State Estimation with Model-Mismatch-Based Secrecy against Eavesdroppers

Selim Özgen, Saskia Kohn, Benjamin Noack, Uwe D. Hanebeck
Intelligent Sensor-Actuator-Systems, KIT, Germany
selim.oezgen@kit.edu, saskia.kohn@student.kit.edu, noack@kit.edu, uwe.hanebeck@ieee.org

***Abstract*—This study takes into consideration remote state estimation, where the state of a system is to be shared with a number of authorized users for any purpose (e.g., tracking, control), in the presence of eavesdroppers. We propose a novel control-theoretic secrecy mechanism to securely transmit the state estimate among the authorized users in the system. Moreover, as there isn't any cryptographic mechanism applied to the shared information in the conventional sense, it is not possible for the eavesdroppers to understand that the state estimate is hidden. A use-case of the proposed secrecy mechanism for a target tracking example is also demonstrated.**

***Index Terms*—eavesdropping, state secrecy, Kalman filtering, model-mismatch.**

I. Introduction

This study takes into consideration remote state estimation in the presence of eavesdroppers. The state of a system, be it a power plant or an airplane, is shared with authorized users through a wireless connection. Due to the vulnerabilities of such a connection, this information can be intercepted by an eavesdropper for any reason, ranging from gaining comparative advantage to disrupting the operation of the system.

A simple schematic for the eavesdropping scenario with a minimal number of users can be seen in Figure 1. We will denote the agent that does the state estimation as sender, the agent that the state estimation is sent to as receiver, and the adversary as eavesdropper. The sender and the receiver are the authorized agents in this scenario, whereas the eavesdropper is the unauthorized agent. Surely, it is possible to consider a higher number of senders and receivers in the wireless environment with different network topologies, where a number of authorized nodes or connections are compromised by the eavesdropper. In this case, the state estimates at different nodes of the system can be used for some clustering ideas, or consensus between the uncompromised nodes can be aimed. Yet, the simple scenario in Figure 1 is fundamental as the grounding idea and can be further extended for multi-agent system scenarios.

To preserve confidentiality, a variety of methods are offered in the literature such as encryption, differential privacy, and information-theoretic methods. The first of these methods, encrypted state estimation, has experienced a surge of interest in the recent years. It is a beneficial method because while service providers cannot access directly the content of the encrypted signals, the data can still be processed in encrypted form to perform the required signal processing tasks [1], [2]. Moreover, there are many alternatives for secrecy considering the encryption mechanisms, but the disadvantage is that they bring forward a cost of computation with respect to the quality of the encryption. As a second area of research, in differential privacy algorithms, some additional noise is added to the signal to be sent [3]. While the aim is to cause maximum damage to the state estimation process at the eavesdropper side, the authorized users are also affected by the distortion introduced to the system. Therefore, differential privacy disrupts the quality of the information not only for the eavesdropper but also for the authorized user. Finally, information-theoretic methods consider developing codes in the physical layer of wireless communications by exploiting the properties of the channel model [4], [5]. As the data travel along unreliable communication channels in a large, wireless, multihop sensor network, the effect of communication delays and loss of information in the control loop cannot be neglected [6], [7].

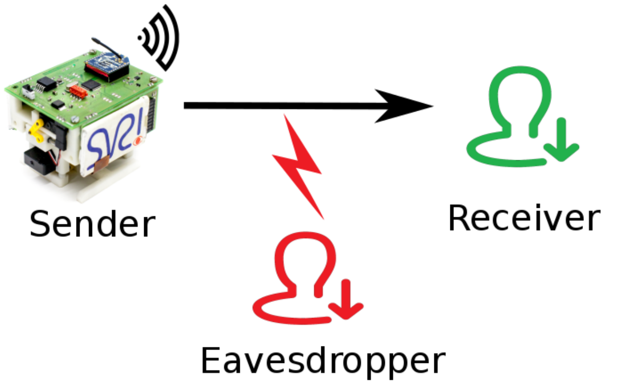


Fig. 1: Eavesdropper in a remote state estimation scenario.

