Distributed Range-Only Localisation that Preserves Sensor and Navigator Privacies

Response to Reviewers' Comments - Submission IEEE-TAC 21-1548

Marko Ristic Benjamin Noack Uwe D. Hanebeck

April 20, 2022

Dear Dr. Zhiwei Gao,
Dear Reviewers,

Thank you all for your detailed reviews and for finding the manuscript suitable for publication. In this letter, we will address the remaining editor and reviewer comments and describe any changes made to the manuscript. 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 I am pleased to inform you that the paper is acceptable for publication in the Transactions provided that you can make the modifications described below. The reviewers would like the authors to clarify some concerns such as the assumption of the EKF design, private sensor variance information, and research motivation and challenge, and so forth.

We are glad to hear the paper is acceptable for publication and have responded to each of the reviewer comments below, hoping to clarify all the remaining concerns.

Response to the Comments of Reviewer 1 (242571)

R1.1 Thank you for updating the manuscript and most of the concerns have been addressed well in the response letter.

We are happy to hear this is the case, thank you.

R1.2 However, there is one problem still confused me. The authors claimed that the Gaussian assumption has been removed in the revised version, however, the EKF (EIF) was still used for prediction (Eqs. 26-27). Basically, the EKF is based on the Gaussian assumption and the prediction is obtained in the sense of mean value. Then, the non-Gaussian dynamics would affect the prediction performance using EKF if the Gaussian assumption is removed. My point is 1) if the assumption is removed, please explain the non-Gaussian influence from the EKF or 2) if the Gaussian assumption remains in the manuscript, please explain from the noise comes from in physics sense.

We regret that there was some confusion about the prediction step of the presented localisation algorithm. Equations (26) – (27) are the EKF (EIF) update equations (rather than the prediction equations), resulting in updated terms $\underline{y}_{k|k}$ and $\mathbf{Y}_{k|k}$ from the predictions $\underline{y}_{k|k-1}$ and $\mathbf{Y}_{k|k-1}$. The Gaussian assumption has indeed been removed from the system model, and obtaining the predictions $\underline{y}_{k|k-1}$ and $\mathbf{Y}_{k|k-1}$ can be computed using any local filter (linearising or otherwise) as mentioned in Section V. The Gaussian assumption that remains is only present in the measurement model, as

is a commonly done to simplify the modelling of sensors, and the non-linear distance-measurement function h_i is linearlised by an appropriate EKF filter for the localisation update step only. We hope this clarifies equations (26) – (27) and the use of the EKF.

Response to the Comments of Reviewer 2 (242573)

R2.1 The authors have significantly improved the readability of the paper. The contribution is significant enough for privacy preserving state estimation.

We thank you for the comment and are glad that the contribution is found significant.

R2.2 However, this reviewer still have few comments:

1- It could be interesting to comment why sensor variance is a private information. Why is it crucial to preserve it if measurements are already protected?

This is a good question that had not been elaborated in the work. The key reason that any sensor-specific information (such as its measurement noise variance) is considered private is that it may hold identifying data if analysed by an adversary. For example, a particular sensor's model may be identified from its measurement noise variance, enabling a targeted attack (cyber or physical) against that sensor. We have made a change to the introduction section to clarify this reasoning.

R2.3 2- In the sentence 'homomorphic encryption is used to make time-independent model-free location estimates where an estimator does not learn sensor measurements or locations.; Shouldn't be 'cannot learn'?

Thank you for pointing this out, we have added the change to the manuscript.

R2.4 3- In problem statement 'we consider the context of privacy-preserving range sensor navigation, where we want no sensor to learn information about the navigator or other sensors beyond their local measurements, and the navigator to learn no information about individual sensors beyond its location estimate.', please specify type of information.

We regret that this was not clear to the reviewer. We refer to leakable content as arbitrary information to stress that *nothing* can be learnt. That is, neither the information we can predict the importance of (such as state estimates or sensor locations) nor that for which we cannot. This is common in cryptography, as no assumptions on the methods or intentions of adversaries can be made. We have updated the sentence to try and make this clearer and note that examples of information that should not be learnt (state estimates and sensor locations) have been given in the preceding section.

R2.5 4- Indistinguishable weights: what would happen if the sensor learns navigator weights?

This is a good question and relates to the abstraction from the previous response. Since a meaningful cryptographic definition cannot make assumptions about what leakable information might be useful, we cannot state what would happen. As the weights originate from the navigator and we do not want sensors to learn any information from the navigator, we can say that no new information should be learnt from the weights (and therefore require cryptographic indistinguishability of weights). In the concrete scheme presented later, it can be seen that the weights correspond to elements of the navigator's state estimate vector, which is stated as an example of information that must remain private to the navigator. We hope this makes the meaning and reasoning of indistinguishability clearer.

R2.6 5- Fix the following sentence: 'If an attacker compromises the navigator, they have control over the weights,'

Unfortunately, we are unable to find an issue with the stated sentence and have asked additional native English speakers that have also agreed that the sentence looks correct. In case the use of "they" (rather than "he" or "she") is being referred to, it is the formal grammatical pronoun for a person when gender is not specified.

R2.7 6- Define IND-CPA.

We apologise for the confusion, the first use of the term "Indistinguishability under the Chosen Plaintext Attack (IND-CPA)" is in section II.A and has been referenced (reference [21]). The full cryptographic game which defines it was originally present in the appendix of the initial submission, but removed after reviewers requested less cryptographic background. For this reason, we have left the definition only referenced and hope this is found satisfactory.

R2.8 7- Simulation: The authors have found that 1.7 s are needed for each computation step, is that compatible with real-time operation?

We agree that a further interpretation of execution times was lacking. It is hard to explicitly say whether a filter update of $1.7s$ is compatible with real-time computation as this is dependent on the use-case (for example, infrequent measurements may suffice for the localisation of a slow-moving object such as a hot air balloon but would be insufficient for a fast-moving object such as a jet). In terms of reducing this time, a smaller key size, optimised code or more powerful hardware could be used depending on the scenario. We have updated the discussion on execution time and choosing key sizes in section VI to elaborate on their relationship and how computation time could be reduced hoping that this makes our reasoning clearer.

R2.9 8- Can you comment why quantization noise, involved in the encryption-decryption schemes, isn't taken into account in the filter equations?

We regret that this was not clearer. The quantisation noise is captured by the precision parameter ϕ, which results in less noise when the parameter is large but is upper-bounded by (20). Here, it is noted that when $M = N$, the upper bound can be practically ignored since ϕ can be chosen to have a bit-length much larger than a floating-point number, making any introduced encoding noise negligible. When pseudocode is presented in subsection V.C, $M = N$ is chosen, and in the results section VI, $\phi = 2^{32}$ leads to a negligible difference in performance between an unencrypted (and non-quantised) EIF and the presented quantised and encrypted one. We have updated subsection V.C to make this clearer and hope that it now explains why there is no need for the quantisation noise to be considered in the filter.

Response to the Comments of Reviewer 3 (246951)

R3.1 Comments:

This paper proposes a novel distributed localisation method in the presence of range-only sensors, which preserves both navigator and sensor privacies. The major contribution of this paper is that a novel private linear combination aggregation scheme is proposed, and based on that, a modified extended Kalman filter is also derived. Some comments are given as follows:

1.In this paper, the full names of some abbreviations are not given. For example, in Section I, page 1, left column, "AES"and "RSA", and in Section I, page 1, right column, "pWSAc" and "pWSAh".

We apologise for having missed these, the full names have now been added.

R3.2 2.The authors should elaborate the advantages and disadvantages of the existing typical cryptographic secrecy scheme and the motivation for proposing private linear combination aggregation scheme in this paper.

This could indeed have been stated more explicitly in the text. Typical symmetric and public-key encryption schemes only support the encryption and decryption of data and therefore imply a trust between encryptor and decryptor (any information from the encryptor is learnt, in whole, by the decryptor). This assumption can be made in some scenarios, for example, when loading a secure webpage, the decryptor wishes to see the page in its entirety while the encryptor wishes to provide it. However, when this trust cannot be assumed, such as in our scenario of a navigator and sensors, we want specific control over what information can be learnt from encryptions, making the typical

schemes (as well as existing homomorphic schemes in our case) no longer applicable. The motivation for the notion of linear combination aggregator obliviousness is the potential for modifying the communications in distributed range-only navigation to a sum of locally weighted sums where the result contains only average sensor data. This notion is defined as part of the problem statement before a scheme that meets it and the appropriately modified navigation are presented as solutions. We have now updated the introduction section to better explain why the typical cryptographic schemes are not applicable to the problem we consider.

R3.3 3.Some symbols are reused. For example, In Section I, Notation, "timestep k" and "will denote encryption and decryption with key k".

Thank you for noticing this. We have updated the notation section and other places throughout the text to remove any found errors.

R3.4 4.The authors need to present theoretical computational complexity of the proposed method.

We thank you for the reasonable suggestion. As the proposed method presents a solution to a novel cryptographic problem, we believe that a lack of methods to which it can be compared reduces the benefits of a complexity analysis to readers. While also keeping the work shorter, the combination of complexities in terms of bit lengths (required for cryptographic components) and number sizes (required for state estimation components) would further complicate the interpretation of any presented analysis. We hope this rationale can be understood as the reason for excluding a theoretical complexity analysis from the work.

R3.5 5.The authors should state how to measure the performance of the private linear combination aggregation scheme proposed in this paper.

Thank you for the interesting suggestion. We found the topic relates to our reasoning in responses to your comments 2 and 4 above. The cryptographic notion of linear combination aggregator obliviousness is presented as a novel part of the problem to which the proposed scheme is a solution. Since the proposed scheme is proven correct (meets the novel notion), and no alternative that meets this notion is known to exist, it is difficult to measure its performance through a meaningful comparison. Instead, the presented use-case for the scheme, distributed range-only localisation, has its performance measured in terms of accuracy (comparison to an industry-standard algorithm without privacy guarantees) and execution time (from our local implementation, including the aggregation scheme). A possible measure of scheme performance would be the execution times of individual operations in the proposed scheme, but due to their implicit presence in figure 5 (predominant computation costs stem from cryptographic operations) and the desire to keep the paper short, we have decided to omit this. We hope this elaborates on our reasoning.

R3.6 6.In practical engineering application, how to balance the relationship between key sizes and computation.

In practice, choosing a cryptographic key size is dependent on the required duration of secrecy and the planned lifetimes of used secret keys. For example, if the location of an object needs only be private on the day of travel and new keys are generated each day, a shorter key can be used than for an object whose past location must remain private for the foreseeable future. Since secrecy is required, computation is not directly considered when choosing key sizes. However, in cases where computation makes the desired secrecy infeasible, shorter required secrecy and more frequent key exchanges can be considered to reduce key sizes and computation times. To elaborate on this requirement, we have added comments discussing the execution time and choosing key sizes in section VI.

Distributed Range-Only Localisation that Preserves Sensor and Navigator Privacies

Marko Ristic[1], Benjamin Noack[1], *Member, IEEE,* and Uwe D. Hanebeck[2], *Fellow, IEEE*

***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 typically involve the leakage of sensor or navigator information by communicating measurements or estimates and thus do not preserve participants' privacy. The existing approaches that do provide such guarantees ~~,~~ fail to address sensor and navigator privacy in the common application of model-based range-only ~~estimation~~localisation, consequently forfeiting broad applicability. In this work, we define a notion of privacy-preserving linear combination aggregation and use it to derive a modified Extended Kalman Filter using range measurements such that navigator location, sensors' locations, and sensors' measurements are kept private during navigation. Additionally, a formal cryptographic backing is presented to guarantee our method's privacy as well as an implementation to evaluate its performance. The novel, provably secure, range-based localisation method has applications in a variety of environments where sensors may not be trusted or estimates are considered sensitive, such as autonomous vehicle localisation or air traffic navigation.**

***Index Terms*—State Estimation, Data Privacy, Sensor Fusion, Extended Kalman Filter.**

I. Introduction

LOCALISATION methods in distributed sensor environments have long been an active topic of research [1], [2], [3] and have characterised many advancements of Kalman and Bayesian estimation theory [4]. In particular, range-based localisation methods, including signal strength measurements [5], [6], acoustic ranges [7] and ultra-wideband ranges [8], have found large application due to the prevalence of suitable sensors. In most cases, these localisation methods require the gathering of measurements centrally, where an estimate of location can be computed. With recent developments in distributed and cloud computing, uses of wireless and public communication channels for data transfer have become widespread, and the additional requirements of data privacy and state secrecy have become particularly relevant [9], [10].

