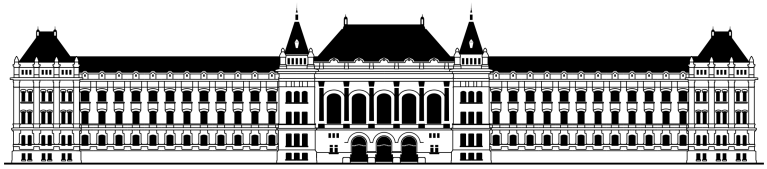


Önszerveződő hálózatok kommunikációjának vizsgálata kvantum eszközökkel

Készítette:

Bányai Dóra (HIT)

bd778@hszk.bme.hu

Konzulensek:

Bacsárdi László (HIT)

bacsardi@hit.bme.hu

Dr. Imre Sándor (HIT)

imre@hit.bme.hu

2011. október

Tartalomjegyzék

1. Bevezetés

Napjaink egyik legérdekesebb területe a kvantum-infokommunikáció. Az infokommunikáció egy olyan területe, mely alapjaiban rengeti meg az általunk ismert világot. A kvantum-infokommunikáció olyan lehetőségeket rejt magában, ami még jobban felgyorsíthatja a már amúgy is rohanó világunkat. Legyen szó az információáramlás sebességének növeléséről, vagy a rendszereink biztonságáról, akár az űrkutatásról, vagy a bonyolult számítást igénylő feladatok megoldásáról, a kvantuminformatika hatalmas előrelépést jelent a különböző területen dolgozó kutatóknak és a hétköznapi életben egyaránt.

A dolgozat egy klasszikus alapokon működő önszerveződő rendszer elemeinek kommunikációját ülteti át kvantum eljárásokra. A CASCADAS rendszer alapja az Autonóm Kommunikációs Egység (ACE, Autonomic Communication Element), melyek a begyűjtött információ alapján képesek külső beavatkozás nélkül alkalmazkodni, és további cselekvéseiket ennek megfelelően alakítani [1]. A CASCADAS project célja egy olyan keretrendszer kialakítása volt, mely autonóm komponens-alapú, és segítségével olyan innovatív szolgáltatások készíthetők, melyek kiszámíthatatlan környezetben is dinamikusan tudnak alkalmazkodni a kialakult helyzethez. Az ACE-k kvantumosított változata a QACE (Quantum ACE) a klasszikus rendszer kommunikációs egységeinek tulajdonságait javítja, gyorsabb és komplexebb számításokat téve lehetővé a kvantuminformatikai Grover algoritmus segítségével [2].

Munkámban egy lépéssel tovább menve azt vizsgálom meg, hogy az autonóm kommunikációs egységek által feldolgozott információ hogyan továbbítható egy önszerveződő hálózaton kvantum alapú algoritmusok segítségével. Dolgozatomban megmutatom, hogyan lehet felhasználni erre az információtovábbításra a teleportációt és a szupersűrűségű tömörítést. A két eljárás közötti egyik fontos különbség, hogy a teleportációhoz szükség van klasszikus adattovábbításra, míg a szupersűrűségű tömörítésnél tisztán kvantum kommunikáció történik. Mindkettőnek jelentős szerepe lehet a hálózatban, így a munkámban bemutatom, hogy melyik milyen peremfeltételek mellett növeli a hálózat hatékonyságát. Dolgozatomban kitérek arra is, hogy az algoritmusok nagy adatmennyiség mellett is megvalósíthatóak maradjanak.

A dolgozat felépítése a következő: a második fejezetben bemutatom a kvantum alapú informatikát, valamint leírom a szakirodalom jelenleg elfogadott azon algoritmusait, melyek a dolgozat második felében összeállított rendszer megértéséhez elengedhetetlenek.
A harmadik fejezetben röviden ismertetem a CASCADAS rendszert, valamint a rendszer alapját képező ACE-k kvantumosított változatával előrevetítem a rendszer kommunikációjának kvantum alapokra való áttérését.
A dolgozat második felében felépítek egy olyan rendszer, mely segítségével a QACE-k kommunikációjukban is kvantum eszközöket és eljárásokat használhatnak. Így a negyedik fejezetben a topológia bemutatása után a két fő kommunikációs algoritmust, a teleportációt

és a szupersűrűségű tömörítést elemzem, valamint a teleportáció eljárását kiegészítem úgy, hogy az komplex rendszerekre is alkalmazható legyen. A kommunikáció gerincét alkotó algoritmusok köré ezután felépítem a különböző kapcsolati szintek szerinti rétegeket, melyek már csak elvétve hasonlítanak az TCP/IP modelljére [3]. Kitérek a fizikai szintű eljárásokra, valamint a logikai kapcsolatok felépítésére, karbantartására, és bontásra is.
Az ötödik fejezetben az ismertetett rendszer teljesítményét és hatásfokát vizsgálom az átvitt bitek, qbitek, felhasznált Bell-párok és az előforduló hibázás alapján, majd a dolgozatot végszóval zárom.

2. A kvantum informatikáról általánosan

A klasszikus informatikában az elemi információs egység a bit, melynek értéke 0 vagy 1 (klasszikus állapot) lehet. A kvantuminformatika világában qbiteket használunk, melyeknek komplex együtthatóik vannak, és sűrűségmátrixszal vagy többdimenziós vektorral írhatók le. Igaz, még nem léteznek sok qbittel operáló kvantum számítógépek, és az infokommunikációs területen sem lehet még iparszerűen alkalmazni a kvantummechanikán alapuló eszközöket, bizonyos feltételezésekkel már most tudunk olyan algoritmusokat készíteni, melyek a hardver kifejlesztése után alkalmazhatóak. Az infokommunikáció területén főleg olyan kvantum algoritmusok születnek, melyek valamilyen klasszikus esetet dolgoznak át, vagy egészítenek ki. (Például rendezetlen adatbázisban való keresés, vagy kulcsszétosztás.) Az elemi információs egység, a qbit vektoros alakja: $|\varphi\rangle = a|0\rangle + b|1\rangle$, ahol a és b komplex együtthatók abszolútértékének négyzete adja meg, hogy mekkora valószínűséggel van a qbit 0 vagy 1 klasszikus állapotban, ezért a nevük valószínűségi amplitúdó, melyek teljesítik az $|a|^2 + |b|^2 = 1$ feltételt. Akkor tiszta egy qbit, ha megadható egy vektorával, ellenkező esetben sűrűségmátrixával írjuk fel. Az ezen a területen dolgozó informatikusoknak rengeteg új lehetősége van gyorsabb, biztonságosabb, megbízhatóbb - egyszóval jobb rendszereket tervezni, mely képes felvenni a versenyt az egyre növekvő igényekkel. Természetesen a megvalósíthatóság dátuma attól is függ, hogy a fizikusoknak mikor sikerül kifejleszteni az első működőképes kvantumszámítógépet. Ugyan a teljes valójában működő kvantumszámítógép még a távoli jövő eszköze, de kvantum algoritmusokat enélkül is tudunk készíteni, sőt, már most léteznek kereskedelmi forgalomban kapható eszközök [4].

2.1. A kvantummechanikai posztulátumok:

A kvantumrendszerek alapját a kvantummechanikai posztulátumok adják. A négy alapelv körbehatárolja a kvantum világot, és segítségükkel bármilyen történés leírható benne. A posztulátumoknak köszönhetően nem kell megvárni, amíg a fizikusoknak sikerül létrehozniuk az első kvantum számítógépet, mérnöki megközelítésben már lehetőségünk van különféle algoritmusokat kidolgozni [5].

I. Posztulátum

Bármilyen zárt fizikai rendszer állapota leírható egy állapotvektorral $|v\rangle$, mely egységnyi hosszú és összetevői a komplex Hilbert térhez tartoznak.
Például a $|\varphi\rangle = a|0\rangle + b|1\rangle$ is egy ilyen állapotvektor, ahol (két dimenziós Hilbert térben) a bázisvektorok $|0\rangle = [1, 0]^T$ és $|1\rangle = [0, 1]^T$ ortogonálisak egymásra.

II. Posztulátum

Bármilyen változás egy zárt fizikai rendszerben leírható unitér transzformációk segítségével, csupán a kezdő és befejező időpontok figyelembevételével.

$$v'(t_2) = U(t_1, t_2)v(t_2) \text{ és } v' \in V$$

III. Posztulátum

Bármely kvantum mérés leírható mérési operátorok segítségével $\{M_m\}$, ahol m a lehetséges kimenetet jelöli. Azt, hogy mérési eredményként m-et kapjunk, ha a rendszer $|v\rangle$ állapotban van, a következőképpen tudjuk felírni:

$$P\left(m\middle||v\rangle\right) = |v\rangle^{+} M_m^{+} M_m |v\rangle$$

Mérés után a rendszer állapota:

$$|v\rangle' = \frac{M_m|v\rangle}{\sqrt{|v\rangle^{+} M_m^{+} M_m |v\rangle}}$$

Ahol a mérési operátorok teljesítik a teljességi feltételt:

$$\sum M_m^{+} M_m \equiv I$$

Ugyanis a klasszikus valószínűségszámítási elmélet alapján

$$\sum_m P\left(m\middle||v\rangle\right) = \sum_m |v\rangle^{+} M_m^{+} M_m |v\rangle \equiv 1$$

A mérések rendkívül fontos részét képezik a kvantum és klasszikus világ közötti átjárásnak, ugyanis ezzel az operációval tudjuk a kvantum bitjeinket klasszikus állapotba billenteni, és a továbbiakban klasszikusan felhasználni. Sajnos a mérés nem unitér transzformáció, így a bebillentett klasszikus állapotból nem tudjuk visszanyerni az eredeti kvantum bitet.

IV Posztulátum

Egy összetett fizikai rendszer W meghatározható a komponenseinek tenzor szorzatával $W = Y \otimes V$, valamint az állapotvektorai felírhatóak a komponens terek állapotvektorainak tenzor szorzatával.

2.2. Építsünk logikai áramkört!

