IoT-based cyber-physical communication architecture: challenges and research directions

Md Masud Rana and Rui Bo

1Department of Electrical and Computer Engineering, Missouri University of Science and Technology, Rolla, Missouri, USA
2E-mail: mrd2090801@gmail.com

Abstract: In order to provide intelligent services, the Internet of Things (IoT) facilitates millions of smart cyber-physical devices to be enabled with network connectivity to sense, collect, process, and exchange information. Unfortunately, the traditional communication infrastructure is vulnerable to cyber attacks and link failures, so it is a challenging task for the IoT to explore these applications. In order to begin research and contribute into the IoT-based cyber-physical digital world, one will need to know the technical challenges and research opportunities. In this study, several key technical challenges and requirements for the IoT communication systems are identified. Basically, privacy, security, intelligent sensors/actuators design, low cost and complexity, universal antenna design, and friendly smart cyber-physical system design are the main challenges for the IoT implementation. Finally, the authors present a diverse set of cyber-physical communication system challenges such as practical implementation, distributed state estimation, real-time data collection, and system identification, which are the major issues require to be addressed in implementing an efficient and effective IoT communication system.

1 Introduction

With the fast development of science and technology, industrial applications are becoming complex and large. Large-scale control systems are present everywhere to sustain the nominal operation of many critical process that we rely on. In fact, cyber-physical systems (CPSs) are a class of more complex large-scale systems, which can integrate physical processes, computational resources, and communication capability [1]. Typical CPSs can sense, process, and control the physical system. Interestingly, many practical systems can be categorised as CPSs, such as smart grids, electric vehicles, wireless power transfer systems, unmanned aerial vehicles, and robotic networks.

The Internet of Things (IoT) is the potential technology that will be able to closely monitor the physical systems such as wristwatches, vending machines, emergency alarms, garage, home appliances, and smart vehicles from the remote control centre [2-4]. It can be seen that all surrounding electronic devices to facilitate our daily life operations are connected to the IoT network and can be monitored as well as controlled remotely [5, 6]. Specifically, the IoT embedded sensors and actuators are integrated into the physical systems such as automated vehicles and microgrids [7]. There are signficant research challenges that arise when the IoT can integrate these smart devices into the digital network.

The main contributions of this paper are summarised as follows:

- First of all, several key technical challenges and requirements for the IoT-based CPSs are identified. Basically, privacy, security, intelligent sensors/actuators design, low cost and complexity, and friendly smart vehicle design are the main challenges for the IoT-based cyber-physical communication systems.
- We present a diverse set of future research directions such as practical implementation, distributed state estimation, real-time data collection, system identification and security.

The rest of the article is organised as follows. The IoT-based cyber-physical communication architecture is described in Section 2. Then the potential research challenges for the IoT systems are summarised in Section 3. Finally, the future research directions and conclusion are presented in Sections 4 and 5, respectively.
communication background and their technical features need to know in advance. Table 1 illustrates the communication technologies, and their real-time applications [3, 14–17]. It can be seen that from the limited analogue communication platform, we are living in IoT digital communication where anyone can communicate and interact with the global information network [18]. Basically, both 3G and 4G use code division multiple access and frequency division multiple access (FDMA) schemes while the 5G uses single-carrier FDMA (SC-FDMA), and orthogonal frequency-division multiple access (OFDMA) which can assign...
subsets of subcarriers to the individual user [3, 14, 15, 19–21]. Consequently, massive number of users can use channel spectrum properly without interference due to orthogonal property. Therefore, the SC-FDMA/OFDMA is the promising technology for 5G IoT as it requires to handle massive amount of smart devices and customers with high data rate. The performance comparisons of 4G and 5G systems are shown in Table 2 [15, 17]. It can be seen that 5G provides better speed and spectral efficiency compared with 4G. Therefore, it is believed that 5G with IoT can integrate any smart devices into the digital world effectively. Several key technical challenges for the IoT-based CPS are presented in the following section.

