Anonim kommunikációs rendszerek a gyakorlatban

Paulik Tamás
paulik.tamas.email@gmail.com

1 Bevezető

Az elektronikus kereskedelem gyakorlatában a megszokott, személyesen történő adásvételhez nagyon hasonló üzleti szempontoknak és érdekeknek kell megfelelnie azoknak, akik adásvételeiket elektronikus úton kívánják bonyolítani. Természetes és magától értetődő, hogy egy elektronikus tranzakciónak is rendelkeznie kell a személyes vásárlás legfontosabb tulajdonságaival és ezen tulajdonságok bele kell tervezni a jövő elektronikus kereskedelmi protokolljaiba, hogy ezek a fizetési módok elterjedhessenek. Néhány ilyen fontos tulajdonság:

- Intuitív kezelhetőség, jelenjen meg a pénzfogalom
- Gyorsaság
- Könnyű és olcsó üzembe helyezhetőség
- Tranzakció bizalmasság
- Tranzakció integritás
- Tranzakció fairség
- Felhasználói anonimitás

A vásárlói anonimitás a személyes vásárlás egyik legnagyobb előnye, készpénzzel fizetve a vásárlónak nem kell felfednie személyazonosságát senki előtt sem a boltban így megőrizhati anonimitását nem csak az eladóval, hanem a boltban tartózkodó, vagy azt megfigyelő személyekkel, biztonsági őrökkel szemben is.

Egy informatikai alapokon nyugvó hálózat azonban mind a mai napig elsősorban a végpontok, a kommunikáló felek azonosításán keresztül biztosítja a kapcsolatot a kommunikációban részt vevő felek között, egyik elől sem rejtve el a másik hálózati azonosítóját, így téve kényelmessé az átküldendő üzenetek címzését. Így egy támadó könnyedén megtudhatja, hogy ki kivel kommunikál és ha a kapcsolat nincs megfelelően védve, akkor akár azt is megtudhatja, hogy mi volt a tranzakció tárgya.

Kijelenthetjük tehát, hogy míg a személyes, készpénzes vásárlás természetéből adódóan alapvetően anonim, addig egy elektronikus kereskedelmi protokoll tervezésekor az anonimitás biztosítását is figyelembe kell venni. A most következőkben áttekintem, hogy mit

is értünk anonimitás alatt, valamint röviden ismertetem néhány sokak által analizált és így a gyakorlatba is könnyen átültethető technológiai megoldást az anonimitás biztosítására.

2 Az anonimitás fogalma

Az informatika világában elérhető anonimitás mérése és vizsgálata igen nagy múltra tekint vissza, jóval az elektronikus kereskedelem megjelenése előtt foglalkoztatta a kutatókat az anonim kommunikáció, illetve a meglévő kommunikációs technológiák anonimmá tétele. Már 1986-ban Pfitzmann és Waidner [1] is komolyan vizsgálták az anonim hálózatok kialakításának lehetőségeit és kutatásuk során olyan anonimitási tulajdonságok fogalmát vezették be, melyek mind a mai napig alapkövei egy anonimizáló szolgáltatás vizsgálatának.

2.1 Anonimitási metrikák

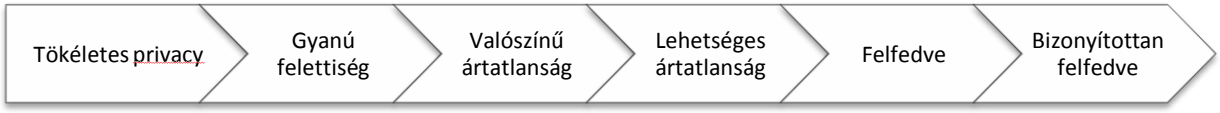
Pfitzmann és Waidner a hálózatuk tervezésekor alapvetően háromféle anonimitást különböztettek meg [1]:

Küldő anonimitás: Egy hálózat, vagy szolgáltatás akkor rendelkezik küldő anonimitás tulajdonsággal, ha egy üzenetről nem mondható meg, hogy ki a küldője

Fogadó anonimitás: Egy hálózat, vagy szolgáltatás akkor rendelkezik fogadó anonimitás tulajdonsággal, ha egy üzenetről nem mondható meg, hogy ki a címzettje

Küldő – Fogadó összeköthetetlenség: Egy hálózat, vagy szolgáltatás akkor rendelkezik küldő – fogadó összeköthetetlenség tulajdonsággal, ha a hálózatban nem állapítható meg, hogy ki kivel kommunikál. Ennek megvalósítására jó példák a MIX-ek, melyek olyan hálózati elemek, amik begyűjtenek több üzenetet, majd átkódolva és véletlenszerűen átsorrendezve bocsátják ki azokat, így akadályozva meg egy támadót egy-egy üzenet nyomon követésében. A MIX-ek képezik, bár továbbfejlesztve, a mai legelterjedtebb anonimizáló hálózatok alapját is.

