SIGNAL PROCESSING FOR ANONYMOUS COMMUNICATIONS

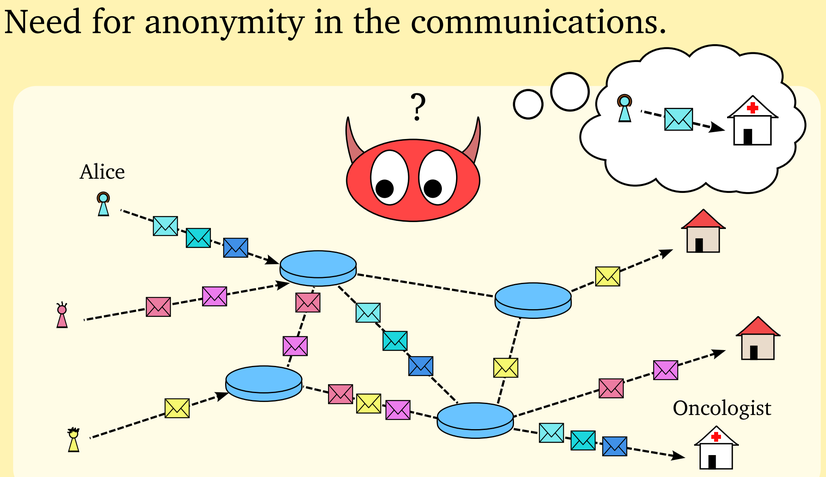
Simon Oya, Carmela Troncoso, and Fernando Pérez-González

simonoya@gts.uvigo.es carmela.troncoso@imdea.org fperez@gts.uvigo.es

Universidad de Vigo
GPSC
Signal Processing in Communications Group

MOTIVATION OF THE WORK

Need for anonymity in the communications.



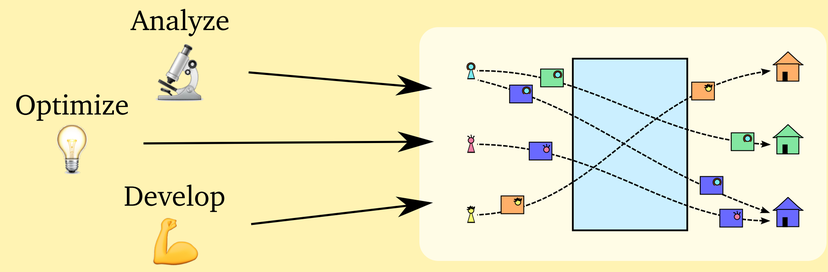
Current Analyses: Idea!! Signal Processing!

- 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.

THESIS OBJECTIVES

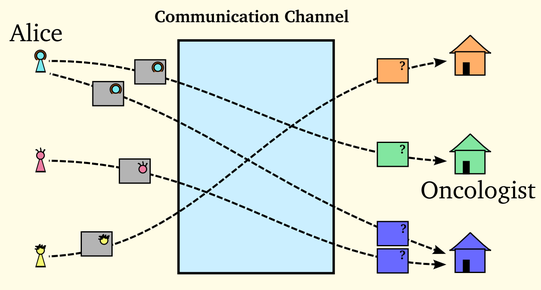
General objective

Apply signal processing tools to anonymous communications.



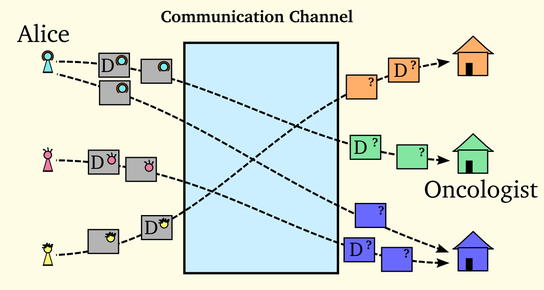
We will study two scenarios:

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



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

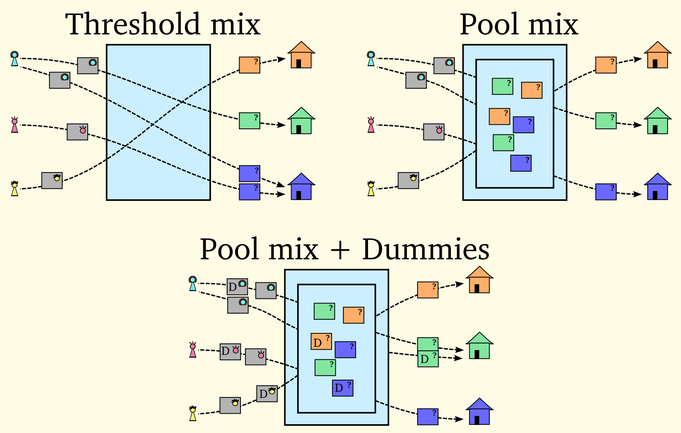
Low-latency communication systems [3][4] (e.g., instant messaging, VoIP, browsing).



