Internet of things for smart grid automation

Abstract

The Internet of Things (IoT) is applied to many areas such as smart grid, air conditioning system, smart agriculture and transportation systems.\(^1\)\(^-\)\(^2\) The main component of IoT framework is the wireless sensor networks. Basically, the energy management system uses the sensing information to estimate the microgrid states so that the power system situation awareness and security will be enhanced.\(^3\)\(^-\)\(^5\) The weighted least squared based AC state estimation is presented in.\(^6\) In Salinas,\(^7\) proposes a Kalman filter (KF) based centralized energy theft detection algorithm. In Keller,\(^8\) proposes a modified unknown input KF algorithm for the state filtering of network controlled systems subject to random cyber attacks. All the KF based approaches are required to know the exact noise statistics which are generally unknown at the energy management system. In fact, the H-infinity based micro grid state estimation is proposed in Rana,\(^9\) but it does not analysis the estimation performance considering sensor faults and large disturbances. Motivated by the aforementioned analysis, this paper proposes an H-infinity based micro grid state estimation using the IoT embedded sensors. The bold case upper and lower letters are used for matrix and vector notations.

Micro grid and IoT enabled sensors

Generally speaking, the micro grid provides clean, green and sustainable energy to the user.\(^6\)\(^-\)\(^9\) In the distribution power system, the micro grid is connected to the feeder circuit. To illustrate, Figure 1 shows a distribution test feeder where the distributed energy resource (DER) is connected to the Point of Common Coupling (PCC) through coupling inductor. Basically, the DER is represented by voltage source Vs which is connected to the PCC whose bus voltage is denoted by Vb. The coupling inductor exists between them. After applying KVL, KCL and discretization process, the discrete-time state-space framework is written as follows:

\[
s(t+1) = Fs(t) + Bu(t) + v(t) \tag{1}
\]

Where F is system state matrix, s(t) is the system state, B is the input matrix, u(t) is the system control effort, and v(t) is the system noise whose covariance matrix is Q(t). The detail parameters are given in Figure 1. The measurement from the IoT embedded sensor is given by:

\[
z(t) = Hs(t) + w(t) \tag{2}
\]

Where z(t) is the measurement information, H is the sensing matrix and w(t) is the noisy measurement whose covariance matrix is R(t). Basically, the sensing measurement is used for state estimation at the energy management system. In the energy management system, the H-infinity filter is applied for state estimations.\(^7\)\(^-\)\(^9\)\(^10\)\(^-\)\(^13\)

Simulation results

Considering typical parameter in,\(^10\)\(^-\)\(^11\) the simulation result is presented in Figure 2. Figure 2 shows the PCC voltage deviation at bus 1 and its estimation result. It is observed that the H-infinity can able to estimate the system state within 20 iterations. Other system states have almost similar estimation performance.
Conclusion and future work

This article proposes an H-infinity based micro grid state estimation algorithm using the IoT based sensors. After representing the micro grid in a state-space framework, the IoT enabled smart sensors are deployed to obtain the sensing state information. In the energy management system, an H-infinity based optimal filtering approach is adopted and verified through numerical simulations. It shows that H-infinity algorithm can able to estimate the micro grid states. In future, we will also apply the control algorithm to stabilize the micro grid states.

Acknowledgments

No acknowledgement.

Conflict of interest

No conflict of interest.

References

1. Pacheco J, Hariri S. IoT security framework for smart cyber infrastructures. International Workshops on Foundations and Applications of Self Systems. 2016. p. 242–247.
2. Shinohara T, Namerikawa T. Manipulative zero–stealthy attacks in cyber–physical systems: Existence space of feasible attack objectives. Conference on Control Technology and Applications. 2017. p. 1123–1128.
3. Zhou Y, Miao Z. Cyber attacks, detection and protection in smart grid state estimation. North American Power Symposium. 2016. p. 1–6.
4. Hug G, Giampapa JA. Vulnerability assessment of AC state estimation with respect to false data injection cyber–attacks. IEEE Transactions on Smart Grid. 2012;3(3):1362–1370.
5. Salinas SA, Li. Privacy–preserving energy theft detection in micro grids: A state estimation approach. IEEE Transactions on Power Systems. 2016;31(2):883–894.
6. JY Keller, D Sauter, K Chabir. State filtering for discrete–time stochastic linear systems subject to random cyber attacks and losses of measurements. Mediterranean Conference on Control and Automation. 2012. p. 935–940.
7. Rana M. Architecture of the internet of energy network: An application to smart grid communications. IEEE Access. 2017;5:4704–4710.
8. Myeong–Jun J, Kyeong–Hwa K. Control of power electronic converters for efficient operation of micro grid consisting of multiple dg units and ess. DES tech Transactions on Engineering and Technology Research. 2017.
9. Salas–Puente R, Marzal S, Gonzalez–Medina R, et al. Experimental study of a centralized control strategy of a dc micro grid working in grid connected mode. Energies. 2017;10(10):1627.
10. Korukonda MP, Mishra SR, Shukla A, et al. Handling multi–parametric variations in distributed control of cyber–physical energy systems through optimal communication design. IET Cyber–Physical Systems: Theory and Applications. 2017;2(2):90–100.
11. Li H, Lai L, Poor HV. Multicast routing for decentralized control of cyber physical systems with an application in smart grid. IEEE Journal on Selected Areas in Communications. 2012;30(6):1097–1107.
12. Simon D. Optimal state estimation: Kalman, H infinity, and nonlinear approaches. USA: John Wiley and Sons; 2006. p. 1–552.
13. Allen R, Lin KC, Xu C. Robust estimation of a manoeuvring target from multiple unmanned air vehicles’ measurements. Collaborative Technologies and Systems IEEE. 2010.

Citation: Masud RM. Internet of things for smart grid automation. Int Rob Auto J. 2017;3(5):359–360. DOI: 10.15406/iraq.2017.03.00070