Privileged Estimate Fusion With Correlated Gaussian Keystreams

Marko Ristic
Autonomous Multisensor Systems Group (AMS),
Institute for Intelligent Cooperating Systems (ICS),
Otto von Guericke University (OVGU),
Magdeburg, Germany
Email: marko.ristic@ovgu.de

Benjamin Noack
Autonomous Multisensor Systems Group (AMS),
Institute for Intelligent Cooperating Systems (ICS),
Otto von Guericke University (OVGU),
Magdeburg, Germany
Email: benjamin.noack@ovgu.de

***Abstract*—The abstract goes here.**

I. Introduction

- $3/4$ of a page including abstract. Can be relatively similar to previous privilege paper.
- Role of estimation and increase in relevance of privacy and state secrecy.
- Usual methods hide all information, sometimes we want some leakage that can be used for a specific task.
- e.g. leakage of control inputs or leakage of information vector sums.
- Idea of privilege, e.g. GPS, chaotic systems.
- Interested in cryptographic quantisation, provided by previous paper which considers linear systems and uses the optimality of the Kalman filter. Doesn't consider the effect of dynaically adding more sensors and the fusion of their measurements.
- Contribution stated explicitly.
- Use case of the scenario, perhaps something where measurements are rare so synchronisation isn't a problem, like weather sensors. Alternatively something relating to cars.

A. Notation

- matrices, vectors.
- pseudorandom distribution.
- negligible fuction and covariance.

II. Problem Statement

- Want to provide levels of privileged estimation where multiple sensors are present and required for practical estimation accuracy.
- Want to gurantee two types of estimation privilege. The difference between estimation performance of unprivileged estimators (ones with no sensor keys) using all present sensors and privileged estimators using only measurements from sensors to which they have keys, should be bounded. Similarly, the difference in estimation performance of privileged estimators using only measurements from sensors to which they have keys and privileged estimators using measurements from all sensors (both ones to which they have keys and those to which they don't) should be bounded.
- The idea being that fusing many additional sensors to which you do not hold keys cannot provide the estimation benefits achieved from aquiring another sensor key.
- Will use the privileged estimation scheme definition from previous paper to cryptographically guarantee the bounds, but will consider measurements from all sensors at each timestep without loss of generality. We therefore consider linear systems only (equations, etc.).

III. Privileged Fusion

- The idea is to use correlated additive pseudorandom Gaussian noise at each sensor, which can only be removed from measurements produced by a specific sensor by an estimator holding the key for that sensor.
- To capture the correlation between measurements, we can consider the estimation problem of n sensors as the stacked equation (stacked eq with modified H and correlation matrix).
-

IV. Cryptographic Privilege

A. Unprivileged Adversaries

B. Privileged Adversaries

V. Simulation

VI. Conclusion

The conclusion goes here.

References

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.