MEGFIGYELHETŐ BLACK-BOX CSATORNA FORRÁSREJTŐ TULAJDONSÁGA

Tóth Gergely, Hornák Zoltán
Budapesti Műszaki és Gazdaságtudományi Egyetem
{tgm, hornak}@mit.bme.hu

Az anonim átviteli protokollok elemzéséhez bevezethető megfigyelhető, black-box csatorna modellje alapján a cikkben meghatározásra kerül, hogy egy passzív megfigyelő milyen bizonyossággal képes kézbesített üzeneteket küldőjükhöz visszakövetni, azaz az anonimitást kompromittálni. Ezek alapján definiálni fogjuk a forrásrejtő tulajdonságot, melyet az elérhető anonimitás objektív mértékének lehet tekinteni. Végül kimondjuk mind a protokollt megvalósító csatorna, mind pedig az üzeneteket küldő entitásokra vonatkozóan azokat a követelményeket, melyek betartása esetén a megfigyelő bizonyossága meghatározható szint alá csökkenthető, azaz garantált minőségű anonimitás biztosítható.

Kulcsszavak: anonimitás, Onion Routing, MIX-net

Bevezetés

Az anonim átviteli protokollok (mint például a MIX-net [1] vagy az Onion Routing [2] [3]) gyökeresen meg fogják változtatni az anonim üzenetküldés gyakorlatát. Céljuk, hogy az alsóbb szintű hálózati rétegtől függetlenül biztosítsák, egy kézbesített üzenetet ne lehessen a küldőjével kapcsolatba hozni. Ezen protokollok kutatása, tervezése folyamatban van, azonban elméleti elemzésük és leírásuk még nem teljes.

A következőkben ismertetett forgatókönyv alkalmazási területének egy anonim orvosi tanácsadó rendszert választottunk. A betegek kérdéseiket a megfelelő orvosnak email formájában teszik fel. Az anonim átviteli protokoll feladata a kérdés eljuttatása az orvoshoz úgy, hogy kézbesítéskor ne lehessen kideríteni, ki kinek, milyen témában tette fel a kérdését. Az orvosok a kérdésekre nyilvános fórumon, például egy honlapon válaszolnak. Amennyiben az anonimitást kompromittálni lehetne, a kérdések tartalmából egy kérdező betegségeire is következtetni lehetne, amit el szeretnénk kerülni, különösen ha érzékenyebb témakörök (pl. szexuális, kábítószeres problémák) is felmerülhetnek. Természetesen az anonim átviteli protokollok nem csak erre a példára használhatók, alkalmazhatók anonim elektronikus szavazásra, vásárlásra vagy csak egyszerű elektronikus levelezésre is. A fenti példa, ahol a kérdések és az orvosi válaszok is nyilvánossá válnak és csak a kérdezők kiléte titkos, nagyon jól reprezentálja a vizsgált anonimitási követelményeket.

Ebben a cikkben ilyen protokollok leírására bevezetésre kerül a megfigyelhető black-box csatorna modellje. A bemutatott vizsgálat tárgyát az képezi, hogy egy csupán lehallgatásra képes megfigyelő milyen következtetéseket vonhat le pusztán az események bekövetkeztének időpontjait ismerve. A modellben definiálható a forrásrejtő tulajdonság, mely az anonimitás fogalmának egy elméletileg megalapozott mértéke. Végül ismertetésre kerül az a feltételrendszer, amelynek teljesülése esetén a megfigyelő bizonyosságát a lehető legkisebbre lehet csökkenteni és így a lehető legmagasabb fokú anonimitást lehet elérni.

A megfigyelhető black-box csatorna modellje

Vizsgálatainkhoz azért ezt a modellt választottuk, mert ebben lehet az egész átviteli rendszert egyszerűen, mégis a számunkra érdekes tulajdonságok szem előtt tartása mellett elemezni:

- A csatorna black-box, mert az egészét vizsgáljuk, a belső implementációs sajátságokat figyelmen kívül hagyjuk. A megfigyelő nem láthatja, mi történik az üzenetekkel a csatorna belsejében, hogy kerülnek ezek továbbküldésre illetve átkódolásra.

