Privacy-Preserving Localization Using Private Linear-Combination Aggregation

Response to Reviewers' Comments - Submission IEEE-TAC 20-2108

Marko Ristic Benjamin Noack Uwe D. Hanebeck

June 16, 2021

Dear Dr. Zhiwei Gao,
Dear Reviewers,

We would like to thank you all for your thorough and helpful reviews. In this letter, we will describe how editor and reviewer comments, questions and suggestions have been addressed. Throughout this response, reviewers' comments are in blue.

Sincerely,
Marko Ristic, Benjamin Noack, and Uwe D. Hanebeck

Response to the Editor's Report

E.1 Based on the reviews, it is our decision that the paper cannot be accepted for publication in the Transactions in its present form.

The reviewers feel the paper interesting, which many include publishable materials. On the other hand, the reviewers feel the paper should be reorganized by shortening the length (e.g. introduction etc.), and highlight the novelty and contribution. Also the relevance of the paper to the journal should be clarified.

Thank you for the response. We have undertaken a large overhaul of the manuscript in order to accommodate the suggested changes of the reviewers. The work has been shortened by four pages, the introduction shortened to a single page and the novelty of our method clearly stated within it. We state the estimation problem tackled, namely, a modified EKF estimator for range-only sensor localisation with specific security requirements, and its benefits over existing and comparable approaches. We believe that the more clarified contribution and novelty also better justify the relevance of the paper to the TAC journal.

E.2 We encourage you to examine carefully the comments of the enclosed reviews and to consider making a major revision of the paper, which can be resubmitted as a Technical Note, to the Transactions on Automatic Control. If you do submit a revised version of the paper as a Technical Note, you should take care that the paper is reduced to no more than 8 double-column pages using IEEE template.

In your letter of transmittal, you should include a detailed "author's response" document describing the changes in the paper and you should refer to the present paper number.

Please login, click on the "Author" link at the bottom of your access page, and upload your technical note under the SAME reference number. A new reference number will be assigned to your revised paper.

After a large revision of our manuscript, including the suggested additions and modifications from the reviewers, we have rearranged and greatly shortened the work (in particular the introduction and cryptography sections, but all sections have been partially modified to be clearer). Due to the novelty

of the tackled problem and the cryptographically backed solution, the manuscript, albeit four pages shorter, is still too long for submission as a Technical Note, and we would like to resubmit the work as a full paper again. We hope that this decision is made clearer from the newly revised and rearranged manuscript. Below, we have detailed how each of the reviewer comments have been taken into account when revising the work.

Response to the Comments of Reviewer 1 (222511)

R1.1 This paper concerns the localization problem under privacy constraints. Cryptographic schemes have been devised by the authors to achieve some privacy requirements. The contribution is significant enough and the paper is well written but hard to understand for a usual reader of IEEE TAC due to sections with cryptographic background.

We thank the reviewer for their comment on our contribution and are sorry that the work was not made easier to understand. We have rearranged the paper to make both the problem tackled and the solution presented easier to follow and more concise. Additionally, we have greatly reduced the amount of cryptographic background presented, and hope that these changes make the work much easier to follow for the usual target audience of IEEE TAC.

R1.2 As a TAC paper, performance analysis in terms of estimation accuracy was expected but is actually missing.

We regret that the method of analysis for our approach was not made clearer. As the proposed method we present is inherently a modified EKF, we directly compare the estimation accuracy of our method to the industry standard EKF (EIF reformulation in our case). To make this clearer, we have rewritten the results section to portray this evaluation better and changed the results figure to be far more legible. Direct comparisons between the EIF and our method are now made for each simulation considered, and the estimation error (accuracy of the filters) can be seen much more clearly. We hope this makes the evaluation of the presented method easier to understand.

R1.3 This reviewer wonders if IEEE TAC is well adapted for an efficient exposition of the authors' findings.

