Abstract

Modern Smart Home Energy Management Systems (SHEMSs) are inherently prone to cyber-attacks due to their high exposure to the Information and Communication Technology (ICT), thereby requirement of scheduling schemes resilient to cyber-attacks is important. Further, current scenario of SHEMS may result in increased charging and discharging cycles deteriorating the battery life. Therefore, demand scheduling formulations also need to cater the effect of battery degradation cost along with user comfort. The present work attempts to formulate a comprehensive scheduling problem in terms of energy cost minimization considering the battery degradation cost. Further, a cyber-attack resilient scheduling model is proposed in the present study. This work investigates the effect of demand scheduling on the life span of battery as well as the energy cost. Further, False Data Injection (FDI) attack has been modelled using machine learning techniques, and its effects on the scheduling has been incorporated in the objective function. Scenario tree based stochastic bill generation has also been formulated to develop an FDI attack resilient scheduling. Optimisation results of the study have established that the resulting formulation is robust against FDI attacks.

A game-theory based optimal and cyber-attack resilient energy scheduling in multiple smart buildings framework considering FDI attack has been proposed in this work. The proposed resilient scheduling is based on the consumers' past behaviour, and import and export power between the smart buildings and grids. An optimal resilient energy scheduling framework is designed considering Renewable Energy Sources (RESs), Combined Heat and Power (CHP) generators, Battery Storage Systems (BSSs), various Smart Home (SH) appliances and FDI attack. An iterative algorithm is used to solve a game-theory based Mixed Integer Quadratic Constrained Program (MIQCP) problem in General Algebraic Model System (GAMS) environment with a CPLEX solver. For identifying the FDI attack and making a resilient scheduling against possible attacks, the proposed technique

uses the difference between the actual and forecasted bills as well as maximum change in demand. The impacts of FDI attack which can be detrimental can be avoided, however, there may be a small difference between energy cost without considering attack and energy cost with considering resilient scheduling.

Further, the proposed resilient scheduling also been formulated for interconnected multiple smart buildings having power exchange capability among themselves. It is considered that each smart building is equipped with different types of Distributed Energy Resources (DERs), BSSs, CHP generators, Thermal Storage Systems (TSSs) and smart appliances.

Thus, in this work, a comprehensive optimal and robust scheduling is formulated to mitigate the effects of FDI attacks. The proposed method uses the information of anomaly between the actual and forecasted bills for detecting the cyber attack and making a resilient scheduling against possible attacks.