Dissertation for the Faculty of Computer Science (FIN),
Otto von Guericke University (OVGU), Magdeburg

Data Confidentiality for Distributed Sensor Fusion

Marko Ristic

August 11, 2022

Reviewers:

Prof. Dr.-Ing. Benjamin Noack (OVGU, Magdeburg, Germany)

...

Contents

Acknowledgements

Acks go here.

Abstract

Distributed sensing and fusion algorithms are increasingly present in public computing networks and have led to a natural concern for data security in these environments. This thesis aims to present generalisable data fusion algorithms that simultaneously provide strict cryptographic guarantees on user data confidentiality. While fusion algorithms providing some degrees of security guarantees exist, these are typically either provided at the cost of solution generality or lack formal security proofs. Here, novel cryptographic constructs and state-of-the-art encryption schemes are used to develop formal security guarantees for new and generalised data fusion algorithms. Industry standard Kalman filter derivates are modified and existing schemes abstracted such that novel cryptographic notions capturing the required communications can be formalised, while simulations provide an anlysis of practicality. Due to the generality of the presented solutions, broad applications are supported, including autonomous vehicle communications, smart sensor networks and distributed localisation.

Kurzfassung

German abs goes here.

Notation

Complete notation here.

1. Introduction

Data fusion and state estimation growing in application

Growing distributed networks have put a greater stress on the need for broadly applicable data fusion algorithms that support processing of different types of measurements and estimates with different accuracies and availabilities

examples

The use of Bayesian estimation methods, in particular the popular Kalman filter and its non-linear derivatives have found particularly prevalent applications due to their recursive and often optimal estimation properties

The filters also allow modelling of cross correlations between local estimates, a common cause of challenges in estimation theory, and a requirement for consistent or optimal fusion.

While the challenges faced due to the correlations between error statistics have existed for some time and have been well studied, the advancements in distributed algorithms, cloud computing and public networks are bringing additional security oriented challenges to estimation solutions.

privacy and security

can use normal RSA and AES

more complicated examples have different requirements where these are not suitable

more complicated schemes

differential privacy as a statistical security

Due to the nature of cryptographic goals and proofs in distributed environments, security goals in estimation and fusion are often very context specific and have led to numerous solutions for various scenarios and security desires

leads us into the state-of-the-art

1.1. State-of-the-Art and Research Questions

As mentioned in the previous section, the nature of cryptographic notions in distributed environments typically requires communications between participating parties to be known exactly. This in turn has lead to many, otherwise general estimation algorithms, to be restricted in some way to make communication and security easier to discuss.

For example, [aristov] presents a distributed Kalman filter, namely an Information filter, where sensor measurements and measurement errors are kept private to the measuring sensors only, while the final estimation update (sum of this information) is leaked to an estimator. For this to be achieved, however, sensors must form a heirachical communication structure and measurement models must be linear, restricting the otherwise more broadly applicable information filter and its non-linear variants.

[proloc]
pwsac and pwsah papers
aggregation papers
differentially private kalman filtering
privacy-preserving optimisation with security based on statistical estimation
added noise estimation
–
privacy preserving image based localisation
eavesdropper paper with a secure return channel and a lossier channel for eavedroppers
GPS
chaotic system paper
physical layer noise paper (similar to chaotic noise paper)
–

The two different approaches, restricting existing broad estimation methods in some ways to make cryptgraphic analysis plausible and ignoring formal security when assumptions and conclusions are intuitive demontrate a gap in the existing literature and brings us to the target research topics this thesis aims explore.

- dot point topics

These broad topics aim to fulfil the goal of generalisable but cryptographically provable estimation and fusion methods in distributed environments and leads to the concrete problems tackled in this work

1.2. Contributions

The contributions tackle the research topics in section .. by considering three concrete problems that coincide with the broader problems in the field

1.3. Thesis Structure

2. Preliminaries

2.1. Estimation Preliminaries

2.1.1. Kalman Filter

2.1.2. Kalman Filter Optimality

2.1.3. Extended Kalman Filter

2.1.4. Information Filter

2.1.5. Extended Information Filter

2.1.6. Fast Covariance Intersection

2.2. Encryption Preliminaries

2.2.1. Meeting Cryptographic Notions

2.2.2. Paillier Homomorphic Encryption Scheme

2.2.3. Joye-Libert Aggregation Scheme

2.2.4. Lewi Order-Revealing Encryption Scheme

2.2.5. Encoding Numbers for Encryption

3. Estimate Fusion on an Untrusted Cloud

3.1. Problem Formulation

3.2. Related Literature

3.3. Confidential Cloud Fusion Leaking Fusion Weights

3.4. Confidential Cloud Fusion Without Leakage

3.5. Conclusions

4. Distributed Non-Linear Measurement Fusion with Untrusted Participants

4.1. Problem Formulation

4.2. Related Literature

4.3. Confidential Range-Only Localisation

4.3.1. Unidirectional Alternative

4.3.2. Solvable Sub-Class of Non-Linear Measurement Models

4.4. Conclusions

5. Provable Estimation Performances

5.1. Problem Formulation

5.2. Related Literature

5.3. Covariance Privilege

5.4. Privileged Estimation for Linear Systems

5.4.1. Extension to Non-Linear Systems

5.5. Conclusions

6. Conclusion

A. Linear-Combination Aggregator Obliviousness

B. Cryptographic Proof of LCAO Scheme Security

List of Figures

List of Tables