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. Preliminaries

A. Cryptographic Estimation Privilege

- A series of covariances such that the difference between the best possible estimation from a privileged estimator and an unprivileged one is bounded by the series for all k.
- Give equations and definitions for privilege from previous paper.

B. Gaussian keystream

- A stream of pseudorandom Gaussian samples which relies on a key for it's generation. The sample are indistinguishable from a trully random stream of Gaussian samples to someone without the key, while someone with the key is able to replroduce the stream exactly.
- Equations for turning a stream cipher into a multivariate Gaussian stream.
- Note the assumption made about floating point numbers and why it is reasonable to use them as truly randomly generated reals in cryptography proofs.

IV. 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 C).

- Similarly to the pseudorandom Gaussian multivariate stream, we can generate noises for each sensor with correlation C by following the same process but using different keys to generate the standard Gaussians in the generation equation.
- Give equation for generating Gaussian noise in the stacked model, and how the measurement at each sensor at time k is modified accordingly.
- Computing this with an arbitrary $C^{1/2}$ however, would require an estimator hold all n keys to replicate the added noise locally before it can be removed. That is, each Gaussian in the resulting sensors noises vector p_i may depend on standard Gaussians z_i generated by all the other keys.
- Instead, finding a $C^{1/2}$ such that each p_i can be computed sequentially given only the keys $< i$ allows removing noises from some sensors depending on the keys that are held. It does hoever restrict the subsets of keys that can be used to remove noises to sequential keys i, and therefore also restricts the privileges that are available to estimators. In this case, there are n possible privileges, each holding one more key than the last (and allowing better estimation).
- These are the privilege levels and associated keys that we consider in this work and the cryptographic analysis ahead. Alternative method allowing for different subsets of keys to be sufficient for generating the relevant correlated noises are left for future work.
- We can now write the measurement equations for the measurements avaiable at a privileged estimator holding a key subset j as (j non-noised measuremend and $n - j$ noised ones - where the covariance is computed given the first j variables).
- This contrasts the measurements equations for the unprivileged esitmator (holding no keys) given by (single block equation, all sensors - or as many as they have access to).
- Intuitively, the correlation between added pseudorandom noise stops an unprivielged estimator from gaining too much information from fusing measurements, while the uncorrelation between them stops the using of one key available at a privileged estimator from being used to gain too much information from remaining measurements for which they do not hold a key.

V. Cryptographic Privilege

- To provide the cryptographic privilege provided by the presented multisensor scheme, we will rely on the optimality of the linear Kalman filter to produce series of covariances that are the best achieveable (smallest possible) for a given estimator, and take the difference between estimators in question to bound their difference.
- Similarly to the previous paper, the bounding series can be used in a cryptography sketch proof which shows that the existence of an estimator violating the bound would imply the existence of a better linear estimator than the Kalman filter, proved not to exist.
- We consider two types of unprivileged estimation which we want to bound, namely estimators holding no keys and estimators holding only a subset of keys.

A. Unprivileged Adversaries

-

B. Privileged Adversaries

-

VI. Simulation

VII. Conclusion

The conclusion goes here.

References

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