2.2.1. Szuperpozíció és a Bloch-gömb

Ahogyan azt már láttuk, a $|\varphi\rangle$ állapotvektor bázisvektorai ortonormált párokat alkotnak, melyek jól reprezentálhatóak egy foton vízszintes illetve horizontális polarizációjaként. Az *a*

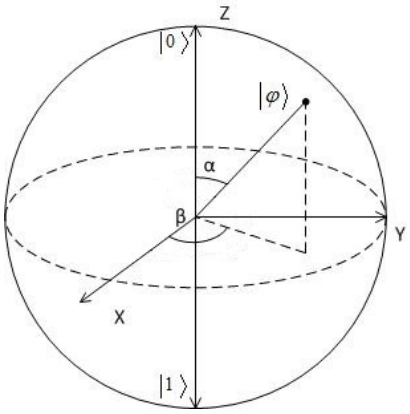
és b valószínűségi amplitúdók adják meg ezen bázisok lineárisan súlyozott szuperpozícióját. Egy qbit geometriai reprezentációjához az általános alakot egy kézenfekvőbb alakra kell átírni [5]:

$$|\varphi\rangle = e^{j\gamma}\left[cos\left(\frac{\alpha}{2}\right)|0\rangle + e^{j\beta}\, sin\left(\frac{\alpha}{2}\right)|1\rangle\right],$$

ahol α, β, γ ∈ ℝ. Az $e^{j\gamma}$ a globális fázis, s mivel az abszolút értéke 1, ezért semmilyen hatással nincs a mérési eredményekre, így sokszor elhagyják a kvantum rendszerek analizálásánál. A globális fázis elhagyásával a fenti forma már ábrázolható egy háromdimenziós Descartes koordinátarendszerben, melyet Felix Bloch után Bloch-gömbnek neveztek el. A polár koordináták átalakítása után a következő Descartes koordinátás leírást kapjuk:

$$|\varphi\rangle = [\mathrm{x,y,z}]^{\mathrm{T}} = [cos(\beta)sin(\alpha), sin(\beta)sin(\alpha), cos(\alpha)]^{\mathrm{T}}.$$

Ennek az eredmények a segítségével felrajzolt Bloch-gömb az 1. ábrán látható.



1. ábra Bloch-gömb - egy qbit térbeli ábrázolása

2.2.2. Kvantum regiszter

A klasszikus rendszerben n bit tárolásához egy n bit nagyságú regiszterre van szükségünk. Ha feltöltöttük a regisztert az n bittel, akkor a kinyerhető információ csak ez az n bitnyi *n-es* lehet. Ha egy másik információhordozó *n-es*t szeretnénk használni, akkor vagy egy új regisztert kell alkalmazni, vagy felül kell írni a régi regisztert, így viszont a törléssel elveszítjük az előző n bit által hordozott információt. Ha 2^n darab n hosszúságú bitet szeretnénk tárolni, akkor 2^n darab, illetve 1 darab 2^n nagyságú regiszterre lenne szükségünk, amely egy kellően nagy n megválasztása esetén már igen költséges lehet.

Ugyanakkor 2^n darab klasszikus *n-es* tárolásához kvantum esetben elég csupán 1 darab n qbit nagyságú kvantum regiszter, hiszen minden qbit helyén egyszerre állhat 0 és 1 is különböző valószínűségi amplitúdókkal. Ha ismerjük a tárolt qbitek állapotát, akkor a negyedik posztulátum értelmében a kvantum regiszter állapotát felírhatjuk a qbitek tenzor szorzataként. $|\varphi\rangle = |qbit_{N-1}\rangle \otimes |qbit_{N-2}\rangle \otimes \ldots \otimes |qbit_0\rangle$. Általános esetben a valószínűségi

amplitúdókat is figyelembe véve a kvantum regiszter állapota a következőképpen írhatjuk fel:

$$|\varphi\rangle = \sum_{i=0}^{2^n-1} \varphi_i |i\rangle$$

ahol φ_i a valószínűségi amplitúdó, és $|i\rangle$ az i. qbithez tartozó bázis vektor.

2.2.3. Kvantum kapuk

Mint klasszikus esetben, itt is szükségünk van univerzális építőelemekre, logikai kapukra, hogy különféle rendszereket tudjunk építeni. A második posztulátum értelmében mivel a változásokat unitér transzformációk segítségével tudjuk leírni, ezért ezeket nevezhetjük kvantum kapuknak is. Az egy qbiten végzett unitér transzformáció nem más, mint az elemi kvantum kapu: $|\varphi\rangle = U|\psi\rangle$.

Az alábbiakban nézzünk néhány fontosabb elemi kvantum kaput, melyben a kiindulási állapot mindig egy 1 qbites állapot: $|\psi\rangle = a|0\rangle + b|1\rangle$.

2.2.3.1. Pauli-X - bit felcserélő kapu

Az unitér transzformációkat mátrixaikkal adjuk meg. Az X kapu mátrixa:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Az X kapu funkciója, hogy a $|\psi\rangle$ kiindulási állapot amplitúdóit felcseréli, s a végeredmény $|\varphi\rangle = b|0\rangle + a|1\rangle$ lesz.

2.2.3.2. Pauli-Z - fázis cserélő kapu

A Z kapu a qbit összetevőinek fázisát cseréli meg, így az eredmény $|\varphi\rangle = a|0\rangle - b|1\rangle$.

A Z kapu mátrixa:

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

2.2.3.3. Pauli-Y

Az Y kapu az összetevők amplitúdójának *j*-szeresét cseréli fel.

$$Y = \begin{bmatrix} 0 & -j \\ j & 0 \end{bmatrix}$$

A kapott állapot: $|\varphi\rangle = -jb|0\rangle + ja|1\rangle$.

2.2.3.4. Fázis kapu

A P fázis forgató kapu, ahogyan a nevében is szerepel a qbit fázisát forgatja el a megadott α szöggel.

$$P(\alpha)|\psi\rangle = \begin{bmatrix} 1 & 0 \\ 0 & e^{j\alpha} \end{bmatrix}$$

A kimeneti állapot: $|\varphi\rangle = a|0\rangle + e^{j\alpha}b|1\rangle$.

2.2.3.5. Hadamard kapu

Ezt a kvantum kaput lehet a legkönnyebben előállítani, már egy féligáteresztő tükör is elég hozzá. Feladata az amplitúdók megegyező arányban való szétosztása. A kapu megadható a mátrixával, amely a következő:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

A kapott kimenet: $\mathrm{H}|\varphi\rangle = \frac{\mathrm{a}+\mathrm{b}}{\sqrt{2}}|0\rangle + \frac{\mathrm{a}-\mathrm{b}}{\sqrt{2}}\mathrm{b}|1\rangle$.

A Hadamard kapu bármilyen beadott klasszikus állapotból egyenlő amplitúdójú kvantum állapotokat készít úgy, hogy egyedül az előjelek különböznek.
A kapott végeredmény klasszikus állapotú bemenetek esetén:

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

A Pauli és Hadamard kapuk között speciális kapcsolat van. A megfelelő transzformációk egymásutánja egy másik kaput, vagy annak egy módosított változatát adja.

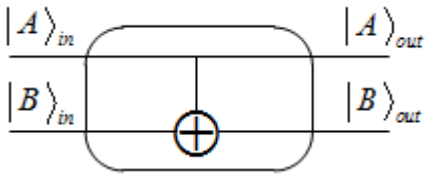
$$HXH = Z,\ HYH = -Y \text{ és } HZH = X$$

2.2.3.6. Controlled-NOT kapu

A Hadamard kapu mellet az egyik legérdekesebb építőelem a CNOT kapu (vezérelt NOT kapu). Segítségével összefonódásokat hozhatunk létre két qbit között, illetve további qbiteket adhatunk a már létező összefonódásunkhoz. A 2. ábra a CNOT kapu logikai felépítését mutatja.

A kapu mátrixa:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



2. ábra CNOT kapu

Az $|A\rangle_{in}$ klasszikus bemeneti állapot esetén vezérlő szerepet játszik, mely 0 érték esetén átengedi a $|B\rangle_{in}$ bemenetet, 1 esetén pedig a negáltját. Innen az elnevezés: vezérelt NOT. Például: $|B\rangle_{out} = |A\rangle_{in} \oplus |B\rangle_{in}$, vagyis $0 \oplus 1 = 1$.

Ha a kontroll bemenetre egy tetszőleges kvantum bitet $|\varphi\rangle = a|0\rangle + b|1\rangle$ adunk a másikra pedig egy tetszőleges klasszikus állapotot (például: $|0\rangle$), akkor a kimeneten egy összefonódott állapotban lévő párt fogunk kapni. A közös bemeneti állapot: $|A\rangle_{in} \oplus |B\rangle_{in} =$ $a|00\rangle + b|10\rangle$, a kimeneti közös állapot $a|0,0 \oplus 0\rangle + b|1,1 \oplus 0\rangle = a|00\rangle + b|11\rangle$, amely valóban egy összefonódott állapot.

2.3. Az összefonódás

A kvantummechanika egyik legérdekesebb jelensége az összefonódás. Két vagy több részecske úgy hordozza az információt, hogy ha ebből az egyiknek megváltozik az állapota, akkor az a változás a párjában (párjaiban) is azonnal észlelhető. A legáltalánosabb és legtisztább összefonódott párokat Bell-pároknak vagy EPR-pároknak hívjuk, fontos tulajdonságuk, hogy a normálvektoraik ortogonális párokat alkotnak. Egy tetszőleges összefonódás előállítható egy CNOT kapu segítségével.

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

1. táblázat Bell állapotok

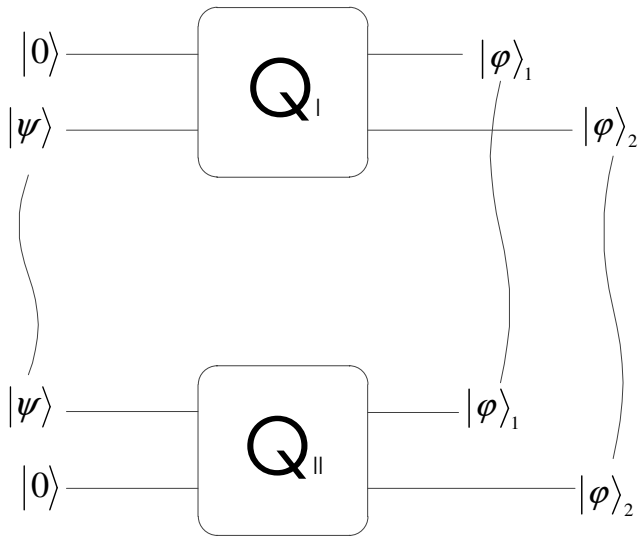
A kérdés az, hogy ezt az állapotot hogyan, mennyi ideig, milyen távolságban lehet fenntartani. Továbbá, ha már van ilyen állapotunk, akkor hogyan szedjük szét őket, ha ez egyáltalán megtehető? A nagy távolságú kommunikációhoz legjobban a fotont lehet felhasználni, ám ennek is megvannak a maga korlátai. Egy fotont jelenleg maximum 100km-

es távolságra lehet eljuttatni egy optikai kábelcsatornán, a környezeti hatások és dekoherencia miatt. Ezt a távolságot ún. kvantum ismétlőkkel lehet növelni [6].