We understand that the state of the initial submission was not as well suited to the TAC journal as could be desired and thank the reviewer for pointing this out. Existing literature published at TAC and concerning cryptographic constructs (for example, "Cloud-based quadratic optimization with partially homomorphic encryption" by Andreea Alexandru et al.), has been used as reference during our revision. For the resubmission, we have greatly reduced the cryptographic components of the work and stated our contribution and its novelty more clearly to clarify the suitability of the proposed estimation method to the TAC journal. We will additionally consider some of the heavier cryptographic computations presented for an alternative submission elsewhere.

R1.4 In the framework of a Control theory paper, cryptographic notions would be kept as minimum as possible in the main body of the paper or moved to Appendices.

As above, we regret that the quantity of presented cryptographic content was so poorly suited to the context of TAC and have greatly modified the work to make it a better fit. Much of the cryptographic discussion has been removed and the remaining, necessary but dense, novel notions have been put in the appendix. We hope this makes the work better suited in the context of TAC.

Response to the Comments of Reviewer 2 (222527)

R2.1 This paper deals with a suitable notion of linear-combination aggregation encryption and provides a cryptographically secure instance applied to a filter with range-sensor measurements. This approach keeps navigator location, sensor's location and sensors' measurements private during navigation.

The proposed approach is interesting and the results are technically sound. The literature review is

OK. But the organization of paper and its length make its reading difficult.

The reviewer encourages the authors to reorganize the article by greatly shortening it and to highlight the novelty.

We're happy to hear that the results were found interesting and regret that the length and organisation have made the manuscript hard to read. We have heavily reorganised and rewritten parts of the work to make it easier to follow, including shortening the work by four pages. We hope that the flow of information is now easier to follow and that the method is more concisely described.

R2.2 Some additional comments are given below:

-Introduction (2 pages) is too long and does not focus on the main ideas of the paper. There are too many reminders of classical notions.

We're sorry that the introduction was found too long and agree that it could be made shorter. We have now greatly reduced the length of the introduction and removed a lot of the cryptographic reminders throughout the work. We hope that the new layout is easier to read and follow.

R2.3 -Equation (3): i from 1 to n must be added.

Thank you for pointing this out, this has now been added to the manuscript.

R2.4 -The actual computation steps are in fact scattered all over the paper, in several sections. In the current version, the reader has to collect all the scattered pieces to come out with the approach. I would therefore, strongly recommend the authors to summarize all the steps of the approach gathered by the end of the paper, to help the reader directly use and implement the algorithm.

Due to the number of components in the proposed method (encoding, encryption and estimation), we aimed to present the algorithm pseudocode as the summary of the method, and regret that this was not made clearer. We have rewritten and reorganised the localisation section and have tried to make a pseudocode summary, and its purpose, clearer. We hope that the updated manuscript now presents a better overall summary after all the components are presented.

R2.5 -Page 10, Equation (36), Right part of Equation: d is from 0 to D

This was indeed missing. After shortening the paper, this subsection was removed and the equation is no longer there, but we thank you for pointing it out regardless.

R2.6 -Inequality (50) must be clarified,

We apologies for not making this clearer. The section has been modified and the reason for adding standard deviations to give a conservative estimate has been rewritten and clarified.

R2.7 -Algorithm 1, steps 2/3/4, it is F_{k-1},

Thank you for pointing this out. This was due to an error in notation in a previous section which gave incorrect timestep subscripts in the EKF prediction equations. This has now been fixed and results in $\mathbf{F}_k$ being the correct notation in the pseudocode section.

R2.8 -Section VIII-some explanations on the process model must be added. Figure 6 is too small; it is difficult to distinguish the different lines.

Process model information was indeed missing and the figure hard to read. The section has been modified to include details of the models used in the simulation and the figure modified to display comparisons between the privacy-preserving filter and the EIF separately for each considered sensor layout. We hope that the comparison and the drawn conclusions are now much easier to follow.