Recently, scholars inspired by the use of information-theoretic methods for state secrecy have offered to exploit the inherent properties of the system as a means of encrypting the state estimation [8], [9]. They have managed to use some foundational tools from stochastic estimation and control theory as a secrecy mechanism that would allow to share the state estimate confidentially in between the authorized users with very relaxed assumptions on the broadcast channel. Inspired from this approach, we offer to use some other results from state estimation theory under model mismatch to 'encrypt' the information shared among the authorized users in an environment. In this way, we propose a secrecy mechanism that would mislead the eavesdropper to do falsified updates in the state estimation but still would cause minimal damage to the state estimation of the authorized user (no damage, i.e., optimal estimation, in the case of linear systems).

At this moment, we want to make a formal definition of secrecy. Basically, perfect secrecy is achieved when the intercepted communication gives no more information on the transmitted message than a random guess [5]. For the information-theoretic state secrecy, scholars have shown that when the channel state information for both the receiver and eavesdropper are available and the eavesdropper has a degraded channel compared to the receiver, it is possible to achieve perfect secrecy [10], [11]. This degraded channel assumption is reasonable when we interpret it as the randomness in the interception of the eavesdropper; because in practical scenarios, the eavesdropper cannot intercept all messages or it overhears the communication from a distance. As a special case of this problem, scholars have worked on a control-theoretic definition of secrecy for remote state estimation and the design of simple mechanisms that satisfy perfect secrecy criterion [8], [12], [13]. In their work, the degraded channel assumption is inherited and they aim for a control rule that would cause the eavesdropper to attain a state estimate with unbounded covariance. Therefore, even if the eavesdropper gets a state estimate, it will be valueless due to the high uncertainty in the estimation.

Not surprisingly, the solution offered for state secrecy would depend on the problem formulation. Many of the papers in the literature assume that the actual system model is known not only by the authorized users but also by the eavesdropper. This is a reasonable assumption; even when the dynamic system model is not available to the eavesdropper, she can use some a priori information to deduce the process and the measurement equations of the dynamic system.

Another determinant in the formulation of the problem is the shared information between the agents in the wireless environment. In a basic scenario, where the sender is only capable of sending the measurements of a sensor, the receiver is supposed to run a filtering algorithm for the state estimation from the received measurements. However, if the sender has enough computational capacity to do the state estimation by her own, it is possible to share the estimated state to the receiver. It is a fair assumption to assume the state estimation to be made at the sender side when we consider the expanding micro-controller technology of our day. Yet, the methods that can be used to ensure secrecy are completely different from each other when measurements or state estimates are shared between the sender and the receiver.

The greatest strength of our novel approach is its discreetness of the secrecy mechanism. For the modeling assumption, we will also accept that the eavesdropper has prior information about the dynamic system, in this case, its system model. What the eavesdropper does not know is a number of artificial system models that has been shared between the authorized users from or even before the beginning of the estimation process. The sender will do the state estimation by the aid of these models and then send it via the broadcast channel. While it is possible for the authorized users to 'decrypt' these state estimates (without loss of optimality for linear systems), the eavesdropper will be doing systematic errors in the state estimation process, possibly without even noticing that.

This paper is formulated as follows. In Section II, the state secrecy problem in presence of eavesdroppers and general solution method will be introduced. In Section III, a selection criteria for the artificial system models will be discussed and in Section IV, a particular solution will be demonstrated for a two dimensional target tracking example. Section V will conclude the paper.

II. Problem Formulation

We will assume that the system considered will follow a discrete-time linear Gaussian model. Therefore, the system and measurement models of the dynamic system will be represented as

$$\underline{\boldsymbol{x}}_k = \mathbf{A}\underline{\boldsymbol{x}}_{k-1} + \underline{\boldsymbol{w}}_{k-1} \,, \tag{1}$$

$$\underline{\boldsymbol{z}}_k = \mathbf{H}\underline{\boldsymbol{x}}_k + \underline{\boldsymbol{v}}_k \,, \tag{2}$$

where $k = 0, 1, \ldots$ is the discrete time index, both $\mathbf{A}$ and $\mathbf{H}$ are time-invariant matrices, and $\underline{\boldsymbol{w}}_k \sim \mathcal{N}(0, \mathbf{C}^w)$, $\underline{\boldsymbol{v}}_k \sim \mathcal{N}(0, \mathbf{C}^v)$ denote the process and measurement noises, respectively. $\mathcal{N}(m, P)$ denotes normal probability distribution with mean m and covariance P. For a complete representation of the system dynamics, we will also consider the initial system state to be $\underline{\boldsymbol{x}}_0 \sim \mathcal{N}(\hat{\underline{x}}_0^e, \mathbf{C}_0^e)$. Using this information, we can write the following recursion of the Kalman filter:

