achieve more coverage, with the cost of greater channel entropy.

During my work I examined the properties of a possible satellite-based quantum network using the Orekit satellite orbit simulator. I developed an optical transmittance-based route planning algorithm. With this, I examined entanglement-based quantum networks along a variety of satellite systems. The main motivation of my work was to investigate the simulation of a small, interconnected quantum network covering Europe.

# 1. fejezet - Bevezetés

Az RSA alapú publikus kulcsú kriptográfia minden napjaink részét képezi. Használják bankok, weboldalak és minden olyan entitás mely szeretne biztonságos kommunikációt folytatni az interneten. Azonban a kvantuminformatika fejlődésével és Shor [1] algoritmusának köszönhetően az idő amikor a legtöbb ma használt publikus kulcs alapú titkosítás feltörhető lesz már egyre kevésbé egy tudományos fantasztikum. A kvantuminformatika segítségével nemcsak a ma legtöbbet használt titkosítási algoritmusokat törhetjük fel, hanem több eddig óriási számítási kapacitást igénylő problémát is felgyorsíthatunk. Groover [2] algoritmusának segítségével rendezetlen tömbökben kereshetünk elemeket  $\sqrt{N}$  lépésből. Egy másik algoritmussal szintén rendezetlen tömbökben kereshetünk szélsőséges értékeket [3]. Mint láthatjuk a kvantuminformatika többszörösen felgyorsíthatja mai világunkat, ezért is fontos a kvantumszámítógépeket összekapcsoló hálózatok vizsgálata.

Kvantuminformatikával lassan már két éve foglalkozom behatóbban. Munkásságom során többféle hálózattal is dolgoztam, ezek közül kiemelten a szabadtéri kvantumrendszerekkel. A szabadtéri kvantumhálózatok egyik legfontosabb alfaja a műhold alapú, hiszen így óriási területeket fedhetünk le minimális földi, kötött infrastruktúra kiépítésével. Emellett a műhold-műhold kommunikáció esetén a legkör – vagy bármely más sűrű közeg – zavaró hatásait is elkerülhetjük.

Amikor kvantuminternetéről beszélünk, kétféle dolog járhat az eszünkben: egy kvantumkulcs-szétosztó rendszer, mely a mostani internettel tandemben működne, hogy segítse a biztonságos kommunikációt vagy egy tényleges kvantumhálózat mely segítségével a világ távoli pontjain lévő kvantumszámítógépek képesek kvantuminformációt megosztani egymással. Ez utóbbival képesek lehetünk elosztottan működtetni olyan nagy méretű kvantumrendszereket melyeket lehetetlen lenne a mostani technológiával létrehozni.

Fő céloom a műholdas rendszerek vizsgálatával az volt, hogy egy alternatív, kevesebb műholdból álló rendszert tudjak felmutatni. A mostani műholdas kvantumhálózati tervek fő elve, hogy egy folytonos csatorna szükséges a kvantuminformáció küldésére, ennek hatására akár több száz műhold is szükséges lehet. Munkám során egy olyan algoritmust hoztam létre, mely segítségével úgy tudok útvonalat tervezni a rendszerben, hogy közben a kvantumbitek akár hosszabb ideig is „egy helyben vannak”. Ezzel a módszerrel képes voltam olyan működő rendszert létrehozni, amely csak 16 műholdból állt.

A második fejezetben egy rövid áttekintést adok a szimulált kvantumhálózat értelmezéséhez szükséges kvantummechanikai alapokról, leginkább olyan részleteire fókuszálva melyek kritikusak az általam szimulált rendszerben. A Harmadik fejezetben a különféle műhold pálya szimulátorokat mutatok be. Ezután, a negyedik fejezetben elmagyarázom és bemutatom saját algoritmusom működését, majd az ötödik fejezetben magát a szimulátort és felépítését mutatom be. Végül, a 6. fejezetben a kapott eredményeim ismertetem.

## 2. fejezet - Kvantum hálózatoki alapok

A kvantumszámítógépek fejlődésével egyre fontosabb az olyan kvantumhálózatok létrehozása, melyek segítségével azok összeköthetők. Mint már a bevezetőben is említettem, kvantuminternet alatt két, teljesen más alapú rendszerre is lehet gondolni. Ebben dolgozatban a kvantuminternetre mint egy kvantumszámítógépeket összekötő kvantumbiteket szállító hálózatra gondolunk. Egy ilyen rendszer működésének megértéséhez szükségünk lesz a kvantummechanika egy egyszerűsített változatára. A kvantummechanika a mikroszkopikus rendszerek működését és a látható világgal való kapcsolatát írja le, aminek az alapja a 4 posztulátum:

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  $P(x|\phi) = \langle\phi|M_X^T M_X|\phi\rangle$  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 öt felépítő  $V$  és  $Y$  rendszerek állapotából az az:  $w = x \otimes y$  ahol  $w \in W$  és  $y \in Y$ .

A posztulátumok megértése nem csak azért szükséges mert a kvantumfizika alapjait képzik, hanem mert a kvantumszámítógépek elemei is megfeleltethetőek nekik. Ezek a következők:

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

### 2.1. Kvantumbit

A kvantumbit a bit kvantuminformaticai megfelelője, mely ábrázolható egy kétdimenziós  $\nu \in H$  vektorral, ennek következtében egy  $|\phi\rangle$  kvantumbit felírható a következő képen:  $|\phi\rangle = \alpha \binom{1}{0} + \beta \binom{0}{1}$ , ahol  $\alpha, \beta \in \mathbb{C}$  valószínűségi változók és  $|\alpha|^2 + |\beta|^2 = 1$  a valószínűségi eloszlás. Bár



ez az ábrázolás egyszerűbb, látványosabb és elégséges az egyszerűbb rendszerek ábrázolásához, ahogy a rendszer dimenziószáma emelkedik, úgy kevésbé lesz követhető ez a jelölés. Emiatt a bra-ket felírást fogom a dolgozatban ezentúl használni amely a következő:  $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$  és  $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ . Az eredeti egyenletünk pedig az új alakban  $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$  lesz. Fontos itt még megemlítenem, hogy az itt tárgyalt valószínűségi változók eredménye úgynevezett igazi véletlen, más néven a rendszer állapotának teljes ismerete mellett sem lehet biztosra megjósolni a kimenetelét.

## 2.2. Kvantumkapuk

A kvantumkapuk unitér operátorok melyek segítségével kvantumbiteken hajtunk végre változtatásokat. Többféle kvantumkaput ismerünk melyek egy vagy több kvantumbiten hajtanak végre műveleteket. Míg a kvantumbiteket vektorokkal, a kvantumkapukat mátrixokkal ábrázoljuk, így a kvantumkapuk hatásait mátrix műveletként jellemezhetjük. Kvantumkapuk esetén fontos kitétel, hogy kötelezően unitér transzformáció kell legyen, azaz minden  $N$  kvantumkapura igaz, hogy  $NN = I$  ahol  $I$  egy  $N$ -el megegyező dimenziójú identitás mátrix.

## 2.3. Kvantumösszefonódás

A kvantumhálózatok egy fontos összetevője a kvantumösszefonódás. Összefonódott állapotnak hívjuk azt a rendszert, melyet nem lehet felírni a két rendszer állapotainak tenzorszorzataként. Összefonódott kvantumrendszerek esetén az egyik tag méréséből kikövetkeztethető a másik tag mérési eredménye. Többféle összefonódási állapot is létezik, ezek közül a Bell-állapotokat (EPR-párok) használjuk, mivel ezek egymásra ortogonálisok és így könnyen megkülönböztethetőek. Ezek sorrendben:

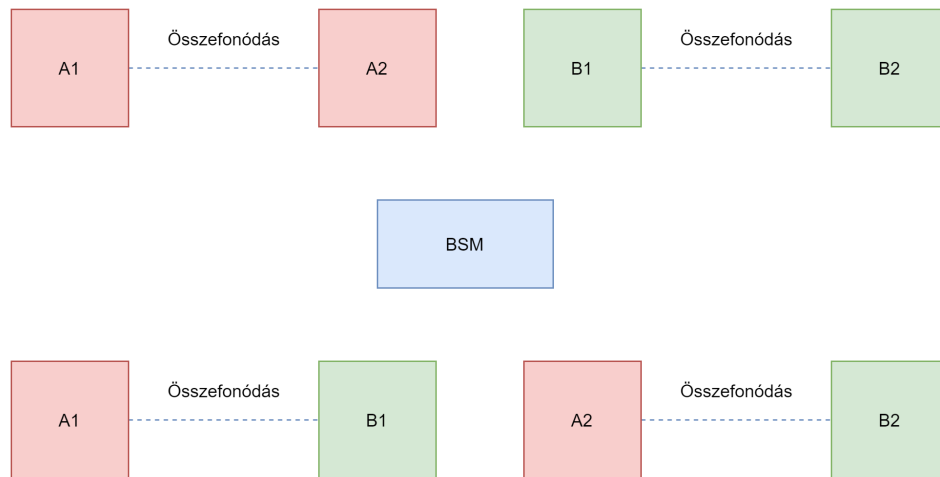
$$\begin{aligned} \beta_{00} &= \frac{|00\rangle + |11\rangle}{\sqrt{2}} & \beta_{01} &= \frac{|01\rangle + |10\rangle}{\sqrt{2}} \\ \beta_{10} &= \frac{|00\rangle - |11\rangle}{\sqrt{2}} & \beta_{11} &= \frac{|01\rangle - |10\rangle}{\sqrt{2}} \end{aligned}$$

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

Amikor kvantum összefonódásról beszélünk, általában a fentebb említett párok egyikét használjuk. Ez a fajta összefonódás a kvantumhálózatok és több kvantumkulcsszétosztó rendszer alapja.

## 2.4. Kvantumösszefonódás-csere

A kvantumösszefonódás-csere egy fontos lépés volt a kvantumkommunikáció fejlődésében. Először a Genfi egyetemen [4] hajtották végre ezt a műveletet két, egymástól független összefonódott fotonpáron. Mint az az 2.2. ábrán is látható az összefonódás megcserélődött a Bell állapot mérés (BSM - Bell State Measurement) után.



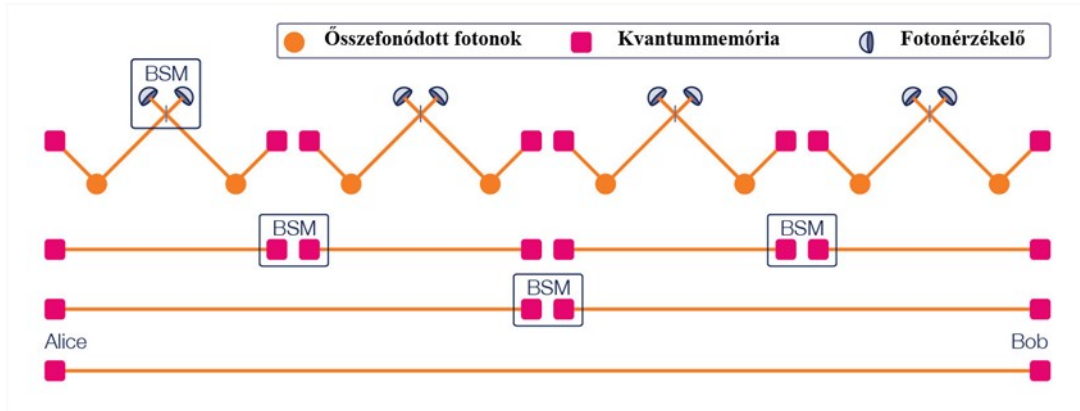
**2.2. ábra.** Kvantumösszefonódás-csere BSM által. Az ábra tetején a két összefonódott foton pár található, míg az ábra alján a megcserélt összefonogassuak.

A BSM hatására a maradék két foton (A2 és B2), melyek eddig nem voltak egyszer sem kapcsolatban - mint a 2.2 ábrán is láthatjuk - összefonódtak egymással. Ezt a műveletet több helyen is használják, mint például a kvantumismétlők vagy Artur Ekert alkotta E91 [5] protokoll során.

