Automatica 87 (2018) 184–194

Contents lists available at ScienceDirect

Automatica

journal homepage: www.elsevier.com/locate/automatica

Attack allocation on remote state estimation in multi-systems: Structural results and asymptotic solution☆

Xiaoqiang Ren [a], Junfeng Wu [b,c,1], Subhrakanti Dey [d], Ling Shi [a]

[a] Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology, Hong Kong
[b] College of Control Science and Engineering, Zhejiang University, Hangzhou, PR China
[c] ACCESS Linnaeus Center, School of Electrical Engineering, Royal Institute of Technology, Stockholm, Sweden
[d] ITR, University of South Australia, Mawson Lakes, SA 5095, Australia

ARTICLE INFO

Article history:
Received 18 July 2016
Received in revised form 4 September 2017
Accepted 13 September 2017
Available online 23 October 2017

Keywords:
Attack
State estimation
Kalman filters
Structural results
Markov decision process
Multi-armed bandit

ABSTRACT

This paper considers optimal attack attention allocation on remote state estimation in multi-systems. Suppose there are M independent systems, each of which has a remote sensor monitoring the system and sending its local estimates to a fusion center over a packet-dropping channel. An attacker may generate noises to exacerbate the communication channels between sensors and the fusion center. Due to capacity limitation, at each time the attacker can exacerbate at most N of the M channels. The goal of the attacker side is to seek an optimal policy maximizing the estimation error at the fusion center. The problem is formulated as a Markov decision process (MDP) problem, and the existence of an optimal deterministic and stationary policy is proved. We further show that the optimal policy has a threshold structure, by which the computational complexity is reduced significantly. Based on the threshold structure, a myopic policy is proposed for homogeneous models and its optimality is established. To overcome the curse of dimensionality of MDP algorithms for general heterogeneous models, we further provide an asymptotically (as M and N go to infinity) optimal solution, which is easy to compute and implement. Numerical examples are given to illustrate the main results.

1. Introduction

Motivations and backgrounds. Cyber–physical systems, integrating information technology infrastructures with physical processes, are ubiquitous and usually critical in modern societies. Examples include sensor networks, power grids, water and gas supply systems, transportation systems, and water pollution monitoring systems. The use of open communication networks, though enabling more efficient design and flexible implementation, makes cyber–physical systems more vulnerable to attacks (Pasqualetti, Dorfler, & Bullo, 2015; Teixeira, Sou, Sandberg, & Johansson, 2015). Illustrative examples are Iran's nuclear centrifuges accident (Farwell & Rohozinski, 2011) and western Ukraine blackout (BBC, 2016).

Many research works on attackers' possible behaviors for cyber–physical systems have been done recently. Generally speaking, attacks can be classified as either denial of service (DoS) attacks or deception attacks (Amin, Cárdenas, & Sastry, 2009). DoS attacks, comprising availability of data, are most likely threats (Byres & Lowe, 2004) due to their easy implementation. DoS attacks in networked control systems are studied in Amin et al. (2009). Optimal off-line DoS attack on remote state estimation over a finite horizon for a single sensor system is investigated in Zhang, Cheng, Shi, and Chen (2015). An interactive decision of sending data by sensor and jamming channel by an attacker for remote state estimation in a zero-sum game setting is studied in Li, Shi, Cheng, Chen, and Quevedo (2015), and a similar setting is investigated for a control system in Gupta, Langbort, and Basar (2010). Optimal DoS attacks were also studied in the context of detection (Ren, Mo, & Shi, 2014). Deception attacks, comprising integrity of data, are more subtle. Various types of deception attacks have been studied, for example, replay attacks (Mo & Sinopoli, 2009), stealthy deception attacks (Guo, Shi, Johansson, & Shi, in press) and covert attacks (Teixeira et al., 2015).

Related works and contributions. In this paper, we consider the DoS attacks. Each sensor monitors a (different) system and sends its estimates to a fusion center over a packet-dropping channel. An

☆ The work by X. Ren and L. Shi is supported by a Hong Kong RGC General Research Fund 16210015. The work by J. Wu was supported in part by the National Natural Science Foundation of China under Grant No. U1401253 and in part by the Knut and Alice Wallenberg Foundation, the Swedish Research Council. The material in this paper was not presented at any conference. This paper was recommended for publication in revised form by Associate Editor Juan I. Yuz under the direction of Editor Torsten Söderström.

