Consensus-based distributed estimation under linear attacks

Yuanyuan Xia[1], Wen Yang[1]

Abstract— **In this paper, we consider a consensus-based distributed filtering over wireless sensor networks under linear attacks. Suppose that in the network a malicious attacker injects false data into the data. First, we design an optimal estimator by minimizing the covariance of state estimation error. Then, we propose an effective detector for each sensor to resist the malicious data transmitted between the sensors in the network. Finally, the performances of the proposed estimator with the detector is demonstrated by comparing with the other typical attacking strategies.**

Index Terms— **Distribute estimation; Linear attack; χ^2 detector; Wireless sensor networks**

I. Introduction

A wireless sensor network is composed by a group of homogeneous sensors, which aims to cooperatively perceive, collect and process the information distributed in the geographical area including the deserts, the forest and so on. Wireless sensor networks have attracted great attention due to its broad potential applications in the area of forest fire detection, transportation surveillance, and industrial automation [1], [2]. In practical applications, it is usually deployed in an open, unattended or even hostile environment, which brings the security issue due to its distributed structure, see [3]. Generally, the attacking methods can be classified into two types: Denial of Service Attacks, and Integrity Attacks [4]. In [5], Liu *et al.* considered the integrity attack on parameter estimation in smart grid. Similar results can be found in [6] [7], Mo *et al.* considers linear deception attacks in the linear estimation process. Intuitively, if the data is modified under integrity attacks, the statistical properties in general change accordingly. Motivated by these problems, the residue-based χ^2 detectors are widely deployed to distinguish the attacks by checking the characteristics of the received data [8].

II. Problem formulation

A. System Model

Consider the following linear discrete-time system:

$$x(k+1) = Ax(k) + w(k), \tag{1}$$

where $x(k) \in \mathbb{R}^m$ is the state vector, $w(k) \in \mathbb{R}^m$ is the process noise, which is zero-mean white Gaussian with covariance matrix $Q > 0$. The initial state $x(0)$ is also zero-mean Gaussian matrix with covariance $\Pi_0 \geq 0$, and is independent of $w(k)$ for all $k \geq 0$.

The measurement equation of the ith sensor is given by

$$y_i(k) = H_i x(k) + v_i(k), \tag{2}$$

where $y_i(k) \in \mathbb{R}^m$ is the measurement of sensor i, the measurement noise $v_i(k) \in \mathbb{R}^m$ is zero-mean white Gaussian with covariance matrix $R_i > 0$ which is independent of x_0, $w(k)$ $\forall k, i$, and is independent of $v_j(s)$ when $i \neq j$ or $k \neq s$.

We model the sensor network as a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with the nodes $\mathcal{V} = \{1, 2, ..., n\}$ being the sensors and the edges $\mathcal{E} \subset \mathcal{V} \times \mathcal{V}$ representing the communication links. The existence of edge(i, j) means the ith sensor receives data from the jth sensor. Define the neighboring sensors of the ith sensor by $N_i = j : (i, j) \in E$. Let $d_i = |N_i|$ be the number of neighboring sensors of the ith sensor.

Consider the following distributed state estimator at ith sensor:

$$\hat{x}_i(k+1|k) = A\hat{x}_i(k|k-1) + K_p^i(k)[z_i(k) + \varepsilon \sum_{j \in N_i} z_j(k)], \tag{3}$$

where $z_i(k) = y_i(k) - H_i\hat{x}_i(k|k-1)$. The innovation $z_i(k)$ is zero-mean Gaussian; $z_i(k)$ and $z_j(k)$ are independent, $\forall i \neq j$; Moreover, the innovation covariance is denoted by $\Sigma_z \triangleq E[z_i(k)z_i(k)^T]$. ε is the consensus gain and in the range of $(0, 1/\Delta)$ with $\Delta = max_i(d_i)$.

Lemma 1: The optimal estimator gain is derived by minimizing the estimation error covariance $P_i(k)$ at each time step,

$$K_p^{i*}(k) = AYM^{-1}, \tag{4}$$

where

$$\begin{aligned} M &= \varepsilon^2 \sum_{s,r \in N_i} H_r P_{r,s}(k) {H_s}^T + H_i P_i(k) {H_i}^T + R_i \\ &\quad + \varepsilon \sum_{r \in N_i} (H_r P_{r,i}(k) {H_i}^T) + \varepsilon \sum_{s \in N_i} (H_i P_{i,s}(k) {H_s}^T), \\ Y &= \varepsilon \sum_{s \in N_i} P_{i,s}(k) {H_s}^T + P_i(k) {H_i}^T, i = 1, 2, \ldots, n. \end{aligned}$$

*This work was supported by the National Natural Science Foundation of China under Grant No 61573143 and the Programme of Introducing Talents of Discipline to Universities (the 111 Project) under Grant B17017.

[1] Y. Y. Xia and W. Yang are with the Key Laboratory of Advanced Control and Optimization for Chemical Processes, East China University of Science and Technology, Shanghai, 200237, China. weny@ecust.edu.cn

B. Attack Model

In this paper, we consider an attack model as

$$\tilde{z}_i(k) \triangleq T_k z_i(k) + b_i(k), \tag{5}$$

where $T_k \in \mathbb{R}^{m\times m}$ is an arbitrary attack matrix. Note that $z_i(k) \sim (0, \Sigma_z)$ and $b_i(k) \sim (0, \Sigma_b)$, it is easy to see that $\tilde{z}_i(k)$ still follows zero-mean Gaussian distribution with covariance $\Sigma_{\tilde{z}} = T_k \Sigma_z {T_k}^T + \Sigma_b$.

