Trust-Based Distributed Kalman Filtering for Target Tracking under Malicious Cyber Attacks

Citation for the original published paper (version of record):
Liang, C., Wen, F., Wang, Z. (2019)
Trust-Based Distributed Kalman Filtering for Target Tracking under Malicious Cyber Attacks
Information Fusion, 46: 44-50
http://dx.doi.org/10.1016/j.inffus.2018.04.002

Trust-Based Distributed Kalman Filtering for Target Tracking under Malicious Cyber Attacks

Chen Liang[a], Fuxi Wen[b,*], Zhongmin Wang[a]

[a] *School of Computer Science & Technology, Xi'an University of Posts & Telecommunications, China*
[b] *Department of Electrical Engineering, Chalmers University of Technology, Sweden*

Abstract

As one of the widely used applications in wireless sensor networks, target tracking has attracted considerable attention. Although many tracking techniques have been developed, it is still a challenging problem if the network is under cyber attacks. Inaccurate or false information is maliciously broadcast by the compromised nodes to their neighbors. They are likely to threaten the security of the system and result in performance deterioration. In this paper, a distributed Kalman filtering technique with trust-based dynamic combination strategy is developed to improve resilience against cyber attacks. Furthermore, it is efficient in terms of communication load, only local instantaneous estimates are exchanged with the neighboring nodes. Numerical results are provided to evaluate the performance of the proposed approach by considering random, false data injection and replay attacks.

Keywords: Distributed Kalman filtering, information fusion, wireless sensor networks, cyber attack, target tracking, state estimation.

*Corresponding author.
Email addresses: mumulc@xupt.edu.cn (Chen Liang), wenfuxi@hotmail.com (Fuxi Wen), zmwang@xupt.edu.cn (Zhongmin Wang)

1. Introduction

Wireless sensor network (WSN) combines a large number of low-power and low-cost tiny sensors with limited processing and communicating resources [1, 2]. It has a wide range of applications, including collaborative target tracking [3, 4], control of unmanned aerial vehicles [5, 6], automated vehicle guidance [7, 8] and smart grids [9]. The major benefit of WSNs is that they perform in-network cooperative and distributed processing [10]. These computationally efficient distributed processing techniques are scalable with respect to network size and suitable for real-time implementation [11]. For example, system monitoring and security control for large scale power grids are challenging problems as envisioned by smart grids [12]. Therefore, distributed processing techniques are desirable to incorporate adaptability to dynamic network topologies and flexible reconfiguration for subnetwork faults [13]. Decentralized Kalman filtering is one of the fundamental information processing techniques in WSNs [14]. Due to its underlying state space model that accounts for observational noise, it has proven to be advantageous in terms of enhanced accuracy and faster convergence rates.

Information fusion plays an important role in distributed processing strategies. In general, it can be classified into four categories: signal or measurement level (low-level), feature or attributes level (medium-level), decision level (high-level) and combination of various level of information (multilevel) [15]. Here, we focus on distributed Kalman filtering algorithms in which each node only shares local estimates with its single-hop neighbors [16]. With covariance and cross-covariance information available, the linear gains mini-

mizing the mean squared error have been proposed in [17]. This information is typically known locally for distributed processing scenarios. Hence, different strategies have been exploited to deal with unknown cross-covariance matrices. Simple topology-based static techniques are proposed by ignoring the correlations. Typical static combination rules include uniform, maximum degree, metropolis, relative degree-variance or no cooperation [18, 19]. However, such static combination rules are sensitive to the variation of signal and noise statistics across the network. Alternatively, the unknown correlations can be explicitly modeled. Covariance intersection was proposed in [20] for fusion without knowing correlations. Since then, lots of variants have been proposed in [21, 22, 23, 24] and the computational complexity is further reduced in [25, 26, 27, 28]. Recently, ellipsoidal intersection is presented in [29], it provides smaller covariances than the bounds obtained with covariance intersection. In [30, 31], efficient adaptive combination schemes are developed to handle the variation of node profiles across the network. Please refer to [14] for a bibliographic review.

Most of the existing distributed Kalman filtering techniques assume that all the nodes are working properly [14]. However, WSN is a specific cyber-physical system and it poses unique security challenges [32, 33, 34, 35]. Firstly, to make networks economically viable, sensors have limited computation and communication capabilities. Secondly, sensors are often deployed in accessible areas, increasing the risks of physical attacks. Thirdly, sensor networks interact closely with environments and people, posing new security problems. Attackers may cause serious security issues to WSN by launching cyber attacks, such as random [36], false data injection (FDI) [37, 38, 39, 40]

and replay attacks [41, 42]. As mentioned in [43], very few studies have been directed to distributed state estimation under cyber attacks, where information is exchanged between neighboring nodes. Such a scheme has some potential risks of being attacked, once a node or communication link is compromised, the false data or information is diffused to the whole network.