- A csatorna teljesen megfigyelhető, azaz egy lehetséges megfigyelő érzékelheti a csatornába bemenő és az azt elhagyó üzeneteket [4]. Erre azért van szükség, mert egyrészt a kriptográfiával szemben az események időzítésének fontosságára szeretnénk felhívni a figyelmet, másrészt az elvi megfontolások alapján kimondott felső korlátok a gyakorlatban előforduló részleges megfigyelhetőség mellett is érvényesek maradnak.
- Továbbá a csatornán áthaladó üzenetekről feltesszük, hogy azonos méretűek és megfelelően titkosítottak, így a megfigyelő csak az események bekövetkeztének időpontjából képes következtetéseket levonni.

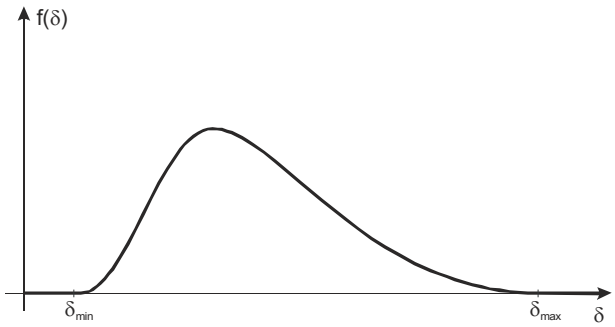
A környezet leírása

Jelölje S a küldők halmazát, R a fogadókét, míg M az üzenetek halmazát. Jelölje továbbá $S(m_i)$ az m_i üzenet küldőjét, $R(m_i)$ az m_i üzenet fogadóját, $t_S(m_i)$ az m_i üzenet elküldésének, $t_R(m_i)$ pedig a fogadásának időpontját. A rendszer folytonos időben működik, ugyanazon időpillanatban nem történhet két különböző esemény. Az üzenet továbbításának idejét a küldő és a csatorna, valamint a csatorna és a fogadó között nem vesszük figyelembe. Ezt az egyszerűsítés kedvéért vezettük be, a végkövetkeztetést érdemben nem befolyásolja. Az orvosi kérdez-felelek példánk értelmében S a betegeket jelöli, R az orvosokat, míg M a feltett kérdések halmazát.

A csatorna meghatározása

A csatorna az üzenetek továbbítására szolgál, a csatornán belül nem születik új üzenet, valamint a csatorna nem dob el beérkezett üzenetet. Egy beérkezett üzenet a következő szabályok szerinti késleletetés után kerül kézbesítésre:

- a késleltetés δ valószínűségi változó, adott $f(\delta)$ sűrűségfüggvénnyel, $\delta = t_R - t_S$, ahol δ üzenet- és időinvariáns;
- a csatorna minden üzenetet egy előre meghatározott konstans, üzenet- és időinvariáns $\delta_{\max}$ (time-to-live) késleltetésen belül, de legalább egy konstans, üzenet- és időinvariáns $\delta_{\min}$ (minimális késleltetés) elteltével kézbesít, azaz $\forall_{m_i}[\delta_{\min} < t_R(m_i) - t_S(m_i) < \delta_{\max}]$.



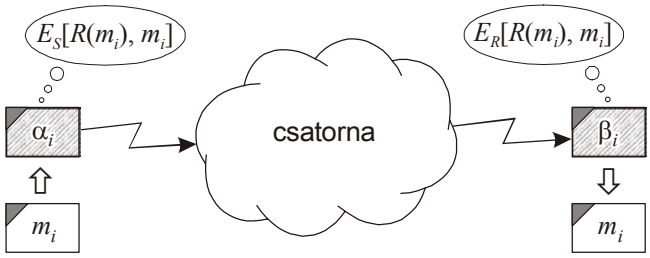
1. ábra – A csatorna késleltetésének $f(\delta)$ sűrűségfüggvénye

A C csatornát így az $f(\delta)$, $\delta_{\min}$, $\delta_{\max}$ paraméterekkel jellemezhetjük. A példa szerint a csatorna feladata a betegek által feltett kérdések eljuttatása az orvosokhoz úgy, hogy a kézbesítéskor már ne lehessen kideríteni, a kérdést ki tette fel, illetve hogy egy feltett kérdés melyik szakterületű orvosnak szól.