$$\begin{aligned}
\hat{\underline{x}}_k^p &= \mathbf{A}\hat{\underline{x}}_{k-1}^e \,, \\
\mathbf{C}_k^p &= \mathbf{A}\mathbf{C}_{k-1}^e\mathbf{A}' + \mathbf{C}^w \,, \\
\hat{\underline{x}}_k^e &= \hat{\underline{x}}_k^p + \mathbf{K}_k(\underline{z}_k - \mathbf{H}\hat{\underline{x}}_k^p) \,, \\
\mathbf{C}_k^e &= (I - \mathbf{K}_k\mathbf{H})\mathbf{C}_k^p \,, \\
\mathbf{K}_k &= \mathbf{C}_k^p\mathbf{H}'(\mathbf{H}\mathbf{C}_k^p\mathbf{H}' + \mathbf{C}^v)^{-1} \,.
\end{aligned} \tag{3}$$

Note that a one-to-one correspondence between the dynamic system mentioned and the 6-tuple $\mathcal{S} = (\mathbf{A}, \mathbf{H}, \mathbf{C}^w, \mathbf{C}^v, \hat{\underline{x}}_0^e, \mathbf{C}_0^e)$ can be formed. As long as the 6-tuple $\mathcal{S}$ and the measurement sequence $\underline{z}_k$ (or the state estimate sequence $\hat{\underline{x}}_k^e$) are available to any user, be it an eavesdropper or an authorized receiver, it is possible for this agent to do the state estimation by itself. In our problem formulation, we will assume that the system dynamics is already available to the eavesdropper. Moreover, thanks to the wireless communication environment, she can listen to the sent information, be it the measurement sequence $\underline{z}_k$ or the $\hat{\underline{x}}_k^e$.

Our idea is to share an artificial system model i among the authorized users as follows;

$$\underline{\boldsymbol{x}}_k = \mathbf{A}_i\underline{\boldsymbol{x}}_{k-1} + \underline{\boldsymbol{w}}_{i,k-1} \,, \tag{4}$$

$$\underline{\boldsymbol{z}}_k = \mathbf{H}_i\underline{\boldsymbol{x}}_k + \underline{\boldsymbol{v}}_{i,k} \,, \tag{5}$$

where both $\mathbf{A}_i$ and $\mathbf{H}_i$ are time-invariant matrices, and $\underline{\boldsymbol{w}}_{i,k} \sim \mathcal{N}(0, \mathbf{C}_i^w)$, $\underline{\boldsymbol{v}}_{i,k} \sim \mathcal{N}(0, \mathbf{C}_i^v)$. Similar to the actual dynamic system, this information can be represented by the 6-tuple

$\mathcal{S}_i = (\mathbf{A}_i, \mathbf{H}_i, \mathbf{C}_i^w, \mathbf{C}_i^v, \underline{\hat{x}}_{i,0}^e, \mathbf{C}_{i,0}^e)$. As long as a user has both the actual system information $\mathcal{S}$ and an artificial model $\mathcal{S}_i$, it is possible to 'encrypt' the state estimation using $\mathcal{S}_i$ at the sender side producing some false state estimate $\underline{\hat{x}}_{i,k}^e$, send the information through the wireless communication environment and 'decode' it at the receiver side to recover $\underline{\hat{x}}_k^e$. If the eavesdropper does not have the artificial system models, it is not possible for her to find the optimal state estimate. This situation is depicted in Figure 2.

