Measure for Anonymity

Gergely Tóth, Zoltán Hornák
Budapest University of Technology and Economics
{tgm, hornak}@mit.bme.hu

In this paper a model for the anonymous transport protocols will be introduced. Based upon this model certainty will be determined than an observer can trace back delivered messages to their senders, this way compromising anonymity. Building on this model the source-hiding property will be defined, which acts as a numerical measure for anonymity. Finally requirements will be given both for the channel implementing the anonymous transport protocol and for the senders to have a given upper limit for the certainty of the observer, thus providing guaranteed level of anonymity.

1 Introduction

Anonymous transport protocols (such as MIX-net [1] or Onion Routing [2] [3]) established the ground of sending anonymous messages. They aim to guarantee that no delivered message can be traced back to its sender independently from lower network layers. Research of such protocols is currently under way but their theoretical analysis and description is not complete.

For the use case of the here-described scenario we chose an anonymous medical consulting system. Patients ask their questions the respective doctors via anonymous e-mails. Task of the anonymous transport protocol is to deliver the questions to the appropriate doctor, so that the message cannot be traced back to the patient. Doctors answer the questions in a public forum, for instance on a web site. Could the anonymity be compromised, then one could conclude from the asked questions to the illnesses and symptoms of the patient, which we want to prohibit, especially when sensitive topics (e.g. sexual, narcotic problems) are handled.

Of course anonymous transport protocols may also be used for other purposes as well, they could be applied in anonymous electronic election systems, in anonymous on-line shopping or simply in electronic mailing. The above example, where both the questions and the answers from the doctors will become public and only the identity of the patient is secret illustrates pretty well the analyzed requirements for anonymity.

For description of such protocols the model of the PROB[✦]-channel will be introduced. It will be analyzed what conclusions a passive observer can draw by only knowing public parameters and timing of events (sending & delivery). Based on the model the source-hiding property will be defined, which can act as a numerical measure for anonymity. Finally requirements will be introduced in order to limit the certainty of the adversary observer and to ensure a given level of anonymity.

2 Model of the PROB-channel

Consider a channel between the senders of the messages (in our example the patients) and the recipients (the doctors). This channel is responsible for providing anonymity for the patients, thus it implements the anonymous transport protocol. In the paper — if not otherwise specified — a PROB-channel is assumed.

[✦] The acronym PROB stands for passive, real-time, observable, black-box.

Model of the PROB-channel comprises the following criteria:

- The channel is *passive*, as its operation is not affected by properties and distribution of incoming messages, i.e. network delay has static distribution.
- The channel is *real-time*, thus messages will be delivered before a message-invariant maximal delay.
- All input and output of the channel is *observable*, so an observer can detect all incoming and delivered messages [4].
- The channel is *black-box*, since it is analyzed as a whole, internal implementation is not considered. The observer cannot see what happens to the messages inside the channel and how they are encoded and delivered.
- We furthermore assume that messages passing through the channel are equally sized and properly encrypted, thus an observer can only draw conclusions from the timing of the messages, content does not provide information. Since this condition can easily be satisfied it does not mean restriction to practical implementations.

2.1 Description of the Environment

Let S denote the set of senders, R the set of recipients, and M the set of messages. Let $S(m_i)$ denote the sender of message m_i, $R(m_i)$ the recipient of message m_i, whereas $t_S(m_i)$ the time of sending of message m_i and $t_R(m_i)$ the time if delivery of message m_i. According to our patient-doctor example, R is the set of patients, S the set of doctors and M is the set of questions. The system operates in continuous time, thus events cannot happen at the same time (no parallel entry into the channel). Time of transporting the message from the sender to the channel and from the channel to the recipient will not be considered. This simplification does not substantially affect the conclusions drawn.

