ANONYMITY IN CONTINUOUS-TIME SYSTEMS

Gergely TÓTH
Advisor: Zoltán HORNÁK, Ferenc VAJDA

I. Introduction

Anonymous communication is a rapidly evolving area: it is needed for several privacy related services, such as anonymous electronic voting, payment or consultancy. Numerous techniques have been developed for the main goal: to deliver messages from senders to recipients in a manner that an adversary should find it difficult to identify who communicates with whom.

In this paper we analyze two representatives of a relatively new field of the continuous-time anonymity systems: the SG-Mix [1] and the PROB-channel [2]. We will compare them based on simulations and come to an interesting result: although the SG-Mix was proven to be optimal[1] in [3], our numbers show that the PROB-channel outperforms it in the evaluated scenarios.

II. Continuous-time Anonymity Systems for Anonymous Communication

A. *Continuous-time Systems in General*

Continuous-time anonymity systems realize anonymous communication according to the following model: senders ($s_i \in S$) send encrypted messages ($\alpha_j \in \varepsilon_S$) at times $t_S(\alpha_j)$ through the continuous-time system (CTS). The CTS receives the sent messages and performs cryptographic operations on them to obtain a different representation. In order to further confuse the adversary, the CTS delays messages. After the delay the CTS delivers the reencoded messages ($\beta_k \in \varepsilon_R$) to the recipients ($r_l \in R$) at times $t_R(\beta_k)$. Both the sent and the delivered messages have a common, fixed size not to reveal information about their relationship.

The adversary's aim is to match the delivered messages to senders ($\beta_k \rightarrow s_i = S(\beta_k)$). For that he can eavesdrop on communication channels and see when messages are being sent or delivered.

B. *Delay Strategies*

The heart of the anonymous communication is the delay of the messages. In case of continuous-time systems this delay is randomized according to a probability variable δ with a given density function $f(\delta)$. For the SG-Mix the delay density is chosen to be exponential with parameter μ: $f^{\text{SG}}(\delta) = \mu \cdot e^{-\mu \cdot \delta}$. From this it follows that the mean delay of such a system is $\frac{1}{\mu}$. In order to achieve real-time properties, the density function for the PROB-channel is limited by a maximal delay $\delta_{\text{max}}^{\text{PROB}}$. To indicate that the channel needs a certain amount of time for message processing, a minimal delay ($\delta_{\text{min}}^{\text{PROB}}$) was also introduced. The density function of the delay was chosen to be uniform, thus $f^{\text{PROB}}(\delta) = \frac{1}{\delta_{\text{max}}^{\text{PROB}} - \delta_{\text{min}}^{\text{PROB}}}$

III. Simulation results

A. *Simulation Environment*

For the simulation MIN/MAX senders were used: the solution from [2] requires that each sender sends at least one message in τ_{max} time (minimal message sending frequency) and no sender sends more than one message in τ_{min} time (maximal message sending frequency). If a sender does not have real messages to send, he should send dummy messages to randomly chosen recipients.

[1] Under special conditions: the authors assumed Poisson-distributed incoming messages and quantified anonymity with the help of entropy.

For the adversary a *locally back-tracing passive* one was chosen [2]. The idea is to match each delivered message to the senders individually. With the following two sets ($\mu_{\beta_k} = \{\alpha_j | \, (t_R(\beta_k) - \delta_{\max}) < t_S(\alpha_j) < (t_R(\beta_k) - \delta_{\min})\}$ and $\eta_{\beta_k,s_l} = \{\alpha_j | (\alpha_j \in \mu_{\beta_k}) \wedge (S(\alpha_j) = s_l)\}$) equation (1) gives his guess, what is the probability of a certain message β_k being sent by a certain sender s_l:

$$P_{\beta_k,s_l} = \frac{\sum_{\alpha_j \in \eta_{\beta_k,s_l}} f\left(t_R(\beta_k) - t_S(\alpha_j)\right)}{\sum_{\alpha_j \in \mu_{\beta_k}} f\left(t_R(\beta_k) - t_S(\alpha_j)\right)} \tag{1}$$

B. Numerical Results

The figures below show the difference between the SG-Mix and the PROB-channel. In the simulations 20 senders sent messages during a 5000 seconds long interval. The mean delay for both systems was the same, and $\tau_{\min}$ was 1 second in all cases. Measured was the ratio of correctly matched messages while the adversary assigned probabilities to messages and senders according to (1). Figure 1 shows the absolute difference of the success ratios, positive values indicate that the PROB-channel outperformed the SG-Mix. Figure 2 shows the relative differences.

Figure 1: Absolute difference

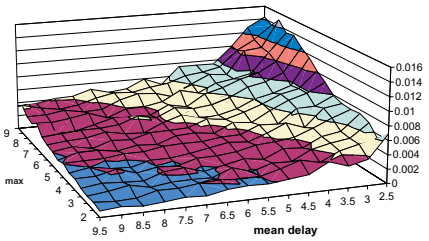
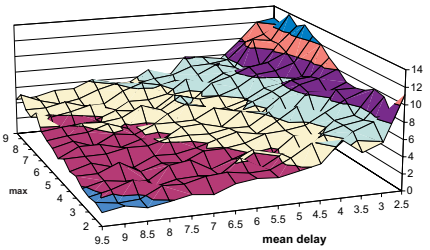


Figure 2: Relative difference (%)



IV. Conclusion

In this paper two continuous-time anonymity systems, the SG-Mix and the PROB-channel were compared. In several publications anonymity systems are evaluated under the assumption of Poisson-distributed incoming messages: e.g. in [3] the SG-Mix was proven to be optimal. However from [4] we know, messages to real systems do not follow this approximation. Furthermore, entropy is often used as anonymity metrics, although in [5] it was shown that this may lead to false results. The simulation results presented here show also, despite the proven optimality of the SG-Mix the PROB-channel outperforms it under equal conditions. With this in mind the task ahead is significant: the assumption of the Poisson-distributed messages and entropy based anonymity metrics should be reconsidered.

References

[1] D. Kesdogan, J. Egner, and R. Büschkes, "Stop-and-go MIXes: Providing probabilistic anonymity in an open system," in *Proceedings of Information Hiding Workshop (IH 1998)*, vol. 1525 of *Springer-Verlag, LNCS*, Berkeley, CA, 1998.

[2] G. Tóth and Z. Hornák, "Measuring anonymity in a non-adaptive, real-time system," in *Proceedings of Privacy Enhancing Technologies (PET2004)*, Springer-Verlag, LNCS, Forthcoming, 2004.

[3] G. Danezis, "The traffic analysis of continuous-time mixes," in *Proceedings of Privacy Enhancing Technologies (PET2004)*, Springer-Verlag, LNCS, Forthcoming, 2004.

[4] C. Díaz, L. Sassaman, and E. Dewitte, "Comparison between two practical mix designs," in *In proceedings of ESORICS: 9th European Symposium on Research in Computer Security*, vol. 3193 of *Springer-Verlag, LNCS*, pp. 141–159, French Riviera, France, September 2004.

[5] G. Tóth, Z. Hornák, and F. Vajda, "Measuring anonymity revisited," in *Proceedings of the Ninth Nordic Workshop on Secure IT Systems*, S. Liimatainen and T. Virtanen, Eds., pp. 85–90, Espoo, Finland, November 2004.