## 2.5. Kvantumismétlő

Kvantumismétlőkre, mint hálózati elem két okból van szükségünk. Üvegszál hálózatok esetén 150 km-es távolságok fölött a csillapítás túl nagy mértékű lesz és szükséges egy erősítő (fontos megjegyezni, hogy a kvantumismétlő nem valódi erősítést hajt végre). Erre viszont nincs lehetőség kvantumbitek klónozhatatlansága miatt. A második eset pedig egy szabadtéri kvantumcsatorna esetén áll fent, amikor is szükségünk van erősítésre vagy akár irányításra is (például műhold rendszerek esetén irányváltáskor).

Az egyetlen probléma a kvantumbitek már fentebb említett klónozhatatlansága. Erre a megoldás az 2.3. ábrán is látható rendszer, mely annyiban hasonlít a klasszikus rendszerre, hogy több kis szakaszra osztjuk a távolságot. Kvantumismétlő esetén erősítők helyett kvantummemóriával felszerelt csomópontokat használunk, melyek kvantumösszefonódás-csere segítségével küldik át az összefonódást. [6]



**2.3. ábra.** Alice és Bob kapcsolata több ismétlőn keresztül. Az ábrán látható a szintén kvantumösszefonódás menete.

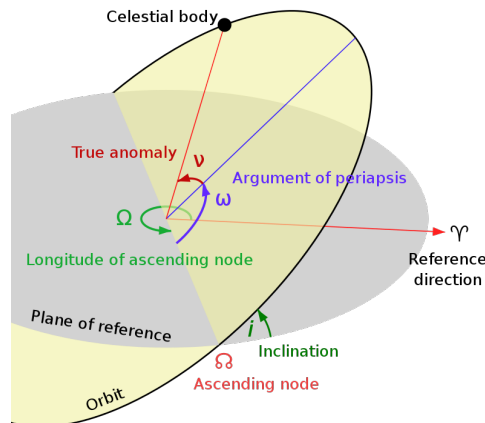
### 3. fejezet - Műholdpálya-propagátorok

Műholdak pályáinak megadására és későbbi helyzetének kiszámítására több különböző bonyolultságú rendszer és azokat feldolgozni képes alkalmazás készült már el. Ezeket az alkalmazásokat hívjuk műholdpálya-propagátoroknak. Pályapropagátorok segítségével tudjuk egy kezdeti értékrendszerből kiszámítani a műhold későbbi helyzetét. Több ilyen rendszer is létezik, közülük a leghíresebb a TLE és Kepleri. A TLE-t – two-line element set – Max Lane 1860-as űrbéli ellenállással kapcsolatos kutatásának [7] továbbfejlesztésével hozta létre a NORAD, megalakulása időszakából következően lyukkártyákra lett tervezve, ez látható is az 3.1 ábrán is. A TLE-t a mai napig is használják űrtörmelékek ütközési pályáinak számításához.

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 programja, a képen zölddel van jelölve az azonosításra használt elemek, pirossal pedig a pályaelemeket tartalmazók.

A Kepleri pályaleíró a TLE-nél egy egyszerűbb rendszert feltételez – és ennek következtében pontatlanabb is hosszútávon. A hosszútávú pontatlansága nem volt kritikus számomra hisz szimulációim időtartamai legfeljebb 3 napot tesznek ki. Mint az a 3.2 ábrán is látható maga a rendszer sokkal kevesebb változóval rendelkezik mint a TLE. Ezen változók a következők:



3.2. ábra. Kepleri pálya rendszer vizuális bemutatása, a változókhöz tartozó részletes magyarázatok a 3.1. táblázatban találhatóak.

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

**Inclination (i)** - pálya egyenlítővel bezárt szöge

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

**Longitude of the ascending node ( $\Omega$ )** - pálya referencia ponttal bezárt szöge

**Argument of periapsis ( $\omega$ )** - a pálya legmagasabb pontja és a referencia pont által bezárt szög

**True anomaly ( $\nu$ )** - a test hol helyezkedik el a pályán annak legmagasabb pontjához képest.

**3.1. táblázat.** A Kelperi pályarendszer elemeinek részletes leírása

### 3.1. Poliastro

A Poliastro [8] egy python alapú pálya propagátor és vizualizáló. 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 [9]. A teljesség igénye nélkül néhány a funkciói közül: atmoszféra adatainak modellezése vizualizációja; pálya vizualizáció Celsium [10] segítségével; műholdak földi nyomvonalainak bemutatása; sertésszelet ábrázolás; manőverek és azok pályára való hatásainak vizualizálása

Mint látható, a Poliastro egy részletes és funkciógazdag szimulátor, ami mellett támogat több vizualizációs technikát is. Az, hogy nem erre esett választásom két oka volt. Az első, hogy amikor először rátaláltam dokumentációjára, funkciói is hiányosak voltak ezért nem volt alkalmas számomra. A második pedig, hogy az optikai áteresztés számolásához használt QSCS [11] kódja Java-ban íródott, ami megnehezítette volna a közös működést is a Poliastroval.

### 3.2. Orekit

Az Orekit egy alacsony szintű úrdinamikai szimulációs könyvtár, mely 2008 óta open-source [12]. A könyvtárat a világ minden táján használják: a Svéd Űrtársaságtól (SSC) kezdve egészen az Amerikai haditengerészeti kutatólaboratóriumig (NRL). A könyvtár funkcionálisai a Poliastrohoz képest sokkal alacsonyabb szintűek. Ezek, a teljesség igénye nélkül, a következők: 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 nemcsak egy kész verzió volt (általam használt verzió: 10.3) hanem sok és változatos

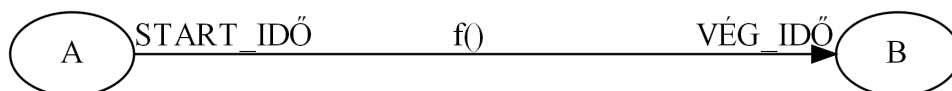
helyen használják, ezért a kijelölt fórumán [13] és weboldalán [14] könnyedén lehetett segítséget kapni.

# 4. fejezet - Optikai áteresztőképesség alapú útvonaltervező

A kutatásom kezdeti stádiumában szembesültem a ténnyel, hogy habár a kvantumkommunikáció esetén nem szükséges az alacsony késleltetés és folyamatos kapcsolat, a mai műholdas kvantumhálózatok tervezetei mégis ezen elvek alapján készítik műholdrendszerüket [15]. Ha Alice (feladó) küldeni akar összefonódott-kvantumbiteket Bob-nak (vevő), azt alapesetben egy folytonos csatornán tenné. Másnéven, minimalizálva lenne a kvantumbitek csomópontokon eltöltött ideje. Ehhez akár többszáz műholdra is szükség lehet, mint azt már megállapították a Louisianai Állami Egyetem kutatói [15]. Az algoritmusom alapötlete a következő: folytonos csatorna helyett Alice először küld  $n$  darab bitet egy műholdnak, mely ahelyett, hogy egyből tovább küldené, eltárolja azt a kvantummemóriájában. Ezekután, a műhold egy optimális időpontban továbbítja a következő csomópont felé a kvantumbiteket. Ezt az tárolás-és-továbbítást addig folytatják, ameddig meg nem érkeznek a kvantumbitek a cél csomóponthoz. Ezt a módszert többek között store and forward-nak is nevezik. Azt, hogy milyen sorrendbe mikor és melyik csomópontoknak kell küldeni, az összefonódott kvantumbiteket az algoritmusom segítségével meghatározható.

## 4.1. Időbélyegzett intervallumgráf

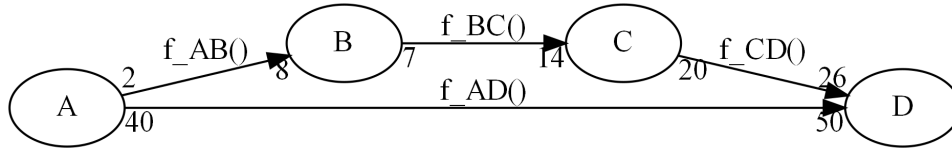
Az algoritmusom futtatásához az első logikai alkotó elem, amit szükséges ismerni, az időbélyegzett intervallumgráf (IIG).  $SAT1, SAT2 \in V$  csomópont között van él, ha igaz, hogy látni fogják egymást. Ekkor az él a 4.1. ábra mintájára fog alakulni:  $E(\text{START\_IDŐ}, \text{VÉG\_IDŐ}, f())$  ahol  $\text{START\_IDŐ}$  a láthatóságnak kezdetének,  $\text{VÉG\_IDŐ}$  a láthatóság végének ideje és  $f()$  az adott élrész súlyfüggvénye.



**4.1. ábra.** IIG él példa, a  $\text{START\_IDŐ}$  az intervallum kezdeti pontját jelöli, a  $\text{VÉG\_IDŐ}$  pedig annak végét. Az  $f()$ -el jelölt függvény egy adott élrész súlya.

Az  $f()$  súlyfüggvény futtatható egy vagy két bemenettel is, visszatérési értéként pedig megadja az élrész súlyát. A különbség aközött, hogy egy vagy két értékkel hívjuk meg az hogy

míg  $a, b \in [\text{START\_IDŐ}, \text{VÉG\_IDŐ}]$   $f(a, b)$  esetén az  $[a, b]$  intervallumon adja meg  $f()$  az élrész súlyát, addig  $f(a)$  esetén az  $[a, a+\delta]$  intervallum adataival tér vissza. Egy komplett gráf a 4.2. ábrán látható, melyről könnyedén leolvasható az intervallumok mérete és kezdete.



**4.2. ábra.** Példa IIG, az élek kezdetén van jelölve az intervallum kezdete, míg az élek végén a vége,  $F_{XY}$  pedig az  $XY$  él függvényét jelöli.

## 4.2. Az algoritmus felépítése

Az algoritmus 5 fő függvényre osztható melyek pseudokódja lent megtalálható. A függvények sorrendben:

- LEGJOBBÚT: a fő függvény, megívásával kapjuk meg a két választott város közötti útvonalat.
- HOZZÁAD: a már meglévő útvonalhoz hozzá add egy új élt
- MEGVÁG: két kapott élet összevág, hogy ne fedjék egymást
- VÁGÁSAZABLAKMÉRETHEZ: egy kapott útvonalat az előre beállított  $\text{MIN\_ABLAK}$  értékhez igazít, ha lehetséges
- OPTIKAIÁTERESZTÉSMAX: kiszámolja egy útvonal optikai áteresztés maximumát. A legnagyobb áteresztést adja vissza melyet a teljes útvonal elbír

A Következőkben a fent említett függvények működését fogom bemutatni, az előző a felsorolás szerinti sorrendben.



## LEGJOBBÚT (IGG, Város1, Város2):

Értékek:

MAX\_IDŐ - egy adott útvonal maximális hossza

MIN\_ABLAK - minimális élhossz

Bemenet: IGG melyet műhold pálya adatok alapján inicializáltunk és a két város melyek között szeretnénk megkapni a legjobb útvonalat

Kimenet: A legnagyobb optikai áteresztéssel rendelkező útvonalak

Kreálunk egy listát az útvonalaknak

index=0

legjobb = null

Ciklus:

Belevesszük az útvonalak közé Város1-ből induló  $e = \text{Város.Élek}[\text{index}]$ -t

Egy ciklusban végig megyünk az  $e$  végpontjának összes élén, és meghívjuk rájuk az  $e.HOZZÁADD()$  függvényt

Ha az így keletkező útvonal létrejött és hossza nagyobb, mint MAX\_IDŐ, akkor azt az útvonal VÁGÁ SAZABLAKMÉRETHÉZ függvényével próbáljuk kiküszöbölni. Amennyiben ez nem sikerül a következő éllel folytatjuk az előző lépéstől.

Ha az így keletkezett útvonal utolsó éle a Város2-ben ér véget megnézzük, hogy az új útvonal vagy a legjobb-nak a magasabb az OPTIKAIÁTERESZTÉSMAX értéke, a nagyobbal tesszük egyenlővé a legjobb-at.

Ha a létrejött útvonal egyik esetben sem tartozik bele, akkor azt bele vesszük az Új útvonalak közé (mindig csak a legfrissebb iterációból származókat tartjuk meg).

Újra futtattjuk az algoritmust az új útvonal listával egészen addig míg el nem fogynak az útvonalak (nem tudunk újat hozzá adni) .

