www.revistageintec.net
ISSN: 2237-0722

revista GEINTEC
Gestão, Inovação e Tecnologias

Distributed Observer-based Cyber-security Control of Complex Dynamical Networks

M.D. Nazmoddin[1]; Dr. Neeraj Sharma[2]

[1]Research Scholar, Dept. of Computer Science & Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Bhopal-Indore Road, Madhya Pradesh, India.

[2]Research Guide, Dept. of Computer Science & Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Bhopal-Indore Road, Madhya Pradesh, India.

Abstract

A large number of interconnected nodes in which each node is a nonlinear dynamic system is a complex dynamic system. Complex cyber physical system refers to a new generation of complex systems which depend on close interactions between their physical components and cyber components. Many modern critical infrastructures as complex cyberphysical systems can be appropriately modelled. Distributed network is used in computer distribution. The distributed network infrastructure in the computer application, software and its data is distributed across many computers. The objective of the distributed network to share the resource, usually with a specific or comparable objective. With a lower transmission implication and computation costs in CPS, the proposed distributed cyber-physical algorithms will converge fast and thus increase the reliability. The results of the simulation verify the feasibility of the solution proposed.

Key-words: Complex Dynamical Networks, Cyber-physical Networks, Internet of Things (IoT).

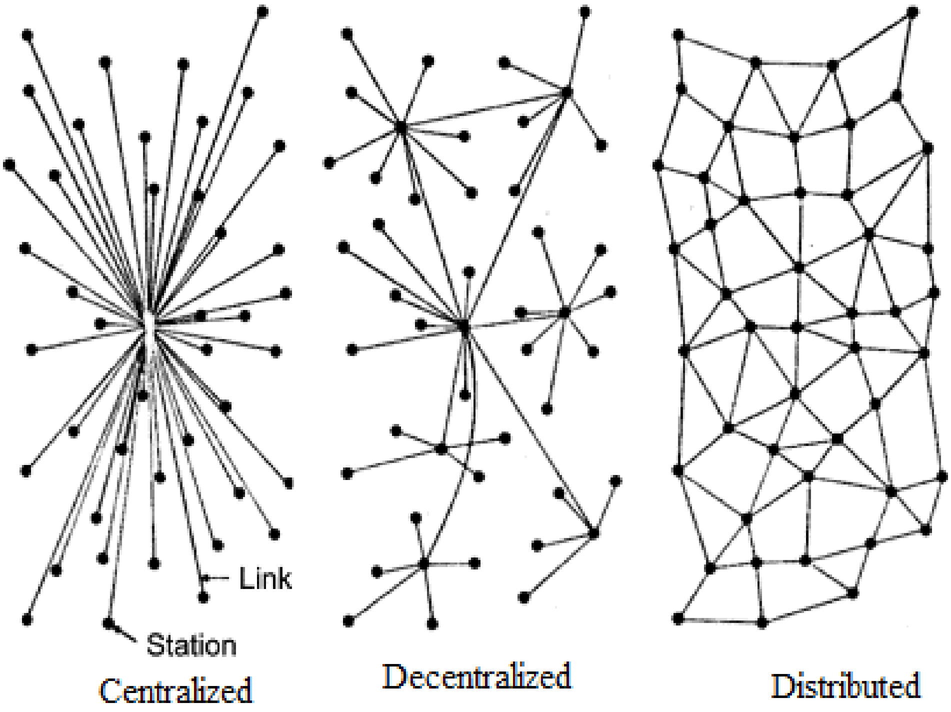
1. Introduction

Complex networks have today become an integral part of our everyday lives. Examples include transportation and telephone networks, internet, cellular networks, and, to name only a few, the World Wide Web. A graph in mathematics may define a complex dynamic network. Each node in such a graph represents a fundamental element with some dynamics and the borders represent the interactive topology of the network. In the past decade, analysis and control of complicated networks consisting of several dynamic nodes has drawn great attention in various fields. In particular, the control and synchronisation of large complex dynamic networks with certain types of topology were

Received: 10.06.2021 – Accepted: 11.07.2021

based. The development of systemic schemes for topology recognition is also an attractive subject in complex networks. Applications are available in various fields of science and engineering. For example, if a significant malfunction happens in a communication network, a power network or the Internet, the location of the defective spot or border is very important. Figure 1 shows the distributed network architecture as a framework with many priorities that your organisation will significantly gain. Three key aspects of systems with wide networks are taken care of by distributed network architecture. Centralized, distributed and decentralised are accessible.

