This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2020.2969352, IEEE Transactions on Mobile Computing

Secure Information Fusion using Local Posterior for Distributed Cyber-Physical Systems

Xiuming Liu, *IEEE Student Member*, Edith C.-H. Ngai, *IEEE Senior Member*, Jiangchuan Liu, *IEEE Fellow*

Abstract—In modern distributed cyber-physical systems (CPS), information fusion often plays a key role in automate and self-adaptive decision making process. However, given the heterogeneous and distributed nature of modern CPSs, it is a great challenge to operate CPSs with the compromised data integrity and unreliable communication links. In this paper, we study the distributed state estimation problem under the false data injection attack (FDIA) with probabilistic communication networks. We propose an integrated "detection + fusion" solution, which is based on the Kullback-Leibler divergences (KLD) between local posteriors and therefore does not require the exchange of raw sensor data. For the FDIA detection step, the KLDs are used to cluster nodes in the probability space and to partition the space into secure and insecure subspaces. By approximating the distribution of the KLDs with a general χ^2 distribution and calculating its tail probability, we provide an analysis of the detection error rate. For the information fusion step, we discuss the potential risk of double counting the shared prior information in the KLD-based consensus formulation method. We show that if the local posteriors are updated from the shared prior, the increased number of neighbouring nodes will lead to the diminished information gain. To overcome this problem, we propose a near-optimal distributed information fusion solution with properly weighted prior and data likelihood. Finally, we present simulation results for the integrated solution. We discuss the impact of network connectivity on the empirical detection error rate and the accuracy of state estimation.

Index Terms—Distributed cyber-physical system, information fusion, false data injection attack, Kullback-Leibler divergence

1 Introduction

Information fusion is a technique of combining information from multiple sources, in order to enhance the system's knowledge about the physical world [1], [2]. In a typical design of distributed cyber-physical systems (CPSs), tasks such as control and optimization are solved. Information fusion serves as a stepping stone for intelligent and autonomous decision making, and therefore has a great impact on the system's quality of service (QoS). As the sensing and communication technologies become ubiquitous today, information fusion has been widely applied in distributed CPSs, such as power grids management [3], vehicular sensing networks [4], [5], smart buildings or cities [6], and health-care applications using body area sensors [7].

However, CPSs operated over distributed networks are under increasing risk of various attacks [8], [9]. From the perspective of information fusion, the availability and the integrity of information are of the greatest concern. Unfortunately both properties can be imperilled in an adversarial environment: the availability of information can be compromised by the denial-of-service (DoS) attacks on the network layer, such as jamming attacks on the wireless channels, which reduce the probability of successful information transmission; the integrity of information can be undermined by the false data injection attack (FDIA), which is a type of deception attacks implemented by hijacking vulnerable nodes and manipulating their sensors' data. Considering the threat of the FDIA and unreliable communication links, it is especially challenging to perform secure information fusion in distributed CPSs operated over distributed networks. First, as the system offloads computations and decision making tasks to individual nodes, only the local and neighbours' information are available for the FDIA detector. Second, the distributed and probabilistic communication poses difficulties to the dissemination of raw sensor measurements, such as the heavy signalling messages for data caching and synchronization. Therefore, it is preferable for the distributed CPS to exchange the latest processed information which encapsulates historical data, instead of disseminating raw sensor measurements.

Studies have been dedicated to designing secure and robust information fusion solutions for CPSs. However, majority of the existing solutions are based on the assumption that the local filtering residuals can be accessed in a centralized manner via the communication network with a deterministic topology [10]–[13]. In many real-world systems (such as a network of autonomous vehicles), the information is exchanged in a distributed manner and the network topology is time-variant [5]. Thus an important task for distributed CPSs is to detect FDIA and carry out secure information fusion, when local information are exchanged with neighbours via probabilistic communications.

In this paper, we study the problem of secure information fusion in distributed CPSs. Specifically, the problem is formulated as a distributed state estimation problem with FDIA and probabilistic communications. The local information are exchanged between neighbouring nodes in the mobile network with a time-variant topology. We propose an integrated solution to detect the FDIA and perform information fusion, based on the Kullback-Leibler

- *Xiuming Liu and Edith C.-H. Ngai are with Department of Information Technology, Uppsala University in Uppsala, Sweden. Email: xiuming.liu@it.uu.se, edith.ngai@it.uu.se.*
- *Jiangchuan Liu is with School of Computing Science, Simon Fraser University in Vancouver, British Columbia, Canada. Email: jcliu@cs.sfu.ca.*

1536-1233 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: Uppsala Universitetsbibliotek. Downloaded on May 07,2020 at 09:42:47 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2020.2969352, IEEE Transactions on Mobile Computing

divergences (KLDs) between local posterior distributions [14]. The proposed solution consists of three sequential steps, which are executed in an iterative manner: 1) Local Bayesian filtering (LBF), which updates the local posterior with the latest sensor measurements; 2) KLD-based FDIA detection, which performs hierarchical clustering of local posteriors based on the average symmetrised KLDs matrix; 3) KLD-based consensus formulation, which dynamically weights the shared priors and local data likelihoods. By carrying out both theoretical analysis and numerical simulations, we validate the KLD-based detection and consensus formulation methods, and provide interesting insights and interpretations in terms of information geometry. Finally the proposed solution is demonstrated with an application of spatial-temporal signal monitoring, using a mobile sensor network. The performance of the proposed solution is examined under different levels of network connectivity.

The contributions of this paper are summarized as the following.

- We proposed an integrated "detection + fusion" solution for the distributed state estimation problem with probabilistic communications. The solution does not require dissemination or synchronization of raw sensor measurements, and can be implemented in mobile networks with dynamic typologies;
- We design a novel KLD-based FDIA detector. The average symmetrised KLDs between local posteriors can be approximated with general χ^2 distributions. We present an theoretical analysis of the detection error rate based on the tail probabilities of the symmetrised KLDs.
- We present a KLD-based consensus formulation, where the shared priors and local data likelihoods are dynamically weighted in order to avoid double counting the shared information. This method significantly reduces the performance gap between the near-optimal distributed solution and the optimal centralized solution.

The paper is organized as the following. In Section 2, we review the literature related to distributed estimation under FDIA. In Section 3, we present the system model and an overview of the proposed solution. The FDIA detetor design and its performance analysis are presented in Section 4. The information fusion algorithm is presented in Section 5. In Section 6, we provide simulation results and discussions to verify the proposed solution. Finally, we conclude this paper and discuss future work in Section 7.

2 Related Work

As the risk of cyber-physical attacks increases significantly in the modern society, significant research effort has been dedicated to improve the robustness of CPSs under various types of attacks. In [8], the authors reviewed the general problem of secure control in CPSs, and concluded that robust state estimation method is one of the important components for survivable CPSs. The performance of detectors and estimators, such as the Kalman filter, has been studied under the packet drop and FDIA [10], [15]. The smart and feasible strategies of both defence and attack have been investigated, relying on the centralised χ^2 test of the measurement residual or the Kalman filter's prediction residual [11]. Yan *et al*. presented a protection mechanism for consensus-based spectrum sensing with outlier detection, when the system is under covert adaptive data injection attacks [16]. More recently, the distributed detection and secure estimation problem was studied in [17], [18]. The distributed FDIA detection under jamming attack was studied very recently in [18], where the system consisted of decoupled sensing and processing networks. Machine learning detection methods gain increasing attentions too. For example, a neural network based detection method against FDI attacks was presented in [13]. Nevertheless, the problem of secure information fusion in distributed CPSs with probabilistic communications is yet to be investigated.

In parallel, the distributed information fusion in networked systems has been investigated intensively [19]. The development of distributed Kalman-consensus filters has enabled information fusion based on local and neighbours' estimates [20], [21]. As reported by the authors in [20], the algorithms based on all-to-all communications are infeasible for large networks. Therefore it is reasonable to focus on the consensus filtering methods which only require communication between neighbours. Another advantage of the consensus-based methods is that, they are naturally robust to the probabilistic communication networks as well as the false data: the error covariance matrices are utilized to quantify the uncertainty of local posteriors and hence to weight their contributions to the final estimation result.

The KLD-based anomaly detection and information fusion methods have attracted increasing attentions recently. Mathematically, the KLD between two probability density functions (PDFs) $p_i(\boldsymbol{x})$ and $p_j(\boldsymbol{x})$ of the random variable $\boldsymbol{x}$ is given by

$$D_{\mathrm{KL}}(p_i \,||\, p_j) = \int p_i(\boldsymbol{x}) \ln \frac{p_i(\boldsymbol{x})}{p_j(\boldsymbol{x})} d\boldsymbol{x},$$

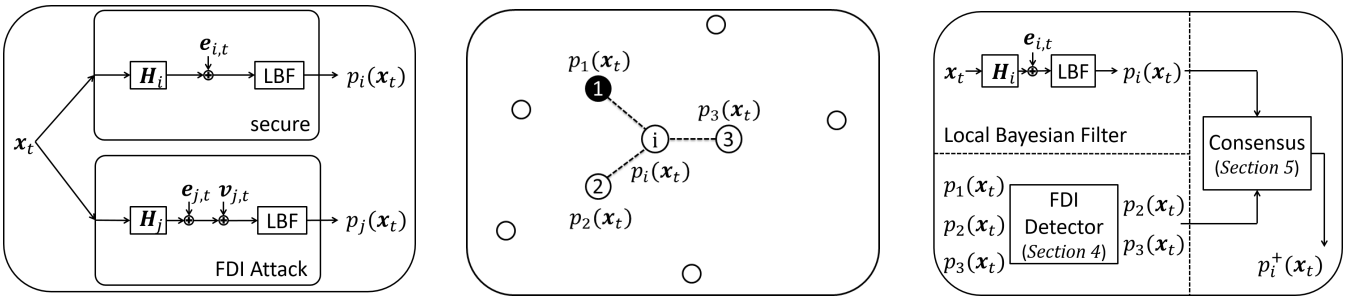
which has several meaningful interpretations. In Bayesian filtering, the KLD between a prior and a posterior measures the information gain of observing the sensor data [22]. In information geometry, the KLD measures the difference between two PDFs in a space of functions [23]. In the following we review related work about KLD-based detection and information fusion, and discuss the difference between existing methods and the proposed solution.

KLD-based false data detection

The KLD has been used as a metric of differences between distributions of normal and false data in many probabilistic detection problems [24]–[27]. In [12], the authors investigated the FDI detection problem for power grid systems. A centralized detector is able to access the historical data collected from the network and compare the distributions of current variations and the distributions of historical variations. In [28], the authors studied the fault detection problem using KLDs between healthy and test data. In [29], the author studied the multi-sensor fusion and fault detection problem. The authors used the KLDs between the data distributions obtained from the prediction step and the correction step to detect and isolate the fault. More recently, Guo *et al*. studied the FDIA from the attacker's point of view [30]. The authors define the KLD between the distributions of secure and modified measurement innovation as

1536-1233 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: Uppsala Universitetsbibliotek. Downloaded on May 07,2020 at 09:42:47 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2020.2969352, IEEE Transactions on Mobile Computing



(a) Models of sensing, filtering and FDI attacks (b) Distributed communication (c) An overview of the proposed solution

Fig. 1. An illustration of the system model and an overview of the proposed solution: (a) The sensing and filtering models of the secure case and the corrupted case. (b) The distributed and probabilistic communication. (c) The proposed solution consists of local Bayesian filtering, FDI detection, and consensus formulation.

a measure of the stealthiness of an attack scheme. However, few of previous KLD-based detectors are designed for fully distributed and mobile networks with probabilistic communication links. And most of the previous detectors are based on the sample KLDs, which is a random variable itself [31] and therefore not reliable as a metric for the detection. A more reliable detector shall utilize the different statistical properties of the sample KLDs between secure data distributions and KLDs between secure and false data distributions. In this paper, we design a FDIA detector based on the average symmetrised KLD matrix, which is an empirical estimation of the first cumulant of the distribution of the symmetrised KLDs.