Üzenetküldés

A következőkben feltesszük, hogy $s_a \in S$, $s_a = S(m_i)$ küldő $m_i \in M$ üzenetet küld $r_b \in R$, $r_b = R(m_i)$ fogadónak. Az m_i üzenet a csatornába a titkosított $\alpha_i := E_S(r_b, m_i)$ formában $t_S(m_i) = t_S(\alpha_i)$

időpontban érkezik meg, míg a fogadóhoz egy más kulccsal titkosított $\beta_i := E_R(r_b, m_i)$ formában $t_R(m_i) = t_R(\beta_i)$ időpontban fog megérkezni.



2. ábra – Üzenetküldés a csatornán keresztül

Azt is feltesszük, hogy E_S és E_R tökéletes titkosítás, így α_i-t csak a csatorna, míg β_i-t csak r_b tudja dekódolni, azaz $I[E_S(r_b, m_i), (r_b, m_i)] = 0$ és $I[E_R(r_b, m_i), (r_b, m_i)] = 0$ (ahol I a kölcsönös információtartalmat jelöli). További elemzést érdemel annak eldöntése, hogyan változnak az ebben a cikkben levont következtetések, ha az elméletileg tökéletes titkosítót egy gyakorlati értelemben vett erős titkosítóra cseréljük. Feltehetően ez nem jelent majd érdemi változást megfelelően erős gyakorlati rejtjelezés esetén; a modellben megfogalmazott ideális rejtjelezés azonban jelentősen egyszerűsíti a matematikai elemzést.

Példánkban a titkosításra azért van szükség, mert amennyiben a kérdések nyílt szövegként kerülnének továbbításra, úgy egy megfigyelő a csatorna be- és kimeneteit lehallgatva pontosan kideríthetné, ki melyik kérdést tette fel.

A megfigyelő

Vizsgáljuk meg egy passzív megfigyelő lehetőségeit ebben a modellben, aki csak lehallgatni tudja a titkosított üzeneteket, azokat nem tudja dekódolni (csak ha neki küldték), valamint azokat sem módosítani, sem elnyelni, sem visszajátszani, sem késleltetni* nem áll módjában. A megfigyelő célja, hogy a kézbesített üzeneteket (β_i-k) a küldőkhöz rendelje – vagy legalább is az összetartozást minél nagyobb valószínűséggel megtippelje – és így megmondja, ki kivel kommunikál.

Aktív támadót feltételezve, aki ha üzenetet értelmesen módosítani nem is, de üzenetet késleltetni tud, a levont következtetések sajnos nem érvényesek. Ez a lehetőség további elemzést, kutatást érdemel, de túlmutat jelen cikk tartalmán.

A megfigyelő ismeretei

A megfigyelőről feltételezzük, hogy képes a csatorna minden kimenetét megfigyelni, azaz ismeri a csatornába érkezett titkosított üzeneteket, azok küldési időpontját, a csatornát elhagyó titkosított üzeneteket, azok kézbesítési időpontját, valamint a csatorna paramétereit és környezetét. Ennek megfelelően a megfigyelő a következőket ismeri:

- a csatorna környezetét (S, R) és paramétereit ($f(\delta)$, $\delta_{\min}$, $\delta_{\max}$);
- $\varepsilon_S := \{\alpha_i := E_S[S(m_i), m_i]\}$ és $\vartheta_S := \{t_S(\alpha_i)\}$ – a csatornába érkezett üzeneteket, valamint érkezésük időpontját;
- $\varepsilon_R := \{\beta_i := E_R[R(m_i), m_i]\}$ és $\vartheta_R := \{t_R(\beta_i)\}$ – a csatornát elhagyó üzeneteket, valamint kézbesítésük időpontját.

Feltehető továbbá, hogy a megfigyelő lehet az egyik küldő, vagy az egyik fogadó is. Amennyiben a megfigyelő az egyik fogadó, úgy ismeri az összes neki küldött üzenet tartalmát és tipikusan ezekről

* Vegyük észre, hogy az anonimitás megsértése érdekében a támadó a klasszikus manipuláláson túl az üzenetkésleltetés módszerével is élhet.

szeretné kideríteni, hogy ki küldte őket. Azonban mivel E_S tökéletes titkosító függvény és független E_R-től, így egy ilyen fogadó-megfigyelő sem jut olyan többlet információhoz, ami a következőkben levont következtetéseket befolyásolná.