### Challenges of IoT-based cyber-physical communication systems

Generally speaking, CPSs can sense, process, and control the physical system effectively. Interestingly, many practical systems can be categorised as CPSs, such as smart grids, wireless power transfer systems, electric vehicles, and robotic networks. There are significant research challenges that arise when the IoT can integrate any smart devices into digital network. The key technical challenges are shown in Fig. 3. It can be seen that the privacy, security, intelligent sensors/actuators design, low cost and complexity, friendly smart CPS design are the main challenges for the IoT implementation. The key technical challenges for IoT-based CPSs are described as follows:

#### i. Security and privacy

There are massive number of smart objects connected to the IoT. They are mostly situated in the open space where they used simple encryption and pass keys [22, 23]. Therefore, it is easy for eavesdroppers to hack smart objects. For example, after hacking the electric vehicle, the hacker can take all items and personal information. Furthermore, the fare can also be manipulated and transferred. Consequently, security and privacy are the main challenges to design IoT-based smart electric vehicles.

#### ii. Modelling hybrid physical systems

Most of the physical system is continuous and non-linear in nature. For instance, the state-space representation of the power system and electric vehicle are non-linear and continuous time [24, 25]. The system is processed by the digital computer where discrete-time scheme is preferred. Generally, the discrete-time system is easy to implement in the digital computer, while the continuous system is easy to analyse from the mathematical perspective [26]. Furthermore, the non-linear system requires to linearise around the operating points, and it introduces errors. Considering the linearised and quantisation errors in state-space model is originally reflected the true system. However, considering these errors, it is very difficult to develop an estimation and control algorithm [26]. Due to mathematical difficulties, sometimes researchers analysed the algorithmic convergence in continuous-time while the developed algorithm is discrete time [26, 27].

#### iii. Smart control centre design

In order to visualise and monitor the physical system, the control centre such as SCADA uses state estimation and stabilisation algorithms [28]. For different systems such as vehicle monitoring and smart grid, there are different types of SCADA systems designed and implemented in real time. However, most of the approaches are developed without considering cyber attacks and noises. As we are living in the IoT-based two-way communication era, so the system impairments such as noises and cyber attacks are considered in

---

**Table 1** Comparisons of different IoT communication protocols and services

| Technology | Protocol | Power rating | Speed       | Frequency   | Coverage |
|------------|----------|--------------|-------------|-------------|----------|
| NFC        | PAN      | very low     | 100–400 kbps | 13.56 MHz   | 10 cm    |
| Bluetooth  | PAN      | low          | 2 Mbps      | 2.4 GHz     | 0.1–0.25 km |
| WiFi       | LAN      | medium       | 54 M–1 Gbps | 2.4 and 5 GHz | 50 m |
| Zigbee     | LAN      | very low     | 250 kbps    | 2.4 GHz     | 10–100 m |
| WiMax      | WAN      | high         | 11–100 Mbps | 10–66 GHz   | 50 km    |
| LoRa       | WAN      | high         | 50 kbps     | 868/915 MHz | 25 km    |
| 4G         | WAN      | high         | 12 Mbps     | 800, 1800, 2600 MHz | 10 km |
| 5G         | WAN      | high         | 3.6–10 Gbps | 600 MHz–86 GHz | 10 km |
| NB-IoT     | WAN      | high         | 250 kbps    | 900 MHz     | 35 km    |

**Table 2** Performance comparisons of 4G and 5G systems for IoT-based cyber-physical applications

| Features       | 4G performance | 5G performance |
|----------------|----------------|----------------|
| mobility       | 350 km/h       | 500 km/h       |
| speed          | 0.01–1 Gbps    | 0.01–20 Gbps   |
| latency        | 10–100 ms      | 1–50 ms        |
| energy efficiency | 0.1 mJ/100 bits | 0.1 mJ/100 bits |
| device density | 100 k/km²      | 1000 k/km²     |
| spectral efficiency | 1.5            | 4.5            |

**Fig. 3** Key challenges of the IoT-based CPSs
estimation process. Without considering these impairments, the estimated system states cannot reflect the true system states. Consequently, it can cause social, economic, and national problems depending on impairments [29, 30].

iv. **Intelligent sensors and actuators design:** Generally speaking, designing smart sensors and actuators are key to be interconnected for sustainable, clean, and green modern society. There are different types of sensors such as temperature, pressure, humidity, and phasor measurement units available in real time [31–33]. However, each sensor can do the particular task and cannot perform other sensing activity at all [34]. Therefore, the researchers and industry people will need to categorise sensors based on the specific characteristics and applications. In this way, it will not be so difficult to design the universal sensors in future. Unfortunately, there is a little effort to design such sensors and actuators so far. As the IoT can connect anything and anytime, so IoT expects to design the universal sensors which can sense anything [34, 35].