2.4. No-cloning elmélet

A klasszikus informatikában megszokott, hogy könnyen tudunk biteket másolni. A kvantuminformatikában sajnos nem így van, a kvantummechanika elég szoros megkötéseket tesz a bitek másolására, azaz a klónozásra. Tetszőleges kvantum állapotot nem lehet másolni, de előre ismert ortogonális állapotot már tudunk sokszorosítani. Ez a megállapítás a kvantum kriptográfiánál lesz nagyon fontos, ugyanis ezen tulajdonság miatt tudjuk biztosan megmondani, ha valaki a kvantum kulcsszétosztás közben lehallgatta a kulcscserét. Az összefonódott párokat is tudjuk klónozni, ha előre ismertek és ortogonálisak (ilyen például a Bell állapotú párok), legalábbis amíg a lokalitás feltételének eleget teszünk (vagyis a pár két része egy helyen van). Mint látni fogjuk, a kommunikációs algoritmusokban ismert Bell állapotú qbiteket használunk, viszont ezek egymástól távollévő felek birtokában vannak, így sajnos nem tudjuk őket másolni. Ezért a Bell-párok sokszorosítására a desztillációs protokollt fogom felhasználni, mely egy nagyobb (több qbitből álló) összefonódásból készít, több két qbitből álló összefonódást.

A kutatóknak már sikerült azt megmutatni, hogy egymástól távollévő összefonódott qbiteket le tudnak lokális transzformációkkal másolni úgy, hogy a bemenetre lokálisan adott egy-egy qbit a másik oldalon lévő bemeneti Bell állapotú qbittel lesz összefonódva, míg az eredeti összefonódás megszűnik [7]. Végeredményül két pár összefonódást kapunk. Az eljárás hátránya, hogy a kezdeti Bell-pár amplitúdóját nem tartja meg, így állapotot nem, csak az összefonódást sikerült másolni. (3. ábra)



3. ábra Összefonódás másolása lokális transzformációkkal

2.5. Kvantum párhuzamosság

Az összefonódás mellett a kvantuminformatika legjelentősebb tulajdonsága a párhuzamos számítások lehetősége. Képzeljük el, hogy valamilyen kérdés megválaszolásához klasszikus esetben csak exponenciális lépésben tudunk eljutni, a kvantum világban azonban ezeket a problémákat egy lépésből is meg lehet oldani. Egy ilyen kvantum eljárás például a Deutsch-Józsa algoritmus [5].
A kvantum párhuzamosság tulajdonságát használja ki a Grover algoritmus is. Ahhoz, hogy egy rendezetlen adatbázisban tudjunk keresni, a Grover algoritmus először az összes potenciális válasz amplitúdóját egyenlő értékre hozza a kvantum-párhuzamosítással. Majd olyan transzformációkat hajt végre, mellyel a keresett elem amplitúdóját közel 1 értékre erősíti, a többi elemét pedig közel 0-ra. Mivel általában nem lehet a kívánt eredményt az eljárás egyszeri lefuttatásával megkapni, ezért lehetséges, hogy a lépéseket egymás után többször is végre kell hajtani, de a kereséshez felhasznált idő még így is töredéke a klasszikus megoldásének. Bár a Grover algoritmust adatbázis kereső algoritmusnak nevezik, más felhasználási területei is vannak, mint a középérték és medián keresés, vagy az ütközési probléma megoldása.

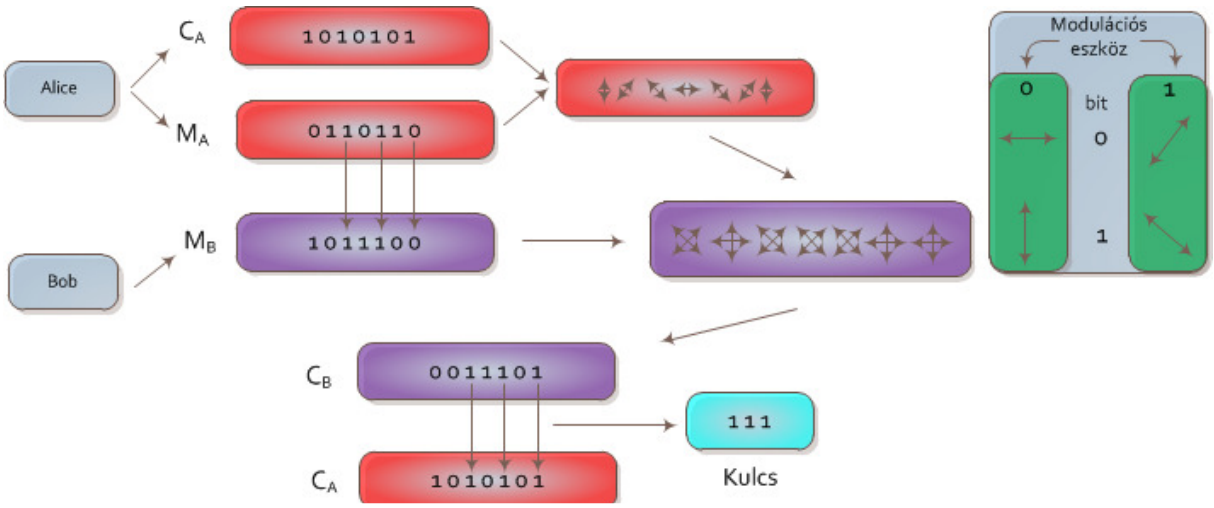
2.6. Kvantum kulcsszétosztás

Az qbitekben megjelenő változások, és reprodukálhatatlanság miatt a kvantum rendszer abszolút biztonságos lehet a lehallgatással és manipulációval szemben. Mivel a kvantum algoritmusok a másodperc töredéke alatt lefutnak, ezért a klasszikus rendszerek nagy veszélynek vannak kitéve. A klasszikus világban az egyik leggyakrabban használt titkosítási eljárás az RSA, mely egy nyílt kulcsú, aszimmetrikus titkosító algoritmus [8]. A kódoláshoz és a dekódoláshoz két kulcsra van szükség, egy privát kulcsra, mely csak az egyik fél által ismert, és egy publikus mindenki által hozzáférhető kulcsra. A publikus kulcs a kódoláshoz, míg a privát kulcs a dekódoláshoz szükséges. Az RSA algoritmus azért olyan elterjedt, mert bár (nagyon hosszú) idővel feltörhető lenne, de ezen intervallum alatt rengetegszer cserélődnek a kulcsok, és klasszikus eszközökkel szinte lehetetlen feltörni, azaz megtalálni a privát kulcsot. Tegyük fel, hogy Eve-nek (Eve az általában rosszindulatú szereplő az infokommunikációs eljárások szemléltetésénél) sikerül először kvantum számítógépet készítenie, a Deutsch-Józsa és Grover algoritmussal egy akár rendezetlen adatbázisban is képesek pillanatok alatt megtalálni a dekódoláshoz szükséges privát kulcsot. Ezáltal a másodperc töredéke alatt válnak sebezhetővé a nemzetbiztonsági és a rendkívül kényes információkat tartalmazó adatbázisok. Mielőtt Eve megtalálná a kulcsot, a támadásnak kitett klasszikus rendszert kell a kvantum infokommunikáció előnyeivel felvértezni. Az egyik legbiztonságosabb kommunikációs védekezés a szimmetrikus kulcsú titkosítás, mely azon alapszik, hogy a két kommunikáló fél – Alice és Bob – ugyanazt a kulcsot használja a kódoláshoz és a dekódoláshoz is [9]. A probléma ott kezdődik, amikor ezt a kulcsot meg kell osztaniuk egymás között. Ha ugyanazt a csatornát használják, melyen a kommunikációt

folytatni szeretnék, akkor nagy az esélye annak, hogy Eve is elkapja ezt a kulcsot, és innentől kezdve visszafejthető a titkosítás. A legbiztonságosabb az lenne, ha Alice és Bob egymás fülébe súgnák a kulcsot, amelyet távollévő felek esetén elég nehéz lenne kivitelezni. Viszont a kvantum infokommunikáció olyan lehetőséget biztosít a szimmetrikus kulcsú titkosításra, mely biztos lábakon áll a külső támadókkal szemben. Klasszikus esetben Eve-nek elég lenne eljátszani a fogadó felet – Bob-ot – a kulcsszétosztási folyamatban, majd továbbítani a kapott biteket az igazi Bob felé. Ám kvantum esetben Eve-nek nincs lehetősége érintetlenül, eredeti formájukat megőrizve továbbítani a qbiteket, Alice és Bob tudni fogja, hogy valaki megpróbálta őket lehallgatni.

Az alap kvantum kulcsszétosztás algoritmusa a BB84 [5]. A folyamat lehetséges két vagy három fél között is. Utóbbi esetben az egyik fél csak a házigazdát játssza, amíg a másik két fél között kialakul a titkos kulcs. A titkosítás azzal kezdődik, hogy a házigazda (vagy kétszereplős esetben Alice) kitalál egy random klasszikus kódsorozatot, amelyen modulációt fog végrehajtani egy másik random, azonos hosszúságú kódsorozat alapján, mely a 0-áinak és 1-einek megfelelően alkalmaz az első sorozatnak megfelelő fotonjain különböző fázisú polarizációt. Mivel a nem ortogonális állapotok nem másolhatóak, ezért két olyan polarizációs eszközt alkalmazunk, amelyben a 0-nak megfelelő polarizáció vízszintes, míg az 1-nek megfelelő polarizáció a függőleges lesz. A másik eszközben a 0-nak megfelelő polarizáció $+\frac{\pi}{4}$, míg az 1-nek megfelelő a $-\frac{\pi}{4}$. Miután kialakult a polarizált sorozat, a házigazda átküldi a qbiteket a két szereplőnek (vagy Alice Bob-nak), akik saját random sorozat alapján alkalmaznak vertikális-horizontális, vagy $\pm\frac{\pi}{4}$ polarizációs szűrőt. A kapott bitsorozat elemei ott biztosan megegyeznek, ahol a modulációnak megfelelő szűrőt alkalmaztak, rossz szűrő esetén 50% valószínűséggel mérhető be a jó bit. Ezután Alice és Bob (a házigazda kihagyásával) egy klasszikus csatornán nyilvánossá teszik a modulációs kódsorozatukat, és ahol azok bitjei megegyeznek, a demodulált sorozatban az azokon a helyeken álló bitekből összeálló új sorozat adja szimmetrikus kulcsot. A kulcsból meghatározott biteket elküldenek egymásnak, és ha azok egyeznek, akkor a kulcscsere lehallgatás nélkül megtörtént.