Jelölje Ψ a rendszer történetét, amit a következő paraméterek határoznak meg: C, S, R, ε_S, ε_R, ϑ_S, ϑ_R. A továbbiakban levont következtetéseknél feltételezzük, hogy a megfigyelő a rendszer teljes Ψ történetét ismeri, azaz minden lehetséges számára elérhető információt a rendszer működésének teljes időszakában képes megfigyelni. Mint látni fogjuk, még ilyen esetben is jelentősen lecsökkenthető annak esélye, hogy egy üzenet feladóját vissza lehessen követni.

Példánk szerint a megfigyelő célja annak kiderítése, melyik kérdést ki tette fel. Ehhez feltesszük, hogy legrosszabb esetben minden kommunikációs csatornát le tud hallgatni. A megfigyelő szándéka az egyszerű zsarolástól a globális adatgyűjtésig bármilyen ok lehet.

A megfigyelő bizonyossága

Legyen a rendszer egy konkrét története $\Psi^* := (C^*, S^*, R^*, \varepsilon_S^*, \varepsilon_R^*, \vartheta_S^*, \vartheta_R^*)$. Annak érdekében, hogy el lehessen dönteni, melyik üzenetet ki küldte, minden β_k^* titkosított kézbesített üzenethez és minden lehetséges s_l^* küldőhöz meghatározható az a valószínűség, amely megadja, mekkora eséllyel lehetett s_l^* a β_k^* üzenet küldője. A megfigyelő ismeretei alapján így β_k^* üzenetet az s_l^* küldő ezzel a meghatározható $P_{\beta_k^*, s_l^*, \Psi^*}$ valószínűséggel küldte.

Jelölje $\mu_{\beta_k^*, \Psi^*}$ azon α_j^* titkosított elküldött üzenetek halmazát, melyek az $f^*(\delta)$ sűrűségfüggvény tulajdonságainak figyelembevételével egyáltalán β_k^*-ként elhagyhatták a csatornát (1). Jelölje továbbá $\eta_{\beta_k^*, s_l^*, \Psi^*}$ azon $\mu_{\beta_k^*, \Psi^*}$-beli α_j^*-ket, melyeket s_l^* küldött (2). Azaz:

$$\mu_{\beta_k^*, \Psi^*} := \{\alpha_j^* \mid [t_R(\beta_k^*) - \delta_{\max}^*] \le t_S(\alpha_j^*) \le [t_R(\beta_k^*) - \delta_{\min}^*]\} \tag{1}$$

$$\eta_{\beta_k^*, s_l^*, \Psi^*} := \{\alpha_j^* \mid [\alpha_j^* \in \mu_{\beta_k^*, \Psi^*}] \wedge [S(\alpha_j^*) = s_l^*]\} \tag{2}$$

Amennyiben a megfigyelő a kézbesített üzenet $\rightarrow$ küldő összerendelést minden β_k^* kézbesített üzenetre függetlenül – pusztán a csatorna késleltetési karakterisztikája alapján – végzi, úgy a következő képlet adja $P_{\beta_k^*, s_l^*, \Psi^*}$-t:

$$P_{\beta_k^*, s_l^*, \Psi^*} = P[S(\beta_k^*) = s_l^* \mid \Psi = \Psi^*] = \frac{\sum\limits_{\substack{\forall [\alpha_i^* \in \eta_{\beta_k^*, s_l^*, \Psi^*}] \\ \alpha_i^*}} f^*[t_R(\beta_k^*) - t_S(\alpha_i^*)]}{\sum\limits_{\substack{\forall [\alpha_j^* \in \mu_{\beta_k^*, \Psi^*}] \\ \alpha_j^*}} f^*[t_R(\beta_k^*) - t_S(\alpha_j^*)]} \tag{3}$$

A megfigyelő természetesen a legvalószínűbb küldőt keresi, ahol $P_{\beta_k^*, \Psi^*} := \max\limits_{s_l^*} P_{\beta_k^*, s_l^*, \Psi^*}$.