1998-as munkájukban Reiter és Rubin [2] az előbbi három tulajdonságot kiegészítik egy anonimitási skálával, melyen a felhasználót elhelyezve megállapítható, hogy szolgáltatás milyen fokú anonimitást biztosít számára, így mérhetővé tették az anonimitást. Ez a skála és a főbb anonimitási fokok láthatóak az 1. ábrán.



1. ábra - az anonimitás fokozatai

A skálán a felhasználó anonimitása balról jobbra fokozatosan romlik, a bal szélen a **tökéletes privacy** az elérendő cél, amikor a felhasználó tökéletes anonimitásba burkolózva élvezheti a szolgáltatást, a felhasználó szempontjából legrosszabb kategóriák a **felfedve** és a

bizonyítottan felfedve, melyekben a támadó azonosítani tudja a felhasználót, sőt utóbbi esetben erre még bizonyítékot is fel tud mutatni. Mint tanulmányukban leírják, az internet anonimitási fokát alapértelmezésben felfedve kategóriájúnak tekinthetjük.

A gyakorlati alkalmazások szempontjából a fennmaradó három kategória a legfontosabb. Egy felhasználók anonimitása **gyanú feletti**, ha a támadó számára egy kommunikáció kezdeményezője nem megkülönböztethető a többitől. **Valószínű ártatlanság** esetén valamely felhasználó, vagy entitás valószínűbb kezdeményezője a kommunikációnak, mint bármely másik, de még mindig nagyobb az esélye annak, hogy nem ő volt, mint annak, hogy igen. **Lehetséges ártatlanság** esetén a támadó szempontjából igen valószínű, hogy megtalálta a feladót, de még mindig nem elhanyagolható annak a valószínűsége, hogy nem a meggyanúsított felhasználó a feladó.

2.2 A leggyakoribb támadómodellek

Az anonimizáló protokollok ellen több sikeresen alkalmazható támadási módszer is létezik, ezek közül a legismertebbek [3]:

Lehallgatás: A lehallgató támadó megfigyeli a hálózatban keringő üzeneteket, erősségétől függően, vagy a hálózat egészében, vagy csak egyes részein rendelkezik megfigyelési képességekkel. Ha a protokollban a résztvevő felek nem azonos mértékben küldenek, vagy fogadnak üzeneteket, akkor időzítés alapú analízissel összeköthetí a kommunikáló feleket.

Predecesszor támadás: A predecesszor támadás során a támadó, vagy támadók a fogadó felet használják kiindulási pontnak és minden befutó üzenethez igyekeznek rögzíteni a lehetséges küldők halmazát. Az a felhasználó lesz a legvalószínűbb feladó, aki ezen halmazok mindegyikében szerepel.

Sybil támadás: Sybil támadáskor a támadók igyekeznek úgy helyezkedni és cselekedni az anonimizáló hálózatban, hogy a később csatlakozó felhasználó arra kényszerüljön, hogy abba a csoportba kerüljön, melynek ő az egyetlen nem rosszindulatú tagja. Ekkor a felhasználó nyilvánvalóan kompromittálódik, hiszen a csoport tagjai el fogják tudni különíteni üzeneteit a csoport többi üzenetétől.

Szolgáltatás megtagadás: A szolgáltatás megtagadás támadás során a támadó igyekszik használhatatlanná tenni az anonimizáló szolgáltatást. Ilyen helyzetekben komoly probléma, hogy a támadó is anonim résztvevője lehet a hálózatnak, így különösen nehéz lehet megtalálni.

A következő fejezetben bemutatom azokat az anonimizáló szolgáltatásokat, melyek jelenleg a legismertebbek és a legtöbbet analizáltak is egyben, így alkalmasak lehetnek egy elektronikus kereskedelmi protokoll részeként biztosítani a az anonim kommunikációt.

