Electrical Power and Energy Systems 62 (2014) 540–548

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

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

A real-time management and evolutionary optimization scheme for a secure and flexible smart grid towards sustainable energy

D. Vijayakumar [a,*], V. Malathi [b]

[a] Electronics and Communication Engineering, Lathamathavan Engineering College, Alagarkoil, Tamil Nadu, India
[b] Electrical and Electronics Engineering, Anna University Regional Centre, Madurai, Tamil Nadu, India

ARTICLE INFO

Article history:
Received 10 December 2013
Received in revised form 22 April 2014
Accepted 10 May 2014
Available online 5 June 2014

Keywords:
Critical time
Control center
Distributed state estimator (DSE)
Fault distance
Genetic Algorithm (GA)
Reactive power

ABSTRACT

Sustainable energy is the energy production without compromising the energy production for the future generations. The existing power grid model does not provide real-time information of transmission devices, security during emergency events, and frequency and voltage control. The proposed scheme consists of location-centric hybrid system architecture for the coordinated processing among proximate devices. The neighboring devices follow a collaboration algorithm to handle faulty and incomplete information. The proposed scheme also consists of distributed algorithm for the maintenance of the local state of the smart grid and a real-time accessibility control of transmission devices. The security of the system can be guaranteed by reconfiguration through power-electronics and switches. An embedded intelligence is inserted into the power-electronics to facilitate the reconfiguration of the system, and thereby ensuring security. A generalized optimization formulation determines the optimum location of the transmission devices. In this paper, Genetic Algorithm (GA) is used to handle the reactive power management. The use of GA decreases execution time of resource scheduling. This method performs better than the existing power grid models in terms of fault detection, degree of power saving due to power optimization, memory usage, consumer-GW (gateway) communication overhead, consumer computational overhead, and critical time.

Introduction

THE SMART GRID is an evolution of the electrical grid to a flexible power network through distributed intelligence, automated control systems, and communication technologies. The power management techniques must yield sustainable energy; although there is increasing power blackouts due to the excessive power consumption. The demerits in the existing power grid models occur at the system level and local level. The control area operators in the power grid cannot, obtain the real-time information about the transmission devices, respond quickly to emergency events (or) blackouts, and perform the functions in an automated and coordinated manner. The conventional hardware used in the electrical grid lacks the frequency and voltage control according to the increasing system requirements, and cannot secure the system quickly during emergency events. A real-time coordination scheme enhances the coordination among the geographically separated devices during power blackouts.

The energy resources in the transmission systems must be efficiently utilized over the conventional high-energy resources to increase the reliability of the power system. The security of a power grid is mainly focused on dynamic and transient stability issues. The power systems can also crash via physical interconnection even when the communication system is secure. A controller can be compromised due to destabilization and higher response to minor load variations. A security control can be designed by providing a feedback for the detection and isolation of information flow targeted attacks. The information collaboration and feedback to the perfect generator units may isolate the offence unit of the system.

The attacks on the power grids may partially compromise the secure communication or fully control some of the system components. Multiple lines of defense must be designed in a power grid system. It needs to fulfill the following goals:

- Accurate detection of attacks depicted as current, voltage, or frequency changes.
- Distributed processing at the local level and robust collaboration between the grid devices.
- Protection of the system against collapse.

---

* Corresponding author. Tel.: +91 4526454125; fax: +91 0452 247 0570.
E-mail address: vijayakumarphd2013@hotmail.com (D. Vijayakumar).

http://dx.doi.org/10.1016/j.ijepes.2014.05.013
0142-0615/

Location-centric hybrid system architecture is chosen for the cooperative processing among neighboring devices. The electrical devices in the power grid follow a collaboration algorithm to address the faulty and incomplete information. A distributed algorithm is used for the real-time accessibility control of transmission devices and the maintenance of the local states of the smart grid. The reconfiguration of the grid via power-electronics and switches enhance the security of the electrical grid. An embedded intelligence is fixed into the power-electronics to enable the system reconfiguration. An evolutionary algorithm like Genetic Algorithm (GA) is chosen to address the reactive power management and optimum transmission device placement. The execution time of the resource scheduling is decreased by the optimization of GA.

This method performs better than the existing power grid models in terms of fault detection, degree of power saving due to power optimization, memory usage, consumer-GW (gateway) communication overhead, consumer computational overhead, and critical time. The existing methods taken for comparative analysis are fault detection and classification using Functional Analysis and Computational Intelligence (FACI), Efficient and Privacy-Preserving Aggregation (EPPA) scheme, Lightweight Message Authentication (LMA) scheme, Multi-terminal DC Wind farm collection Internal Fault Analysis (MDWIFA), and traditional scheme (TRAD) without any data aggregation.