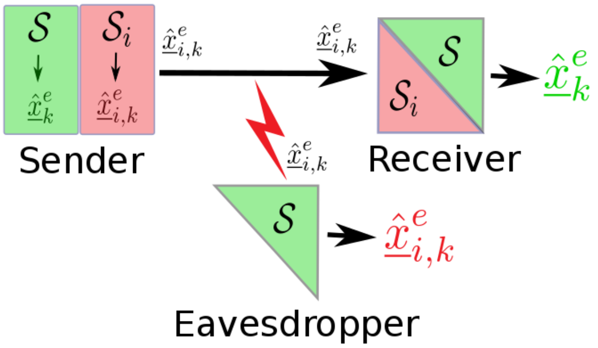

$\mathcal{S}$
$\underline{\hat{x}}_k^e$
$\mathcal{S}_i$
$\underline{\hat{x}}_{i,k}^e$
$\underline{\hat{x}}_{i,k}^e$
$\underline{\hat{x}}_{i,k}^e$
$\mathcal{S}$
$\mathcal{S}_i$
$\underline{\hat{x}}_k^e$
Sender
$\underline{\hat{x}}_{i,k}^e$
Receiver
$\mathcal{S}$
$\underline{\hat{x}}_{i,k}^e$
Eavesdropper

Fig. 2: The state estimation information is distorted using $\mathcal{S}_i$, and $\underline{\hat{x}}_{i,k}^e$ is produced. As the receiver also has $\mathcal{S}_i$, she can use this information to recover back the actual state estimate $\underline{\hat{x}}_k^e$.

III. Solution Method

A. The encryption-decryption mechanism

By using the system model $\mathcal{S}_i$ and the measurement history $\underline{z}_k$, the sender can also calculates the following recursion;

$$\underline{\hat{x}}_{i,k}^p = \mathbf{A}_i \underline{\hat{x}}_{i,k-1}^e \,, \tag{6}$$

$$\mathbf{C}_{i,k}^p = \mathbf{A}_i \mathbf{C}_{i,k-1}^e \mathbf{A}_i' + \mathbf{C}_i^w \,, \tag{7}$$

$$\underline{\hat{x}}_{i,k}^e = \underline{\hat{x}}_{i,k}^p + \mathbf{K}_{i,k}(\underline{z}_k - \mathbf{H}_i \underline{\hat{x}}_{i,k}^p) \,, \tag{8}$$

$$\mathbf{C}_{i,k}^e = (I - \mathbf{K}_{i,k}\mathbf{H}_i)\mathbf{C}_{i,k}^p \,, \tag{9}$$

$$\mathbf{K}_{i,k} = \mathbf{C}_{i,k}^p \mathbf{H}_i' (\mathbf{H}_i \mathbf{C}_{i,k}^p \mathbf{H}_i' + \mathbf{C}_i^v)^{-1} \tag{10}$$

and sends the state sequence $\underline{\hat{x}}_{i,k}^e$ to the communication channel. It is possible for the receiver to use this sequence to find the actual measurement. Using (6) and (8), we can write

$$\mathbf{K}_{i,k}\underline{z}_k = \underline{\hat{x}}_{i,k}^e - (I - \mathbf{K}_{i,k}\mathbf{H}_i)\mathbf{A}_i \underline{\hat{x}}_{i,k-1}^e \,, \tag{11}$$

$$\underline{z}_k = \mathbf{K}_{i,k}^\dagger \left(\underline{\hat{x}}_{i,k}^e - (I - \mathbf{K}_{i,k}\mathbf{H}_i)\mathbf{A}_i \underline{\hat{x}}_{i,k-1}^e\right) \tag{12}$$

where $\mathbf{K}_{i,k}^\dagger = (\mathbf{K}_{i,k}'\mathbf{K}_{i,k})^{-1}\mathbf{K}_{i,k}'$ is the pseudo-inverse of $\mathbf{K}_{i,k}$. With $\underline{z}_k$ in hand, the receiver can use the system model $\mathcal{S}$ to carry out the same state estimation procedure as at the sender side.

B. Analysis for the eavesdropper

Similar to the receiver side, the eavesdropper will get the estimates $\underline{\hat{x}}_{i,k}^e$. In case of suspicion, the eavesdropper can resort to statistical tests to understand if the measurements are fitting to the system model in hand. The well-known test for this case is checking the whiteness of the innovation process. It is known that the innovation process $\tilde{\underline{z}}_k = \underline{z}_k - \mathbf{H}\underline{\hat{x}}_k^p$ is white for the actual system model $\mathcal{S}$. The eavesdropper would also find the innovation sequence by using the state estimates but it won't be the same as the innovation process of the authorized users. We will name this process as $\tilde{\underline{z}}_{i,k}$ and it is found as follows:

$$\mathbf{K}_k \tilde{\underline{z}}_{i,k} = \underline{\hat{x}}_{i,k}^e - \underline{\hat{x}}_{i,k}^p \,, \tag{13}$$