C. Detection and Estimation Model

In the following, we propose a distributed estimator for the considered system under linear attacks.

A typical χ^2 detector for the innovation $z_i(k)$ adopts the following hypothesis testing,

$$\xi_i(k) = \sum_{i=k-J+1}^{k} z_i(k)^T \Sigma_z^{-1} z_i(k) \lessgtr_{H_1}^{H_0} \eta, \tag{6}$$

where the null hypotheses H_0 means that the system is operating normally, while the alternative hypotheses H_1 means that the system is under attacks, J is the window size of detection and the threshold η is designed by χ^2 test threshold table properly.

Here, a detector based on the real time innovation is proposed,

$$\gamma_{ij}(k) = \begin{cases} 1, & \xi_i(k) < \eta, \\ 0, & otherwise. \end{cases} \tag{7}$$

From (3) and (7), we derive the distributed estimator with the detector for each sensor as the following,

$$\begin{aligned} \hat{x}_i(k+1|k) =& A\hat{x}_i(k|k-1) + K_p^i(k)[z_i(k)+ \\ & \varepsilon \sum_{j\in N_i} \gamma_{ij}(k)\tilde{z}_j(k)], \end{aligned} \tag{8}$$

where $\gamma_{ij}(k)$ is a binary variable representing the detection decision. If the detector of sensor i regards the edge (i, j) being attacked, i.e., the received data from sensor j is suspicious, then $\gamma_{ij}(k) = 0$, otherwise, $\gamma_{ij}(k) = 1$.

III. Simulation and Comparison

In this section, we will present some numerical examples. Consider a wireless sensor network with $n = 5$ sensors and the system parameters are defined as follows,

$$A = \begin{bmatrix} 1.01 & 0 \\ 0 & 1.01 \end{bmatrix}, \quad H_i = \begin{bmatrix} 2\zeta_i & 0 \\ 0 & 2\zeta_i \end{bmatrix}, \quad Q = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$$

$$R_i = \begin{bmatrix} 2v_i & 0 \\ 0 & 2v_i \end{bmatrix}, \quad T(k) = \begin{bmatrix} 2\delta_i & 0 \\ 0 & 2\delta_i \end{bmatrix}, \quad B_i = \begin{bmatrix} \sigma_i & 0 \\ 0 & \sigma_i \end{bmatrix},$$

where $\zeta_i, v_i, \delta_i, \sigma_i \in (0, 1]$ for all i, and $\varepsilon = 0.05$. As Fig. 1 shows, all the sensors (blue curves) track the unstable considered system (red curve) well as time evolving.

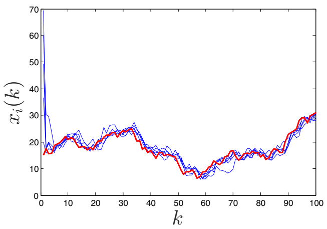

Fig. 1: Tracking performance.

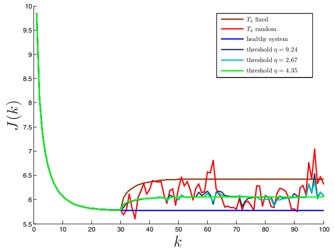

Fig. 2: The estimation error covariances of different cases.

We first define the trace of the averaged estimation error covariance, as $J(k) = \frac{1}{n}\sum_{i=1}^{n} tr(P_i(k))$.

As shown in Fig. 2, all the estimation error covariances of the four different cases converge to a limit. In the case of random attack matrix T_k, the estimation error covariance with the χ^2 detector is bounded as k goes infinity as well.

IV. Conclusion

In this paper, we have investigated the detection issue for consensus-based distributed filtering under linear attacks over wireless sensor networks. We proposed a χ^2 square detector for the distributed estimator, which effectively resist the linear attacks from the attacker. We have also provided a sufficient condition to ensure the stability of the estimation error covariances, and verified the effectiveness of the proposed detector by a numerical example. In the future, we will further explore the effects of the proposed detector under different types of attacks.

References

[1] B. D. O. Anderson and J. B. Moore, "Optimal filtering," *IEEE Transactions on Systems Man and Cybernetics*, vol. 12, no. 2, pp. 235–236, 1979.

[2] A. Ajith Kumar S, K. Ovsthus, and L. M. Kristensen, "An industrial perspective on wireless sensor networks ął a survey of requirements, protocols, and challenges," *IEEE Communications Surveys and Tutorials*, pp. 1391–1412, 2014.

[3] A. Proaño and L. Lazos, "Packet-hiding methods for preventing selective jamming attacks," *IEEE Computer Society Press*, pp. 101–114, 2012.

[4] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," pp. 495–500, 2008.

[5] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," pp. 21–32, 2009.

[6] Y. Mo, H. J. Kim, K. Brancik, and D. Dickinson, "Cyber-physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2012.

[7] Z. Guo, D. Shi, K. H. Johansson, and L. Shi, "Optimal linear cyber-attack on remote state estimation," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 4–13, 2017.

[8] Y. Mo and B. Sinopoli, "Integrity attacks on cyber-physical systems," pp. 47–54, 2012.