Typical cryptographic secrecy involves hiding all transferred data such that external parties in the communication network learn no new information from acquired encryptions. This can be achieved with common symmetric and public-key encryption ~~scheme such as AES [11] and RSA~~ schemes such as the Advanced Encryption Standard (AES) [11] and the Rivest-Shamir-Adleman cryptosystem (RSA) [12], respectively. These scenarios, however, imply trust between the encrypting and decrypting parties in the network. In some cases~~however, partial data leakage or encrypted data processing is required for achieving a desiredgoal which~~ , this assumption cannot be made and control over what can be learnt or performed with encryptions is desired. This has led to several homomorphic and functional encryption schemes [13], [14], [15], [16] finding uses in ~~signal processing or~~ various signal processing and localisation tasks. In [17], homomorphic encryption is used to make time-independent model-free location estimates where an estimator ~~does not~~ cannot learn sensor measurements or locations. In [18], similar secrecy is achieved with a linear Kalman filter when a hierarchical sensor network is present. In [14], [15], privacy-preserving aggregation schemes are presented as a means to compute total ~~powergrid~~ power grid usage without disclosing individual contributions, while in [19], [20], ~~centralised and hidden weighted sum aggregations,~~ private Weighted Sum Aggregation with centralised or hidden weights (pWSAc and pWSAh, respectively) are introduced as a means for computing ~~local~~ control inputs in a distributed ~~environment~~ network without learning individual ~~inputs~~contributions.

Our contribution in this work presents a range-only localisation method meeting formal cryptographic requirements that ensure sensors keep their measurements, sensor variances and locations private while the navigator keeps its estimates private. We first define a novel ~~notion for private~~ cryptographic notion for linear combination aggregation and present an implementation ~~that satisfies these~~ satisfying the requirements, before using it to derive a filter based on the Extended Kalman Filter with no hierarchical sensor layout assumptions. The linear combination aggregation scheme ~~we put forward~~ is in principle similar to the pWSAh scheme in [20], however, a formal definition with different communication assumptions and leakages is given, crucial for its cryptographic security. To the best of the authors' knowledge, no existing method for Bayesian state estimation using range-only sensors and meeting the desired privacy requirements exists.

We motivate this scenario with ~~the~~ an example of vehicle localisation in the presence of privately owned measurement stations. While the intention of ~~measurement~~ stations is the accurate navigation of passing vehicles, it may be reasonable to desire identifying ~~location or hardware details~~details, such as hardware specifications or physical locations, to remain unknown to the other ~~present~~ stations and the navigator. Similarly, a navigator may not wish to disclose their ~~most~~

[1]Marko Ristic and Benjamin Noack are with the Autonomous Multisensor Systems Group (AMS), Institute for Intelligent Cooperating Systems (ICS), Otto von Guericke University Magdeburg (OVGU), Germany (e-mail: {marko.ristic, benjamin.noack}@ovgu.de).

[2]Uwe D. Hanebeck is with the Intelligent Sensor-Actuator-Systems Laboratory (ISAS), Institute for Anthropomatics, Karlsruhe Institute of Technology (KIT), Germany (e-mail: uwe.hanebeck@kit.edu).

accurate location estimates to untrusted third-party measurers.

In section II, we introduce both the cryptographic and estimation problems considered in this work, before giving some relevant preliminaries in section III. Section IV proposes a cryptographic scheme meeting our desired security properties, and section V gives a solution to the estimation problem making use of this scheme. Simulation results are discussed in section VI, and concluding remarks are made in section VII.

A. Notation

Throughout this work, we make use of the following notation. Underlined characters, $\underline{a}$, denote vectors, uppercase bold characters, $\mathbf{A}$, denote matrices. $\mathbf{A}^{-1}$ is the matrix inverse while $\mathbf{A}^\top$ is its transpose. The expected value of a random variable is denoted by $\mathsf{E}[\cdot]$, while the variance of a random scalar and covariance of a random vector by $\mathsf{Var}[\cdot]$ and $\mathsf{Cov}[\cdot]$, respectively. $|a|$ denotes absolute value, $\|\underline{a}\|$ the vector norm, $\{\dots\}$ is used for sets and $\langle\dots\rangle$ for ordered sequences. When estimating a state, notation ~~$\hat{x}_{k|l}$~~ $\hat{\underline{x}}_{k|e}$ will denote an estimate of $\underline{x}$ at timestep k given measurements from timesteps up to and including ~~l~~ timestep e. When discussing cryptography, ~~$\mathcal{E}_k(\cdot)$ and $\mathcal{D}_k(\cdot)$~~ $\mathcal{E}_{sk}(\cdot)$ and $\mathcal{D}_{sk}(\cdot)$ will denote encryption and decryption with key ~~k~~sk, respectively, with ~~k~~ sk ommited when inferrable from context. ~~$\mathbb{Z}_n$~~ $\mathbb{Z}_N$ is used for the set of integers modulo ~~n and $\mathbb{Z}_n^*$~~ N and $\mathbb{Z}_N^*$ for its multiplicative group. $\mathsf{lcm}(\cdot,\cdot)$ is the lowest common denominator, $\|$ the binary concatination operator, and the term *negligible function* refers to its cryptographic definition in [21].

II. Problem Statement

In this work, we consider the context of privacy-preserving range sensor navigation, where we want no sensor to learn any information about the navigator or other sensors beyond their local measurements, and the navigator ~~to learn no~~ not to learn any information about individual sensors beyond its location estimate. The problem is two-fold, in that we require explicit cryptographic requirements with a suitable encryption scheme meeting them ~~,~~ as well as an estimation scheme that can use the ~~scheme~~ encryption in the context of range-only navigation.

To give a formal cryptographic requirement in a distributed setting, we must first consider the communication requirements of our context ~~,~~ and define the attacker capabilities and the desired security of a suitable encryption scheme. In this section, we will define a communication protocol and the relevant formal definition of security we aim to achieve, followed by the estimation problem to which we will apply it.

A. Formal Cryptographic Problem

The communication between the navigator and sensors in our estimation problem will be decomposed into a simple two-step bi-directional protocol that will simplify defining formal security. In section V, we will show how this protocol is sufficient to compute the location estimate at a navigator while meeting our desired privacy goals. The communication protocol is as follows.

At every *instance* t (used to distinguish from an estimation *timestep*), the navigator first broadcasts m weights $\omega_j^{(t)}, j \in \{1,\dots,m\}$ to all sensors $i \in \{1,\dots,n\}$, who individually compute linear combinations $l_i^{(t)} = \sum_{j=1}^m a_{j,i}^{(t)} \omega_i^{(t)}$ based on their measurement data $a_{j,i}$. Linear combinations are then sent back to the navigator, who computes their sum $\sum_{i=1}^n l_i^{(t)}$. This two-step linear combination aggregation protocol has been visually displayed in figure 1. In addition, we note that an

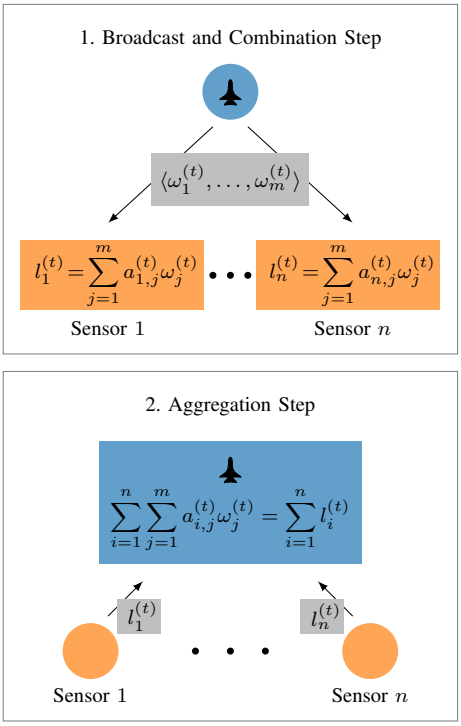

Fig. 1. Required linear combination aggregation steps at instance t.

alternative approach to the two-step protocol is computing $\sum_{j=1}^m (\omega_j^{(t)} \sum_{i=1}^n a_{i,j}^{(t)})$ at the navigator, requiring only values $a_{i,j}^{(t)}, j \in \{1,\dots,m\}$ to be sent from each sensor i. We justify the use of bi-directional communication by reducing communication costs when the number of weights is larger than the number of sensors, $m > n$, and by sending fewer weights in the presence of repeats, as will be shown to be the case in section V.

Before giving a formal definition for the construction and security of our desired encryption scheme, we make the following assumptions on the capabilities of the participants.

Global Navigator Broadcast We assume that broadcast information from the navigator is received by *all* sensors involved in the protocol.

Consistent Navigator Broadcast We assume that broadcast information from the navigator is received equally by all sensors. This means the navigator may not send different weights to individual sensors during a single instance t.

Honest-but-Curious Sensors We adopt the honest-but-curious attacker model for all involved sensors, meaning that they follow the localisation procedure correctly but may store or use any gained sensitive information.

We justify the global broadcast assumption by noting that any subset of sensors within the range of the navigator can be

considered a ~~complete~~ group and treated as the global set ~~for estimationpurposes~~during estimation, generalising the method, while the wide-spread use of cheap non-directional antennas supports the assumption of consistent broadcasts. The final assumption refers to the known problem of misbehaving sensors [22], [23], often requiring additional complicated detection mechanisms, and will not be considered in this work.

We are now ready to define the type of encryption scheme we want for the specified communication protocol and the security guarantees it should provide. We let a linear combination aggregation scheme be defined as a tuple of the four algorithms $(\mathsf{Setup}, \mathsf{Enc}, \mathsf{CombEnc}, \mathsf{AggDec})$. These will be used by a trusted setup party, the navigator, and sensors $i \in \{1, \dots, n\}$. They are defined as follows.

$\mathsf{Setup}(\kappa)$ On input of security parameter κ, generate public parameters pub, the number of weights m, the navigator's public and private keys pk_0 and sk_0 and the sensor private keys sk_i, $i \in \{1, \dots, n\}$.

$\mathsf{Enc}(pk_0, x)$ The navigator and sensors can encrypt any value x with the navigator's public key pk_0 and obtain the encryption $\mathcal{E}_{pk_0}(x)$.

$\mathsf{CombEnc}(t, pk_0, sk_i, \mathcal{E}(\omega_1^{(t)}), \dots, \mathcal{E}(\omega_m^{(t)}), a_{i,1}^{(t)}, \dots, a_{i,m}^{(t)})$ At instance t, sensor i computes and obtains the encrypted linear combination denoted $l_i^{(t)} = \mathcal{E}_{pk_0, sk_i}(\sum_{j=1}^{m} a_{i,j}^{(t)} \omega_j^{(t)})$ using its secret key sk_i.

$\mathsf{AggDec}(t, pk_0, sk_0, l_1^{(t)}, \dots, l_n^{(t)})$ At instance t, the navigator computes the aggregation of linear combinations $\sum_{i=1}^{n} l_i^{(t)} = \sum_{i=1}^{n} \sum_{j=1}^{m} a_{i,j}^{(t)} \omega_j^{(t)}$ using its public and private keys pk_0, sk_0.

The security notions we want these algorithms to meet reflect the previously stated estimation privacy goals. The navigator should learn no information from individual sensors while sensors should learn no information from the navigator or any other sensors. In the context of the introduced communication protocol, this can be summarised as the following notions.