To address these security challenges, trust-based distributed Kalman filtering approach is proposed in [44]. It is a high level fusion based technique, only local estimates are exchanged. Dynamic combiners are determined by information accuracy of the estimated covariance matrix or belief divergence of the current estimates. Recently, multi-agent filtering scheme is combined with trust-based scheme for distributed state estimation in smart grids [45]. For trust based scheme, each agent associates a trust metric to its neighbors, information from the untrusted nodes is disregarded. While one limitation of these methods is that subject judgment is required to choose the threshold. In this paper, a new trust-based distributed Kalman filtering approach is proposed, it is resilient against cyber attacks, such as random, false data injection and replay attacks. Different from [44, 45], both the estimated states and error covariance matrices are exchanged between the neighboring nodes. Because error covariance matrix provides useful information about the accuracy or uncertainty of the estimated states. Meanwhile, K-means clustering is utilized to classify the trusted and untrusted nodes, it is one of the simplest unsupervised learning algorithms to solve the clustering problem [46]. The performance of the proposed approach is evaluated in target tracking, meanwhile, it can be applied to other applications, such as distributed power system state estimation in smart grids. A brief comparison of distributed

Kalman filtering techniques under different cyber attacks is given in Table 1.

Table 1: Comparison of Distributed Kalman Filtering Techniques under Cyber Attacks

Algorithm	Fusion Level	Combiner	Random	FDI	Replay
[47]	High	Static	✗	✗	✗
[48]	High	Dynamic	✓	✗	✗
[30, 49, 50]	Low and High	Dynamic	✓	✗	✗
[18, 31]	High	Dynamic	✓	✗	✓
[44, 45]	High (state)	Dynamic	✓	✓	✓
Proposed	High (state and variance)	Dynamic	✓	✓	✓

Our contributions are summarized as follows:

- A new trust-based distributed Kalman filtering technique is proposed to enhance the resilience against cyber attacks. Different from the existing works, both local state estimate and error covariance matrix are exchanged between the neighboring nodes.

- In order to bypass the bad data detection techniques utilized by the defender, attacker may compromise state and error covariance matrix independently. To enhance the attack resilience of the proposed approach, for each node, the combiners for state and covariance matrix are calculated independently.

- Communication load of the proposed approach is lower than that of the low level measurement fusion scheme. Furthermore, compromised nodes detection and localization are byproducts of the proposed approach. Besides distributed Kalman filtering, the proposed fusion strategy can be applied to other distributed filtering techniques.

The rest of the paper is organized as follows. In Section 2, problem formulation and preliminaries about Kalman filtering are provided. In Section 3, the proposed trust-based Kalman filtering for distributed estimation over WSN is introduced. Numerical results are given in Section 4. Finally, the paper is concluded in Section 5.

2. Problem Formulation

The Kalman filter model assumes that the current system state $\boldsymbol{x}_t$ evolved from the prior state $\boldsymbol{x}_{t-1}$ according to the following equation:

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

where $\boldsymbol{x}_t$ is the system state vector at time t, $\mathbf{A}_t$ is the state transition matrix and process noise $\boldsymbol{w}_t$ is zero mean multivariate normally distributed random variable with covariance $\mathbf{Q}_t$ [51]. Measurement of the system $\boldsymbol{y}_t$ is given by

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

where $\mathbf{H}_t$ is the transformation or measurement matrix and measurement noise $\boldsymbol{v}_t$ is zero mean multivariate normally distributed random variable with covariance $\mathbf{R}_t$. For distributed Kalman filter, the model is defined in a similar manner. At node k, the linear measurement equation is given by

$$\boldsymbol{y}_{k,t} = \mathbf{H}_{k,t} \boldsymbol{x}_t + \boldsymbol{v}_{k,t}, \tag{3}$$

where $\mathbf{H}_{k,t}$ is the measurement matrix and $\mathbf{R}_{k,t}$ is the covariance matrix of measurement noise $\boldsymbol{v}_{k,t}$.

As shown in Fig.1, distributed Kalman filtering based target tracking in WSN with compromised nodes is considered in this paper. Inaccurate or false estimates are broadcast by the compromised nodes. We assume that less than half of the nodes are under cyber attacks. To evaluate the performance

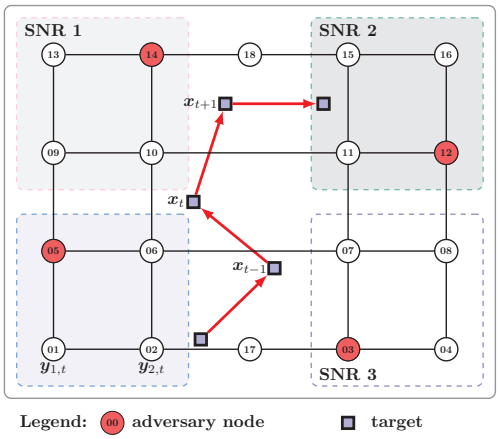

Figure 1: Target tracking in wireless sensor networks with unreliable nodes. The unreliability may be caused by noisy operational environments and/or cyber attacks.

of the proposed approach, the following cyber attacks are considered:

1. *Random Attack:* The attacker simply manipulates the sensor observations with a random attack vector. The random attack 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:* The adversary can bypass the existing bad data detection schemes and introduce arbitrary errors to system states without being detected by system operators.

3. *Replay Attack:* The attacker replays a previous snapshot of a valid communication packet sequence that contains measurements to deceive the system.

