Kvantumkommunikáción alapuló műholdas hálózat vizsgálata

Bacsárdi László, Kiss András
Nyugat-magyarországi Egyetem,
Informatikai és Gazdasági Intézet, Sopron

A kvantum alapú űrkommunikáció a nagy távolságot lefedő, biztonságos adatátvitel igényén alapszik. A kvantumos kulcsszétosztó protokollok a kvantummechanikai szabályoknak megfelelően működnek. A kulcsszétosztó folyamat alatt a kulcs lehallgatására irányuló kísérletek megzavarják a kvantumállapotokat, így a lehallgató észlelhetővé válik. Az elmúlt években több tanulmány is foglalkozott lézer alapú űrkommunikációval, de ez még mindig egy megvalósítatlan technika a Föld–űr és űr–űr kommunikációs csatornák esetében. A célunk egy olyan összetett hálózati modell fejlesztése, amely lehetővé teszi a globális méretű kvantum alapú kulcscserét. Az elmúlt évek során egy szimulációs eszközt fejlesztettünk a kommunikációs hálózat modellezésére, és elemeztünk különböző fontos jellemzőket, például a bithiba-arányt.

1. Bevezető

Napjainkban szükség van nagy távolságot lefedő, biztonságos kommunikációra és ebben a kvantum alapú műholdas kommunikáció fontos szerepet játszhat [1]. A biztonságos adatátvitel során az adatok titkosítására különböző algoritmusokat használnak. Szimmetrikus kulcsú titkosítás esetén azonos kulcsot használunk az üzenetek kódolására az adóoldalon és dekódolására a vevőoldalon. A kérdés az, hogyan történik meg a kódoláshoz szükséges kulcs cseréje a kommunikáló felek között. Ehhez több klasszikus algoritmus is rendelkezésre áll, de a probléma megközelíthető kvantumos módon is. A kvantumos kulcsszétosztó protokollok a kvantummechanikai szabályoknak megfelelően működnek. A kvantummechanika elve alapján a kulcsszétosztó folyamat alatt a kulcs lehallgatására irányuló kísérletek megzavarják a kvantumállapotokat, így a lehallgatás ténye észlelhetővé válik a kommunikáló felek számára [2].

A kvantum alapú kulcsszétosztást nem csak vezetékes hálózatban használhatjuk, hanem szabad térben is (angol szakszóval free-space quantum key distribution). Az elmúlt években több tanulmány is foglalkozott lézer alapú űrkommunikációval, de a kvantum alapú kulcsszétosztás még mindig egy megvalósítatlan technika a Föld–űr és űr–űr kommunikációs csatornák esetében.

Mint ahogy arról az Űrtan évkönyv 2010-2011 kötetben is már beszámoltunk [3], kutatásunk során egy olyan összetett hálózati

modell fejlesztésébe kezdtünk, amely lehetővé teszi a globális szintű kvantum alapú kulcscsere modellezését és vizsgálatát [4-8]. Az egyfoton forrásokon alapuló modellünkkel lehetőségünk van modellezni a nyalábszélesedésből és célzási hibából származó különböző veszteségeket. Terveztünk egy földi állomásokból és műholdpályákból felépülő hálózatot, és kifejlesztettünk egy olyan szimulációs eszközt, amellyel a kvantum alapú kulcsszétosztást vizsgálhatjuk ebben a hálózatban.

2. A műholdas kvantumkommunikáció felé

2.1. Kvantumbit

A kvantummechanikai alapú informatikát kvantuminformatikának nevezzük, napjaink rendszereit pedig a kvantumos világ nézőpontjából a klasszikus jelzővel illetjük. A klasszikus információelméletben a legkisebb egység a bit. A digitális számítógépekben a lemezek és kondenzátorok közötti feszültség reprezentálja az információ egy bitjét, például a feltöltött kondenzátor jelenti az 1-es bitértéket, a nem feltöltött kondenzátor jelenti a 0 bitértéket. A kvantuminformatikában az alapegység a kvantumbit (angolul qubit vagy qbit), amely egy kétállapotú kvantummechanikai rendszer. Ez reprezentálható például a fotonok számával (vákuum vagy egyfoton állapot), elektron spinekkel (felfelé vagy lefelé). Kommunikációban a foton polarizációját használjuk (vízszintes vagy függőleges polarizáció) [9].

