SIGNAL PROCESSING FOR ANONYMOUS COMMUNICATIONS

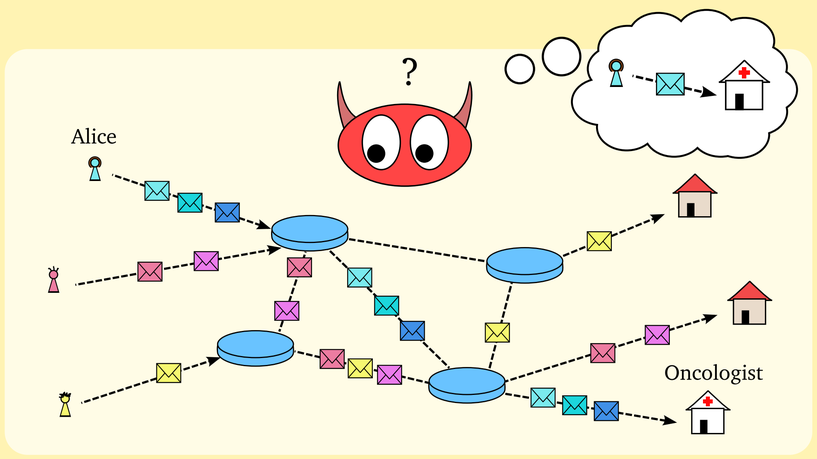
Simon Oya, Carmela Troncoso, and Fernando Pérez-González

simonoya@gts.uvigo.es ctroncoso@gradiant.org fperez@gts.uvigo.es

Universidad de Vigo
GPSC
Signal Processing in Communications Group

MOTIVATION OF THE WORK

Need for anonymity in the communications. → Need for tools to analyze and improve anonymous communication systems.



Current Analyses: 😞

- Simplify the problem with unrealistic hypotheses. → Applicable to very complex problems (digital communications, forensics, etc).
- Rely on very complex mathematical devices. → Simplifies the problem.
- Provide only empirical results. → Provides analytical results.

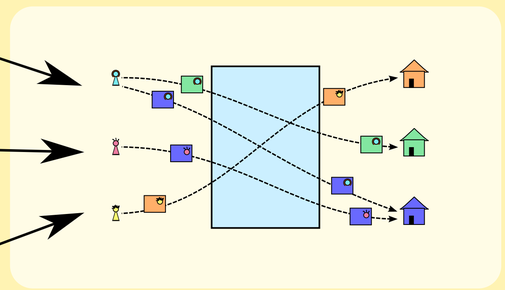
Idea!! Signal Processing! 💡

THESIS OBJECTIVES

General objective

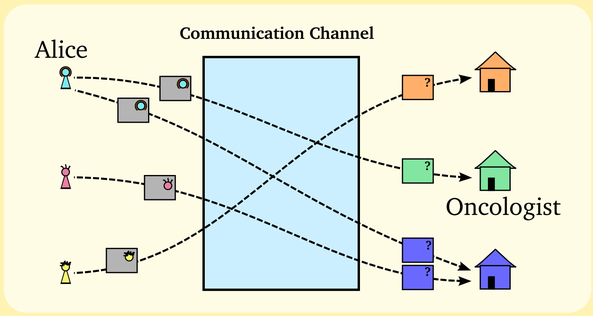
Apply signal processing tools to anonymous communications.

Analyze 🔬
Optimize 💡
Develop 💪



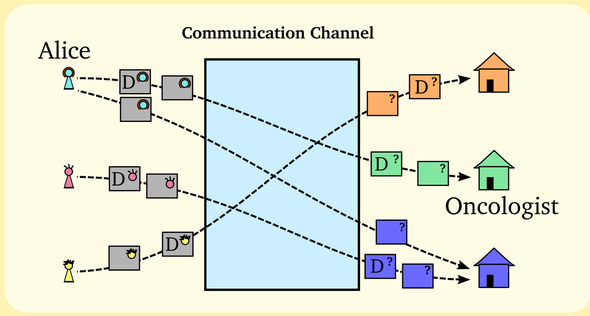
We will study two scenarios:

High-latency communication systems [1][2] (e.g., email).