2.2 Specification of the Channel

The channel delivers messages from senders to recipients. No messages are born inside the channel and messages won't be dropped by the channel. An incoming message from its sender will be delivered to its recipient after a delay with the following properties:

- the delay δ is a probability variable with a given $f(\delta)$ density function, $\delta = t_R - t_S$, where δ is message- and time-invariant;
- the channel will deliver all messages before a predefined, message- and time-invariant maximal delay $\delta_{\max}$ (time-to-live) and after a predefined, message- and time-invariant minimal delay $\delta_{\min}$, thus $\forall_{m_i}[\delta_{\min} < t_R(m_i) - t_S(m_i) < \delta_{\max}]$ (see Figure 1).

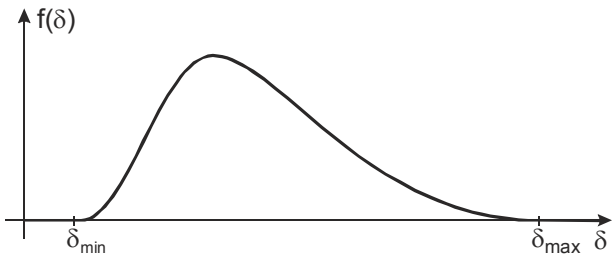

Figure 1 – Distribution function of the delay δ

Therefore channel C can be characterized by the parameters $f(\delta)$, $\delta_{\min}$, $\delta_{\max}$.

2.3 Message sending

In the following we assume that sender $s_a \in S$, $s_a = S(m_i)$ sends a message $m_i \in M$ to recipient $r_b \in R$, $r_b = R(m_i)$. Message m_i enters the channel in the encrypted form $\alpha_i := E_S(r_b, m_i)$ at time

$t_S(m_i) = t_S(\alpha_i)$, whereas it will be delivered to the recipient in the form $\beta_i := E_R(r_b, m_i)$, encrypted with a different key, at time $t_R(m_i) = t_R(\beta_i)$ (see Figure 2).

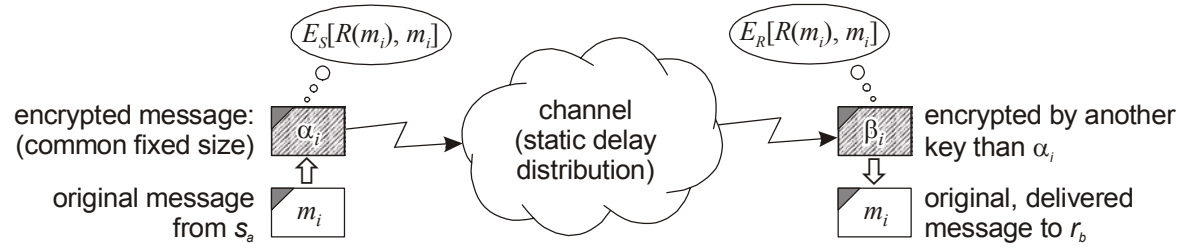

Figure 2 – Message sending through the channel

We assume furthermore that E_S and E_R are perfect encryption functions, thus α_i can only be decrypted by the channel, while β_i can be decoded by only r_b.

3 The Observer

Let us now analyze what are the possibilities of a passive observer in this model. Such an observer can only eavesdrop encrypted messages, he cannot decrypt them (unless sent to him) nor can he modify, delete, replay or delay[▲] messages. Aim of the observer is to match delivered messages (β_i) with their senders — or at least guess the link with good probability — and so get a good assumption who communicates with whom.

3.1 Knowledge of the Observer

We assume that the observer can eavesdrop all ends of the channel, this way he knows all sent encrypted messages and their time of sending, all delivered encrypted messages and their time of receipt. He also knows the parameters and the environment of the channel. Thus he is in the possession of the following information:

- environment (S, R) and parameters ($f(\delta)$, $\delta_{\min}$, $\delta_{\max}$) of the channel;
- $\varepsilon_S := \{\alpha_i := E_S[S(m_i), m_i]\}$, $\vartheta_S := \{t_S(\alpha_i)\}$ — sent messages and their time of sending;
- $\varepsilon_R := \{\beta_i := E_R[R(m_i), m_i]\}$, $\vartheta_R := \{t_R(\beta_i)\}$ — received messages and their time of receipt.