3. Trust-Based Diffusion Kalman Filtering

Distributed Kalman filter starts from prior mean $\tilde{\boldsymbol{x}}_{k,0|-1}$ and covariance $\tilde{\mathbf{P}}_{k,0|-1}$, where $\tilde{\boldsymbol{x}}_{k,i|j}$ denotes the estimate of $\boldsymbol{x}_i$ at node k given observations up to time j and $\tilde{\mathbf{P}}_{k,i|j}$ is the covariance matrix of the estimation error [49].

3.1. Measurement-Update:

Let us first define

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

where * denotes conjugate transposition. With predicted state $\tilde{\boldsymbol{x}}_{k,t|t-1}$ and covariance $\tilde{\mathbf{P}}_{k,t|t-1}$ available, the state is updated as

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

where

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

and covariance is updated as

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

Let $\mathcal{N}_k$ be the single-hop physical neighbors of node k and includes itself. State $\tilde{\boldsymbol{x}}_{k,t|t}$ and covariance $\tilde{\mathbf{P}}_{k,t|t}$ are exchanged within nodes in $\mathcal{N}_k$,

3.2. Trust-Based Information Fusion

Combiner $\boldsymbol{c}_{k,t}$ plays a critical role at information fusion stage, it even influences the performance of the whole network. In general, larger weights should be assigned to the reliable nodes with accurate local estimates. The objective is to construct the weights, that are adaptable to the variation of the estimates. The adaptation is achieved using locally available information at every node. In this sense, the algorithm is fully distributed, accessing to global information is not required. Communication burden and energy consumption of the sensors are reduced [52].

The simplest unsupervised learning algorithm K-means is used to classify the estimates into trust and untrust clusters. The proposed approach is majority voting based. Cluster with the largest number of elements is considered as the trusted set, while the other untrusted clusters are ignored. The number of clusters is required to apply K-means algorithm and it can be determined by using hierarchical maximum likelihood clustering approach [53, 54]. Because majority of the nodes are working properly, for simplicity, a suboptimal solution is considered. Two clusters are assumed to avoid estimating the actual number of clusters.

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

between two points $\boldsymbol{z}_i$ and $\boldsymbol{z}_j$, which is defined as

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

where $\|\cdot\|_2$ denotes ℓ_2-norm.

The two-step iterative clustering algorithm includes an ASSIGNMENT STEP and an UPDATE STEP. In the beginning, $\boldsymbol{m}^{(1)}$ and $\boldsymbol{m}^{(2)}$ are initialized with random values.

Assignment Step. Estimate state $\tilde{\boldsymbol{x}}_{\ell,t|t}$ is assigned to cluster g, if

$$g = \arg\min_c \left\{ d\left(\boldsymbol{m}^{(c)}, \tilde{\boldsymbol{x}}_{\ell,t|t}\right) \right\}, c = 1, 2. \tag{9}$$

Let $r_\ell^{(g)}$ be the indicator to describe the assignment of $\tilde{\boldsymbol{x}}_{\ell,t|t}$ to cluster g. In the assignment step, if mean $\boldsymbol{m}^{(g)}$ is closer to the estimate state, then $r_\ell^{(g)} = 1$, otherwise $r_\ell^{(g)} = 0$.

Update Step. To match the sample mean of the data points that have been assigned to that cluster, means are updated as fellows:

$$\boldsymbol{m}^{(c)} = \frac{\sum_\ell r_\ell^{(c)} \tilde{\boldsymbol{x}}_{\ell,t|t}}{\sum_\ell r_\ell^{(c)}}, \ell \in \mathcal{N}_k, \text{ and } c = 1, 2. \tag{10}$$

Repeat the assignment and update steps until the assignments do not change. Let $k^{(c)} = \sum_\ell r_\ell^{(c)}, \ell \in \mathcal{N}_k$ be the number of data points belongs to cluster c, and

$$g_k = \arg\max_c k^{(c)}, c = 1, 2. \tag{11}$$

Then only the data points within cluster g_k are considered as trusted estimates, the corresponding nodes are denoted as $\mathcal{C}_k$, the other untrusted nodes are ignored. Let $\text{card}(\mathcal{C}_k)$ be the cardinality of set $\mathcal{C}_k$, which measures the number of elements of the set.

The weight is computed as

$$w_{k\leftarrow l,t} = \frac{1}{\text{card}(\mathcal{C}_k)}, \text{for } l \in \mathcal{C}_k. \tag{12}$$

Let $\tilde{\boldsymbol{p}}_{k,t|t} = \text{diag}\{\tilde{\mathbf{P}}_{k,t|t}\}$, where operator $\text{diag}\{\cdot\}$ returns a column vector of the main diagonal elements of a matrix. For node k, the n_k available estimates $\{\tilde{\boldsymbol{p}}_{\ell,t|t}, \ell \in \mathcal{N}_k\}$ are put into two clusters. Let $\mathcal{D}_k$ be the trusted node set, the weight is computed as

$$\lambda_{k\leftarrow l,t} = \frac{1}{\text{card}(\mathcal{D}_k)}, \text{for } l \in \mathcal{D}_k. \tag{13}$$

Refined estimation of the state and variance are given by

$$\tilde{\boldsymbol{x}}_{k,t|t} = \sum_{l\in\mathcal{C}_k} w_{k\leftarrow l,t}\tilde{\boldsymbol{x}}_{l,t|t}, \tag{14}$$

and

$$\tilde{\mathbf{P}}_{k,t|t} = \sum_{l\in\mathcal{D}_k} \lambda_{k\leftarrow l,t}\tilde{\mathbf{P}}_{l,t|t}. \tag{15}$$

