Digital Signal Processing ••• (••••) •••–•••

Contents lists available at ScienceDirect

Digital Signal Processing

www.elsevier.com/locate/dsp

Distributed Kalman filtering for robust state estimation over wireless sensor networks under malicious cyber attacks

Fuxi Wen [a,c,*], Zhongmin Wang [b,c]

[a] Department of Electrical Engineering, Chalmers University of Technology, SE-412 96, Göteborg, Sweden
[b] School of Computer Science and Technology, Xi'an University of Posts and Telecommunications, Xi'an, Shaanxi 710121, China
[c] Shaanxi Key Laboratory of Network Data Analysis and Intelligent Processing, Xi'an University of Posts and Telecommunications, Xi'an, Shaanxi 710121, China

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Distributed Kalman filtering
Wireless sensor networks
Cyber attacks
Secured nodes
Clustering

ABSTRACT

We consider distributed Kalman filtering for dynamic state estimation over wireless sensor networks. It is promising but challenging when network is under cyber attacks. The compromised nodes are likely to influence system security by broadcasting malicious false measurements or estimates to their neighbors, and result in performance deterioration. To increase network resilience to cyber attacks, in this paper, trust-based dynamic combination strategy is developed. The proposed distributed Kalman filtering scheme is resilient to random, false data injection and replay attacks. Furthermore, it is efficient in terms of communication load, only instantaneous estimates are exchanged between the neighboring nodes and compromised nodes localization is a byproduct.

1. Introduction

Kalman filter [1] is one of the widely used techniques in information fusion [2,3]. To process information over wireless sensor networks (WSN), the emerging distributed Kalman filtering has received great attentions [4–8]. For decentralized sensor networks, cross-correlations of the estimates between the agents are usually unknown. To fuse with unknown correlations, covariance intersection (CI) algorithms are proposed in [9–13]. However, well designed malicious attacks can make CI algorithms invalidate. Because information is exchanged between the neighboring nodes, such a scheme naturally has some potential risks. Once a node or communication link is compromised with false data, then the hostile bias might be broadcast to the whole network.

Security issue has been a big obstacle to the applications of WSN due to its vulnerabilities to various types of potential hostile attacks [14]. As pointed out in [15], few studies have been directed to distributed state estimation with cyber attacks. To solve the security problem, centralized Kalman filtering combined with χ^2- or Euclidean detectors are proposed in [16] to deal with attacks, such as denial-of-service (DoS), random and false data injection (FDI) [17]. In spite of these preliminary efforts, the security aspect of information fusion is still largely unexplored especially for distributed processing over WSN. A successful attack could cause the collapse of the network, therefore, integrating security is an essential component for distributed data fusion techniques [18]. To deal with cyber attacks, efficient majority voting based schemes are proposed in [19]. However, it is invalidate when more than half of the sensors are compromised. Another promising scheme is introducing a subset of secured nodes into the network. The secured nodes can provide highly trusted measurements or estimates. As long as there is a path connected to a secured node, the attacker cannot succeed even when most of the sensors are compromised [20].

To handle the challenging scenarios, such as more than half of the nodes are compromised, WSN with secured nodes is considered. In this paper, we propose a clustering-based distributed Kalman filtering approach and it is resilient to different type of cyber attacks. Furthermore, because communication usually consumes more energy than computation [21], to reduce communication load and energy consumption, only local estimates are exchanged within the neighboring nodes. Our contributions are summarized as follows:

- Different from [20,19], both the estimated states and error covariance matrices are exchanged between the neighboring nodes. Since attackers can compromise mean and/or variance of the states independently. To increase attack tolerance of the proposed approach, two different combiners are applied on the estimated mean and variance. The combiners are obtained independently but in a similar manner.

