Article

Localisation and Sensor Privacy Using the Extended Information Filter and Secure Weighted Aggregation

Marko Ristic [1], Benjamin Noack [1] and Uwe D. Hanebeck [1,*]

[1] Intelligent Sensor-Actuator-systems Laboratory, Institute for Anthropomatics, Karlsruhe Institute of Technology, 76131 Karlsruhe, Germany; marko.ristic@kit.edu; noack@kit.edu; uwe.hanebeck@kit.edu
* Correspondence: uwe.hanebeck@kit.edu; Tel.: +49-721-608-43909

Version July 24, 2020 submitted to Sensors

Abstract: Distributed state estimation and localisation methods have become increasingly popular with the rise of ubiquitous computing, and have led naturally to an increased concern regarding data and estimation privacy. Traditional distributed sensor navigation methods involve the leakage of sensor information or navigator location during localisation protocols and fail to preserve participants' data privacy. Secure existing methods fail to address sensor and navigator privacy in some common model-based non-linear measurement localisation methods forfeiting broad applicability. We define a modified, cryptographically secure, weighted aggregation scheme which we apply to the Extended Kalman Filter with range-sensor measurements, and show that navigator location, sensor locations and sensor measurements can remain private during navigation. The requirements and cryptographic proof are given for the weighted aggregation scheme, and simulations of the private filter are used to evaluate the accuracy and performance of the method. Our approach defines a novel, computationally plausible and cryptographically private, model-based localisation filter with direct application to environments where nodes may not be fully trusted and data is considered sensitive.

Keywords: Extended Kalman Filter; Secure Localisation; Private Aggregation

---

1. Introduction

Introduce localisation, filtering and the need for privacy.

Examples of environments where privacy is relevant and concrete examples where lack of privacy could have large costs

Methods for introducing security and privacy include differential privacy methods and encryption methods.

Differential privacy involves using statistical noise as security to make individual users' information cannot be deduced. Often requires a trusted aggregator, although secure aggregation methods exist. always requires noising result such that the outcome is not exact (a problem in localisation).

Encryption schemes involve formal indistinguishability proofs typically over bits or integers. They rely on computationally hard problems involving security parameters of a sufficiently large size; therefore the additional computational requirements of using encryption schemes should be pointed out and what this means in a real-time distributed sensor system. Continuing, explain public-key cryptography applicability to distributed systems; difference to symmetric schemes. Homomorphic encryption power and use case. Why FHE isn't used often, why additive partially homomorphic encryption is.

Advancements in function providing encryption schemes such as homomorphic encryption have also led to several other types of schemes which have found uses in signal processing. Private aggregation schemes allow the secure computation of the sum of encrypted values originating from different parties, leaking only the final result. When considering such multi-party encryption protocols, formal security definitions must now also incorporate the added dangers of colluding malicious parties, and lead to new notions of security. For example Aggregator Obliviousness (AO) is typically proven for private aggregation schemes, while alternatives such as Private Weighted Secure Aggregator Obliviousness (pWSAO) exist for other specific use-cases.

Another example of function providing encryption, and a generalisation of private aggregation, is called functional encryption (FE) and its distributed extension, multi-client functional encryption (MCFE), which allow the unencrypted result of an arbitrary function to be computed from encrypted inputs. General FE and MCFE are known to be quite computationally expensive (from meeting with ITI and student Johannes - need ref.) but alternatives providing only a subset of possibly computable function exist; for example, inner product encryption.

Several of the aforementioned encryption schemes have found uses in secure localisation, estimation, and control.

1.1. Relevant Literature on Encrypted Localisation and Estimation

Model-free localisation using homomorphic encryption examples include polygon thing, WSN examples which protect against adversaries but in the case of the WSN paper. don't preserve anchor privacy. Importantly, model-based filtering and localisation provide more accurate estimates and these are not applicable there.

Model-based estimation examples include Aristov paper (which requires a linear model, and a hierarchy of sensors), Farokhi paper (which requires the controller compute entirely in encrypted space and send input back to actuator - supporting only cloud as a service type architectures) and Alexandru paper (which implements a distributed control environment but requires a constant gain matrix K)

pWSAO achieved in Alexandru weighted aggregation, but requires redistributing keys at every timestep resulting in a costly operation, and a complicated communication protocol.