3 Az anonimizáló technológiák

Ebben a fejezetben néhány olyan anonimizáló hálózatról, illetve protokollról ejtek szót, melyek más-más módon igyekeznek magvalósítani a kitűzött célt. Ezek a protokollok mind bemutatnak az olvasó számára egy-egy olyan hatékony technikát, mely sikerrel alkalmazható az anonimitás elérésére. Ezek a technikák:

- MIX-ek, illetve az azokra alapozott onion és garlic routing: ilyen a TOR és az I2P
- Rendszerben köröztetett anonim tárolók: Buses
- Étkező kriptográfusok hálózat (Dining Cryptographers Network – DCN): Herbivore
- Üzenetszórás: P^5 és Hordes
- Tömegben történő rejtőzködés: Crowds és Hordes

A bemutatandó technikák kiválasztásakor elsődleges szempont volt, hogy az a néhány kerüljön bemutatásra, melyek a legalkalmasabbak lehetnek egy elektronikus tranzakciós rendszerben az anonimitás biztosítására, elsősorban azért mert vagy általános sémát adnak meg, vagy olyan protokollokat támogatnak melyek elég sokrétűek ahhoz, hogy alapjául szolgáljanak egy anonim tranzakciónak. Fontos szempont volt még ezen felül, hogy olyan technológiák kerüljenek ismertetésre, melyeket már többen megismertek és analizáltak, ezáltal ezek a protokollok feltehetően kevesebb ismeretlen hibával, gyengeséggel rendelkeznek, mint mások. A válogatáskor szintén előnyt élveztek azok a technológiák, melyek már implementálásra is kerültek, így ez az implementáció esetlegesen már kész építőeleme lehet egy kereskedelmi protokollnak.

3.1 TOR és I2P

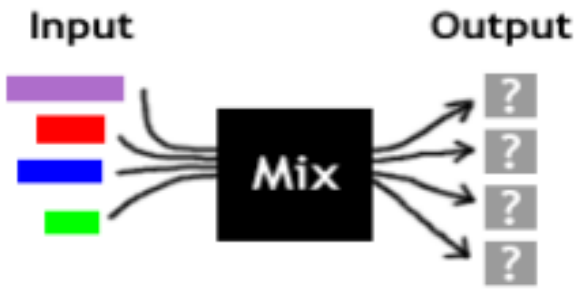
A TOR[1] [4] és az I2P[2] [5] is a Chaum által bevezetett MIX-eken [6], egészen pontosan azok továbbfejlesztésén alapul. A MIX lényege, hogy egy olyan hálózati csomópontot valósítson meg, mely begyűjti az üzeneteket, majd átkódolva és átsorrendezve bocsájtja ki őket magából, így rejtve el a küldő és fogadó közötti kapcsolatokat (2. ábra). Ilyen elemeken alapul Chaum anonimizáló hálózata.

2004-ben publikálták a Tor hálózat technikai specifikációját, mely a MIX technológián alapulva úgynevezett onion routing alkalmazásával épített ki anonimizáló hálózatot. Az onion routing lényege, hogy a küldő előre kiválasztja, hogy a hálózatnak mely csomópontjain szeretné átküldeni üzenetét, majd az üzenetet rétegesen, mint a hagyma rétegeit kódolja az egyes csomópontok kulcsaival (3. ábra). Amikor a csomag megérkezik egy csomópontba, az lefejti a neki szóló réteget, majd így megtudva a következő csomópont címét továbbküldi annak a csomagot.

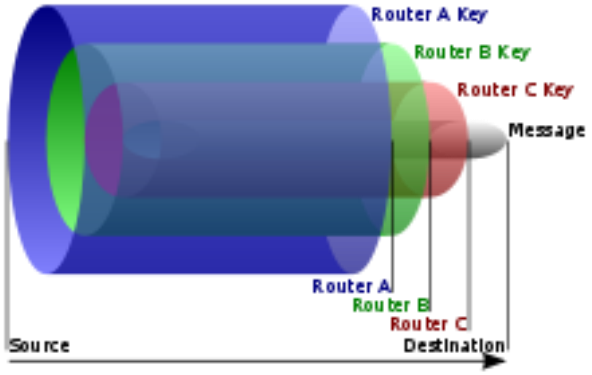
[1] https://www.torproject.org/
[2] http://www.i2p2.de

Az átviteli késleltetés csökkentésére a Tor csomópontok nem feltétlen várják meg, míg kellően nagy mennyiségű csomag gyűlik össze ahhoz, hogy kibocsájtáskor a csomópontot elhagyó csomagok sorrendje kellően véletlenszerű legyen, ugyanakkor igyekeznek palástolni a csomag méretét egy véletlen hosszúságú padding alkalmazásával. A Tor lehetőséget biztosít anonim szolgáltatásnyújtásra is, anonim módon kapcsolva össze a klienst a szerverrel. A Tor jelenleg a legismertebb és legelterjedtebb anonimizáló hálózat.

