**Differential Privacy in Control and Network Systems: Literature Review**

**Abstract**

* Concerns are growing about the way that large-scale distributed monitoring and control systems collect and make use of privacy-sensitive data.
* This paper gives a systems and control perspective on privacy preserving data analysis.
* Specifically consider mechanisms enforcing differential privacy.
  + “Differential privacy: a state of the art definition of privacy initially introduced to analyse large, static datasets, and whose guarantees hold against adversaries with arbitrary side information.”
* This paper discusses how to perform tasks including signal estimation, consensus and distributed optimisation between multiple agents under differential privacy constraints.

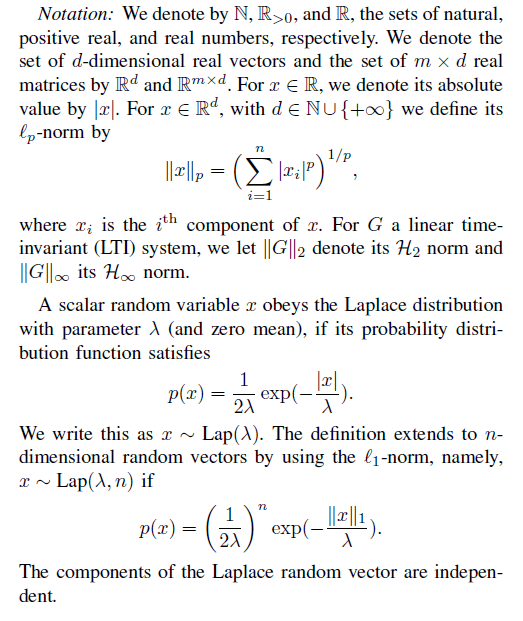
**Introduction**

* Heavy reliance on data collected from private individuals for distributed automated systems. These individuals naturally want to preserve the confidentiality of their own data.
* There’s an assumption that data aggregators are trustworthy. This is a risky assumption.
* The notion of differential privacy has emerged as a standard privacy specification.
  + A system processing privacy sensitive inputs is made differentially private by randomising its answers in such a way that the distribution over published outputs is not too sensitive to the data provided by any single participant.
* DP is being employed by Google (in Google Chrome web browser) and Apple (iOS 10 uses learning usage patterns without compromising individual privacy by using DP).
* DP has made its way into systems and controls where researchers have used it to design privacy-aware algorithms:
  + Control.
  + Average consensus.
  + Network topology.
  + Estimation and filtering.
  + Convex optimisation.

**Organisation**

* <Just lists the organisation of the document; sections 2 – 6>

**Notation**



**II: Foundations of Differential Privacy**