Míg a klasszikus bit a bináris 0 és 1 értékekkel jellemezhető, addig a kvantumbitnek végtelen számú állapota lehet 0 és 1 szuperpozíciójában. Egy kvantumbit a következő módon definiálható:

$$|\varphi\rangle = a\,|0\rangle + b\,|1\rangle ,$$

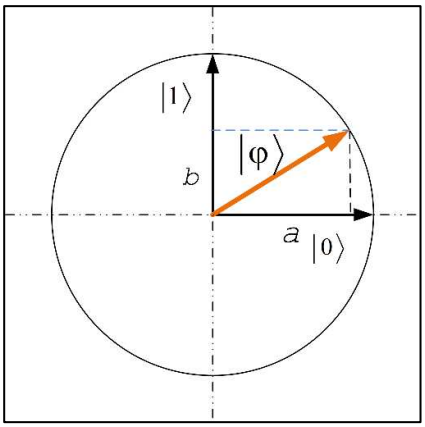
ahol a és b komplex számokat komplex valószínűségi amplitúdóknak nevezzük. $|a|^2$ és $|b|^2$ határozzák meg, mekkora valószínűséggel fogunk 0 illetve 1 értéket kapni a kvantumbitünk kiolvasása során (szakkifejezéssel akkor, ha mérést hajtunk végre a kvantumbitünkön). Az $|a|^2 + |b|^2$ egyenletnek teljesülnie kell a teljes valószínűség törvénye alapján (a kvantummechanika alapjául szolgáló ún. Hilbert-térben csak egység hosszú vektorok engedélyezettek) [10]. A kvantumbit egy illusztrációja az 1. ábrán látható.

2.2 Kvantum alapú űrkommunikáció

A kvantumbitek tere egy folytonos tér, a kvantumbiteken végzett műveletek pedig unitér transzformációk. Ezek a kvantumtranszformációk véges pontosságúak, és az ideális kvantumcsatorna megvalósításához a kvantumbitnek tökéletesen izoláltnak kellene lennie a környezetétől. Ez a gyakorlatban nehézkes, de lehetőség van a de-

koherenciából (környezettel való összefonódás) származó hibák javítására. Szabadtéri kvantumcsatorna esetében a legnagyobb problémákat a szabadtéri csatorna zaja és az optikai útból származó veszteségek jelentik [11].

Amikor földi környezet helyett űrbeli környezetről beszélünk, három különböző típusú kommunikációt különböztethetünk meg. Műhold–Föld (vagy Föld–műhold) közötti, műhold–műhold közötti, illetve két földi állomás között műholdon keresztül zajló kommunikáció. Mindezt a 2. ábrán illusztráltuk.

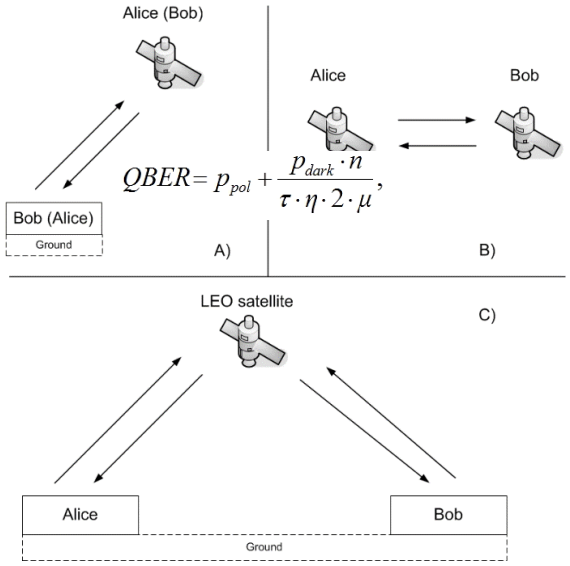


1. ábra: Egy kvantumbit vizuális reprezentációja. A narancssárga vektor jelöli az ismeretlen kvantumbitet, míg a vízszintes és függőleges vektorok az alapállapotokat reprezentálják.