E-mail addresses: xren@connect.ust.hk (X. Ren), jfwu@zju.edu.cn (J. Wu), Subhra.Dey@unisa.edu.au (S. Dey), eesling@ust.hk (L. Shi).
[1] Fax: +86 571 8795 1879.

https://doi.org/10.1016/j.automatica.2017.09.021
0005-1098/

attacker is present and is capable of attacking a certain number of channels at each time. When a channel is under attack, the packet arrival rate decreases. The problem is to study the optimal attack policy to maximize the averaged estimation error at the fusion center. A threshold structure of optimal policies is proved. The related works are Leong, Dey, and Quevedo (2015), Mo, Sinopoli, Shi, and Garone (2012) and Ren, Cheng, Chen, Shi, and Zhang (2014), which study the structure of sensor scheduling policy. Our work differs from these works as follows. First, our work focuses on multi-systems, while a single sensor scenario is studied in aforementioned three papers. Second, we use a fundamentally different methodology. Specifically, both Mo et al. (2012) and Ren, Cheng et al. (2014) proved the structure results by analyzing the stationary probability distribution of states, which, however, works only in very special and simple cases (e.g., a single sensor case). On the contrary, we resort to the MDP theory, a more general and powerful tool. Although an MDP approach was also adopted in Leong et al. (2015), the methods used to prove either the existence of optimal stationary and deterministic policy or the threshold structure is significantly different due to the different problem models (multi-systems versus single sensor system, different cost/reward structures[2]). Lastly, we provide an asymptotically optimal policy, which is rather easy to compute and implement.

In summary, the main contributions of this paper are as follows.

(1) The problem of attack on remote state estimation in multi-systems is studied by an MDP formulation. The existence of a deterministic and stationary optimal policy is proved, which means that standard MDP algorithms (e.g., value iteration algorithm) can be utilized to compute the optimal policy. Moreover, a threshold structure of optimal policy is proved, by exploiting which a specialized algorithm may be developed to reduce the computational complexity. By the threshold structure, a myopic policy is proposed and its optimality is established for homogeneous models. The myopic policy is such that the expected reward at the next time is maximized.
(2) To overcome the curse of dimensionality of MDP algorithms for general heterogeneous models, we provide an asymptotically optimal index-based policy using the multi-armed bandit theory. Since the indices are computed based on each system *solely*, they are quite easy to compute. The index-based policy is implemented just by comparing these indices. What is more, our numerical examples show that this asymptotically optimal policy works quite well even when the number of total systems is small.

The remainder of this paper is organized as follows. In Section 2, the mathematical formulation of the considered problem is given. The main results, including the MDP formulation, existence of a stationary and deterministic optimal policy, threshold structure of the optimal policy and the asymptotically optimal index-based policy, are provided in Section 3. The numerical examples are given in Section 4 to illustrate the main results, after which we conclude the paper in Section 5. All the proofs are presented in Appendices.

Notation: $\mathbb{R}$ ($\mathbb{R}_+$) is the set of real (nonnegative) numbers and $\mathbb{N}$ the set of nonnegative integer numbers. $\mathbb{S}_+^n$ ($\mathbb{S}_{++}^n$) is the set of n by n real positive semi-definite (definite) matrices. For a matrix X, we use $\mathrm{Tr}(X)$, $X^\top$ and $|X|$ to denote its trace, transpose and spectral radius, respectively. We write $X \succeq 0$ ($X \succ 0$) if $X \in \mathbb{S}_+^n$ ($X \in \mathbb{S}_{++}^n$). For a vector x, denote its ith element as $x_{[i]}$. We use $\circ$ to denote function composition, i.e., for two functions f and g, $(f \circ g)(x) = f(g(x))$, and $g^i(x) \triangleq \underbrace{g \circ g \circ \cdots \circ g}_{i \text{ times}}(x)$ with $g^0(x) \triangleq x$.