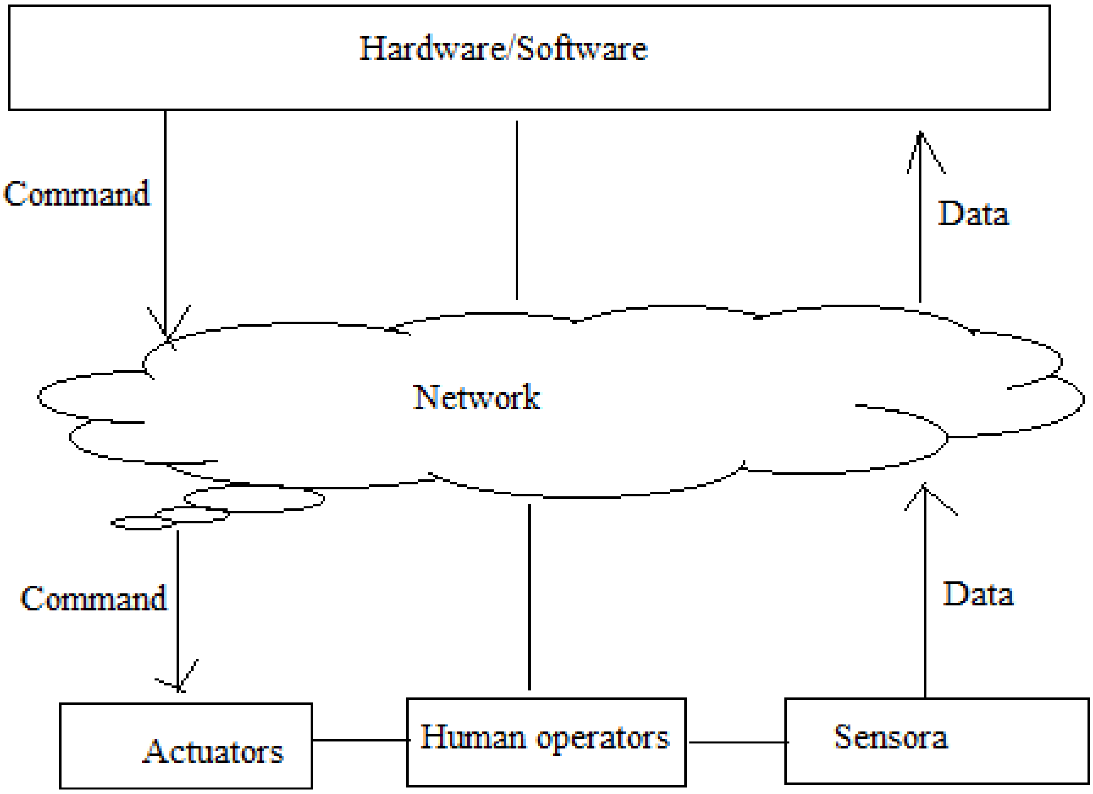
Fig. 1 - Distributed Network



Recently, complex cyber-physical networks have become a popular topic that emphasises the holistic perspective that combines the physical infrastructure with the cyberspace of complex networks. Cyber-physical framework means the combination of physical and cyber-communications elements and calculation processes. Physical components influence communication and computing, while embedded computers track and manage physical elements in networks. Fig 2 Cyber-physical systems are computing, networking and physical process integrations. Embedded computers and networks track and manage physical processes with feedback loops that influence calculations and vice versa. Physical processes.

Received: 10.06.2021 – Accepted: 11.07.2021

Fig. 2 - Cyber Physical System



Cyber-attacks include the assault on unsuspecting internet users either by using a device as a crime target (hacking, phishing, spamming...) or as a weapon to further crime (cyber stalking, identity theft, child pornography etc.). In this digital age, cyber attacks are growing rapidly making cyber security a challenge. Once successfully launched, cyber attacks can lead to monumental losses for businesses and individual response to individual incidents is necessary in order to rescue the situation if cyber attacks occur. However, this paper has shown that cyber attacks can be a targeted, untargeted or insider attack. The study found that the often illusory tactics and the omnipresent existence of cyber criminals are one of the biggest challenges for cyber security. The study highlighted practises that could contribute to deter cyber attacks while suggesting that companies adopt, enforce and regularly update their incident response plans. The study also established cyber security measures to combat cyber attacks. Systems like this are known as cyberphysical systems (CPS). They combine cyber abilities (communication, computing and control) with physical abilities (sensing and actuation) to solve issues not solved by any single component. The Logical Foundations of CPS aim to identify the common core, the essence of CPS and their evidence-based principles that can serve as simultaneous mathematical basis, while CPS is widely appreciated for its diverse fields of application (e.g. auto- and aerospace, medical, transportation, civil engineering, materials, chemistry, energy).

