MEGFIGYELHETŐ BLACK-BOX CSATORNA FORRÁSREJTŐ TULAJDONSÁGA

Tóth Gergely[1], Hornák Zoltán[2]
doktorandusz
Budapesti Műszaki és Gazdaságtudományi Egyetem
tanársegéd
Budapesti Műszaki és Gazdaságtudományi Egyetem

BEVEZETÉS

Az anonim átviteli protokollok (mint például a MIX-net [1] vagy az Onion Routing [2]) 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 folyamatban van, azonban elemzésük még nem teljes.

Ebben a cikkben ezen protokollok leírására bevezetésre kerül a megfigyelhető black-box csatorna modellje. A bemutatott vizsgálat tárgyát az képezi, hogy egy csupán lehallgatása 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.

Az alkalmazások (mint például a MIX-net) az ismertetésre kerülő modellhez hasonlón alapulnak és így érvényesek rájuk az itt megállapítottak. A következtetések többségét az implementációk alkalmazzák is, azonban például a MIN/MAX tulajdonság megkövetelése gyakorlati problémákhoz vezetne, így azt mellőzik.

A MEGFIGYELHETŐ BLACK-BOX CSATORNA MODELLJE

A következőkben bevezetésre kerül a megfigyelhető black-box csatorna modellje. Egy csatornát akkor hívunk megfigyelhetőnek, ha egy lehetséges megfigyelő érzékelheti a csatornába bemenő és az azt elhagyó üzeneteket [3]. A csatorna black-box, ha a megfigyelő nem láthatja, mi történik az üzenetekkel a csatorna belsejében, hogy kerülnek ezek továbbküldésre illetve átkódolásra. Továbbá a csatornán áthaladó üzenetekről feltesszük, hogy azonos méretűek és megfelelően titkosítottak.

A környezet és a csatorna 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 csatornán belül nem születik új üzenet és a csatorna nem dob el beérkezett üzenetet. Egy beérkezett üzenet a következő szabályok szerinti késleletetés után kerül kézbesítésre:

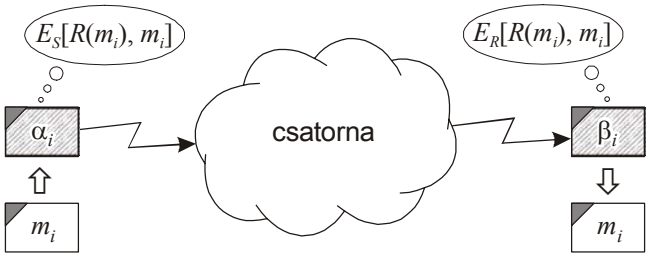
- a késleltetés δ valószínűségi változó, adott $f(\delta)$ sűrűségfüggvénnyel, $\delta = t_R - t_S$, ahol δ üzenet- és időinvariáns;

− a csatorna minden üzenetet egy előre meghatározott konstans, üzenet- és időinvariáns $\delta_{\max}$ késleltetésen belül, de legalább egy konstans, üzenet- és időinvariáns $\delta_{\min}$ elteltével kézbesít, azaz $\forall_{m_i}[\delta_{\min} < t_R(m_i) - t_S(m_i) < \delta_{\max}]$.

A C csatornát így $f(\delta)$, $\delta_{\min}$, $\delta_{\max}$ paraméterekkel jellemezhetjük.

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 $t_R(m_i) = t_R(\beta_i)$ érkezik meg.



1. ábra
Üzenetküldés a csatornán keresztül

Ebben a cikkben 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).

A MEGFIGYELŐ

Vizsgáljuk meg egy passzív megfigyelő lehetőségeit ebben a modellben, aki csak lehallgatni tudja a titkosított üzeneteket, azokat nem tudja dekódolni, 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.

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.

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 feltételezem, hogy

a megfigyelő a rendszer teljes Ψ történetét ismeri, azaz minden lehetséges számára elérhető információt a rendszer működésének teljes időszakában képes megfigyelni.

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

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

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

Amennyiben a megfigyelő a kézbesített üzenet → 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:

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

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

FORRÁSREJTŐ TULAJDONSÁG

A rendszer Ψ = (*C*, *S*, *R*, ε_S, ε_R, ϑ_S, ϑ_R) története forrásrejtő tulajdonságú Θ paraméterrel, amennyiben semelyik β_k titkosított kézbesített üzenethez sem tud a megfigyelő Θ-nál nagyobb valószínűséggel küldőt hozzárendelni:

$$\forall_{\beta_k \in \varepsilon_R} P_{\beta_k, \Psi} \le \Theta \quad (4)$$

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.

Ennek megfelelően a tört számlálójában levő összegzést minél kisebb halmazon kell elvégezni, ezért a küldők nem küldhetnek bizonyos időn belül egynél több üzenetet. A tört nevezőjében levő összegzést minél nagyobb halmazon kell

elvégezni, tehát a küldőknek bizonyos időn belül legalább egy 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 semelyik küldő sem küld $\tau_{\min}$ időn belül két üzenetet és minden küldő küld $\tau_{\max}$ időnként legalább egy üzenet. Ezen feltételek teljesülése esetén a megfigyelő által tetszőleges kézbesített üzenethez és küldőhöz hozzárendelhető valószínűségre a következő üzenetinvariáns $\hat{P}_\Psi$ felső becslés adható:

$$P_{\beta_k,\Psi} \le \hat{P}_\Psi = \frac{\sum_{i=1}^{\Delta_{\min}} \max_{(i-1)\cdot\tau_{\min} \le q < i\cdot\tau_{\min}} f(q)}{|S| \cdot \sum_{i=1}^{\Delta_{\max}} \min_{(i-1)\cdot\tau_{\max} \le q < i\cdot\tau_{\max}} f(q)} \tag{5}$$

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

LEGJOBB ESET – EGYENLETES ELOSZLÁSÚ KÉSLELTETÉS

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 üzenetre a következő érvényes:

$$P_{\beta_k,\Psi} = \frac{\max_{s_l} \left| \eta_{\beta_k, s_l, \Psi} \right|}{\left| \mu_{\beta_k,\Psi} \right|} \tag{6}$$

Amennyiben Ψ MIN/MAX tulajdonságú $\tau_{\min}$, $\tau_{\max}$ paraméterekkel – ahol $\tau_{\max} \le (\delta_{\max} - \delta_{\min})$ – úgy a felső becslés (6)-os képlete tovább egyszerűsödik:

$$P_{\beta_k,\Psi} \le \hat{P}_\Psi = \frac{\Delta_{\min}}{|S| \cdot \Delta_{\max}} \approx \frac{\tau_{\max}}{|S| \cdot \tau_{\min}} \tag{7}$$

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.

IRODALOMJEGYZÉK

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

[2] REED M., SYVERSON, P., GOLDSCHLAG, D.: **Anonymous Connections and Onion Routing**, IEEE Journal on Selected Areas in Communication Special Issue on Copyright and Privacy Protection, 1998.

[3] PFITZMAN, A., KOHNTOPP, M.: **Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology**, Designing Privacy Enhancing Technologies, H. Federrath (szerkesztő), Springer-Verlag LNCS 2009, pp. 1–9, 2001