Az I2P a Torhoz nagyon hasonló struktúrát követ, azonban csomópontjai és hálózata nem onion routingot alkalmaz, hanem garlic routingot. A garlic routing lényege, hogy az egy irányba továbbítandó üzeneteket nem egyesével bocsájtja ki magából, hanem azokat egyesíti egy nagyobb titkosított üzenetbe. Egy garlic router a beérkező garlicokat szétbontja üzenetekre, majd azokból újabb garlicokat képez és azokat bocsájtja ki magából. Ez a megoldás még nehezebbé teszi az egyes, individuális üzenetek nyomon követését a hálózatban.



2. ábra - a MIX működése [3]



3. ábra - az onion routing[3]

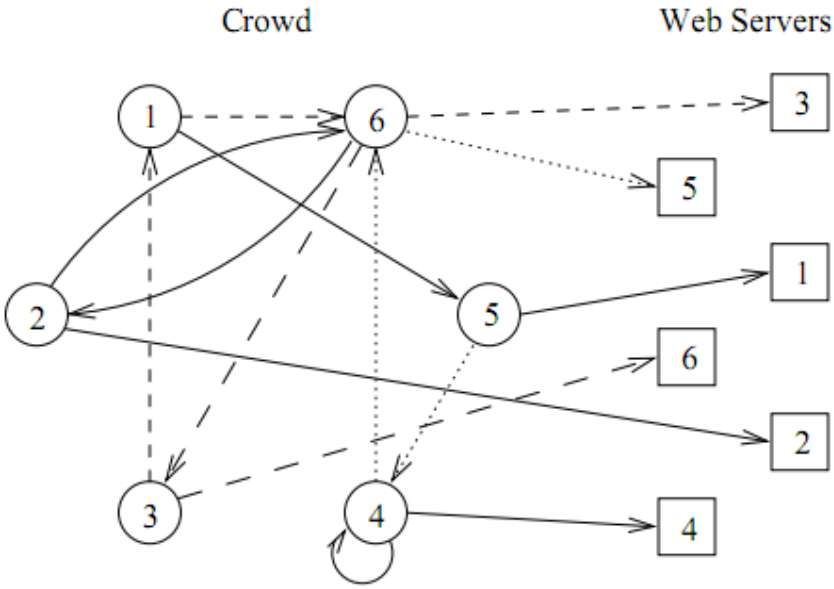
3.2 Crowds és Hordes

A Crowds [2] alapja egy nagy felhasználói halmaz, melyben a protokoll futása az alábbi. Amikor a felhasználó csatlakozik a csoporthoz a központi entitástól lekéri a csoport tagjainak listáját. Mivel a csoportban mindenki egyenértékű és egyformának látszik, ezért a szerzők az egyes node-okat „jondo”-nak nevezik (utalva a John Doe elnevezésre).

Ha az egyik jondo kapcsolatba szeretne lépni egy szolgáltatással, akkor kérését átküldi egy véletlenszerűen választott társának. A másik jondo ekkor feldob egy súlyozott pénzérmét és a dobás kimenetelétől függően vagy továbbítja a kérést a szervernek, vagy továbbadja egy következő jondónak, melyet ő is véletlenszerűen választ ki a tömegből (Akár saját magát is választhatja!). Ilyen módon a kérés véletlenszerűen sok jondón keresztül előbb-utóbb eléri a szervert, aki képtelen lesz megállapítani, hogy kitől eredeztethető a kérés. (4. ábra)

[3] forrás: http://en.wikipedia.org/wiki/Onion_routing

Az üzenet továbbítása közben a jondók rögzítik, hogy kitől kapták a csomagot a szerver pedig a láncban utolsó jondóhoz kapcsolódva küldi a válaszát, amit a rögzített láncban visszafelé továbbítva az eléri a kezdeményező kliens.