$$\mathbf{K}_k \tilde{\underline{z}}_{i,k} = \underline{\hat{x}}_{i,k}^e - \mathbf{A}\underline{\hat{x}}_{i,k-1}^e \,, \tag{14}$$

$$\tilde{\underline{z}}_{i,k} = \mathbf{K}_k^\dagger(\underline{\hat{x}}_{i,k}^e - \mathbf{A}\underline{\hat{x}}_{i,k-1}^e) \tag{15}$$

where $\mathbf{K}_k$ is the Kalman gain calculated by using the system model $\mathcal{S}$ and $\mathbf{K}_k^\dagger$ is the pseudo-inverse of $\mathbf{K}_k$. Using (6) and (8) we can write,

$$\tilde{\underline{z}}_{i,k} = \mathbf{K}_k^\dagger(\underline{\hat{x}}_{i,k}^p + \mathbf{K}_{i,k}(\underline{z}_k - \mathbf{H}_i\underline{\hat{x}}_{i,k}^p) - \mathbf{A}\underline{\hat{x}}_{i,k-1}^e) \tag{16}$$

$$= \mathbf{K}_k^\dagger((\mathbf{A}_i - \mathbf{A})\underline{\hat{x}}_{i,k-1}^e + \mathbf{K}_{i,k}(\underline{z}_k - \mathbf{H}_i\underline{\hat{x}}_{i,k}^p)) \tag{17}$$

From (17), it can be seen that the sequence $\tilde{\underline{z}}_{i,k}$ is not white. The first term is a multiple of the state estimate sequence $\underline{\hat{x}}_{i,k}^e$ and therefore will present a correlation between the terms of the sequence. Moreover, the second term is also not equal to the innovation sequence $\tilde{\underline{z}}_k$ when $\mathbf{H}_i\underline{\hat{x}}_{i,k}^p$ is not equal to $\mathbf{H}\underline{\hat{x}}_k^p$. Therefore, unless the artificial system model $\mathcal{S}_i$ is not designed carefully, the eavesdropper can become suspicious using this simple test.

C. Solution strategy for the authorized users

A careful selection of the artificial system is necessary to pass the whiteness test discussed in Section III-B. We will use rotations for our selection of the artificial system model, that is to say, we will rotate the target state in a fixed coordinate system with a predetermined angle θ before sending the estimate. Clearly the corresponding rotation matrix will be a function of $\mathbf{R}(\theta)$ with the property $\mathbf{R}(-\theta) = \mathbf{R}(\theta)^{-1} = \mathbf{R}(\theta)'$. We will rotate the state estimate before sending it to the receiver by $\underline{\hat{x}}_{k,i}^e = \mathbf{R}(\theta)\underline{\hat{x}}_k^e$ and then, at the receiver side, we can recover by $\underline{\hat{x}}_k^e = \mathbf{R}(-\theta)\underline{\hat{x}}_{k,i}^e$. For this example, a reasonable artificial system n-tuple can be described as follows:

$$\begin{aligned}
\mathbf{A}_i &= \mathbf{R}(\theta)\mathbf{A}\mathbf{R}(-\theta) \,, \\
\mathbf{H}_i &= \mathbf{H}\mathbf{R}(-\theta) \,, \\
\mathbf{C}_i^w &= \mathbf{R}(\theta)\mathbf{C}^w\mathbf{R}(-\theta) \,, \ \ \mathbf{C}_i^v = \mathbf{C}^v \,, \\
\underline{\hat{x}}_{i,0}^e &= \mathbf{R}(\theta)\underline{\hat{x}}_0^e \,, \\
\mathbf{C}_{i,0}^e &= \mathbf{R}(\theta)\mathbf{C}_0^e\mathbf{R}(-\theta) \,.
\end{aligned} \tag{18}$$