Digital computer science has revolutionised the development of systems and the functioning of our entire society. When software hits our physical world, we need even stronger foundations. By means of a heterogeneous architectures of interconnected sensors and devices, cyber physical systems (CPS) can provide a wide range of controls for complex industrial systems on the Internet of Things (IOT) setting. CPS systems are supposed to operate in real-time, such as the sensing, processing, communication and operation of information through different CPS infrastructure nodes. A compressed sensing-oriented consensus approach is implemented for distributed detection, estimate and tracking techniques such as CPS measurement, detection and tracking, which can guarantee efficiency in the hazardous setting, such as random packet losses, the asymmetry of the links, etc. Most CPS devices are not designed properly and more than 47 percent of all CPS and IoT devices have no trust in the protection of CPS and IoT. When protection in CPS in even apparently harmless devices or systems is not enough, it poses endemic vulnerabilities and hazards. As a CPS consists of several components, secure solutions must be developed to ensure that protection is integrated against attacks aimed at connected systems and devices. The consensus will increase the safety of all devices in a CPS system. Wireless Sensor Networks (WSNs) are simple CPS components and were used for the detection and collection of information. CPS will offer various advantages in comparison to WSNs: self-organization, real-time sharing of information, mutual control and reliable consensus in the status of events. Thus, CPS can be operated at high efficiency and at low cost. However, the implementation of CPS requires a synthesis of skills from various technical backgrounds due to its particular characteristics: (1) application background knowledge necessary for the development of the CPS services, (2) intelligent sensor sensing expertise essential for performing a task of sensing; (3) reliable wireless communication necessary to exchange information between nodes or the equipment, and (4) reliable networked data processing expertise necessary to understand the reliable exchange of data.

2. Literature Review

Tao Fei et al (2019) The same aim is to achieve seamless convergence between the physical and cyber worlds: the cyber-physical systems (CPS) and digital twins (DT). CPS offers a robust integrated and compatible platform and DT can be regarded as an oriented programme. CPS features such as cyberphysical mapping, lock control and a three-tier hierarchy, while CPS-based cyberphysical integration (for example, high fidelity models, fused data and on-demand services) can also be enhanced. In this chapter the implementation structure of the DT-based CPS is proposed,

Received: 10.06.2021 – Accepted: 11.07.2021

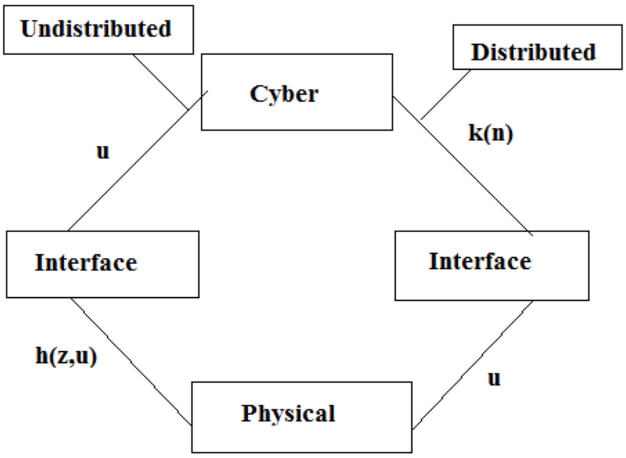
based on the relationship between these two principles, to effectively combine the physical and cyber worlds. In addition, the Internet of Things (IoT) is used to realise the links in and around the physical and cyber world so that each item is interactively linked.

Gujrati et al. Sumeet et al (2013) In this article, we propose a cyber-physical system model that presents algorithms for a range of computer problems, based on this model. The cyber-physical framework is described by our model as a combination of cyber infrastructure, physical infrastructure and user behaviour. The cyber infrastructure is overlapping the physical infrastructure and is constantly monitoring its evolving condition (physical infrastructure). Users work in the physical infrastructure and use hand-held devices and sensors to communicate with cyber infrastructure; and their activities are defined as to how to perform (e.g., move, observe). While users only communicate with the underlying cyber infrastructure in conventional distributed systems, users in a cyber-physical system can interact directly with each other, gain direct access to sensor data and take actions asynchronously in relation to underlying cyber infrastructure. These other forms of interactions influence the way distributed algorithms are constructed for cyber-physical systems. We increase mutual exclusion and predict algorithms for identification in order to accommodate user behaviours, interactions between them and physical infrastructure. The latest algorithms have two components - one describing the physical infrastructure behaviour of the users and the other describing the cyber infrastructure algorithms. The different cyber-physical device algorithms result from each combination of user behaviour and an algorithm in the cyber-infrastructure. Our algorithms were extensively simulated using the simulation engine and Uppsala model control. We also provide Cyber-Physical System Modeling Language (CPSML) for cyberphysical systems and a centralised, global state algorithm to record.