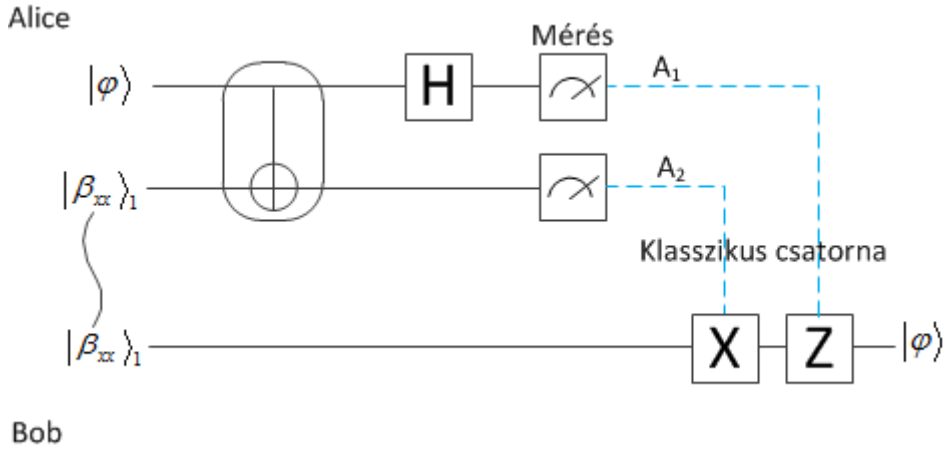
Ha lehallgatták a csatornát, az azonnal kiderül, ugyanis a lehallgató a no-cloning elmélet szerint nem tud tetszőleges, előre nem ismert, nem ortogonális állapotokat másolni. Vagyis, ha a lehallgató kiadja magát Bob-nak, és elkapja a Bob-nak szánt qbiteket, akkor azokat már nem tudja lemásolni, és azonos állapotban továbbküldeni neki. Amikor Alice és Bob ellenőrizné a kulcs adott bitjeit, akkor az eltérést fog mutatni, és innen tudják, hogy valaki megszemélyesítéses támadással próbált beférkőzni a kommunikációjukba.



4. ábra BB84 - Kétszereplős kvantum kulcsszétosztás

2.7. Teleportáció

Miután felállt a biztonságos, szimmetrikus kulccsal titkosított csatornánk, és szeretnénk a klasszikus kommunikációs sebességünket átlépni, akkor az egyik legjobb választásunk lehet a teleportáció (5. ábra), melyhez optikai szabad-csatornára van szükségünk (vagyis nem optikai kábelre). A teleportáció gyakorlati határa az összefonódással függ össze, tekintve hogy az eljárás egy összefonódott pár szétosztásán alapszik. Kínai tudósoknak sikerült eddig a leghosszabb távon fenntartani az összefonódást, így a teleportációt mintegy 16 km-en keresztül előidézni [10]. Ehhez az eljáráshoz azonban klasszikus csatornára is szükség van. Miután Alice és Bob megosztozott az összefonódott párokon, a kommunikáció egy része klasszikus csatornán zajlik. A klasszikus közegen érkező információ a másik fél kvantum kapuit vezérli, ezért ezt a csatornát nevezhetjük vezérlő csatornának is. A transzformációk végén Bob az Alice által küldött kvantum bitet fogja megkapni. Mivel ez a csatorna lehet közös hozzáférésű, ezért itt szükség lehet az ismert klasszikus hibavédelmi és közeghozzáférési eljárások alkalmazására.



5. ábra Az alap teleportációs eljárás

Tegyük fel, hogy Alice át akar juttatni Bob-nak egy tetszőleges $|\varphi\rangle$ qbitet. Ehhez nem kell mást tennie, mint a már előre megosztott $|\beta_{00}\rangle$ Bell-párját és a továbbítani kívánt qbitet egy CNOT kapun összefonódtatnia, a $|\varphi\rangle$ vezetéket további Hadamard kapuba vezetni, majd a használt két kvantum vezetéket megmérni. Az így kapott klasszikus biteket továbbítja Bob-nak, aki előre elkészítette, hogy a bit pároknak megfelelően milyen állapotban lehet az ő Bell-párja, amely Alice CNOT kapus manipulálásakor nála is megváltozott. Vagyis az információ már akkor megérkezett Bob-hoz, a problémát az jelenti, hogy nem tudja segítség nélkül kinyerni az adatot a Bell-párjából. Erre kell Alice által küldött két klasszikus bit.

A_1A_2	$\|\beta_{00}\rangle$	Alice által elvégzett transzformáció
00	$\frac{a\|0\rangle + b\|1\rangle}{2}$	I
01	$\frac{a\|1\rangle + b\|0\rangle}{2}$	X
10	$\frac{a\|0\rangle - b\|1\rangle}{2}$	Z
11	$\frac{a\|1\rangle - b\|0\rangle}{2}$	ZX

2. táblázat Alice-től érkezett klasszikus bitek alapján Bobnak fordított sorrendben kell a transzformációkat elvégeznie. A táblázat a 00-ás bemeneti Bell-párra vonatkozik.

A 2. táblázatból azt láthatjuk, hogy az Alice A_1 és A_2 vezetéken érkezett bitek szerint Bob Bell-párja milyen állapotban lehet. A 3. oszlopban láthatjuk, hogy a megváltozott Bell állapotot milyen unitér transzformációval kaphattuk. Bob-nak nem kell mást tennie, mint a megfelelő transzformációkat fordított sorrendben elvégezni a qbitjén. Ezek a transzformációk az X és Z Pauli kapuk megfelelő kombinációjának alkalmazását jelentik. Az A_1 és A_2 vezeték ezt a két kaput vezérli a táblázatnak megfelelően, ha 0, akkor a kapu ki van kapcsolva, ha 1, akkor végrehajtódik a transzformáció. Fontos megjegyezni, hogy az információhordozó $|\varphi\rangle$ qbitről sem Alice-nak sem Bob-nak nem kell tudnia semmilyen információt, ám Alice klasszikus bitjei nélkülözhetetlenek a qbit Bell-állapotból való kinyeréséhez, ami azt jelenti, hogy valójában nem gyorsabb az információáramlás a két fél között, mint klasszikus esetben. Viszont ahhoz, hogy klasszikusan kódoljunk egy tetszőleges $|\varphi\rangle$ állapotot – vagyis annak amplitúdóit – rengeteg klasszikus bitre lenne szükségünk, tehát végeredményben több információt küldhetünk át egy kvantum bittel, mint egy bittel tehetnénk.

2.8. Szupersűrűségű tömörítés

Az alap eljárás szerint Alice a klasszikusan kódolt bitsorozatát szeretné elküldeni Bob-nak (6. ábra) [5]. A biteket kettesével csoportosítja, és ezen dibiteknek megfelelően dönti el, hogy milyen transzformációt fog végrehajtani a Bell-párján. Az 3. táblázatban szereplő adatokból Bob elkészíti a megfelelő dekódoló egységet [CNOT(H ⊗ I)], mely segítségével visszanyerheti az eredeti két bitet. Ezt csak úgy tudja megtenni, ha a Bell-pár mindkét fele nála van, ezért szükséges, hogy Alice a nála lévő Bell állapotú qbitet elküldje Bob-nak. Ha a kvantum csatornán megérkezett a Alice qbitje, akkor Bob végrehajtja a dekódolást az egész Bell-páron. Ebben a formában az eljárással dupla annyi információt továbbítunk, mint klasszikus esetben, hiszen a csatornán egy Bell-félpár került továbbításra a két bit helyett.

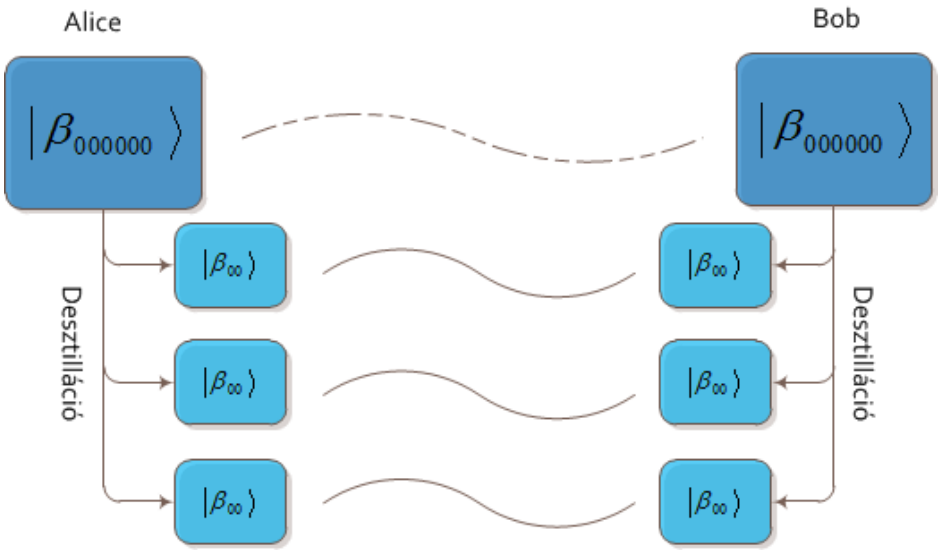
6. ábra Szupersűrűségű tömörítés

A_1A_2	Transzformáció	Közös állapot
00	I	$\frac{\|00\rangle + \|11\rangle}{\sqrt{2}}$
01	Z	$\frac{\|00\rangle - \|11\rangle}{\sqrt{2}}$
10	X	$\frac{\|10\rangle + \|01\rangle}{\sqrt{2}}$
11	jY	$\frac{\|01\rangle - \|10\rangle}{\sqrt{2}}$

3. táblázat Alice kódoló táblája, melyet Bob is elkészít a megfelelő dekódoláshoz

2.9. A desztillációs eljárás

A desztillációs folyamat lényege, hogy egy nagyobb Bell-összefonódást osztunk szét a két fél között, majd lokális transzformációkkal több kisebb, de tisztábban összefonódott Bell-párokra osztjuk őket [11]. Mivel a valóságban a csatorna nem zajmentes, ezért az átvitt részecskék állapota sem lesz a megérkezéskor teljesen tiszta. A desztillációs – más néven tisztítási - protokoll úgy készít tisztább, erősebben összefonódott párokat, hogy közben csökkenti az összefonódásban résztvevő részecskék számát. Az eljárás végén Alice és Bob több, egyszeresen összefonódott tiszta Bell-párral fog rendelkezni.



7. ábra Desztillációs eljárás - nagyobb, de gyengébb összefonódásból, kisebb, de erősebb összefonódást készít.

3. CASCADAS – (Q)ACE és a kommunikáció

A CASCADAS (Component-ware for Autonomic Situation-aware Communications, and Dynamically Adaptable Services) egy európai fejlesztésű klasszikus infokommunikációs projekt volt 2006 és 2009 között [1]. Alapja az Autonóm Kommunikációs Egység (ACE, Autonomic Communication Element), melyek a begyűjtött információ alapján képesek alkalmazkodni, és további cselekvéseiket ennek megfelelően alakítani. A rendszer külső beavatkozás nélkül működik, s ez az automatikus, önszervező tulajdonság elengedhetetlen a jövő infokom-hálózatainak kialakításához. A CASCADAS célja egy olyan keretrendszer kialakítása volt, mely autonóm komponens-alapú, és segítségével olyan innovatív szolgáltatások készíthetők, melyek kiszámíthatatlan környezetben is dinamikusan tudnak alkalmazkodni a kialakult helyzethez. Vegyük példának a jövő internetét, ahol az önszerveződő komponensek képesek bármilyen kívánt szolgáltatást kialakítani s kiszolgálni. Vagyis elképzelhetünk magunk köré egy olyan világot, ahol a hálózati eszközeink és szolgáltatásaink önmaguktól hozzánk igazodnak, csupán megfigyeléseik alapján. Legyen szó akár intelligens házról, légi vagy autósforgalom-figyelő és irányító rendszerekről, reklámokról vagy akár kórházi felügyelő rendszerekről, a személyi beavatkozást nem igénylő, önszerveződő hálózatoknak minden területen nagy hasznát vennénk.