v. **Find suitable cross-domain application:** There is a significant research gap between practical application and academic research in the IoT-based CPSs. In biomedical engineering, the IoT can be used for signal transmission whereas they are not well familiar in this emerging technology [36–38]. Similarly, the machine learning tools such as deep learning and reinforcement learning can be used for CPS state estimation in data-driven approach [39–41]. However, there is a significant cross-domain research gap between electrical and computer engineering.

vi. **Optimal smart meter design for IoT-based CPS modernisation:** In order to modernise the CPS, the placement and number of meter can play a vital role for the utility operator. Typical example of CPSs is the electricity, water, and gas meters [42–45]. However, it is very difficult to find proper location and number of optimal smart meters installation. Moreover, designing the low-cost smart meters and installation are also the challenging tasks for developing counties.

vii. **Smart antenna design for IoT-based CPS:** The antenna can play a vital for CPS signal transmission and reception. Different applications require diverse specification and requirements. For biomedical application, it requires small and wearable antenna whereas the communication industry requires high gain and directivity [46–48]. Therefore, the antenna should design for specific IoT applications, and there is an open challenge to design an universal antenna.

viii. **Design complexity:** When designing the IoT-based CPSs, the algorithm and physical structure should be low complexity and affordable connectivity to the low-power devices as shown in Table 1. In order to do this, the signal processing, computer science, and mechanical engineering communities will need to take necessary action to design such a cyber-physical model and algorithms [29, 49, 50].

ix. **Interoperability:** It is most common problem in today's society that designed software and hardware are not compatible with other models, companies, and generations. One of the main targets of IoT is the sustainable future, so designing IoT-based CPSs should be compatible with other generations, standards, technologies, and models [11, 51].

After identification of the challenges, one will need to know the potential research directions.

### 4. Future research directions

We present a diverse set of future research directions such as practical implementation, distributed state estimation, real-time data collection, and system identification from data time. The key future research directions are shown in Fig. 4. The key technical challenges are described as follows:

i. **Implementation of CPSs:** It can be seen that the most of algorithm is verified through numerical simulations. In order to practically implement and place in the market, it will require money and support for sustaining the product and services. Efforts should be concentrated in developing reliable state estimation algorithm considering fading channel and cyber attacks into consideration [52–54].

ii. **Developed distributed CPSs and algorithms:** Most of the CPSs are centralised so it will need to deregulate and propose distributed algorithms. The distributed system provides low computational complexity and easy to diagnosis, if needed [55, 56].

iii. **Effective communication infrastructure design:** Designing a reliable IoT communication infrastructure is one of the open research challenges [54, 57, 58]. The facility of IoT is significantly increased in the recent years, so designing two-way effective communication infrastructure is not only requirement but also a challenging task [33, 59]. In order to design IoT-based digital communication systems, the sensing analogue signal is firstly need to be digitised. Interesting, the IoT can integrate any physical smart devices at any time and their signal is real-value analogue. Therefore, the designing universal analogue-to-digital converter is one of the future research directions [60].

iv. **Apply machine learning approaches for CPS modernisation:** Machine learning algorithms such as deep learning and reinforcement learning can be used for CPS state estimation in a data-driven fashion [39, 41, 61, 62]. When there is significant fluctuation or unreliable information, these approaches cannot be able to perfectly describe and predict the real system [63].

v. **Real-time data collection, analysis, and decisions:** Generally, service providers monitor the system dynamics after certain intervals. For instance, the power system is monitored by every 15 s [31, 64]. Sometimes, it is redundant or inappropriate to gather large amount of data within this time frame. Basically, system operators have processing, storage, and resource limitations. It is better to design a control centre which can continuously monitor the system dynamics and avoid unnecessary information for storages.