KLD-based information fusion

On the other hand, given a set of posterior distributions of the system's states, the KLDs between those posteriors can be used to generate a consensus distribution. The KLD-based consensus filtering method was first studied by Battistelli *et al*. [32]. The authors defined the consensus as the probability distribution which minimizes the average KLD to neighbours' local posteriors, and provided the proof of guaranteed stability for such filtering method. The KLD-based fusion method has been applied for the multi-object estimation and multi-target density problem [33], [34]. More recently, in [35], the KLD-based consensus filtering is integrated with the hybrid Bernoulli random set filtering for secure state estimation for CPSs, when the clustered sensors and fusion nodes are under various attacks. Nevertheless, the prior information can be shared by a subset of the network, and therefore enlarges the performance gap between the centralized optimal solution and the distributed solution. It is unclear that how the double-counting prior information problem shall be avoided in those previous studies. In this work we will address the problem of double-counting prior information by dynamically weighting the shared priors and local data likelihoods.

3 System Model

In this section, we present the state-space model for the dynamic process and the distributed network. We also present the models for probabilistic communications and false data injection attacks. In the end, we give a overview of the proposed solution.

3.1 System dynamics and distributed sensing

Consider a discrete linear time-invariant (LTI) system monitored by a distributed network of N nodes. The state space model of the dynamic and the distributed sensing network is

$$\boldsymbol{x}_t = \boldsymbol{A}\boldsymbol{x}_{t-1} + \boldsymbol{w}_t, \tag{1}$$

$$\boldsymbol{y}_{i,t} = \boldsymbol{H}_i\boldsymbol{x}_t + \boldsymbol{e}_{i,t}, \tag{2}$$

where in the dynamic equation (1), $\boldsymbol{x}_t \in \mathbb{R}^M$ is the multi-dimensional system states, $\boldsymbol{A}$ is the system dynamic matrix, and $\boldsymbol{w}_t \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{\Sigma}_{\boldsymbol{w}})$ is the stochastic input process at time t; in the distributed sensing equation (2), $\boldsymbol{y}_{i,t}$ is the measurement of node i at time t, $\boldsymbol{H}_i$ is the sensing matrix of node i, and $\boldsymbol{e}_{i,t} \sim$ i.i.d $\mathcal{N}(0, \sigma_{\boldsymbol{e}}^2\boldsymbol{I})$ is the measurement noise.

As it is pointed out in [20], the sensing matrix $\boldsymbol{H}_i$ are generally different across the network for different nodes, meaning that each node is monitoring different sub-dimensions of the states vector $\boldsymbol{x}_t$. For example, when $\boldsymbol{x}_t$ is a spatial-temporal signal and the network is a vehicular network, each node in the network is measuring the signal at different locations. Nevertheless, the measurements between different sensors are correlated. For example, the covariance matrix $\boldsymbol{\Sigma}_{\boldsymbol{w}}$ describes the spatial covariances of the stochastic process $\boldsymbol{w}_t$. In case of a disconnected network and therefore information fusion cannot be performed, node i produces a local posterior $p_i(\boldsymbol{x}_t)$ solely based on $\boldsymbol{y}_{i,t}$. This is implemented by a local Bayesian filter on node i. The upper block of Figure 1(a) illustrates the model of distributed sensing and the local Bayesian filter.

3.2 Probabilistic communications

The communication links of the distributed network at time t is modelled with an undirected random graph $\mathcal{G}_t = (\mathcal{V}, \mathcal{E}_t)$, where $\mathcal{V} = \{1, \ldots, N\}$ is the set of nodes and $\mathcal{E}_t$ is the set of edges which change according to t. For nodes $\{i, j\} \in \mathcal{V}$, the probability of establishing a communication link between i and j is $\Pr(i, j)$ depends on the locations of the nodes. In wireless communication, $\Pr(i, j)$ is a function of the distance between i and j and the channel conditions. We adopt an exponentially decaying function, which depends on the distance between a pair of nodes, to model the probability of establishing a communication link between i and j:

$$\Pr(i, j) = \exp(-\lambda||\boldsymbol{s}_i - \boldsymbol{s}_j||_2), \tag{3}$$

1536-1233 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: Uppsala Universitetsbibliotek. Downloaded on May 07,2020 at 09:42:47 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2020.2969352, IEEE Transactions on Mobile Computing

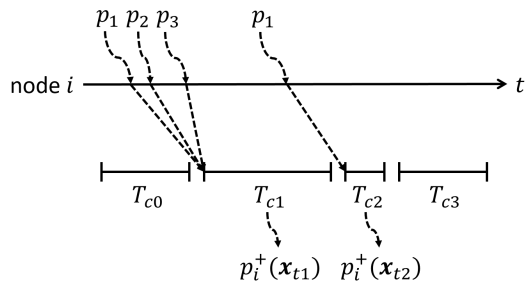


Fig. 2. An illustration of the asynchronous communication. At node i, the communication and the information fusion layers are running concurrently. When an information fusion task T_{c0} is executing, newly received local posteriors (p_1, p_2, p_3) are stored in the memory. When T_{c1} starts, the information fusion task takes the information in the memory as the input, and broadcast its output to neighboring nodes. The execution time of a information fusion task depends on the batch size of received local posteriors.

where $\boldsymbol{s}_i$ and $\boldsymbol{s}_j$ are the coordinates of nodes i and j respectively, and λ is the decay rate. Under poor radio propagation condition, the decay rate λ is large and therefore $\Pr(i,j)$ is degraded for i and j. If the communication link (i,j) is successfully established at time t, node j is node i's neighbour, $j \in N_t(i)$, and vice versa. At time t, node i has the access to local posteriors of itself and from its neighbours:

$$p_i(\boldsymbol{x}_t) \text{ and } \{p_j(\boldsymbol{x}_t) \mid j \in N_t(i)\}.$$

Considering the time-variant network topology and the probabilistic communications, the information are shared in an asynchronized manner between neighbouring nodes. In the network, a node processes the incoming information and share its latest estimate of the system states via broadcasting messages to its neighboring nodes. For example, as illustrated in Figure 2, node i received local posteriors $(\{p_1, p_2, p_3\})$ from its neighbors at different moments, while node i's previous iteration of information fusion is still executing. Those newly received messages are stored in the memory and will be used in the next iteration of information fusion. Therefore, the execution time of the information fusion task depends on the batch size of received local posteriors.

3.3 The attack model

Next we present the FDIA model. Assuming that the attacker is able to hijack node j and manipulate its measurements by exploring the system's vulnerabilities, the integrity of information from node j is compromised.

Definition 1 (False Data Injection Attack)**.** *The distributed sensing equation under the FDI attack is*

$$\boldsymbol{y}'_{j,t} = \boldsymbol{H}_j \boldsymbol{x}_t + \boldsymbol{e}_{j,t} + \boldsymbol{v}_{j,t}, \tag{4}$$

where $\boldsymbol{v}_{j,t}$ is the injected false data with configurable level of variance $\sigma_{\boldsymbol{v}}^2$.

An illustration of the FDI attack model is shown in the lower block of Figure 1(a), where $\boldsymbol{v}_{j,t}$ is injected into the sensor's local measurement which then becomes the input of the local Bayesian filter. For centralized systems, especially the electrical power grids, intensive research effort has been dedicated to constructing a smart attack sequence $\{\boldsymbol{v}_{j,t} \mid t = 0, \ldots, T\}$. We refer readers to [36] for a comprehensive review. The most common idea is to design the attack sequence such that it can bypass the χ^2 hypothesis test based on the measurement residual or the Kalman prediction residual [10], [11]. However, in the distributed CPS, it is infeasible for attackers to have global access to raw measurement data or local Bayesian filters' gains. Therefore it remains as a research question of how to smartly construct false data sequences which can bypass the distributed detection. Although it is not the focus of this study, we will briefly discuss this question based on our proposed FDIA detector in the next section.

3.4 An overview of the solution

At time t, node i is in possession of three information elements: the information fusion result from previous time step $p_i^+(\boldsymbol{x}_{t-1})$; the local measurements $\boldsymbol{y}_{i,t}$; and, in case of $N_t(i) \neq \emptyset$, the local posteriors from its neighbours $\{p_j(\boldsymbol{x}_t) \mid j \in N_t(i)\}$. The goal is to produce a combined estimate of current system states $p_i^+(\boldsymbol{x}_t)$. The proposed solution consists of three sequential steps which are executed in an on-line manner: (a) local Bayesian filtering, (b) FDI detection, and (c) consensus formulation. An overview of the proposed solution is illustrated in Figure 1(c).

Based on the previous information fusion result $p_i^+(\boldsymbol{x}_{t-1})$ and the dynamic model (1), a local predictive distribution $p_i^-(\boldsymbol{x}_t) \sim \mathcal{N}(\boldsymbol{\mu}_{i,t}^-, \boldsymbol{\Sigma}_{i,t}^-)$ is given by the Chapman-Kolmogorov equation

$$p_i^-(\boldsymbol{x}_t) = \int p(\boldsymbol{x}_t \mid \boldsymbol{x}_{t-1}) p_i^+(\boldsymbol{x}_{t-1}) d\boldsymbol{x}_t; \tag{5}$$

and the local posterior is

$$p_i(\boldsymbol{x}_t) = \frac{p(\boldsymbol{y}_{i,t} \mid \boldsymbol{x}_t) p_i^-(\boldsymbol{x}_t)}{\int p(\boldsymbol{y}_{i,t} \mid \boldsymbol{x}_t) p_i^-(\boldsymbol{x}_t) d\boldsymbol{x}_t}. \tag{6}$$

For the linear Gaussian dynamic system described in equations (1) and (2), the local filtering mean and covariance are given by the closed-form solution (Kalman filter). For nonlinear dynamic system, the filtering mean and covariance can be estimated using the sequential Monte Carlo (SMC) methods, such as the particle filter [37]. In case of the current neighbour set of node i is an empty set, the local posterior will be used as the estimate of the current system states $\boldsymbol{x}_t$. That is, if $N_t(i) = \emptyset$, $p_i^+(\boldsymbol{x}_t) = p_i(\boldsymbol{x}_t) \sim \mathcal{N}(\boldsymbol{\mu}_{i,t}, \boldsymbol{\Sigma}_{i,t})$.

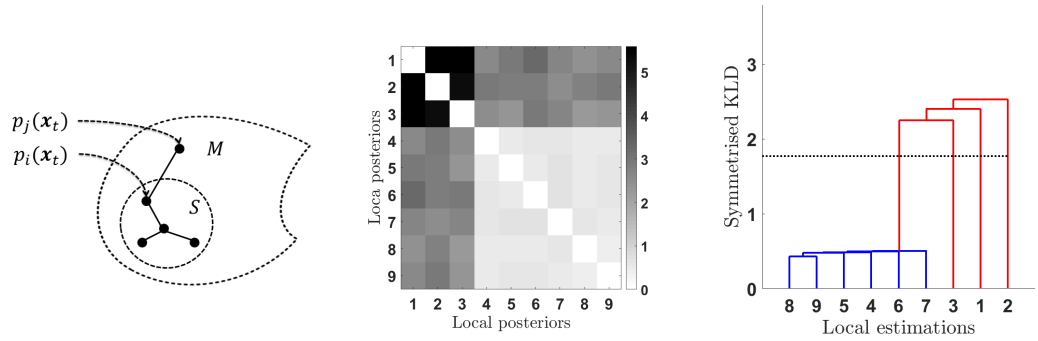
Assuming $N_t(i) \neq \emptyset$. At time t, node i receives the local posteriors $\{p_j(\boldsymbol{x}_t) \mid j \in N_t(i)\}$. Using the proposed FDIA detector in Section 4, node i then identifies the secure subset of neighbours $N_t^*(i) \subseteq N_t(i)$. Thereafter, node i combines the local posteriors from its secure neighbours and produced an updated estimate $p_i^+(\boldsymbol{x}_t)$, using the KLD-based fusion method in Section 5.