2.3 Kvantum alapú kulcsszétosztás

Az 1984-ben Bennett és Brassard által publikált BB84 protokoll volt az első kvantumkriptográfiai protokoll [12]. Az eljárás során olyan véletlenszerű bitszekvenciákat hoz létre, amely csak a küldő és a fogadó fél számára ismeretek, és mindezt biztonságos és lehallgathatatlan módon teszi. Egészen pontosan, ha egy támadó megpróbál Alice és Bob közé férkőzve hozzáférni a kulcshoz, akkor arról a kommunikáló felek értesülnek. A BB84 protokollnak ez a tulajdonsága az úgynevezett másolhatatlansági elven (angolul No-Cloning Theorem) alapul. A BB84 protokoll továbbfejlesztett változata az 1992-ben megjelent B92 [13], de ezeken kívül még számos kvantum-kriptográfiai protokoll létezik, például az S09 [14] vagy a Gisin-protokoll [15].

Az első szabadtéri kvantum alapú kulcsszétosztást 1991-ben hajtották végre egy 30 cm-es optikai csatornán, amit több különböző kísérlet követett (például 205 méteren laboratóriumban illetve 75 méteren kültéri körülmények között). 1998-ban egy kutatócsoport 950 méteres szabadtéri optikai csatornán, éjszakai körülmények között hajtott végre sikeres kísérletet. Négy évvel később demonstrálták, hogy a szabadtéri kvantum kulcsszétosztás 10 km-es távolságon is megvalósítható, 2006-ban pedig egy nemzetközi kutatócsoportnak sikerült elérnie a 144 km-es távolságot [16].



2. ábra: Űrkommunikációban alkalmazható kvantumcsatorna általános esetei. A nemzetközi szakirodalom alapján a két kommunikáló felet Alice-nek és Bobnak nevezzük.

2.4 Kvantumkulcs szétosztás műholdak segítségével

Űrkommunikáció esetében számos fizikai paraméter befolyásolja a kommunikációs csatorna működését. Föld–műhold kommunikációban megkülönböztethetjük a felfelé irányuló csatornát a lefelé irányuló csatornától. A levegő jellegéből adódó fényszóródás és nyalábszélesedés miatt, lefelé irányuló csatorna esetében a szóródás és nyalábszélesedés az optikai útnak csak az utolsó szakaszában fordul elő, ami alacsonyabb veszteséget jelent, míg a felfelé irányuló csatorna esetében ez az optikai út első szakaszában fordul elő, ami a fotonok szögelmozdulásából magasabb térbeli elmozdulást tesz lehetővé az optikai csatornában, ami nagyobb veszteséget eredményezhet. Pont ezért előnyben vannak azok a megoldások, amelyek a lefelé irányuló csatornát használják. A lefelé (műhold–Föld) irányuló csatornáknak van egy másik praktikus oldaluk is: csak a földi állomást kell nagy tükrökkel és detektorokkal felszerelni, amelyekhez könnyen lehet külön hűtést biztosítani a sötét zaj csökkentéséhez. Ez egyértelműen egyszerűbb, mint műholdakra helyezni nagy és nehéz eszközöket.

Műhold–műhold kommunikáció esetében nincsenek légköri hatások, ebből adódóan a lézernyaláb terjedésének számítása is egyszerűbb a Föld–műhold változatnál.

A csatorna áteresztőképességét a transzmittanciával jellemezhetjük. Ha azonban az átvitel sikerességét szeretnénk mérni, akkor a kommunikáció bithiba-arányát határozzuk meg, egészen pontosan a

kvantum bithiba-arányt (angol szakkifejezéssel Quantum Bit Error Rate, QBER). A QBER meghatározásához számos paramétert kell ismernünk. A BB84 protokoll esetében a QBER képlete az alábbi módon írható le [17]:

$$QBER = p_{pol} + p_{op} + \frac{p_{dark} \cdot n}{\tau_{AB} \cdot \tau_{BA} \cdot \eta \cdot \mu},$$

ahol p_{pol} annak a valószínűsége, hogy a foton rossz detektorba érkezik p_{dark} a detektor által érzékelt hibás beütéseknek a valószínűsége, n a detektorok száma τ a csatorna transzmittanciája, η az átlagos fotonszám, μ a detektor kvantumhatásfoka.

BB84 esetében nem tudjuk garantálni a protokoll biztonságát, ha a QBER 11% fölötti. Ebből kiindulva meghatározhatjuk a BB84 protokoll használatával elérhető maximális csatornahosszúságot [18].

