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 the 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 [1], chaotic systems.
- Interested in cryptographic quantisation, provided by the previous paper which considers linear systems and uses the optimality of the Kalman filter. Doesn't consider the effect of multiple privilege-providing sensors and the effect of fusing of their measurements without keys to obtain better estimates.
- Contribution stated explicitly.
- Use case of the scenario, perhaps something where measurements are infrequent so synchronisation isn't a problem, like weather sensors. Alternatively, something relating to privileged access to sensor features.

A. Notation

- Matrices, vectors.
- Positive definitness.
- Pseudorandom distribution.
- Estimator in cryptographic sense.
- Negligible fuction and negligible covariance.

II. Problem Formulation

- We are considering an environment where multiple sensors are present and required for the greatest estimation accuracy of the system they are measuring.
- We want to provide multiple levels of privilege to estimators, such that estimators with a higher level of privilege can achieve better estimates given the same measurements.
- We consider linear system and measurement models, given by the usual equations, which will make proving relevant cryptographic privileges straightforward. Each sensor i holds its own secret key sk_i, which can be made available to an estimator of a suitable privilege.
- While we are interested in a cryptographic difference in estimation between estimators who do and do not hold sensor keys, respectively, the involvement of multiple sensors means that access to additional sensors and the fusing of measurements from sensors whose key is not known also need to be considered.
- We want to provide a scheme for estimation privileges that guarantees two types of estimation differences.
- Firstly, we want a lower bound on the difference between estimation performance of an estimator that holds no sensor keys (an unprivileged estimator) but has access to all measurements, and an estimator holding a subset of sensor keys (a privileged estimator) using only measurements from sensors to which they hold a key. This construction means the bound remains a lower-bound when the unprivileged estimator has access to fewer sensors or when the privileged estimator has access to more and exhaustively captures the benefits of knowing sensor keys.
- Secondly, we want an upper bound on the additional estimation performance a privileged estimator can achieve by fusing measurements from sensors to which they do not hold a key. The motivation behind this guarantee is that fusing additional measurements from sensors whose keys are not known should not provide as much estimation benefit as acquiring another sensor key, thus preserving the order of possible estimation performance across privileges.
- The construction of the resulting scheme should be such that two free parameters can be chosen to control the values of these two bounds, respectively.

III. Preliminaries

A. Cryptographic Estimation Privilege

- The formal definition of a privileged estimation scheme was introduced in (previous paper) and captures a reduction in estimation performance that can always be achieved for an estimator not knowing the scheme key

compared to one knowing it and unmodified measurements.
- We will use a slight generalisation of this definition to capture an arbitrary difference in estimation that can always be achieved between estimators knowing and not knowing the scheme key, respectively.
- Give the definition of a privileged estimation scheme (Setup and Noise) but with modified Noise to allow the case that neither estimator has access to true measurements.
-
- 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.
- This now allows for an unprivileged estimator to have a potentially better estimate (but still bounded by how much better). Also, the matrices D in the definition itself no longer need to be valid covariances (since they can be 'negative').

B. Gaussian keystream

- A stream of pseudorandom Gaussian samples which relies on a key for its generation. The samples are indistinguishable from a truly random stream of Gaussian samples to someone without the key, while someone with the key can reproduce 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 the 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 to 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 however 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. An 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 available at a privileged estimator holding a key subset j as (j non-noised measurement and $n - j$ noised ones - where the covariance is computed given the first j variables).
- This contrasts the measurements equations for the unprivileged estimator (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 unprivileged 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 prove 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 achievable (smallest possible) for a given estimator, and take the difference between estimators in question to bound their difference and achieve cryptographic estimation privilege.
- Similarly to the previous paper, the bounding series can be used in a cryptographic 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, known not to exist. This then guarantees the bound by contrapositive.
- 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

- If we assume an unprivileged estimator can access all n sensors, then their stacked estimation model can be described by the appropriate equation at each timestep k.
- We can then write the combined Kalman predict and update equation as the equation with params from the previous one.

- Due to the KF preserving error covariance order, by setting $P_0 = 0$ we get a series of covariance such that no unprivileged estimator can estimate with error covariances less than or equal to the series (lower-bound).
- Similarly we can do the same for an estimator to which we want to lower-bound the estimation difference with the unprivileged estimator.
- A privileged estimator of privilege j (access to the first j keys) and that can only access the first j sensors, has the appropriate measurement equation. Similarly, setting the initial covariance to zero gives the lower bound series on the best possible estimation error achievable by the privileged estimator using only the measurements from the sensors to which it holds keys.
- Taking the difference of the two estimator bounding series' produces the difference series.
- In the context of cryptographic privileged estimation scheme, the Setup and Noise algorithms are given accordingly. The optimality of the KF can then be used to achieve the security notion.
- In the above, we assume the unprivileged estimator has access to all n sensors, while the j privilege estimator has access to only the first j sensors. In the case when the unprivileged estimator has access to fewer sensors or the privileged one to more, their difference in estimation can only increase, thus keeping the computed lower-bound a lower-bound and the cryptographic guarantee does not change (albeit the definitions of Setup and Noise will to capture the now available sets of measurements).

B. Privileged Adversaries

- We can use a similar approach to guarantee the largest possible benefit in estimation available to an estimator of privilege j (access to first j keys) by fusing measurements from sensors to which they do not hold keys to get a better state estimate.
- We can again write stacked estimation models for the two estimators and use the optimality of the KF to give their best possible performances as a series of covariances.
- Taking the difference of the bounds now gives a bound on how much better an estimate can become when unprivileged measurements are fused to the privileged ones.
- In the context of a cryptographic privileged estimation scheme, the Setup and Noise algorithms can be given as follows. KF optimality can then be used to achieve the security notion.
- We note that unlike in the unprivileged adversary case, or the previous paper, here we do not use unmodified measurements for the privileged estimates and the resulting algorithms provide better estimation for the adversary than the privileged estimator. In this form, we show bound how much better an adversary can estimate when using unprivileged estimates resulting in series D_k consisting of negative-definite rather than positive definite matrices.

VI. Simulation

- In addition to showing how to derive the bounds to the benefits of using unprivileged measurements, we have simulated concrete scenarios to demonstrate the methods.
- We consider the following linear system, and linear measurement models for 5 sensors. Correlated and uncorrelated noise covariances are given by Y and Z.
- Implementation details.
- First figure shows 4 plots. Each plot shows the traces of estimator covariances for the unprivileged estimator holding no keys, a privileged estimator holding $1, 2, 3$ and 4 keys, respectively (estimating only using the privileged measurements) and the difference between the privilege and unprivileged traces. The difference here is equal to the trace of the difference series given in the previous section (for each of the 4 privileges).
- The second figure will again show 4 plots. Now, each plot will show the traces of estimate covariances for the privileged estimator holding $1, 2, 3$ and 4 keys, respectively, estimating using only the privileged measurements and estimating with all measurements (fusing unprivileged ones as well). The difference between the two traces will be plotted as well, which will in the case be negative (as the difference here is negative definite) and again be equal to a difference series from the previous section.

VII. Conclusion

- Concluding remarks.
- Future work includes exploring key subsets that do not need to be sequential and decentralised methods for multi-key correlated noise generation.

References

[1] P. D. Groves, "Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems," *IEEE Aerospace and Electronic Systems Magazine*, vol. 30, no. 2, pp. 26–27, 2015.