3. Proposed Algorithm

The proposed Distributed cyber-physical algorithms for broad-area power systems operation. In this article we suggest a distributed communication and computation using this distributed network of cyber-physical algorithms. Figure 3 is about The modelling and simulation of cyber physical systems is developed in order to model and simulate cyber-physical systems. The main focus is on this physical process model, finite state machines, calculations and transforms between physical and cyber variables.

Fig 3: Cyber Physical System



The modern cyber-physical structure then combines with digital and analogue instruments, interfaces. The interface on distributed and non-distributed networks can be linked. If the physical network is linked to h(z,u), u and cyber to u, k (n). The essential interconnected and heterogeneous compound of the behaviour in this network is a challenge for networking analysis and design.

Input: Each node calculates LLR as x (j) t , sets λj and c empirically, initializes estimate

x (j) (0) = 0

and local multiplier vector

z (j) (0) = 0.

Let T be the maximum number of iterations and e be the tolerable variance, all under conditions of convergence.

Output: the algorithm converges to the perfect result, and each node gets the global estimate

x = x (j) (T), ∀j ∈ N.

repeat All nodes update z (j) (t) and x (j) t via, ∀j;

All nodes transmit x (j) t (t + 1) to their one-hop neighbours in Nj , ∀j; t ← t + 1.

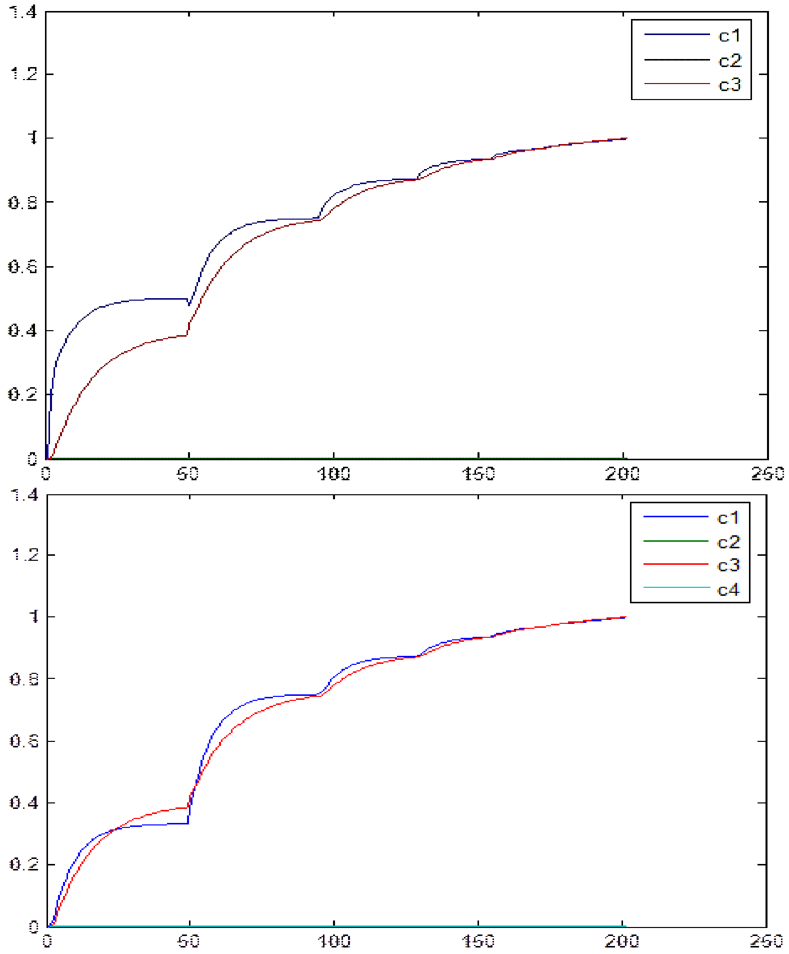
until t > T or kx (j) t (t + 1) − x (j) t (t)k ≤ e;