A B92 protokoll esetében a QBER számítása a következő:

$$R_{TOTAL} = \frac{R_{RAW}}{4} = \frac{1}{4} \cdot f_{pulse} \cdot \tau \cdot \eta \cdot \mu,$$

$$QBER = \frac{R_{TOTAL} \cdot p_{pol} + \frac{1}{4} \cdot f_{pulse} \cdot p_{dark} \cdot n}{R_{TOTAL}},$$

ahol f_{pulse} a lézer elsütésének frekvenciája.

Az S09 protokoll esetében a QBER-t az alábbi módon számoljuk:
ahol
p_{op} Bob kvantumműveleteinek hatásfoka,
p_{dark} a detektor által érzékelt hibás beütéseknek a valószínűsége,
τ_{AB} az Alice–Bob csatorna transzmittanciája,
τ_{BA} a Bob–Alice csatorna transzmittanciája.

A Gisin-protokoll esetében a QBER a következő:

$$QBER = \frac{R_{WRONG}}{R_{TOTAL}},$$

$$c = \cdot\tau \cdot \eta^2,$$

$$R_{TOTAL} = \frac{1}{2} \cdot f_{pulse} \cdot c \cdot (1 - p_{noise})^{n-1} + \frac{1}{2} \cdot f_{pulse} \cdot (1-c) \cdot n \cdot p_{noise} \cdot (1 - p_{noise})^{n-1}$$

$$R_{WRONG} = \frac{1}{2} \cdot f_{pulse} \cdot c \cdot p_{depol} \cdot (1 - p_{noise})^{n-1} + \frac{1}{2} \cdot f_{pulse} \cdot (1-c) \cdot (n-1) \cdot p_{noise} \cdot (1 - p_{noise})^{n-1}$$

ahol

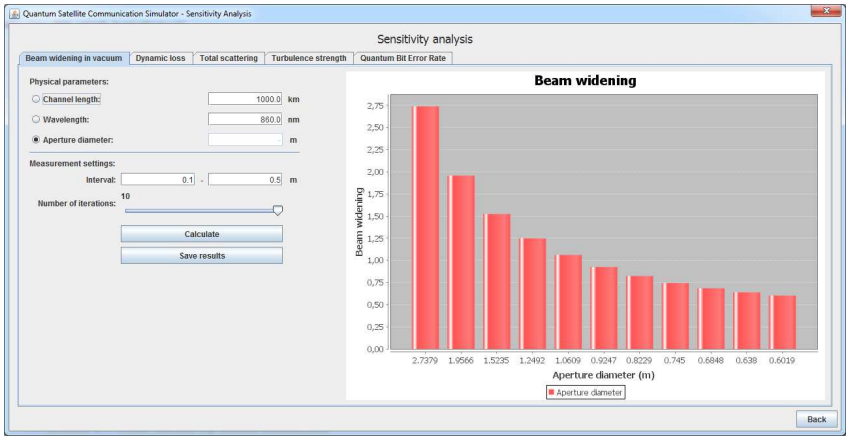
p_{depol} annak a valószínűsége, hogy a foton rossz detektorba érkezik

p_{noise} a detektor által érzékelt hibás beütéseknek a valószínűsége.

3. Műholdas szimulátorunk

Az eddigiekben láthattuk, hogy a kvantum alapú műholdas kommunikáció modellezése egy meglehetősen sokrétű és sokváltozós probléma. Azért, hogy a különböző elemzéseket minél könnyebben tudjuk elvégezni, 2011-ben egy szimulátor fejlesztésébe kezdtünk, amely támogatja a kapcsolódó hazai és nemzetközi kutatásokat. A Quantum Satellite Communication Simulator nevet viselő alkalmazásunk legfrissebb verzióját 2014 szeptemberében jelentettük meg, jelen pillanatban is ingyenesen hozzáférhető az alábbi címen: http://mcl.hu/quantum/simulator/.