4 FDIA Detection And Analysis

In this section, we design the FDIA detector for distributed CPSs operated over probabilistic communication networks. We also present a performance analysis for the proposed FDIA detector.

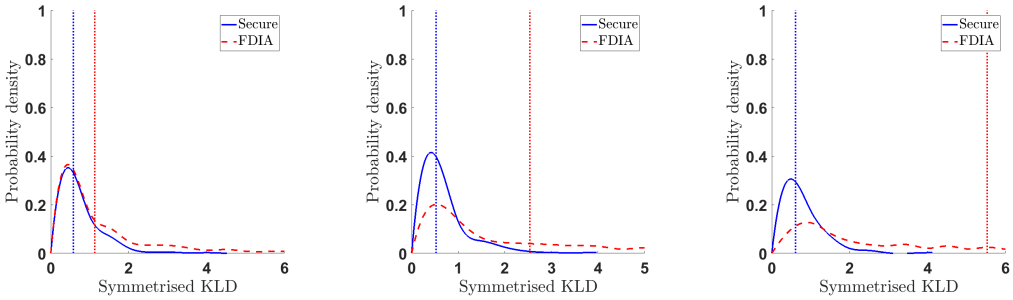
1536-1233 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: Uppsala Universitetsbibliotek. Downloaded on May 07,2020 at 09:42:47 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2020.2969352, IEEE Transactions on Mobile Computing



(a) The geometric interpretation (b) An average SKLD matrix (c) A dendrogram of clusters

Fig. 3. An illustrative example of FDIA detection with hierarchical clustering, using the average symmetrised KLD matrix. In this example, nodes $\{1, 2, 3\}$ are under FDIA. The matrix is built locally at node 9 at $t = 500$. The dendrogram shows the detection result at node 9.



(a) $\sigma_{\boldsymbol{v}}^2/\sigma_{\boldsymbol{e}}^2 = 5$ dB (b) $\sigma_{\boldsymbol{v}}^2/\sigma_{\boldsymbol{e}}^2 = 10$ dB (c) $\sigma_{\boldsymbol{v}}^2/\sigma_{\boldsymbol{e}}^2 = 15$ dB

Fig. 4. The empirical distribution density of symmetrised KLDs. In each sub figure, two distributions are visualized: the distribution of symmetrised KLD between secure local posteriors; and the distribution of symmetrised KLDs between a secure posterior and a local posterior under FDIA. The mean values of the distributions of symmetrised KLDs are marked by the vertical lines.

4.1 KLD-based FDI detection

Assuming $N_t(i) \neq \emptyset$, at time t, node i receives the local posteriors $\{p_j(\boldsymbol{x}_t) \mid j \in N_t(i)\}$. The goal is to identify local posteriors which are produced by nodes under FDIA.

In the information geometry theory, the local posteriors of node i and its neighbours can be viewed as points in a manifold of probability distributions. In this regard, the problem of detecting the FDIA can be intuitively interpreted as the problem of finding a boundary of the sub-manifold which consists of the secure local posteriors. See Figure 3(a) for an illustration. A node is identified as under the FDIA if it produces a local posterior which locates outside of the boundary. Therefore, it is crucial to define a metric which measures the distance between a pair of local posteriors, and then find a proper threshold of the distance which defines the decision boundary. The divergence between a pair of local posteriors, $p_i(\boldsymbol{x}_t)$ and $p_j(\boldsymbol{x}_t)$, can be measured by the KLD, $D_{\text{KL}}(p_i \,||\, p_j)$, which equals zero if and only if $p_i(\boldsymbol{x}_t) = p_j(\boldsymbol{x}_t)$. By constructing the matrix of symmetrised KLDs, the FDIA can be detected by applying the clustering-based detection techniques [38].

Nevertheless, there are two difficulties for identifying the FDIA by clustering directly based on the symmetrised KLDs. First, due to probabilistic communications and the time-variant set of neighbours $N_t(i)$, it is likely that node i only evaluates the symmetrised KLD between a small number of local posteriors at time t. Second, the local posterior produced by the local Bayesian filter is dependent of the measurement $\boldsymbol{y}_{i,t}$, which is a random variable, hence the symmetrised KLD matrix evaluated at time t is a random matrix. The clustering method based on the elements of the random symmetrised KLD matrix is unreliable.

Algorithm 1 The KLD-based FDI detector

for all $i \in \mathcal{V}$ at time $t = 0$ **do**
  initiate $\boldsymbol{D}_{i,t=0}$;
end for
for all $i \in \mathcal{V}$ at time t **do**
  input $p_i(\boldsymbol{x}_t)$ and $\{p_j(\boldsymbol{x}_t) \mid j \in N_t(i)\}$
  for all $(j, j') \in N_t(i)$ **do**
    Increase the counter $c_{j,j'}$ by 1;
    if $c_{j,j'} = 1$ **then**
      $\boldsymbol{D}_{i,t}(j, j') = D_{\text{SKL}}(p_j \,||\, p_{j'})$;
    else
      Update $\boldsymbol{D}_{i,t}(j, j')$ with Equation (7);
    end if
  end for
  Hierarchical classification based on $\boldsymbol{D}_{i,t}$;
  return The set of secure neighbours $N_t^*(i)$;
end for

In light of the above discussion, we design a FDIA detector based on the average symmetrised KLD. To begin with, node i initiates a $N \times N$ average symmetrised KLD matrix, denoted as $\boldsymbol{D}_{i,t=0}$. At time t, node i updates the elements $\boldsymbol{D}_{i,t}(i, j) = \boldsymbol{D}_{i,t}(j, i)$ for node $j \in N_t(i)$ with

1536-1233 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: Uppsala Universitetsbibliotek. Downloaded on May 07,2020 at 09:42:47 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2020.2969352, IEEE Transactions on Mobile Computing

the average symmetrised KLD. The elements of the average symmetrised KLD matrix can be evaluated in an on-line manner

$$\boldsymbol{D}_{i,t}(i,j) = \boldsymbol{D}_{i,t-1}(i,j) + \frac{D_{\text{SKL}}(p_i \,||\, p_j) - \boldsymbol{D}_{i,t-1}(i,j)}{N_{i,j}}, \tag{7}$$

where $N_{i,j}$ is the counter value of node j being the neighbour of node i since the beginning of time. Similarly, the elements $\boldsymbol{D}_{i,t}(j,j') = \boldsymbol{D}_{i,t}(j',j)$ can be updated for the pair of nodes $(j,j') \in N_t(i)$. As the time evolves, each node constructs the average symmetrised KLD matrix for the network. Finally, the hierarchical clustering and the decision boundary are applied to the latest average symmetrised KLD matrix. The KLD-based FDIA detector is summarized in Algorithm 1.

Figure 3(b) shows an example of the average symmetrised KLD matrix built by node 9 in a $N = 9$ network at $t = 500$, with $\sigma_{\boldsymbol{v}}^2/\sigma_{\boldsymbol{e}}^2 = 10$ dB. Node i detects the FDIA by using the average symmetrised KLD matrix as the distance matrix for hierarchical clustering and cutting the distance tree at the decision boundary α. An example of the distance tree is shown in Figure 3(c), which is a dendrogram constructed based on the matrix of Figure 3(b).

4.2 Performance analysis

In this subsection, we present a performance analysis for the KLD-based FDIA detector. Since the decision rule is based on the average symmetrised KLD matrix, we are interested in the statistical properties of the symmetrised KLD between a pair of local posteriors: for example, the distribution of symmetrised KLDs and the its tail probability. To proceed with our analysis, we make the following assumptions without loss of generality: first, the network of nodes are stabilized in locations where their local sensor measurements have uniform information gains (Kalman gains); second, the network of nodes share the same prior distribution.

In our linear Gaussian system, the KLD between a pair of local posteriors, $p_i(\boldsymbol{x}_t)$ and $p_j(\boldsymbol{x}_t)$, is given by

$$\begin{aligned} D_{\text{KL}}(p_i \,||\, p_j) = &\frac{1}{2}[\underbrace{\text{Tr}(\boldsymbol{\Sigma}_{j,t}^{-1}\boldsymbol{\Sigma}_{i,t}) - M + \ln(\frac{|\boldsymbol{\Sigma}_{j,t}|}{|\boldsymbol{\Sigma}_{i,t}|})}_{\text{deterministic}} \\ &+ \underbrace{(\boldsymbol{\mu}_{j,t} - \boldsymbol{\mu}_{i,t})^\top \boldsymbol{\Sigma}_{j,t}^{-1}(\boldsymbol{\mu}_{j,t} - \boldsymbol{\mu}_{i,t})}_{\text{a quadratic form of random variables}}], \end{aligned} \tag{8}$$

where $\boldsymbol{\Sigma}_{j,t} = \boldsymbol{\Sigma}_{i,t}$ due to the assumptions of the uniform Kalman gains and the shared prior. Therefore, the constant part of (8) is equal to zero, and $D_{\text{KL}}(p_i \,||\, p_j) = D_{\text{KL}}(p_j \,||\, p_i)$ in this special case.

The distribution of $D_{\text{KL}}(p_i \,||\, p_j)$ is therefore determined by the distribution of the quadratic form

$$(\boldsymbol{\mu}_{j,t} - \boldsymbol{\mu}_{i,t})^\top \boldsymbol{\Sigma}_{j,t}^{-1}(\boldsymbol{\mu}_{j,t} - \boldsymbol{\mu}_{i,t}), \tag{9}$$

where $\boldsymbol{\Sigma}_{j,t}^{-1}$ is a symmetric positive definite matrix by the definition of covariance matrices, and $(\boldsymbol{\mu}_{j,t} - \boldsymbol{\mu}_{i,t})$ is a M-dimensional multivariate Gaussian variable. It is a famous problem in mathematical statistics to study the distribution of the quadratic form of Gaussian variables with symmetric and non-negative definite coefficient matrices. Based on [39] and [40], the distribution of such a quadratic form can be approximated with a general χ^2 distribution. We derive the fist cumulant (the mean value) of the symmetrised KLDs between a pair of secure local posteriors in the following.

