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.**

[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