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 14, 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 accomodate for 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, range-only sensor localisation with specific security requirements, and its benefits over existing and comparable approaches. We believe that the more clarified novelty and contribution also better justifies 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.

Our response.

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

Our response.

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

Our response.

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.

Our response.

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.

Our response.

R2.2 The reviewer encourages the authors to reorganize the article by greatly shortening it and to highlight the novelty.

Our response.

R2.3 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.

Our response.

R2.4 -Equation (3): i from 1 to n must be added.

Our response.

R2.5 -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.

Our response.

R2.6 -Page 10, Equation (36), Right part of Equation: d is from 0 to D

Our response.

R2.7 -Inequality (50) must be clarified,

Our response.

R2.8 -Algorithm 1, steps 2/3/4, it is F_{k-1},

Our response.

R2.9 -Section VIII-some explanations on the process model must be added. Figure 6 is too small; it is difficult to distinguish the different lines.

Our response.

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.

Our response.

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.

Our response.

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

Our response.

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?

Our response.

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.

Our response.

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?

Our response.

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.

Our response.