Lemma 1. *Assume the equal Kalman gains $\boldsymbol{G}_{\text{KF}}$ of the sensor measurements, and the shared prior distribution $\mathcal{N}(\boldsymbol{\mu}_0, \boldsymbol{\Sigma}_0)$, the distribution of symmetrised KLD between a pair of secure local posteriors, $p_i(\boldsymbol{x}_t)$ and $p_j(\boldsymbol{x}_t)$, can be approximated with a general χ^2 distribution with the kth cumulant [40],*

$$c_k = \text{Tr}\left((\boldsymbol{\Sigma}_0\boldsymbol{\Sigma}_{(i,j)})^k\right) + k\boldsymbol{\mu}_{(i,j)}^\top(\boldsymbol{\Sigma}_0\boldsymbol{\Sigma}_{(i,j)})^{k-1}\boldsymbol{\Sigma}_0\boldsymbol{\mu}_{(i,j)}, \tag{10}$$

where

$$\boldsymbol{\mu}_{(i,j)} = \boldsymbol{G}_{KF}(\boldsymbol{H}_{j,t} - \boldsymbol{H}_{i,t})(\mathbb{E}[\boldsymbol{x}_t] - \boldsymbol{\mu}_0), \tag{11}$$

and

$$\boldsymbol{\Sigma}_{(i,j)} = \boldsymbol{G}_{KF}[(\boldsymbol{H}_{j,t} - \boldsymbol{H}_{i,t})\boldsymbol{\Sigma}_{\boldsymbol{w}}(\boldsymbol{H}_{j,t} - \boldsymbol{H}_{i,t})^\top + 2\sigma_e^2\boldsymbol{I}]\boldsymbol{G}_{KF}^\top. \tag{12}$$

Proof. Consider the quadratic form in (8),

$$(\boldsymbol{\mu}_{j,t} - \boldsymbol{\mu}_{i,t})^\top \boldsymbol{\Sigma}_0^{-1}(\boldsymbol{\mu}_{j,t} - \boldsymbol{\mu}_{i,t}), \tag{13}$$

where $(\boldsymbol{\mu}_{j,t} - \boldsymbol{\mu}_{i,t}) \sim \mathcal{N}(\boldsymbol{\mu}_{(i,j)}, \boldsymbol{\Sigma}_{(i,j)})$, and $\boldsymbol{\Sigma}_0^{-1}$ is a symmetric positive definite covariance matrix. Given the uniform Kalman gains $\boldsymbol{G}_{\text{KF}}$ and the shared prior distribution $\mathcal{N}(\boldsymbol{\mu}_0, \boldsymbol{\Sigma}_0)$, the mean of $(\boldsymbol{\mu}_{j,t} - \boldsymbol{\mu}_{i,t})$ is

$$\begin{aligned} \boldsymbol{\mu}_{(i,j)} &= \mathbb{E}[\boldsymbol{\mu}_{j,t} - \boldsymbol{\mu}_{i,t}] \\ &= \mathbb{E}[\boldsymbol{G}_{\text{KF}}(\boldsymbol{y}_{j,t} - \boldsymbol{H}_{j,t}\boldsymbol{\mu}_0) - \boldsymbol{G}_{\text{KF}}(\boldsymbol{y}_{i,t} - \boldsymbol{H}_{i,t}\boldsymbol{\mu}_0)]. \end{aligned} \tag{14}$$

Plug in the linear measurement equation in (2), we have

$$\begin{aligned} \boldsymbol{\mu}_{(i,j)} &= \mathbb{E}[\boldsymbol{\mu}_{j,t} - \boldsymbol{\mu}_{i,t}] \\ &= \boldsymbol{G}_{\text{KF}}(\boldsymbol{H}_{j,t} - \boldsymbol{H}_{i,t})\{\mathbb{E}[\boldsymbol{x}_t + \boldsymbol{e}_{j,t} - \boldsymbol{e}_{i,t}] - \boldsymbol{\mu}_0\}, \\ &= \boldsymbol{G}_{\text{KF}}(\boldsymbol{H}_{j,t} - \boldsymbol{H}_{i,t})\{\mathbb{E}[\boldsymbol{x}_t] - \boldsymbol{\mu}_0\} \end{aligned} \tag{15}$$

If the prior $\mathcal{N}(\boldsymbol{\mu}_0, \boldsymbol{\Sigma}_0)$ is produced by an unbiased estimator of $\boldsymbol{x}_t$, for instance, a decentralized Kalman filter without interference from false data, the residual $\{\mathbb{E}[\boldsymbol{x}_t] - \boldsymbol{\mu}_0\}$ equals to zero and the random variable $(\boldsymbol{\mu}_{j,t} - \boldsymbol{\mu}_{i,t})$ has therefore zero mean.

The covariance of $(\boldsymbol{\mu}_{j,t} - \boldsymbol{\mu}_{i,t})$, $\boldsymbol{\Sigma}_{(i,j)}$, is given by

$$\begin{aligned} &\mathbb{E}[(\boldsymbol{\mu}_{j,t} - \boldsymbol{\mu}_{i,t} - \boldsymbol{\mu}_{(i,j)})(\boldsymbol{\mu}_{j,t} - \boldsymbol{\mu}_{i,t} - \boldsymbol{\mu}_{(i,j)})^\top] \\ =&\boldsymbol{G}_{\text{KF}}(\boldsymbol{H}_{j,t} - \boldsymbol{H}_{i,t})\{\mathbb{E}[(\boldsymbol{e}_{j,t} - \boldsymbol{e}_{i,t})(\boldsymbol{e}_{j,t} - \boldsymbol{e}_{i,t})^\top] \\ &+ \mathbb{E}[(\boldsymbol{x}_t - \mathbb{E}[\boldsymbol{x}_t])(\boldsymbol{x}_t - \mathbb{E}[\boldsymbol{x}_t])^\top]\}(\boldsymbol{H}_{j,t} - \boldsymbol{H}_{i,t})^\top\boldsymbol{G}_{\text{KF}}^\top \\ =&\boldsymbol{G}_{\text{KF}}[(\boldsymbol{H}_{j,t} - \boldsymbol{H}_{i,t})\boldsymbol{\Sigma}_w(\boldsymbol{H}_{j,t} - \boldsymbol{H}_{i,t}) + 2\sigma_e^2\boldsymbol{I}]^\top\boldsymbol{G}_{\text{KF}}^\top, \end{aligned} \tag{16}$$

where $\sigma_e^2\boldsymbol{I}$ is the variance of noise, and $\boldsymbol{\Sigma}_w$ is the conditional variance of $\boldsymbol{x}_t$ given $\boldsymbol{x}_{t-1}$ is fixed. Given the mean and the covariance of the Gaussian random variable $(\boldsymbol{\mu}_{j,t} - \boldsymbol{\mu}_{i,t})$, the kth cumulant of the quadratic form is given by

$$c_k = \text{Tr}\left((\boldsymbol{\Sigma}_0\boldsymbol{\Sigma}_{(i,j)})^k\right) + k\boldsymbol{\mu}_{(i,j)}^\top(\boldsymbol{\Sigma}_0\boldsymbol{\Sigma}_{(i,j)})^{k-1}\boldsymbol{\Sigma}_0\boldsymbol{\mu}_{(i,j)}. \tag{17}$$

□

After approximating the distribution of the symmetrised KLDs with a general χ^2 distribution, we are able to approximate the probability

$$\Pr\left((\boldsymbol{\mu}_{j,t} - \boldsymbol{\mu}_{i,t})^\top \boldsymbol{\Sigma}_{j,t}^{-1}(\boldsymbol{\mu}_{j,t} - \boldsymbol{\mu}_{i,t}) > \alpha\right) \tag{18}$$

1536-1233 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: Uppsala Universitetsbibliotek. Downloaded on May 07,2020 at 09:42:47 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2020.2969352, IEEE Transactions on Mobile Computing

with the tail probability $\Pr\left(\chi_l^2(\delta) > \alpha\right)$. The parameters $\{l, \delta\}$ of the general χ^2 distribution can be determined according to the cumulants c_k derived previously. Following the similar technique, we can also approximate the distribution of symmetrised KLDs between the secure local posterior and the local posterior under FDIA, and calculate its tail probabilities.

In light of the above analysis, we remark the following properties of the KLD-based FDIA detector. First, we give a statistical explanation of the average symmetrised KLD matrix.

Remark 1. *At time t, sensor i possesses an average symmetrised KLD matrix $\boldsymbol{D}_{i,t}$. Its element $\boldsymbol{D}_{i,t}(j, j')$ is an empirical estimate of the first cumulant of the distribution of symmetrised KLDs between local posteriors from the pair of nodes (j, j').*

The reliability of the average symmetrised KLD matrix, however, largely depends on the connectivity of the network. For a strongly connected network, each sensor has more opportunities to exchange information with the rest of the network and produce a better empirical estimation of the first cumulant; for a weakly connected network, the empirical estimation is based on only a small number of sample KLDs and therefore not reliable. The FDIA detector based on an unreliable average symmetrised KLD matrix leads to high detection error rate.

Another key factor of designing the KLD-based FDIA detector is the configuration of decision boundary α.

Remark 2. *Let c_1 be the maximum first cumulant of the symmetrised KLD between posteriors produced by a pair of secure nodes, and c_1' be the minimum first cumulant of the symmetrised KLD between posteriors from a secure node and a node under FDIA. The detector is able to identify the FDIA if $c_1 < c_1'$ if the decision boundary α satisfies the condition*

$$c_1 < \alpha < c_1'. \tag{19}$$

In the early stage of the iterative FDIA detection procedure (Algorithm 1), the reliability of average symmetrised KLD matrices $\{\boldsymbol{D}_{i,t} \mid i \in \mathcal{V}\}$ can be unsatisfying, which will lead to high detection error rate. We provide an analysis of the error rate in the next result.

Theorem 1. *For secure node i at time t, the expected FDIA detection error rate P_e is given by*

$$\begin{aligned} P_e = \frac{1}{|N_t(i)|}\{ &\sum_{j \in N_t^*(i)} \prod_{j' \in \{N_t^*(i) \setminus j\}} \Pr\left(\boldsymbol{D}_{i,t}(j, j') > \alpha\right) \\ &+ \sum_{j \in \{N_t(i) \setminus N_t^*(i)\}} \prod_{j' \in N_t^*(i)} [1 - \Pr\left(\boldsymbol{D}_{i,t}(j, j') > \alpha\right)]\}. \end{aligned} \tag{20}$$

Proof. For a secure node i at time t, let $N_t(i)$ be its neighbour nodes and $N_t^*(i) \subseteq N_t(i)$ is the set of secure neighbour nodes. The expected FDI detection error rate is defined as

$$\frac{\text{expected number of errors}}{\text{number of neighbours}},$$

where the number of neighbours, $|N_t(i)|$, depends on the size of the network and the channel condition described in (3); and the expected number of errors consists of two types of errors, type 1 and type 2 errors. For a node $j \in N_t(i)$, there are two possible miss-detection scenarios:

- Type 1 error: j is secure, but detected as under FDIA. In this scenario, the minimum distance between j and $j' \in \{N_t^*(i) \setminus j\}$ is larger than the decision boundary α,

$$\begin{aligned} P_{e,\text{type 1}}(j) &= \Pr\big(\min_{j' \in \{N_t^*(i) \setminus j\}} \boldsymbol{D}_{i,t}(j, j') > \alpha\big) \\ &= \prod_{j' \in \{N_t^*(i) \setminus j\}} \Pr\left(\boldsymbol{D}_{i,t}(j, j') > \alpha\right), \end{aligned} \tag{21}$$

and the expected number of type 1 errors is given by

$$\sum_{j \in N_t^*(i)} P_{\text{type 1}}(j). \tag{22}$$

- Type 2 error: j is under FDIA, but detected as secure. In this scenario, the minimum distance between j and $j' \in \{N_t^*(i) \setminus j\}$ is smaller than the decision boundary α,

$$\begin{aligned} P_{e,\text{type 2}}(j) &= \Pr\big(\min_{j' \in N_t^*(i)} \boldsymbol{D}_{i,t}(j, j') < \alpha\big) \\ &= 1 - \Pr\big(\min_{j' \in N_t^*(i)} \boldsymbol{D}_{i,t}(j, j') > \alpha\big) \\ &= 1 - \prod_{j' \in N_t^*(i)} \Pr\left(\boldsymbol{D}_{i,t}(j, j') > \alpha\right) \end{aligned} \tag{23}$$

and the expected number of type 2 errors is given by

$$\sum_{j \in \{N_t(i) \setminus N_t^*(i)\}} P_{\text{type 2}}(j). \tag{24}$$

To conclude, the expected detection error rate is given by

$$P_e = \frac{\sum_{j \in N_t^*(i)} P_{\text{type 1}}(j) + \sum_{j \in \{N_t(i) \setminus N_t^*(i)\}} P_{\text{type 2}}(j)}{|N_t(i)|}. \tag{25}$$

□

As mentioned previously, the reliability of the average symmetrised KLD matrix plays a key role in determining the performance of the FDIA detector. The performance of the detector can be improved by enhancing the communication channel condition, which will be demonstrated in Section 6.