- Delaying messages is allowed!!
- Robust against global adversaries.

Low-latency communication systems [3][4] (e.g., instant messaging, VoIP, browsing).

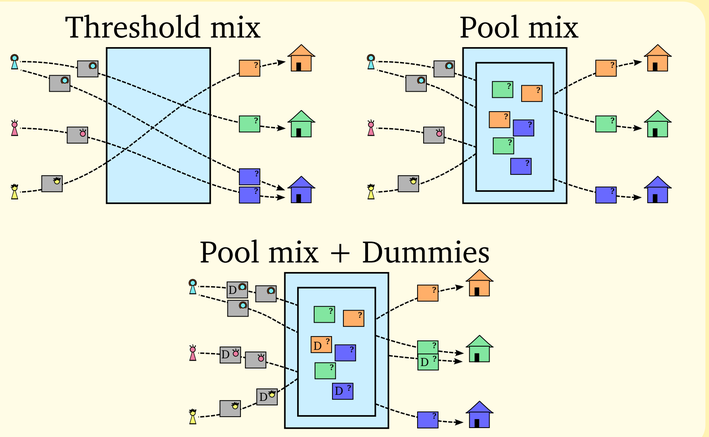


- Delaying messages is NOT allowed!!
- Explore other posibilities: dummy messages, re-routing...

RESEARCH PLAN

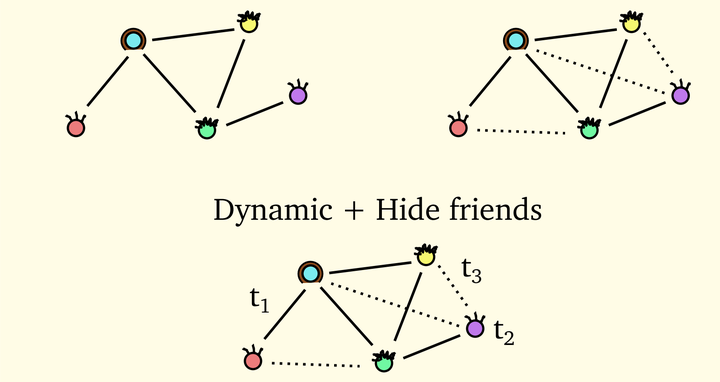
6 m.
- Study the state of the art.
- High latency anonymous communications: Mixes:

17 m.



- Low latency anonymous communications: Instant Messaging:

11 m.



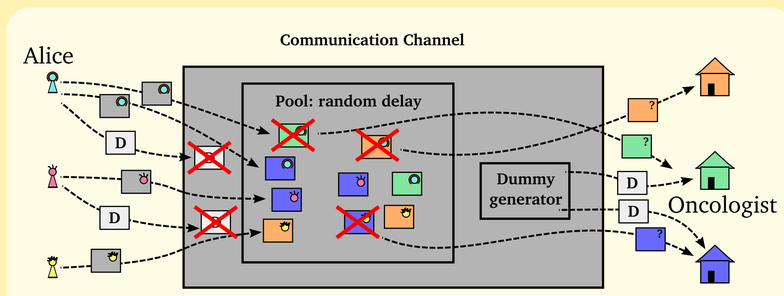
Methodology

1. Develop theoretical models.
2. Apply signal processing tools to analyze the privacy properties.
3. Optimize the privacy mechanisms.
4. Propose new protection mechanisms.
5. Empirical evaluation of our findings.

2 m.
- Wrapping up, conclusions and writing.

RESULTS AND DISCUSSIONS

- Previous work: new attack on mixes, the Least Squares Disclosure Attack (LSDA) [5].
- Proof that LSDA outperforms the family of statistical disclosure attacks [6].
- Analysis of a pool mix with dummies [7].