Ha nem tudunk újat hozzáadni növeljük az index változó értékét egyel és újakezdjük a műveletet.

Visszatérünk a legjobb útvonallal minden Város.Élek élhez.

## HOZZÁADD():

Bemenet: Egy él

Kimenet: új útvonal a hozzáadott éllel együtt.

Mostani időben utolsó él: V1

Új él: V2

Ellenőrizzük, hogy V1 kezdete után kezdődik e V2 és V2 nem vezet egy olyan csomópontba, ahol már jártunk.

Kiszámoljuk, hogy mekkora az új él és a mostani legutolsó él között mekkora az átfedés. Ha nincs akkor az új élet hozzáadjuk az útvonalhoz, és visszatérünk vele.

Ha van átfedés akkor meghívjuk a MEGVÁG (Átfedés, V1, V2) függvényt majd, ha az sikeresen lefut hozzáadjuk az általa létrehozott éleket, és úgy térünk vissza. Ha sikertelen volt üres (null) értékkel térünk vissza.

## MEGVÁG (Átfedés mértéke, V1, V2)

Bemenet: Átfedés mértéke, Utolsó él az útvonalból, Az új él  
Kimenet: Két új megvágott él melyek nem fedik egymást  
Kiszámítjuk melyik élnek a magasabb az optikai áteresztése, a kisebből levágunk egy egységnyi elemet, egyenlőség esetén a kisebb értékű szeletet vágjuk ki. Csökkentjük az átfedés mértéke értékét.  
A lépést addig ismételjük míg az átfedés mértékének értéke nem lesz  $\leq 0$ .  
Ha közben bármelyik él mérete lecsökken MIN\_ABLAK alá akkor a futás sikertelen volt.

## VÁGÁSAZABLAKMÉRETHEZ ()

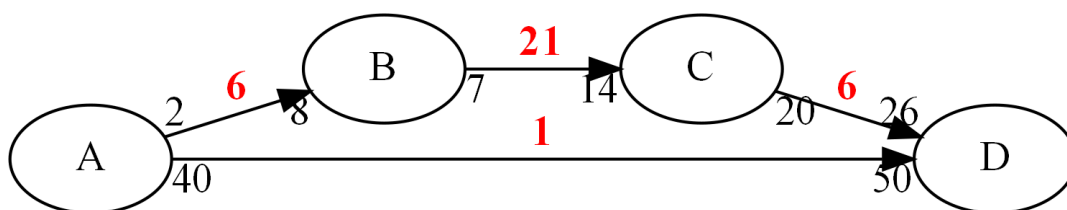
Bemenet: Útvonal  
Kimenet: Útvonal mely összesített hossza kisebb, mint MAX\_IDŐ  
Az útvonal elejéből és végéből a MEGVÁG algoritmusban is használt módszer segítségével addig nyesünk darabokat míg nem értük el a megfelelő méretet.  
Ha közben bármelyik él mérete lecsökken MIN\_ABLAK alá akkor a futás sikertelen volt.

## OPTIKAIÁTERESZTÉSMAX ()

Bemenet: Útvonal  
Kimenet: Útvonal maximális optikai áteresztése  
Végig megyünk az útvonalat tartalmazó összes élen és kiszámoljuk az optikai áteresztésüket és a legkisebbel térünk vissza. // Nem lehet több az áteresztés mint a legalacsonyabb csatornáé.

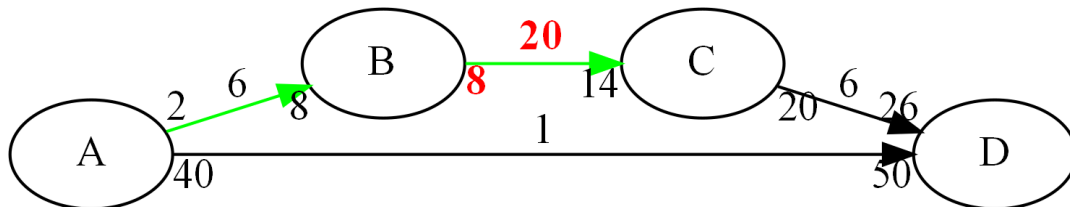
## 4.3. Az algoritmus működése

Az algoritmusom könnyebb és átfogóbb megértése érdekében működését bemutatom a 4.2. ábrán látható gráfon is. Az első lépés előtt fontos még definiálni az intervallum élek súlyfüggvényeit, legyen:  $f_{AB}(x) = 1$ ;  $f_{BC}(x) = 3$ ;  $f_{CD}(x) = 1$ ;  $f_{AD}(x) = 0.1$ . Ezekután behelyettesítjük a START\_IDŐ és VÉG\_IDŐ paramétereket a súlyfüggvényekbe. Az eredményt a 4.3. ábrán láthatjuk. Legyen a célunk az, hogy A-ból D-be jussunk, emellett globális (egész algoritmusra kiterjedő) változóink legyenek: MIN\_ABLAK := 2, MAX\_IDŐ := 20.



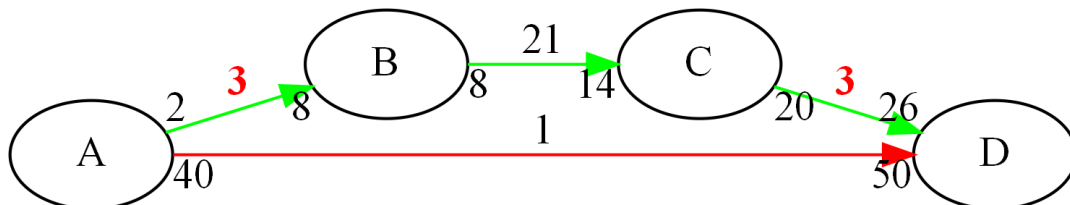
4.3. ábra. Példa IGG gráf, pirossal jelölve a kiszámított súlyfüggvények láthatóak.

Első lépésként vesszük az AB élet és behelyezzük az út listánkba, mely eddig üres volt. Hozzáadjuk az első (és egyben egyetlen) útvonalat és észrevehetjük, hogy fedés lép fel ( $AB.VÉG\_IDŐ > BC.START\_IDŐ$  és  $\Delta := 1$ ). A  $MEGVÁG(1, AB, BC)$  eredményeként BC rövidebb lesz 1-el (start előre mozdult 1-el). Ez látható a 4.4 ábrán is.



4.4. ábra. IGG példa gráf, zölddel jelölve az éppen aktuálisan használatban lévő útvonal, pirossal pedig a megváltoztatott értékek.

Majd az eddig használt utunkat bővítjük a CD éllel is. Itt észrevehető, hogy az új útvonal hossza túllépte a  $MAX\_IDŐ$  értékét, így meg kell hívni rá a  $VÁGÁSAZABLAKMÉRÉTHEZ$  nevű függvényt is. Ennek következtében az AB és CD élek lecsökkennek 3-3 értékűre. Így az adott út  $OPTIKAIÁTERESZTÉS\ MAX$  által megadott értéke 3 lesz. Az AD útvonal értéke a 4.5. ábráról leolvasható. A 4.5. ábrán látható, hogy a zölddel jelzett AB-BC-CD útvonal jobb optikai áteresztéssel rendelkezik mint a pirossal jelölt AD.



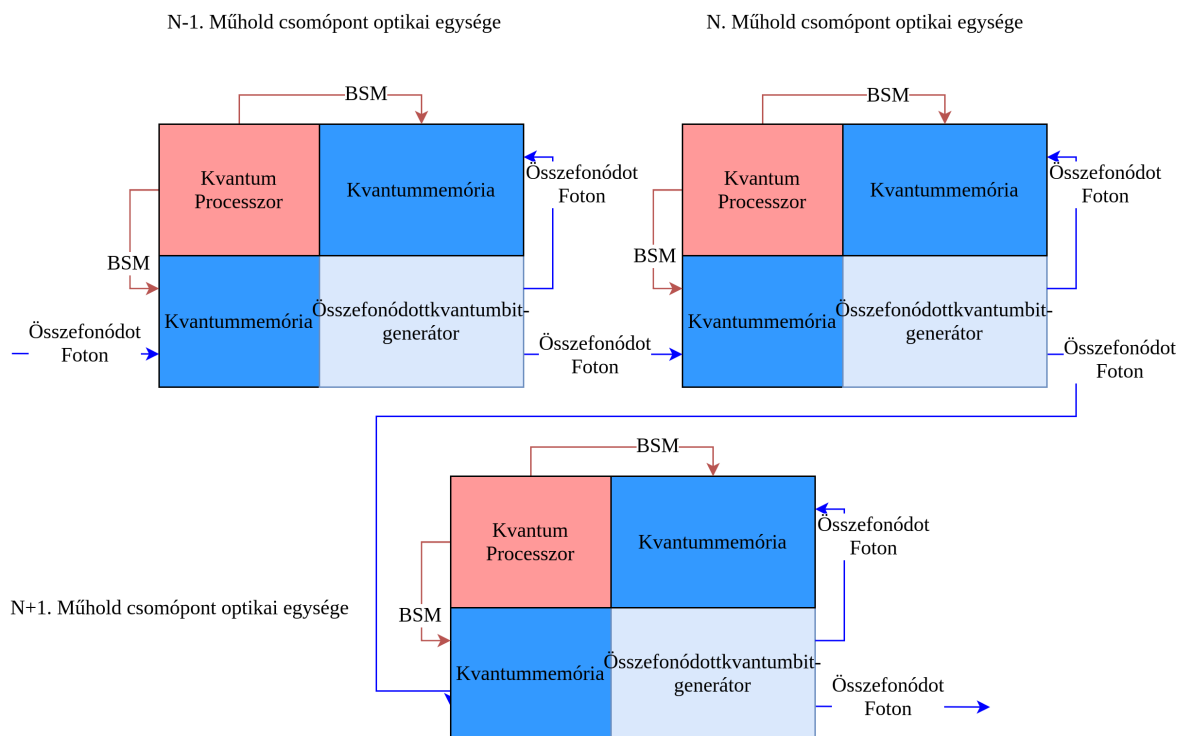
4.5. ábra. IGG gráf példa, zölddel jelölve a magasabb optikai áteresztésű útvonal, pirossal pedig a kisebb AD útvonal.

## 5. fejezet - Az elkészült szimulátor

A szimulátor a 3. és 4. fejezetben bemutatott elemek és a QSCS [11] optikai áteresztést számító moduljából áll. Az időbélyegzett intervallumgráfot az Orekit pályaszimulátor segítségével hoztam létre. A csomópontokat szimulált elemek (műholdak és földi csomópontok) alapján hoztam létre. A csomópontokat összekötő élek a hozzájuk tartozó elemek láthatósága alapján kerülnek a gráfba. Például az A1 és A2 csomópont között akkor van egy él, ha A1 látja egy bizonyos ideig az A2-t. A QSCS optikai áteresztést számító modulját felhasználva meghatároztam az élekhez tartozó függvényeket. Ezután futtatam az algoritmusomat az így kapott IIG-n. Ezt a művelet sorozatot megismételtem az összes műholdas rendszerre. A különböző műholdas rendszerek optikai áteresztése és az ebből legújabb eszközök alapján kiszámolt [16] összefonódott kvantumbitrátája a következő fejezetben található.

