Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics
San Antonio, TX, USA - October 2009

An Autonomous Agent-based Framework for Self-Healing Power Grid

Zeinab Noorian
Department of Computer Science
University of New Brunswick
Fredericton, Canada
z.noorian@unb.ca

Hadi Hosseini
Department of Computer Science
University of New Brunswick
Fredericton, Canada
h.hosseini@unb.ca

Mihaela Ulieru
Canada Research Chair
Faculty of Computer Science
University of New Brunswick
Fredericton, Canada
Ulieru@unb.ca

***Abstract*—Reliable, secure and robust power grid network is a necessity for crucial financial, industrial and business networks. Since national electrical grid, telecommunication, information networks and transportation networks are interdependent critical infrastructures, having an agent-based self-healing framework to reduce cascading failures through the networks and finding reasonable solution for potential faults – would be an essential asset. In response to this need we propose a self-healing framework that employs advanced failure diagnosis techniques along with autonomous web services to provide temporary recovery solutions. Furthermore, it provides a cognitive planning cycle to find ultimate corrective solutions as well as evaluation service to verify the effectiveness and performance of the final solution.**

***Keywords*—power grid, Autonomous web service, hierarchal self-healing framework,Failure detection.**

I. INTRODUCTION

Demand for electricity has increased steadily for decades, yet power generating strategies of renewable and non-renewable power plants or consumption methods of different individual or industrial users have not been upgraded at the same pace. As a result, the power grid has become overloaded, making it more prone to blackouts, which have risen in number, severity and cost in annual economic losses. Since modern infrastructure systems are highly interdependent, a change in conditions at any one location can have immediate impacts over a wide area and the effect of a local disturbance can be magnified as it propagates through a network. Large-scale cascading failures can occur almost instantaneously with consequences in remote regions or seemingly unrelated businesses [2, 5]. To address this problem we propose a self-healing framework which endows the power grid with self-awareness and enable it to identify emerging vulnerabilities in order to reconfigure itself to attain resilience for different types of failures [1].

The proposed self-healing framework for intelligent power grid has primary characteristics as follows:

It provides real-time monitoring and reactive services that are performed by arrays of sensors which notify slight changes in power plants to a dedicated agent in order to verify the potential problems that could trigger larger disturbances. In fact, this agent hinders insignificant trouble signs from getting distributed in the network.

The other fundamental characteristic of the proposed self-healing framework is taking advantage of Autonomic Web Services in identifying the temporary corrective solutions as a first aid action in order to prevent the system from blackout even for a short period of time.

In addition, it can find a long term optimized solution for failure recovery among several available solutions by taking system policies and dynamic parameters into account.

The rest of the paper is organized as follows: the related work is presented in section II; section III introduces the self-healing framework for power grid. In section IV, we explain failure detection and recovery techniques in self-healing power grid and present the self-healing solution in detail. A scenario of how the proposed framework works is described in section V. Finally, we conclude the discussion in the last section.

II. RELATED WORK

In [8, 10], the three layered self-healing infrastructure is proposed. It provides preprogrammed self-healing actions which are performed by reactive

978-1-4244-2794-9/09/$25.00

agents in bottom layer. The reactive nature of this layer is unable to proactively adapt its final decisions and actions with unexpected conditions. A suitable recovery plan is developed in the top layers using perceptive information.

Subsequently, in [11], the multilayered Strategic Power Infrastructure Defense (SPID) architecture is presented which support adaptive self-healing and protection strategies. One of the main features of this infrastructure is providing Dynamic Decision Event Tree (DDET) component which contributes in analysis and control of self-healing actions like controlled islanding in case of a progressive damage through the network.

Moreover, the [12] presents a scalable and modular framework for high performance computing and communication infrastructure to support a self-healing grid. It is based on distributed autonomous architecture and includes various functions such as data acquisition and maintenance, monitoring, performance and reliability enhancement as well as on-line analytical capabilities like forecasting, dynamic analysis and ATC calculation.

Finally, the [13] proposed the flexible event-based software architecture to create a self-healing system. This framework offers a significant degree of loose coupling and autonomy of components. It provides run-time adaptation capabilities for the creation, analysis and execution of repair strategies on software systems.

Meanwhile, due to the fact that in most cases, the planning cycle is time consuming and may result in blackouts for a specific period of time, in the proposed self-healing framework we underscore an autonomous service to address this issue by providing a temporal self-healing recovery solution. The autonomous agent manager provides an inspection and analysis on received data from sensor agents to identify an attack or false report that may happen as a result of malicious activities.