Ezek alapján a megfigyelő minden kérdéshez a (3)-as képlet alapján kiszámolja annak valószínűségét, hogy egy adott kérdést egy adott beteg tett fel. Majd ezen valószínűségek alapján megtippeli, ki lehetett a kérdést feltevő tényleges beteg.

Forrásrejtő tulajdonság

A rendszer $\Psi = (C,\ S,\ R,\ \varepsilon_S,\ \varepsilon_R,\ \vartheta_S,\ \vartheta_R)$ története forrásrejtő tulajdonságú Θ paraméterrel, amennyiben semelyik β_k titkosított kézbesített üzenethez sem tud a megfigyelő Θ-nál nagyobb valószínűséggel küldőt hozzárendelni:

$$\forall_{\beta_k \in \varepsilon_R} P_{\beta_k, \Psi} \le \Theta \tag{4}$$

A MIN/MAX-tulajdonság

Annak érdekében, hogy a forrásrejtő tulajdonságot alapvetően befolyásoló (3)-as képlet konkrét értékeit garantáltan a legrosszabb esetben is egy határ alá lehessen szorítani, az üzenetküldések között eltelt időre megkötéseket kell tenni:

- A tört számlálójában levő összegzést minél kisebb halmazon kell elvégezni. Ennek érdekében a küldők nem küldhetnek bizonyos időintervallumon belül egynél több üzenetet.
- A tört nevezőjében levő összegzést minél nagyobb halmazon kell elvégezni. Ennek érdekében a küldőknek bizonyos időintervallumon belül legalább egy üzenetet kell küldeniük. (Ha ez máshogy nem érhető el, akkor a küldőnek véletlenszerűen választott fogadóknak üres üzenetet kell küldeniük.)

A fenti megkötéseket figyelembe véve a rendszer $\Psi = (C, S, R, \varepsilon_S, \varepsilon_R, \vartheta_S, \vartheta_R)$ története MIN/MAX-tulajdonságú $\tau_{\min}$, $\tau_{\max}$ paraméterekkel ($\tau_{\min} \le \tau_{\max}$), ha teljesül, hogy semelyik küldő sem küld $\tau_{\min}$ időn belül két üzenetet (5) és minden küldő küld $\tau_{\max}$ időnként (vagy azon belül) legalább egy üzenet (6):

$$\bigvee_{s_l \in S} \bigvee_{\alpha_j | S(\alpha_j)=s_l} \xi_{s_l,\alpha_j} = \varnothing \tag{5}$$

$$\bigvee_{s_l \in S} \bigvee_{\alpha_j | S(\alpha_j)=s_l} \neg(\zeta_{s_l,\alpha_j} = \varnothing) \tag{6}$$

Ahol ξ_{s_l,α_j} azon elküldött titkosított üzenetek halmaza, melyeket az s_l küldő α_j elküldése után legfeljebb $\tau_{\min}$ idő elteltével küldött (7), valamint ζ_{s_l,α_j} azon elküldött titkosított üzenetek halmaza, melyeket az s_l küldő α_j elküldése után legfeljebb $\tau_{\max}$ idő elteltével küldött (8):

$$\xi_{s_l,\alpha_j} := \{\alpha_i \mid (S(\alpha_i) = s_l) \wedge (t_S(\alpha_i) > t_S(\alpha_j)) \wedge ([t_S(\alpha_i) - t_S(\alpha_j)] < \tau_{\min})\} \tag{7}$$

$$\zeta_{s_l,\alpha_j} := \{\alpha_i \mid (S(\alpha_i) = s_l) \wedge (t_S(\alpha_i) > t_S(\alpha_j)) \wedge ([t_S(\alpha_i) - t_S(\alpha_j)] < \tau_{\max})\} \tag{8}$$

