1. Hi everyone, my name is Marko Ristic, I’m with the Autonomous Multisensor Systems lab at the Otto von Guericke University in Magdeburg, Germany, and today I’ll give a talk on our paper on Privileged Estimate Fusion with Correlated Gaussian keystreams.
2. The broad context of the work is the application and provability of privacy within networks, and more specifically in state estimation within these networks. This has naturally become a greater concern with the increased prevalence of small network devices and the growing accessibility of public networks such as the internet. Problems are typically context specific and can be applied to a variety of networks, including private individuals, commercial parties and government bodies.
3. The concrete privacy problem that we’re interested in is privileged estimation. This problem captures the idea of estimation on a network where measurements are public but some special users are granted a privilege that allows then to get more information out of measurements. The goal in this scenario is that measurements are useful to some degree to everyone on the network but more useful to a select few. An example of this in practice is the original implementation of GPS where a second encrypted channel allowed better position estimation.
4. And as it is security that we’re interested in, in this scenario this is captured by formally guaranteeing a difference in performance between privileged and unprivileged estimators.
5. For those of you present at our virtual talk last year, you may remember that a single sensor scheme that achieves these goals was presented. In essence, additive cryptographically pseudorandom noise was added to measurements and removable by those holding a key.
6. Linear systems were considered to accompany cryptographic proofs and resulted in two measurement models holding different amount of information per measurement dependent on whether an estimator held a key or not. [picture][models]
7. This led to an intuitive difference in estimation performance, where privileged estimators, here green, performed better than unprivileged ones, here red. Ellipses here are the estimate error covariances and are larger for estimates made with more noisy estimates.
8. In addition to the intuitive performance difference, the key aspect of this scheme was the ability to prove the difference in performance in a cryptographic sense. Without going into detail in the presentation, cryptographic algorithms are defined and appropriate definitions including a negligible small covariance are defined before the notion of covariance privilege is presented. This notion allows to capture and prove the performance difference between estimators when models are such that optimal estimators exist, hence the linear models on the previous slide.
9. Now, the scenario we were interested given this scheme is the presence of multiple sensors. Here, each sensor has a key and estimators can hold some subset of these keys to obtain progressively better estimates than an unprivileged estimator that holds no keys.
10. What makes this scenario more interesting is that now there are two ways in which an estimator can obtain better estimates. Either by removing added pseudorandom noises from measurements that it has access to or by simply fusing more measurements. Of course, when we want to guarantee some privilege gained from holding keys, we want the first case to always make estimates better, but for fusing to only better estimates when corresponding keys are held as well.
11. To formalise the problem similarly to the single sensor case, we consider linear systems to aid cryptographic proofs about differences in estimations, but now have n different measurements and modification, for now, can be considered an action that produces some modified measurements using a secret key unique to each sensor. A small example on the right shows the measurements of 3 noises sensors of some path that estimators which to estimate.
12. In addition to the standard linear model assumption we formalise some notation and add assumptions on which sensors can be accessed to simplify notation as well as support number generation which I will get to later. We define an estimator as having access to q measurements and access to a subset p of the measurement keys.
13. The added assumptions we make are on this subset. We say that access to measurements is sequential, that is when q equals 3, an estimator has access to measurements 1,2 and 3, and similarly for privilege, where privilege encompasses having keys up to and including the privilege value p. Lastly, we also assume that when an estimator holds a key it also has access to the measurements associated with that key so simplify computing bounds.
14. This in essence lets us group estimators into three classes. Those with no keys that are unprivileged, those that only have access to the measurements for which they hold keys and those with more measurements than keys, which are all still sequential. It can also be noted here that the only assumption that affects the methods presented is that keys that are held are sequential, while the other assumptions are just there to make notation and explanation easier.
15. Now, with the problem defined, we can describe the performances that we are interested in. That is, how to capture this gain in performance when keys are held or when additional measurements are fused from a cryptographic point of view.
16. The first difference we’re interested in the performance loss lower bound. It is the difference between an estimator that holds keys for its measurements and one that holds no keys and is specific to a privilege p. Note that if the unprivileged estimator has access to fewer measurements or the privileged one to more measurements for which is does not hold a key, the bound remains a lower bound [explain on pic].
17. The second bound is the performance gain upper bound. It is the difference between the same estimator that hold keys to its measurements and one that has the same number of keys but also access to the remaining measurements. This is an upper bound as access to fewer remaining measurements can only decrease this difference.
18. The goal is for these bounds to be computable and capture minimum decrease in performance possible when not being privileged and the maximum performance increase when fusing unprivileged measurements. And needs to be computable for each privilege p you may be interested in.