Az ilyen hálózatok alapja az ACE, melyek nem csak a saját maguk által begyűjtött adatokat használják fel, hanem a többi ilyen egység információját is. Így minden ACE-nek önállóan kialakított képe van a világról, és még az előtt képesek preventív lépéseket tenni, hogy valamely eszkalálódott helyzet az ő pozíciójukat is elérné (például egy forgalmi dugó). Az, hogy milyen jól döntenek, a viselkedésüket meghatározó, beléjük programozott mesterséges intelligenciától függ. De vértezzük fel a hálózatot alkotó elemeinket a kvantum informatika adta lehetőségeinkkel! Így jutunk el a QACE-hez (Quantum ACE), melynek belső működése teljesen kvantum alapokon nyugszik. Gondoljunk egy olyan komplex rendszerre, ahol egy-

egy QACE-nek hatalmas tudásbázisa van, és meg kell keresnie az adott helyzetben a legjobb döntést, akkor a belső kvantum rendszere a Grover algoritmus segítségével pillanatok alatt megtalálja a leghelyesebb viselkedést, majd ezt a még kvantum állapotban lévő információt egy mérés segítségével bebillenti a klasszikus helyzetbe [2].

Az QACE-k a kialakított tudás-hálózaton legegyszerűbb, ha vezeték nélküli módon kommunikálnak, így lehetőség van mobil QACE-k használatára is. A kvantum egységek kommunikációját is átültethetjük kvantum alapokra. A tudás-háló kvantumosítására többféle algoritmust lehet választani, jelen dolgozatban a teleportációt és a szupersűrűségű tömörítést fogom felhasználni. Bár az algoritmusok már régóta léteznek, most az önszerveződő hálózatok kommunikációjának vizsgálatára fogom ezeket a kvantum eszközöket felhasználni. Az előbbi esetben a QACE egység döntésének végeredményét ez annyiban befolyásolja, hogy az utolsó lépést nem hajtjuk végre – az adatbázisból kikeresett elemet nem mérjük be klasszikus állapotba –, hanem ezt a qbit információt szállítjuk a hálózat többi eleméhez.

A kvantum eszközeink lehetnek mozgó és egyhelyben álló elemek is. Az általuk kialakított hálózat lehet központosított, vagy központi elem nélküli. Az sem feltétlen szükséges, hogy minden résztvevő mindenkivel tartson kapcsolatot, vagyis a QACE-ek elhelyezése területekre (area) bonthatók, így egy csoporton belül elég egy központnak számon tartani a többiekhez tartozó qbit párokat. Az elővigyázatosság is fontos szempont, így a QACE-ek között létrejövő kommunikációnál a hibavédelemre és a titkosításra is figyelmet kell fordítani.

4. Az önszerveződő hálózat és a kvantum kommunikáció

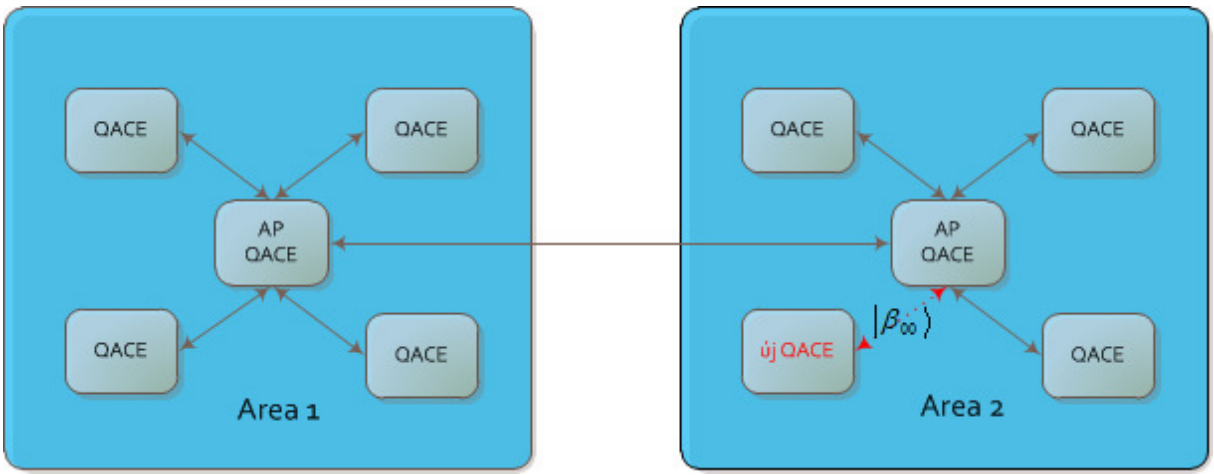
4.1. Motiváció

A kvantum rendszerekkel és a kvantum kommunikáció kialakításával egy olyan hálózat megalkotása a célom, mely rendkívül gyors, megbízható, a klasszikus rendszerekhez alig mérhető sebessége az információáramlást a következő szintre emeli. A gyors számítások és keresések olyan eszközök használatát teszik lehetővé, melyek klasszikus változatának alkalmazása a lassúságuk miatt nem volt kívánatos, vagy nem teljes potenciállal működött. A kvantum eszközeinkbe már a komplexebb mesterséges intelligenciával működő ágenseket is belerakhatjuk, s ha ezt hálózati elemek formájában képzeljük el (QACE), akkor egy olyan önszerveződésre képes autonóm, tanuló hálózati elemeket kapunk, melyek ténylegesen képesek a legszélsőségesebb helyzetekben is alkalmazkodni. Természetesen a cél egy autonóm önszerveződő *hálózat*, így a dolgozat további részében a QACE hálózati elemek kommunikációjáról lesz szó.

4.2. Topológia

Az eszközök elrendezése elég változatos lehet. Lehetnek mozgó és álló csomópontjaink. A legegyszerűbb, ha egy klasszikus ad-hoc hálózathoz hasonlítjuk, melyben az álló, ám könnyen elmozdítható eszközök, az hozzáférési pontok (AP, access point) itt a központjainkat alakítják, felépítésükben megegyeznek a sima QACE eszközökkel. Feladatukat úgy határoztam meg, hogy a kvantum AP a QACE-k közötti kapcsolatfenntartásért felelős, valamint felülbírálhatja a QACE-k által gyűjtött információra adott viselkedésüket.

4.2.1. Központi elemmel rendelkező topológia



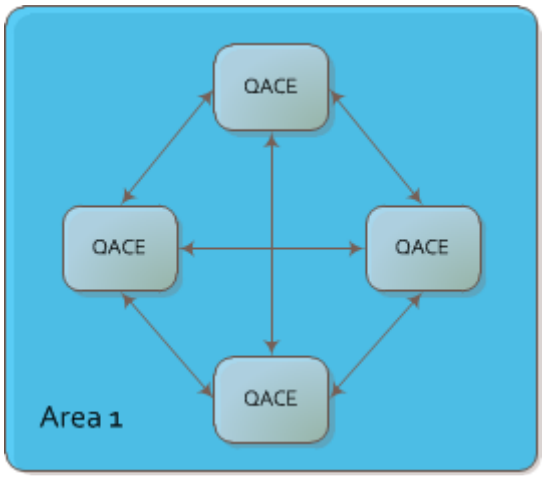
8. ábra Központosított topológia egy QACE area váltásával

Az egyik változatban vannak álló AP csomópontok, melyek szintén QACE-k, valamint a nekik a jelentő mozgó QACE egységek. Ha elég nagy területet kell lefednie a hálózatnak, akkor érdemes az ad-hoc hálózatot csoportokra (area) bontani. Ilyenkor előfordulhat, hogy az egyik

QACE a barangolása közben csoportot vált. Erre gondolhatunk úgy, mint a klasszikus mobil hálózatok cellaváltására. Amikor egy QACE másik csoportba érkezik, bejelentkezik az ottani AP-nak, amely egy összefonódott qbit párral válaszol az új tagnak, ezzel beregisztrálva a hozzá tartozó csoportba. A központok lehetővé teszik a csoportok közti információ cserét is, vagyis a szomszédos AP QACE egységek egymással is kapcsolatban állnak.

4.2.2. Központi elemmel nem rendelkező topológia

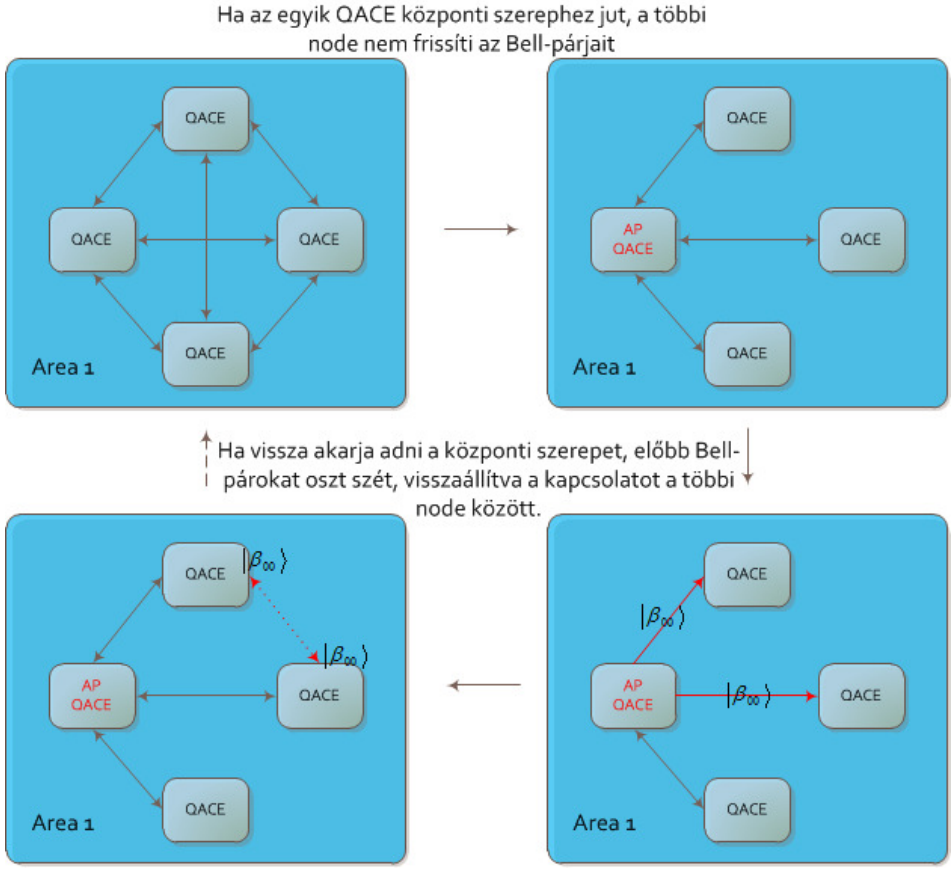
Egy másik lehetséges elrendezésben az összes használt eszköz mozog, kapcsolatban van egymással, és nincs kijelölt központi egység sem, ekkor viszont nincs felügyelet a választott viselkedés felett (9. ábra).