III. THE PROPOSED SELF-HEALING FRAMEWORK

Our proposed hierarchal self-healing framework (Fig. 1) is based on a four-layered architecture: Reactive, Diagnosis, Evaluation, and Cognitive layer. The reactive layer is composed of sensor agents that are responsible to notify the middle layer about any changes in the environment particularly in energy resources or power plants. Each sensor agent monitors predefined renewable and non-renewable energy resources such as thermal power stations, solar power plants, hydro-electric power stations, fossil fuel power plants, etc.

The diagnosis layer is responsible to detect and analyze failures and propose the temporary solution for failure recovery as a first aid action in order to prevent blackouts even for a short period of time. Moreover, it will notify the top layers with the detailed descriptive information to determine the ultimate solution for failure recovery and prevent any further cascading damage to the power system.

The evaluation layer is responsible for validation and verification of a proposed recovery plan that is received from the top layer. Changes to the status of the system after failure detection are set by a Crisis Measurement Agent (CMA) in order to display the current condition of the power grid.

The cognitive layer of the proposed architecture is the actual processor of the system as it creates the final solution. All the preferences, policies and intentions of the system are defined in this layer so it can make new decision according to the perceptions that it gets from other layers. As failures may cause unexpected conditions, various solutions should be recommended to match the problem.

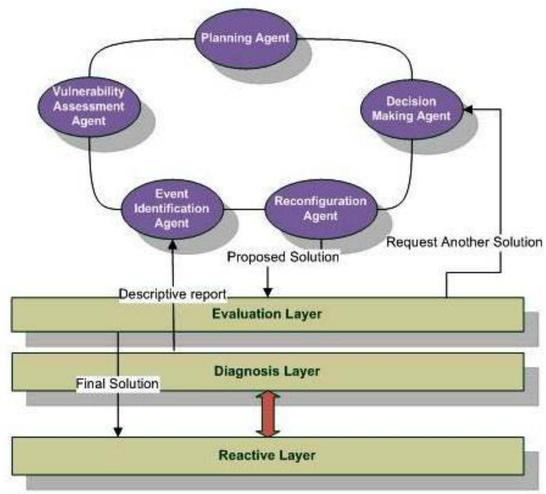

Figure 1.Cognitive layer architecture

As depicted in Figure 1, when the diagnosis layer detects a failure, it transmits a brief report of failure to the CMA. Immediately, this agent changes the status flag from green to red expressing current system status to the outside. Then it registers the failure report in the History Knowledge Base in order to be logged for further references. Simultaneously, the diagnosis layer sends a descriptive report of failure to the cognitive layer. In this layer, the Event Identification

Agent (EIA) decodes and analyzes this report to find out all the detailed information including criticality of failure, type of failure, exact location of failure and etc. This information is then sent to the Vulnerability Assessment Agent (VAA) to measure up its consequences to the whole power system. For example, crucial failures should be fixed on time and may need a system restart to prevent any more damages. Next, the failure information is sent to the Planning agent to originate solutions to handle the failure. Given the same information about the failure, the planning agent may recommend various solutions. Furthermore, by having utilities and probabilities assigned to each policy (solution), the Decision Making Agent (DMA) assesses these various solutions and passes the most optimum solution for that specific failure to the Reconfiguration agent. Then, reconfiguration agent recommends new system configuration for the proposed solution in order to make it adaptable to the current state.

Finally, all gathered information is forwarded to the Evaluation agent. The evaluation agent measures the effectiveness of this proposed solution by comparing all the parameters of the current state with all the estimated parameters of the system after applying the solution to the system. If the results from the evaluation agent meet our pre-specified system thresholds (like security, reliability and robustness) this solution will be sent to a mobile action agent to fix the problem, otherwise, another solution will be requested from the cognitive layer.

IV. DETAILED DESIGN

A. Failure Detection and Recovery in the Self-Healing intelligent Power Grid

Any change in the environment triggers data-gathering sensor agents in the reactive layer which are constantly monitoring and tracking failures in power resources.

As soon as any slight change or unexpected event is detected in energy resources, they are forwarded to the Observer Agent Manager (OAM) together with relevant information. Note that, OAM is responsible for diagnosis, analysis and management of received data and is always being updated by the Information Server (IS). (Fig. 2)

To elaborate, IS contains comprehensive information about weather forecast, resource availability, production capacity, states of other power stations, resource allocation policy, etc. It includes statistical information about energy resources (nuclear, fossil fuel, and renewable resources) and governmental policies such as priority of using one resource over the other. For instance, burning of fossil fuels for producing electrical energy has an adverse effect on global warming [9]. As a result, government policy may dictate not to consume these energy resources unless in a critical situation.