Indistinguishable Weights No colluding subset of sensors gains any new knowledge about the navigator weights $\omega_j^{(t)}$, $j \in \{1, \dots, m\}$ when receiving only their encryptions from the current and previous instances and having the ability to encrypt plaintexts of their choice.

Linear Combination Aggregator Obliviousness No colluding subset *excluding* the navigator gains additional information about the remaining sensor values to be weighted, $a_{i,j}^{(t)}$, $j \in \{1, \dots, m\}$, where sensor i is not colluding, given only encryptions of their linear combinations l_i from the current and previous instances. Any colluding subset *including* the navigator learns only the sum of all linear combinations weighted by weights of their choice, $\sum_{i=1}^{n} l_i^{(t)} = \sum_{i=1}^{n} \sum_{j=1}^{m} a_{i,j}^{(t)} \omega_j^{(t)}$.

While indistinguishable weights can be achieved by encrypting weights with an encryption scheme meeting the notion of Indistinguishability under the Chosen Plaintext Attack (IND-CPA) [21], the novel notion of Linear Combination Aggregator Obliviousness (LCAO) has been formalised as a typical cryptographic game between attacker and challenger in appendix A.

Lastly, we conclude the cryptographic problem definition with the following important remark.

Remark. A leakage function including weights from the navigator requires extra care to be taken when giving its definition. If an attacker compromises the navigator, they have control over the weights, and therefore the leakage function. We note that in the leakage function above, $\sum_{i=1}^{n} \sum_{j=1}^{m} a_{i,j}^{(t)} \omega_j^{(t)}$, an individual sum weighted by the same weight may be ~~learned~~ learnt by an attacker, *e.g.*, $\sum_{i=1}^{n} a_{i,1}^{(t)}$ given weights $(1, 0, \dots, 0)$, but that individual sensor values $a_{i,j}^{(t)}$ remain private due to the assumption of a consistent broadcast.

B. Estimation problem

The estimation problem we consider, for which we will reformulate communication to the protocol above, is localisation with range-only sensors. In this work, we will focus on the two-dimensional case for simplicity but will derive methods suitable for extension to a three-dimensional equivalent. The state that we wish to estimate must capture the navigator position, x and y, and may contain any other components relevant to the system. It is of the form

$$\underline{x} = \begin{bmatrix} x & y & \cdots \end{bmatrix}^\top . \tag{1}$$

This state evolves following some known system model, which at timestep k can be written as

$$\underline{x}_k = \underline{f}_k(\underline{x}_{k-1}, \underline{w}_k) , \tag{2}$$

with noise term $\underline{w}_k$. Measurements of $\underline{x}_k$ follow a measurement model dependent on sensor $i \in \{1, \dots, n\}$, given by

$$z_{k,i} = h_i(\underline{x}_k) + v_{k,i} , \tag{3}$$

with Gaussian measurement noises $v_{k,i} \sim \mathcal{N}(0, r_{k,i})$ and measurement function

$$\begin{aligned} h_i(\underline{x}) &= \left\| \begin{bmatrix} x & y \end{bmatrix}^\top - \underline{s}_i \right\| \\ &= \sqrt{(x - s_{x,i})^2 + (y - s_{y,i})^2} , \end{aligned} \tag{4}$$

where

$$\underline{s}_i = \begin{bmatrix} s_{x,i} & s_{y,i} \end{bmatrix}^\top \tag{5}$$

is the location of sensor i.

We aim to provide a filter that estimates the navigator's state $\underline{x}_k$, at every timestep k, without learning sensor positions $\underline{s}_i$, measurements $z_{k,i}$ and measurement variances $r_{k,i}$ beyond the information in the corresponding aggregation leakage function. Similarly, sensors should not learn any information about current state estimates or any other sensor information. Leakage will be further discussed in section V-D, but we note that from any sequential state estimates, following known models, some sensor information leakage can be computed by the navigator. In the context of our leakage function, we will show that this corresponds to the global sums of private sensor information, while individual, or subsets of sensors', information remain private. Similarly, corrupted sensors with access to one or more measurements can produce state estimates of their own, leaking information about navigator state estimates, however, the most accurate estimates, requiring all measurements, will always remain private to the navigator.

III. Preliminaries

When proposing an encryption scheme meeting the LCAO notion, we will base our method on the additively homomorphic Paillier encryption scheme [13] and the Joye-Libert privacy-preserving aggregation scheme [15]. These schemes have been summarised below. Additionally, the estimation problem we consider uses real-valued inputs and functions and will require encoding real numbers for use with the aforementioned encryption schemes. The method used for encoding has been summarised afterwards.

A. Paillier Encryption Scheme

The Paillier encryption scheme [13] is an additively homomorphic encryption scheme that bases its security on the decisional composite residuosity assumption (DCRA) and meets the security notion of IND-CPA. Key generation of the Paillier scheme is performed by choosing two sufficiently large primes p and q, and computing $N = pq$. A generator g is also required for encryption, which is often set to $g = N+1$ when p and q are of equal bit length [21]. The public key is defined by (N, g) and the secret key by (p, q).

Encryption of a plaintext message $a \in \mathbb{Z}_N$, producing ciphertext $c \in \mathbb{Z}^*_{N^2}$, is computed by

$$c = g^a \rho^N \pmod{N^2} \tag{6}$$

for a randomly chosen $\rho \in \mathbb{Z}_N$. Here, ρ^N can be considered the noise term which hides the value $g^a \pmod{N^2}$, which due to the scheme construction, is an easily computable discrete logarithm. The decryption of a ciphertext is computed by

$$a = \frac{L(c^\lambda \pmod{N^2})}{L(g^\lambda \pmod{N^2})} \pmod{N} \tag{7}$$

where $\lambda = \mathsf{lcm}(p-1, q-1)$ and ~~$L(u) = \frac{u-1}{N}$~~ $L(\psi) = \frac{\psi-1}{N}$.

In addition to encryption and decryption, the following homomorphic functions are provided by the Paillier scheme. $\forall a_1, a_2 \in \mathbb{Z}_N$,

$$\mathcal{D}(\mathcal{E}(a_1)\mathcal{E}(a_2) \pmod{N^2}) = a_1 + a_2 \pmod{N}, \tag{8}$$
$$\mathcal{D}(\mathcal{E}(a_1) g^{a_2} \pmod{N^2}) = a_1 + a_2 \pmod{N}, \tag{9}$$
$$\mathcal{D}(\mathcal{E}(a_1)^{a_2} \pmod{N^2}) = a_1 a_2 \pmod{N}. \tag{10}$$

B. Joye-Libert Privacy-Preserving Aggregation Scheme

The Joye-Libert privacy-preserving aggregation scheme [15] is a scheme defined on time-series data and meets the security notion of Aggregator Obliviousness (AO) [14]. Similarly to the Paillier scheme, it bases its security on the DCRA. A notable difference to a public-key encryption scheme is its need for a trusted party to perform the initial key generation and distribution.

Key generation is computed by first choosing two equal-length and sufficiently large primes p and q, and computing $N = pq$. A hash function $H : \mathbb{Z} \to \mathbb{Z}^*_{N^2}$ is defined and the public key is set to (N, H). n private keys are generated by choosing sk_i, $i \in \{1, \ldots, n\}$, uniformly from $\mathbb{Z}_{N^2}$ and distributing them to n participants (whose values are to be aggregated), while the last key is set as

$$sk_0 = -\sum_{i=1}^{n} sk_i, \tag{11}$$

and sent to the aggregator.

Encryption of plaintext $a_i^{(t)} \in \mathbb{Z}_N$ to ciphertext $c_i^{(t)} \in \mathbb{Z}_{N^2}$ at instance t is computed by user i as

$$c_i^{(t)} = (N+1)^{a_i^{(t)}} H(t)^{sk_i} \pmod{N^2}. \tag{12}$$

Here, we can consider $H(t)^{sk_i}$ the noise term which hides the easily computable discrete logarithm $g^{a_i^{(t)}} \pmod{N^2}$, where $g = N + 1$ (as with the Paillier scheme above).

When all encryptions $c_i^{(t)}$, $i \in \{1, \ldots, n\}$ are sent to the aggregator, summation and decryption of the aggregated sum are computed by the functions

$$c^{(t)} = H(t)^{sk_0} \prod_{i=1}^{n} c_i^{(t)} \pmod{N^2} \tag{13}$$

and

$$\sum_{i=1}^{n} a_i^{(t)} = \frac{c^{(t)} - 1}{N} \pmod{N}. \tag{14}$$

Correctness follows from $\sum_{i=0}^{n} sk_i = 0$, and thus

$$\begin{aligned}
&H(t)^{sk_0} \prod_{i=1}^{n} c_i^{(t)} \pmod{N^2} \\
\equiv &H(t)^{sk_0} \prod_{i=1}^{n} (N+1)^{a_i^{(t)}} H(t)^{sk_i} \pmod{N^2} \\
\equiv &H(t)^{\sum_{j=0}^{n} sk_j} \prod_{i=1}^{n} (N+1)^{a_i^{(t)}} \pmod{N^2} \\
\equiv &(N+1)^{\sum_{i=1}^{n} a_i^{(t)}} \pmod{N^2},
\end{aligned}$$

removing all noise terms.

C. Integer Encoding for Real Numbers

In both the Paillier and Joye-Libert schemes, as well as the one we introduce, meaningful inputs a are bounded to $a \in \mathbb{Z}_N$. For this reason, real-valued estimation variables require quantisation and integer mapping for encryption and aggregation. We will rely on a generalised Q number encoding [24] due to implementation simplicity and applicability.

We will consider a subset of rational numbers in terms of a range $M \in \mathbb{N}$ and fractional precision $\phi \in \mathbb{N}$. This contrasts with the common definition in terms of total and fractional bits [24], [25], [26], but allows for a direct mapping to integer ranges which are not a power of two. A rational subset $\mathbb{Q}_{M,\phi}$ is then given by

$$\mathbb{Q}_{M,\phi} = \left\{ \underline{q}o \;\middle|\; \phi \underline{q}o \in \mathbb{N} \wedge -\left\lfloor \frac{M}{2} \right\rfloor \leq \phi \underline{q}o < \left\lfloor \frac{M}{2} \right\rfloor \right\}, \tag{15}$$

and we can quantize any real number a by taking the nearest rational ~~$q \in \mathbb{Q}_{M,\phi}$~~ $o \in \mathbb{Q}_{M,\phi}$, that is, ~~$\arg\min_{q \in \mathbb{Q}_{M,\phi}} |a - q|$~~ $\arg\min_{o \in \mathbb{Q}_{M,\phi}} |a - o|$. In this form, mapping rationals $\mathbb{Q}_{M,\phi}$ to an encryption range $\mathbb{Z}_N$ is

achieved by choosing $M = N$ and handling negatives by modulo arithmetic. Additionally, we note that the Q number format requires a precision factor ϕ to be removed after each encoded multiplication. This is captured by a third parameter d; the number of additional precision factors present in encodings.

The function for *combined* quantisation and encoding, $\mathsf{E}_{M,\phi,d}(a)$, of a given number $a \in \mathbb{R}$ and with an integer range $\mathbb{Z}_M$, precision ϕ and scaling for d prior encoded multiplications is given by

$$\mathsf{E}_{M,\phi,d}(a) = \left\lfloor \phi^{d+1} a \right\rceil \pmod{M}. \tag{16}$$

Decoding of an integer $u \in \mathbb{Z}_M$, is given by

$$\mathsf{E}^{-1}_{M,\phi,d}(u) = \begin{cases} \dfrac{u \pmod{M}}{\phi^{d+1}}, & u \pmod{M} \leq \left\lfloor \dfrac{M}{2} \right\rfloor \\ -\dfrac{M - u \pmod{M}}{\phi^{d+1}}, & \text{otherwise} \end{cases}. \tag{17}$$

This encoding scheme provides the following homomorphic operations,

$$\mathsf{E}_{M,\phi,d}(a_1) + \mathsf{E}_{M,\phi,d}(a_2) \pmod{M} = \mathsf{E}_{M,\phi,d}(a_1 + a_2) \tag{18}$$

and

$$\mathsf{E}_{M,\phi,d}(a_1)\mathsf{E}_{M,\phi,d}(a_2) \pmod{M} = \mathsf{E}_{M,\phi,d+1}(a_1 a_2), \tag{19}$$

noting that when $M = N$, the operations and modulus correspond with those in the Paillier homomorphic operations (8), (9) and (10), and the Joye-Libert sum (14).