9. ábra Egy központ nélküli topológia egy csoportja

A topológiát úgy alkottam meg, hogy egy belső algoritmus segítségével, ha szükséges, választhatnak ideiglenesen egy központi elemet játszó QACE-t, így a két topológia között valamekkora átjárás biztosított. Ha egy QACE a tudásbázisa alapján olyan állapotba kerül, amely szükségessé teszi, hogy ő legyen a központ, akkor broadcastolja magáról, hogy központtá változott. Természetesen egyszerre több egység is dönthet így, ezért központi szerepért versenyezniük kell. Lehetséges a QACE egységeknek prioritást adni (például: helyzetük, kapcsolataik száma szerint), így a központi szerep azé lehet, aki magasabb prioritással rendelkezik. A broadcastolás központ (illetve központtá válni akaró eszköz) részéről úgy történik, hogy a vele összefonódott qbittel kapcsolatban álló QACE-knek, ezen párokon keresztül küldi az információt, vagyis semmiben nem különbözik a peer-to-peer kommunikációtól. Ha az ideiglenes központ befejezte a tevékenységet, akkor az area aktuális tagjai között szétosztja az összefonódott qbit párokat, majd lemond a központi szerepről, így a hálózat visszakerül a központ nélküli topológiába (10. ábra). Fontos megjegyezni, hogy az ideiglenes központ esetében nincs lehetőség arra, hogy a szomszédos központok kapcsolatba lépjenek egymással, ez csak a fixen központosított esetben lehetséges.
A csoportokra bontást központ nélküli esetben is alkalmazhatjuk, area váltásnál új tag broadcastolja az adatait, melyre központ nélküli csoportban, mindenki válaszol egy

összefonódott Bell-párral. Az ideiglenes központtal rendelkező area-ban csak a központ válaszolhat szintén egy összefonódott Bell-párral. Az utóbbi eljárásban a többi csomópont természetesen tudja, hogy az area AP-vel rendelkezik, ezért ők nem válaszolnak a kérésre.



10. ábra Átjárás szemléltetése a központ nélküli és a központtal rendelkező topológia között

Azt, hogy egy area-ban ki a központ (fix központ esetén), illetve van-e, azt a csomópontok vándorlásuk során frissítik a többi area-nak, így a hálózat topológiájáról alkotott kép mindig aktuális marad.

4.3. A kommunikáció vizsgálata kvantum eszközökkel

A QACE-k kommunikációja az összefonódáson alapszik, vagyis azon, hogy Alice-nek és Bob-nak van egy-egy qbitje, amelyek összefonódott állapotban vannak egymással. Az első felmerülő probléma, hogy honnan tudjuk, ha információáramlás történt? Klasszikus esetben a bizonyos frekvenciával mintavételezett feszültség-minták határozzák meg, hogy a küldött információs bit 0 vagy 1, és például a csupa 0 sorozat jelenti, ha éppen nincs üzenet. A kvantum világban viszont nem mérhetjük be a qbiteket klasszikus állapotba, hiszen a mérés során elveszítenénk a qbitek lényegét adó amplitúdókat, ezért ezen irreverzibilis tulajdonság miatt nem lehet a klasszikus csatornafigyelési módszert alkalmazni. A kvantum infokommunikációban a beérkezett fotonok jelentik az egyes qbiteket, ezért azt kell

eldönteni, hogy a beérkezett fotonok közül melyikre kell figyelni. Az összefonódott állapotban lévő qbitek állapotváltozását is fel kell ismerni, ezeknek a problémáknak a megoldása nem témája a jelen dolgozatnak. A csatorna fizikai felépítésével és a felépítéséből adódó hibákkal nem foglalkozom, viszont fontos megemlíteni a klasszikus és kvantum fizikai információáramlás közötti különbségeket.

Az általános protokoll leírások szerint, Alice és Bob kezdetben „nagyon sok" Bell-páron osztoztak meg, és nem foglalkoznak azzal, hogy a valóságban ez nagyon absztrakt leírás. Ezért olyan megoldást kellett alkalmaznom, amely túllép az egyszerű elméleti „nagyon sok páron megosztoztak" leíráson. Azért, hogy a QACE kommunikáció megvalósíthatóság keretein belül maradjon, felhasználtam a desztillációs eljárást, amely biztosítja a folyamatos Bell-pár utánpótlást. Ez a megvalósíthatóság szempontjából azt jelenti, hogy megadott időnként egy többszörösen összefonódott Bell-párt továbbítunk a kvantum csatornán. Ezt helyileg kisebb darabokra desztilláljuk, így lecsökkentve az összefonódott párok szétosztásából adódó forgalmat a hálózaton.

4.3.1. Teleportáció és szupersűrűségű tömörítés

Az üzeneteinket két csoportra oszthatjuk ugyanúgy, mint klasszikus esetben: lehetnek jelzés/karbantartó és információs üzenetek. Az üzeneteket keretezzük, és a kereteik alapján döntjük el, hogy melyik kategóriába tartoznak, illetve milyen információt hordoznak számunkra. A QACE-k kétféle eljárást alkalmazhatnak: a teleportációt vagy a szupersűrűségű tömörítést.

4.3.1.1. Teleportáció

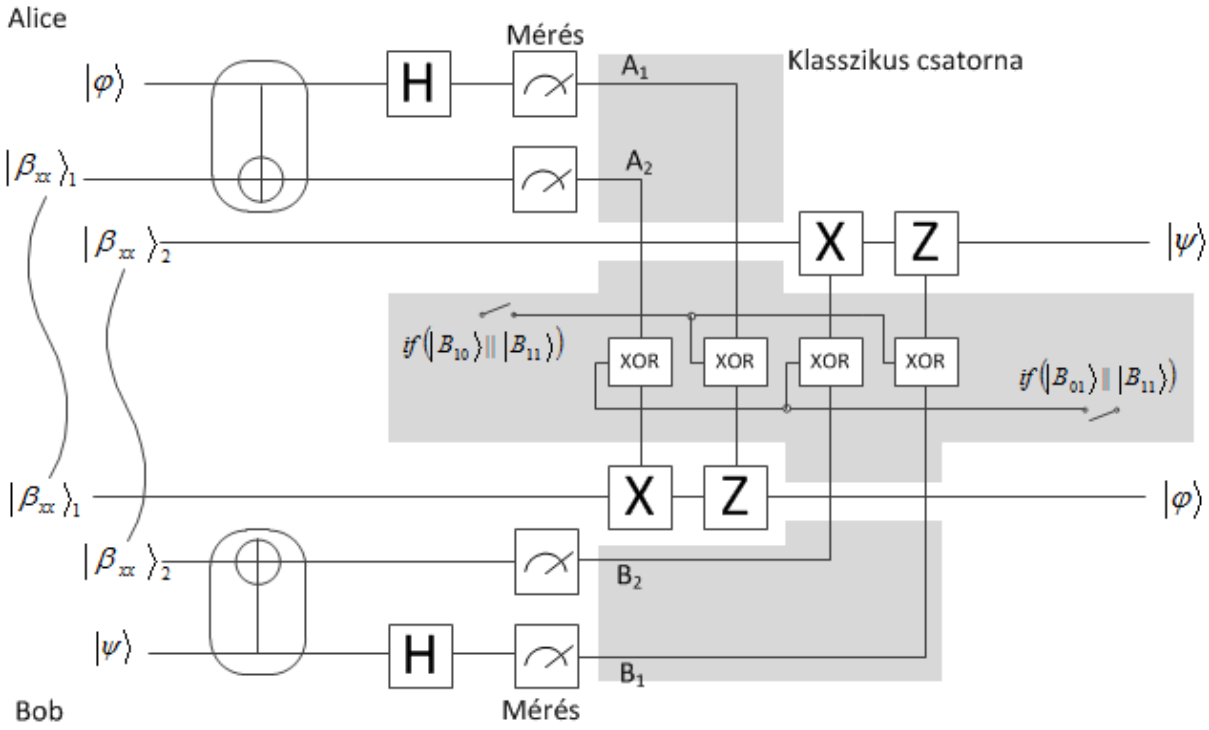
Teleportációs eljáráshoz szükség van klasszikus és ideiglenesen felépített kvantum csatornára is. Az utóbbi csupán addig kell, amíg Alice és Bob megosztozik a Bell-párjaikon, ahogyan azt feljebb olvashattuk.

Tovább alakítottam a korábbi fejezetben ismertetett teleportációs algoritmust. Az alap algoritmust úgy tettem univerzálissá, hogy nem kell csak a $|\beta_{00}\rangle$ állapotú Bell-párokra hagyatkozni, bármelyik Bell-állapotot használhatjuk. Mivel előre ismerjük a megosztott párokat, csak az ezeknek megfelelő transzformációkat kell átgondolni, s láthatjuk, hogy az ortogonalitás miatt csak a kapuk alkalmazása ugrott másik állapothoz. A 4. táblázatban láthatjuk, hogy a megfelelő bemenetű Bell-pár és az Alice-től érkező klasszikus dibit esetén, Bob oldalán lévő Bell qbit milyen állapotban található, az ettől jobbra található oszlopban az Alice által elvégzett transzformáció látható.

A megvalósításhoz plusz XOR vezérlő egységeket vezettem be. Ezeket Bob oldalára kell beépíteni. A XOR kaput annak megfelelően vezérlejük, hogy éppen milyen Bell-párral dolgozunk. Mivel szétosztáskor már tudjuk, ezért a XOR kapukat ennek megfelelően előre be tudjuk állítani. Amint a 11. ábrán látható, az imént bemutatott eljárást az ellenkező oldalra is kiépítettem, s így Alice és Bob képes egymással duplex módon is kommunikálni.