When we apply the selected artificial system model to (6) and (8), we can see that $\underline{\hat{x}}_{i,k}^p = \mathbf{R}(\theta)\underline{\hat{x}}_k^p$ and $\underline{\hat{x}}_{i,k}^e = \mathbf{R}(\theta)\underline{\hat{x}}_k^e$ for $k \in \{0, 1, \ldots\}$. Recall that our aim is to preserve the whiteness of (17). Then;

$$\tilde{\underline{z}}_{i,k} = \mathbf{K}_k^\dagger\left((\mathbf{A}_i - \mathbf{A})\underline{\hat{x}}_{i,k-1}^e + \mathbf{K}_{i,k}(\underline{z}_k - \mathbf{H}_i\underline{\hat{x}}_{i,k}^p)\right) \tag{19}$$

$$\begin{aligned}
&= \mathbf{K}_k^\dagger((\mathbf{R}(\theta)\mathbf{A}\mathbf{R}(-\theta) - \mathbf{A})\underline{\hat{x}}_{i,k-1}^e \\
&\qquad + \mathbf{K}_{i,k}(\underline{z}_k - \mathbf{H}\mathbf{R}(-\theta)\mathbf{R}(\theta)\underline{\hat{x}}_k^p))
\end{aligned} \tag{20}$$

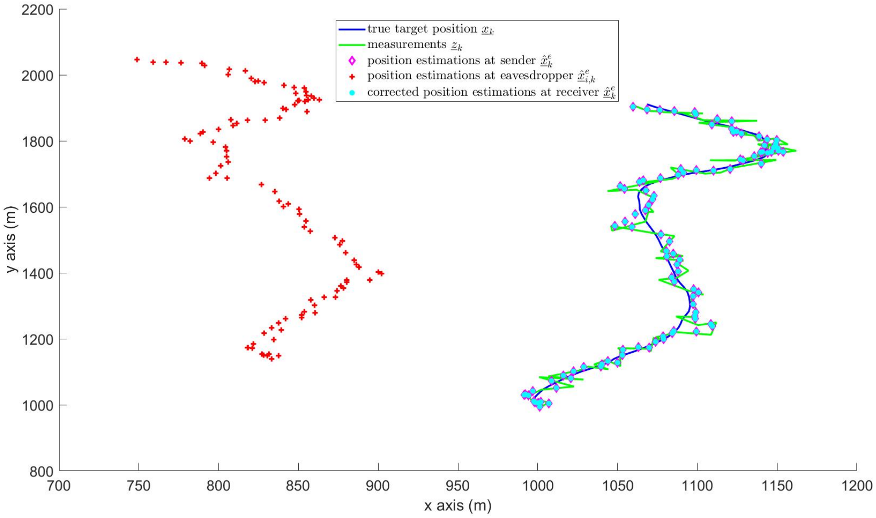


Fig. 3: Single run of the algorithm with $\theta = 0\;05\mathrm{rad}$.

Note that the second term of (20) is already equal to $\mathbf{K}_{i,k}\tilde{\underline{z}}_k$ which is a white process. Therefore if we assure that $(\mathbf{R}(\theta)\mathbf{A}\mathbf{R}(-\theta) - \mathbf{A})\hat{\underline{x}}^e_{i,k-1} = 0$, $\tilde{\underline{z}}_{i,k}$ also becomes a white process. Such a property is definitely dependent on the problem definition. We will demonstrate a solution for the problem for a two dimensional tracking problem in the rest of the paper.

IV. Simulations

A. Problem definition

We consider the problem of tracking a single target in two dimensions x, y. The state vector is defined as $\underline{\boldsymbol{x}} = [p_x\, p_y\, v_x\, v_y]'$. Both the target and the tracker use a constant velocity model as defined below [14];

$$\underline{\boldsymbol{x}}_k = \begin{bmatrix} 1 & 0 & T & 0 \\ 0 & 1 & 0 & T \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \underline{\boldsymbol{x}}_{k-1} + \underline{\boldsymbol{w}}_{k-1}\,, \tag{21}$$

$$\underline{\boldsymbol{y}}_k = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \underline{\boldsymbol{x}}_k + \underline{\boldsymbol{v}}_k\,, \tag{22}$$

where T is the sampling time.