In general, the choice of a large precision parameter ϕ may reduce quantisation errors introduced in (16), but risks overflow after too many multiplications. Given the largest number of encoded multiplications, d_{max}, and the largest value to be encoded a_{max}, the parameter should be chosen such that

$$\left| \phi^{d_{max}+1} a_{max} \right| < \left\lfloor \frac{M}{2} \right\rfloor. \tag{20}$$

In practice, N is typically very large ($N > 2^{1024}$) and this condition can be ignored when $M = N$, as ϕ can be made sufficiently large to make quantisation errors negligible.

IV. Private Linear Combination Aggregation Scheme

In this section, we introduce an encryption scheme meeting the desired security properties in section II-A. The scheme is a combination of the Paillier and Joye-Libert schemes and provides encrypted weights meeting IND-CPA and encrypted aggregation meeting the notion of LCAO defined in section II-A. Similarly to its constituents, the scheme bases its security on the DCRA and, as with the Joye-Libert scheme, requires a trusted party for initial key generation and distribution.

As aggregation is typically performed on scalar inputs, we extend our notation to the context of multidimensional estimation data by letting an instance $t_{k,\tau}$ uniquely capture the scalar aggregation during an estimation timestep k for a single element with position index τ. To achieve this in practice, any injective function can be used, such as the concatenation $t_{k,\tau} = k \parallel \tau$. The four algorithms defining our scheme are given as follows.

$\mathsf{Setup}(\kappa)$ On input parameter κ, generate two equal-length, sufficiently large, primes p and q, and compute $N = pq$. Define a hash function $H : \mathbb{Z} \to \mathbb{Z}^*_{N^2}$, choose the number of weights to combine, $m > 1$, and set public parameter $\mathsf{pub} = H$, navigator public key $pk_0 = N$ and navigator private key $sk_0 = (p, q)$. Sensor secret keys are generated by choosing sk_i, $i \in \{1, \ldots, n-1\}$ uniformly from $\mathbb{Z}_{N^2}$ and setting the last key ~~as $sk_n = -\sum_{i=1}^{n-1} sk_i \pmod{N^2}$~~ to $sk_n = -\sum_{i=1}^{n-1} sk_i$.

$\mathsf{Enc}(pk_0, x)$ Public-key encryption is computed by the Paillier encryption scheme with implicit generator $g = N + 1$. This is given by

$$\mathcal{E}_{pk_0}(x) = (N+1)^x \rho^N \pmod{N^2}, \tag{21}$$

for a randomly chosen $\rho \in \mathbb{Z}_N$.

~~At~~ $\mathsf{CombEnc}(t_{k,\tau}, pk_0, sk_i, \mathcal{E}_{pk_0}(\omega_1^{(k,\tau)}), \ldots, a_{i,1}^{(k,\tau)}, \ldots)$ At the instance $t_{k,\tau}$, encrypted linear combination is ~~computed as~~ given by

$$l_i^{(k,\tau)} = H(t_{k,\tau})^{sk_i} \prod_{j=1}^{m} \mathcal{E}_{pk_0}(\omega_j^{(k,\tau)})^{a_{i,j}^{(k,\tau)}} \pmod{N^2}, \tag{22}$$

and makes use of the homomorphic property (10). Correctness follows from

$$\begin{aligned} l_i^{(k,\tau)} &= H(t_{k,\tau})^{sk_i} \prod_{j=1}^{m} \mathcal{E}_{pk_0}(\omega_j^{(k,\tau)})^{a_{i,j}^{(k,\tau)}} \pmod{N^2} \\ &= H(t_{k,\tau})^{sk_i} \prod_{j=1}^{m} \mathcal{E}_{pk_0}(a_{i,j}^{(k,\tau)} \omega_j^{(k,\tau)}) \pmod{N^2} \\ &= H(t_{k,\tau})^{sk_i} \cdot \prod_{j=1}^{m} (N+1)^{a_{i,j}^{(k,\tau)} \omega_j^{(k,\tau)}} \rho_j^N \pmod{N^2} \\ &= H(t_{k,\tau})^{sk_i} \cdot (N+1)^{\sum_{j=1}^{m} a_{i,j}^{(k,\tau)} \omega_j^{(k,\tau)}} \tilde{\rho}_i^N \pmod{N^2}, \end{aligned}$$

for some values ~~$\rho_i, \rho_j \in \mathbb{Z}_N, j \in \{1, \ldots, m\}$~~ $\rho_j \in \mathbb{Z}_N, j \in \{1, \ldots, m\}$ and $\tilde{\rho}_i = \prod_{j=1}^{m} \rho_j$. Here, ~~$\rho_i^N$~~ $\tilde{\rho}_i^N$ and $H(t_{k,\tau})^{sk_i}$ can be considered the noise terms corresponding to the two levels of encryption from pk_0 and sk_i, respectively.

$\mathsf{AggDec}(t_{k,\tau}, pk_0, sk_0, l_1^{(k,\tau)}, \ldots, l_n^{(k,\tau)})$ Aggregation is computed as $l^{(k,\tau)} = \prod_{i=1}^{n} l_i^{(k,\tau)} \pmod{N^2}$, removing the aggregation noise terms, and is followed by Paillier scheme decryption

$$\sum_{i=1}^{n} \sum_{j=1}^{m} a_{i,j}^{(k,\tau)} \omega_j^{(k,\tau)} = \frac{L((l^{(k,\tau)})^\lambda \pmod{N^2})}{L((N+1)^\lambda \pmod{N^2})} \pmod{N}, \tag{23}$$

with $\lambda = \mathsf{lcm}(p-1, q-1)$ and ~~$L(u) = \frac{u-1}{N}$~~ $L(\psi) = \frac{\psi-1}{N}$. The correctness of the aggregation can be seen from

$$\begin{aligned} l^{(k,\tau)} &= \prod_{i=1}^{n} H(t_{k,\tau})^{sk_i} \cdot \\ &\quad (N+1)^{\sum_{j=1}^{m} a_{i,j}^{(k,\tau)} \omega_j^{(k,\tau)}} \tilde{\rho}_i^N \pmod{N^2} \\ &= H(t_{k,\tau})^{\sum_{i=1}^{n} sk_i} \cdot \\ &\quad \prod_{i=1}^{n} (N+1)^{\sum_{j=1}^{m} a_{i,j}^{(k,\tau)} \omega_j^{(k,\tau)}} \tilde{\rho}_i^N \pmod{N^2} \\ &= (N+1)^{\sum_{i=1}^{n} \sum_{j=1}^{m} a_{i,j}^{(k,\tau)} \omega_j^{(k,\tau)}} \rho' \tilde{\rho}^N \pmod{N^2}, \end{aligned}$$

for some values ~~$\rho_i, \rho' \in \mathbb{Z}_N, i \in \{1, \ldots, n\}$~~ $\tilde{\rho}_i \in \mathbb{Z}_N, i \in \{1, \ldots, n\}$ and $\tilde{\rho} = \prod_{i=1}^{n} \tilde{\rho}_i$.

Additionally, we note that in the above construction, all weights $\omega_j^{(k,\tau)}$ and values $a_{i,j}^{(k,\tau)}$ are integers and the resulting linear combinations and aggregation are computed modulo N.

The security proof of this scheme must both show that encrypted weights meet IND-CPA and that encrypted aggregation meets LCAO. As weights are encrypted with the Paillier encryption scheme, the first requirement is already met. To show that aggregation meets LCAO, a reduction proof is given in appendix B.

Remark. Given the construction of the scheme above, it can be seen that any weights $\omega_j^{(k,\tau)}$, whose values are known at each sensor, do not need to be broadcast by the navigator. In this case, sensors can replace

$$\mathcal{E}_{pk_0}(\omega_j^{(k,\tau)})^{a_{i,j}^{(k,\tau)}} = (N+1)^{\omega_j^{(k,\tau)} a_{i,j}^{(k,\tau)}} \rho_j^N \pmod{N^2} \quad (24)$$

in (22), by

$$(N+1)^{\omega_j^{(k,\tau)} a_{i,j}^{(k,\tau)}} \pmod{N^2}. \quad (25)$$

This is due to the removal of ρ_j^N terms during decryption and can be used to reduce the navigator's broadcast communication cost by the number of weights $\omega_j^{(k,\tau)}$ that do not hold any information private to the navigator and are known by the sensors in advance.

V. Privacy-Preserving Localisation

With a concrete scheme meeting the LCAO notion, we can now put forward a localisation filter with communication that can be reformulated to the required protocol. To produce an estimate of the state $\underline{x}_k$, we make use of an algebraic reformulation of the Extended Kalman Filter (EKF), the Extended Information Filter (EIF) [27], which reduces the filter update step to a single summation. The EIF update step requires the predicted state estimate $\hat{\underline{x}}_{k|k-1}$ and estimate covariance $\mathbf{P}_{k|k-1}$ in the information vector and matrix forms

$$\hat{\underline{y}}_{k|k-1} = \mathbf{P}_{k|k-1}^{-1} \hat{\underline{x}}_{k|k-1} \quad \text{and} \quad \mathbf{Y}_{k|k-1} = \mathbf{P}_{k|k-1}^{-1}, \quad (26)$$

respectively. In this form, the update equations for n sensor measurements at time k, with measurement models (3), are given by

$$\begin{aligned} \hat{\underline{y}}_{k|k} &= \hat{\underline{y}}_{k|k-1} + \\ &\sum_{i=1}^{n} \mathbf{H}_{k,i}^{\top} r_i^{-1} \left(z_{k,i} - h_i(\hat{\underline{x}}_{k|k-1}) + \mathbf{H}_{k,i} \hat{\underline{x}}_{k|k-1} \right) \end{aligned} \quad (27)$$

and

$$\mathbf{Y}_{k|k} = \mathbf{Y}_{k|k-1} + \sum_{i=1}^{n} \mathbf{H}_{k,i}^{\top} r_i^{-1} \mathbf{H}_{k,i}, \quad (28)$$

with Jacobians

$$\mathbf{H}_{k,i} = \left. \frac{\partial h_i}{\partial \underline{x}} \right|_{\hat{\underline{x}}_{k|k-1}} \quad (29)$$

for sensors $i \in \{1, \ldots, n\}$. After converting the updated information vector and matrix back to state estimate $\hat{\underline{x}}_{k|k}$ and estimate covariance $\mathbf{P}_{k|k}$, the filter's prediction step can be computed by the navigator locally using any suitable filter for the known system model (2).

In the form above, at every timestep k, all sensitive sensor information required for state estimation is captured in the measurement vector

$$\underline{i}_{k,i} = \mathbf{H}_{k,i}^{\top} r_i^{-1} \left(z_{k,i} - h_i(\hat{\underline{x}}_{k|k-1}) + \mathbf{H}_{k,i} \hat{\underline{x}}_{k|k-1} \right) \quad (30)$$

and the measurement matrix

$$\mathbf{I}_{k,i} = \mathbf{H}_{k,i}^{\top} r_i^{-1} \mathbf{H}_{k,i}, \quad (31)$$

namely, their measurements $z_{k,i}$, measurement variances $r_{k,i}$ and locations $\underline{s}_i$; captured in measurement functions h_i and Jacobians $\mathbf{H}_{k,i}$. ~~However,~~ To compute $\underline{i}_{k,i}$ and $\mathbf{I}_{k,i}$ ~~also require~~, however, the current predicted state estimate $\hat{\underline{x}}_{k|k-1}$ ~~to be computed~~ is also required (in h_i and $\mathbf{H}_{k,i}$). ~~For this reason~~ Therefore, our goal is to ~~reformulate~~ rearrange (30) and (31) ~~to be computable at each sensor i~~ as a linear combination of functions of ~~the navigator state estimate~~ $\hat{\underline{x}}_{k|k-1}$ (the navigator weights) computable at each sensor i, to be subsequently aggregated at the navigator. Application of the linear combination aggregation scheme proposed ~~would in turn guarantee~~ in turn guarantees that sensors do not learn the navigator state, and the navigator learns only the aggregation required for updating its state estimate in (27) and (28).