4. ábra - A Crowds működése [2]. Az azonos mintázatú nyilak egy kapcsolat útvonalát jelölik. (1→5→server; 2→6→2→server; 3→1→6→server; 4→4→server; 5→4→6→server; 6→3→server;)

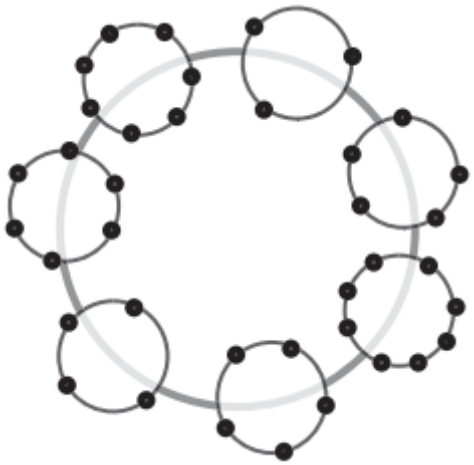
A Hordes [7] megoldása nagyban hasonlít a Crowdshoz, azonban néhány nagyon értékes fejlesztést tartalmaz ahhoz képest. Míg a Crowds, bár sémája általános, elsősorban http protokollhoz van tervezve, ezt támasztja alá meglévő implementációja a JonDo és a JonDoFox[4] is., addig a Hordes UDP kapcsolatokat használ, így általánosabb megoldásnak tekinthető. Ezen felül a Hordes nem rögzíti az egyes kapcsolatokhoz a válaszutakat, így tehermentesítve a hálózati csomópontokat, hanem az válaszcím helyére multicasting címet helyez el, így a szerver a választ többeknek elküldi, melyek között valahol megbújik a valódi címzett is.

3.3 Herbivore

A Herbivore [8] protokoll a DC-Net [9] elvén alapul és így anonimitást biztosít mind a küldőnek, mind a fogadónak. A DC hálózatok alapvető működési elve a következő. Tegyük fel, hogy a hálózatban három résztvevő van, Alice, Bob és Charlie. Bob szeretne átküldeni 1 bit információt Charlienak anonim módon. Ehhez Alice és Bob titkosan feldobnak egy pénzérmét, majd Alice elmondja a dobás eredményét Charlienak, Bob pedig, attól függően, hogy egyet vagy nullát szeretne küldeni, vagy hazudik a dobás eredményéről, vagy igazat mond. Charlie összeveti a két választ, ha egyeznek, akkor az üzenet nulla, ha különböznek, akkor egy. Charlie tehát hozzájutott az egy bit információhoz, ugyanakkor nem képes megmondani, hogy Alice, vagy Bob volt e a küldő.

[4] Mindkét alkalmazás elérhető a https://anonymous-proxy-servers.net/en/software.html címen

A Herbivore rendszernek két kulcskomponense van az egyik a *round protocol,* amely a bitek küldésének megszervezéséért és így az ütközések elkerüléséért felelős, valamint a *global topology control protocol*, amely a hálózat topologikus szervezésért felelve garantálja a megfelelő skálázhatóságot. A belépő klienseket kisebb csoportokba szervezi és ezeket a csoportokat fűzi fel egy gyűrű topológiájú kommunikációs hálózatra. Ennek a struktúrának a kialakítását azt tette szükségessé, hogy a DC-Net-ek hatékonysága a részvevő elemek számának növekedésével fokozatosan csökken, így ha egy csoport túl nagyra nőne, a GTC protocol szétválasztja az, több kisebb csoportra. A Sybil támadások elkerülésére a protokoll garantálja, hogy a belépő kliensek véletlenszerűen kerülnek besorolásra.



5. ábra - A Herbivore topológiája[8]

A csoportokba sorolás az alábbi módon történik. Amikor egy node csatlakozni kíván a hálózathoz, generál egy publikus-privát kulcspárt. Ezt követően keres egy olyan *y* vektort, amely nem egyezik meg publikus kulcsával, azonban egy, a rendszerben definiált egyirányú függvényre nézve $f(K_{publikus})$ és f(y) alsó néhány bitje megegyezik. Ekkor a node meghatározza a $g(K_{publikus},y)$ egyirányú függvény kimenetét és ahhoz a csoporthoz csatlakozik, melynek csoportkulcsához ez az érték a legközelebb esik. Csatlakozáskor felfedi $K_{publikus}$ és y vektorokat, így a csoport többi tagja ellenőrizheti, hogy a megfelelő helyre csatlakozott e.