We will exploit the properties of the particular system matrix defined in (21). To be able to use the fake model described in (18), we need to find a proper $\mathbf{R}(\theta)$ for our problem. Define

$$\mathbf{r}(\theta) = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}\,, \quad \mathbf{R}(\theta) = \begin{bmatrix} \mathbf{r}(\theta) & 0 \\ 0 & \mathbf{r}(\theta) \end{bmatrix}\,. \tag{23}$$

One can see that the property $\mathbf{R}(-\theta) = \mathbf{R}(\theta)^{-1} = \mathbf{R}(\theta)'$ is preserved for the selected rotation matrix. Moreover we can easily show that $\mathbf{R}(\theta)\mathbf{A}\mathbf{R}(-\theta) = \mathbf{A}$. Therefore, for this setup $\tilde{\underline{z}}_{i,k} = \mathbf{K}^{\dagger}_k\mathbf{K}_{i,k}\tilde{\underline{z}}_k$. While this term is a multiple of $\tilde{\underline{z}}_k$, which is already a white process, the whiteness property is preserved.

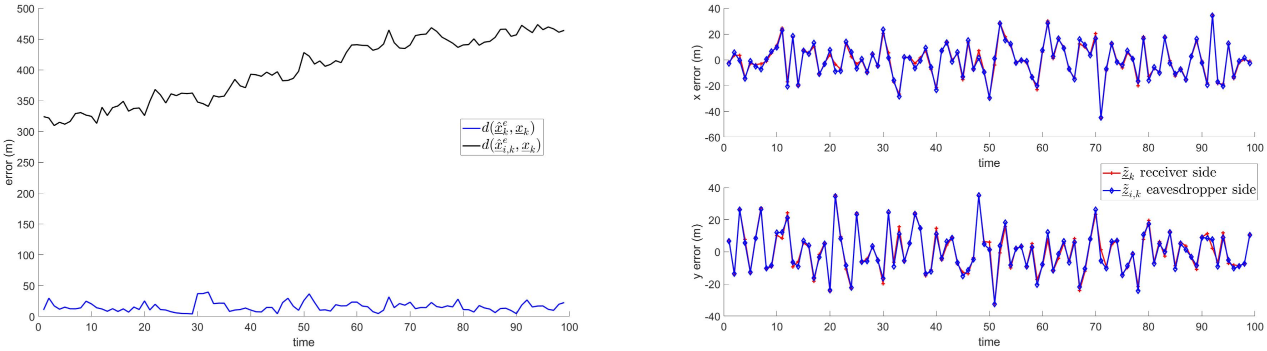
B. Evaluation

The simulation environment and the tracker codes were written in MATLAB environment. For the evaluation, the relevant parameters for the system and measurement model are given as $\mathbf{C}^w = \mathbf{L}\mathbf{L}'$ where

$$\mathbf{L} = \begin{bmatrix} T^2/2 & 0 \\ 0 & T^2/2 \\ T & 0 \\ 0 & T \end{bmatrix}\,,$$

$\mathbf{C}^v = 10^2 I_{2\times2}$, $\hat{\underline{x}}^e_0 = [1000\mathrm{m}\ 1000\mathrm{m}\ 0\mathrm{m/s}\ 0\mathrm{m/s}]'$ and $\mathbf{C}^e_0 = \mathrm{diag}(100^2, 100^2, 10^2, 10^2)$. We have selected the sampling time as $T = 1\mathrm{s}$ and $\theta = 0.05\pi\mathrm{rad}$. The selection of θ is random and can be specified regarding the application. We have selected for this experiment a small value of θ for demonstration purposes. In Figure 3, the true target position, corresponding measurements and the state estimates for the sender, eavesdropper, and receiver are depicted for a single run of the algorithm. As it is not easy to depict the velocity components of the state vector $\underline{\boldsymbol{x}}$, only the position components are depicted. It can be seen from the graph that, the receiver is able to perfectly 'decode' the state estimates; that is, the estimation results $\hat{\underline{x}}^e_k$ are recovered at the receiver side from the estimates $\hat{\underline{x}}^e_{i,k}$ by using (12). We have also demonstrated the estimation errors in Figure 4(a). Here, the error is calculated by using a distance function $d(x, y) = |x - y|'[1\ 1\ T\ T]'$. As can be seen from the figure, the estimation error for the eavesdropper is systematically increasing with the movement of the target while the estimation error for the receiver presents a steady character in proportion to the measurement quality. With increasing rotation angle θ, it is possible to increase the estimation error for the eavesdropper.

As discussed in Section III, it is possible to use the proposed state secrecy mechanism for any artificial system model $\mathcal{S}_i$, yet for an arbitrary selection of such a system, the eavesdropper



(a) Estimation errors for the receiver and the eavesdropper.

(b) Innovation processes for the receiver and the eavesdropper.