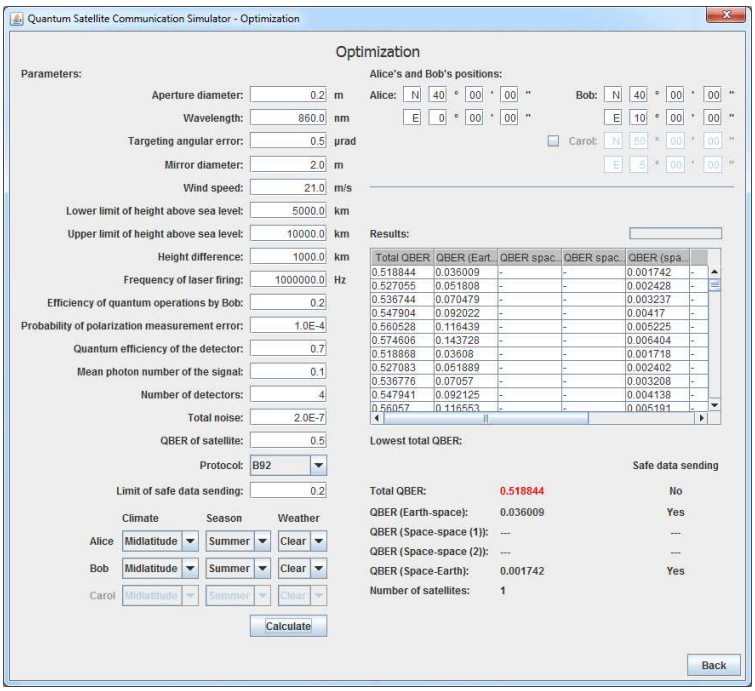
Ebben a verzióban újdonság a *Csatorna analízis szcenárió*, amelynek segítségével különböző protokollokat vizsgálhatunk úgy, hogy egy földi állomás és egy adott műholdpályán keringő műhold közötti csatornán végezzük a szimulációt.



3. ábra: A program felülete – érzékenyvizsgálat

Az alkalmazás további öt üzemmódban működik: számítás konstans paraméterekkel, számítás változó paraméterekkel, érzékenységvizsgálat, optimalizálás és idővezérelt kommunikáció.

A *Számítás konstans paraméterekkel* szcenárióban Föld–műhold, műhold–műhold és műhold–Föld csatornákra hajthatunk végre számításokat. Mindhárom csatornatípus esetében a program a különböző fizikai számítások eredményeként meghatározza az adott protokoll QBER értékét.



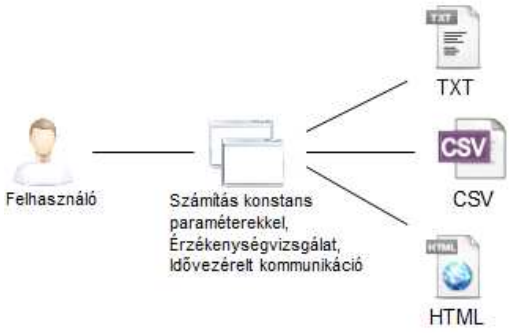
4. ábra: Az Optimalizáció szcenárió beállítási felülete

A *Számítás változó paraméterekkel* szcenárióban a program által kezelt négy kvantumprotokoll használatával hajthatunk végre szimulációkat. Minden protokoll minden bemeneti változójára beállíthatunk különböző értelmezési tartományokat. A szimuláció futása alatt a program minden változó értékét változtatja, így meghatározza az adott protokoll minden lehetséges QBER értékét.

Az *Érzékenységvizsgálat* az előzőtől eltérően még összetettebb fizikai számításokat is tud kezelni. A futás alatt egyszerre csak egy bemeneti paraméter értékét változtatja, kiszámítja az adott képlet eredményét, amelyet diagram formájában meg is jelenít a felhasználói felületen.

Az *Optimalizálás szcenárió* földi állomások közötti, műholdakon alapuló kulcsszétosztáshoz keresi az ideális műholdpozíciókat. Az

optimalizáló algoritmus figyelembe veszi, hogy minél kevesebb műholdat szeretnénk felhasználni, úgy, hogy a teljes hálózatra alkalmazott protokoll QBER értéke is a lehető legalacsonyabb legyen. Számítási korlátok miatt a szcenárió legfeljebb három földi állomásból és legfeljebb három műholdból felépülő hálózatra alkalmazható.



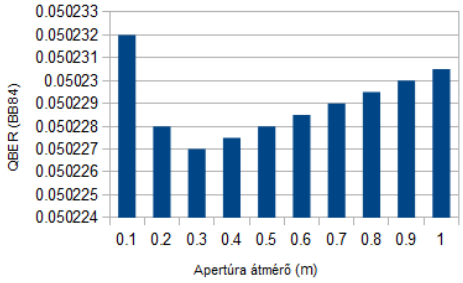
5. ábra: Szimulációs eredmények mentése és tárolása.