---

**Fig. 4 Potential research directions of IoT-Based CPS**
vi. Developed effective state estimation algorithms: The CPS states such as synchronous generator states such as rotor angle and speed are unknown. In order to estimate the cyber-physical state, the weighted least squared, least mean squared, Kalman filter, extended Kalman filter, and H-infinity are key schemes [65-67]. Unfortunately, all of these methods work well when there are no cyber attacks and packet losses. Considering some impairments, the cyber-physical state estimation algorithms will need to develop. When the energy storage is connected to the CPS system, then the state of charge can be estimated using signal processing algorithms.

vii. Security, reliability, and trusts: The IoT can connect and provide service to the massive devices and networks, so their security, reliability, and privacy are the main concern [68]. In future, one can design a channel coding based reliable IoT communication network where eavesdroppers can hardly identify the transmitted bit sequences [69]. Furthermore, most of the physical systems are non-linear, so the cyber attacks can be handled accordingly [70, 71]. Moreover, identification of key vulnerabilities in the communication network serves as weak entry points for various attacks [21]. Therefore, researcher can develop reliable communication network with strong encryption and cryptographic algorithm.

5 Conclusion

In this paper, we have presented a review of recent works along with research opportunities on the networking aspect of IoT for CPSs. After identifying several key technical challenges for IoT system, eight key research directions and potential solutions are critically summarised. Based on the findings, summarised technical challenges, research directions, and potential solutions, it is believed that this paper acts as an informative source for IoT and cyber-physical researchers.