Response to the Comments of Reviewer 3 (229727)

R3.1 This paper presented a theoretical framework for privacy-preserving localisation combining the encryption scheme and filtering. In particular, the private linear-combination aggregation has been

adopted in the presented framework. Basically, the contribution of the paper is clearly indicated with an interesting and important topic. However, some technical problems need to be further clarified. Therefore, a major revision is necessary in my opinion.

We're glad to hear that the contribution was found interesting and important. We have made a very large revision of the work, including rewriting, reorganising and shortening the text to make the information easier to follow.

R3.2 1) Is any filtering method can be integrated into the presented framework? If so, can we replace the method via numerical approach such as particle filter.

The method proposed achieves the desired security properties by modifying the range-only measurement model and rearranging the terms in the Extended Information Filter (EIF) during the filter update step. With this method, using the EIF is crucial for reducing participant communication to a protocol that can use the introduced encryption scheme, and thus meet the security properties. It may be possible to rearrange a particle filter to suit some other type of encryption scheme, but to the best of our knowledge, this does not yet exist.

During only the prediction step of the filter (performed locally by the navigator), it is possible to use any filter, including a particle filter, but we have decided to use the prediction equations of the EKF for simplicity and consistency with the presented update step.

R3.3 2) How does the linear combination reflect the dynamics of the investigated system in Eq.(2)?

The linear combination aggregation scheme is only used to encrypt the required communication during the computation of the EIF update step. Ideally, the encryption does not affect the proposed filter in any way, but in practice, minor discrepancies are introduced with the quantisation of floating-point numbers. The proposed filter itself requires a modified measurement function to use linear combination aggregation, which is where differences to the standard EIF are introduced. The system model given in (2) is unaffected by both encryption and measurement model modification, in that both the proposed filter and the standard EIF assume the state follows these dynamics exactly.

R3.4 3) Why is the noise of the system Gaussian? In Eq.(2), function f() is known then what is the physical meaning of the Gaussian process noise?

Thank you for pointing this out. It is correct that the Gaussianity of additive system noise is not required by either the standard EIF or our approach and has now been removed from the manuscript.

R3.5 4) In the paper, the noise is depended on covariance matrix Q which is also particularly used in Algroithm 1, however, in practice, Q is unmeasurable and unknown. How to estimate the value of Q in terms of performance guarantee.

Estimating the second moment of the system noise, $\mathbf{Q}$, is the standard procedure when using linearising filters such as the EKF (see, for example, "Bayesian Estimation and Tracking: A Practical Guide" by Anton J. Huag), and is specific to the system being modelled. As it is possible to use a different, non-linearising, filter for the prediction step of the algorithm, it is possible to avoid having to compute $\mathbf{Q}$, but as we have stated above, we have presented the EKF equations for state prediction where computing it would be necassary.

R3.6 5) The experimental results are limited. The comparison is essential to validate the performance of the presented algorithm. What about using the existing filtering method to demonstrate the various encryption scheme?

We agree that the results section was lacking and have rewritten it to try and make the evaluation clearer. To validate the accuracy of the algorithm, it has been compared to the industry standard EKF (reformulated as the EIF) and the comparison figure changed to make it clearer that the proposed filter performs very similarly. The computational performance is more difficult to compare. Comparison with a different encryption scheme would require another scheme meeting LCAO (required to meet the security requirements), but no such scheme exists (we define the novel LCAO notion and present a scheme that meets it in the manuscript). Future work is being done on a similarly modified EIF

which can used a scheme meeting Aggregator Oblivousness (AO) instead, and that could be used for such a comparison, but is beyond the scope of this work.

R3.7 6) There are some typos in the manuscript please correct them, for example, page 1 Notation, '$\left\|\underline a\right\|$ the vector norm' should be '$\left\|\underline a\right\|$ is the vector norm' etc.

The sentence has now been corrected, along with others throughout the work.