Az egyes klikkek belül egy logikailag teljes, fizikailag csillag topológiájú szervezés garantálja a DC-Net működését. Egy anonim bit küldéséhez minden résztvevő, minden más résztvevővel közös kulcsával meghajt egy véletlenszám generátort, amely egy egyes, vagy nulla bitet ad ki. Mindenki összeadja a kisorsolt kulcsokat és hozzáadja azt az egy bites üzenetet amelyet küldeni szeretne. Az így kialakuló paritás értéket broadcastolja a hálózatba. Ha az akinek adási joga volt ebben a körben hazudik a paritásról, akkor az üzenetek összege egy lesz, ekkor a küldött bit is egy, ellenkező esetben az összeg és így az üzenet is nulla.

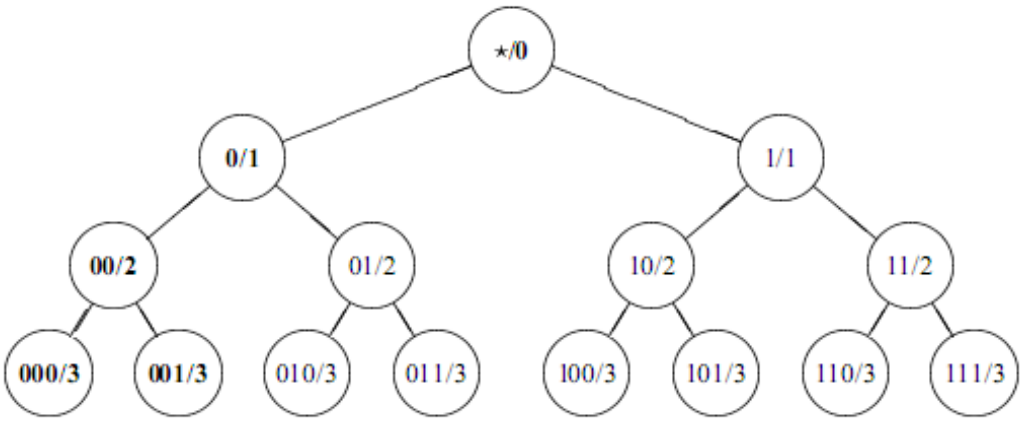
A Herbivore protokollnak létezik gyakorlati megvalósítása is, azonban ez csak a teljes felhasználhatóságnak egy szűk esetét fedi le, a Carnivores [10] ugyanis egy Herbviore-on alapuló anonim fájlcserélő alkalmazás.

3.4 P^5

A P^5 [11] egy üzenetszóráson alapuló hálózat kiépítésével biztosítja a küldő-, fogadó anonimitást és az összeköthetetlenséget. Az üzenetszórás hatékonyságának növelésére a felhasználókat csoportokba szervezi, ezeket a csoportokat pedig egy bináris fa struktúrában

helyezi el. Minden node-nak rendelkeznie kell egy publikus-privát kulcspárral és a küldő erre a hierarchiára alapozva építi ki az üzenetszórás csatornáját.

A bináris fa struktúrája a 6.ábrán látható. A fa minden egyes csomópontja egy b/m azonosítóval jelölt üzenetszórási csoport, ahogy b egy bináris sorozat, m pedig annak a mérőszáma, hogy b sorozat első hány bitje érvényes. Amikor egy kliens csatlakozik a hálózathoz, publikus kulcsa alapján generál egy b sorozatot, majd maga választ hozzá egy m mintahosszat, így elfoglalja helyét a b/m csoportban.



6. ábra - A P^5 csoportjainak struktúrája [11]. Félkövérrel kiemelve a 00/2 csoportnak címzett üzenet által elért csoportok

Amikor egy node üzenetet küld egy másiknak, b/m csoportba, akkor az üzenet a az alábbi csoportoknak kerül kézbesítésre:

- **Lokális csoport:** az üzenetet az b/m csoport minden tagja megkapja
- **Csoportok a gyökér felé**: az üzenetet megkapja minden olyan b'/m' csoport, ahol b' első m' bitje megegyezik b első m' bitjével, ahol m'<m. Ezek pont azok a csoportok, melyek a gyökérből b/m-be vezető úton helyezkednek el
- **Részfa csoportok:** az üzenetet megkapja minden olyan csoport, mely a fában az b/m gyökerű részfában helyezkedik el, vagyis azon b''/m'' csoportok, ahol b'' első m bitje megegyezik b első g bitjével, ahol m''>m

Így ha két tag kommunikálni akar egymással, akkor nincs más dolguk, mint meghatározni azt az f'/g' csoportot, melynek címzett üzeneteket mindketten megkapják, így oda küldve az üzeneteket olyan üzenetszórást valósíthatnak meg, melynek mindketten részei, így anonim módon kommunikálhatnak.