In addition to applying suitable encryption schemes to signal processing tasks, care must be taken when converting sensor output into an encryptable homomorphic format. As is the case with our proposed localisation method, real number sensor output doesnot trivially encode to integers such that the homomorphic properties provided by an additive encryption scheme over integers keep the underlying real numbers consistent. Methods for handling the encoding of real numbers such that they can be used in homomorphic encryption exist. Google bignum adds power but risks overflow and leaks exponents, Farokhi leaks no information but allows only a single multiplication (extendable to more but each further multiplication limits the real number size and increases the risk of overflow).

Briefly describe navigator scenario and our contributions

Section Summary

1.2. Notation

Notation

2. Problem Statement

Restate the scenario but more formally. Give concrete example - plane and signal towers.

Exact security guarantees we aim for, as well as the definitions for these guarantees (pWSAO and indistinguishability but in context of localisation as well). Note that learning only the sum in aggregation (as is normal in AO) would in this case tell the navigator the average location and measurements of all sensors, which is fine as it does not disclose any exact sensor.

Passive attacks only from sensors to learn navigator position (Otherwise could do some kind of attack that would send fake measurement and note the change in it's own measurements - possible this would give away average of other sensors' measurements but unclear). Any largely incorrect inputs from sensors may also be detectable by comparison to alternative navigator onboard sensors (GPS etc.). Justify by saying sensors need to behave for localisation to work in the first place.

Active attacks from navigator to find sensor location allowed, but assume that weights sent to all sensors are the same. In a wireless setting all sensors would recieve all broadcast weights anyway. While special hardware which would support directional broadcasting and recieving could be used to locate sensors individually this is beyond the scope of what is considered in our problem.

Point out that learning the aggregation of sensor outputs, which contains measurement and location information also means that the average location and measurment of the sensors may be leaked, and is accepted as a part of the leakage as it is inferrable from the aggregation scheme and any functioning model-based localisation where measuremments are not known

Rough computational capabilities expected by parties

Fixed sensor subsets of which only whole subsets can be used at once. Maybe a picture of what this might look like in a high level distributed localisation diagram. Should consider that this subt grouping would also mean the leakage of the average sensor/measurment of each subset not all sensors at once. This should be considered when choosing sensor subsets and locations.

3. Private Weighted Aggregation Preliminaries

3.1. Paillier Encryption Scheme

3.2. Joye-Libert Privacy-Preserving Aggregation

4. Private Weighted Aggregation

Explain it in overview

4.1. Proof

Give the reduction proof here for pWSAO and implicit indistinguishability of weights. alternatively sketch it out here and give reduction in appendix.

5. Private Localisation Preliminaries

5.1. Integer Encoding for Real Numbers

5.2. Extended Information Filter

6. Private Localisation with Privacy-Preserving Sensors

Explain it in overview. How is the aggregation scheme used, what does this require from the measurement model, why can this be a problem for normal distance sensors.

Explain how leakage of the final aggregation sum to the navigator means leakage of the average sensor location and meausurement to the navigator. This is the reason for the accaptance of this leakage, as we pointed out in the problem statement section.

6.1. Requirements for Measurement Model

6.2. Localisation Measurement Modification

Show here the weighted integrals that give mean and variance of the new noise. If wanting to show more working, do this in appendix section, but probably not needed.

Point out here that the further away the sensor is when it makes its distance measurement (the larger the measurement) the more Gaussian the noise and the better the filter. Give flight navigation as an applicable example with typically high distances.

Additionally increased range accuracy may be possible when sensors know the process model of the navigator, allowing them to run their own filter (more accurate than only measumrements but not as accurate as the navigator's estimate from multiple sensors) and use their filtered estimated distance as the scaling factor when computing the modified measurement variance.

6.3. Expanding Aggregation for Multi-dimensional Inputs

Give 1D example that's intuitive (with a^2b) and then reduce the equivalent ND case ($A^\top BA$) to a set of weighted sums.