3.3. Time-Update

With $\tilde{\boldsymbol{x}}_{k,t|t}$ and $\tilde{\mathbf{P}}_{k,t|t}$, the time-updates are implemented as

$$\tilde{\boldsymbol{x}}_{k,t+1|t} = \mathbf{A}_t\tilde{\boldsymbol{x}}_{k,t|t}, \tag{16}$$

and

$$\tilde{\mathbf{P}}_{k,t+1|t} = \mathbf{A}_t \tilde{\mathbf{P}}_{k,t|t} \mathbf{A}_t^* + \mathbf{Q}_t. \tag{17}$$

The proposed trust-based distributed Kalman filtering technique is summarized in Algorithm 1.

Algorithm 1: Trust Based Distributed Kalman Filtering

Initialize $\tilde{\boldsymbol{x}}_{k,0|-1}$ and $\tilde{\mathbf{P}}_{k,0|-1}$, for $k = 1, 2, \cdots, N$.
for $t = 0$ **to** t_{max} **do**
  for $k = 1$ **to** N **do**
    `/* Measurement-Update */`
    Estimate $\tilde{\boldsymbol{x}}_{k,t|t}$ and $\tilde{\mathbf{P}}_{k,t|t}$ using (5) and (7).
  end
  for $k = 1$ **to** N **do**
    Exchange $\tilde{\boldsymbol{x}}_{l,t|t}$ and $\tilde{\mathbf{P}}_{l,t|t}$ with node k, $\ell \in \mathcal{N}_k$.
    `/* Information Fusion */`
    Compute $\boldsymbol{w}_{k,t}$ and $\boldsymbol{\lambda}_{k,t}$ using (12) and (13).
    Estimate $\tilde{\boldsymbol{x}}_{k,t|t}$ and $\tilde{\mathbf{P}}_{k,t|t}$ using (14) and (15).
    `/* Time-Update */`
    Update $\tilde{\boldsymbol{x}}_{k,t+1|t}$ and $\tilde{\mathbf{P}}_{k,t+1|t}$ using (16) and (17).
  end
end

4. Simulation Results

Computer simulations have been carried out to evaluate the performance of the proposed approach by comparing with uniform [55] and relative degree-variance [56] fusion schemes. Cyber attacks, such as random, false data

injection (FDI) and replay attacks are considered. As shown in Fig.2, a fully connected WSN with 7 nodes is considered. Nodes 02, 04 and 06 are under cyber attacks. For simplicity, we assume that both $\mathbf{A}_t$ and $\mathbf{H}_{k,t}$ are time

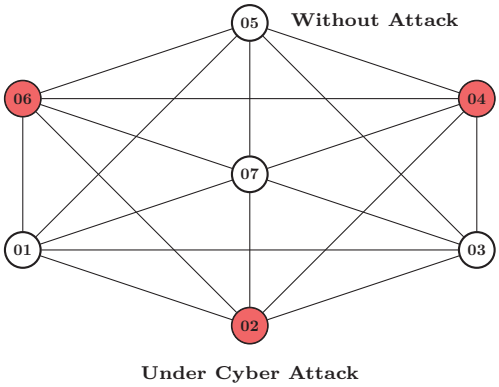

Figure 2: A WSN with 7 nodes, nodes 02, 04 and 06 are under cyber attacks.

invariant. The system parameters are as follows:

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \text{ and } \mathbf{H}_k = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}. \tag{18}$$

The states are initialized as $\tilde{\boldsymbol{x}}_{k,0|-1} = \begin{bmatrix} 10 & 10 & 1 & 0 \end{bmatrix}^T$, $\tilde{\mathbf{P}}_{k,0|-1} = 10\mathbf{I}_4$, covariance $\mathbf{Q} = 0.1\mathbf{I}_4$ and $\mathbf{R}_k = \sigma^2\mathbf{I}_2$. Here $\mathbf{I}_n$ denotes the identity matrix of size n.

4.1. Random Attack

The attacker simply manipulates the sensor measurements with a randomly generated attack vector. The attack can be launched at any point in

time. It might be a long-term continuous attack or a short-term attack. The actual trajectory and the estimated trajectory using the proposed trust-based information fusion approach, as well as the trajectory estimated by the noisy node is shown in Fig. 3. The corresponding root-mean-square error (RMSE) performance results are shown in Fig. 4.

For uniform and relative degree-variance weighting schemes, both trust and untrust nodes are used for information fusion. They are not robust to random attacks. The error is mainly caused by the compromised nodes. The greater the attack strength, the larger the RMSE. Compared with uniform scheme, better performance is achieved for relative degree-variance scheme. Because smaller weights are given for the compromised nodes. The random attack is mitigated to some extend. For the proposed scheme, since clustering techniques are used to classify the nodes into trust and untrust sets. Only the trust nodes are used for information fusion. The effects of the compromised nodes are eliminated. Therefore, it is robust to the random attack and lowest RMSE is achieved.