5 KLD-BASED INFORMATION FUSION

After identifying the secure neighbours $N_t^*(i) \subseteq N_t(i)$, node i proceeds to formulate a consensus distribution based on the secure local posteriors.

Let $\{p_j(\boldsymbol{x}_t) \mid j \in N_t^*(i)\}$ be the set of secure local posteriors which can be accessed by node i. The consensus distribution $p_i^+(\boldsymbol{x}_t)$ is defined as the following.

Definition 2. *For node i, given its local posterior $p_i(\boldsymbol{x}_t)$ and its secure neighbours' local posteriors $\{p_j(\boldsymbol{x}_t) \mid j \in N_t^*(i)\}$, the consensus is defined as*

$$p_i^+ \triangleq \arg\min_q \pi_i D_{KL}(q \| p_i) + \sum_{j \in N_t^*(i)} \pi_j D_{KL}(q \,\|\, p_j), \tag{26}$$

where π_i and π_j, $j \in N_t^*(i)$, are associated weights with the summation equals to one.

The equation (26) defines that the consensus distribution minimizes the weighted average KLD to $p_i(\boldsymbol{x}_t)$ and

1536-1233 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: Uppsala Universitetsbibliotek. Downloaded on May 07,2020 at 09:42:47 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2020.2969352, IEEE Transactions on Mobile Computing

$\{p_j(\boldsymbol{x}_t) \mid j \in N_t^*(i)\}$. In the minimization problem, the loss function consists of two parts: the first element is the KLD between the consensus distribution and node i's local posterior; the second element is the summation of KLDs between the consensus distribution and the local posteriors from node i's secure neighbours. It is insightful to point out that the KLD minimization problem can be related to other existing works. In Bayesian inference, the minimization is similar to the general belief updating framework proposed in [41], where the summation of KLDs is selected as the loss function. From the multi-agent system's perspective, the minimization yields a consensus on the local filtering distributions [32].

Similar to the result in [32], the solution of the KLD minimization problem (26) is reported here.

Theorem 2 (KLD-based consensus information fusion)**.** *For node i ($i \in \mathcal{V}$), given the local posteriors $p_i(\boldsymbol{x}_t)$ and $\{p_j(\boldsymbol{x}_t) \mid j \in N_t^*(i)\}$, the solution of the KLD minimization problem in* (26) *is*

$$p_i^+(\boldsymbol{x}_t) = \frac{p_i(\boldsymbol{x}_t)^{\pi_i} \prod_{j\in N_t^*(i)} p_j(\boldsymbol{x}_t)^{\pi_j}}{\int p_i(\boldsymbol{x}_t)^{\pi_i} \prod_{j\in N_t^*(i)} p_j(\boldsymbol{x}_t)^{\pi_j} d\boldsymbol{x}_t}. \tag{27}$$

Furthermore, for Gaussian variables, the result in Theorem 2 can be simplified to

$$p_i^+(\boldsymbol{x}_t) = p_i(\boldsymbol{x}_t)^{\pi_i} \prod_{j\in N_t^*(i)} p_j(\boldsymbol{x}_t)^{\pi_j} \sim \mathcal{N}(\boldsymbol{\mu}_{i,t}^+, \boldsymbol{\Sigma}_{i,t}^+), \tag{28}$$

where the mean and covariance are obtained by convex combinations of means and covariances of local posteriors,

$$(\boldsymbol{\Sigma}_{i,t}^+)^{-1} = \pi_i \boldsymbol{\Sigma}_{i,t}^{-1} + \sum_{j\in N_t^*(i)} \pi_j \boldsymbol{\Sigma}_{j,t}^{-1}, \tag{29}$$

$$(\boldsymbol{\Sigma}_{i,t}^+)^{-1} \boldsymbol{\mu}_{i,t}^+ = \pi_i \boldsymbol{\Sigma}_{i,t}^{-1} \boldsymbol{\mu}_{i,t} + \sum_{j\in N_t^*(i)} \pi_j \boldsymbol{\Sigma}_{j,t}^{-1} \boldsymbol{\mu}_{j,t}, \tag{30}$$

which can be computed in a recursive manner. The above solution has the similar form as the method of Fisher information matrix (FIM) weighted averaged of maximum likelihood estimations [42]. Indeed, both methods pursue the optimal combination of estimates.

5.1 Dynamic weighting of local posteriors

Another challenging question emerges from the dynamic topology in a mobile network poses: how to assign proper weights for the local posterior and the secure neighbours' estimates? That is, for each node i, we need to determine π_i and π_j, $j \in N_t^*(i)$, under the condition of $\pi_i + \sum_{j\in N_t^*(i)} \pi_j = 1$.

In the mobile network, each node has a time-variant degree (number of connections to other nodes). The high degree a node has, the more information sources it holds. The local posterior from a highly connected node is built based on more estimates from its secure neighbours (i.e., secure information source), and shall be assigned with a higher weights, comparing to the local posterior from a secure neighbour with lower degree. To address this issue, for each node, we design an auxiliary message sent together with its local posterior to the neighbour nodes. The message contains an integer number which indicates how many secure information sources contributes to the node's previous consensus distribution.

Remark 3. *For node i, the number of secure information sources contributes to its previous consensus $p_i^+(\boldsymbol{x}_{t-1})$ is $|N_{t-1}^*(i)|$ (see Theorem 2). Since the local posterior $p_i(\boldsymbol{x}_t)$ is updated based on $p_i^+(\boldsymbol{x}_{t-1})$ via the local Bayesian filter* (6)*, $|N_{t-1}^*(i)|$ is also an indicator of the informativeness of $p_i(\boldsymbol{x}_t)$.*

Therefore, for node i at time t, besides the local posteriors from itself and its secure neighbours $\{p_i(\boldsymbol{x}_t)\} \cup \{\{p_j(\boldsymbol{x}_t) \mid j \in N_t^*(i)\}\}$, it also possesses the indicators $|N_{t-1}^*(i)|$ and $|N_{t-1}^*(j)|, \forall j \in N_t^*(i)$. Given those indicators, we design the weights

$$\pi_i^t = \frac{|N_{t-1}^*(i)|}{|N_{t-1}^*(i)| + \sum_{j\in N_t^*(i)} |N_{t-1}^*(j)|}, \tag{31}$$

$$\pi_j^t = \frac{|N_{t-1}^*(j)|}{|N_{t-1}^*(i)| + \sum_{j\in N_t^*(i)} |N_{t-1}^*(j)|}, \tag{32}$$

for the local posteriors from node i itself and its secure neighbours $j \in N_t^*(i)$. Note that π_i^t and π_j^t are time-variant, due to the dynamic topology of the mobile network and therefore the set of secure neighbours $N_t^*(i)$. Finally, the dynamic weights are used in formulating the consensus in Theorem 2.

5.2 The shared prior in formulating consensus

Although that the consensus-based information fusion is intuitive and has shown its efficiency in studies such as [32]. There is a hidden risk of double-counting the information from the same prior, which has not been properly addressed in previous studies. In this section, we present analytic results which reveal the double-counted prior information, and provide a method to mitigate this problem.

Consider a simple example illustrated in Figure 5. In the case of $5(a)$, two nodes started from the same prior $p_0(\boldsymbol{x}_t)$ and then each obtain a local measurement ($\boldsymbol{y}_{1,t}$ or $\boldsymbol{y}_{2,t}$). The local Bayesian update gives

$$p_1(\boldsymbol{x}_t) \propto p_0(\boldsymbol{x}_t) p(\boldsymbol{y}_{1,t} \mid \boldsymbol{x}_t), \tag{33}$$

$$p_2(\boldsymbol{x}_t) \propto p_0(\boldsymbol{x}_t) p(\boldsymbol{y}_{2,t} \mid \boldsymbol{x}_t). \tag{34}$$

Given the same degrees of two nodes, the local posteriors from a node itself and its neighbour are weighted uniformly. The consensuses reached by both nodes are

$$p_1^+(\boldsymbol{x}_t) = p_2^+(\boldsymbol{x}_t) \propto p_0(\boldsymbol{x}_t) p(\boldsymbol{y}_{1,t} \mid \boldsymbol{x}_t)^{\frac{1}{2}} p(\boldsymbol{y}_{2,t} \mid \boldsymbol{x}_t)^{\frac{1}{2}}. \tag{35}$$

Comparing to the case of centralized Bayesian update in Figure 5(b), where the updated estimate is

$$p(\boldsymbol{x}_t) \propto p_0(\boldsymbol{x}_t) p(\boldsymbol{y}_{1,t}, \boldsymbol{y}_{2,t} \mid \boldsymbol{x}_t) \tag{36}$$

we see that not only the likelihood $p(\boldsymbol{y}_{1,t}, \boldsymbol{y}_{2,t} \mid \boldsymbol{x}_t)$ from the data are approximated by the composition $p(\boldsymbol{y}_{1,t} \mid \boldsymbol{x}_t) p(\boldsymbol{y}_{2,t} \mid \boldsymbol{x}_t)$, but also down weighted by $\frac{1}{2}$. In other words, in the consensus formulated by Theorem 2, the information from the prior is relatively over weighted, comparing to the optimal Bayesian update. Formally, in the following proposition, we reveal the problem of double-counting information from the prior, when formulating consensus.

Lemma 2. *In a strongly connected network with the same shared prior, when the size of network increases to infinity, the consensus reached by the network converges to the prior.*

1536-1233 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: Uppsala Universitetsbibliotek. Downloaded on May 07,2020 at 09:42:47 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2020.2969352, IEEE Transactions on Mobile Computing

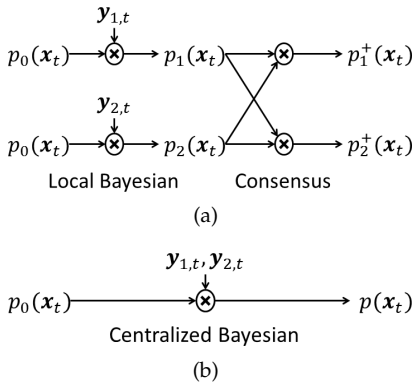


Fig. 5. An illustrative example of double-counting the information from the same prior, using the consensus-based fusion in Theorem 2. In 5(a), the same prior used in local Bayesian updates are over-weighted in the consensus, when compare to the centralized Bayesian updated in 5(b).

Proof. Consider a strongly connected network of size N, and the same prior $p_0(\boldsymbol{x}_t)$ is shared by all nodes. The consensus formulated by node i in the network is given by

$$p_i^+(\boldsymbol{x}_t) \propto p_0(\boldsymbol{x}_t) \prod_{j\in\{1,\dots,N\}} p(\boldsymbol{y}_{j,t} \mid \boldsymbol{x}_t)^{\frac{1}{N}}, \tag{37}$$

where $1/N$ is the uniform weight for local posteriors. When $N \to \infty$, the weights on the composite likelihoods from data goes zero. Therefore,

$$\lim_{N\to\infty} p_i^+(\boldsymbol{x}_t) = p_0(\boldsymbol{x}_t). \tag{38}$$

□

From the above analysis, we understand that there will be a gap of estimation accuracy (for example, mean square error (MSE)) between the optimal centralized Bayesian update and the distributed consensus formulation, even when the network is strongly connected. And the gap will become bigger when the size of network increases. This gap comes from two factors: 1, double-counting the information from the same prior; 2, the approximation of full likelihood with the composite likelihood. While the gap caused by the second factor is an inevitable and small (given the spatial-temporal data) price to pay for distributed systems; the gap due to the first factor is the major concern and shall be eliminated if possible. In the next, we present methods for properly weighting the prior.