Ensure that timestamps are concatenated with position so that no aggregation values are blinded by the same noise.

6.4. Algorithm

Piece together the whole algorithm here. Give the algorithm as a pseudocode (including encoding and encryption)

7. Results

Decide on what kind of simulations and which plots to make. run times would be nice this time around

Time results can be captured in one graph. Y axis is time, x axis in number of sensors, each line (different colour) will show how the runtime changes as sensors are increased for different Paillier bitsizes (at least 3: 512, 1024, 2048). Every data point should be the average over some X number of simulations.

Accuracy plots will describe error due to encoding, number of sensors (more adding may increase error in encoding), and the average distance of the sensors to the navigator. All plots will use the same ground truth and initial state and covariance estimates (this way average error at each timestep from multiple runs makes sense).

Plot 1 will plot the RMSE of the average of X runs at each encoding size. A fixed layout of 4 mediumly spaced sensor will be used, and a fixed Paillier bit size.

Plot 2 will plot the RMSE of the average of X runs with different numbers of sensors. A fixed encoding method will be used, and a fixed Paillier bit size.

Plot 3 will plot the RMSE as the average distance of sensors changes. Fixed encoding and Paillier bit size. Vary between 4 layouts where 4 sensors are either very close to the center (and ground truth, and progressivly further out)

Plot 4 will accompany plot 3 and display the 4 layours (arrow for ground truth and points for the sensors).

8. Conclusion

Possible future work to consider writing here: Hardware implementations, measurement handling which preservers Gaussian noise, or non-Gaussian noise methods, ways of sending less information form the navigator to the sensors at each time step, active sensor attacker model, different state encryptions recieved at sensors.

<Rest is template>

9. How to Use this Template

The template details the sections that can be used in a manuscript. Note that the order and names of article sections may differ from the requirements of the journal (e.g., the positioning of the Materials and Methods section). Please check the instructions for authors page of the journal to verify the correct order and names. For any questions, please contact the editorial office of the journal or support@mdpi.com. For LaTeX related questions please contact latex@mdpi.com.

10. Introduction

The introduction should briefly place the study in a broad context and highlight why it is important. It should define the purpose of the work and its significance. The current state of the research field should be reviewed carefully and key publications cited. Please highlight controversial and diverging hypotheses when necessary. Finally, briefly mention the main aim of the work and highlight the principal conclusions. As far as possible, please keep the introduction comprehensible to scientists outside your particular field of research. Citing a journal paper [1]. And now citing a book reference [2]. Please use the command [1] for the following MDPI journals, which use author-date citation: Administrative Sciences, Arts, Econometrics, Economies, Genealogy, Humanities, IJFS, JRFM, Languages, Laws, Religions, Risks, Social Sciences.

11. Results

This section may be divided by subheadings. It should provide a concise and precise description of the experimental results, their interpretation as well as the experimental conclusions that can be drawn.

> This section may be divided by subheadings. It should provide a concise and precise description of the experimental results, their interpretation as well as the experimental conclusions that can be drawn.

11.1. Subsection

11.1.1. Subsubsection

Bulleted lists look like this:

- First bullet
- Second bullet
- Third bullet

Numbered lists can be added as follows:

1. First item
2. Second item
3. Third item

The text continues here.

11.2. Figures, Tables and Schemes

All figures and tables should be cited in the main text as Figure 1, Table 1, etc.

Figure 1. This is a figure, Schemes follow the same formatting. If there are multiple panels, they should be listed as: (**a**) Description of what is contained in the first panel. (**b**) Description of what is contained in the second panel. Figures should be placed in the main text near to the first time they are cited. A caption on a single line should be centered.

Text
Text

Table 1. This is a table caption. Tables should be placed in the main text near to the first time they are cited.

