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

Data Confidentiality for Distributed Sensor Fusion

Marko Ristic

August 3, 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

1.1. Thesis Structure

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

3. Preliminaries

3.1. Estimation Preliminaries

3.1.1. Kalman Filter

3.1.2. Kalman Filter Optimality

3.1.3. Extended Kalman Filter

3.1.4. Information Filter

3.1.5. Extended Information Filter

3.2. Encryption Preliminaries

3.2.1. Meeting Cryptographic Notions

3.2.2. Paillier Homomorphic Encryption Scheme

3.2.3. Joye-Libert Aggregation Scheme

3.2.4. Lewi Order-Revealing Encryption Scheme

4. Estimate Fusion on an Untrusted Cloud

4.1. Problem Formulation

4.2. Related Literature

4.3. Confidential Cloud Fusion Leaking Fusion Weights

4.4. Confidential Cloud Fusion Without Leakage

4.5. Conclusions

5. Distributed Non-Linear Measurement Fusion with Untrusted Participants

5.1. Problem Formulation

5.2. Related Literature

5.3. Confidential Range-Only Localisation

5.3.1. Unidirectional Alternative

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

5.4. Conclusions

6. Provable Estimation Performances

6.1. Problem Formulation

6.2. Related Literature

6.3. Covariance Privilege

6.4. Privileged Estimation for Linear Systems

6.4.1. Extension to Non-Linear Systems

6.5. Conclusions

7. Conclusion

A. Linear-Combination Aggregator Obliviousness

B. Cryptographic Proof of LCAO Scheme Security

List of Figures

List of Tables