Let Ψ denote the history of the system given by the following parameters: C, S, R, ε_S, ε_R, ϑ_S, ϑ_R. In the following we assume that the observer knows the full history Ψ of the system and he can perceive all the observable properties during the whole operation of the system. As we will see, the probability that a delivered message can be traced back to its sender, can even in this case be limited. According to our example, aim of the observer is to find out, which patient asked which question.

4 Confidence of the Observer

Let a specific history of the system be $\Psi^* := (C^*, S^*, R^*, \varepsilon_S^*, \varepsilon_R^*, \vartheta_S^*, \vartheta_R^*)$. In order to evaluate, which sender sent which message, for each encrypted delivered message β_k^* and for each sender s_l^* a probability $P_{\beta_k^*, s_l^*, \Psi^*}$ can be determined. If the observer knows the history Ψ^* of the system, he can conclude that β_k^* was sent by s_l^* with the probability $P_{\beta_k^*, s_l^*, \Psi^*}$:

$$P_{\beta_k^*, s_l^*, \Psi^*} = P[S(\beta_k^*) = s_l^* \mid \Psi = \Psi^*] \tag{1}$$

[▲] Note that besides the traditional manipulation techniques an attacker can also delay messages in order to compromise anonymity. We will see that this might be a successful attack method against passive channels.

The observer naturally looks for the most probable source where $P_{\beta_k^*,\Psi^*} := \max_{s_l^*} P_{\beta_k^*,s_l^*,\Psi^*}$.

In order to back-trace the messages to their senders the observer calculates the probabilities (1) and marks the most probable sender as the potential real sender of the message in question.

The following sets need to be defined for simplifying upcoming equations. Let $\mu_{\beta_k^*,\Psi^*}$ denote the set of encrypted sent messages α_j^*, which might left the channel as β_k^* (2) considering the properties of $f^*(\delta)$. Furthermore let $\eta_{\beta_k^*,s_l^*,\Psi^*}$ denote the set of α_j^* in $\mu_{\beta_k^*,\Psi^*}$, which were sent by s_l^* (3).

$$\mu_{\beta_k^*,\Psi^*} := \{\alpha_j^* \mid [t_R(\beta_k^*) - \delta_{\max}^*] < t_S(\alpha_j^*) < [t_R(\beta_k^*) - \delta_{\min}^*]\} \tag{2}$$

$$\eta_{\beta_k^*,s_l^*,\Psi^*} := \{\alpha_j^* \mid [\alpha_j^* \in \mu_{\beta_k^*,\Psi^*}] \wedge [S(\alpha_j^*) = s_l^*]\} \tag{3}$$

4.1 Global Back-tracing

In order to compute the probabilities in (1) the obvious and optimal solution would be to perform a global back-tracing, thus the observer would try all possibilities and choose the most probable one.

In order to do this, one has to generate all possible match combinations (the g_i-s) of sent and received messages (4). A match $g_i := \left\langle g_i^1, g_i^2, ..., g_i^{|M^*|} \right\rangle$ means that the delivered encrypted message β_k^* entered the channel as g_i^k.

$$G_{\Psi^*} := \{g_i := \left\langle g_i^1, g_i^2, ..., g_i^{|M^*|} \right\rangle \mid [g_i \in \bigtimes_{1 \le k \le |M^*|} \mu_{\beta_k^*,\Psi^*}] \wedge [\forall_{1 \le j \le |M^*|} \forall_{\substack{(1 \le k \le |M^*|) \wedge \\ (j \ne k)}} (g_i^j \ne g_i^k)]\} \tag{4}$$

After having all match combinations G_{Ψ^*}, based upon their probabilities the observer can calculate (1) as follows (where $E_S^{-1}(\alpha_j) = m_j$ and $E_R^{-1}(\beta_k) = m_k$):

$$P_{\beta_k^*,s_l^*,\Psi^*} = \sum_{S(g_i^k)=s_l^*} P(\bigwedge_{1 \le j \le |M^*|} [E_S^{-1}(g_i^j) = E_R^{-1}(\beta_j^{-1})] \mid \Psi = \Psi^*) \tag{5}$$

Unfortunately this approach is exponential by the number of messages and thus ineffective for practical use.