Title 1	**Title 2**	**Title 3**
entry 1	data	data
entry 2	data	data

Text

Text

11.3. Formatting of Mathematical Components

This is an example of an equation:

$$a + b = c \tag{1}$$

Please punctuate equations as regular text. Theorem-type environments (including propositions, lemmas, corollaries etc.) can be formatted as follows:

Theorem 1. *Example text of a theorem.*

The text continues here. Proofs must be formatted as follows:

Proof of Theorem 1. Text of the proof. Note that the phrase 'of Theorem 1' is optional if it is clear which theorem is being referred to. □

The text continues here.

12. Discussion

Authors should discuss the results and how they can be interpreted in perspective of previous studies and of the working hypotheses. The findings and their implications should be discussed in the broadest context possible. Future research directions may also be highlighted.

13. Materials and Methods

Materials and Methods should be described with sufficient details to allow others to replicate and build on published results. Please note that publication of your manuscript implicates that you must make all materials, data, computer code, and protocols associated with the publication available to readers. Please disclose at the submission stage any restrictions on the availability of materials or information. New methods and protocols should be described in detail while well-established methods can be briefly described and appropriately cited.

Research manuscripts reporting large datasets that are deposited in a publicly available database should specify where the data have been deposited and provide the relevant accession numbers. If the accession numbers have not yet been obtained at the time of submission, please state that they will be provided during review. They must be provided prior to publication.

Interventionary studies involving animals or humans, and other studies require ethical approval must list the authority that provided approval and the corresponding ethical approval code.

14. Conclusions

This section is not mandatory, but can be added to the manuscript if the discussion is unusually long or complex.

15. Patents

This section is not mandatory, but may be added if there are patents resulting from the work reported in this manuscript.

Author Contributions: For research articles with several authors, a short paragraph specifying their individual contributions must be provided. The following statements should be used "Conceptualization, X.X. and Y.Y.; methodology, X.X.; software, X.X.; validation, X.X., Y.Y. and Z.Z.; formal analysis, X.X.; investigation, X.X.; resources, X.X.; data curation, X.X.; writing–original draft preparation, X.X.; writing–review and editing, X.X.; visualization, X.X.; supervision, X.X.; project administration, X.X.; funding acquisition, Y.Y. All authors have read and agreed to the published version of the manuscript.", please turn to the CRediT taxonomy for the term explanation. Authorship must be limited to those who have contributed substantially to the work reported.

Funding: Please add: "This research received no external funding" or "This research was funded by NAME OF FUNDER grant number XXX." and and "The APC was funded by XXX". Check carefully that the details given are accurate and use the standard spelling of funding agency names at https://search.crossref.org/funding, any errors may affect your future funding.

Acknowledgments: In this section you can acknowledge any support given which is not covered by the author contribution or funding sections. This may include administrative and technical support, or donations in kind (e.g., materials used for experiments).

Conflicts of Interest: Declare conflicts of interest or state "The authors declare no conflict of interest." Authors must identify and declare any personal circumstances or interest that may be perceived as inappropriately influencing the representation or interpretation of reported research results. Any role of the funders in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript, or in the decision to publish the results must be declared in this section. If there is no role, please state "The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results".

Abbreviations

The following abbreviations are used in this manuscript:

MDPI	Multidisciplinary Digital Publishing Institute
DOAJ	Directory of open access journals
TLA	Three letter acronym
LD	linear dichroism

Appendix A

Appendix A.1

The appendix is an optional section that can contain details and data supplemental to the main text. For example, explanations of experimental details that would disrupt the flow of the main text, but nonetheless remain crucial to understanding and reproducing the research shown; figures of replicates for experiments of which representative data is shown in the main text can be added here if brief, or as Supplementary data. Mathematical proofs of results not central to the paper can be added as an appendix.

Appendix B

All appendix sections must be cited in the main text. In the appendixes, Figures, Tables, etc. should be labeled starting with 'A', e.g., Figure A1, Figure A2, etc.

References

1. Author1, T. The title of the cited article. *Journal Abbreviation* **2008**, *10*, 142–149.
2. Author2, L. The title of the cited contribution. In *The Book Title*; Editor1, F., Editor2, A., Eds.; Publishing House: City, Country, 2007; pp. 32–58.

Sample Availability: Samples of the compounds ...... are available from the authors.