Ad Hoc Networks 98 (2020) 102056

Contents lists available at ScienceDirect

Ad Hoc Networks

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

Multiagent approach for consensus control in the energy internet network

Steven Y.M. Chen

Faculty of Automation, Guangdong University of Petrochemical Technology (GDUPT), China

ARTICLE INFO

Article history:
Received 11 October 2019
Revised 22 November 2019
Accepted 1 December 2019
Available online 13 December 2019

Keywords:
Multiagent systems
Consensus control
Energy internet(EI)
Cyber-attacks

ABSTRACT

Energy internet network is an energy supply and demand system which based on the power grid, that can make a variety of energy interoperability, allowing all constituent elements to exchange information and interaction. However, any anomaly/failure in a part of the network can quickly spread over the network and lead to new unpredicted failures. Hence, timely cyber-attacks detection and mitigation is crucial. In this study, for timely detection, firstly propose a distributed state estimator assuming regular system operation, that achieves near-optimal performance based on the local Kalman filters and with the exchange of necessary information between local nodes over EI network. To enhance the security, consensus control approach can provide fault tolerance and timely attack mitigation and further recovery, thereby providing the EI with strong security in distributed. In this paper, therefore, a distributed Kalman filter with consensus control approach for multiagent systems (MAS) was proposed to investigate the energy internet recovered with links failure by cyber-attacks. The proposed algorithm is verified in the energy internet through a MAS model using MATLAB software.

1. Introduction

Recently, the energy internet(EI) network has been considered as a next-generation power system to modernize the power grid to improve its security, connectivity, efficiency and sustainability. The EI, an energy-based cyber-physical system(CPS), can be regarded as a form of the Internet of things (IoT) from an energy aspect [10]. The information and communication technologies(ICT) network build around the EI network becomes more and more integrated and the whole system is transitioning into a CPS [17]. One of the key functions of EI is to perform state estimation, which converts physical layer sensors measurements and other available information into an estimate of the state of the electric power system [7]. The estimated physical states in the system are processed by cyber computational layer to support operational and pricing decisions respectively. State estimation is given to the key role of combining network layers (field sensor measurements and communication networks) with physical and market operations, the physical and cyber layer risks associated with an attack on state estimation require utmost attention. Practically, a challenge task in the EI is reliable state estimation based on online measurements [3]. Also prevent the opponent's damage/misleading state estimation mechanism to cause error/manipulation decisions, resulting in power interruption or manipulation of electricity prices [7]. They create much more serious problems in the EI compared with the traditional power grid. Consensus control, therefore, become an approach that is used to achieve a reliable agreement on a quantity of interest among distributed, potentially unreliable, multi-agent network [5]. Our objective in this study is to design a highly secure and resilient state estimation mechanism for EI, that provides reliable state estimates in a fully-distributed manner, even in the case of cyber-attacks and other network anomalies. Motivated by the above discussion, this paper focuses on a distributed Kalman filter with consensus control approach for multiagent systems(MAS) was proposed to investigate the energy internet recovered with links failure by cyber-attacks. This study is based on the MAS approach, where intelligent agents, geographically distributed in the EI, receive (local) measurements on the state of the power grid and compute local Kalman filters estimate based on their own measurements and on the estimates of the neighboring agents as well. For multiagent systems (MAS) under cyber-attacks, the connectivity of network topology cannot be guaranteed and the resulting varying topology issue poses essential difficulties for the consensus control. Motivated by the above discussion, this paper is concerned with aim to design a distributed Kalman filter with consensus concept update approach to compensate for the undesirable

E-mail address: chenyeeming@gmail.com

https://doi.org/10.1016/j.adhoc.2019.102056
1570-8705/

effects of the failure links or nodes and the consensus property is retained after the recovery process in energy internet consensus control of networked multiagent systems for distributed coordination. The main contributions of this paper are summarized as follows:

(1) Assuming regular EI system operation (no anomaly), a fully-distributed dynamic state estimation scheme that achieves near-optimal performance thanks to the distributed Kalman filters and with the exchange of necessary information between neighbors in the network.
(2) Embed consensus control approach into the distributed Kalman filter to make it secure against measurement anomalies, and
(3) Detect and eliminate the effects of misbehaving nodes by cyber-attacks via the distributed Kalman filter with consensus coordinated control algorithm update approach to recovery the network operation.

The organization of the remaining part is presented as follows. Background and related work in Section 2. In Section 3, distributed Kalman filter and consensus control approach are introduced. In Section 4, a distributed Kalman filter with consensus control approach for multiagent networks are presented and numerical simulations are given to show the effectiveness of the approach results in Section 5. In the final section, concluding remarks are drawn.