4.2. False Data Injection Attack

For FDI attack, it assumes that the attacker knows the system model and the parameters. It can bypass the residual based bad data detection techniques that are widely used by the system operators. To launch the attack, attack vector $\boldsymbol{a}_{k,t|t}$ is added to the local estimate $\tilde{\boldsymbol{x}}_{k,t|t}$. In the simulation, the elements of the attack vector is generated from a normal distribution $N(\mu, \sigma^2)$ with mean μ and standard deviation σ.

The actual trajectory and the estimated trajectory using the proposed trust-based diffusion approach, as well as the trajectory estimated by the

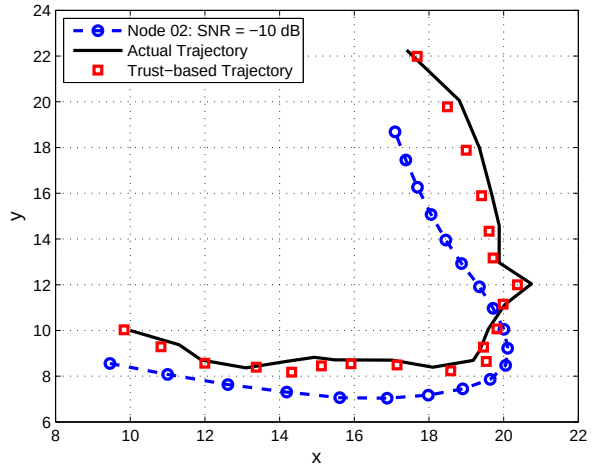

Figure 3: The actual trajectory and the estimated trajectory using the proposed trust-based information fusion approach, as well as the trajectory estimated by the noisy node.

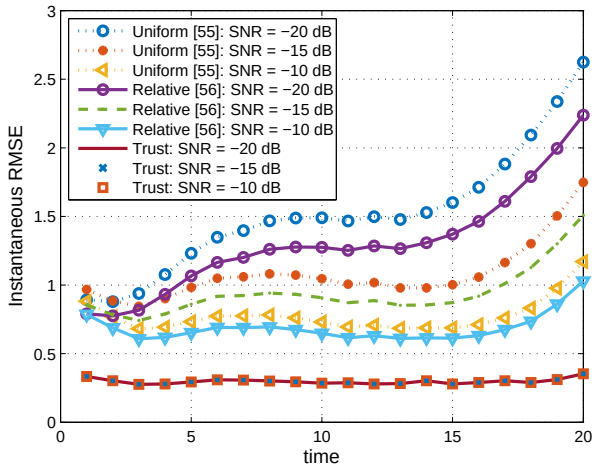

Figure 4: The instantaneous RMSE for uniform [55], relative degree-variance [56] and the proposed trust-based fusion schemes under different SNR scenarios.

node under FDI attack are shown in Fig. 5. The corresponding RMSE performance results are shown in Fig. 6.

For uniform and relative degree-variance weighting schemes, all the 7

nodes are used for information fusion. They are not robust to FDI attacks and the compromised nodes will cause large estimation errors. Better performance is achieved for relative degree-variance scheme as compared to uniform weighting scheme. Larger μ and/or σ will contribute to larger RMSE. For the proposed scheme, only the trusted nodes are used for information fusion. It is robust and the effects of FDI attacks are eliminated. Compared with the other two schemes, lowest RMSE is achieved for the proposed scheme.

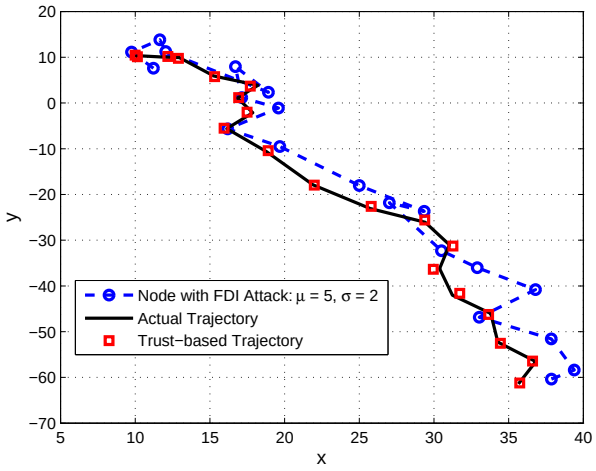

Figure 5: The actual trajectory and the estimated trajectory using the proposed trust-based information fusion approach, as well as the trajectory estimated by the node under FDI attack.

4.3. Reply Attack

In the last simulation, reply attack is considered. The attacker replays previous snapshots of a valid communication packet sequence that contains local estimates to deceive the system. For the three compromised nodes, the previous states are used to launch replay attacks. At time t, for nodes 02, 04 and 06, $\widetilde{\boldsymbol{x}}_{t-\tau}, \tau = 1, 2, 3$, are broadcast to their neighboring nodes. Since they

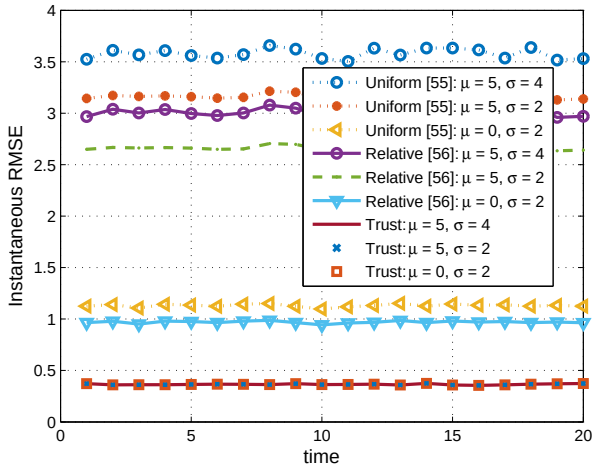

Figure 6: The instantaneous RMSE for uniform [55], relative degree-variance [56] and the proposed trust-based fusion schemes under FDI attacks, SNR = 10 dB.

are the actual states of the system, so they can bypass the residual based bad data detection schemes.