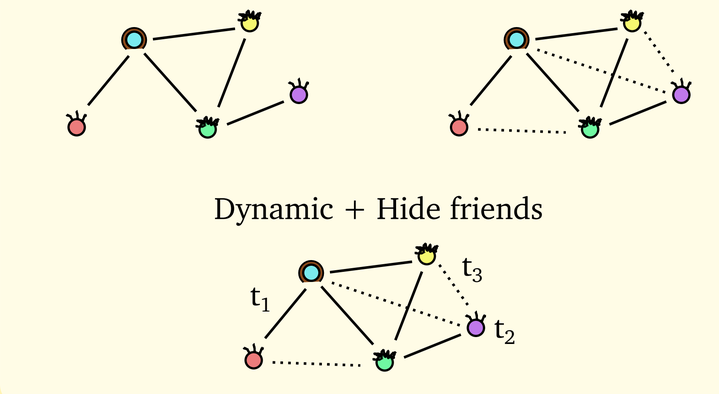
- Delaying messages is NOT allowed!!
- Explore other posibilities: dummy messages, re-routing...

RESEARCH PLAN

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



17 m.
- Low latency anonymous communications:



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.

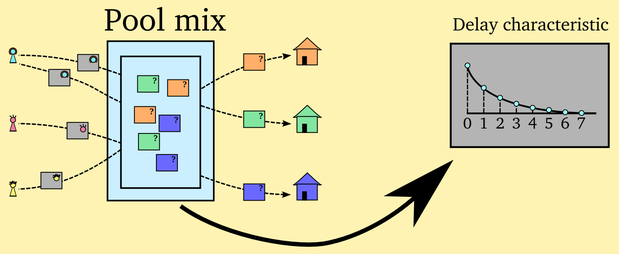
2 m.
- Wrapping up, conclusions and writing.

PREVIOUS RESULTS

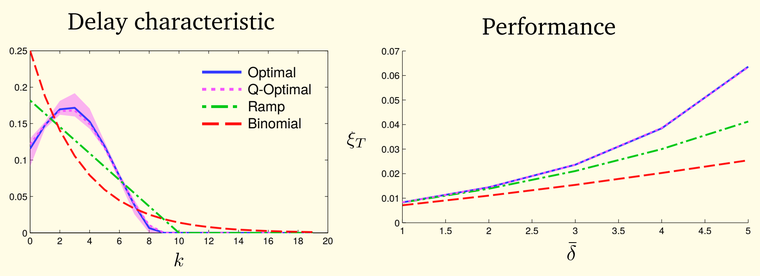
- Related work: new attack on mixes, the Least Squares Disclosure Attack (LSDA) [5].
- Proof that LSDA outperforms the family of statistical disclosure attacks [7].
- Analysis of a pool mix with dummies [8].
- In-depth study of LSDA on pool mixes [9].
- Analysis of the mix in real scenarios [10].

NEW RESULTS

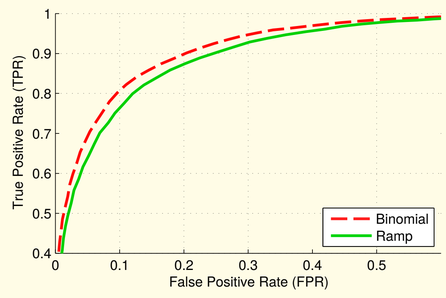
- Analysis of the pool mix in real scenarios. Optimal delay function for the pool mix [11].



Results with real data:



Performance under a traffic analysis attack [6].

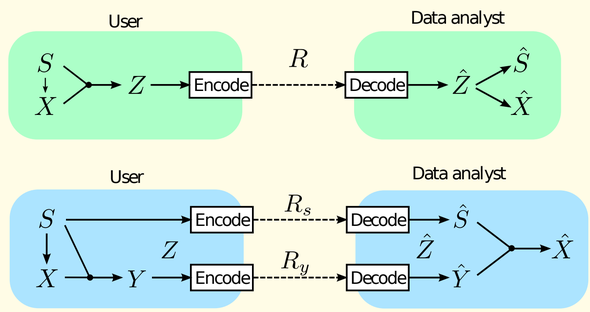


Analogy with a filter design problem.

→ Continue in future work?

- Privacy-Bandwidth-Utility trade-offs. Can we use bandwidth to provide privacy?

Started in **Rutgers University** (NJ) with Professor Anand Sarwate.



NEXT YEAR PLANNING

- Continue the work started in Rutgers University: can we use extra bandiwdth to provide privacy whithout worsening performance?
- Connect this work with mixes (mixes can be seen as devices that perform time quantization).
- Delve into the delay characteristic design problem as a filter design problem.

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] G. Danezis, “The traffic analysis of continuous-time mixes,” in Privacy Enhancing Technologies, 2005, pp. 35–50.

[7] **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.
[8] **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.
[9] 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.
[10] **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.

[11] **S. Oya**, F. Pérez-González, and C. Troncoso, "Design of Pool Mixes Against Profiling Attacks in Real Conditions", IEEE /ACM Transactions on Networking, 2016.