A. Range Measurement Modification

The first thing we notice when wanting to ~~decompose~~ rearrange $\underline{i}_{k,i}$ and $\mathbf{I}_{k,i}$ to a linear combination of functions of $\hat{\underline{x}}_{k|k-1}$, is that h_i cannot be rearranged in this way due to the present square-root. Similarly, the Jacobian of h_i at $\hat{\underline{x}}_{k|k-1}$,

$$\mathbf{H}_{k,i} = \begin{bmatrix} \frac{\hat{x}_{k|k-1} - s_{x,i}}{\sqrt{(\hat{x}_{k|k-1} - s_{x,i})^2 + (\hat{y}_{k|k-1} - s_{y,i})^2}} \\ \frac{\hat{y}_{k|k-1} - s_{y,i}}{\sqrt{(\hat{x}_{k|k-1} - s_{x,i})^2 + (\hat{y}_{k|k-1} - s_{y,i})^2}} \\ 0 \\ \vdots \end{bmatrix}^{\top}, \quad (32)$$

cannot be either. We, therefore, consider the modified measurement functions

$$h_i'(\underline{x}) = h_i(\underline{x})^2. \quad (33)$$

A measurement function in this form allows rearrangement of h_i' and the corresponding Jacobian $\mathbf{H}_{k,i}'$ to a linear combination of powers of location elements in $\hat{\underline{x}}_{k|k-1}$, as

$$\begin{aligned} h_i'(\underline{x}) &= \left\| \begin{bmatrix} x & y \end{bmatrix}^{\top} - \underline{s}_i \right\|^2 \\ &= (x - s_{x,i})^2 + (y - s_{y,i})^2 \\ &= x^2 + y^2 - 2s_{x,i}x - 2s_{y,i}y + s_{x,i}^2 + s_{y,i}^2 \end{aligned}, \quad (34)$$

and

$$\mathbf{H}'_{k,i} = \begin{bmatrix} 2\hat{x}_{k|k-1} - 2s_{x,i} \\ 2\hat{y}_{k|k-1} - 2s_{y,i} \\ 0 \\ \vdots \end{bmatrix}^{\top}_{\sim}. \tag{35}$$

Here, h'_i and $\mathbf{H}'_{k,i}$ are linear combinations of $\hat{x}^2_{k|k-1}$, $\hat{y}^2_{k|k-1}$, $\hat{x}_{k|k-1}$ and $\hat{y}_{k|k-1}$. To show how the corresponding modified measurement vectors $\underline{i}'_{k,i}$ and matrices $\mathbf{I}'_{k,i}$ can be similarly rearranged and used for localisation, we also require the existence of measurements following a modified measurement model of the form

$$z'_{k,i} = h'_i(\underline{x}_k) + v'_{k,i}\,, \tag{36}$$

where $z'_{k,i}$ is the modified measurement, and noise term $v'_{k,i}$ is zero-mean and has a known variance $r'_{k,i}$.

Computing $z'_{k,i}$ and its variance $r'_{k,i}$ from the original measurements $z_{k,i}$ are complicated by the noise term $v_{k,i} \sim \mathcal{N}(0, r_{k,i})$, and simply squaring the original range measurements produces

$$\begin{aligned} z^2_{k,i} &= (h_i(\underline{x}_k) + v_{k,i})^2 \\ &= h'_i(\underline{x}_k) + 2h_i(\underline{x}_k)v_{k,i} + v^2_{k,i}\,, \end{aligned} \tag{37}$$

with a new noise term $2h_i(\underline{x}_k)v_{k,i} + v^2_{k,i}$, now dependent on the measurement function h_i, and no longer zero-mean. We can compute the mean of this new noise term (a function of the Gaussian term $v_{k,i}$) as $\mathsf{E}[2h_i(\underline{x}_k)v_{k,i} + v^2_{k,i}] = r_{k,i}$ and mean-adjust modified measurements as

$$\begin{aligned} z'_{k,i} &= z^2_{k,i} - r_{k,i} \\ &= h_i(\underline{x}_k)^2 + 2h_i(\underline{x}_k)v_{k,i} + v^2_{k,i} - r_{k,i} \\ &= h'_i(\underline{x}_k) + v'_{k,i}\,, \end{aligned} \tag{38}$$

with now zero-mean noise $v'_{k,i} = 2h_i(\underline{x}_k)v_{k,i} + v^2_{k,i} - r_{k,i}$. The noise in this case (again a function of $v_{k,i}$) has variance

$$\mathsf{Var}[v'_{k,i}] = 4h_i(\underline{x}_k)^2 r_{k,i} + 2r^2_{k,i} \tag{39}$$

and is also dependent on h_i. To use the modified measurement (38) with the EIF, we require an estimate for $\mathsf{Var}[v'_{k,i}]$ at the sensor as well. Additionally, a conservative estimate (*i.e.*, a larger variance resulting in less confidence in measurements) is desirable to reduce filter divergence. While the naive approach, replacing $h_i(\underline{x}_k)$ with $z_{k,i}$ in (39), may not provide a conservative estimate when $z^2_{k,i} < h_i(\underline{x}_k)^2$, the Gaussianity of $v_{k,i}$ can be exploited to provide a conservative estimate with 95% confidence by shifting the replacement term $z_{k,i}$ by two of its standard deviations $\sqrt{r_{k,i}}$. The modified measurement's variance at timestep k can therefore be conservatively approximated by

$$\begin{aligned} r'_{k,i} &= 4(z_{k,i} + 2\sqrt{r_{k,i}})^2 r_{k,i} + 2r^2_{k,i} \\ &\gtrapprox \mathsf{Var}[v'_{k,i}]\,, \end{aligned} \tag{40}$$

at each sensor i.

The modified measurement model (36) can now be used for localisation, when measurements are modified by (38) and their new variance estimated with (40).

B. Localisation

To complete the EIF update as a linear combination aggregation, modified vectors $\underline{i}'_{k,i}$ and matrices $\mathbf{I}'_{k,i}$, using the modified measurement model (36), can be rearragned as follows.

$$\begin{aligned} \underline{i}'_{k,i} &= \mathbf{H}'^{\top}_{k,i} r'^{-1}_{k,i}(z'_{k,i} - h'_i(\underline{\hat{x}}_{k|k-1}) + \mathbf{H}'_{k,i}\underline{\hat{x}}_{k|k-1}) \\ &= \begin{bmatrix} \alpha^{(k,1)}_i & \alpha^{(k,2)}_i & 0 & \cdots \end{bmatrix}^{\top}, \end{aligned} \tag{41}$$

with

$$\begin{aligned} \alpha^{(k,1)}_i &= (2r'^{-1}_{k,i})\hat{x}^3_{k|k-1} + (2r'^{-1}_{k,i})\hat{x}_{k|k-1}\hat{y}^2_{k|k-1} \\ &\quad + (-2r'^{-1}_{k,i}s_{x,i})\hat{x}^2_{k|k-1} + (-2r'^{-1}_{k,i}s_{x,i})\hat{y}^2_{k|k-1} \\ &\quad + (2r'^{-1}_{k,i}z'_{k,i})\hat{x}_{k|k-1} + (-2r'^{-1}_{k,i}s^2_{x,i})\hat{x}_{k|k-1} \\ &\quad + (-2r'^{-1}_{k,i}s^2_{y,i})\hat{x}_{k|k-1} + (2r'^{-1}_{k,i}s^3_{x,i}) \\ &\quad + (2r'^{-1}_{k,i}s_{x,i}s^2_{y,i}) + (-2r'^{-1}_{k,i}s_{x,i}z'_{k,i}) \text{ and} \\ \alpha^{(k,2)}_i &= (2r'^{-1}_{k,i})\hat{y}^3_{k|k-1} + (2r'^{-1}_{k,i})\hat{x}^2_{k|k-1}\hat{y}_{k|k-1} \\ &\quad + (-2r'^{-1}_{k,i}s_{y,i})\hat{x}^2_{k|k-1} + (-2r'^{-1}_{k,i}s_{y,i})\hat{y}^2_{k|k-1} \\ &\quad + (2r'^{-1}_{k,i}z'_{k,i})\hat{y}_{k|k-1} + (-2r'^{-1}_{k,i}s^2_{x,i})\hat{y}_{k|k-1} \\ &\quad + (-2r'^{-1}_{k,i}s^2_{y,i})\hat{y}_{k|k-1} + (2r'^{-1}_{k,i}s_{y,i}s^2_{x,i}) \\ &\quad + (2r'^{-1}_{k,i}s^3_{y,i}) + (-2r'^{-1}_{k,i}s_{y,i}z'_{k,i})\,, \end{aligned}$$

and

$$\begin{aligned} \mathbf{I}'_{k,i} &= \mathbf{H}'^{\top}_{k,i} r'^{-1}_{k,i} \mathbf{H}'_{k,i} \\ &= \begin{bmatrix} \alpha^{(k,3)}_i & \alpha^{(k,4)}_i & 0 & \cdots \\ \alpha^{(k,5)}_i & \alpha^{(k,6)}_i & 0 & \cdots \\ 0 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix}, \end{aligned} \tag{42}$$

with

$$\begin{aligned} \alpha^{(k,3)}_i &= (4r'^{-1}_{k,i})\hat{x}^2_{k|k-1} + (-8r'^{-1}_{k,i}s_{x,i})\hat{x}_{k|k-1} \\ &\quad + (4r'^{-1}_{k,i}s^2_{x,i})\,, \\ \alpha^{(k,4)}_i &= (4r'^{-1}_{k,i})\hat{x}_{k|k-1}\hat{y}_{k|k-1} + (-4r'^{-1}_{k,i}s_{y,i})\hat{x}_{k|k-1} \\ &\quad + (-4r'^{-1}_{k,i}s_{x,i})\hat{y}_{k|k-1} + (4r'^{-1}_{k,i}s_{x,i}s_{y,i})\,, \\ \alpha^{(k,5)}_i &= \alpha^{(k,4)}_i \text{ and} \\ \alpha^{(k,6)}_i &= (4r'^{-1}_{k,i})\hat{y}^2_{k|k-1} + (-8r'^{-1}_{k,i}s_{y,i})\hat{y}_{k|k-1} \\ &\quad + (4r'^{-1}_{k,i}s^2_{y,i})\,. \end{aligned}$$

The above rearrangements give $\underline{i}'_{k,i}$ and $\mathbf{I}'_{k,i}$ as linear ~~comabinations~~ combinations of elements in

$$\begin{aligned} &\{\hat{x}^3_{k|k-1},\ \hat{y}^3_{k|k-1},\ \hat{x}^2_{k|k-1}\hat{y}_{k|k-1},\ \hat{x}_{k|k-1}\hat{y}^2_{k|k-1}, \\ &\ \hat{x}^2_{k|k-1},\ \hat{y}^2_{k|k-1},\ \hat{x}_{k|k-1}\hat{y}_{k|k-1},\ \hat{x}_{k|k-1},\ \hat{y}_{k|k-1}\}\,, \end{aligned} \tag{43}$$

which capture all of the private state information in $\underline{\hat{x}}_{k|k-1}$ required at the sensors. The corresponding EIF update steps (27) and (28) then become

$$\underline{\hat{y}}_{k|k} = \underline{\hat{y}}_{k|k-1} + \sum_{i=1}^{n} \underline{i}'_{k,i} \tag{44}$$

and

$$\mathbf{Y}_{k|k} = \mathbf{Y}_{k|k-1} + \sum_{i=1}^{n} \mathbf{I}'_{k,i}\,, \tag{45}$$

respectively.