Ehhez a másik fél publikus kulcsát használják fel, mégpedig úgy, hogy a küldő fél a cél node publikus kulcsa alapján kiszámítja annak b értékét, majd egy nagy m-ről indítva a keresést üzenetet küld b-nek. Ha nem kap választ, akkor az üzenet nem érte el a másik felet, így újraküld egy kisebb m-mel. Ilyen módon addig csökkenti m-et míg fel nem tudja venni a kapcsolatot a másik féllel. Ilyen módon megvalósítva egy anonimitás szempontjából kellően

nagy, az üzenetküldés hatékonysága szempontjából pedig remélhetőleg a teljes hálózatnál kisebb létszámú csoportot kell csak terhelni az üzenetszórással.

A P^5 nagy előnye tehát, hogy képes kihasználni a multicast/broadcast küldés előnyeit, ugyanakkor lokalizálva azok hatását, így csökkentve hálózati terhelést. Ugyanakkor sajnos nagy a valószínűsége annak, hogy a két kommunikáló fél a fának külön főágába kerül, így a */0, tehát a teljes broadcast lesz az egyetlen közös csoportjuk. Ennek megoldására a szerzők azt ajánlják, hogy egy virtuálisan több helyen is csatlakozzon a fához.

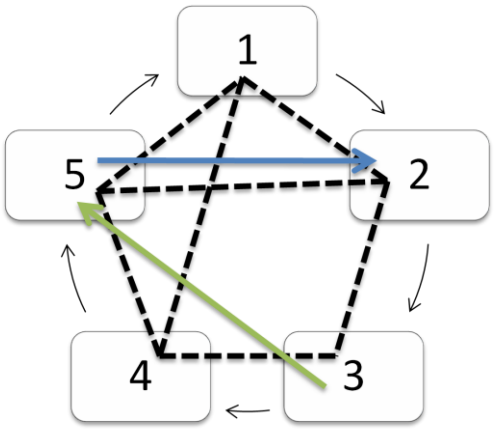
3.5 Buses

A Buses [12] protokoll az anonimizálás során a tömegközlekedés alapvető tulajdonságait aknázza ki, miszerint az utakon közlekedő buszok a külső szemlélők számára nehezen megkülönböztethetőek, még akkor is ha „tartalmuk” egészen más.

A protokollban olyan tárolók, buszok, keringenek a hálózatban, melyek üléseire helyezhetik el a csomópontok az üzeneteiket, illetve ezen székeken találhatják meg a nekik címzett üzeneteket is. A protokoll több optimalizációra is lehetőséget ad, attól függően, hogy a kommunikáció számítási, vagy időbeli költségét szeretnénk minimalizálni.

Az optimális számítási költséget jelentő megoldásban a csomópontok gráfjában egy kör mentén mindösszesen egy busz kering, melynek N^2ülése van, ha a csomópontok száma N. A busz b_{ij} ülésén kap helyet azon üzenet, melyet az i. csomópont kíván küldeni a j.-nek. Amikor a busz megérkezik az i. csomópontba, az az i. sorban található összes széket módosítja, vagy hamis adattal, vagy a j. csomópontnak küldendő adattal feltöltve azt. Természetesen a székékre mindig titkosított formában kerülnek az üzenetek. Szintén a busz megérkezésekor megvizsgálja az i. oszlopot is, mely a neki küldött üzeneteket tartalmazza (7.ábra).

	1	2	3	4	5
1	-				
2		-			
3			-		
4				-	
5					-



7. ábra - A Buses protokoll "busza" a legkisebb kommunikációs költséggel járó esetben

A legkisebb időbeli költségű esetben minden kapcsolaton mindkét irányban található egy busz a csomópontok pedig a buszok között mozgatják az üléseket úgy, hogy az egyes ülések mindig a két kommunikáló fél közötti legrövidebb úton mozogjanak. A szerzők a protokollt

bemutató írásukban megmutatják a két véglet közötti skálázás lehetőségeit, valamint néhány további optimalizációt is.

A Buses protokoll nagy előnye, hogy nem használja ki a hálózati kommunikáció statisztikai tulajdonságait, így nincs szükség folyamatos álforgalom generálására, illetve a hálózat broadcast üzenetekkel történő terhelésére. A legkisebb kommunikációs költséggel rendelkező esetben például egyszerre csak egy csomópont dolgozik. Természetesen az időbeli hatékonyság növelésével a hálózat terhelése is nő.

