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.