Fig. 4: Simulation results.

can use the statistical test proposed in Section III-B to realize such a secrecy mechanism. Figure 4b shows that for the proposed artificial system model given in (18), the whiteness of the innovation process is preserved. In other words, both $\tilde{\underline{z}}_k$ and $\tilde{\underline{z}}_{i,k}$ are white processes and therefore, the eavesdropper has no reason to think that such a state estimate sequence is falsified.

V. Conclusions

In this paper, we have dealt with the problem of remote state estimation with state secrecy. The problem has attracted more interest in the last two decades, especially due to development of wireless communication technology and use of cheap and reliable sensors for many different purposes from tracking to control.

In this study, the problem is discussed for a generalized set of linear Gaussian systems, but a solution strategy is proposed for only a subset of these systems. Yet the formulation of the problem is promising for a novel field of research, as there is a huge degree of freedom in the artificial system selection process. It is possible to tailor a solution for each specific dynamic system considered. Moreover it might also be possible to select a special set of possible systems and try to reach a generalized solution.

Another aspect of the proposed idea is its contribution to the definition of perfect secrecy. In the literature, perfect secrecy takes place when intercepted communication gives no more information on the transmitted message than a random guess. Here, the proposed secrecy mechanism assures that there is a systematic error in the state estimation and unless the artificial system model is not available to the eavesdropper, there is no possibility to recover the actual state estimate, that is to say, alleviate this error in the estimation.

As long as the artificial system model can be securely shared between the authorized users in the communication environment, the proposed method provides a robust solution strategy. Even when there is a perfect channel quality for both the eavesdropper and the receiver, a systemic error is always preserved in the estimates that are received by the eavesdropper. Moreover, it is possible to broaden the research for cases when the artificial system model is also known by the eavesdropper. One reasonable strategy then would be increasing the number of artificial models available to all users and using a sequence of different models.

References

[1] R. L. Lagendijk, Z. Erkin, and M. Barni, "Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation," *IEEE Signal Processing Magazine*, vol. 30, no. 1, pp. 82–105, Jan. 2013.

[2] 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; United Kingdom; 10 July 2018 through 13 July 2018*. IEEE, Piscataway (NJ), 2018, pp. 1631–1637.

[3] A. D. Sarwate and K. Chaudhuri, "Signal Processing and Machine Learning with Differential Privacy: Algorithms and Challenges for Continuous Data," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 86–94, Sep. 2013.

[4] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016, arXiv: 1505.07919.

[5] P. A. Regalia, A. Khisti, Y. Liang, and S. Tomasin, "Secure Communications via Physical-Layer and Information-Theoretic Techniques [Scanning the Issue]," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1698–1701, Oct. 2015.

[6] B. Sinopoli, L. Schenato, M. Franceschetti, K. Poolla, M. I. Jordan, and S. S. Sastry, "Kalman filtering with intermittent observations," *IEEE Transactions on Automatic Control*, vol. 49, no. 9, pp. 1453–1464, Sep. 2004.

[7] Y. Mo and B. Sinopoli, "A characterization of the critical value for Kalman filtering with intermittent observations," in *2008 47th IEEE Conference on Decision and Control*, Dec. 2008, pp. 2692–2697.

[8] A. Tsiamis, K. Gatsis, and G. J. Pappas, "State estimation codes for perfect secrecy," in *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, Dec. 2017, pp. 176–181.

[9] A. Tsiamis, K. Gatsis, and G. Pappas, "An Information Matrix Approach for State Secrecy," *arXiv:1809.07312 [cs, math]*, Sep. 2018, arXiv: 1809.07312.

[10] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[11] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[12] A. Tsiamis, K. Gatsis, and G. J. Pappas, "State Estimation with Secrecy against Eavesdroppers," *arXiv:1612.04942 [cs, math]*, Dec. 2016, arXiv: 1612.04942.

[13] A. S. Leong, D. E. Quevedo, D. Dolz, and S. Dey, "Remote State Estimation over Packet Dropping Links in the Presence of an Eavesdropper," *arXiv:1702.02785 [cs]*, Feb. 2017, arXiv: 1702.02785.

[14] S. Blackman and R. Popoli, "Design and Analysis of Modern Tracking Systems," *Artech House, Norwood, MA*, pp. 967–1068, 1999.