The remaining part of the paper is organized as follows: Section 'Related work' involves the works related to the security enhancement and optimization in a power grid. Section 'Requirements for a secure power grid' involves the requirements for a secure power grid. Section 'Real-time management and evolutionary optimization scheme for a secure and flexible smart grid (RMOSFS)' involves the detailed description of the proposed real-time management and optimization scheme for a secure and flexible smart towards sustainable energy. Section 'Performance analysis' involves the performance analysis and comparison of the existing and proposed security enhancement and optimization techniques in a power grid. The paper is concluded in Section 'Conclusion'.

Related work

This section deals with the existing secure and optimized power grid models. A smart grid is a modern electrical grid infrastructure for higher efficiency and reliability via automated control, modern communications, sensing, high power converters, metering technologies, and energy management schemes [1]. The recent smart grid management and protection systems were surveyed by [2,3]. These smart protection systems enhanced the reliability and security of the smart grid. The suitability of Attribute Based Encryption (ABE) was analyzed for the security of smart grids [4]. A key policy based ABE was applied at the smart grid's control center, where an encrypted message was broadcast to a defined group of users. This eliminated the requisite for multiple unicast message broadcast, which further ensured the computation and communication efficiencies.

Miao and Junshan proposed a dependency graph based fault detection and localization towards secure smart grid [5]. The phasor angles across the communication links were modeled as a Markov random field (MRF), whose conditional correlation coefficients were measured in terms of physical properties of power systems. A multiscale network interference algorithm was devised to detect and localize the faults in a decentralized manner. Fouda et al. designed a Lightweight Message Authentication technique for smart grids [6]. The smart meters were distributed at various hierarchical smart grid networks. A shared session key was established between a hash-based authentication code and the smart meters. Young–Jin et al. formed a data-centric, decentralized and secure information infrastructure for smart grid [7]. The secure middleware architecture can coexist with both LAN and WAN. Rodri et al. used a grid synchronization algorithm for three-phase grid-connected power networks [8]. This method is based on two adaptive filters designed using a dual second-order generalized integrator (SOGI).

Chouder and Silvestre implemented automatic and supervisory fault detection technique on the Photo–Voltaic (PV) systems of the smart grid [9]. The fault detection is based on analysis of power losses. Budischak et al. modeled the cost-minimized combinations of various renewable energy sources in smart grid to power up the grid up to 99.9% of the time [10]. The essential cyber security issues in a smart grid infrastructure were dealt in [11–13]. A layered approach was introduced to evaluate the risk on physical power applications and cyber infrastructure. A classification was performed to highlight the dependencies between the cyber-physical smart grid controls. Huimin et al. designed a protection scheme for smart MVDC (Medium–Voltage DC) grid [14]. The self-healing ability against the measurement faults in power systems and protection systems enhances the fault resilience of the power grid. This method efficiently handles both measurement system fault and power system fault.

Rongxing et al. proposed an Efficient and Privacy-Preserving Aggregation methodology for securing the smart grid communications [15]. This method encrypts the multi-dimensional data using a homomorphic Paillier cryptosystem technique. The authentication cost was significantly reduced by using a batch verification method. Calderaro et al. detected and localized the failures in smart grids using petri net (PN) modeling [16]. The detection of faults was modeled as matrix operations. This method enabled the fault identification the strong effect of distributed generation. Ui–Min et al. formulated open-switch fault detection in a grid-connected NPC (Neutral-Point-Clamped) inverter system [17]. This technique also determined the location of the fault besides detecting them. The fault condition was detected depending on the Concordia current pattern radius. The detection scheme does not require any additional sensors and identified the faulty switches within two fundamental periods.

Jin et al. modeled a multi-terminal DC wind farm collection grid with protection design and internal fault analysis [18]. This method focused on DC faults and their transients. Lee et al. used quantum Genetic Algorithm (QGA) for solving the issue of economic dispatch in wind power generation of smart grids [19]. The QGA implemented quantum bit coding where the population of individuals contained an inherent diversity. The fittest solution for the optimization problem was easily obtained because the initial population did not have the need to be large to attain the consequence of species diversity. Lima et al. presented a control mechanism for the rotor-side converter (RSC) of wind turbines (WTs) during grid faults [20]. The power system faults in doubly fed induction generators (DFIG) were detected to control the initial overcurrent's during the voltage saps. Katuri et al. designed an approach for reactive power optimization with voltage stability objective using Genetic Algorithm (GA) [21]. Reactive power optimization in the power system aims to maintain good voltage profile by enhancing the voltage quality other than decreasing the power loss. Ela et al. suggested a differential evolution algorithm for optimal reactive power research [22]. In this paper, a differential evolution (DE) optimization algorithm has been developed and applied to solve Reactive Power Dispatch (RPD) problem. Ali et al. [23] presented a fuzzy logic based system that monitors and controls Heating, Ventilation and Air-Conditioning Systems (HVACs) units, where demand exceeds the supplied electrical power.

The proposed method performs better than these existing power grid models in terms of fault detection, degree of power