* Corresponding author at: Department of Electrical Engineering, Chalmers University of Technology, SE-412 96, Göteborg, Sweden.
E-mail address: wenfuxi@hotmail.com (F. Wen).

https://doi.org/10.1016/j.dsp.2018.03.002
1051-2004/

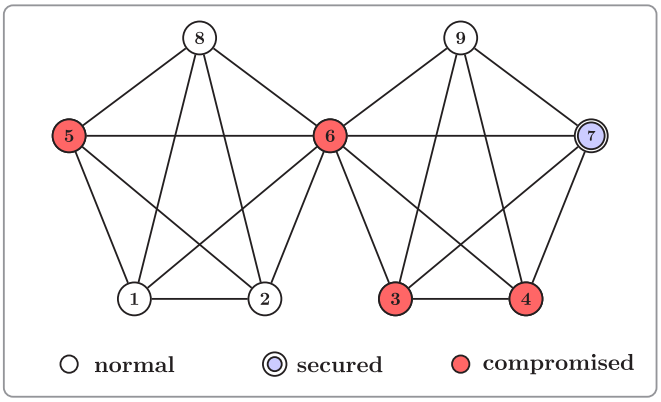

Fig. 1. Each node runs a local Kalman filtering and information is exchanged between the neighboring nodes. The WSN is consisted of normal, secured and compromised nodes.

- K-means algorithm is applied to classify the local estimates, because it is one of the simplest unsupervised learning algorithms to solve the clustering problem [22]. The cluster contains the estimates from the secured nodes are considered as the trusted estimates. For simplicity, after ignoring the untrusted estimates, uniform weights are utilized to fuse the trusted estimates. While K-means clustering can't handle non-convex data sets. Other well-developed clustering and weighting techniques can be applied to further improve the performance.
- As a demonstration, distributed target tracking is considered, meanwhile, it can be applied to other applications, such as distributed power system state estimation in smart grids. Furthermore, unreliable or compromised nodes localization is a byproduct of the proposed approach.

The rest of the paper is organized as follows. In Section 2, problem formulation and background introduction are provided. In Section 3, the proposed clustering-based distributed Kalman filtering approach is introduced. Numerical results are given in Section 4. Finally, we conclude the paper in Section 6.

2. Problem formulation

At time t, system state vector $\boldsymbol{x}_t$ evolved according to the following equation,

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

where $\mathbf{A}_t$ is the state transition matrix and $\boldsymbol{w}_t \sim \mathcal{N}(\mathbf{0}, \mathbf{Q}_t)$ is the Gaussian process noise.

For node k, system measurement at time t is given by

$$\boldsymbol{y}_{k,t} = \mathbf{H}_{k,t} \boldsymbol{x}_t + \boldsymbol{v}_{k,t}, \tag{2}$$

where $\mathbf{H}_{k,t}$ is the transformation or measurement matrix, and $\boldsymbol{v}_{k,t} \sim \mathcal{N}(\mathbf{0}, \mathbf{R}_{k,t})$ is the Gaussian measurement noise.

As shown in Fig. 1, distributed Kalman filtering in WSN with normal, secured and compromised nodes is considered. Inaccurate or false estimates are broadcast by these compromised nodes.

As a demonstration, the following three cyber attacks are considered:

1. *Random Attack:* The attacker simply manipulates the observations with random attack vectors. The attacks can be launched at any time point and could be a long-term continuous attack or a short-term intermittent attack.
2. *False Data Injection Attack:* With measurement matrix available, the adversary can bypass the existing bad data detection schemes and introduce arbitrary errors to state estimation without being detected.
3. *Replay Attack:* To deceive the system, the attacker replays a previous snapshot of a valid communication packet sequence that contains measurements.

3. Clustering based distributed Kalman filtering

Let $\boldsymbol{x}_{k,i|j}$ be the linear minimum mean square error estimate of $\boldsymbol{x}_i$ at node k given observations up to and including time j. And $\mathbf{P}_{k,i|j}$ denotes the covariance matrix of the estimation error, which is defined as

$$\hat{\boldsymbol{x}}_{k,i|j} \triangleq \boldsymbol{x}_i - \boldsymbol{x}_{k,i|j}. \tag{3}$$

Kalman filter starts from prior mean $\boldsymbol{x}_{k,0|-1}$ and covariance $\mathbf{P}_{k,0|-1}$ [8,3].