Conceived and implemented networked control systems face many challenges relating to computing time and case, software, variable time retards, failures, reconfiguration and distributed decision support systems. Protocol design to guarantee real-time service quality across wireless networks, agreements between control law design and real-time implementation complexity, the bridging of the difference between continuous and discrete-time systems and the robustness of large-scale systems are some of CPS research's challenges. The high reliability and safety requirements for heterogenous co-operating components that communicate through a complex, combined physical environment, operating over several spatial and temporal scales are required by means of frameworks, algorithms, methods and resources. CPS cross-engineering and physical world approach and the cyber world of information technology and computer science. Mathematical model, physical model, analysis and algorithm, system design and distribution, with their associated unpredictability and risk, are fundamental theories of the physical world. Sensors are key hardware aqueducts between the physical and cyber worlds, the sensor's properties and real world behaviour, and the processing techniques of signals are developed. Control assumption is a CPS significance. The appropriate aspect then includes stability, optimization and control of the distributed and digital systems.

4. Result Evaluation

The distributed cyber-physical algorithms will be developed in this section to detect sparse events.

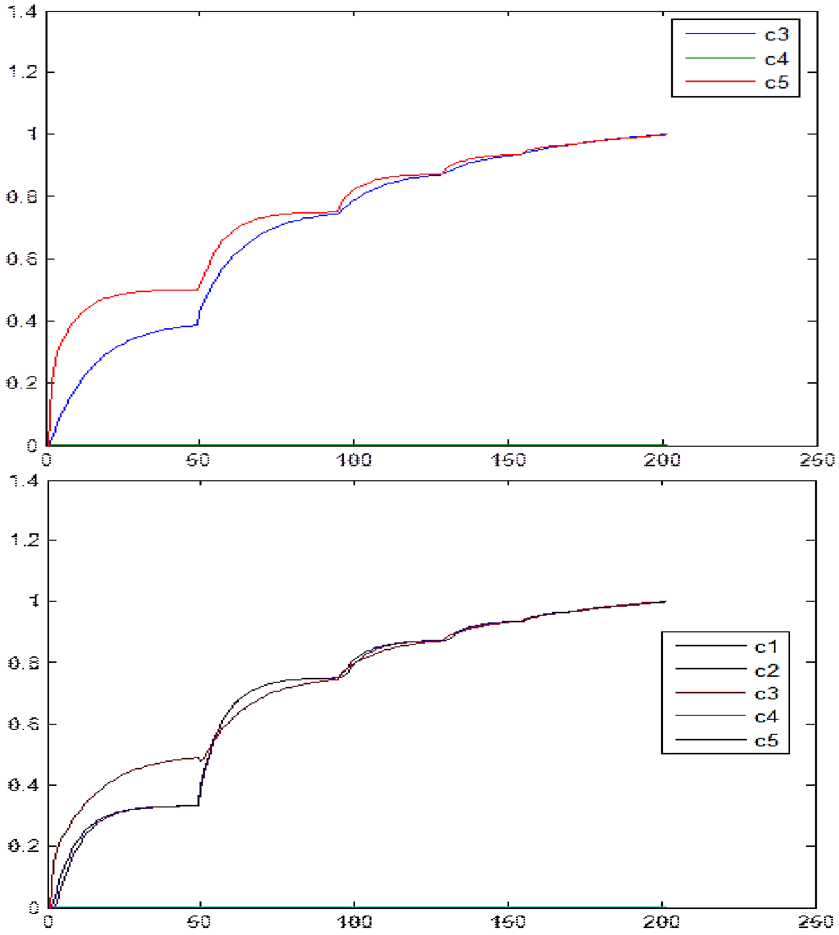
Fig. 4 - Preliminary Result at n 1 and n 2



Received: 10.06.2021 – Accepted: 11.07.2021

It is possible to see that the neighbour set of n1 contains nodes n2, n3. Similarly, n2 has the neighbours set to n1, n3, n4, n3, n3 has the neighbour set to n1, n2, n4,n5, n4 and n2 respectively has a neighbour set to n2, n3, n5 and n5 has the neighbours set to n3, n4. The consensus algorithm can only be executed at the nodes n1, n2, and n3 and can report decision results if the nodes n2 and n4 are in sleep mode. As previously mentioned, however, the active nodes can report the results of the decision by themselves and their neighbouring active nodes can report the decision results of their neighbouring inactive nodes. Events c1 and c2 are successfully observed at node n1. Then n2 observed c1, c2, and c3 successfully as the nodes n1 and n2 were its neighbours. Since the status of c3 and c4 is 0, i.e. there was no event at v3 and v4, nodes n3 and n4 have announced the detection results of their neighbours.