5.3 Dynamic weighting of data likelihood and prior

Based on the previous discussion, when the network is sharing the same prior, each node need to down weight the prior and increase the weight for the likelihood of the latest local measurement, in order to eliminate the double-counted information from the same prior in the consensus.

Considering the illustrative example in Figure 5 again, if both nodes increase the weights for their local data likelihoods by 2 (the number of secure neighbours plus a node itself), the local Bayesian update gives

$$p_1'(\boldsymbol{x}_t) \propto p_0(\boldsymbol{x}_t) p(\boldsymbol{y}_{1,t} \mid \boldsymbol{x}_t)^2, \tag{39}$$

$$p_2'(\boldsymbol{x}_t) \propto p_0(\boldsymbol{x}_t) p(\boldsymbol{y}_{2,t} \mid \boldsymbol{x}_t)^2. \tag{40}$$

Algorithm 2 Secure Information Fusion

for all $i \in \mathcal{V}$ at time t **do**
  input $p_i^+(\boldsymbol{x}_{t-1})$ and $\boldsymbol{y}_{i,t}$
  Compute $p_i^-(\boldsymbol{x}_t)$ using $p_i^+(\boldsymbol{x}_{t-1})$;
  Compute $p_i(\boldsymbol{x}_t)$ using $p_i^-(\boldsymbol{x}_t)$ and $\boldsymbol{y}_{i,t}$;
  // Local Bayesian Filtering
  if $N_t(i) = \emptyset$ **then**
    $p_i^+(\boldsymbol{x}_t) = p_i(\boldsymbol{x}_t)$;
  else
    Obtain $N_t^*(i)$ by calling Algorithm 1.
    // FDIA detection
    if $N_t^*(i) = \emptyset$ **then**
      $p_i^+(\boldsymbol{x}_t) = p_i(\boldsymbol{x}_t)$;
    else
      Compute $p_i^+(\boldsymbol{x}_t)$ using (43);
      // Consensus formulation with dynamic weights
    end if
  end if
  return $p_i^+(\boldsymbol{x}_t)$;
end for

Remark 4. *For the linear Gaussian system in* (1) *and* (2)*, the increased weights on local data likelihood is effectively equivalent to the increased Kalman gain. Although the local Bayesian update and the Kalman gains are optimal in the case of an isolated node, they are not optimal if the local posterior will be used in the further consensus formulation. Therefore, in order to eliminate double-counting the same prior, we want to increase the Kalman gain, such that the local posterior are more responsive to the local measurement.*

Thereafter, the consensus formulated at each node is

$$p_1'^+(\boldsymbol{x}_t) = p_2'^+(\boldsymbol{x}_t) \propto p_0(\boldsymbol{x}_t) p(\boldsymbol{y}_{1,t} \mid \boldsymbol{x}_t) p(\boldsymbol{y}_{2,t} \mid \boldsymbol{x}_t), \tag{41}$$

which is an approximation of the centralized Bayesian update with the composite likelihood and the properly weighted prior. Formally, we present the following method for distributed consensus formulation without double-counting the information from the same prior.

Theorem 3 (Consensus with Properly Weighted Data and Prior)**.** *Assume the network of size N is sharing the same prior $p_0(\boldsymbol{x}_t)$ and strongly connected. For node i ($i \in \mathcal{V}$), the local Bayesian update with the increased weight on data is given by*

$$p_i'(\boldsymbol{x}_t) \propto p_0(\boldsymbol{x}_t) p(\boldsymbol{y}_{i,t} \mid \boldsymbol{x}_t)^N, \tag{42}$$

and the consensus formulated by node i is

$$p_i^+(\boldsymbol{x}_t) \propto p_0(\boldsymbol{x}_t) \prod_{j\in\{1,\dots,N\}} p(\boldsymbol{y}_{j,t} \mid \boldsymbol{x}_t), \tag{43}$$

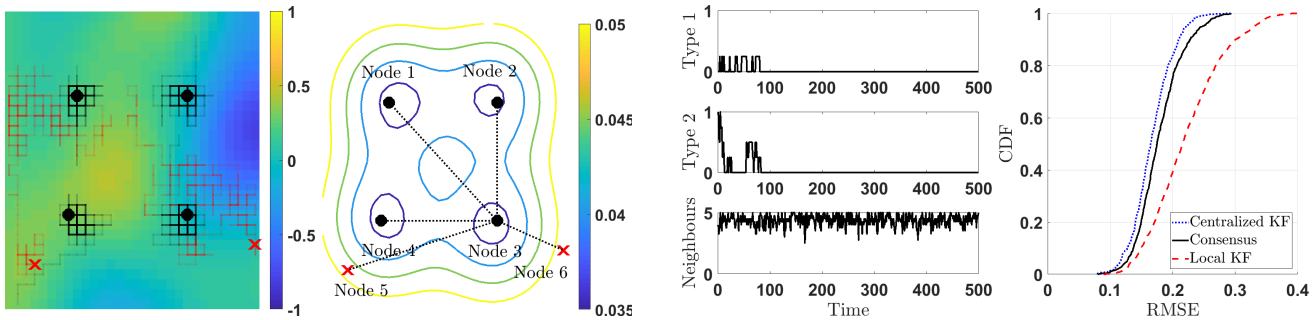
which is an approximation of the centralized Bayesian update with the properly weighted data and prior.

The proof of the above results naturally follows our previous analysis and therefore omitted here.

Nevertheless, a problem rises from the mobility of the network is that, the network is not always strongly connected and therefore does not share the same prior. Even when the network started with the same initial prior $p_0(\boldsymbol{x}_0)$ at time $t = 0$, after a few steps, due to their different

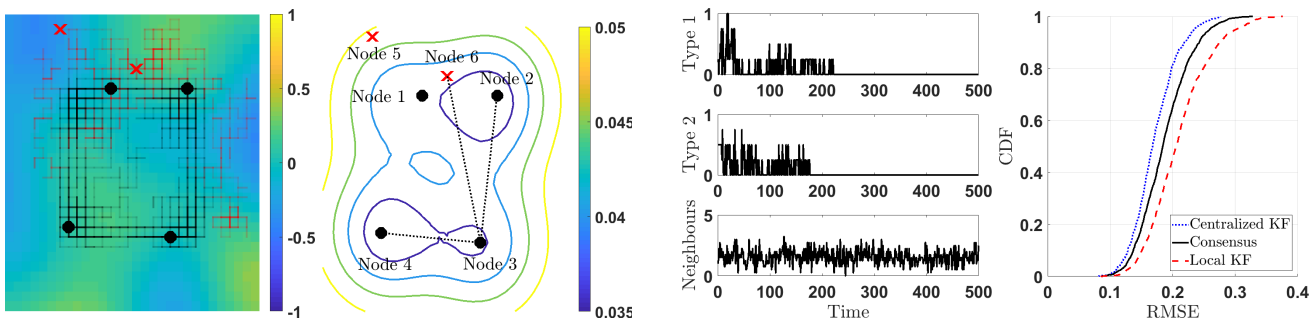
1536-1233 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: Uppsala Universitetsbibliotek. Downloaded on May 07,2020 at 09:42:47 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2020.2969352, IEEE Transactions on Mobile Computing



(a) Trajectories (b) The variance map of node 3 (c) Convergence of FDI detection (d) Distribution of estimation errors

Fig. 6. The case of FDI + high probability of connections ($\lambda = 0.01$). The secure and corrupted nodes are marked with black dots and red crosses, respectively.



(a) Trajectories (b) The variance map of node 3 (c) Convergence of FDI detection (d) Distribution of estimation errors

Fig. 7. The case of FDI + low probability of connections ($\lambda = 0.1$). The secure and corrupted nodes are marked with black dots and red crosses, respectively.

paths and neighbour sets, the priors used in local Bayesian updates diverge and become intractable.

To address this issue, we propose the following solution for dynamically weighting the data and prior. Note that although the number of secure neighbours differs from node to node and varies according to the time, but in the long run, each node has its average number of neighbours (degree), especially when the mobile network stabilize at locations with maximum information gains (illustrated by the examples and simulations in following sections). Therefore, we use the average degree of a node as the increased weight for its local data likelihood,

$$p(\boldsymbol{y}_{i,t} \mid \boldsymbol{x}_t)^{1+\beta\mathbb{E}[|N_t^*(i)|]}, \tag{44}$$

where $\mathbb{E}[|N_t^*(i)|]$ is the time-averaged number of secure neighbours for node i up to the current time t, and $0 \leq \beta \leq 1$ is the linear coefficient which can be tuned based on the topology of the network. For the linear measurement equation in (2), $\boldsymbol{y}_{i,t}$ is an affine transformation of $\boldsymbol{x}_t$. In this case, increasing the weight of the data likelihood is equivalent to shrinking $\boldsymbol{y}_{i,t}$'s variance $(\boldsymbol{H}_i\boldsymbol{\Sigma}_{i,t}^{-}\boldsymbol{H}_i^{\top}+\boldsymbol{\Sigma}_{\boldsymbol{e}_i})$ by $\frac{1}{1+\beta\mathbb{E}[|N_t^*(i)|]}$, or increasing the Kalman gain by $1+\beta\mathbb{E}[|N_t^*(i)|]$.

In summary, for node i, given the previous information fusion result $p_i^{+}(\boldsymbol{x}_t)$ and the latest measurements $\boldsymbol{y}_{i,t}$, the integrated secure information fusion solution is presented in Algorithm 2.

6 Simulation

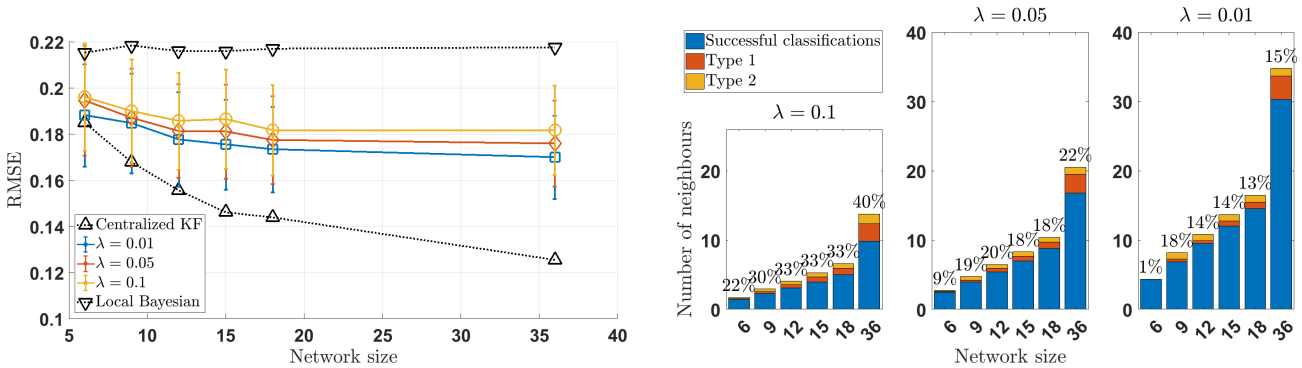
In this section, we present an application of the proposed solution for monitoring the spatial-temporal signals in a distributed vehicular sensor network. An example of such scenario is monitoring the dynamic of air and sound pollution in urban environment with sensors based on unmanned ground or aerial vehicular systems [43].