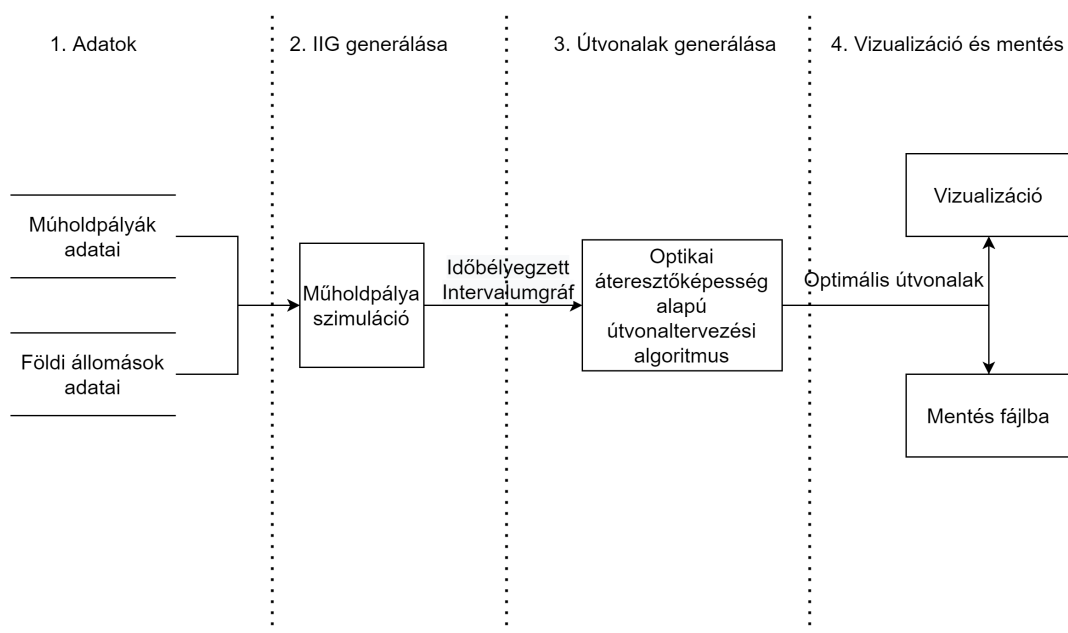
### 5.1. Műholdas kvantumsiméltő felépítése

A műholdas kvantumsiméltő architektúráis felépítését a szimulátoromon belül az 5.1. ábra mutatja. A műhold a kvantumösszefonódás generátorból kinyert fotonok egyikét a saját kvantummemóriájába helyezi, míg a másikat továbbküldi a következő műholdnak, amely azt eltárolja a saját kvantummemóriájába. A kvantummemóriába helyezett fotonokon a kvantumprocesszor végrehajtja a BSM-et, aminek hatására az  $N-1$  és  $N+1$  műhold kvantummemóriájában található kvantumbitek összefonódnak. Ennek a műveletnek az ismétlésével az összefonódás elteleportálható akár több csomóponton keresztül is. A szimulációm során feltételezem, hogy a műhold csak azután tudja elkezdni a kvantumbitek küldését, miután befejezte az előző csomópont felől azok vételét. Emellett szimulációm során nem térek ki olyan részletekre, mint a műhold iránya és annak megváltoztatásához kellő idő és erőforrások.



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

## 5.2. Szimulátor felépítése



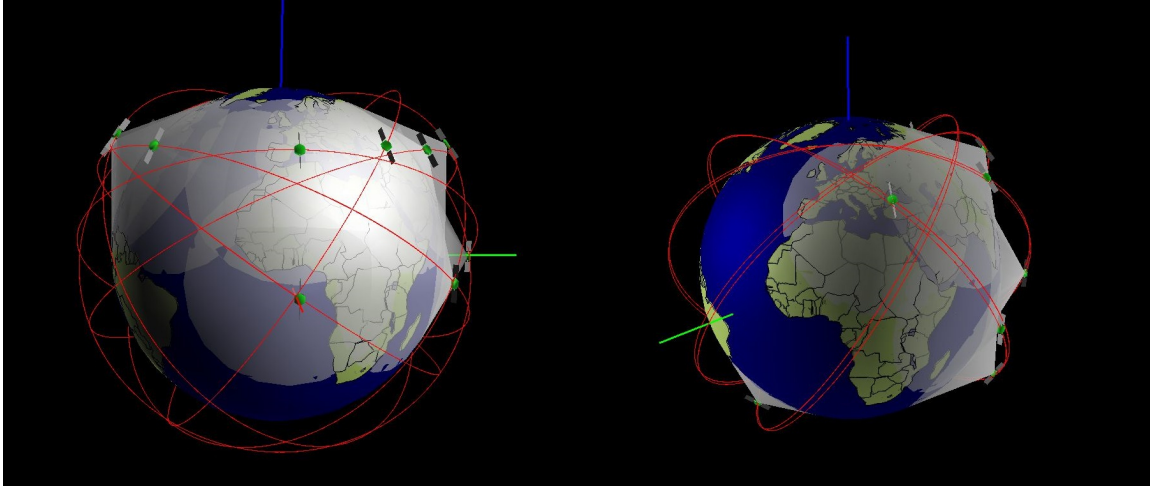
5.2. ábra. A szimulátor felépítése. Négy fő részből tevődik össze, valamint a hozzájuk tartozó modulokból. A fő részek a következők: 1. Adatok, 2. IIG generálása, 3. Útvonalak generálása, valamint 4. Vizualizáció.

Mint az az 5.2. ábrán is látható, a szimuláció felépítése négy fő részre osztható. Ezek balról jobbra olvasva a következők:

1. Adatok: Műholdpályák és városok helyzeti adatai. A műholdpálya adatok kepleri pálya formátumban kerültek megadásra. Összesen 6 féle rendszer van, melyek részletes leírása az 5.3. fejezetben. A városok állomásai szélesség, hosszúság és magasság formátumban vannak megadva.
2. IIG generálása: A műholdpropagációs-modul a kapott adatokból kiszámítja, hogy az adott műholdak és városokban található állomások mikor és meddig láthatják majd egymást. Ebből készíti el az IIG éleit, ahol a csomópontok pedig a műholdak és városok lesznek.
3. Útvonalak generálása: A már korábban többször is tárgyalt algoritmus segítségével kiszámítjuk az optimális útvonalakat minden város állomása között.
4. Vizualizáció és mentés: Ebben a fázisban az optimális útvonalakat vizualizáljuk Plotly [17] és Graphviz [18] segítségével vagy elmentjük egy fájlba.

### 5.3. Felhasznált műhold rendszerek

A szimulációim során nyolc műholdrendszerrel dolgoztam, azon belül két különböző architektúrán négy-négy konstellációval. Mindkét architektúra a felépítésének egy közös pontja, hogy kétféle inklinációval rendelkeznek. Az első architektúra a retrográd típusú, itt az pályák felének inklinációjának iránya szembe megy az alapbeállítással. Egy retrográd típusú műhold rendszer látható az 5.3. ábrán is. A második architektúra a kereszt pályás. Itt az inklinációt  $90^\circ$  fokkal módosítottam minden második pálya esetén. A keresztpályás architektúrára található egy példa az 5.3 ábrán.



5.3. ábra. Keresztpályás műholdkonsteláció (baloldalt) és retrográd műholdkonsteláció (jobbaldalt) vizualizációja.

Mindkét architektúrát ugyanazokkal a beállításokkal (az inklinációt leszámítva) hoztam létre. A műholdak pályadatainak összesen két változóját módosítottam, a pálya referencia ponttal bezárt szögét  $\Omega$  és a pálya legmagasabb pontja és a referencia pont által bezárt szöget  $\omega$ . Ezeket az értékeket változtattam rendszerenként különböző szögtartományokon  $45^\circ$  fokos léptékben (a  $45^\circ$  volt az az érték melyen még pont látták egymást a műholdak és egyenletes eloszlást is adott). A négyféle műholdas-pályarendszer szögtartományai a 5.1. táblázatban találhatóak.

Név	$\Omega$ szögtartomány	$\omega$ szögtartomány
Kicsi	$180^\circ$	$180^\circ$
Közepes I	$180^\circ$	$360^\circ$
Közepes II	$360^\circ$	$180^\circ$
Nagy	$360^\circ$	$360^\circ$

5.1. táblázat. A négyféle műholdpálya-rendszer szögtartományai.

## 5.4. Bemeneti adatok

A szimuláció során használt adatok a műholdak pályáihoz az 5.2. táblázatban találhatóak.

a	e	i	$\Omega$	$\omega$	$\nu$
1000 km	0.0002090	56.0568°	változó°	változó°	18°

**5.2. táblázat.** Műholdpályákhoz felhasznált adatok.

Az optikai áteresztéshez felhasznált adatok, melyek nem alapértékként szerepelnek a QSCS-ben az 5.3. táblázatban láthatóak.

Név	új érték
Kvantumérzékelő hatásfoka	70%
Évszak	nyár
Időjárás	tiszta

**5.3. táblázat.** QSCS-ben változtatott adatok.



## 6. fejezet - Eredmények

Munkám során kétféle műholdrendszer architektúrával dolgoztam, azon belül négy-négy konstellációval. A műholdrendszerek összetételei megtalálhatóak az 5.1. táblázatban. Fontos megjegyezni, hogy az átviteli sebességet úgy kaptam, hogy az optikai áteresztést megszoroztam a már említett kutatásban [16] is bemutatott 3.51 kHz-es maximális vételi frekvenciával. Ennek a behelyettesítésnek célja, hogy a számolt optikai áteresztőképességet kontextusba helyezze. Az itt bemutatott rendszerek részletes leírása az 5.3 fejezetben található.

### 6.1. Retrográd műholdkonstelláció

A retrográd műholdrendszer alapötlete az algoritmusom működéséből adódik, hiszen működésére pozitívan hat, ha a műholdak sok rövid időintervallumon keresztül látják egymást. Amint később látható lesz, az itt alkalmazott teljesen ellentétes irányú keringési pálya túlságosan lerövidíti a láthatósági időintervallumokat. Ennek hatására hoztam létre a 6.2 szakaszban is tárgyalt kereszt pályás műholdkonstellációt.

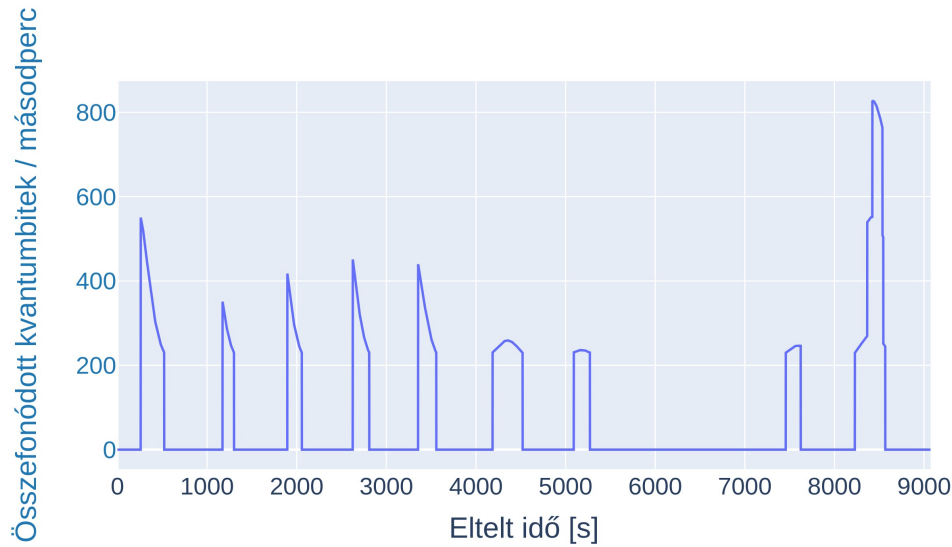
#### 6.1.1. Kicsi műholdas-pályarendszer

A kicsi műholdas-pályarendszer, mint az látható az 5.1. táblázatban,  $180^\circ$  fokos szögtartományt használ mindkét paraméteréhez, ennek következtében az egyik legkisebb műholdrendszer mindössze 16 műhoddal. Az alacsony műholdszám ellenére, mint az a 6.1. táblázatban is látható, ez rendszer képes az akár 60 aeqb/s-t (average entangled quantum bits per second – másodpercenként átlagosan átküldött összefonódott kvantumbitek száma) elérni.