The actual trajectory and the estimated trajectory using the proposed trust-based approach is shown in Fig. 7. The corresponding RMSE performance results are shown in Fig. 8. For uniform and relative degree-variance weighting schemes, as in the previous two simulations, they are not robust to replay attacks. While for the proposed approach, it outperforms the other two schemes and again lowest RMSE is achieved.

Remark 1. *The proposed approach is a majority voting based scheme. As shown in the simulation results, robust performance is achieved for the proposed approach, provided that a minority of the sensors are compromised. It might be a realistic assumption. Because the attacker is either limited access to nodes, due to physical protection by system operators, or limited resources to compromise large scale networks [37]. While for the proposed trust-based*

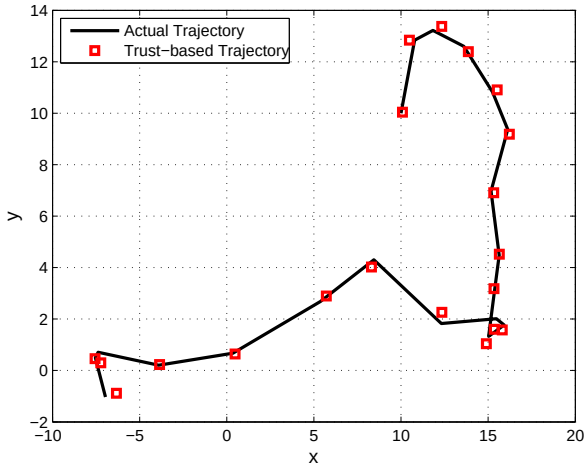

Figure 7: The actual trajectory and the estimated trajectory using the proposed trust-based diffusion approach, three nodes are under replay attacks.

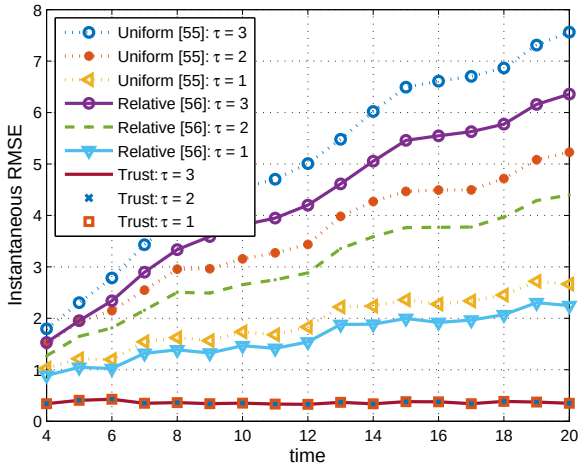

Figure 8: The instantaneous RMSE for uniform [55], relative degree-variance [56] and the proposed trust-based fusion schemes under replay attacks, SNR = 10 dB.

approach, the limitation can be overcome by introducing a subset of secured nodes, which are special nodes that can be highly trusted [57].

5. Conclusion

We propose a trust-based distributed Kalman filtering scheme for target tracking under malicious cyber attacks. Clustering technique is adapted to remove the bad data and/or the inaccurate estimates. After clustering, a dynamic combiner is obtained. Furthermore, it is robust to the cyber attacks, such as random, false data injection and reply attacks. And compromised nodes detection and localization are byproducts of the proposed approach. Even though the proposed technique is introduced in target tracking, the key idea can be applied to other applications, such as navigation, smart grids.

Acknowledgment

This work is partially supported by National Nature Science Foundation of China under Grant No. 61373116, Science and Technology Innovation Project of Shaanxi Province under Grant No. 2016KTZDGY04-01. This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 700044.

References

[1] C. Karlof, D. Wagner, Secure routing in wireless sensor networks: attacks and countermeasures, Ad Hoc Networks 1 (2-3) (2003) 293–315.

[2] A. Ribeiro, I. D. Schizas, S. I. Roumeliotis, G. Giannakis, Kalman filtering in wireless sensor networks: Reducing communication cost in state-estimation problems, IEEE Control Systems 30 (2) (2010) 66–86.

[3] J. Lin, W. Xiao, F. L. Lewis, L. Xie, Energy-efficient distributed adaptive multisensor scheduling for target tracking in wireless sensor networks, IEEE Transactions on Instrumentation and Measurement 58 (6) (2009) 1886–1896.

[4] A. Ez-Zaidi, S. Rakrak, A comparative study of target tracking approaches in wireless sensor networks, Journal of Sensors 2016 (2016) 1–11.

[5] Y. Zeng, R. Zhang, T. J. Lim, Wireless communications with unmanned aerial vehicles: opportunities and challenges, IEEE Communications Magazine 54 (5) (2016) 36–42.