6 References

[1] Ge, H., Zhao, Z.: ‘Security analysis of energy internet with robust control approaches and defense design’, IEEE Access., 2018, 6, pp. 11203–11214
[2] Lin, J., Xu, W., Zhang, N., et al.: ‘A survey on internet of things: architecture, enabling technologies, security and privacy, and applications’, IEEE Internet Things J., 2017, 4, (5), pp. 1125–1142
[3] Shi, W., Cao, J., Zhang, Q., et al.: ‘Edge computing: vision and challenges’, IEEE Internet Things J., 2016, 3, (5), pp. 637–646
[4] Rana, M.M., Li, L., Su, S.W., et al.: ‘Consensus-based smart grid state estimation algorithm’, IEEE Trans. Ind. Inf., 2017, 13, (8), pp. 3368–3375
[5] Marjani, A., Basaruddin, F., Gani, A., et al.: ‘Big IoT data analytics: architecture, opportunities, and open research challenges’, IEEE Access., 2017, 5, pp. 5247–5261
[6] Rana, M.M., Xiang, W., Wang, E.: ‘IoT-based state estimation for microgrids’, IEEE Internet Things J., 2018, 5, (2), pp. 1345–1346
[7] Razzaque, M.A., Milojkovic-Jevric, M., Palade, A., et al.: ‘Middleware for internet of things: a survey’, IEEE Internet Things J., 2016, 3, (1), pp. 70–95
[8] Perez, C., Zalezak, J., Christin, A.: ‘Next awareness: a new concept for the internet of things: a survey’, IEEE Commun. Surv. Tutor., 2014, 16, (1), pp. 414–454
[9] Rana, M.M., Xiang, W., Wang, E.: ‘Internet of things infrastructure for wireless power transfer systems’, IEEE Access., 2016, 6, pp. 19295–1936
[10] Frustaci, M., Pace, P., Alois, G., et al.: ‘Evaluating critical security issues of the IoT world: present and future challenges’, IEEE Internet Things J., 2017, 4, (5), pp. 2483–2495
[11] Porambage, P., Vlantitila, M., Schmitt, C., et al.: ‘The quest for privacy in the internet of things’, IEEE Cloud Comput., 2016, 3, (2), pp. 36–45
[12] Ren, J., Guo, H., Xu, C., et al.: ‘Serving at the edge: a scalable IoT architecture based on transparent computing’, IEEE Netw., 2017, 31, (5), pp. 96–105
[13] Yang, Y., Wu, L., Yin, G., et al.: ‘A survey on security and privacy issues in internet-of-things’, IEEE Internet Things J., 2017, 4, (5), pp. 1250–1258
[14] Rana, U., Kulkarni, P., Sooryabandana, M.: ‘Low-power wide area networks: an overview’, IEEE Commun. Surv. Tutorials, 2017, 19, (2), pp. 855–873
[15] Sain, M., Kang, Y.J., Lee, H.J.: ‘Survey on security in internet of things: state of the art and challenges’, Proc. of Int. Conf. on Advanced Communication Technology, Jeju, South Korea, 2012, pp. 1699–1704
[16] Rana, M.M., Kim, J.: ‘LMS based blind channel estimation of SC-FDMA systems using variable step size and phase information’, Electron. Lett., 2011, 47, (5), pp. 346–348
[17] Rana, M.M., Kim, J., Cho, W.-K.: ‘Lms based adaptive channel estimation for LTE uplink’, Radioengineering, 2010, 19, (4), pp. 678–688
[18] Tauqife, A., Jaber, M., Imran, A., et al.: ‘Planning wireless cellular networks of future: outlook, challenges and opportunities’, IEEE Access., 2015, 7, pp. 4821–4845
[19] Rana, M.M., Hosain, M.K.: ‘Adaptive channel estimation techniques for MIMO OFDM systems’, Int. J. Adv. Comput. Sci. Appl., 2010, 1, (6), pp. 134–138
[20] Rana, M., Islam, M.S., Kouzani, A.Z.: ‘Peak to average power ratio analysis for LTE systems’, Proc. of Int. Conf. of Communication software and networks, Singapore, Shanghai, 2010, pp. 516–520
[21] Mehmood, Y., Ahmad, F., Yaoqib, I., et al.: ‘Internet-of-things-based smart cities: recent advances and challenges’, IEEE Commun. Mag., 2017, 55, (9), pp. 16–24
[22] Rana, M.M., Li, L., Su, S.W.: ‘Cyber attack protection and control in microgrids using channel code and semidefinite programming’. Proc. of Power and Energy Society General Meeting, Boston, MA, USA, 2016, pp. 1–5
[23] Tidjon, L.N., Frappier, M., Mammar, A.: ‘Intrusion detection systems: a cross-domain overview’, IEEE Commun. Surv. Tutorials, to appear in 2019
[24] Rana, M., Li, L.: ‘An overview of distributed microgrid state estimation and control for smart grids’, Sensors, 2015, 15, (2), pp. 4302–4325
[25] Kran, O., Becherer, M., Ayad, M., et al.: ‘States feedback control applied to the electric vehicle’, Energy Convers. Manage., 2014, 88, pp. 89–96
[26] Offati-Saber, R.: ‘Distributed Kalman filtering for sensor networks’. Proc. Conf. on Decision and Control, USA, 2007, pp. 5492–5498
[27] Rana, M.M., Li, L., Su, S.W.: ‘Controlling the renewable microgrid using semidefinite programming technique’, Int. J. Electric Power Energy Syst., 2017, 84, pp. 225–231
[28] Yao, L., Lim, W.H., Tsai, T.S.: ‘A real-time charging scheme for demand response in electric vehicle parking station’, IEEE Trans. Smart Grid, 2017, 8, (1), pp. 52–62
[29] Rana, M.M., Li, L., Su, S.W.: ‘An adaptive-then-combine dynamic state estimation considering renewable generations in smart grids’, IEEE J. Sci. Areas Commun., 2016, 34, (12), pp. 3954–3961
[30] Yang, Q., Jiang, L., Hao, W., et al.: ‘PMU placement in electric transmission networks for reliable state estimation against false data injection attacks’, IEEE Internet Things J., 2017, 4, (6), pp. 1978–1986
[31] Rana, M., Shuvo, M.R.: ‘Detection of primary user emulation attack in sensor networks’. Proc. of Int. Telecommunication Networks and Applications Conf., Sydney, Australia, 2018, pp. 1–6
[32] Said, D., Mouftah, H.T.: ‘Novel communication protocol for the EV charging/discharging service based on VANETS’, IEEE Trans. Intell. Veh., 2017, 2, (1), pp. 25–37
[33] Silva, R., Reis, J., Neto, L., et al.: ‘Universal parser for wireless sensor networks in industrial cyber physical production systems’. Proc. of Int. Conf. on Industrial Informatics, 2017, pp. 633–638
[34] Lin, Y.-W., Lin, Y.-B., Hsiao, C.-Y., et al.: ‘IoTtalk-RC: sensors as universal remote control for aftermarket home appliances’, IEEE Internet Things J., 2017, 4, (4), pp. 1104–1112
[35] Yaqoob, T., Abbas, H., Atiquzzaman, M.: ‘Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices–a review’, IEEE Commun. Surv. Tutorials, to appear in 2019
[36] Wu, C.K., Tsang, K.F., Liu, Y., et al.: ‘An IoT tree health indexing method using heterogeneous neural network’, IEEE Access., to appear in 2019
[37] Alam, M.G.R., Abedin, S.F., Moon, S.I., et al.: ‘Healthcare IoT-based affective state mining using a deep convolutional neural network’, IEEE Access., to appear in 2019
[38] Sun, Y., Meng, P., Zhou, Y., et al.: ‘Application of machine learning in wireless networks: key techniques and open issues’, IEEE Commun. Surv. Tutorials, to appear in 2019
[39] Zhang, C., Patras, P., Haddadi, H.: ‘Deep learning for LTE systems’. Proc. of Int. Conf. on communication software and networks, Bongpyeong, South Korea, 2017, pp. 699–704
[40] Qureshi, Z., Wang, R., et al.: ‘Healthcare IoT-based affective state mining using a deep convolutional neural network’, IEEE Access., to appear in 2019
[41] Aboelmaged, M., Abdelghani, Y., El Ghany, M.A.A.: ‘Wireless IoT based metering system for energy efficient smart cities’. Proc. of Int. Conf. on Microelectronics, Bari, Puglia, Italy, 2017, pp. 1886–1931
[42] Suresh, M., Muthukumar, U., Chandapillai, J.: ‘A novel smart water-meter based on IoT and smartphone app for city distribution management’. Proc. of Region 10 Symp., Cochin, India, 2017, pp. 1–5
Wang, Y., Zhang, J., Peng, F., et al.: ‘A glasses frame antenna for the applications in internet of things’, *IEEE Internet Things J.*, to appear in 2019