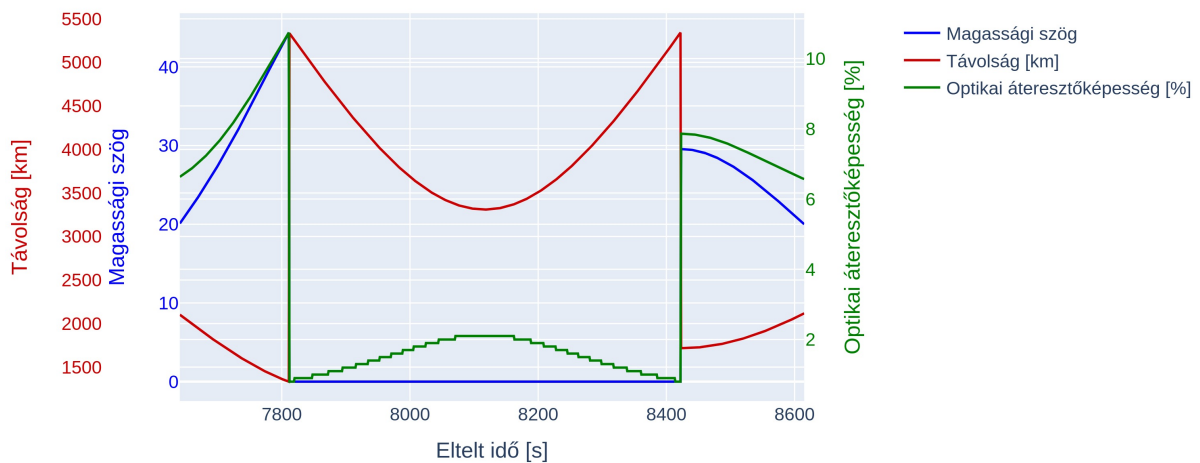
-	Berlin	Budapest	Koppenhága	Párizs	Róma	Bécs	Helsinki
Berlin	-	64.42812	41.31180	22.95357	49.47702	59.02426	46.77974
Budapest	45.29421	-	37.79582	25.05377	52.57554	58.68008	58.76313
Koppenhága	49.12164	65.32778	-	21.89001	45.12614	58.49806	51.09931
Párizs	38.15695	46.84172	31.23979	-	54.30229	46.76494	11.77207
Róma	37.79717	62.75925	30.52582	28.74644	-	55.33416	34.31658
Bécs	45.18255	65.65733	37.49431	25.22934	52.29786	-	51.13031
Helsinki	28.49015	38.26060	29.28240	8.62247	19.94570	32.13625	-

**6.1. táblázat.** Kicsi retrográd műholdas pályarendszer városok között mért aeqb/s mértéke.

A 6.1. ábrán láthatóak a Budapest-Helsinki csatornán keresztül átküldött összefonódott kvantumbitek másodperces leosztásban. Észrevehető, hogy a műholdak alacsony száma miatt a létrejött kapcsolatok időben szórtak. Emellett látható a 6.2. ábrán, hogy az optikai áteresztés és az ebből következő aeqb/s miként korrelál a magassági szöggel és a csomópontok egymás közötti távolságával.



**6.1. ábra.** Kicsi retrográd konstelláció esetén a Budapest-Helsinki csatorna összefonódott kvantumbitek átvitele másodperces leosztásban. A függőleges tengelyen a másodperceként átvihető összefonódott kvantumbitek száma látható. A vízszintes tengelyen látható a szimuláció kezdetétől eltelt idő másodpercben.



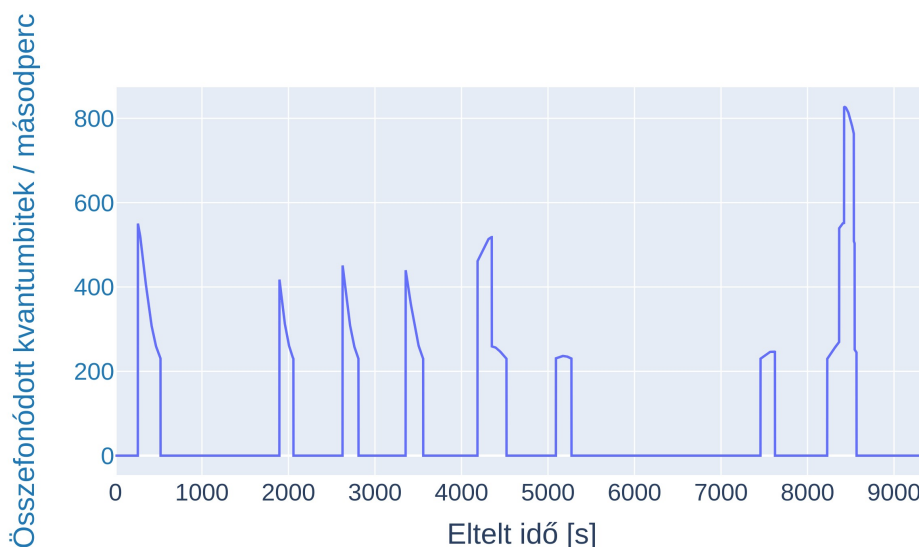
**6.2. ábra.** Kicsi retrográd konstelláció esetén a Budapest-Helsinki csatorna optikai átvitelének változása a távolság és magassági szög mentén. A függőleges tengelyen késsel a magassági szög, pirossal a csomópontok közötti távolság kilométerben és zölddel pedig az optikai áteresztőképesség található. A vízszintes tengelyen a szimuláció kezdetétől eltelt idő látható másodpercben.

### 6.1.2. Közepes I. műholdas-pályarendszer

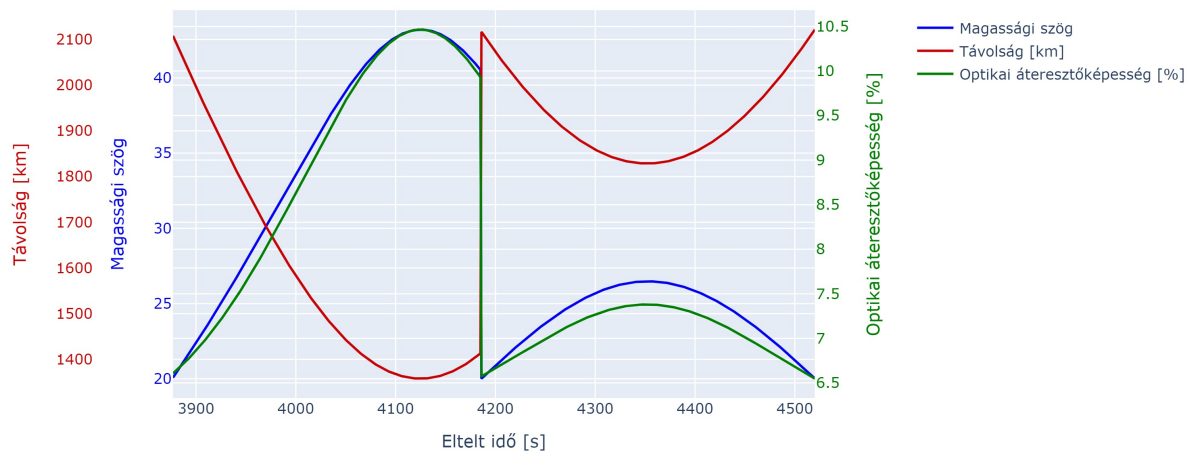
Bár a műholdak száma megduplázódott, mint az a 6.2. táblázatban is látható, a városok közötti átvitel nem nőtt számottevően. Ennek oka, hogy mivel az  $\omega$  paramétert módosítottuk, az új műholdpályák hasonlóan metszették az egyenlítő vonalát mint a kicsi konstelláció esetén. Ennek hatása látható a 6.3. ábrán.

-	Berlin	Budapest	Koppenhága	Párizs	Róma	Bécs	Helsinki
Berlin	-	82.14925	64.72415	53.10107	76.15665	79.60466	62.05818
Budapest	65.29231	-	62.51567	54.14387	74.77457	76.22060	69.52699
Koppenhága	76.06209	85.84532	-	58.28770	74.87705	83.26067	69.37869
Párizs	61.00009	68.52142	53.98463	-	73.59016	69.19954	35.44380
Róma	60.91048	83.36521	60.10333	64.59721	-	77.79544	53.83245
Bécs	62.79858	78.36456	60.33751	51.44698	72.57279	-	61.46090
Helsinki	65.46293	66.54681	66.95193	46.73272	54.74560	65.37252	-

6.2. táblázat. Közepes I. retrográd műholdas pályarendszer városok között mért aeqb/s mértéke.



6.3. ábra. Közepes I. retrográd konstelláció esetén a Budapest-Helsinki csatorna összefonódott kvantumbit átvitele másodperces leosztásban. A függőleges tengelyen a másodperceként átvihető összefonódott kvantumbitek száma látható. A vízszintes tengelyen látható a szimuláció kezdetétől eltelt idő másodpercben.



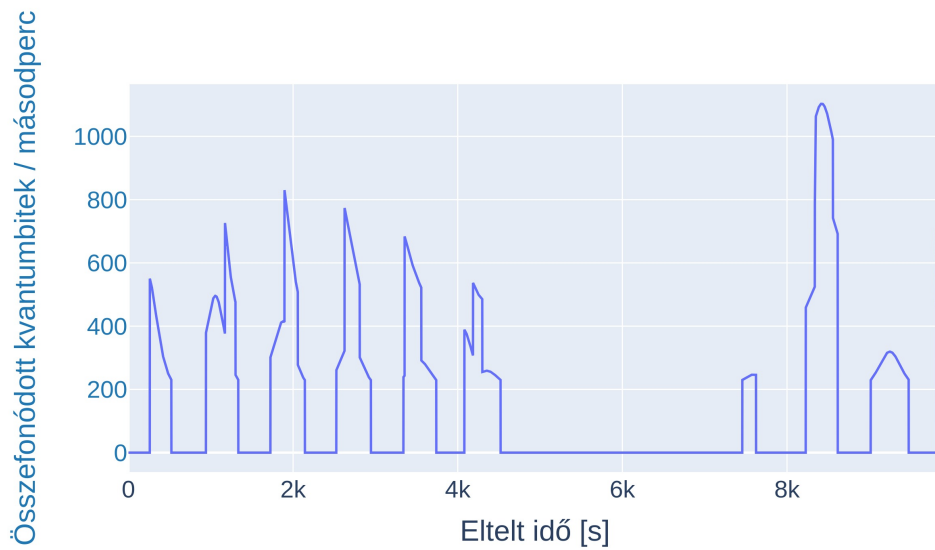
**6.4. ábra.** Közepes I. retrográd konstelláció esetén a Budapest-Helsinki csatorna optikai átvitelének változása a távolság és magassági szög mentén. A függőleges tengelyen késsel a magassági szög, pirossal a csomópontok közötti távolság kilométerben és zölddel pedig az optikai áteresztőképesség található. A vízszintes tengelyen a szimuláció kezdetétől eltelt idő látható másodpercben.

### 6.1.3. Közepes II. műholdas-pályarendszer

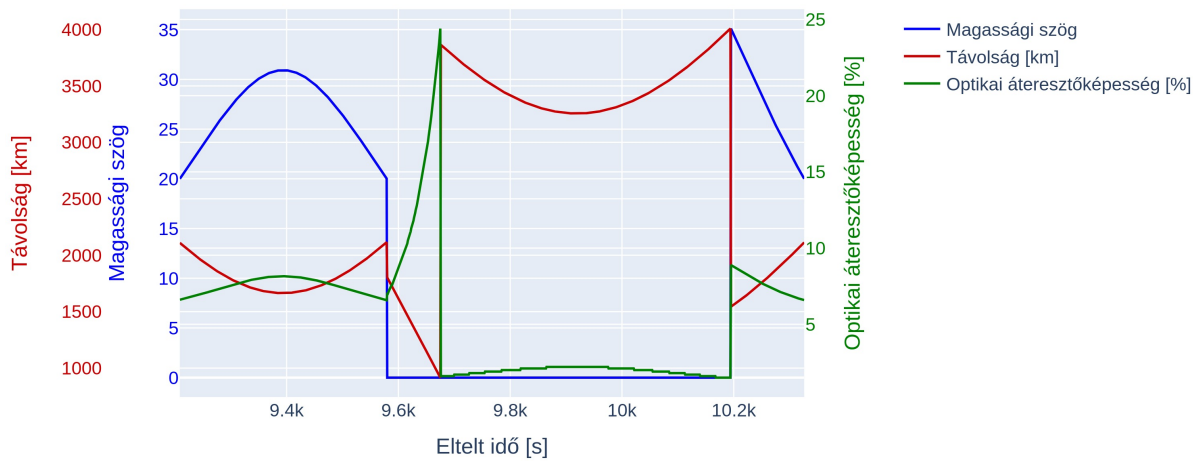
A közepes II. konstelláció műholdpályáinak száma megegyezik a közepes I. konstellációéval. Ennek ellenére a 6.3. táblázatban is látható, hogy nagyobb  $aeq_b/s$ -t lehetett így elérni. Ennek oka, mint az leolvasható a 6.6. ábráról is, hogy ebben a konstrukcióban a műholdpályák több helyen metszették az egyenlítőt. Ennek hatására sokkal több műholdon (és hosszabb útvonalakon) keresztül tudta a rendszer a kvantumbiteket küldeni. Emellett még a földi csomópontból induló élek száma is megnövekedett a közepes I-hez képest mint az a 6.5. ábrán látható.