Remark. The above has been derived for two-dimensional localisation but can be similarly derived for the three-dimensional case. However, the number of weights increases combinatorially with the number of dimensions, thus affecting the cost of communication as well.

C. Pseudocode

Measurement modification, real number encoding and linear combination aggregation are all required to compute the modified EIF from the previous section in a privacy-preserving manner. In this section, we summarise this entire localisation process and give the pseudocode for its execution. For brevity, we will assume ϕ and $M = N$ from section III-C to be public information and thus simplify the encoding notation $\mathsf{E}_{N,\phi,d}(\cdot)$ to $\mathsf{E}_d(\cdot)$. The privacy-preserving localisation filter consists of the following steps.

Setup The Setup algorithm from section IV is run only once by a trusted party, N and H are made public, and the navigator and sensor secret keys, $sk_0 = \lambda = \mathsf{lcm}(p-1, q-1)$ and sk_i, $i \in \{1, \dots, n\}$, are distributed accordingly.

Prediction At each timestep k, the navigator computes the prediction of the current state and its covariance with a local filter before encrypting weights (43) with algorithm Enc and broadcasting them to the sensors. This is given by algorithm 1.

Measurement At each timestep k, sensors modify their measurements with (38) and (40) before computing encryptions of $\underline{i}'_{k,i}$ and $\mathbf{I}'_{k,i}$ using algorithm CombEnc for each element and sending them back to the navigator. This is given by algorithm 2.

Update At each timestep k, the navigator aggregates and decrypts recieved measurement vectors and matrices with algorithm AggDec, before computing the EIF update equations (44) and (45). This is given by algorithm 3.

Algorithm 1 Navigator Prediction

procedure PREDICTION($\hat{\underline{x}}_{k-1|k-1}$, $\mathbf{P}_{k-1|k-1}$, N)
  Compute $\hat{\underline{x}}_{k|k-1}$ with a local filter
  Compute $\mathbf{P}_{k|k-1}$ with a local filter
  Compute $\mathsf{E}_0(\hat{x}^3_{k|k-1})$ by (16)
  Compute $\mathcal{E}_{pk_0}(\mathsf{E}_0(\hat{x}^3_{k|k-1}))$ by (21)
  Broadcast $\mathcal{E}_{pk_0}(\mathsf{E}_0(\hat{x}^3_{k|k-1}))$ to sensors
  for Remaining weights in (43) **do**
    Broadcast weight in the form above
  end for
  return $\hat{\underline{x}}_{k|k-1}, \mathbf{P}_{k|k-1}$
end procedure

Algorithms 1, 2 and 3 have also been summarised graphically in figure 2. Here, for brevity, $\mathcal{E}_{pk_0,sk_i}(\cdot)$ and $\mathsf{E}_d(\cdot)$ denote elementwise operations with the same parameters.

D. Leakage

With the privacy-preserving EIF defined in the previous section, we can now interpret the aggregation leakage of an LCAO

Algorithm 2 Measurement at Sensor i

procedure MEASUREMENT(i, $s_{x,i}$, $s_{y,i}$, $r_{k,i}$, N, H)
  Measure $z_{k,i}$
  Compute $z'_{k,i}$ by (38)
  Compute $r'_{k,i}$ by (40)
  Recieve $\mathcal{E}_{pk_0}(\mathsf{E}_0(\hat{x}^3_{k|k-1}))$
  for Remaining weights in (43) **do**
    Recieve weight in the form above
  end for
  Let $\boldsymbol{\alpha}_i^{(k,\tau)}$ represent the encryption of $\alpha_i^{(k,\tau)}$ in (41) and (42)
  $\boldsymbol{\alpha}_i^{(k,1)} \leftarrow \mathcal{E}_{pk_0}(\mathsf{E}_0(\hat{x}^3_{k|k-1}))^{\mathsf{E}_0(2r'^{-1}_{k,i})}\cdot$
  $\mathcal{E}_{pk_0}(\mathsf{E}_0(\hat{x}_{k|k-1}\hat{y}^2_{k|k-1}))^{\mathsf{E}_0(2r'^{-1}_{k,i})}\cdot$
  $\mathcal{E}_{pk_0}(\mathsf{E}_0(\hat{x}^2_{k|k-1}))^{\mathsf{E}_0(-r'^{-1}_{k,i}s_{x,i})}\cdot\mathcal{E}_{pk_0}(\mathsf{E}_0(\hat{x}^2_{k|k-1}))^{\mathsf{E}_0(-2r'^{-1}_{k,i}s_{x,i})}\cdot$
  $\mathcal{E}_{pk_0}(\mathsf{E}_0(\hat{y}^2_{k|k-1}))^{\mathsf{E}_0(-2r'^{-1}_{k,i}s_{x,i})}\cdot$
  $\mathcal{E}_{pk_0}(\mathsf{E}_0(\hat{x}_{k|k-1}))^{\mathsf{E}_0(2r'^{-1}_{k,i}z'_{k,i})}\cdot$
  $\mathcal{E}_{pk_0}(\mathsf{E}_0(\hat{x}_{k|k-1}))^{\mathsf{E}_0(-2r'^{-1}_{k,i}s^2_{x,i})}\cdot$
  $\mathcal{E}_{pk_0}(\mathsf{E}_0(\hat{x}_{k|k-1}))^{\mathsf{E}_0(-2r'^{-1}_{k,i}s^2_{y,i})}\cdot$
  $(N+1)^{\mathsf{E}_1(2r'^{-1}_{k,i}s^3_{x,i})}(N+1)^{\mathsf{E}_1(2r'^{-1}_{k,i}s_{x,i}s^2_{y,i})}\cdot$
  $(N+1)^{\mathsf{E}_1(-2r'^{-1}_{k,i}s_{x,i}z'_{k,i})}H(k \parallel 1) \pmod{N^2}$
  Compute remaining $\boldsymbol{\alpha}_i^{(k,\tau)}$ using (41), (42), (22) and the remark from section IV in the form above
  for $\tau \leftarrow 1$ to 6 **do**
    Send $\boldsymbol{\alpha}_i^{(k,\tau)}$ to the navigator
  end for
end procedure

Algorithm 3 Navigator Update

procedure UPDATE($\hat{\underline{x}}_{k|k-1}$, $\mathbf{P}_{k|k-1}$, N, λ)
  for $\tau \leftarrow 1$ to 6 **do**
    Receive $\boldsymbol{\alpha}_i^{(k,\tau)}$ from each sensor $i \in \{1, \dots, n\}$
  end for
  Let $\boldsymbol{\alpha}^{(k,\tau)}$ represent an encryption of $\sum_{i=1}^n \alpha_i^{(k,\tau)}$
  for $\tau \leftarrow 1$ to 6 **do**
    $\boldsymbol{\alpha}^{(k,\tau)} \leftarrow \prod_{i=1}^n \boldsymbol{\alpha}_i^{(k,\tau)}$
    Compute $\mathcal{D}_{sk_0}(\boldsymbol{\alpha}^{(k,\tau)})$ with λ by (23)
    Compute $\mathsf{E}_1^{-1}(\mathcal{D}_{sk_0}(\boldsymbol{\alpha}^{(k,\tau)}))$ by (17)
  end for
  Construct $\sum_{i=1}^n \underline{i}'_{k,i}$ and $\sum_{i=1}^n \mathbf{I}'_{k,i}$ from decoded decryptions above
  $\hat{\underline{y}}_{k|k} \leftarrow \mathbf{P}^{-1}_{k|k-1}\hat{\underline{x}}_{k|k-1} + \sum_{i=1}^n \underline{i}'_{k,i}$
  $\mathbf{Y}_{k|k} \leftarrow \mathbf{P}^{-1}_{k|k-1} + \sum_{i=1}^n \mathbf{I}'_{k,i}$
  $\hat{\underline{x}}_{k|k} \leftarrow \mathbf{Y}^{-1}_{k|k}\hat{\underline{y}}_{k|k}$
  $\mathbf{P}_{k|k} \leftarrow \mathbf{Y}^{-1}_{k|k}$
  return $\hat{\underline{x}}_{k|k}, \mathbf{P}_{k|k}$
end procedure

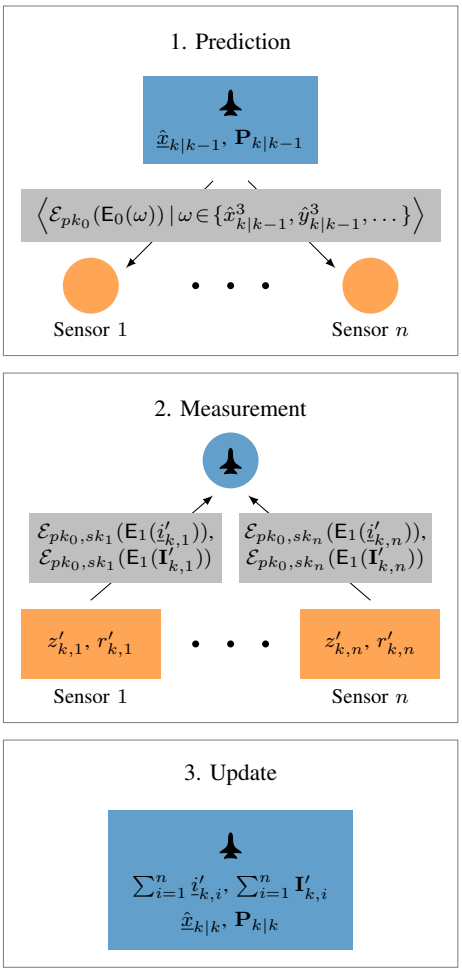

Fig. 2. Procedure at timestep k for the proposed privacy-preserving EIF.

scheme in the context of range sensor localisation. The leakage function from the AggDec algorithm corresponds to the information vector and matrix sums, $\sum_{i=1}^n i'_{k,i}$ and $\sum_{i=1}^n \mathbf{I}'_{k,i}$, respectively. However, recalling that a compromised navigator can learn the individual sums weighted by the same weight, $\{\sum_{i=1}^n 2r_{k,i}^{-1}, \sum_{i=1}^n -r_{k,i}^{-1}s_{x,i}, \sum_{i=1}^n -2r_{k,i}^{-1}s_{x,i}, \dots\}$ can be leaked as well. From this leakage, we can see that private sensor information, $z'_{k,i}$, $r'_{k,i}$ and $\underline{s}_i$, is present only in their complete sums

$$\sum_{i=1}^n z'_{k,i}\,, \quad \sum_{i=1}^n r'_{k,i}\,, \quad \sum_{i=1}^n s_{x,i} \text{ and } \sum_{i=1}^n s_{y,i}\,, \tag{46}$$

which in practice correspond to their averages. Therefore, in the context of our proposed localisation method, LCAO leakage corresponds to the averages of sensor private information, while individual sensor information remains private.

VI. Simulation and Results

As well as having shown the theoretical backing for the security of our scheme, we have simulated the proposed localisation method to evaluate its performance. A two-dimensional, linear, constant velocity process model,

$$\underline{x}_k = \begin{bmatrix} 1 & 0 & 0.5 & 0 \\ 0 & 1 & 0 & 0.5 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot \underline{x}_{k-1} + \underline{w}_k\,,$$

where noise term $\underline{w}_k \sim \mathcal{N}(\underline{0}, \mathbf{Q})$ and

$$\mathbf{Q} = \frac{1}{10^3} \cdot \begin{bmatrix} 0.4 & 0 & 1.3 & 0 \\ 0 & 0.4 & 0 & 1.3 \\ 1.3 & 0 & 5.0 & 0 \\ 0 & 1.3 & 0 & 5.0 \end{bmatrix},$$

was simulated and tracked with the algorithms in section V-C, using a linear Kalman filter for the navigator's local state prediction. Code was written in the C programming language using the MPI library [28] to support asynchronous computations by the sensors and navigator. The MG1 mask generation function and the SHA256 hash function, from the OpenSSL library [29], were used to implement the required hash function H, and the Libpaillier library [30] was used for the Paillier encryption scheme. Additionally, GNU libraries, GSL [31] and GMP [32], were used for algebraic operations and multiple-precision encoded integers, respectively. All execution was performed on a 3.33GHz Xeon W3680 CPU, running on the Windows Subsystem for Linux (WSL).