A_1A_2	$\lvert\beta_{00}\rangle$		$\lvert\beta_{01}\rangle$		$\lvert\beta_{10}\rangle$		$\lvert\beta_{11}\rangle$	
00	$\frac{a\lvert0\rangle+b\lvert1\rangle}{2}$	I	$\frac{a\lvert1\rangle+b\lvert0\rangle}{2}$	X	$\frac{a\lvert0\rangle-b\lvert1\rangle}{2}$	Z	$\frac{a\lvert1\rangle-b\lvert0\rangle}{2}$	ZX
01	$\frac{a\lvert1\rangle+b\lvert0\rangle}{2}$	X	$\frac{a\lvert0\rangle+b\lvert1\rangle}{2}$	I	$\frac{a\lvert1\rangle-b\lvert0\rangle}{-2}$	ZX	$\frac{a\lvert0\rangle-b\lvert1\rangle}{-2}$	Z
10	$\frac{a\lvert0\rangle-b\lvert1\rangle}{2}$	Z	$\frac{a\lvert1\rangle-b\lvert0\rangle}{2}$	ZX	$\frac{a\lvert0\rangle+b\lvert1\rangle}{2}$	I	$\frac{a\lvert1\rangle+b\lvert0\rangle}{2}$	X
11	$\frac{a\lvert1\rangle-b\lvert0\rangle}{2}$	ZX	$\frac{a\lvert0\rangle-b\lvert1\rangle}{2}$	Z	$\frac{a\lvert1\rangle+b\lvert0\rangle}{-2}$	X	$\frac{a\lvert0\rangle+b\lvert1\rangle}{-2}$	I

4. táblázat Univerzális táblázat a vevő oldali XOR kapu vezérlésére



11. ábra Duplex teleportáció változtatható Bell állapotokkal

4.3.1.2. Szupersűrűségű tömörítés

A szupersűrűségű tömörítéses eljárásnál csak egy kvantumcsatornára van szükségünk. A Bell-párokat ugyanúgy osztjuk szét, mint a teleportálós esetben, illetve ahogyan azt feljebb

olvashatjuk. Az algoritmus egyszerűsége miatt, itt nem szükséges az eljárást a 2.8-as fejezetben leírtakhoz képest módosítani.

4.4. Kommunikáció folyamata

Miután ismertettem az általam kialakított kommunikációs környezet topológiáját, eszközeit és eljárásait, szeretném bemutatni az általam kidolgozott kommunikációs folyamatot a kapcsolat felépítésétől a bontásáig.

4.4.1. Kapcsolat felépítés

Első lépésként fel kell építeni a kapcsolatot az eszközeink között. Ebből a szempontból nincs jelentősége annak, hogy központokkal dolgozunk, vagy egyenrangú QACE eszközökkel, hogy átregisztráció miatt történik a kapcsolat felvétel, vagy teljesen új eszközt állítunk a hálózatba.
Az új QACE a másik kommunikáló féllel kezdeményezi a kapcsolat felvételt. Ha lehetősége van rá, akkor kvantum csatornán kéri a kapcsolat felvételt, de klasszikusan is jelezheti kérelmét a másik fél felé. Mielőtt bármilyen értékes információ gazdát cserélne, a felek közötti kommunikációt megfelelő módón titkosítani is kell. A csomópontok a kvantum kulcsszétosztás segítségével kialakítják a közös kulcsukat, amely teljesen biztonságossá teszi az információcserét. Kvantum kommunikációnál az esetek nagy részében a két fél összefonódott párokat alkalmaz, ezért itt a titkosítás nem lenne szükséges, de mivel előfordulhat olyan eset, hogy egy csomópont csak továbbítja az adatot, ezért a továbbított információt itt is titkosítani kell, a magukat a hálózat elemeinek kiadó rosszindulatú elemek ellen. A klasszikus kommunikációs folyamatnál a titkosításon kívül minden történhet úgy, ahogyan a már ismert infokommunikációs hálózatokban történne.

Ha megtörtént a titkosítás, a két fél megegyezik, hogy milyen eljárás szerint fog a kommunikáció lezajlani. Legyen szó szupersűrűségű tömörítésről, vagy kvantum teleportációról, mindkettő alapja az összefonódott qbitek, ezért inicializálás első lépéseként egy nagyobb Bell-párt osztanak meg, majd a desztillációs protokoll segítségével több, kisebb, erősebben összefonódott qbiteket kapnak. A szupersűrűségű tömörítésnél a kvantum csatornát nem bontjuk le, hiszen az algoritmus folyamatosan használja. Ezután el is kezdődhet a információ csere.
Az új tag és az area központja (ha van ilyen) kölcsönösen frissítik a hálózatról alkotott tudásukat, többek között, hogy melyik szomszédos csoportban található (fix) központ. Erre azért van szükség, hogy ha a QACE tovább mozog tudja, hogy cél csoportban kihez kell bejelentkeznie, illetve broadcastolással kell-e felvennie a kapcsolatot a tagokkal. Az inkonzisztencia elkerüléséért feltételezzük, hogy minden tudáselem időbélyeggel van ellátva. Ezután a központ a csoport tagjai között broadcastolja az új QACE által frissített információkat.

Ha az új csoportnak nincs központja, akkor a broadcastolásra válaszoló QACE-k mindegyikével lefolytatja a tudásbázis frissítést.

4.4.2. Üzenet típusok

4.4.2.1. Vezérlő üzenetek

A kapcsolat felépítés után, a hálózat a 4.2 fejezetben leírtaknak megfelelően működik. A megosztott üzenetek lehetnek általános vezérlő információk, mint például eljárás-váltásra való felhívás, vagyis a hálózatnak lehetősége van működés közben teleportációról szupersűrűségű tömörítésre áttérni, illetve fordítva. De kezdeményezhetnek további összefonódott qbit megosztást is, amennyiben az ütemezett szétosztás valamilyen okból nem megfelelő. Előfordulhat, hogy az egyik QACE olyan információkat kap, amely arra készteti a csomópontot, hogy átlépjen központi szerepbe, és közvetlenül befolyásolja a többi QACE viselkedését. Ha egy másik QACE is versengett a központi szerepért, akkor az információt, amely őt erre késztette megosztja az aktuális központtal, s az ennek megfelelően dönt a hálózat további viselkedését illetően. Ha a központ tudásbázisa alapján a központi felügyeletet igénylő szituáció elmúlt, akkor lemond a központi szerepről.

4.4.2.2. Adat üzenetek

A fő üzenetek a QACE-k környezetükről alkotott képei, valamint az aktuális helyzetre adott viselkedésük. Teleportáció esetén a QACE-k valójában nem tudják, hogy milyen adatot kerestek ki a tudásbázisukból a Grover algoritmussal, nincs képük a helyzetről, nem tudnak önálló döntést hozni. Ugyanis az utolsó lépés kihagyásával egy qbithez jutnak, amelyet nem dolgozhatnak fel, mert az a klasszikus állapotba való bemérést jelentené, s így elveszítenék a qbit lényegét adó amplitúdókat. A keresés eredményét a fogadó fél fogja feldolgozni, melynek az a feltétele, hogy a küldő és fogadó fél azonos állapottérrel rendelkezzen. A szupersűrűségű tömörítésnél a küldő fél végrehajtja az utolsó lépést a Grover algoritmusban, s így a csomópontoknak képe lesz a környezetéről, tud önálló döntést hozni. A teleportációt központosított, a szupersűrűségű tömörítést központ nélküli esetben érdemes használni, ugyanakkor nem kizárt a két eljárás egyszerre történő alkalmazása sem. Vagyis, ha egy már bemért adatot szeretnénk továbbítani, akkor a szupersűrűségű tömörítést használjuk, ha pedig egy csomópont jelent a központnak, akkor a teleportációt.

4.4.3. Viselkedés mozgás közben

Ameddig a QACE area-n belül mozog, addig a mozgásból adódóan semmilyen tennivaló nincsen. Amikor area-t vált, a régi csoportból ki kell jelentkeznie, vagyis az ottani kapcsolatait bontani kell, az új csoportba be kell regisztrálnia, vagyis kapcsolat felvételt kell kezdeményeznie az ottani elemekkel.

4.4.4. A kapcsolat bontása

A kommunikációs eljárásaink alapja az összefonódott qbit, ezért a kapcsolat bontására irányuló üzenetben jelezni kell, hogy a továbbiakban nincs szükség a megosztásukra. Csak a megosztás felfüggesztése azért nem elegendő, mert ez lehet egy sima kontroll üzenet is: amennyiben nincs nagy információáramlás, úgy előfordulhat, hogy néhány ütemezett Bell-pár szétosztást ki kell hagyni.
A másik fél nyugtája után, a megmaradt összefonódások eldobhatóak.

5. Eljárások elemzése

Ebben a fejezetben összehasonlítom az önszerveződő hálózat működését a klasszikus és a tárgyalt eljárások felhasználásával. Az összehasonlítási szempontok: a választott rendszer gyorsasága, a felhasznált klasszikus és kvantum bitek, valamint a választott topológia. A fejezet végén ajánlást teszek arra, hogy melyik összeállítást érdemesebb használni.

5.1. Cél

Az elemzésem célja megmutatni, hogy az általam összeállított kvantum kommunikációs eszközökkel megvalósított önszerveződő autonóm hálózat valóban hatékonyabb, mint a klasszikus kommunikációs eljárásokon alapuló változat.

5.2. Gyorsaság vagy többletinformáció

Mind a teleportációnak, mind a szupersűrűségű tömörítésnek van előnye ott, ahol a másik kicsit gyengébben teljesít. Ezért nem lehet teljesen egyértelműen eldönteni, hogy melyik eljárás hatékonyabb. Kommunikáció szempontjából a két eljárás ugyanazokat az üzeneteket használja, a különbség az üzenetenkénti bitek és qbitek felhasználásból adódik. Az 5. táblázatban látható, hogy egy üzenetküldés alatt a választott eljárás egy tranzakciója milyen arányban használ fel biteket és qbiteket.

Teleportáció		**Szupersűrűségű tömörítés**
2	Használt klasszikus bit	0
1	Használt Bell-pár	1
1 qbit	Szállított információs egység	2 bit
2 bit	Csatornán küldött egység (a kezdeti Bell-pár osztáson kívül)	1 qbit (Bell-pár másik fele)

5. táblázat Két csomópont közötti kommunikációban az egy tranzakció alatt felhasznált bitek és qbitek

A táblázatban szereplő adatok azt a benyomást kelthetik, hogy a szupersűrűségű tömörítés egyértelműen jobb lenne, mint a teleportáció. Viszont utóbbi eljárás egy kvantum állapotú információs bitet továbbít, míg az előbbinél a fogadó fél két klasszikus bitet fog kapni a dekódolás után.
A szupersűrűségű tömörítés tisztán kvantum kommunikációt alkalmaz, viszont az algoritmus bemenetén klasszikus bitek találhatók, s melynél a fogadó fél az összefonódott párjából egy dekódoló egység segítségével ismét klasszikus biteket kap. Amennyiben a qbit továbbítása, és a dekódoló működése egység gyorsabb, mint ahogy a teleportációnál szükséges két klasszikus bit átér a csatornán, úgy kijelenthetjük, hogy ennek az eljárásnak egy tranzakciója gyorsabb, mint riválisáé. Mivel a dekódoló egység kvantum kapukat tartalmaz, ezért az előbbi kérdésre azt a válasz adhatjuk, hogy igen, a szupersűrűségű tömörítés tranzakciója valóban gyorsabb, ugyanakkor csupán két klasszikus bitet sikerült továbbítani. A klasszikus

ki- és bemenet a QACE egységek hatásfokát is rontják, ugyanis ilyen esetben az Grover algoritmus utolsó lépését is végre kell hajtani, vagyis az adatbázisból kikeresett adatot be kell mérni klasszikus állapotba. A teleportációnál ez a lépés kihagyható, ugyanakkor a fogadó oldal csak akkor tudja felhasználni az átküldött kvantum információt, ha a két klasszikus bit is megérkezik. Mivel a fogadó oldal egy kvantum alapokon működő egység, a kommunikáció végén kapott qbit több információt hordoz számára, mint egy (vagy kettő) klasszikus bit.
Tehát van két eljárásunk, melyeknél az egyik "gyorsabb", a másik pedig több információt szállít egy tranzakció alatt. Így viszont egy kellően hosszú üzenetnél a szupersűrűségű tömörítés már nem hatékonyabb a teleportációnál, ugyanakkor rövid üzeneteknél ez még lehet kedvezőbb.