-	Berlin	Budapest	Koppenhága	Párizs	Róma	Bécs	Helsinki
Berlin	-	147.51227	96.75487	68.57751	109.09861	134.38081	160.61676
Budapest	99.76350	-	84.85981	67.58029	107.34048	126.25456	179.97743
Koppenhága	109.51873	139.58650	-	63.58533	97.43632	127.12833	150.53527
Párizs	95.06740	111.49410	79.08020	-	115.58327	111.06273	109.35876
Róma	97.88389	145.86209	78.22572	67.84189	-	130.69961	162.68432
Bécs	104.19434	146.74887	87.59853	67.12310	111.52030	-	171.42306
Helsinki	70.08267	89.96576	64.62559	53.76247	63.00812	79.70668	-

**6.3. táblázat.** Közepes II. retrográd műholdas pályarendszer városok között mért  $aeq_b/s$  mértéke.



**6.5. ábra.** Közepes II. retrográd konstelláció esetén a Budapest-Helsinki csatorna összefonódott kvantumbitek átvitele másodperces leosztásban. A függőleges tengelyen a másodpercként átvihető összefonódott kvantumbitek száma látható. A vízszintes tengelyen látható a szimuláció kezdetétől eltelt idő másodpercben.



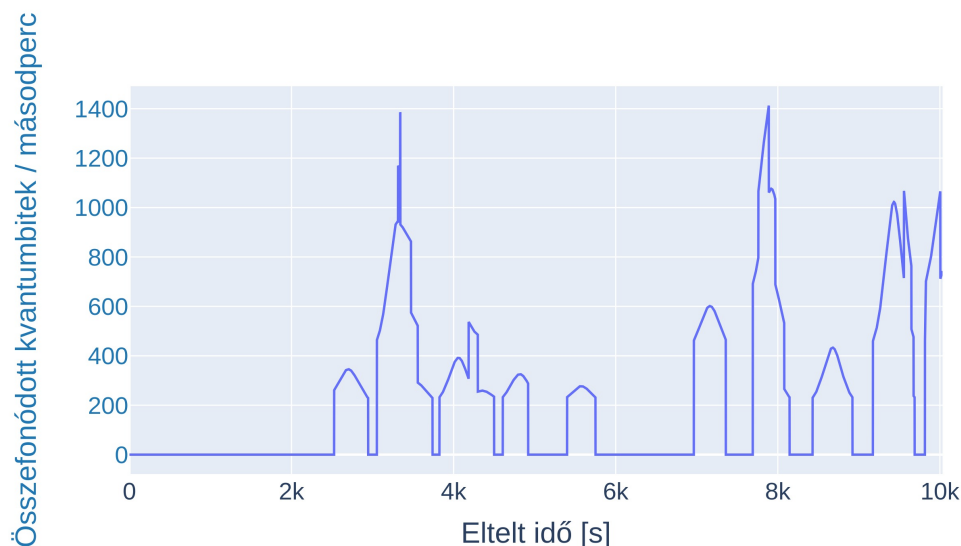
**6.6. ábra.** Közepes II. retrográd konstelláció esetén a Budapest-Helsinki csatorna optikai átvitelének változása a távolság és magassági szög mentén. A függőleges tengelyen kékkel a magassági szög, pirossal a csomópontok közötti távolság kilométerben és zölddel pedig az optikai áteresztőképesség található. A vízszintes tengelyen a szimuláció kezdetétől eltelt idő látható másodpercben.

### 6.1.4. Nagy műholdas-pályarendszer

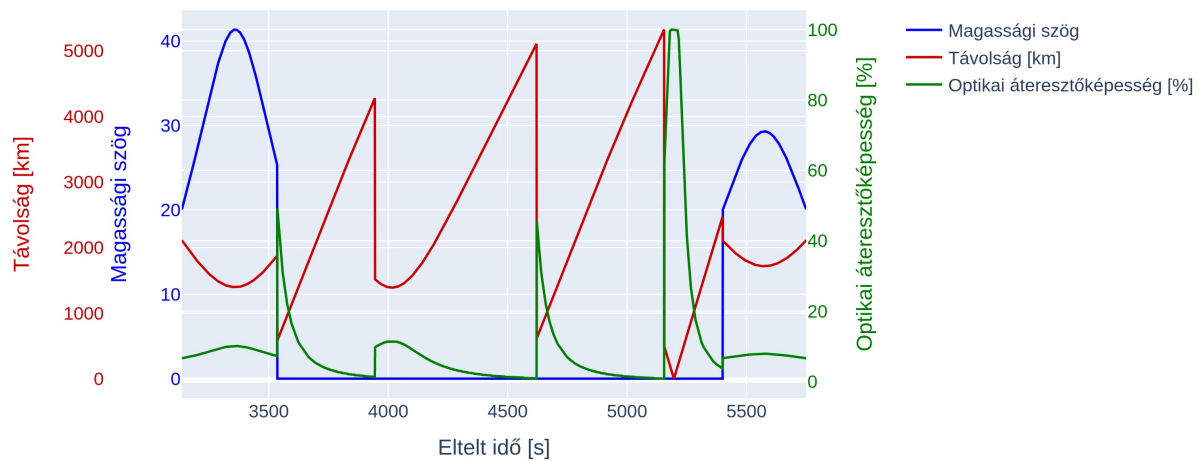
A nagy műholdas-pályarendszer az előző konstellációk műholdpályáinak kétszeresével rendelkezik. Ennek hatására, mint ahogy az a 6.4. táblázaton is látható, a nagy konstellációhoz tartozik a legmagasabb aeqb/s érték. A műholdpályák számának növekedése miatt, mint az a 6.7. ábrán is látható, az átviteli intervallumok sűrűbben szerepelnek, mint az többi konstelláció esetén. Emellett megfigyelhető az optikai áteresztés változásának nem-linearitása a 6.8. ábrán az 5400. másodperc pillanatában. Az optikai áteresztés megközelíti a 100%-ot az egymás mellett elhaladó műholdak alacsony távolságának köszönhetően.

-	Berlin	Budapest	Koppenhága	Párizs	Róma	Bécs	Helsinki
Berlin	-	255.24907	266.39334	234.36360	281.10237	257.90713	236.54618
Budapest	285.27226	-	288.68686	232.26338	286.65069	280.04034	239.66653
Koppenhága	264.52359	253.86092	-	235.13251	278.08865	260.09756	235.55939
Párizs	192.40191	194.49171	187.06306	-	226.48654	201.20572	176.07644
Róma	245.55478	238.74375	243.49532	194.48043	-	243.54502	220.70148
Bécs	268.02030	258.44857	272.76778	227.10067	272.33064	-	231.96909
Helsinki	297.52615	296.72203	304.81222	214.91711	293.61188	295.45121	-

6.4. táblázat. Nagy retrográd műholdas pályarendszer városok között mért aeqb/s mértéke.



6.7. ábra. Nagy retrográd konstelláció esetén a Budapest-Helsinki csatorna összefonódott kvantumbit átvitele másodperces leosztásban. A függőleges tengelyen a másodperceként átvihető összefonódott kvantumbitek száma látható. A vízszintes tengelyen látható a szimuláció kezdetétől eltelt idő másodpercben.



**6.8. ábra.** Nagy retrográd konstelláció esetén a Budapest-Helsinki csatorna optikai átvitelének változása a távolság és magassági szög mentén. A függőleges tengelyen késsel a magassági szög, pirossal a csomópontok közötti távolság kilométerben és zölddel pedig az optikai áteresztőképesség található. A vízszintes tengelyen a szimuláció kezdetétől eltelt idő látható másodpercben.

## 6.2. Keresztpályás műholdas rendszer

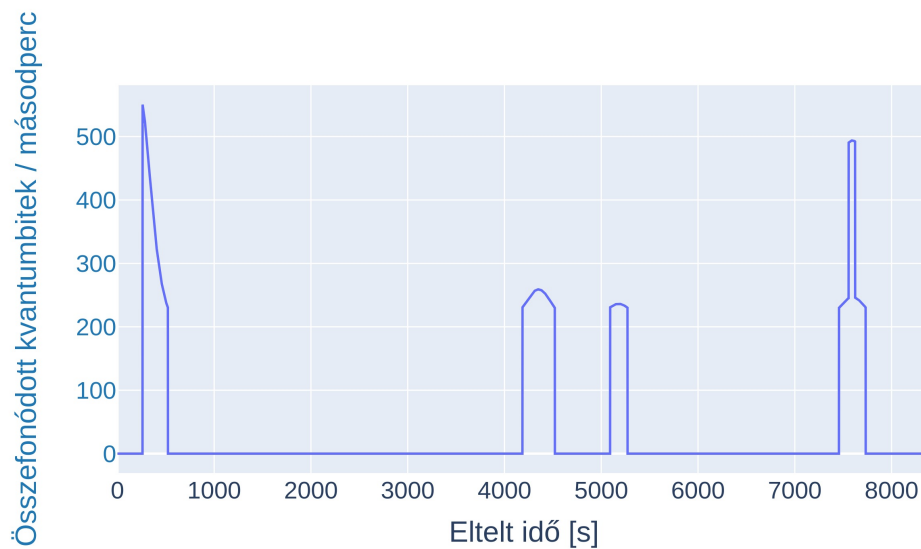
A keresztpályás architektúra lényege, hogy a kisebb szöggel ( $90^\circ$ ) elforgatott inklináció miatt a műholdak hosszabb ideig lesznek egymás látóterében a retrográdhoz képest. Ezt az architektúrát, a retrográdhoz hasonlóan végigpróbáltam a 4 konstelláción.

### 6.2.1. Kicsi műholdas-pályarendszer

Mint az látható a 6.5. táblázatban is, a kis konstelláció esetén lényegesen kisebb átviteli rátát eredményezett a keresztpályás konstrukció. Ez az inklináció forgatási szögének csökkenéséből következik, mivel így hosszabb ideig, de kevesebb alkalommal kerülnek a műholdak a földi állomások látószögén belülre. Ez látható a 6.9. ábrán is, ahol észrevehetően kevesebb vételi intervallum található, mint a retrográd architektúra esetén.

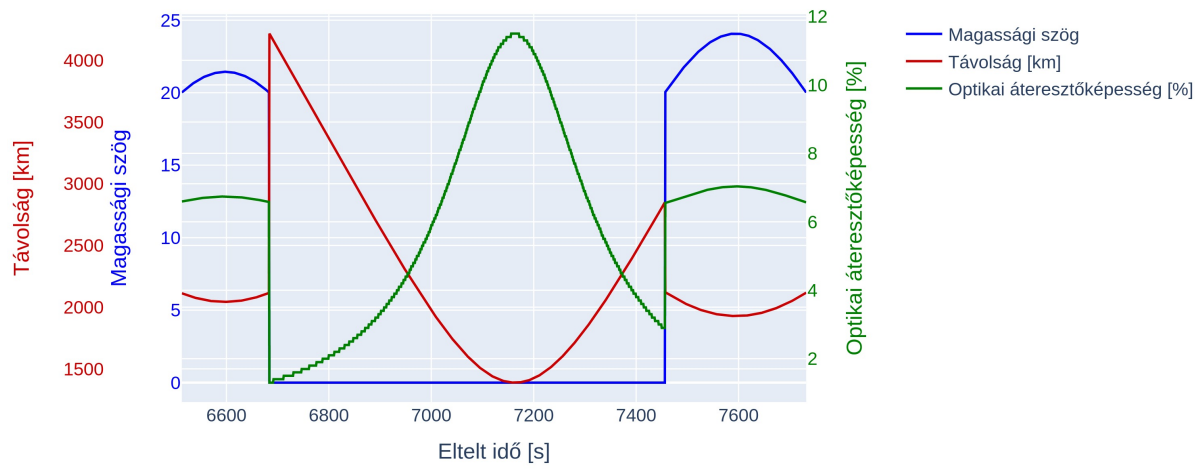
-	Berlin	Budapest	Koppenhága	Párizs	Róma	Bécs	Helsinki
Berlin	-	8.80317	25.49884	36.91194	11.86039	14.52381	13.98029
Budapest	32.96018	-	37.18134	34.94577	20.04431	24.06261	28.10296
Koppenhága	25.57932	4.81463	-	41.57362	10.91598	12.85361	13.16004
Párizs	17.45124	4.11815	17.74429	-	10.41773	9.22140	4.12009
Róma	32.06430	30.75552	34.86586	39.33664	-	29.25053	22.81289
Bécs	29.74071	20.26730	31.28992	30.54627	19.88941	-	24.44117
Helsinki	32.86433	8.00622	33.32758	33.14869	19.99601	21.96028	-

**6.5. táblázat.** Kicsi keresztpályás műholdas pályarendszer városok között mért aeqb/s mértéke.



**6.9. ábra.** Kicsi keresztpályás konstelláció esetén a Budapest-Helsinki csatorna összefonódott kvantumbit átvitele másodperces leosztásban. A függőleges tengelyen a másodperceként átvihető összefonódott kvantumbitek száma látható. A vízszintes tengelyen látható a szimuláció kezdetétől eltelt idő másodpercben.