We have considered multiple sensor layouts, each with four sensors, to capture the dependence of estimated modified measurement variances $r'_{k,i}$ on the original measurements $z_{k,i}$. These layouts of varying sensor distances are shown next to the simulation initial state and a sample track in figure 3. To

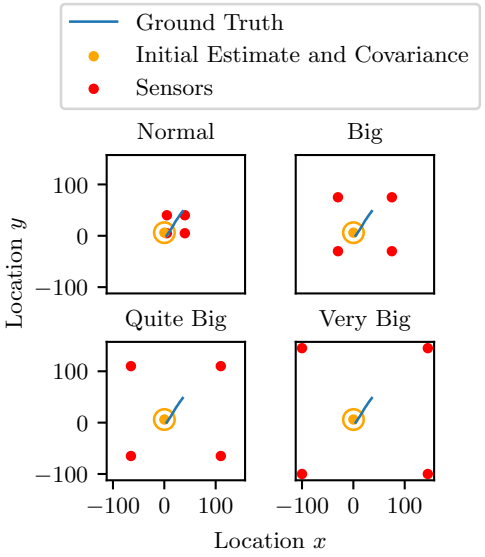

Fig. 3. Different simulation layouts with varying distances between navigator and sensors.

demonstrate the accuracy of the method, we have compared the root mean square error (RMSE) of the privacy-preserving filter to the standard EIF using unmodified measurements, which is algebraically equivalent to the EKF typically used in industry for linearising non-linear state estimation. Estimation

in each layout from figure 3 consisted of 50 filter iterations and was run 1000 times. Unmodified measurement variances were taken as $r_{k,i} = 5$ for all $k > 0$ and a large fractional precision factor, $\phi = 2^{32}$, was chosen. The results can be seen in figure 4. From these results, we can see a strong

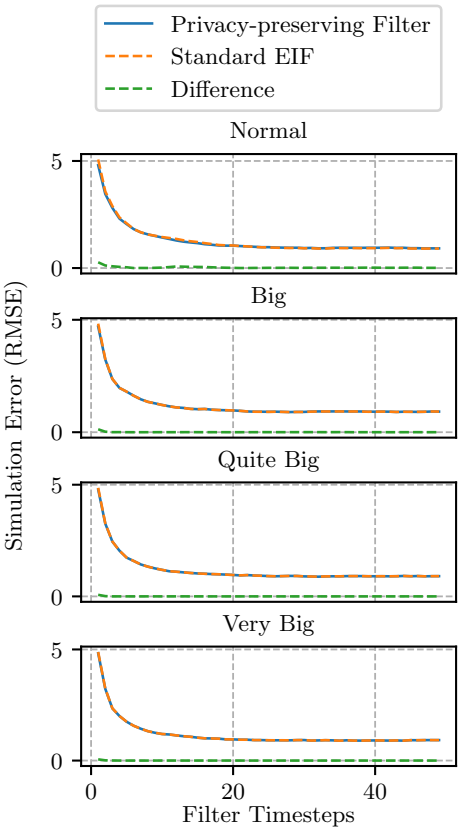

Fig. 4. Average RMSE of our privacy-preserving filter and the standard EIF for different layouts.

similarity in filter performance between the privacy-preserving method and that of the traditional EIF. We can also see that the varying average distances between sensors and the navigator have little impact on the differences in performance. We attribute this similarity in RMSE to the conservativeness of estimated modified measurement variances $r'_{k,i}$, ~~resulting in few~~ eliminating additional filter divergences, and to the high fractional precision factor, keeping computations consistent with the floating-point arithmetic of the EIF.

In addition to filter error, computational performance is important to consider when relying on cryptographic methods. Figure 5 shows the averages of 10 execution times when varying the numbers of sensors and key sizes (bit lengths of N). Here, increasing the number of sensors primarily ~~affected~~ affects the number of inter-process communications and aggregation ~~modular multiplications~~ steps due to the asynchronous implementation. We can see ~~from the figure~~ that the predominant computational costs stem from cryptographic computations and are directly dependent on the chosen key size. ~~The~~ In practice, choosing a key size should ~~be chosen such that sufficient security is achieved, and the current recommendation, when~~ take into account the duration

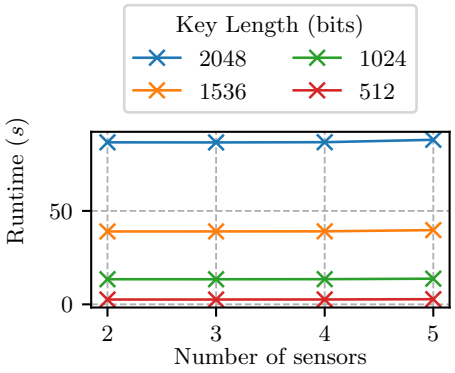

Fig. 5. Runtimes for varying key sizes and numbers of sensors.

of secrecy and the secret key lifetime. When relying on the DCRA for security~~(difficulty of factorising N),~~ , the current recommendation for encrypting government documents is the use of 2048 bit length keys [33]. For our implementation ~~of the filter, run on the~~ and aforementioned hardware, this results in a filter update ~~computation duration of roughly~~ roughly every $1.7s$. In a scenario where sensors are mobile and past navigations can be made public, reduced key sizes can be considered, while a further decrease in computation time could be achieved with code optimisations and more powerful hardware.

VII. Conclusion

We have presented a localisation filter in the presence of range-only sensors, which preserves both navigator and sensor privacies. A suitable cryptographic scheme has been introduced and a filter implementation compared and evaluated. Privacy-preserving range-only localisation is suitable for use in environments where sensor networks are untrusted or location is considered private and we hope to extend the method to broader measurement models in the future. Additional future work includes exploring more computationally efficient encryption schemes~~and filter reformulations to decrease the filter update duration, exploring the possible~~ , the security implications of sensors that are not only honest-but-curious and expanding the LCAO notion to ~~guarantee that consistent broadcasts are always made by the navigator~~enforce the consistent broadcast assumption.

Appendix A
Linear Combination Aggregator Obliviousness (LCAO)

The following game between attacker and challenger defines the security notion of LCAO.

Setup The challenger chooses security parameter κ, runs the $\mathsf{Setup}(\kappa)$ algorithm and gives pub, m and pk_0 to the attacker

Queries The attacker can now perform encryptions or submit queries that are answered by the challenger. The types of actions are:

1) *Encryption:* The attacker chooses a value x and computes an encryption of x under the aggregator's public key pk_0, obtaining $\mathcal{E}_{pk_0}(x)$.
2) *Weight Queries:* The attacker chooses an instance t and receives the weights for that instance encrypted with the aggregator's public key, $\mathcal{E}_{pk_0}(\omega_j^{(t)})$, $j \in \{1,\dots,m\}$.
3) *Combine Queries:* The attacker chooses a tuple $(i,t,a_{i,1}^{(t)},\dots,a_{i,m}^{(t)})$ such that for any two chosen combine query tuples $(i,t,a_{i,1}^{(t)},\dots,a_{i,m}^{(t)})$ and $(i',t',a_{i',1}^{\prime(t')},\dots,a_{i',m}^{\prime(t')})$, the following condition holds:

$$i = i' \wedge t = t' \implies a_{i,j}^{(t)} = a_{i',j}^{\prime(t')},\ j \in \{1,\dots,m\}\,.$$

The attacker is then given back the encryption of the linear combination $\mathcal{E}_{pk_0,sk_i}(\sum_{j=1}^m a_{i,j}^{(t)}\omega_j^{(t)})$ encrypted under both the aggregator public key pk_0 and the secret key sk_i.
4) *Compromise queries:* The attacker chooses i and receives the secret key sk_i. The aggregator's secret key may also be compromised (when choosing $i = 0$).

Challenge Next, the attacker chooses an instance t^*, and a subset of users $S \subseteq U$ where U is the complete set of users for which no combine queries, for the instance t^*, and no compromise queries, are made for the duration of the game. The attacker then chooses two series of tuples

$$\left\langle \left(i,t^*,a_{i,1}^{(t^*)(0)},\dots,a_{i,m}^{(t^*)(0)}\right) \,\middle|\, i \in S \right\rangle$$

and

$$\left\langle \left(i,t^*,a_{i,1}^{(t^*)(1)},\dots,a_{i,m}^{(t^*)(1)}\right) \,\middle|\, i \in S \right\rangle,$$

and gives them to the challenger. In the case that $0 \in S$ (*i.e.*, the aggregator is compromised) and $S = U$, it is additionally required that

$$\sum_{i\in S}\sum_{j=1}^m a_{i,j}^{(t^*)(0)}\omega_j^{(t^*)} = \sum_{i\in S}\sum_{j=1}^m a_{i,j}^{(t^*)(1)}\omega_j^{(t^*)},$$

for weights $\omega_j^{(t^*)}$, $j \in \{1,\dots,m\}$ returned by a *Weight Query* with chosen instance t^*. The challenger then chooses a random bit $b \in \{1,0\}$ and returns encryptions

$$\left\langle \mathcal{E}_{pk_0,sk_i}\left(\sum_{j=1}^m a_{i,j}^{(t^*)(b)}\omega_j^{(t^*)}\right) \,\middle|\, i \in S \right\rangle.$$

More Queries The attacker can now perform more encryptions and submit queries, so long as the queries do not break the requirements in the Challenge stage. That is, $S \subseteq U$.

Guess At the end, the attacker outputs a bit b' and wins the game if and only if $b' = b$. The advantage of an attacker $\mathcal{A}$ is defined as

$$\mathsf{Adv}^{LCAO}(\mathcal{A}) := \left|\mathrm{P}[b' = b] - \frac{1}{2}\right|.$$

Definition A.1. An encryption scheme meets LCAO security if no probabilistic adversary, running in polynomial-time with respect to security parameter κ, has more than a negligible advantage in winning the above security game. That is, for all adversaries $\mathcal{A}$, there exists a negligible function η, such that

$$\mathsf{Adv}^{LCAO}(\mathcal{A}) \le \eta(\kappa)\,,$$

with probabilities taken over randomness introduced by $\mathcal{A}$, and in Setup, Enc and CombEnc.

Appendix B
LCAO Scheme Proof

The scheme in section IV will be shown to meet LCAO by contrapositive. We show that for any adversary $\mathcal{A}$ playing against a challenger using the scheme, we can always create an adversary $\mathcal{A}'$ playing against a challenger $\mathcal{C}$ using the Joye-Libert scheme, such that

$$\mathsf{Adv}^{LCAO}(\mathcal{A}) > \eta_1(\kappa) \implies \mathsf{Adv}^{AO}(\mathcal{A}') > \eta_2(\kappa)\,,$$

for *any* negligible functions η_1, η_2 and security parameter κ. That is, if we assume our scheme is not LCAO secure, then the Joye-Libert scheme is not AO secure (which is not the case, [15]).

Proof. Consider adversary $\mathcal{A}$ playing the LCAO game. The following is a construction of an adversary $\mathcal{A}'$ playing the AO game [14] against a challenger $\mathcal{C}$ using the Joye-Libert aggregation scheme.

Setup When receiving N and H as public parameters from $\mathcal{C}$, choose an $m > 1$ and give public parameter H, number of weights m, and $pk_0 = N$ to $\mathcal{A}$.