[2] See the details in Footnote 8.

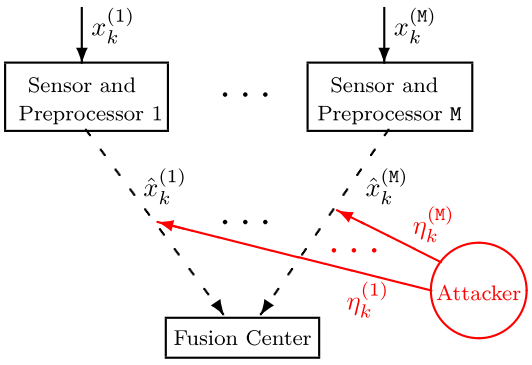

Fig. 1. Remote state estimation with an attacker.

Let $\times$ denote the Cartesian product. For a set $\mathbb{A}$, define the indicator function as $\mathbf{1}_{\mathbb{A}}(x) = 1$, if $x \in \mathbb{A}$; 0 otherwise. Let $\boldsymbol{Pr}(\cdot)(\boldsymbol{Pr}(\cdot|\cdot))$ be the (conditional) probability. For $x \in \mathbb{R}$, denote by $\lfloor x \rfloor$ the largest integer less than or equal to x. Let $\boldsymbol{E}[\cdot]$ be the expectation of a random variable.

2. Problem formulation

2.1. Remote estimation with packet-dropping channels

There are totally $\mathtt{M}$ independent discrete-time (i.e., sampled) linear time-invariant systems and $\mathtt{M}$ sensors. The ith sensor monitors the ith system (Fig. 1):

$$x_{k+1}^{(i)} = A_i x_k^{(i)} + \omega_k^{(i)}, \tag{1a}$$

$$y_k^{(i)} = C_i x_k^{(i)} + \upsilon_k^{(i)}, \tag{1b}$$

where $x_k^{(i)} \in \mathbb{R}^{n_i}$ is the system state vector and $y_k^{(i)} \in \mathbb{R}^{m_i}$ is the observation vector. The noises $\omega_k^{(i)}$ and $\upsilon_k^{(i)}$ are i.i.d. white Gaussian random variables with zero mean and covariance $Q_i \succeq 0$, $R_i \succ 0$, respectively. The initial state $x_0^{(i)}$ is a zero-mean Gaussian random variable that is uncorrelated with $\omega_k^{(i)}$ and $\upsilon_k^{(i)}$. It is assumed that the systems at different sensors are independent of each other. To avoid trivial problems, we assume the systems are unstable, i.e., $|A_i| > 1, \forall i = 1, \ldots, \mathtt{M}$. The pair (C_i, A_i) is assumed to be detectable and $(A_i, Q_i^{1/2})$ stabilizable.

Each sensor is assumed to be intelligent in the sense that a Kalman filter is run locally. With the above detectability and stabilizability assumptions, the estimation error covariance associated with each local Kalman filter converges exponentially to a steady state (Anderson & Moore, 2012). On the other hand, since the nature of asymptotic behaviors of remote estimation under malicious attacks (which will be elaborated later) over an infinite horizon cost is investigated, without any performance loss, we assume the Kalman filter at each sensor enters into the steady state at $k = 0$. Let the steady state estimation error covariance at sensor i be $\hat{P}^{(i)}$.

At each time k, sensor i sends the output of its local Kalman filter (i.e., the *a posterior* minimum mean square error (MMSE) estimate) $\hat{x}_k^{(i)}$ (Anderson & Moore, 2012) to a fusion center over a packet-dropping communication channel. Let $\gamma_k^{(i)} \in \{0, 1\}$ denote whether or not the packet is received error-free by the fusion center. If it arrives successfully, $\gamma_k^{(i)} = 1$; $\gamma_k^{(i)} = 0$ otherwise. Again since the asymptotic behavior over an infinite horizon is studied, it is assumed without any performance loss that $\gamma_0^{(i)} = 1, \forall i = 1, \ldots, \mathtt{M}$. Since the sensor sends the local MMSE estimates instead of raw measurements, the MMSE estimate and the associated error covariance at the fusion center (whether or not the attacker