Az *Idővezérelt kommunikáció* szcenárió földi állomások és előre definiált műholdpályák használatával hajt végre egy valós életszerű szimulációt. A földi állomásokban véletlenszerűen adatküldési igények generálódnak, és ha lehetséges a küldés a fogadó földi állomás felé (van szabad rálátás), akkor megtörténik a továbbítás. Minden végrehajtott adatküldésre a program kiszámítja a QBER értéket és a várakozási időt. Ezekből az adatokból egy statisztikai áttekintés látható a program felületén.

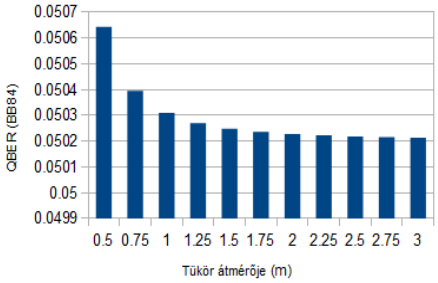
6. ábra: Külső osztálykönyvtárak és források használata

Az alkalmazás eredménykezelésének módja az 5. ábrán látható. Minden szcenárió esetében megjelennek a szimulációs eredmények a felhasználói felületen, az eredmény pedig elmenthető TXT, CSV és HTML formátumokban.

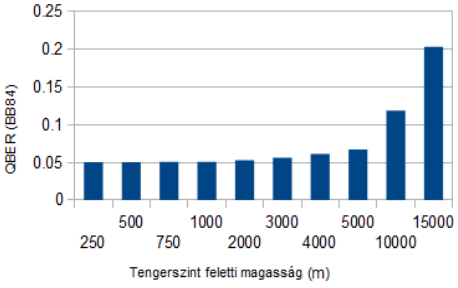
Néhány esetben a program külső forrásokat és osztálykönyvtárakat használ, a 6. ábrán szemléltetett módon. Minden szcenárióban, amelyekben Föld–műhold vagy műhold–Föld csatornákra történik transzmittancia számítás, a program figyelembe veszi a Föld légkörének különböző rétegeire értelmezett abszorpciós és szórási értékeket. A felhasználói felületen a diagramok a JFreeChart osztálykönyvtár segítségével jelennek meg. A Föld forgását és a műholdpályák animációját Java OpenGL (JOGL) osztálykönyvtár segítségével jeleníti meg a program.



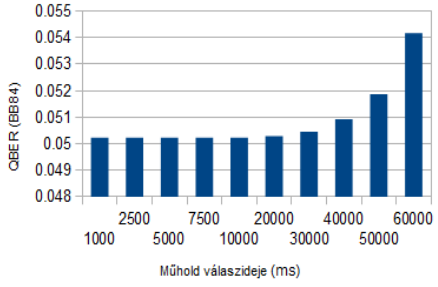
7. ábra: Különböző apertúra átmérőkre értelmezett QBER értékek



8. ábra: Különböző tükörátmérőkre értelmezett QBER értékek



9. ábra: Különböző tengerszint feletti magasságokra kiszámított QBER értékek.



10. ábra: BB84 protokollra értelmezett QBER értékek különböző műhold válaszidők eseteiben

4. Eredmények

A 7. ábrán különböző apertúra átmérők függvényében ábrázoltuk a QBER értékeket. Eredményeink alapján a legalacsonyabb QBER érték 0,3 méteres apertúra átmérővel érhető el. A 8. ábrán láthatók a BB84 protokoll QBER értékei, különböző tükörátmérők függvényében. A 9. ábrán láthatók a különböző tengerszint feletti magasságokra kiszámított QBER értékek. A nagyobb műholdpálya magasság nagyobb távolságot jelent a küldő és a fogadó között, és a nagyobb távolság esetében nagyobb QBER értéket kapunk. A 10. ábrán láthatók a különböző műhold válaszidőkre számított QBER értékek. Ebben az esetben a válaszidő akkor kezdődik, amikor az üzenet megérkezik a műholdra és akkor ér véget, amikor a műhold továbbküldi a fogadó felé. A hosszabb válaszidő nagyobb csatornahosszt és nagyobb zenitszöget eredményez, elsődlegesen ezek okozzák a megnövekedett QBER értékeket.