Ezen feltételek teljesülése esetén a megfigyelő által tetszőleges kézbesített üzenethez és küldőhöz hozzárendelhető valószínűségre a következő üzenetinvariáns $\hat{P}_\Psi$ felső becslés adható (9), amennyiben $\tau_{\max} \le (\delta_{\max} - \delta_{\min})$:

$$P_{\beta_k,\Psi} \le \hat{P}_\Psi = \frac{\sum_{i=1}^{\Delta_{\min}} \max_{(i-1)\cdot\tau_{\min} \le q < i\cdot\tau_{\min}} f(q)}{|S| \cdot \sum_{i=1}^{\Delta_{\max}} \min_{(i-1)\cdot\tau_{\max} \le q < i\cdot\tau_{\max}} f(q)} \tag{9}$$

Ahol $\Delta_{\max} = \left\lfloor \frac{\delta_{\max} - \delta_{\min}}{\tau_{\max}} \right\rfloor$ és $\Delta_{\min} = \left\lceil \frac{\delta_{\max} - \delta_{\min}}{\tau_{\min}} \right\rceil$.

A MIN/MAX tulajdonság lényege példánkra vetítve, hogy a betegeknek egy adott gyakorisággal kérdéseket kell feltenniük, annak érdekében, hogy egy adott szintű anonimitás általános esetben is biztosítható legyen.

Szélsőértékek

A következőkben az $f(\delta)$ sűrűségfüggvény két szélsőséges esetét vizsgáljuk.

Legrosszabb eset – Determinisztikus, fix idejű késleltetés

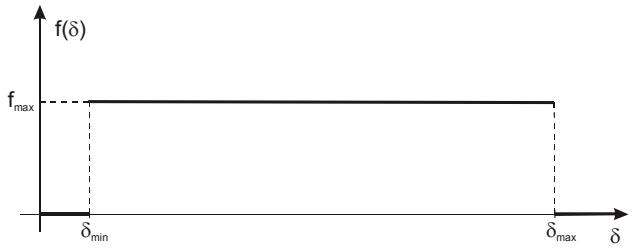
Amennyiben egy rendszer $\Psi = (C, S, R, \varepsilon_S, \varepsilon_R, \vartheta_S, \vartheta_R)$ történetének $f(\delta)$ sűrűségfüggvénye egy eltolt Dirac-delta függvény (azaz a csatorna minden üzenetet egy konstans kézbesítési idő elteltével kézbesít), úgy a megfigyelő minden kézbesített titkosított üzenethez egyértelműen hozzá tudja rendelni küldőjét.

Amennyiben az üzenetküldések rendszerességére nincsen megkötés, vagy ha egy rendszer Ψ MIN/MAX-tulajdonságú történetének $\tau_{\min}$, $\tau_{\max}$ paramétereit nem az $f(\delta)$ sűrűségfüggvénynek megfelelően választották, úgy szintén előfordulhat bizonyos – nem feltétlenül az összes – β_k kézbesített üzenetekre, hogy $P_{\beta_k,\Psi} = 1$, amelyet természetesen szeretnénk elkerülni.

A legrosszabb esetben példánkban a megfigyelő minden kérdéshez hozzá tudja párosítani azt a beteget, aki ténylegesen azt fel is tette, így elérte célját.

Legjobb eset – Egyenletes eloszlású késleltetés

A legjobb esetben a megfigyelő tetszőleges kézbesített titkosított üzenethez csak véletlenszerűen tud küldőt hozzárendelni azok közül, akik a releváns ($\delta_{\min} - \delta_{\max}$) időintervallumban üzenetet küldtek.



3. ábra – A legjobbnak bizonyult (egyenletes eloszlású) sűrűségfüggvény

Amennyiben egy rendszer $\Psi = (C,\ S,\ R,\ \varepsilon_S,\ \varepsilon_R,\ \vartheta_S,\ \vartheta_R)$ történetének $f(\delta)$ sűrűség-függvénye egyenletes eloszlású (azaz $\delta_{\min}$ és $\delta_{\max}$ között konstans $f_{\max}$ értéket vesz fel), úgy minden β_k kézbesített titkosított üzenetre a következő érvényes:

$$P_{\beta_k,\Psi} = \frac{\max\limits_{s_l} \left|\eta_{\beta_k,s_l,\Psi}\right|}{\left|\mu_{\beta_k,\Psi}\right|} \tag{10}$$