4.2 Local Back-tracing

Performs the observer the delivered message → sender matching for each delivered message independently, then the following equation gives the probability (1) that s_l^* is the sender of β_k^* if history Ψ^* is known:

$$P_{\beta_k^*,s_l^*,\Psi^*} = \frac{\sum_{\forall_{\alpha_i^*}[\alpha_i^* \in \eta_{\beta_k^*,s_l^*,\Psi^*}]} f^*[t_R(\beta_k^*) - t_S(\alpha_i^*)]}{\sum_{\forall_{\alpha_j^*}[\alpha_j^* \in \mu_{\beta_k^*,\Psi^*}]} f^*[t_R(\beta_k^*) - t_S(\alpha_j^*)]} \tag{6}$$

Since only local back-tracing is feasible especially for larger sets of messages, in the following we assume a locally back-tracing observer for the drawn conclusions. Unfortunately originating from its local aspect, local back-tracing can overlook important correlations.

5 Source-Hiding Property

History $\Psi = (C, S, R, \varepsilon_S, \varepsilon_R, \vartheta_S, \vartheta_R)$ of a system is source-hiding with parameter Θ if the observer cannot assign a sender to any delivered message β_k with a probability greater than Θ:

$$\forall_{\beta_k \in \varepsilon_R} P_{\beta_k,\Psi} \leq \Theta \tag{7}$$

6 MIN/MAX Property

In order to be able to limit the possible value of equation (6) influencing the source-hiding property even in the worst case, restrictions have to be applied for the intervals between message sending. First, summation in the numerator has to be performed on the smallest possible set. In order to achieve this, senders cannot send more than one message in a given time interval. Second, summation in the denominator has to be performed on the greatest possible set. In order to achieve this, senders have to send at least one message in a given time interval. (If it is otherwise not achievable, senders have to send empty (so called *dummy*) messages to randomly chosen recipients.)

Considering the above limitations, history $\Psi = (C, S, R, \varepsilon_S, \varepsilon_R, \vartheta_S, \vartheta_R)$ of a system possesses the MIN/MAX property with parameters $\tau_{\min}$, $\tau_{\max}$ ($\tau_{\min} \leq \tau_{\max}$), if it holds that no sender sends more than one message within a time interval $\tau_{\min}$ (8) and all senders send at least one message in a time interval $\tau_{\max}$ (9).

$$\forall_{s_l \in S} \; \forall_{\alpha_j | S(\alpha_j)=s_l} \xi_{s_l,\alpha_j} = \varnothing \tag{8}$$

$$\forall_{s_l \in S} \; \forall_{\alpha_j | S(\alpha_j)=s_l} \neg(\zeta_{s_l,\alpha_j} = \varnothing) \tag{9}$$

Where ξ_{s_l,α_j} is the set of sent encrypted messages, which were sent by sender s_l maximal $\tau_{\min}$ after sending α_j (10) and ζ_{s_l,α_j} is the set of sent encrypted messages, which were sent by s_l maximal $\tau_{\max}$ after sending α_j (11).

$$\xi_{s_l,\alpha_j} := \{\alpha_i \mid (S(\alpha_i) = s_l) \wedge (t_S(\alpha_i) > t_S(\alpha_j)) \wedge ([t_S(\alpha_i) - t_S(\alpha_j)] < \tau_{\min})\} \tag{10}$$

$$\zeta_{s_l,\alpha_j} := \{\alpha_i \mid (S(\alpha_i) = s_l) \wedge (t_S(\alpha_i) > t_S(\alpha_j)) \wedge ([t_S(\alpha_i) - t_S(\alpha_j)] < \tau_{\max})\} \tag{11}$$