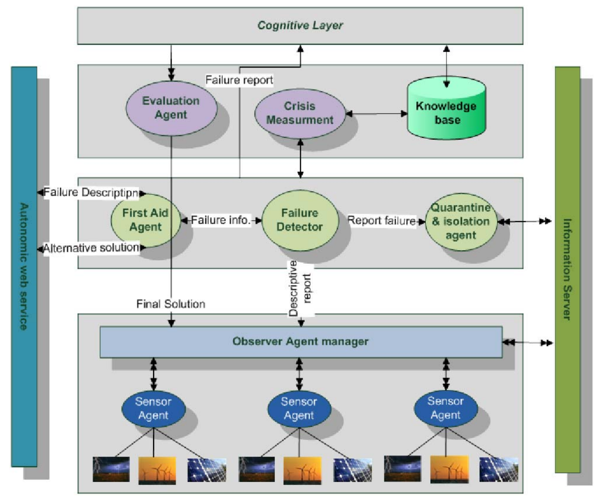

Figure 2. Failure Detection Mechanism

OAM analyzes and verifies the information obtained from sensor agents by accessing the IS in order to alert the Failure Detection Agent (FDA) about any non trivial faulty behavior in the system. Introducing an OAM to handle all the transactions with the higher levels prevents any false notifications and makes a robust integrated system.

In the diagnosis layer, the FDA comprehends the received report and splits it up in order to dispatch among respective correspondent agents. The FDA forwards the information about the type, location and detailed available description to a First Aid Agent (FAA) while it sends accurate information about the location of failure to a Quarantine & Isolation Agent (QIA). Furthermore, it sends the complete failure information to the cognitive layer that is responsible to process it and generate solutions as discussed in previous section.

When the FAA receives the failure information it communicates with the corresponding Autonomic Web Services (AWS) to provide a temporary self-healing solution, as will be detailed in the following section.

Besides, when the QIA receives the failure information, it will choose a strategy for hindering the failure from cascading throughout the interdependent networks. For example, the whole network would break into isolated "islands," each of which must reorganize their power plants and transmission flows in the most optimized manner. Although this might cause voltage fluctuations or even small outages, it would prevent error cascading that causes the major blackouts. As the failures are being repaired, each recovered island smoothly rejoins from the larger network. [2, 5]

B. Failure Analysis by Observer Agent Manager

The OAM (Fig. 2) has the main responsibility in the reactive layer. This component works as a Filter by restricting the diffusion of data to the upper layers. It is equipped with decision making capabilities to verify the significance of the report that is received from sensor agents. Because of the sensitivity of sensor agents, one particular sensor agent may reflect slight environmental change (such as a short-time interruption in wind power) to the OAM. In this case, the OAM is responsible to examine the adverse consequences of this interruption by accessing the IS (e.g. fetching weather forecast information). If OAM realizes that the received data does not have a serious impact on the system (e.g. the weather forecast system indicates that the interruption in wind is temporary) it prevents propagation of this insignificant alert to the upper layers.

On the other hand, some internal failures (like; virus attack, information loss, system failures, etc) may cause some changes in sensor agents' report, therefore, the OAM should continuously examine and analyze responses of the sensor agents to find any suspicious and paradoxical behavior. First, via 'software rejuvenation' [6] it will refresh the state of that sensor by sending some remote commands; If chaotic behavior of that particular sensor persists, the OAM interacts with the upper layer to report potential failure in sensor agent to the FDA .

C. Using Autonomic Web Service to find a temporary self-healing solution for the Power Grid

We envision that Autonomic Web Service in power grids is responsible to provide temporary self-healing solution in order to enable FAA to react upon unexpected failures and prevent blackouts even for a short period of time. (Fig. 3)

In case of a failure, the FAA sends out the failure information to the AWS through the *AgentWeb Gateway Middleware* which is designed for interoperation of software agents and web services [3]. AWS consists of two engines: an Analyzer engine which is designed to identify failure's type and specification and then recommend appropriate recovery solutions. This engine accesses a Symptom database [4] which is an XML file containing symptoms description and relative recovery actions being updated by the IS . By looking up the Symptom database, one or more directives will be found and forwarded to the second engine called Solution engine. The Solution engine uses a Policy Database [4]-which maintains high-level policy of the system-