5. Összefoglalás

Egy olyan szimulációs eszközt fejlesztettünk, amely alkalmas a kvantum alapú műholdas kommunikációs hálózat modellezésére. A hálózat különböző pályán keringő műholdak segítségével különböző földi állomások közötti kvantum-kulcsszétosztást tesz lehetővé, miközben a minimális átviteli hibára törekszik. Szimulátorunk segítségével elkezdtük elemezni a kvantum alapú műholdas hálózat teljesítményjellemzőit. A fentiekben ismertetett eredményeinket 2014 őszén a Nemzetközi Világűrkongresszuson is bemutattuk [19].

Bacsárdi László kutatása a TÁMOP 4.2.4.A/2-11-1-2012-0001 Nemzeti Kiválóság Program című kiemelt projekt keretében zajlott. A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

Irodalomjegyzék:

[1] Bacsardi L. (2013): Efficient Quantum Based Space Communications, LAP Lambert Academic Publishing
[2] Imre S. (2014): Quantum Computing and Communications – Introduction and Challenges. Computers & Electrical Engineering, 40(1), 134
[3] Galambos M., Kiss A., Bacsárdi L. (2012): Kvantum alapú kommunikáció műholdas csatornában, Űrtan évkönyv 2010-2011, 58
[4] Galambos M., Bacsardi L., Kiss A., Imre S. (2011): Analyzing Quantum Based Protocols in LEO and GEO Satellite Communication, In: Proc. 62th International Astronautical Congress, Cape Town, South Africa
[5] Bacsardi L., Imre S. (2012): Supporting Space Communications

with Quantum Communications Links, Global Space Exploration Conference, Washington D.C., USA
[6] Bacsardi L., Galambos M., Imre S., Kiss A. (2012): Quantum Key Distribution over Space-Space Laser Communication Links, In: Proc. AIAA SPACE 2012 Conference & Exposition, Pasadena, USA
[7] Galambos M., Bacsardi L., Imre S. (2013): Comparison of BB84 and S09 Quantum Key Distribution Protocols in Space-Space Links, In: Proc. 31st AIAA International Communications Satellite Systems Conference, Florence, Italy
[8] Kiss A., Bacsardi L. (2014): Analyzing a Satellite-based Quantum Key Distribution Network, In: Proc. Global Space Application Conference, Paris, France
[9] Hanzo L., Haas H., Imre S., O'Brien D., Rupp M., Gyongyosi L. (2012): Wireless Myths, Realities, and Futures: From 3G/4G to Optical and Quantum Wireless, Proceedings of the IEEE, 100, 1853
[10] Imre S., Ferenc B. (2005): Quantum Computing and Communications: An Engineering Approach, Wiley, New York
[11] Bacsardi L. (2007): Satellite Communication Over Quantum Channel. Acta Astronautica, 61(1-6), 151
[12] Bennett C.H., Brassard G. (1984): Quantum cryptography: Public key distribution and coin tossing, In: Proc. IEEE International Conference on Computers, Systems and Signal Processing. Bangalore, India
[13] Bennett C.H. (1992): Quantum Cryptography Using Any Two Nonorthogonal States, Physical Review Letters, 68, 3121
[14] Serna E.H. (2009): Quantum Key Distribution Protocol with Private-Public Key, [online] arXiv:0908.2146v3
[15] Branciard C., Gisin N., Kraus B., Scarani V. (2005): Security of two quantum cryptography protocols using the same four qubit states. Physical Review A, 72, 032301
[16] Bacsardi L. (2013): On the Way to Quantum-Based Satellite Communication, IEEE Communications Magazine, 51(8), 50
[17] Galambos M., Bacsardi L., Imre S. (2010): Modeling and Analyzing the Quantum Based Earth-Satellite and Satellite-Satellite Communications, In: Proc. 61th International Astronautical Congress, Prague, Czech Republic
[18] Gisin N., Ribordy G., Tittel W., Zbinden H. (2001): Quantum cryptography. [online] arXiv:0101.098v2
[19] Bacsardi L., Kiss A. (2014): Overview of a Space Based Quantum Key Distribution Network, In: Proc. 65th International Astronautical Congress, Toronto, Canada