If these conditions hold, for the probabilities (1) assigned to any delivered encrypted message and sender, a message-invariant upper limit $\hat{P}_\Psi$ can be given (12), and thus the source-hiding property can be guaranteed (assuming $\tau_{\max} \leq [\delta_{\max} - \delta_{\min}]$):

$$P_{\beta_k,\Psi} \leq \Theta = \hat{P}_\Psi = \frac{\sum_{i=1}^{\Delta_{\min}} \max_{(i-1)\tau_{\min} \leq q < i\cdot\tau_{\min}} f(q)}{|S| \cdot \sum_{i=1}^{\Delta_{\max}} \min_{(i-1)\tau_{\max} \leq q < i\cdot\tau_{\max}} f(q)} \tag{12}$$

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

7 Optimum — Uniformly Distributed Delay

In the best case — while doing the back-tracing — the observer can only pick randomly for a delivered message from those who sent a message in the relevant time frame ($\delta_{\min} - \delta_{\max}$). Is

the distribution $f(\delta)$ of the delay in a channel uniform (between $\delta_{\min}$ and $\delta_{\max}$ $f(\delta) = f_{\max}$, otherwise zero), then with a history $\Psi = (C, S, R, \varepsilon_S, \varepsilon_R, \vartheta_S, \vartheta_R)$ for all delivered encrypted messages β_k the following equation holds:

$$P_{\beta_k,\Psi} = \frac{\max_{s_l} |\eta_{\beta_k,s_l,\Psi}|}{|\mu_{\beta_k,\Psi}|} \tag{13}$$

If Ψ has the MIN/MAX property with parameters $\tau_{\min}$, $\tau_{\max}$ ($\tau_{\max} \le [\delta_{\max} - \delta_{\min}]$), then the upper limit in (12) can be brought into a simpler form:

$$P_{\beta_k,\Psi} \le \Theta = \hat{P}_\Psi = \frac{\Delta_{\min}}{|S| \cdot \Delta_{\max}} \approx \frac{\tau_{\max}}{|S| \cdot \tau_{\min}} \tag{14}$$

If Ψ also fulfills the condition $\tau_{\min} = \tau_{\max}$ ($\tau_{\max} \le [\delta_{\max} - \delta_{\min}]$), meaning that each sender sends messages with a period exactly $\tau_{\min} = \tau_{\max}$, then the history of the system reaches the global optimum and the observer has to pick the sender for each delivered encrypted message randomly from all senders (from S):

$$P_{\beta_k,\Psi} \le \Theta = \hat{P}_\Psi \approx \frac{1}{|S|} \tag{15}$$

Interpreting these in our example, with uniformly distributed delay the observer does not achieve anything by eavesdropping, he has to pick randomly from the patients who asked questions in the relevant time frame. If the patients satisfy the MIN/MAX conditions as well, then the level of anonymity can even be controlled exactly.

8 Conclusion

In this paper the model of the PROB-channel was introduced. Assuming a passive observer we analyzed what conclusions could be drawn based solely on observation of the timing of events and the parameters of the channel. In the model the source-hiding property was introduced, which acted as a numerical measure for anonymity. Finally we introduced methods for limiting possibilities of the observer and even to achieve global optimum.

In further research it should be evaluated how the conclusions will be affected if the perfect encryption is downgraded to only a practically strong one. Analysis is needed if the black-box channel is opened and the observer can gain information from inside the channel. Finally it should be investigated what an active attacker can accomplish against the here described model and how the PROB-channel should be extended to successfully protect against active opponent (supposingly by becoming an active channel, dynamically reacting to the distribution of actual message arrivals).

9 References

[1] Chaum, D.: *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms*, Communications of the ACM, volume 24, number 2, pp. 84-88, 1981

[2] Reed, M., Syverson, P., Goldschlag, D.: *Anonymous Connections and Onion Routing*, in IEEE Journal on Selected Areas in Communication Special Issue on Copyright and Privacy Protection, pp. 482-494, 1998

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

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