Encrypted Fast Covariance Intersection on the Cloud Without Leaking Weights

Marko Ristic[1] and Benjamin Noack[1]

***Abstract*— State estimate fusion is a common requirement in distributed sensor networks and can be complicated by untrusted participants or network eavesdroppers. We present a method for computing the common Fast Covariance Intersection fusion algorithm on an untrusted cloud without disclosing individual estimates or the fused result. In an existing solution to this problem, fusion weights corresponding to the sensor estimate errors are leaked to the cloud in order to perform the fusion. In this work, we present a method that guarantees no leakage at the cloud by requiring an additional computation step by the party querying the cloud for the fused result. The Paillier encryption scheme is used to homomorphically compute seperate parts of the computation that can be combined after decryption. This encrypted Fast Covariance Intersection algorithm can be used in scenarios where the fusing cloud is not trusted and relative sensor performances must remain confidential.**

I. Introduction

Data fusion and distributed state estimation have long been active fields of research and continue to find many applications in modern systems today []. Methods relying on the Kalman filter and derivatives [] have become particularly prevalent in this area due to their recursive structure and suitability to modelling estimate cross-correlations typically required for data fusion []. The handling of these cross-correlations is especially important when consistent or optimal fusion is desired [] and presents a key challenge in data fusion when they are not known in advance. To overcome this, some methods propagate cross-correlations through time at the cost of repeated reconstruction [] and typically add local computational complexity. Alternative methods approximate error cross-correlations with conservative suboptimal estimates to provide consistent fusion instead []. One such popular method is Covariance Intersection [] and it computationally inexpensive approximation, Fast Covariance Intersection []. These methods minimise fusion estimate error given possible conservative estimates and are popular due to their compatibility with the information form of the Kalman filter [].

While effective and often efficient, these data fusion solutions have traditionally been performed on closed networks with trusted participants and inherently imply a trust between sensors and estimators. In recent years, the ubiquity of distributed public networks has seen the additional challenges of security and privacy become increasingly relevant in distributed sensing environments and has led to an active field of reserach in providing security during data processing and fusion tasks [].

[1]Marko Ristic and Benjamin Noack are with the Autonomous Multisensor Systems Group (AMS), Institute for Intelligent Cooperating Systems (ICS), Otto von Guericke University (OVGU), Magdeburg, Germany {marko.ristic, benjamin.noack}@ovgu.de