Rana, M.M., Khanom, R., Rahman, M.M.: ‘Design and analysis of Vivaldi antennas’, Proc. of Int. Conf. on Innovation and Engineering Technology, Dhaka, Bangladesh, 2019, pp. 1–5

AliHajri, M.I., Ali, N.T., Shubair, R.M.: ‘Indoor localization for IoT using adaptive feature selection: a cascaded machine learning approach’, *IEEE Antennas Wirel. Propag. Lett.*, 2019

Rana, M.M., Kim, J., Cho, W.-K.: ‘Low complexity downlink channel estimation for LTE systems’, Proc. of Int. Conf. on Advanced Communication Technology, Dhaka, Bangladesh, vol. 2, 2010, pp. 1198–1202

Rana, M.M.: ‘Channel estimation techniques and LTE terminal implementation challenges’. Proc. of Int. Conf. on Computer and Information Technology, Dhaka, Bangladesh, 2010, pp. 545–549

Rana, M.M.: ‘Attack resilient wireless sensor networks for smart electric vehicles’, *IEEE Sens. Lett.*, 2017, 1, (2), pp. 1–4

Zhang, H., Zheng, W.X.: ‘Denial-of-service power dispatch against linear quadratic control via a fading channel’, *IEEE Trans. Autom. Control*, to appear in 2018

Rana, M.M.: ‘Least mean square fourth based microgrid state estimation algorithm using the internet of things technology’, *Plos One*, 2017, 12, (5), p. e0176099

Casals, L.C., Garca, B.A.: ‘Communications concerns for reused electric vehicle batteries in smart grids’, *IEEE Commun. Mag.*, 2016, 54, (9), pp. 120–125

Battistelli, G., Chisci, L., Forti, N., et al.: ‘Distributed finite-element Kalman filter for field estimation’, *IEEE Trans. Autom. Control*, 2016, 62, (7), pp. 3309–3322

Vahidpour, V., Rastegarnia, A., Khalili, A., et al.: ‘Partial diffusion Kalman filtering for distributed state estimation in multiagent networks’, *IEEE Trans. Neural Netw. Learn. Syst.*, to appear in 2019

Ma, K., Liu, X., Liu, Z., et al.: ‘Cooperative relaying strategies for smart grid communications: bargaining models and solutions’, *IEEE Internet Things J.*, 2017, 4, (6), pp. 2315–2326