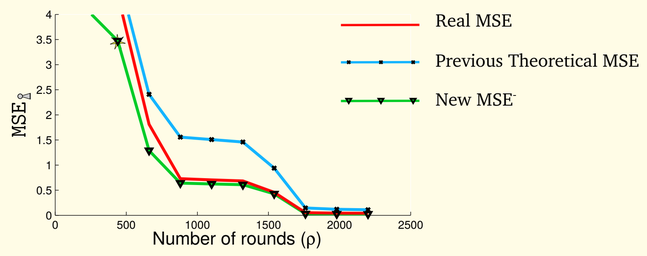


$$\mathrm{MSE}_{\text{🏠},\text{👤}} \approx \frac{1}{\rho}\cdot\frac{2-\alpha}{\alpha}\cdot\frac{\lambda_{\mathrm{OUT},\text{🏠}}}{\lambda_{\mathrm{IN},\text{👤}}}\cdot\left(1+\frac{\delta_{\mathrm{IN},\text{👤}}}{\lambda_{\mathrm{IN},\text{👤}}}\right)\cdot\left(1+\frac{\delta_{\mathrm{OUT},\text{🏠}}}{\lambda_{\mathrm{OUT},\text{🏠}}}\right)$$

- In-depth study of LSDA on pool mixes [8].
- Analysis of the mix in real scenarios [9].

$$\mathrm{MSE}_{\text{👤}}^{-} \approx \frac{1}{\rho}\cdot\frac{1}{\mu_2(\text{👤})}\left(\sum_{\text{👤}\in\text{👥}}\mu(\text{👤})\cdot v_{\text{👤}} + \frac{\mu_3(\text{👤})}{\mu_2(\text{👤})}\cdot v_{\text{👤}}\right)$$

Emails dataset:



NEXT YEAR PLANNING

- Finish the work on mixes: look for the optimal pool mix delay function (in progress).
- Begin with low-latency anonymous communication systems.
  - Revise state of the art.
  - Study the problem of static SN + don't hide friends.
- Internship in Rutgers University (NJ), with Professor Anand Sarwate (signal processing in networks).

BIBLIOGRAPHY

[1] Chaum, David L. "Untraceable electronic mail, return addresses, and digital pseudonyms." Communications of the ACM 24.2 (1981): 84-90.
[2] Diaz, Claudia, and Bart Preneel. "Taxonomy of mixes and dummy traffic." Information Security Management, Education and Privacy. Springer US, 2004. 217-232.
[3] Goldschlag, David M., Michael G. Reed, and Paul F. Syverson. "Hiding routing information." Information Hiding. Springer Berlin Heidelberg, 1996.
[4] Dingledine, Roger, Nick Mathewson, and Paul Syverson. "Tor: The second-generation onion router". Naval Research Lab Washington DC, 2004.
[5] F. Pérez-González and C. Troncoso, "Understanding statistical disclosure: A least squares approach," in Privacy Enhancing Technologies, 7384. Springer-Verlag, 2012, pp. 38–57.

[6] **S. Oya**, C. Troncoso, and F. Pérez-González, "Meet the family of statistical disclosure attacks," IEEE Global Conference on Signal and Information Processing, p. 4p, 2013.
[7] **S. Oya**, C. Troncoso, and F. Pérez-González, "Do dummies pay off? limits of dummy traffic protection in anonymous communications," in 14th Symposium on Privacy Enhancing Technologies, 2014.
[8] F. Pérez-González, C. Troncoso, and **S. Oya**, "A least squares approach to the static traffic analysis of high-latency anonymous communicationsystems," IEEE Transactions on Information Forensics and Security,vol. 9, no. 9, pp. 1341–1355, Sept 2014.
[9] **S. Oya**, C. Troncoso, and F. Pérez-González, "Understanding the effects of real-world behavior in statistical disclosure attacks," in IEEE Workshop on Information Forensics and Security, 2014.