[6] D. Anthony, J.-P. Ore, C. Detweiler, E. Basha, Controlled sensor network installation with unmanned aerial vehicles, in: Proceedings of the 12th ACM Conference on Embedded Network Sensor Systems, ACM, 2014, pp. 348–349.

[7] E. Xu, Z. Ding, S. Dasgupta, Target tracking and mobile sensor navigation in wireless sensor networks, IEEE Transactions on mobile computing 12 (1) (2013) 177–186.

[8] H. Chu, C.-d. Wu, A kalman framework based mobile node localization in rough environment using wireless sensor network, International Journal of Distributed Sensor Networks 11 (5) (2015) 841462.

[9] E. Fadel, V. C. Gungor, L. Nassef, N. Akkari, M. A. Malik, S. Almasri, I. F. Akyildiz, A survey on wireless sensor networks for smart grid, Computer Communications 71 (2015) 22–33.

[10] J. B. Predd, S. Kulkarni, H. V. Poor, Distributed learning in wireless sensor networks, IEEE Signal Processing Magazine 23 (4) (2006) 56–69.

[11] S. P. Talebi, S. Kanna, D. P. Mandic, A distributed quaternion Kalman filter with applications to smart grid and target tracking, IEEE Transactions on Signal and Information Processing over Networks 2 (4) (2016) 477–488.

[12] J. Hao, R. J. Piechocki, D. Kaleshi, W. H. Chin, Z. Fan, Sparse malicious false data injection attacks and defense mechanisms in smart grids, IEEE Transactions on Industrial Informatics 11 (5) (2015) 1–12.

[13] M. Ozay, I. Esnaola, F. T. Vural, S. R. Kulkarni, H. V. Poor, Sparse attack construction and state estimation in the smart grid: Centralized and distributed models, IEEE Journal on Selected Areas in Communications 31 (7) (2013) 1306–1318.

[14] M. S. Mahmoud, H. M. Khalid, Distributed Kalman filtering: a bibliographic review, IET Control Theory & Applications 7 (4) (2013) 483–501.

[15] E. F. Nakamura, A. A. F. Loureiro, A. C. Frery, Information fusion for wireless sensor networks: Methods, models, and classifications, ACM Computing Surveys 39 (3) (2007) 1–55.

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

[17] S. li Sun, Multi-sensor optimal information fusion Kalman filters with applications, Aerospace Science and Technology 8 (1) (2004) 57–62.

[18] N. Takahashi, I. Yamada, A. H. Sayed, Diffusion least-mean squares with adaptive combiners: Formulation and performance analysis, IEEE Transactions on Signal Processing 58 (9) (2010) 4795–4810.

[19] B. H. Fadlallah, J. C. Principe, Diffusion least-mean squares over adaptive networks with dynamic topologies, in: Proc. International Joint Conference on Neural Networks, IEEE, 2013, pp. 1–6.

[20] S. Julier, J. Uhlmann, A non-divergent estimation algorithm in the presence of unknown correlations, in: Proc. American Control Conference, 1997.

[21] O. Hlinka, O. Sluciak, F. Hlawatsch, M. Rupp, Distributed data fusion using iterative covariance intersection, in: Proc. IEEE International Conference on Acoustics, Speech and Signal Processing, 2014.

[22] W.-J. Qi, P. Zhang, G.-H. Nie, Z.-L. Deng, Robust weighted fusion Kalman predictors with uncertain noise variances, Digital Signal Processing 30 (2014) 37–54.

[23] M. Reinhardt, B. Noack, P. O. Arambel, U. D. Hanebeck, Minimum covariance bounds for the fusion under unknown correlations, IEEE Signal Processing Letters 22 (9) (2015) 1210–1214.

[24] B. Chen, G. Hu, D. W. C. Ho, L. Yu, Distributed covariance intersection fusion estimation for cyber-physical systems with communication

constraints, IEEE Transactions on Automatic Control 61 (12) (2016) 4020–4026.

[25] W. Niehsen, Information fusion based on fast covariance intersection filtering, in: Proc. International Conference on Information Fusion, 2002.

[26] D. Franken, A. Hupper, Improved fast covariance intersection for distributed data fusion, in: Proc. International Conference on Information Fusion, 2005.

[27] Y. Wang, X. R. Li, A fast and fault-tolerant convex combination fusion algorithm under unknown cross-correlation, in: Proc. International Conference on Information Fusion, 2009, pp. 571–578.

[28] K. Lu, R. Zhou, J. Zhang, Approximate chernoff fusion of Gaussian mixtures for ballistic target tracking in the re-entry phase, Aerospace Science and Technology 61 (2017) 21–28.

[29] J. Sijs, M. Lazar, State fusion with unknown correlation: Ellipsoidal intersection, Automatica 48 (8) (2012) 1874–1878.

[30] F. Cattivelli, A. H. Sayed, Diffusion distributed Kalman filtering with adaptive weights, in: Proc. Asilomar Conference on Signals, Systems and Computers, 2009.

[31] F. Wen, W. Liu, Diffusion least mean square algorithms with zero-attracting adaptive combiners, in: Proc. IEEE International Conference on Computer and Information Technology, 2015, pp. 252–256.

[32] A. Perrig, J. Stankovic, D. Wagner, Security in wireless sensor networks, Communications of the ACM 47 (6) (2004) 53.