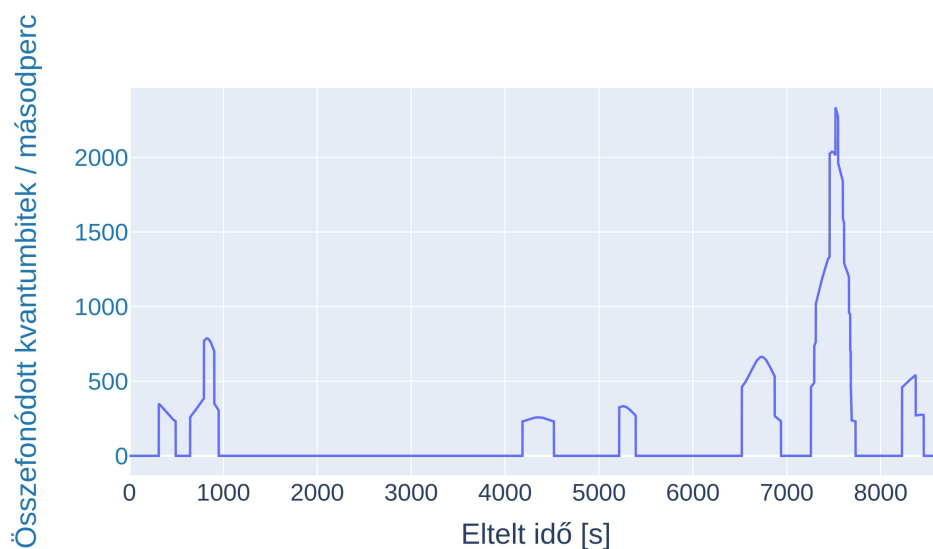
**6.10. ábra.** Kicsi keresztpályás konstelláció esetén a Budapest-Helsinki csatorna optikai átvitelének változása a távolság és magassági szög mentén. A függőleges tengelyen késsel a magassági szög, pirossal a csomópontok közötti távolság kilométerben és zölddel pedig az optikai áteresztőképesség található. A vízszintes tengelyen a szimuláció kezdetétől eltelt idő látható másodpercben.

## 6.2.2. Közepes I. műholdas-pályarendszer

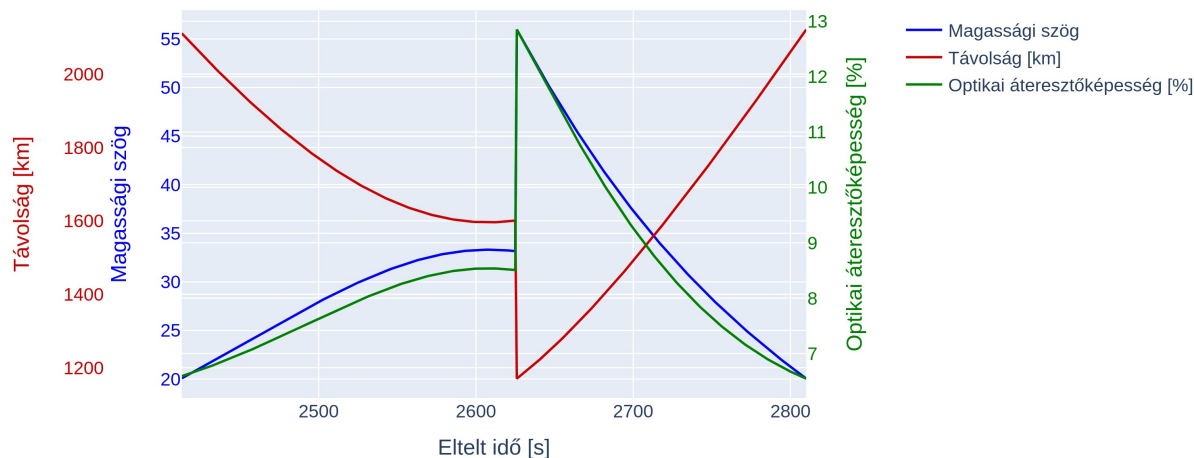
A közepes I. konstellációval, amint a 6.6. táblázatban is láthatjuk jelentős a javulás, a retrográd rendszerhez képest. Ennek oka a szélesebb átviteli intervallumok, ahogyan az a 6.12. És 6.11. ábrákon is látható.

-	Berlin	Budapest	Koppenhága	Párizs	Róma	Bécs	Helsinki
Berlin	-	83.82721	80.70833	96.12476	100.24408	78.82185	70.17809
Budapest	106.95248	-	119.08591	122.87452	113.49236	99.83637	116.89566
Koppenhága	94.59570	90.80703	-	120.99777	112.98851	91.33856	72.50388
Párizs	75.82295	76.30544	78.19215	-	102.53302	78.17207	61.87120
Róma	113.26650	97.84910	126.13099	133.85561	-	97.19303	104.98859
Bécs	86.01448	91.93455	95.44265	102.48189	95.60904	-	93.08823
Helsinki	85.83907	78.19349	90.07197	101.62086	98.21774	84.71151	-

**6.6. táblázat.** Közepes I. keresztpályás műholdas pályarendszer városok között mért aeqb/s mértéke.



**6.11. ábra.** Közepes I. keresztpályás konstelláció esetén a Budapest-Helsinki csatorna összefonódott kvantumbit átvitele másodperces leosztásban. A függőleges tengelyen a másodperceként átvihető összefonódott kvantumbitek száma látható. A vízszintes tengelyen látható a szimuláció kezdetétől eltelt idő másodpercben.



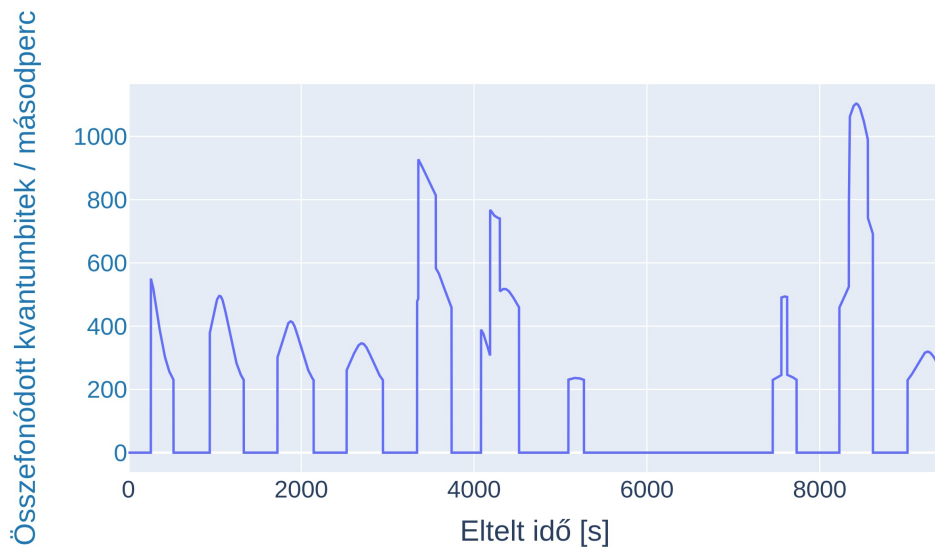
**6.12. ábra.** Közepes I. keresztpályás konstelláció esetén a Budapest-Helsinki csatorna optikai átvitelének változása a távolság és magassági szög mentén. A függőleges tengelyen kékkkel a magassági szög, pirossal a csomópontok közötti távolság kilométerben és zölddel pedig az optikai áteresztőképesség található. A vízszintes tengelyen a szimuláció kezdetétől eltelt idő látható másodpercben.

### 6.2.3. Közepes II. műholdas-pályarendszer

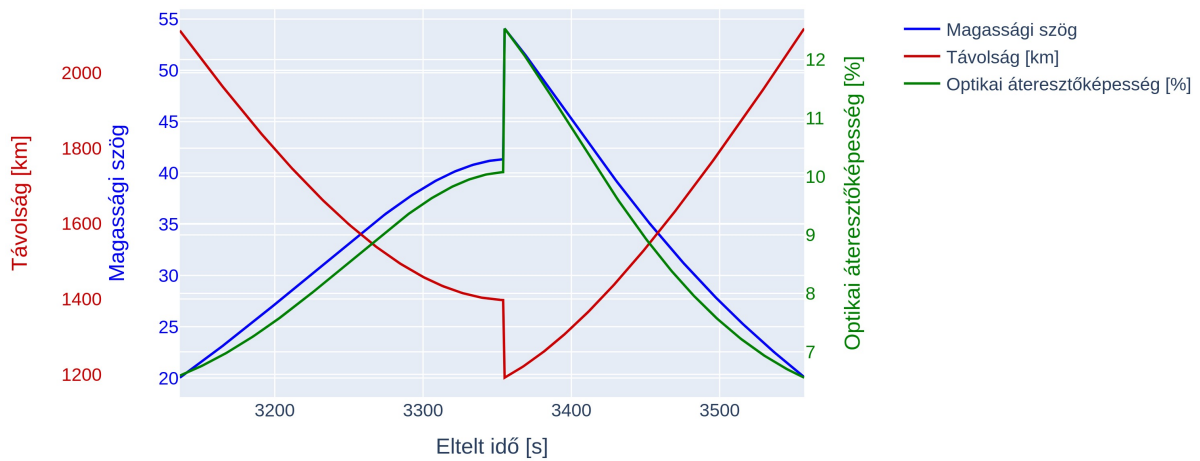
A közepes II. konstelláció, nem mutatta a retrográd párjánál tapasztalt hirtelen javulást a közepes I-hez képest. Ahogyan azt a 6.13. és 6.11. ábrákon láthatjuk, a közepes II. konstelláció összefonódott kvantumbitvételi intervallumai nagyobb időtartományt fednek le, mint a közepes I. esetén. Ennek következtében egy valós környezetben a közepes II. konstelláció sokkal hatásosabb lehet, mivel algoritmusom a linkek kihasználtságát nem veszi figyelembe.

-	Berlin	Budapest	Koppenhága	Párizs	Róma	Bécs	Helsinki
Berlin	-	124.65632	104.57918	106.29057	109.06968	121.61523	122.16698
Budapest	115.22326	-	110.67623	109.11548	107.90561	127.45683	165.45065
Koppenhága	109.02145	107.65310	-	107.38481	96.71343	110.34401	113.84394
Párizs	73.25526	70.58364	70.91834	-	71.75558	71.77694	93.27655
Róma	106.41179	130.33654	97.88157	103.90238	-	121.84738	156.60987
Bécs	109.16530	129.11919	103.27664	103.23634	106.90611	-	140.11992
Helsinki	93.76837	77.16165	95.66630	101.14634	87.67230	84.68098	-

**6.7. táblázat.** Közepes II. keresztpályás műholdas pályarendszer városok között mért aeqb/s mértéke.



**6.13. ábra.** Közepes II. keresztpályás konstelláció esetén a Budapest-Helsinki csatorna összefonódott kvantumbitek átvitele másodperces leosztásban. A függőleges tengelyen a másodperceként átvihető összefonódott kvantumbitek száma látható. A vízszintes tengelyen látható a szimuláció kezdetétől eltelt idő másodpercben.