Rana, M.: ‘Architecture of the internet of energy network: an application to smart grid communications’, *IEEE Access.*, 2017, 5, pp. 4704–4710

Rana, M.M.: ‘Li, L., Su, S.W.: ‘Cyber attack protection and control of microgrids’, *IEEE/CIAJ Autom. Syst.*, 2017, 5, (2), pp. 602–609

Reani, A., Merthav, N.: ‘Universal quantization for separate encodings and joint decoding of correlated sources’, *IEEE Trans. Inf. Theory*, 2015, 61, (12), pp. 6465–6474

Kurt, M.N., Ogundijo, O., Li, C., et al.: ‘Online cyber-attack detection in smart grid: a reinforcement learning approach’, *IEEE Trans. Smart Grid*, to appera in 2019

Kim, J., Tong, L., Thomas, R.J.: ‘Subspace methods for data attack on state estimation: a data driven approach’, *IEEE Trans. Signal Process.*, 2014, 63, (5), pp. 1102–1114

Netto, M., Mili, L.: ‘A robust data-driven Koopman Kalman filter for power systems dynamic state estimation’, *IEEE Trans. Power Syst.*, 2018, 33, (6), pp. 7228–7237

Xu, G., Yu, W., Griffith, D., et al.: ‘Toward integrating distributed energy resources and storage devices in smart grid’, *IEEE Internet Things J.*, 2017, 4, (1), pp. 192–204

Rana, M.M., Li, L., Su, S.W.: ‘Distributed dynamic state estimation over a lossy communication network with an application to smart grids’. Proc. of Conf. on Decision and Control, Las Vegas, NV, USA, 2016, pp. 6657–6662

Shabani, F., Seyedzadeh, M., Vaziri, M., et al.: ‘State estimation of a distribution system using WLS and EKF techniques’. Proc. of Int. Conf. on Information Reuse and Integration, San Francisco, CA, USA, 2015, pp. 609–613

Rana, M., Li, L., Su, S.: ‘Kalman filter based microgrid state estimation and control using the IoT with 5G networks’. Proc. of PES Asia-Pacific Power and Energy Engineering Conf., Brisbane, Australia, 2015, pp. 1–5

Sun, Y., Lampe, L., Wong, W.V.: ‘Smart meter privacy: exploiting the potential of household energy storage units’, *IEEE Internet Things J.*, 2017, 5, (1), pp. 69–78

Miao, F., Zhu, Q., Pajic, M., et al.: ‘Coding schemes for securing cyberphysical systems against stealthy data injection attacks’, *IEEE Trans. Control Netw. Syst.*, 2017, 4, (1), pp. 106–117

Bretas, N.G., Bretas, A.S.: ‘The extension of the Gauss approach for the solution of an overdetermined set of algebraic non linear equations’, *IEEE Trans. Circuits Syst. II, Express Briefs*, 2018, 65, (9), pp. 1269–1273

An, L., Yang, G.-H.: ‘Decentralized adaptive fuzzy secure control for nonlinear uncertain interconnected systems against intermittent Dos attacks’, *IEEE Trans. Cybern.*, 2018, 49, (3), pp. 827–838

Arabali, A., Chalko, E., Etezadi-Amoli, M., et al.: ‘Short-term electricity price forecasting’, Proc. of Power and Energy System General Meeting, Vancouver, BC, Canada, 2013, pp. 1–5

Ding, L., Ge, Q.: ‘Electricity market clearing price forecast based on adaptive Kalman filter’. Proc. of Int. Conf. on Control, Automation and Information Sciences, Hangzhou, China, 2018, pp. 417–421

Bisong, D., Klein, M.T., Chinnathambi, R.A., et al.: ‘A hybrid regression model for day-ahead energy price forecasting’, *IEEE Access.*, 2019, 7, pp. 36833–36842

Rana, M., Xiang, W., Wang, E.: ‘H-infinity-based microgrid state estimations using the IoT sensors’, *Smart Power Distrib. Syst.*, 2019, 14, pp. 285–295

Simon, D.: ‘Optimal state estimation: Kalman, H infinity, and nonlinear approaches’ (John Wiley & Sons, USA, 2006)