2. Background and related work

The energy internet is a network covering power grids, distributed energy and various types of equipment and facilities on generation side, energy storage side, and user side. Due to the integration of advanced signal processing, communication, and control technologies, power grid relies on a critical cyber infrastructure that is subject to adversarial cyber threats [8]. The EI is regulated based on estimated system states and the main aim of attackers is to damage/mislead the state estimation mechanism and thereby to cause wrong/manipulated decisions in the energy management system of the EI [12]. In many realistic EI networks, due to the complexity of systems and undesirable cyber-attacks or disturbance, the occurrence of sensors controllers (generically referred to as 'nodes') or communication link failure is inevitable [10]. There exists a cyber-attack on sensors or a network exchanging data between sensors and controllers, which may be subject to maliciously destroy in common communication setting or wireless communication one [13]. This kind of phenomena is usually implemented by cyber-attacks with the aim of the enormous economy benefits. For real world energy internet network, representative examples of cyber-attacks include an attack on Slammer worm on Davis Besse power plant in Ohio, U.S. [4], and recent Stuxnet worm targeted many industrial control systems [2]. Hence, cyber-attacks significantly threaten the safe and reliable operation of the EI in practice. Effective countermeasures need to be developed considering the worst-case scenarios where the attackers are fully capable of performing a diverse range of cyber-attacks. The first step in a defense mechanism is early detection of cyber-attacks. After detecting an attack, effective mitigation schemes should then be implemented.

Many studies have been carried out to investigate the cyber-attacks in smart grid state estimations. To begin with, most of the state estimation methods use the weighted least squared (WLS) technique under cyber attacks [4], ([14]). Chi-Square detector is also used to detect those attacks [6]. Even though these approaches are easy to be implemented for nonlinear systems, it is computationally intensive and it cannot eliminate the attacks properly [1]. In the literature of state estimators, two different approaches have been taken, distributed and centralized state estimation [6]. The features of energy and channel capacity constraints render the centralized estimator impractical, which motivates researchers to focus on the distributed estimation protocols. Distributed dynamic state estimation has been also studied extensively, see e.g., [11] for a review of the distributed Kalman filtering techniques. Particularly, the advantages of the distributed estimation protocols include the scalability for large-scale networks and high fault tolerance. For distributed estimation problem, multiple sensors can sense the power plant, each sensor may get partial or no measurements related to the state of a power plant. The aim of a distributed estimator is to reconstruct an estimate of the power plant's state using its local measurement and its neighbor's information in the network without requiring a centralized node for information fusion. An agreement on the gathered distributed information can be reached via consensus algorithms. Consensus protocols are extensively studied in formation of multi-agent, distributed estimation, and distributed optimization problems [16]. Generally speaking, the information form of the local Kalman filter is utilized based on the individual sensor's estimation. Then, the average consensus is to reach the average of all nodes' initial values [20]. There has been an increasing activity in the study of distributed estimation in a network environment. This is due to its broad applications in many areas, including formation control Subbotin and Smith [18], Lin et al. (Lin et al.; 2017), distributed sensor network and cyber security Lu et al. [10] 18]. Blockchain (BC) is an emerging secure distributed database technology, operating on a peer-to-peer (P2P) network [15]. Although BC can be useful to secure the network database and the communication channels, the online sensor measurements are still vulnerable to attacks and faults. It would like to design a state estimation mechanism that is secure against all types of anomalies. Towards this goal, as one of the fundamental research topics arising from cooperative control for multiagent systems, consensus control has received considerable attention in various scientific fields ranging from mathematics to control engineering [19]. For the multiagent systems, each agent can only acquire local information about itself and its neighbors, and the objective of consensus is to design distributed control protocol by using local information such that all the agents reach to an agreement on a common value for some interest. This paper examines the problem of distributed estimation in a EI network of subsystems represented by a distributed Kalman filter model. The distributed Kalman filter mode focus is on the cyber-attack detection scenario where each node's sensor obtains some noisy measurements, and broadcasts them to its nearby neighbors' nodes. The neighbors exploit the received information, together with an estimate of their internal states, to make a decision about their detection states. As is well known, the main purpose of consensus control is to design a suitable control protocol such that the states of a team of agents can reach some common features. Obviously, the consensus issues with cyber-attacks deserve adequate research attention simply because of the high requirements of security and reliability in EI environments, and this gives rise to the main motivation for this current research.

3. Distributed Kalman filter

In this section, the distributed Kalman filter was discussed. The distributed Kalman filtering that relies on communicating state estimates between neighboring nodes and refer to it as local node using Kalman filter.

3.1. Local Kalman filtering

Assume that node i only receives information from its neighbors. In each local node Kalman filtering, let $N_i = \{j: (i, j) \in E\}$be the set of neighbors of node i on graph G. Each node i of the EI