	Klasszikus	**Szupersűrűségű tömörítés**	**Teleportáció**
Átviteli sebesség	klasszikus	kvantum	klasszikus
Átvitt adat formája	klasszikus	dupla klasszikus	kvantum

6. táblázat Sebességek összehasonlítása a klasszikus hálózatokhoz mérve

A 6. táblázatban a használható eljárások sebességét láthatjuk a klasszikus sebességhez viszonyítva, ahol a klasszikus sebesség a jelenleg használt rendszerek és hálózatok sebességét jelenti. Az átvitt adat formája az eljárások végén rendelkezésre álló információs egységet jelenti, melyben a klasszikus adatokat a 0 és 1 klasszikus bitek jelentik, a kvantum adatot pedig a $|\varphi\rangle$ qbit, mely információ tartalma több mint egy klasszikus bité.

5.3. Bitek és qbitek a különböző topológiákban

A teljesítményt nagyon fontos topológiai szempontból is vizsgálni, ezért megvizsgáltam központosított és nem központosított esetben is.

Központosított topológia
Mivel a központosított topológiában a központ az, aki az összefonódott qbitekkel tartja a kapcsolatot a csoport csomópontjaival, ezért ha n darab QACE egységet használunk, akkor n-1 darab Bell-párt kell fenntartani, valamint azokra a kapcsolatokra is kell Bell-párt számolni, melyek a szomszédos csoportok központjai között biztosítják a kapcsolatot, de ettől most eltekintek.

Nem központosított topológia
Nem központosított esetben minden node kapcsolatban van egymással. Ez n darab node esetén $\frac{n(n-1)}{2}$ darab Bell-párt jelent. Ezt azt jelenti, hogy egy üzenetváltás egy tranzakciója központosított esetben n-1-szer történik meg, míg központ nélküli esetben $\frac{n(n-1)}{2}$-szer.

Összehasonlítás

A 6. táblázat a teleportáció, a szupersűrűségű tömörítés és a hálózat klasszikus megvalósítása mellett használt biteket és qbiteket mutatja. A szürkített részek jelentik a csatornán ténylegesen továbbított biteket és qbiteket. Mint látható a teleportáció során dupla annyi bit kerül továbbításra, mint klasszikus esetben, ugyanakkor a kvantum eljárás során kvantum bitet nyerünk ki mely további felhasználás során többlet információt jelent a rendszernek. Azt is megfigyelhetjük, hogy a két kvantum eljárásban sosem a tényleges információt szállítjuk, hanem olyan adatot, mely további feldolgozásra szorul, s mely végén több információhoz jutunk, mint klasszikus esetben.

Központosított	**Szállított adat 1 tranzakció alatt**	**Központ nélküli**
Teleportáció		
$2(n - 1)$ bit	Vezérlő vagy vivő **bit**	$n\,(n - 1)$ bit
$n - 1$ qbit	Információs ***qbit***	$\frac{n(n-1)}{2}$ qbit
Szupersűrűségű tömörítés		
$n - 1$ qbit	Vezérlő vagy vivő ***qbit***	$\frac{n(n-1)}{2}$ qbit
$2(n - 1)$ bit	Információs **bit**	$n\,(n - 1)$ bit
Klasszikus eset		
$n - 1$ bit	Információs bitek	$\frac{n(n-1)}{2}$ bit

7. táblázat A hálózat egy n csomópontú csoportjában egy üzenetváltásának egy tranzakciója alatt szállított információs egységek száma

5.4. A helyzetről alkotott kép helyessége

Természetes a rendszerben használt eszközök hibázhatnak is. A hibázás lehetősége a Grover algoritmus többszöri végrehajtása során keletkezhet. Egy minimális ε-nál kisebb hibázási lehetőségnél a végeredmény, s így az eszközök hálózatról kialakított képe még lehet helyes. Egy QACE $P_s = (1 - P_e)$ valószínűséggel alkot a helyzetéről helyes képet, ahol P_s a helyes döntés valószínűsége, és a hibavalószínűség $P_e < \varepsilon$.

Topológiai szempontból mindegy, hogy a központ méri be a Grover algoritmus segítségével kikeresett qbitet, vagy minden csomópont magának végzi el a mérést. Összességében, amikor a QACE-k elterjesztették ezt az információt, a csoport minden eleme ugyanolyan valószínűséggel fogja a hálózat állapotát helyesnek látni. Különbségek az egyes csoportok között jelentkezhetnek. Mivel a csoportoknak nem kell más csoportok állapotát ugyanúgy feldolgozni, hiszen más helyzet és viselkedés vonatkozik rájuk, mint a többire, ezért a csoportok más-más állapotban fogják látni a hálózatot. Ez viszont nem hiba.

5.5. Ajánlás

Amennyiben sok eszközt szeretnénk a hálózatba állítani, úgy a központosított csoportos topológiát ajánlom, teleportációval. Ebben a felállásban csoportonként csak egy eszköznek kell a csoport csomópontjaitól, és a szomszédos központoktól kapott adat alapján felmérni a hálózat állapotát. Továbbra is fontos szerepet játszik, hogy az egyes csomópontok a saját érzékelésük alapján alkotnak képet a világról, csak ezt az információt egy központi agy fogja feldolgozni, majd megmondja a csoport tagjainak, hogyan illetve milyen információ szerint viselkedjenek. Mivel sok csomópont van hálózatban, és csak egy központ, ezért fontos, hogy az információcsere minél gyorsabban megtörténjen, és ne terheljük a hálózatot. Ilyenkor a kvantum bit továbbítása a legkézenfekvőbb, vagyis jelen esetben a teleportáció.

Kevés eszköz használata esetén a központ nélküli topológiát, és a szupersűrűségű tömörítést érdemes használni. Ilyenkor bár minden eszköz kapcsolatban áll egymással, a kevés számuk miatt nem kell egyszerre sok információt feldolgozni, és a hálózat sem terhelődik annyira a kvantum bitek továbbítása során

6. Összefoglalás

Megvalósíthatóság szempontjából úgy állítottam össze az algoritmusokat, hogy azok minél kevésbé legyenek absztraktak, szinte azonnal implementálhatók, amint a hardver eszközök rendelkezésünkre állnak.

A kvantum rendszer fő előnye a klasszikushoz képest, a gyorsasága és biztonsága. Ez a két tulajdonság a 21. század egyik legnagyobb követelménye. Mindenki azt szeretné, ha az őt körbevevő technika minél gyorsabban szolgálná ki az igényeit, és mindezt úgy, hogy a személyes adatait biztonságban tudja.

A dolgozat első felében szó volt az általános kvantum leírásokról: az információhordozó egységekről, kapukról, algoritmusokról, valamint az elméleti tervezést lehetővé tevő kvantummechanikai posztulátumokról.

A dolgozat második felében bemutattam, hogyan lehet egy klasszikus rendszer kommunikációját átültetni kvantum algoritmusokra, ehhez már rendelkezésemre álltak azok a kvantum egységek, melyek a hálózat elemeit alkotják.

Két algoritmus, a teleportáció és a szupersűrűségű tömörítés adott felhasználáshoz való adaptálását láthattuk. Mindkét eljárásnak vannak előnyei és hátrányai egymáshoz képest, de a klasszikus rendszerhez viszonyítva mindkettő fölényesen jobbnak bizonyult. Bár az algoritmusok alapverziói már régóta léteznek, ilyen komplex rendszer építéséhez elengedhetetlen az eljárások módosítása, a célnak megfelelő átalakítása. Végeredményként egy olyan önszerveződő autonóm hálózatot kaptunk, melyben a csoportok megválaszthatják a kommunikációjukhoz használt algoritmust és topológiát is.

Egy ilyen hálózatnak az életünk sok területén hasznát tudnánk venni. Segíthetnének a gyors és adaptív forgalom-irányításban, de a célorientált reklámozás is megoldható ugyanúgy, mint az intelligens házak működése.

7. Irodalomjegyzék

[1] CASCADAS Project: http://acetoolkit.sourceforge.net/cascadas/index.php, Project reference: FP6-027807, utolsó megtekintés 2011.10.19.
[2] L. Gyongyosi, L. Bacsardi, S. Imre - Quantum Probabilistic Decisions for Intelligent Autonomic Networking and Communication. Future Computing, 15-20 Nov. 2009, 586-590
[3] James F. Kurose, Keith W. Ross - Computer Networking: a top-dow approach, Pearson/Addison Wesley (2008)
[4] Forgalomban kapható kvantum eszközök: MagiQ Technologies Inc. http://www.magiqtech.com/MagiQ/Products.html - utolsó megtekintés 2011.10.27.
[5] S. Imre, F. Balazs – Quantum Computing and Communications, WILEY (2005)
[6] Salemian S, Mohammadnejad S. - An error-free protocol for quantum entanglement distribution in long-distance quantum communication. Chinese Sci Bull, 2011, 56: 618−625
[7] V. Buzek, V. Vedral, M. B. Plenio, P.L.Knight, M. Hillery - Broadcasting of entanglement via local copying, Phys.Rev. A55 (1997) 3327-3332, arXiv:quant-ph/9701028v1
[8] Györfi László, Győri Sándor, Vajda István - Információ- és kódelmélet Typotex, 2000, 2002
[9] Atul Kahate, Cryptography and Network Security, Tata McGraw-Hill (2003)
[10] Xian-Min Jin, Ji-Gang Ren, Bin Yang, Zhen-Huan Yi, Fei Zhou – Experimental free-space quantum teleportation. Nature Photonics 4, 376 - 381 (2010)
[11] Jian-Wei Pan, Christoph Simon, Caslav Brukner & Anton Zeilinger - Entanglement purification for quantum communication, Nature 410, 1067-1070 (26 April 2001)