Fig. 5 - Preliminary Result at n 3 and n 4



We build a network to test the efficiency of small events detection in a large CPS. Nodes are connected to their neighbours, whether their neighbours are within the transmission range. If the

Received: 10.06.2021 – Accepted: 11.07.2021

graph (network) is not linked, node positions will be randomly regenerated before the graph is connected.

5. Conclusion

In this paper, a distributed observer-based cyber security control issue for consensus-based dynamic network monitoring. Distributed cyberphysical algorithms that can be used in CPS for sparse event detection, originally derived for consensus by providing every node with complete detection information even when the topology changes. CPS will cover different aspects of social and economic life, carry broad impact and guide computer science and other topics. The numerical results indicate that the estimation of the scarce event detection with the proposed distributed consensus algorithm can be determined successfully. In the design and production of future engineering systems with new technologies that are much greater than today's standards of autonomy, functionality, accessibility, reliability and data protection cyber-physical systems is expected to be of significant importance. The progress of CPS research can be improved by close cooperation with major challenge applications between university disciplines in computing, communication, control and other engineering and computer sciences.

References

G. Wen, W. Yu, X. Yu, and J. Lü, “Complex cyber-physical networks: From cybersecurity to security control,” *J. Syst. Sci. Complex*, 30(1), 46–67, Feb. 2017.

L. Sha, S. Gopalakrishnan, X. Liu, and Q. Wang, “Cyber-physical systems: A new frontier,” in *Machine Learning in Cyber Trust*. New York, NY, USA: Springer, 2009, pp. 3–13.

Mohammed Moness; Ahmed Mahmoud Moustafa, “A Survey of Cyber- Physical Advances and Challenges of Wind Energy Conversion Systems: Prospects for Internet of Energy”, *IEEE Internet of Things Journal*, 3(2), 134-145, 2016.

C. Qi and Y. He, “Design of data collection system based on CPS,” *Comput. Syst. Appl.,* 19(6), 5−8, Jul. 2010.

Y.F. Hu, F.M. Li, and X. H. Liu, “CPS: network system framework and key technologies,” *J. Comput. Res. Dev.,* 47Suppl., pp. 304−311, Nov. 2010.

K. Pereira, *“Cyber-Physical Systems”,* Nov. 1, 2013. http://www.International.rutgers.edu/

J.H. Shi, J.F. Wan, H.H. Yan, and H. Suo, “A survey of cyber-physical systems,” *in Proc. 2011 Int. Conf. IEEE Wireless Communications and Signal Processing (WCSP),* Nanjing, China, 2011.

K.D. Kang and S.H. Son, “Real-time data services for cyber physical systems,” *in Proc. 28th Int. Conf. Distributed Computing Systems Workshops, Beijing, China,* 2008, pp. 483−488.

Houbing Song, Glenn A. Fink, and Sabina Jeschke, Security and Privacy in Cyber-Physical Systems: Foundations, Principles and Applications. *UK: Wiley - IEEE Press*, 2017.

G. Wen, W. Yu, Y. Xia, X. Yu, and J. Hu, "Distributed tracking of nonlinear multiagent systems under directed switching topology: An observer-based protocol," *IEEE Trans. Syst., Man, Cybern., Syst.*, 47(5), 869–881, May 2017.

S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proc. IEEE,* vol. 100, no. 1, pp. 210–224, Jan. 2012.

X. Hu, H. Wang and X. Tang, "Cyber-Physical Control for Energy-Saving Vehicle Following with Connectivity," *IEEE T. Ind. Electron., 64*(11), 8578–8587, Nov. 2017.

M.D. Ilic, L. Xie, U.A. Khan, and J.M.F. Moura, "Modeling of future cyber-physical energy systems for distributed sensing and control," *IEEE Trans. Syst. Man Cybernet. A: Syst. Human.*, 40(4), 825−838, Jul. 2010.

P.L. Tan, J. Shu, and Z.H. Wu, "An architecture for cyber-physical systems," *J. Comput. Res.Dev.,* 47, no. *Suppl.,* 312−316, Nov. 2010.

Y.F. Zhang, C. Gill, and C.Y. Lu, "Reconfigurable real-time middleware for distributed cyber-physical systems with aperiodic events," *in Proc. 28th International Conf. Distributed Computing Systems, Beijing, China,* 2008, 581−588.