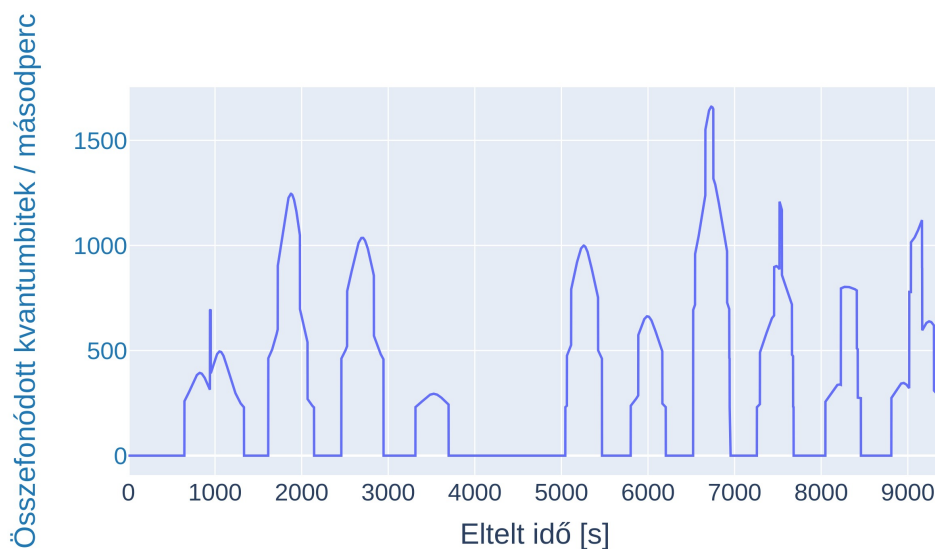
**6.14. ábra.** Közepes II. keresztpályás konstelláció esetén a Budapest-Helsinki csatorna optikai átvitelének változása a távolság és magassági szög mentén. A függőleges tengelyen késsel a magassági szög, pirossal a csomópontok közötti távolság kilométerben és zölddel pedig az optikai áteresztőképesség található. A vízszintes tengelyen a szimuláció kezdetétől eltelt idő látható másodpercben.

### 6.2.4. Nagy műholdas-pályarendszer

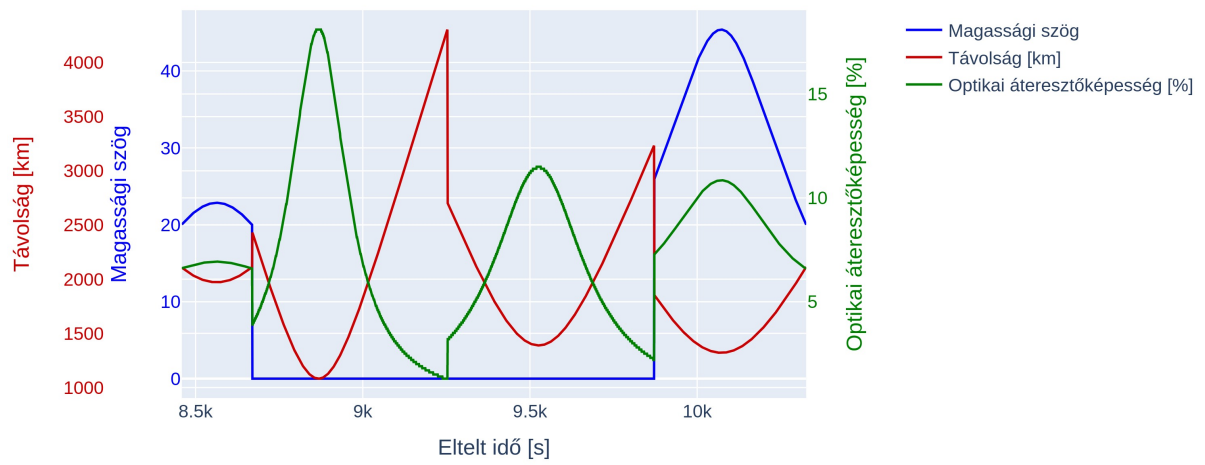
Mint ahogyan a 6.15. ábrán is látható, a nagy konstelláció vételi intervallumai sokkal szélesebbek és szélesebbek, mint a retrográd változat esetén. Ahogyan az a 6.4 és 6.8. táblázatokon is látható, nincsen jelentősebb eltérés aeqb/s-ben a két architektúrát használó konstelláció között.

-	Berlin	Budapest	Koppenhága	Párizs	Róma	Bécs	Helsinki
Berlin	-	229.08025	220.33371	221.49774	259.61238	237.27164	228.21818
Budapest	296.39326	-	284.94728	265.50331	336.24115	323.87205	310.28552
Koppenhága	232.98493	223.58369	-	227.54747	256.80167	234.41200	226.04335
Párizs	222.32739	196.35187	223.16379	-	268.99732	215.99869	242.66861
Róma	262.18038	256.13162	263.93836	259.59142	-	272.61412	282.15459
Bécs	256.66539	264.38853	246.77708	235.69861	288.19515	-	260.59171
Helsinki	310.61381	296.53197	301.08531	272.64197	327.61846	319.09364	-

**6.8. táblázat.** Nagy keresztpályás műholdaspályarendszer esetén számolt, városok közötti átlagos másodpercenkénti összefonódott kvantumbitátvitel



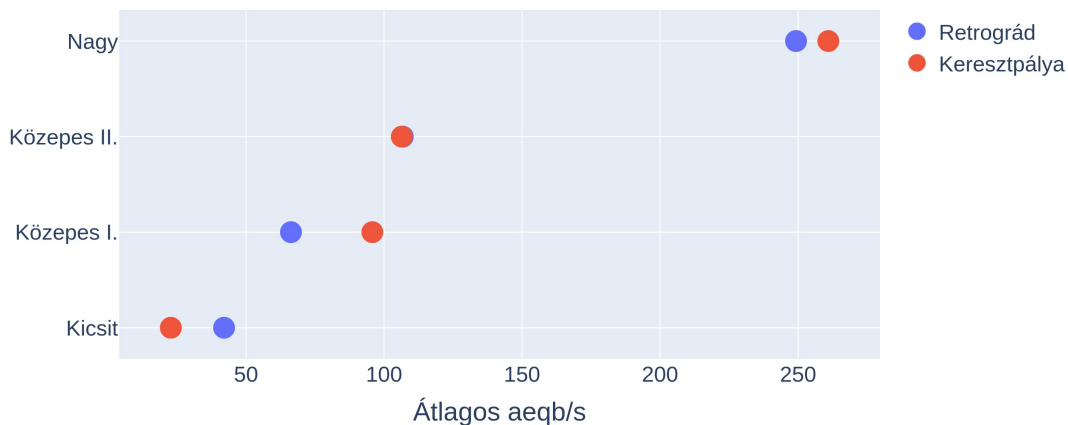
**6.15. ábra.** Nagy keresztpályás konstelláció esetén a Budapest-Helsinki csatorna összefonódott kvantumbit átvitelének másodperces leosztásában. A függőleges tengelyen a másodpercenként átvihető összefonódott kvantumbitek száma látható. A vízszintes tengelyen látható a szimuláció kezdetétől eltelt idő másodpercben.



**6.16. ábra.** Nagy keresztpályás konstelláció esetén a Budapest-Helsinki csatorna optikai átvitelének változása a távolság és magassági szög mentén. A függőleges tengelyen késsel a magassági szög, pirossal a csomópontok közötti távolság kilométerben és zölddel pedig az optikai áteresztőképesség található. A vízszintes tengelyen a szimuláció kezdetétől eltelt idő látható másodpercben.

## 7. fejezet - Összefoglalás

Dolgozatom célja alternatív műholdas konstellációk vizsgálata volt az általam fejlesztett optikai áteresztőképesség alapú útvonaltervező algoritmus segítségével. A munkám során két különböző műholdas architektúrát is megvizsgáltam több konstellációs beállítás mellett. A mért eredmények aggregált grafikonja látható a 7.1. ábrán melyen a különböző konstellációk átlagos aeqb/s értéke található.



**7.1. ábra.** Műholdas konstelláció architektúrák összehasonlítása. Késsel a retrográd, míg pirossal a keresztpályás konstellációk átlag aeqb/s értéke található.

A retrográd műholdas konstrukciók vizsgálataim alapján inkább olyan rendszerek támogatására alkalmasak, melyek nem igényelnek konzisztens kvantumbitátvitelt. Emellett fontos még megemlítenem, hogy mint azt a 6.1.1. és 6.2.1. alfejezetekben is láthattuk, alacsony műholdszám mellett nagyobb aeqb/s-re ad lehetőséget.

Keresztpályás műholdas architektúra esetén, mint azt a releváns fejezetekben is említettem, sokkal elnyújtottabbak az átviteli intervallumok. Ezért egy ezt felhasználó jövőbeli műholdrendszer nagyobb átvitelű és alacsonyabb késleltetésű hálózatot eredményezne.

Szimulációm és algoritmusom segítségével egy lehetséges alternatívát tudtam találni a műholdas kvantumhálózatok számára. Bár az általam használt rendszerek nem képesek valós idejű kvantumkommunikációt biztosítani, egy ilyen rendszerrel már lehetne viszonylag kevés műhold segítségével is egy "valós" kvantuminternetet létrehozni.


Munkámat több irányba is lehet folytatni. Az első egy tükör alapú "hosszabbító" műholdas rendszer. Itt a kvantumműholdak mellett tükrökkel felszerelt segédműholdak segítenék a kommunikációt. Egy másik lehetőség az optikai áteresztés alapú útvonaltervező algoritmus kiegészítése, hogy az egyes élek kihasználtságát is figyelembe vegye. Ezek mellett szerintem egy szintén nagyon érdekes kutatási irány lenne egy műholdas kvantum ismétlő hardverének részletes megtervezése és modellezése.

Végül, de nem utolsósorban, szeretném megköszönni Bacsárdi László konzulensemnek, aki immár több mint két éve segíti a kvantumkommunikációs témában kutatásaimat.

*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] Lov K. Grover. „From Schrödinger’s equation to the quantum search algorithm”. en. *Pramana* 56.2 (2001. febr.), 333–348. old. ISSN: 0973-7111. DOI: 10.1007/s12043-001-0128-3. URL: <https://doi.org/10.1007/s12043-001-0128-3> (elérés dátuma 2021. 10. 21.).
- [3] Sandor Imre. „Quantum Existence Testing and Its Application for Finding Extreme Values in Unsorted Databases”. *IEEE Transactions on Computers* 56.5 (2007. máj.), 706–710. old. ISSN: 1557-9956. DOI: 10.1109/TC.2007.1032.
- [4] 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>.
- [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] 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.).
- [7] 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.).
- [8] *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.).
- [9] *Astrodynamics in python* . URL: <https://docs.poliastro.space/en/v0.15.2/?badge=v0.15.2>.

- [10] *Cesium: The Platform for 3D Geospatial*. en-US. URL: <https://www.cesium.com/> (elérés dátuma 2021. 10. 03.).
- [11] *Quantum Satellite Communication Simulator*. URL: <https://www.mcl.hu/quantum-old/simulator/> (elérés dátuma 2021. 10. 03.).
- [12] Luc Maisonobe, Véronique Pommier és Pascal Parraud. „OREKIT: AN OPEN SOURCE LIBRARY FOR OPERATIONAL FLIGHT DYNAMICS APPLICATIONS”. 2010. ápr.
- [13] *Orekit*. en. URL: <https://forum.orekit.org/> (elérés dátuma 2021. 10. 03.).
- [14] *About Orekit*. URL: <http://orekit.org/> (elérés dátuma 2021. 10. 03.).
- [15] 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.).
- [16] 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.).
- [17] *Plotly: The front end for ML and data science models*. en. URL: <https://plotly.com/> (elérés dátuma 2021. 10. 14.).
- [18] *Graphviz*. en. URL: <https://graphviz.org/> (elérés dátuma 2021. 10. 14.).