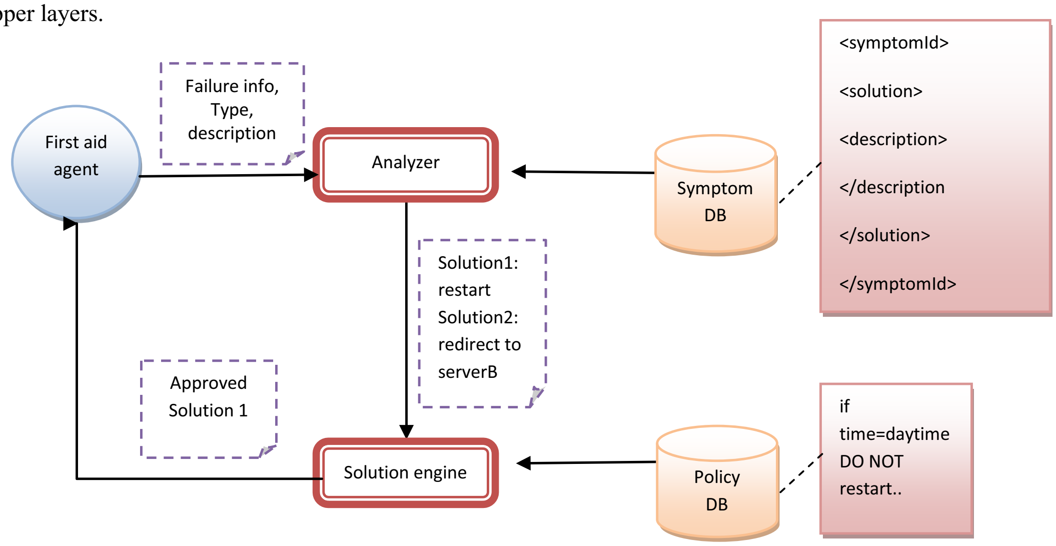

Figure 3. AWS mechanism for finding temporary recovery solution

to match the recommended actions by the Analyzer engine towards system policies in order to ensure no action will have a negative impact on critical system components. Finally, this engine will send an approved solution to the FAA to be applied in the power grid. (Fig. 3)

V. SCENARIO: HOW THE PROPOSED SELF-HEALING FRAMEWORK WORKS

Let's consider the following scenario:

Suppose that the sensor agent in a wind power station informs the OAM of a malfunction, like reduction in wind power. First, the OAM validates the report by sending a request to the IS to retrieve weather forecast information. If the problem is found to be serious, the IS information with descriptive failure report is sent to the upper layer where it triggers the FDA. (Fig. 2)

The FDA examines the report and extracts required information to distribute among the relative agents. In this example, information about the location and sensorID of malfunctioned sensor agent is being sent to QIA. Since this agent is responsible to prevent disturbance from cascading, isolation mechanisms are used to surround the infected area and prevent propagation of the failure throughout the network.

In parallel, an XML file containing full description, event message and type of the failure is forwarded to the FAA. When this agent is alerted by failure information, it invokes AWS to find a temporary self-healing solution in order to prevent the system from interruption even for a short period of time.

Figure 3 demonstrates that the failure type and description are sent to Analyzer engine which is responsible to get appropriate solutions using the Symptom database which suggests various solutions (such as balancing energy consumptions between users, diverting the users in the respective zone to another power station, etc). These available solutions will be forwarded to the Solution engine in order to make a final decision according to the Policy database. For Instance, if the system is capable of balancing the consumption of the energy between blacked-out users in order to prevent a complete blackout (e.g. each user could have minimal electricity for critical consumption), the system is more likely to use this solution. It is noteworthy to mention that this solution requires users to enroll their critical sections to the correspondent station in advance. For example, a university should register its security system in town's station to avoid any blackout for that particular section. However, diverting blacked-out users to other available power stations has its own advantages that are considered by the system policy. Note that, as soon as the temporary recovery solution is received by the FAA, it will be applied to the power grid network.

The detailed description of the failure will be sent to the EIA in the cognitive layer for ultimate self-healing solution. This agent decodes the type and failure description and sends this information to the VAA. Due to the fact that this type of failure cannot lead to serious damage to the whole power system, this agent does not take any serious action (like restarting the system) and just redirects this information to the planning agent. In this step, various solutions will be offered by the planning agent such as: using spare resources like fossil fuel or utilizing multiple distributed stations in order to provide specific amount of power for blacked-out users.