Amennyiben Ψ MIN/MAX tulajdonságú $\tau_{\min}$, $\tau_{\max}$ paraméterekkel – ahol $\tau_{\max} \le (\delta_{\max} - \delta_{\min})$ – úgy a felső becslés (9)-es képlete tovább egyszerűsödik:

$$P_{\beta_k,\Psi} \le \hat{P}_{\Psi} = \frac{\Delta_{\min}}{|S| \cdot \Delta_{\max}} \approx \frac{\tau_{\max}}{|S| \cdot \tau_{\min}} \tag{11}$$

Amennyiben Ψ^* még a $\tau_{\min} = \tau_{\max}$ feltételt is teljesíti (ahol továbbra is $\tau_{\max} \le [\delta_{\max} - \delta_{\min}]$), azaz minden s_l küldő pontosan $\tau_{\min} = \tau_{\max}$ időnként pontosan egy üzenetet küld, akkor a rendszer története eléri a globális optimumot, azaz a megfigyelő tetszőleges kézbesített üzenet küldőjeként a küldők halmazának egy véletlenszerűen választott elemét kénytelen megjelölni, így:

$$P_{\beta_k,\Psi} \le \hat{P}_{\Psi} \approx \frac{1}{|S|} \tag{12}$$

A legjobb eseteben példánkra vonatkoztatva a megfigyelő semmit sem ért el a megfigyeléssel. Az üzenettovábbító csatorna paraméterit ismerve (azok akár nyilvánosak is lehetnek) azon betegek közül, akik a releváns időintervallumban egyáltalán kérdést tettek fel, a megfigyelő véletleszerűen kénytelen választani a tippeléshez. Amennyiben a betegek a MIN/MAX-tulajdonságnak is megfelelnek, akkor még az anonimitás mértéke is pontosan szabályozható.

Összefoglaló

A cikkben ismertetésre került a megfigyelhető black-box csatorna modellje. Passzív megfigyelőt feltételezve megvizsgáltuk, milyen következtetéseket tud a megfigyelő az események bekövetkeztének időzítése és a csatorna tulajdonságai alapján levonni. A modellben definiáltuk a forrásrejtő tulajdonságot, mely az anonimitás fogalmának egy elméletileg megalapozott mértéke.

Végül ismertetésre került egy olyan módszer is, melynek alkalmazásával korlátozhatóak a megfigyelő lehetőségei, sőt a globális optimum is elérhető.

További elemzést igényel annak felmérése, hogy ha a feltételezett elméleti értelemben vett tökéletes titkosítót gyakorlati értelemben vett erős titkosítóra cseréljük. Szintén megvizsgálandó, hogyan változnak a következtetések, ha a jelenlegi black-box csatornát „felnyitjuk" és feltételezzük, hogy a megfigyelő a csatornán belülről is hozzájuthat bizonyos információkhoz. Végül azzal is számolni kell, ha az eddig passzívnak feltételezett megfigyelőt aktív támadóval helyettesítjük, aki az üzeneteket késleltetni és esetleg módosítani is tudja, hogyan módosul az anonimitás biztosítható szintje.

Köszönetnyilvánítás

Köszönet illeti dr. Vajda Ferencet és dr. Selényi Endrét, akik a cikk megírásához értékes tanácsokkal és ötletekkel járultak hozzá, valamint dr. Dobrowiecki Tadeuszt, a cikk kivonatához adott ötleteiért. Külön köszönet Endrődi Csillának és Orvos Péternek a közös ötletelésekért.

Irodalomjegyzék

[1] D. Chaum: „Untraceable Electronil Mail, Return Addresses, and Digital Pseudonyms", *Communications of the ACM*, volume 24, number 2, 1981

[2] M. Reed, P. Syverson, D. Goldschlag: „Anonymous Connections and Onion Routing", in *IEEE Journal on Selected Areas in Communication Special Issue on Copyright and Privacy Protection*, 1998.

[3] D. Goldschlag, M. Reed, P. Syverson: „Hiding Routing Information", in *Information Hiding*, R. Anderson (szerkesztő), Springer-Verlag LLNCS 1174, pp. 137–150, 1996

[4] A. Pfitzman, M. Kohntopp: „Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology", in *Designing Privacy Enhancing Technologies*, H. Federrath (szerkesztő), Springer-Verlag LNCS 2009, pp. 1–9, 2001