3.1. Measurement update

With previous mean $\boldsymbol{x}_{k,t|t-1}$ and covariance $\mathbf{P}_{k,t|t-1}$ available, the state is updated as

$$\boldsymbol{x}_{k,t|t} = \boldsymbol{x}_{k,t|t-1} + \mathbf{P}_{k,t|t-1}\mathbf{H}_{k,t}^{*}\mathbf{G}_{k,t}^{-1}\boldsymbol{r}_{k,t}, \tag{4}$$

where

$$\mathbf{G}_{k,t} = \mathbf{R}_{k,t} + \mathbf{H}_{k,t}\mathbf{P}_{k,t|t-1}\mathbf{H}_{k,t}^{*}, \tag{5}$$

$$\boldsymbol{r}_{k,t} = \boldsymbol{y}_{k,t} - \mathbf{H}_{k,t}\boldsymbol{x}_{k,t|t-1} \tag{6}$$

and * denotes conjugate transposition. The covariance is updated as

$$\mathbf{P}_{k,t|t} = \mathbf{P}_{k,t|t-1} - \mathbf{P}_{k,t|t-1}\mathbf{H}_{k,t}^{*}\mathbf{G}_{k,t}^{-1}\mathbf{H}_{k,t}\mathbf{P}_{k,t|t-1}. \tag{7}$$

For node k, $\boldsymbol{x}_{k,t|t}$ and $\mathbf{P}_{k,t|t}$ are exchanged with nodes $\ell \in \mathcal{N}_k$.

3.2. Clustering based information fusion

Combiner plays a critical role for information fusion and it influences the performance of the whole network. Generally speaking, larger weights should be assigned to nodes with reliable and accurate local estimates. Since the adaptation is achieved by using information locally available at every nodes, accessing to global information is not required. The burden of communication is reduced, because it consumes the main energy of the nodes [23].

3.2.1. State clustering

For node k, our objective is to put the n_k available estimates $\{\boldsymbol{x}_{\ell,t|t}, \ell \in \mathcal{N}_k\}$ into two clusters, which are parameterized by mean vectors $\boldsymbol{x}_k^{(g)}$, $g = 1, 2$. In this paper, squared Euclidean distance is used to measure the distance between two vectors $\boldsymbol{z}_i$ and $\boldsymbol{z}_j$,

$$d(\boldsymbol{z}_i, \boldsymbol{z}_j) = \left\| \boldsymbol{z}_i - \boldsymbol{z}_j \right\|_2^2, \tag{8}$$

where $\|\cdot\|_2$ denotes ℓ_2-norm. The clustering technique we used is an iterative two-step algorithm.

Assignment step Means $\boldsymbol{x}_k^{(1)}$ and $\boldsymbol{x}_k^{(2)}$ are initialized to random values. Estimated state $\boldsymbol{x}_{\ell,t|t}$, $\ell \in \mathcal{N}_k$, is assigned to cluster g, if

$$g = \arg\min_j \left\{ d\left(\boldsymbol{x}_k^{(j)}, \boldsymbol{x}_{\ell,t|t}\right) \right\}, \text{ for } j = 1, 2. \tag{9}$$

Let $r_\ell^{(g)}$ be the indicator to describe the assignment, we set $r_\ell^{(g)} = 1$, if mean $\boldsymbol{x}_k^{(g)}$ is the closest mean to $\boldsymbol{x}_{\ell,t|t}$, otherwise $r_\ell^{(g)} = 0$.

Please cite this article in press as: F. Wen, Z. Wang, Distributed Kalman filtering for robust state estimation over wireless sensor networks under malicious cyber attacks, Digit. Signal Process. (2018), https://doi.org/10.1016/j.dsp.2018.03.002