Subsequently, these proposed solutions will be forwarded to the DMA in order to finalize the optimized solution according to predefined system parameters such as robustness, compatibility and security. The utility of these parameters in the system is determined based on previous experiments or statistical data. This agent identifies corrective solutions, simulates the effectiveness of each solution, and presents the most suitable response to the reconfiguration agent. Assume that the first proposed solution is using spare resources. If this agent realizes that the population of users of the blacked-out area is not negligible or blackout occurred in critical commercial or industrial zones, using fossil fuels will be preferred over redirecting users to multiple distributed stations. Besides, using spare resources provides more robustness and reliability over other available solutions. On the contrary, for the environmental matter and global warming issues, the power system will redirect blacked-out users to distributed stations [9] (e.g. by sending a request to other stations in order to make sure they could increase their production capacity by some specific percentage to satisfy the newly added consumer requirements)

Once the optimized solution is received by the reconfiguration agent, the system adaptation requirements are added to the final solution. Finally the ultimate solution is forwarded to the evaluation agent to measure the performance and effectiveness of the proposed solution. If it satisfies the system thresholds, it will record the solution in History Knowledge Base and generate a mobile action agent to execute the solution on the affected areas. Otherwise, the deficiency of the proposed solution is sent back to the DMA to request another solution.

VI. CONCLUSION

We have proposed an adaptive self-healing framework for power grids based on intelligent agent technologies. The agent-based self-healing smart grid is endowed with awareness and self- reconfigurability to reduce blackouts dramatically. It can sense local problems early, and automatically fix or isolate them before they propagate through the power network.

This multi-agent framework provides a sustainable and coherent engine using deliberative and proactive agents to model an integrated whilst loosely-coupled system.

Since in this paper we have only considered failures in the power network, as a future work we plan to look into the system failures in the agents and components within the framework. Moreover, suitable simulations will be implemented in order to evaluate the applicability of this framework.

REFERENCES

[1] Mihaela Ulieru, e-Networks in an Increasingly Volatile World: Design for Resilience of Networked Critical Infrastructures, The Inaugural IEEE International Conference on Digital Ecosystems and Technologies - IEEE-DEST 2007 - Cairns, Australia, 21-23 February 2007, 540-545.

[2] M.Amin, For the Good of the Grid: Toward Increased Efficiencies and Integration of Renewable Resources for Future Electric Power Networks. , IEEE Power & Energy Magazine, Vol. 6, Number 6, pp. 48-59, November/December 2008

[3] M.O. Shafiq, Y. Ding, and D. Fensel, "Bridging M ulti Agent Systems and Web Services:

towards interoperability between Software Agents and Semantic Web Services", in Proc. EDOC, 2006, pp.85-96.

[4] SA urguis Towards autonomic web services: Achieving self-healing using web services, A Zeid – ACM SIGSOFT Software Engineering Notes, 2005 - portal.acm.org

[5] Amin and Schewe,"Preventing Blackouts," Scientific American, pp. 60-67, ww.Sciam.com, May 2007.

[6] LM Silva, V Batista, JG Silva, Fault-tolerant execution of mobile agents - Dependable systems and Networks, 2000. DSN 2000. Proceedings 2000 - ieeexplore.ieee.org

[7] SM Rinaldi,Modeling and simulating critical infrastructures and their interdependencies System Sciences, 2004. Proceedings of the 37th Annual Hawaii 2004 - ieeexplore.ieee.org

[8] Amin, Toward Self-Healing Energy Infrastructure Systems, cover feature in IEEE Computer Applications in Power, pp. 20-28, Vol. 14, No. 1, January 2001

[9] J Hansen, M Sato, R Ruedy,A Lacis,V Oinas, Global warming in the twenty-first century: An alternative scenario - Proceedings of the National Academy of Sciences, 2000 - National Acad Sciences

[10] Amin,"Toward Self-Healing Infrastructure Systems," in the IEEE Computer Magazine, pp. 44-53, Vol. 33, No. 8, Aug. 2000

[11] Heydt, G.T. Liu, C.C. "Solution for the crisis in electric power supply", IEEE Computer Applications in Power, 2001

[12] K.Moslehi,A.B.R.Kumar,"Framework for a Self-Healing Power Grid" . Power Engineering Society General Meeting, IEEE,2005

[13] EM Dashofy, A van der Hoek,"Towards architecture-based self-healing systems"- Proceedings of the first workshop on Self-healing systems,- portal.acm.org,2002