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

- When defining our scheme and discussing it's cryptographic guarantees, we will make use of Gaussian keystreams and the notion of cryptographic estimation privilege. These have been summarised below.

A. Gaussian keystreams

- A Gaussian keystream is a sequence of pseudorandom Gaussian samples generated using a random key. The sequence is indistinguishable from a trully random Gaussian sequence to any observer that does not hold the key, while it is exactly reproducible if they do hold the key.
- A Gaussian keystream can be constructed from any cryptographic bitstream cipher, when making the floating-point randomness assumption.
- Give the assumption about floating-point numbers and why they are reasonable to use in place of truly random real numbers in cryptography proofs.
- Define the equations for turning a bitstream cipher into into a multivariate Gaussian stream with multivariate covariance denote S.

B. 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 two estimators given the measurements they have access to.
- Define a privileged estimation scheme (Setup and Noise) but with modified Noise to allow the case that neither estimator has access to true measurements.
- Define a privileged estimation scheme where series D_k can be positive or negative definite.
- We note that the difference in the generalised definition above is that the estimator for which we bound estimation performance, considered unprivileged, may perform better than the privileged estimator. That is, the difference series D_k may be negative-definite. This feature will be useful when discussing the additional estimation performance a privileged estimator can achieve by fusing measurements from sensors to which they do not hold a key.

IV. Privileged Fusion

- The idea behind the privileged fusion scheme is to add correlated Gaussian keystreams to measurements from each sensor, which can be removed by estimators holding the respective sensor secret keys.
- To exactly capture the correlation between the modified measurements, we will consider the stacked measurement model when having access to j sensors (stacked eq with modified $H^{(j)}$ and correlation matrix $C^{(j)}$, $j \leq n$).

A. Privileges

- Before we introduce the means of modifying measurements with sensor keys to affect the estimation performance for different privileges, we must also define the considered privilege levels in terms of access to sensor keys.
- In this work, we will consider privileges as knowing sequential sensor keys, in order to make correlated noise generation simpler.
- That is, in the presence of n sensors, we will consider exactly n possible privilege levels, where each privilege j corresponds to holding the sequential sensors' secret keys $sk_1, ..., sk_j$, while being unprivileged corresponds to holding no secret keys.
- As is intuitive, each succesive privilege level, knowing exactly one additional sensor key, will correspond to better estimation results than the previous levels or the unprivileged case.

B. Noise Generation

- Similarly to the Gaussian keystream introduced earlier, pseudorandom standard normal samples can be correlated when transformed together even when generated using different keys.
- To capture a correlation between additive noises from each sensor, we introduce the fully correlated component Z and the uncorrelated component Y and given n sensors we define the generated noise cross-correlation matrix as S (give equation).
- The generation of the additive nosies can then be computed with m standard normal pseudorandom samples generated from keys of each sensor with the following equation (using $S^{1/2}$) and added to the measurements at every timestep k as follows (give measurements equation with two noises).
- In the equation above, computing $S^{1/2}$ requires more than the simpler requirement in single sensor pseudorandom Gaussian keystream ($S^{1/2}S^{1/2} = S$)), as the form of the matrix $S^{1/2}$ will affect which subsets of keys are sufficient for partially computing the correlated noises. That is, privileged estimators that only hold a subset of sensor keys should still be able to generate the correlated pseudorandom Gaussian keystream for the subset of sensors for which they hold keys, but not for the remaining sensors.
- To achieve this, and support the privileges introduced in the previous subsection, a lower-triangular form of $S^{1/2}$ is required, for which we will use the Cholesky decomposition.
- In this form, an estimator of privilege j (holding keys $sk_1, ..., sk_j$, $j \leq n$), can correctly generate the noises for sensors $1, ..., j$ by computing (give partial generation equation up to sensor j).
- The subset of computed noises can then be removed from recieved sensor measurements
- Removing the added noise
- Using a cryptographically sound stream cipher in the generation of Gaussian samples above would mean that an estimator holding no keys
- Intuitively, the components Z and Y control the

-
- 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).
- 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.

C. Noise Distribution

-

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.