4 Összegzés

Láthatjuk tehát, hogy a jelenleg elérhető anonim kommunikációs technológiák, bár magas fokú elméleti anonimitást biztosítanak a gyakorlatban több olyan problémájuk is van, mely egy éles rendszerben való felhasználhatóságukat erősen korlátozza. Kereskedelmi felhasználás szempontjából nagyon komoly probléma a protokollok jellemzően nagy késleltetése, mely egy egy kereskedelmi tranzakciót túl hosszúra nyújthat, valamint a hálózat által generált nagy számítási, illetve forgalomterhelés, mely az esetek többségében szükséges a megfelelő anonimitáshoz.

Ezekből engedve egy használhatóbb, de támadhatóbb hálózathoz jutunk, erre kiváló példa jelenleg a Tor, melynek tervezői nem akartak nagy számú hamis üzenetet generálni, sem várni elegendő beérkező üzenetre és ezen tervezői döntésük hatására a rendszer biztonsága, ha nem is drasztikusan, de csökkent.

Láthatjuk az is, hogy ezen protokollok közül csak néhánynak van működő implementációja és azok közül is a többség még kiforratlan, illetve nem rendelkezik megfelelő felhasználói bázissal. Sok országban a csomópontok felállítása jogi akadályokba is ütközhet, hiszen egyes bíróságok előtt nehézkes lehet bizonyítani, hogy egy, a számítógépről indított támadást nem a számítógép tulajdonosa hajtott végre, hanem az eszközön futó, például Tor, kilépési ponton keresztül támadott egy anonim ismeretlen és a tulajdonos nem felelős azért, amit mások az ő számítógépén keresztül tesznek.

Összegzésként elmondhatjuk, hogy a jelenleg elérhető általános célú anonimizációs technológiák még nem rendelkeznek azokkal a tulajdonságokkal, melyek ahhoz lennének szükségesek, hogy hatékony alapjait képezzék valós szolgáltatásoknak, azonban fejlődésük azt mutatja, hogy a jövőben várhatóan meg fognak majd jelenni olyan technológiák, melyek nem csak az elméleti, hanem az ipari felhasználás követelményeinek is meg fognak felelni, így többek között képesek lesznek hatékonyan biztosítani az elektronikus kereskedelmi protokollok számára az anonimitást.

5 Irodalomjegyzék

1. **Pfitzmann, Andreas és Waidner, Michael.** Networks Without User Observability. *EUROCRYPT 1985.* 1986.

2. **Reiter, Michael K. és Rubin, Aviel D.** Crowds: Anonymity for web transactions. *ACM Transactions on Information and System Security.* 1998.

3. *Anonymous communication on the Internet.* **Jones, Andy.** 2004.

4. **Dingledine, Roger, Mathewson, Nick és Syverson, Paul.** Tor: The Second-Generation Onion Router. *13th USENIX Security Symposium.* 2004.

5. I2P Official Page. *Introducing I2P.* [Online] [Hivatkozva: 2010. 11 20.] http://www.i2p2.de/techintro.html.

6. **Chaum, David L.** Untraceable electronic mail, return adresses, and digital pseudonyms. *Communications of the ACM.* 1981.

7. **Levine, Brian Neil és Shields, Clay.** Hordes: A multicast based protocol for anonymity. *Journal of Computer Security .* 2002.

8. **Goel, Sharad, és mtsai.** Herbivore: A Scalable and Efficient Protocol for Anonymous Communication. *Cornell University technical report 2003-1890.* 2003.

9. **Chaum, David.** The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. *Journal of Cryptology.* 1988.

10. **Sirer, Emin Gün, és mtsai.** Eluding carnivores: file sharing with strong anonymity. *ACM SIGOPS European workshop.* 2004.

11. **Sherwood, Rob, Bhattachrjee, Bobby és Srinivasan, Aravind.** P5: A Protocol for Scalable Anonymous Communication. *Proceedings of the 2002 IEEE Symposium on Security and Privacy.* 2002.

12. **Beimel, Amos és Dolev, Shlomi.** Buses for Anonymous Message Delivery. *Journal of Cryptology.* 2003.

13. **Dazenis, George és Diaz, Claudia.** *A Survey of Anonymous Communication Channels.* 2008. MSR-TR-2008-35.