[33] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, S. Sastry, Challenges for securing cyber physical systems, in: Proc. Workshop on Future Directions in Cyber-physical Systems Security, 2009.

[34] F. Pasqualetti, F. D rfler, F. Bullo, Attack detection and identification in cyber-physical systems, IEEE Transactions on Automatic Control 58 (11) (2013) 2715–2729.

[35] F. Pasqualetti, F. Dorfler, F. Bullo, Control-theoretic methods for cyber-physical security: Geometric principles for optimal cross-layer resilient control systems, IEEE Control Systems 35 (1) (2015) 110–127.

[36] C. M. Ahmed, S. Adepu, A. Mathur, Limitations of state estimation based cyber attack detection schemes in industrial control systems, in: Proc. Smart City Security and Privacy Workshop, 2016, pp. 1–5.

[37] Y. Liu, P. Ning, M. K. Reiter, False data injection attacks against state estimation in electric power grids, ACM Transactions on Information and System Security 14 (1) (2011) 13:1–13:33.

[38] Y. Mo, E. Garone, A. Casavola, B. Sinopoli, False data injection attacks against state estimation in wireless sensor networks, in: Proc. IEEE Conference on Decision and Control, 2010, pp. 5967–5972.

[39] R. Deng, G. Xiao, R. Lu, H. Liang, A. V. Vasilakos, False data injection on state estimation in power systems attacks, impacts, and defense: A

survey, IEEE Transactions on Industrial Informatics 13 (2) (2017) 411–423.

[40] G. Liang, J. Zhao, F. Luo, S. Weller, Z. Y. Dong, A review of false data injection attacks against modern power systems, IEEE Transactions on Smart Grid.

[41] Y. Mo, B. Sinopoli, Secure control against replay attacks, in: Proc. Annual Allerton Conference on Communication, Control, and Computing, 2009, pp. 911–918.

[42] B. Tang, L. D. Alvergue, G. Gu, Secure networked control systems against replay attacks without injecting authentication noise, in: Proc. American Control Conference, 2015, pp. 6028–6033.

[43] L. Lei, W. Yang, C. Yang, H. B. Shi, False data injection attack on consensus-based distributed estimation, International Journal of Robust and Nonlinear Control (2016) 1–11.

[44] T. Jiang, I. Matei, J. S. Baras, A trust based distributed kalman filtering approach for mode estimation in power systems, in: Proc. Workshop on Secure Control Systems, 2010.

[45] I. Matei, J. S. Baras, V. Srinivasan, Trust-based multi-agent filtering for increased smart grid security, in: Proc. Mediterranean Conference on Control & Automation (MED), 2012.

[46] T. Kanungo, D. Mount, N. Netanyahu, C. Piatko, R. Silverman, A. Wu, An efficient k-means clustering algorithm: analysis and implementation,

IEEE Transactions on Pattern Analysis and Machine Intelligence 24 (7) (2002) 881–892.

[47] Y. Zhang, C. Wang, N. Li, J. Chambers, Diffusion Kalman filter based on local estimate exchanges, in: Proc. IEEE International Conference on Digital Signal Processing, 2015.

[48] G. Wang, N. Li, Y. Zhang, Diffusion distributed Kalman filter over sensor networks without exchanging raw measurements, Signal Processing 132 (2017) 1–7.

[49] F. S. Cattivelli, A. H. Sayed, Diffusion strategies for distributed Kalman filtering and smoothing, IEEE Transactions on Automatic Control 55 (9) (2010) 2069–2084.

[50] J. Hu, L. Xie, C. Zhang, Diffusion Kalman filtering based on covariance intersection, IEEE Transactions on Signal Processing 60 (2) (2012) 891–902.

[51] R. Faragher, Understanding the basis of the Kalman filter via a simple and intuitive derivation, IEEE Signal Processing Magazine 29 (5) (2012) 128–132.

[52] V. Shnayder, M. Hempstead, B. rong Chen, G. W. Allen, M. Welsh, Simulating the power consumption of large-scale sensor network applications, in: Proc. of the 2nd International Conference on Embedded networked sensor systems, 2004, pp. 188–200.

[53] A. Mukherjee, P. Goswami, A. Datta, Hml-based smart positioning of

fusion center for cooperative communication in cognitive radio networks, IEEE Communications Letters 20 (11) (2016) 2261–2263.

[54] A. Sharma, K. A. Boroevich, D. Shigemizu, Y. Kamatani, M. Kubo, T. Tsunoda, Hierarchical maximum likelihood clustering approach, IEEE Transactions on Biomedical Engineering 64 (1) (2017) 112–122.

[55] V. D. Blondel, J. M. Hendrickx, A. Olshevsky, J. N. Tsitsiklis, Convergence in multiagent coordination, consensus, and flocking, in: Proc. 44th IEEE Conference on Decision and Control and European Control Conference, IEEE, 2005, pp. 2996–3000.

[56] F. S. Cattivelli, A. H. Sayed, Diffusion lms strategies for distributed estimation, IEEE Transactions on Signal Processing 58 (3) (2010) 1035–1048.

[57] S. Zheng, T. Jiang, J. S. Baras, Robust state estimation under false data injection in distributed sensor networks, in: Proc. IEEE Global Telecommunications Conference, 2010, pp. 1–5.