Consider a two-dimensional space spanned by a set of coordinates $\{\boldsymbol{s}_m = (s_m^1, s_m^2) \mid s_m^1 \in \{1\ldots30\}, s_m^2 \in \{1\ldots30\}\}$, and $\boldsymbol{x}_t \in \mathbb{R}^M$ as the vectorized target spatial-temporal signal, where $M = 30^2 = 900$. The temporal dynamic of $\boldsymbol{x}_t$ is modelled by the linear equation of (1), where $\boldsymbol{A} = 0.9\boldsymbol{I}_M$ is a diagonal matrix. The spatial dynamic of $\boldsymbol{x}_t$ is encoded in the covariance function of the input $\boldsymbol{w}_t$: $\mathrm{cov}(\boldsymbol{w}_{\boldsymbol{s}_m,t}, \boldsymbol{w}_{\boldsymbol{s}'_m,t}) = \alpha^2\exp(\frac{-||\boldsymbol{s}_m-\boldsymbol{s}'_m||_2}{\theta^2})$, which indicates that the spatial covariance decreases exponentially according to the Euclidean distance. In this example, the hyper-parameters are set to $\alpha = 0.1$ and $\theta = 0.01$.

A networked vehicular sensing system of N nodes is deployed in the field to continuously monitor $\boldsymbol{x}_t$, with probabilistic communication channels between each pair of nodes in the network. The communication successful rate decreases exponentially according to the Euclidean spatial distance between a pair of nodes (rate $= \exp(-\lambda||\boldsymbol{s}_m - \boldsymbol{s}'_m||_2)$), where λ is the decay rate representing the connectivity of networks. The number of nodes under FDI attacks is fixed to one third of the total number of nodes in the network. The task for each node is to identify the neighbours under

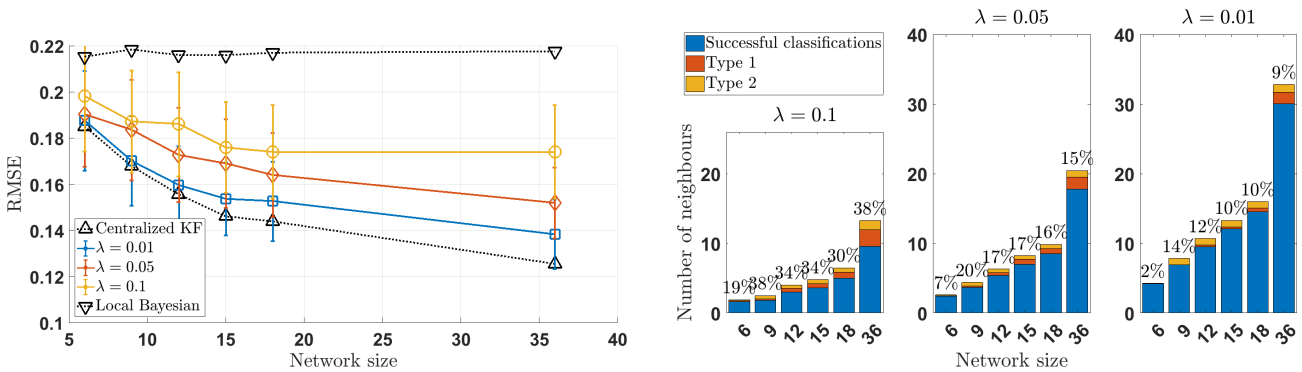
1536-1233 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: Uppsala Universitetsbibliotek. Downloaded on May 07,2020 at 09:42:47 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2020.2969352, IEEE Transactions on Mobile Computing



(a) The average RMSE (b) The percentage of classification errors

Fig. 8. Simulation results with non-weighted prior.



(a) The average RMSE (b) The percentage of classification errors

Fig. 9. Simulation results with dynamically weighted prior.

FDI attacks, and perform secure information fusion. After obtaining the latest estimation of the signal by fusing the information from secure neighbours, each vehicular sensor moves to a new location according to the maximum information gain principle [44].

6.1 An illustrative example

We first present an example of a small scale network with 6 nodes. Among them, 2 nodes are under FDI attack with $\sigma_{\boldsymbol{v}}^2/\sigma_{\boldsymbol{e}}^2 = 10$ dB. The network is deployed in the field to monitor $x(t)$ for $t = 1, \ldots, 500$. In particular, we focus on two performance metrics during the simulation: the number of detection errors and the root mean square error (RMSE), both averaged over the secure subset of the network. In the FDI detection problem, there are two types of detection errors. **Type 1 errors**, or false positive errors, are the errors that nodes are in fact secure but misclassified as under FDI attack. On the other hand, **Type 2 errors**, or false negative errors, are the errors are in fact under FDI attack but misclassified as secure.

The case of FDI + high probability of connections

Figure 6 illustrates the simulation results under only FDI attack with strong connectivity. The network is initialized at random locations within the field. After 500 iterations, the four secure nodes stabilized at the locations which approximately formulate a centroidal Voronoi tessellation (CVT) of the field, by following the paths of maximum information gain (Figure 6(a)). At $t = 500$, node i successfully establishes communication links with all of the rest network, which returns low estimation variances (or high certainty) around the locations of 4 secure nodes (Figure 6(b)). Note that although the 2 corrupted nodes are also connected to node 3, their local posteriors are excluded and contribute no reduction of variances, as node 3 successful detect the FDI attacks. The average number of Type 1 & 2 errors, and the average number of neighbours are plotted in Figure 6(c). With $\lambda = 0.01$, the network remains as almost a complete graph over the entire simulation time. This strong connected network enjoys fast detection of FDI attacks: the Type 2 error converges to zero within less than 100 simulation time. Finally, the empirical cumulative probability function (CDF) of estimation RMSE is plotted in Figure 6(d). The CDF of RMSE given by the centralized and local KFs are also plotted, serving as the optimal bound and the worst case of estimation performance. It can be observed that the proposed secure information fusion solution returns RMSEs which are very close to the optimal results given by the centralized KF.

The case of FDI + low probability of connections

Figure 7 illustrates the simulation results under FDI attack and low probability of connections. Under the low probability of connections (λ increases from 0.01 to 0.1), the probability of successfully establishing a communication link between a pair of nodes is significantly reduced.

1536-1233 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: Uppsala Universitetsbibliotek. Downloaded on May 07,2020 at 09:42:47 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2020.2969352, IEEE Transactions on Mobile Computing

Consequently, the secure nodes become less stable in terms of their locations. They intend to orbit the centre of field (Figure 7(a)). The variance map of node i at $t = 500$ is illustrated in Figure 7(b). Comparing to the high probability of connections case, the upper left secure node is disconnected from node 3, leading to higher estimation variance around the upper left area. Furthermore, the reduced averaged number of neighbours leads to larger number of Type 1 & 2 errors and slower convergence rate. As it is shown in Figure 7(d), the Type 1 & 2 errors converge to zero around $t = 200$, which takes double simulation time comparing to the high probability of connections. Finally, in Figure 7(d), the RMSE given by the local KF is slightly improved comparing to its counterpart in Figure 6(d), due to the fact that nodes orbit in the field and have higher information gain individually. However, after performing information fusion, the estimation performance of the central KF and the consensus methods degrade comparing to the high probability of connections case. And the gap between CDFs of RMSEs given by the KF and the consensus methods increases, due to the consensus is formulated based on less number of neighbours.

6.2 Simulation results

Next we investigate the impact of network connectivity levels (weak, median, and high) and the effectiveness of the dynamically weighted prior on the secure information fusion by carrying out Monte Carlo simulations. The configuration is similar to the illustrative example, except the ratio between the variance of injected data and the variance of the sensor noise is set to 5 dB, which makes it even harder to detect the FDI attacks. The network size varies from $N = 6$ to 18. Again, we are interested in two performance metrics, the RMSE of estimation and the number of errors in detection. The simulation results with non-weighted prior are shown in Figure 8; and the results with dynamically weighted prior are shown in Figure 9.

The impact of network connectivity

In both Figures 8(a) and 9(a), the performance of local Bayesian is shown as the RMSE upper bound, which is the worst case scenario when all nodes solely depend on their local posterior and no information fusion is carried out; and the performance of a centralized KF is shown as the optimal RMSE lower bound, which requires the simultaneous access of all sensor's data and is therefore unrealistic in the distributed system. Under the different level of network connectivity, the performances of the proposed secure information fusion solution are between the centralized KF and the local Bayesian filter. The better network connectivity is provided, the lower RMSE is achieved.

The detection errors and their percentage in the average number of neighbours are shown in Figures 8(b) and 9(b). Several observations are remarked here. First, the average number of neighbours increases as the network size grows (higher density within the fixed field area) and the network connectivity improves (from $\lambda = 0.1$ to 0.01). Second, more important, the percentages of the detection errors (type 1 & 2 combined) in the number of neighbours are more or less stable as the network size increases, but notably reduced when the connectivity is improved. This phenomenon shows the importance of communication in the distributed FDI attack detection problem. In other words, when a node receives larger number of local posteriors, it is able to establish the average divergence matrix with faster convergence speed, and therefore detect the FDI attack with less number of misclassification.

The effectiveness of dynamically weighted likelihoods and priors

Finally, we validate the effectiveness of dynamically weighted likelihoods and priors by comparing results in Figures 8 and 9.

In terms of RMSE, when the prior is not properly weighted, we notice that there is a large cap (≈ 0.04) between the centralized KF and the consensus formulation, even when the network is highly connected ($\lambda = 0.01$). However, with the dynamically weighted priors, the gap between the centralized KF and the consensus formulation is significantly reduced (≈ 0.01). In other words, by increasing the Kalman gain of local measurement and eliminating the double-counted prior, the performance of consensus formulation is much closer to the centralized KF. This comparison also highlights the importance of our theoretical analysis in Section 5.2: without realizing the risk of double-counting the prior, the performance gain of increasing network size from 6 to 18 or improving the network connectivity from $\lambda = 0.1$ to 0.01 is limited; only when the data likelihoods and priors are properly weighted, the consensus formulation can achieve satisfying performance in mobile and distributed systems.

7 Conclusions and Future Work

In this work, we present a secure information fusion solution for the distributed CPS under FDIA with probabilistic communications. The proposed solution relies on the exchange of local posteriors instead of raw sensor measurements. In the FDIA detection step, a detector is designed based on the average symmetrised KLDs between a pair of local posteriors. We derive the approximated distribution of the symmetrised KLDs and analyse the expected error rate. In the information fusion step, we proposed a KLD-based consensus formulation with dynamically weighted common priors and local data likelihoods. The proposed solution is applied to spatial-temporal signal monitoring problem with a mobile sensor network, and the results show promising FDIA detection and estimation accuracy. For the future work, it is interesting to investigate the smart attacking schemes toward the proposed detector in a fully distribution system with probabilistic communications.

References

[1] F. Gustafsson, *Statistical sensor fusion*, 3rd ed. Lund: Studentlitteratur, 2018.

[2] B. Khaleghi, A. Khamis, F. O. Karray, and S. N. Razavi, "Multisensor data fusion: A review of the state-of-the-art," *Information Fusion*, vol. 14, no. 1, pp. 28 – 44, 2013.

[3] Q. D. Ho, Y. Gao, and T. Le-Ngoc, "Challenges and research opportunities in wireless communication networks for smart grid," *IEEE Wireless Communications*, vol. 20, no. 3, pp. 89–95, June 2013.