Queries Handle queries from $\mathcal{A}$:

Weight Query When $\mathcal{A}$ submits a weight query t, choose weights $\omega_j^{(t)}$, $j \in \{1,\dots,m\}$ and random values $\rho_j \in \mathbb{Z}_N$, $j \in \{1,\dots,m\}$, and return encryptions

$$(N+1)^{\omega_j^{(t)}}\rho_j^N \pmod{N^2},\ j \in \{1,\dots,m\}$$

to $\mathcal{A}$.

Combine Query When $\mathcal{A}$ submits combine query $(i,t,a_{i,1}^{(t)},\dots,a_{i,m}^{(t)})$, choose weights $\omega_j^{(t)}, j \in \{1,\dots,m\}$ if not already chosen for the instance t, and make an AO encryption query $(i,t,\sum_{j=1}^m a_{i,j}^{(t)}\omega_j^{(t)})$ to $\mathcal{C}$. The received response will be of the form $(N+1)^{\sum_{j=1}^m a_{i,j}^{(t)}\omega_j^{(t)}}H(t)^{sk_i}$; multiply it by ~~$\rho^N$~~ $\tilde{\rho}^N$ for a random ~~$\rho \in \mathbb{Z}_N$ and return~~ $\tilde{\rho} \in \mathbb{Z}_N$ and return

$$(N+1)^{\sum_{j=1}^m a_{i,j}^{(t)}\omega_j^{(t)}}\rho\tilde{\rho}^N H(t)^{sk_i} \pmod{N^2}$$

to $\mathcal{A}$.

Compromise Query When $\mathcal{A}$ submits compromise query i, make the same compromise query i to $\mathcal{C}$, and return the recieved secret key sk_i to $\mathcal{A}$.

Challenge When $\mathcal{A}$ submits challenge series

$$\left\langle \left(i,t^*,a_{i,1}^{(t^*)(0)},\dots,a_{i,m}^{(t^*)(0)}\right) \,\middle|\, i \in S \right\rangle$$

and

$$\left\langle \left(i,t^*,a_{i,1}^{(t^*)(1)},\dots,a_{i,m}^{(t^*)(1)}\right) \,\middle|\, i \in S \right\rangle,$$

choose weights $\omega_j^{(t^*)}, j \in \{1, \ldots, m\}$ for instance t^* and submit AO challenge series

$$\left\langle \left(i, t^*, \sum_{j=1}^{m} a_{i,j}^{(t^*)(0)} \omega_j^{(t^*)} \right) \middle| \, i \in S \right\rangle$$

and

$$\left\langle \left(i, t^*, \sum_{j=1}^{m} a_{i,j}^{(t^*)(1)} \omega_j^{(t^*)} \right) \middle| \, i \in S \right\rangle ,$$

to $\mathcal{C}$. The received response will be of the form

$$\left\langle (N+1)^{\sum_{j=1}^{m} a_{i,j}^{(t^*)(b)} \omega_j^{(t^*)}} H(t^*)^{sk_i} \middle| \, i \in U \right\rangle ,$$

for an unknown $b \in \{0, 1\}$. Multiply series elements by ~~$\rho_i^N, i \in \{1, \ldots, n\}$~~ $\tilde{\rho}_i^N, i \in \{1, \ldots, n\}$ for randomly chosen ~~$\rho_i \in \mathbb{Z}_N$ and return~~ $\tilde{\rho}_i \in \mathbb{Z}_N$ and return

$$\left\langle (N+1)^{\sum_{j=1}^{m} a_{i,j}^{(t^*)(b)} \omega_j^{(t^*)}} \rho \tilde{\rho}_i^N H(t^*)^{sk_i} \middle| \, i \in U \right\rangle$$

to $\mathcal{A}$.

Guess When $\mathcal{A}$ makes guess b', make the same guess b' to $\mathcal{C}$.

In the above construction, $\mathcal{C}$ follows the Joye-Libert scheme exactly, and to $\mathcal{A}$, $\mathcal{A}'$ follows the scheme in section IV exactly. Since $\mathcal{A}'$ runs in polynomial-time to security parameter when $\mathcal{A}$ does, and no non-negligible advantage adversary to $\mathcal{C}$ exists, we conclude that no non-negligible advantage adversary $\mathcal{A}$ exists. That is, there exists a negligible function η, such that

$$\mathsf{Adv}^{LCAO}(\mathcal{A}) \leq \eta(\kappa)$$

for security parameter κ. Lastly, the function H used by our scheme is treated as a random oracle in the Joye-Libert AO proof and will, therefore, prove our scheme secure in the random oracle model as well. □

References

[1] J. Pierce, "An Introduction to Loran," *Proceedings of the IRE*, vol. 34, no. 5, pp. 216–234, 1946.

[2] M. Liggins, C. Y. Chong, D. Hall, and J. Llinas, *Distributed Data Fusion for Network-Centric Operations*. CRC Press, 2012.

[3] X. Li, Z. D. Deng, L. T. Rauchenstein, and T. J. Carlson, "Contributed Review: Source-Localization Algorithms and Applications Using Time of Arrival and Time Difference of Arrival Measurements," *Review of Scientific Instruments*, vol. 87, no. 4, pp. 921–960, 2016.

[4] A. G. O. Mutambara, *Decentralized Estimation and Control for Multisensor Systems*. CRC press, 1998.

[5] Q. Wang, Z. Duan, X. R. Li, and U. D. Hanebeck, "Convex Combination for Source Localization Using Received Signal Strength Measurements," in *21st International Conference on Information Fusion (Fusion 2018)*. Cambridge, UK: IEEE, 2018, pp. 323–330.

[6] T. He, *et al.*, "Range-Free Localization Schemes for Large Scale Sensor Networks," in *9th Annual International Conference on Mobile Computing and Networking*, 2003, pp. 81–95.

[7] F. Beutler and U. Hanebeck, "A New Nonlinear Filtering Technique for Source Localization," in *3rd IEEE Conference on Sensors (Sensors 2004)*, vol. 1, 2004, pp. 413–416.

[8] S. Gezici, *et al.*, "Localization via Ultra-Wideband Radios: A Look at Positioning Aspects for Future Sensor Networks," vol. 22, no. 4, pp. 70–84.

[9] M. Brenner, J. Wiebelitz, G. von Voigt, and M. Smith, "Secret Program Execution in the Cloud Applying Homomorphic Encryption," in *5th IEEE International Conference on Digital Ecosystems and Technologies (DEST)*, 2011, pp. 114–119.

[10] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, 2012.

[11] S. Gueron, "Intel Advanced Encryption Standard (AES) New Instructions Set," *Intel Corporation*, 2010.

[12] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems," *Communications of the ACM (CACM)*, vol. 21, no. 2, pp. 120–126, 1978.

[13] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," in *Advances in Cryptology (EUROCRYPT)*. Springer, 1999, pp. 223–238.

[14] E. Shi, T.-H. H. Chan, and E. Rieffel, "Privacy-Preserving Aggregation of Time-Series Data," *Annual Network & Distributed System Security Symposium (NDSS)*, p. 17, 2011.

[15] M. Joye and B. Libert, "A Scalable Scheme for Privacy-Preserving Aggregation of Time-Series Data," in *International Conference on Financial Cryptography and Data Security*, ser. Lecture Notes in Computer Science. Springer, 2013, pp. 111–125.

[16] J. Chotard, *et al.*, "Decentralized Multi-Client Functional Encryption for Inner Product," in *Advances in Cryptology (ASIACRYPT)*, ser. Lecture Notes in Computer Science. Springer, 2018, pp. 703–732.

[17] A. Alanwar, *et al.*, "PrOLoc: Resilient Localization with Private Observers Using Partial Homomorphic Encryption," in *16th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, 2017, pp. 41–52.

[18] M. Aristov, B. Noack, U. D. Hanebeck, and J. Müller-Quade, "Encrypted Multisensor Information Filtering," in *21st International Conference on Information Fusion (Fusion 2018)*, Cambridge, UK, 2018, pp. 1631–1637.

[19] A. B. Alexandru, M. S. Darup, and G. J. Pappas, "Encrypted Cooperative Control Revisited," in *58th IEEE Conference on Decision and Control (CDC)*, 2019, pp. 7196–7202.

[20] A. B. Alexandru and G. J. Pappas, "Private Weighted Sum Aggregation," *arXiv*, 2020.

[21] J. Katz and Y. Lindell, *Introduction to Modern Cryptography: Principles and Protocols*. Chapman & Hall, 2008.

[22] L. Lazos and R. Poovendran, "SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks," in *ACM Workshop on Wireless Security (WiSe)*. Philadelphia, PA, USA: ACM, 2004, p. 21.

[23] I. Ben-Gal, "Outlier Detection," in *Data Mining and Knowledge Discovery Handbook*. Boston, MA, USA: Springer, 2005, pp. 131–146.

[24] E. L. Oberstar, *Fixed-Point Representation and Fractional Math*. Oberstar Consulting, 2007.

[25] M. Schulze Darup, A. Redder, and D. E. Quevedo, "Encrypted Cooperative Control Based on Structured Feedback," *IEEE Control Systems Letters*, vol. 3, no. 1, pp. 37–42, 2019.

[26] F. Farokhi, I. Shames, and N. Batterham, "Secure and Private Control Using Semi-Homomorphic Encryption," *Control Engineering Practice*, vol. 67, pp. 13–20, 2017.

[27] P. S. Maybeck, *Stochastic Models, Estimation, and Control*. Academic Press, 1982.

[28] The OpenMPI Project, "Open MPI," https://www.open-mpi.org/, 2020.

[29] The OpenSSL Project, "OpenSSL," https://www.openssl.org/, 2020.

[30] J. Bethencourt, "Libpaillier," http://acsc.cs.utexas.edu/libpaillier/, 2010.

[31] The GSL development team, "GSL - GNU Scientific Library," https://www.gnu.org/software/gsl/, 2019.

[32] T. Granlund and the GMP development team, "GMP - The GNU Multiple Precision Arithmetic Library," https://gmplib.org/, 2020.

[33] E. Barker, *et al.*, "Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography," National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-56Br2, Mar. 2019.

Marko Ristic received his software engineering diploma in 2018 at the University of Melbourne, Australia. In 2019, he began work as a researcher at the Intelligent Sensor-Actuator-Systems Laboratory, Karlsruhe Institute of Technology (KIT), Germany, and since 2021, he has been pursuing a Ph.D. at the Autonomous Multisensor Systems (AMS) group, Otto von Guericke University, Germany. His research interests include encrypted and privacy-preserving signal processing, focusing on state estimation, sensor fusion, and distributed localisation.

Benjamin Noack is a professor of Computer Science at the Otto von Guericke University Magdeburg in Germany and head of the Autonomous Multisensor Systems (AMS) group. He received his diploma in computer science from the Karlsruhe Institute of Technology (KIT), Germany, in 2009. Afterward, he obtained his Ph.D. in 2013 at the Intelligent ~~SensorÔÇôActuator-Systems~~ Sensor-Actuator-Systems Laboratory, Karlsruhe Institute of Technology (KIT), Germany. His research interests are in the areas of multi-sensor data fusion, distributed and decentralized Kalman filtering, combined stochastic and set-membership approaches to state estimation, and event-based systems.

Uwe D. Hanebeck is a chaired professor of Computer Science at the Karlsruhe Institute of Technology (KIT) in Germany and director of the Intelligent ~~SensorÔÇôActuator-Systems~~ Sensor-Actuator-Systems Laboratory (ISAS). He obtained his Ph.D. degree in 1997 and his habilitation degree in 2003, both in Electrical Engineering from the Technical University in Munich, Germany. His research interests are in the areas of information fusion, nonlinear state estimation, stochastic modeling, system identification, and control with a strong emphasis on theory-driven approaches based on stochastic system theory and uncertainty models. He is author and coauthor of more than 500 publications in various high-ranking journals and conferences and an IEEE Fellow.