1536-1233 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: Uppsala Universitetsbibliotek. Downloaded on May 07,2020 at 09:42:47 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2020.2969352, IEEE Transactions on Mobile Computing

[4] K. Golestan, R. Soua, F. Karray, and M. S. Kamel, "Situation awareness within the context of connected cars: A comprehensive review and recent trends," *Information Fusion*, vol. 29, pp. 68 – 83, 2016.

[5] J. Wang, C. Jiang, K. Zhang, T. Q. S. Quek, Y. Ren, and L. Hanzo, "Vehicular sensing networks in a smart city: Principles, technologies and applications," *IEEE Wireless Communications*, vol. 25, no. 1, pp. 122–132, February 2018.

[6] F. Alam, R. Mehmood, I. Katib, N. N. Albogami, and A. Albeshri, "Data fusion and iot for smart ubiquitous environments: A survey," *IEEE Access*, vol. 5, pp. 9533–9554, 2017.

[7] R. Gravina, P. Alinia, H. Ghasemzadeh, and G. Fortino, "Multi-sensor fusion in body sensor networks: State-of-the-art and research challenges," *Information Fusion*, vol. 35, pp. 68 – 80, 2017.

[8] A. A. Cárdenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *2008 The 28th International Conference on Distributed Computing Systems Workshops*, June 2008, pp. 495–500.

[9] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *Proceedings of the 52Nd Annual Design Automation Conference*, ser. DAC '15. New York, NY, USA: ACM, 2015, pp. 54:1–54:6. [Online]. Available: http://doi.acm.org/10.1145/2744769.2747942

[10] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," in *49th IEEE Conference on Decision and Control (CDC)*, Dec 2010, pp. 5967–5972.

[11] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 13:1–13:33, Jun. 2011.

[12] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in ac state estimation," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2476–2483, Sept 2015.

[13] J. J. Q. Yu, Y. Hou, and V. O. K. Li, "Online false data injection attack detection with wavelet transform and deep neural networks," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2018.

[14] T. M. Cover and J. A. Thomas, *Elements of information theory*. New York: Wiley, 1991.

[15] L. Schenato, B. Sinopoli, M. Franceschetti, K. Poolla, and S. S. Sastry, "Foundations of control and estimation over lossy networks," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 163–187, Jan 2007.

[16] Q. Yan, M. Li, T. Jiang, W. Lou, and Y. T. Hou, "Vulnerability and protection for distributed consensus-based spectrum sensing in cognitive radio networks," in *2012 Proceedings IEEE INFOCOM*, March 2012, pp. 900–908.

[17] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "Distributed fault detection and isolation resilient to network model uncertainties," *IEEE Transactions on Cybernetics*, vol. 44, no. 11, pp. 2024–2037, Nov 2014.

[18] Y. Guan and X. Ge, "Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 48–59, March 2018.

[19] M. Cetin, L. Chen, J. W. Fisher, A. T. Ihler, R. L. Moses, M. J. Wainwright, and A. S. Willsky, "Distributed fusion in sensor networks," *IEEE Signal Processing Magazine*, vol. 23, no. 4, pp. 42–55, July 2006.

[20] R. Olfati-Saber, "Distributed kalman filtering for sensor networks," in *2007 46th IEEE Conference on Decision and Control*, Dec 2007, pp. 5492–5498.

[21] ——, "Kalman-consensus filter : Optimality, stability, and performance," in *Proceedings of the 48h IEEE Conference on Decision and Control (CDC) held jointly with 2009 28th Chinese Control Conference*, Dec 2009, pp. 7036–7042.

[22] S. Särkkä, *Bayesian Filtering and Smoothing*. New York, NY, USA: Cambridge University Press, 2013.

[23] S.-i. Amari, *Information Geometry and Its Applications*, 1st ed. Tokyo: Springer Japan, 2016, vol. 194.

[24] M. Afgani, S. Sinanovic, and H. Haas, "Anomaly detection using the kullback-leibler divergence metric," in *2008 First International Symposium on Applied Sciences on Biomedical and Communication Technologies*. IEEE, 2008, pp. 1–5.

[25] J. Harmouche, C. Delpha, and D. Diallo, "Incipient fault detection and diagnosis based on kullback–leibler divergence using principal component analysis: Part i," *Signal Processing*, vol. 94, pp. 278–287, 2014.

[26] J. Zeng, U. Kruger, J. Geluk, X. Wang, and L. Xie, "Detecting abnormal situations using the kullback–leibler divergence," *Automatica*, vol. 50, no. 11, pp. 2777–2786, 2014.

[27] A. Anderson and H. Haas, "Kullback-leibler divergence (kld) based anomaly detection and monotonic sequence analysis," in *2011 IEEE Vehicular Technology Conference (VTC Fall)*. IEEE, 2011, pp. 1–5.

[28] A. Youssef, C. Delpha, and D. Diallo, "An optimal fault detection threshold for early detection using kullbackleibler divergence for unknown distribution data," *Signal Processing*, vol. 120, pp. 266 – 279, 2016.

[29] J. A. Hage, M. E. E. Najjar, and D. Pomorski, "Multi-sensor fusion approach with fault detection and exclusion based on the kullbackleibler divergence: Application on collaborative multi-robot system," *Information Fusion*, vol. 37, pp. 61 – 76, 2017.

[30] Z. Guo, D. Shi, K. H. Johansson, and L. Shi, "Worst-case stealthy innovation-based linear attack on remote state estimation," *Automatica*, vol. 89, pp. 117–124, 2018.

[31] D. I. Belov and R. D. Armstrong, "Distributions of the kullback–leibler divergence with applications," *British Journal of Mathematical and Statistical Psychology*, vol. 64, no. 2, pp. 291–309, 2011.

[32] G. Battistelli and L. Chisci, "Kullback-leibler average, consensus on probability densities, and distributed state estimation with guaranteed stability," *Automatica*, vol. 50, no. 3, pp. 707–718, Mar. 2014.

[33] G. Battistelli, L. Chisci, C. Fantacci, A. Farina, and B.-N. Vo, "Average kullback-leibler divergence for random finite sets," in *2015 18th International Conference on Information Fusion (Fusion)*. IEEE, 2015, pp. 1359–1366.

[34] K. Da, T. Li, Y. Zhu, H. Fan, and Q. Fu, "Kullback-leibler averaging for multitarget density fusion," in *International Symposium on Distributed Computing and Artificial Intelligence*. Springer, 2019, pp. 253–261.

[35] N. Forti, G. Battistelli, L. Chisci, S. Li, B. Wang, and B. Sinopoli, "Distributed joint attack detection and secure state estimation," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 96–110, March 2018.

[36] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, July 2017.

[37] M. S. Arulampalam, S. Maskell, N. Gordon, and T. Clapp, "A tutorial on particle filters for online nonlinear/non-gaussian bayesian tracking," *IEEE Transactions on signal processing*, vol. 50, no. 2, pp. 174–188, 2002.

[38] D. Müllner, "fastcluster: Fast Hierarchical, Agglomerative Clustering Routines for R and Python," *Journal of Statistical Software*, vol. 53, no. i09, 2013.

[39] J.-P. Imhof, "Computing the distribution of quadratic forms in normal variables," *Biometrika*, vol. 48, no. 3/4, pp. 419–426, 1961.

[40] H. Liu, Y. Tang, and H. H. Zhang, "A new chi-square approximation to the distribution of non-negative definite quadratic forms in non-central normal variables," *Computational Statistics & Data Analysis*, vol. 53, no. 4, pp. 853 – 856, 2009.

[41] P. G. Bissiri, C. C. Holmes, and S. G. Walker, "A general framework for updating belief distributions," *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, vol. 78, no. 5, pp. 1103–1130, 2016.

[42] D. Zachariah, S. Dwivedi, P. Händel, and P. Stoica, "Scalable and passive wireless network clock synchronization in los environments," *IEEE Transactions on Wireless Communications*, vol. 16, no. 6, pp. 3536–3546, June 2017.

[43] X. Liu, T. Xi, E. Ngai, and W. Wang, "Path planning for aerial sensor networks with connectivity constraints," in *2017 IEEE International Conference on Communications (ICC)*, May 2017, pp. 1–6.

[44] A. Krause, A. Singh, and C. Guestrin, "Near-optimal sensor placements in gaussian processes: Theory, efficient algorithms and empirical studies," *J. Mach. Learn. Res.*, vol. 9, pp. 235–284, Jun. 2008.

1536-1233 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: Uppsala Universitetsbibliotek. Downloaded on May 07,2020 at 09:42:47 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2020.2969352, IEEE Transactions on Mobile Computing

Xiuming Liu is a Ph.D. student in Department of Information Technology, Uppsala University, Sweden. He received the BEng degree from Beijing Jiaotong University, Beijing, China, in 2013, and the Master of Science degree from Royal Institute of Technology (KTH), Stockholm, Sweden, in 2014, both in electrical engineering. His research interests include statistical signal processing, machine learning, and networked systems. Xiuming is a student member of IEEE.

Edith C.-H. Ngai is currently an Associate Professor in Department of Information Technology, Uppsala University, Sweden. She received her PhD from The Chinese University of Hong Kong in 2007. She was a post-doc in Imperial College London, United Kingdom in 2007-2008. Her research interests include Internet-of-Things, mobile crowdsourcing, data analytics and urban computing, security and privacy. She was a guest researcher at Ericsson Research Sweden in 2015-2017. She has also been a visiting researcher in Simon Fraser University, Tsinghua University, and UCLA. Edith was a VINNMER Fellow (2009) awarded by Swedish Governmental Research Funding Agency VINNOVA. She have served as TPC members in many international conferences, including IEEE ICC, IEEE ICDCS, IEEE Infocom, IEEE Globecom, IEEE/ACM IWQoS, IEEE CloudCom, etc. She was a program chair of ACM womENcourage 2015, TPC co-chair of IEEE SmartCity 2015, IEEE ISSNIP 2015, and ICNC 2018 Network Algorithm and Performance Evaluation Symposium. She is currently an Associate Editor of IEEE Access, IEEE Internet of Things Journal, and IEEE Transactions of Industrial Informatics. Edith is a Senior Member of ACM and IEEE.

Jiangchuan Liu (S'01-M'03-SM'08-F'17) is a University Professor in the Schoolof Computing Science, Simon Fraser University, British Columbia, Canada. He is a Fellow of Canadian Academy of Engineering, an IEEE Fellow and an NSERC E.W.R. Steacie Memorial Fellow. He is an EMC-Endowed Visiting Chair Professor of Tsinghua University, Beijing, China and an Adjunct Professor of Tsinghua Shenzhen Graduate School.

He received the BEng degree (cum laude) from Tsinghua University, Beijing, China, in 1999, and the PhD degree from The Hong Kong University of Science and Technology in 2003, both in computer science. He is a co-recipient of the inaugural Test of Time Paper Award of IEEE INFOCOM (2015), ACM SIGMM TOMCCAP Nicolas D. Georganas Best Paper Award (2013), and ACM Multimedia Best Paper Award (2012).

His research interests include multimedia systems and networks, cloud computing, social networking, online gaming, big data computing, RFID, and Internet of things. He has served on the editorial boards of IEEE/ACM Transactions on Networking, IEEE Transactions on Big Data, IEEE Transactions on Multimedia, IEEE Communications Surveys and Tutorials, and IEEE Internet of Things Journal. He is a Steering Committee member of IEEE Transactions on Mobile Computing and Steering Committee Chair of IEEE/ACM IWQoS (2015-2017).

1536-1233 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: Uppsala Universitetsbibliotek. Downloaded on May 07,2020 at 09:42:47 UTC from IEEE Xplore. Restrictions apply.