RESILIENCE OF DISTRIBUTED MICROGRID CONTROL SYSTEMS TO ICT FAULTS

Tom RIGOLE
K.U.Leuven – Belgium
tom.rigole@esat.kuleuven.be

Koen VANTHOURNOUT
K.U.Leuven – Belgium
koen.vanthournout@esat.kuleuven.be

Geert DECONINCK
K.U.Leuven - Belgium
geert.deconinck@esat.kuleuven.be

ABSTRACT

Recent years a growing deployment of distributed generation (DG) in low voltage power grids is seen, and the amount of DG is expected to increase further in the near future. Distribution grids are however not designed to contain generators. Furthermore, no coordinated control for these generators exists and they provide little or no ancillary services. Therefore control strategies have been designed based on inexpensive ICT equipment and public communication networks. One such agent based control system is introduced in this paper. Also, several scenarios are simulated with ICT-fault injections to assess the systems' resilience to these faults. After discussing the specific scenarios, the root causes of most limitations and vulnerabilities in generalized open, unbounded and distributed control systems are pointed out.

INTRODUCTION

The liberalization of the power grid, together with increasing concerns for the environment, has lead to an increasing use of DG. The biggest problem with current practices of DG is that these generators mainly produce active power, without any controls that contribute to the (distribution) grid operation, such as voltage or frequency control, or VAR compensation [1, 2]. A similar argument can be made for more general distribution grid equipment, in which there is no active control of resources. Despite the theoretical ability of many small loads to adjust their load profiles based on some external signal, there is very little active demand side management for small loads these days. To improve this passive management of distribution grid resources, we propose the use of decentralized, **multi-agent systems (MAS)** [3-6] employing **peer-to-peer (p2p)** networking protocols. More specifically, a multi-agent control system for DG was developed, which optimizes voltage levels, frequency (when islanded), and production costs.

This paper first briefly presents a distributed control system for DG applications forming a microgrid. Next, an analysis is made of the impact of ICT faults on the system considering both accidental and malicious faults using computer simulations. We finally conclude by pointing out current limitations of such MAS in an open environment. The analysis is based on work in progress of the European project CRUTIAL, which covers interdependencies between the power grid and its ICT control systems.

AGENTS AND P2P NETWORKING

Multi-agent paradigm

Although many definitions exist, one could define an agent as "an autonomous system that is situated in an environment and acts on it, based on inputs from the environment or other agents, in order to pursue its goals, and is often able to learn from previous experiences". When many cooperating agents exist in the environment, it is called a multi-agent system. It is believed that in such system, with proper incentives given, low-level autonomous behaviour of individual agents will lead to near-optimal high-level emerging behaviour of the whole system.

In the context of the deregulated power market, the multitude of autonomous parties involved can be seen as a large community of agents, each pursuing their own goals defined by economical and regulatory concerns, rendering (hopefully) the emerging behaviour of having a reliable grid operation build upon a free market. It seems quite straightforward to apply this multi-agent paradigm to power grid control, which is illustrated in this paper.

Peer-to-peer networking

Continuing upon the multi-agent methodology, which avoids centralized management, peer-to-peer[1] networking is an ideal structure to organize the agent community in open unbounded environments. These p2p-networks enable agents to find one another based on agent-IDs or agent attributes in the multitude of agents (**resource discovery**). In such p2p networks each node has only a couple of known other nodes, called its neighbours. This way, all nodes in the network are directly or indirectly connected in a graph-like structure. Well known examples of p2p-networks are file-sharing programs such as Kazaa. Over the Internet they build a p2p-network (among file-sharing peers) over which files can be queried. By routing queries from one peer to the other, no central indexing server is needed. The lack of a central server and the multiplicity of peer-to-peer links per peer make a p2p network quite resilient to peer crashes and communication network infrastructure failures [7].

A MICROGRID CONTROL SYSTEM

As an example MAS implemented on a p2p network using the Internet for communications, we present a system for controlling a microgrid with high DG penetration [5, 6].

1 A *peer* or *node* is a networked computer within a distributed ICT-system; they may be considered synonyms.

The majority of DGs in this system are equipped with a droop control scheme, which enables them to quickly react to voltage and frequency changes by injecting more or less (re)active power based on local measurements [8, 9]. Although this droop control scheme is an important asset of the system, the multi-agent based control loop operates orthogonally to this droop control.

The DG units in the system each have a controller agent which may adjust power output settings of the generator. All these agents of the different DGs communicate with one another using a p2p network set up over the Internet. The fundamental operation of the **two optimization control loops** implemented by the MAS, namely secondary (**voltage and frequency optimization**) and tertiary control (**economical optimization**) [6], are elaborated further in this section.

Secondary control

The main purpose of secondary control is to optimize voltage within the microgrid. Given a reasonable amount of DGs with a droop controller, the microgrid reacts fast to imbalances. Though, since this droop control is a proportional controller, voltage and frequency do not remain at their rated value. A coordinated, distribution grid wide, control system is needed to keep these as close as possible to their rated values. In this secondary control algorithm, every agent records the local divergence from the rated value. Using a distributed averaging algorithm, a system wide average divergence is estimated by each agent. In this averaging algorithm each agent sends its current average to a random neighbour in the p2p network. The agent and this neighbour estimate a new average by averaging their averages. Continuing this process leads to a system wide estimation in every agent. Figure 1 illustrates the algorithm. The average voltage divergence gives each agent a clue as to how to adjust power outputs in order to minimize system wide divergence, without risking oscillations.

Tertiary control

Tertiary control also uses the gossiping primitive, but in a different way than secondary control. During a single gossiping step, two controller agents exchange their current power outputs and their (marginal) cost curves. Based on this, both update their settings so that production cost is equal, but their combined power output stays the same. After a while this algorithm will equalize production costs of all generators in the microgrid. Notice that there is a need to weigh power quality concerns against economical concerns (i.e. secondary vs. tertiary control). The solution taken here is to permit voltage divergence within certain limits, which allows optimizing economically as long as these limits are observed.

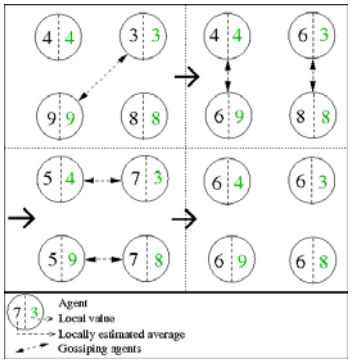

Figure 1: Example of distributed averaging in 4 steps

ICT FAULT SCENARIOS

Given the fact that the decentralized microgrid control system introduced in this paper has been proven to function in a small laboratory setup and in larger scale computer simulations, **how resilient is it to various ICT faults**? In an Internet environment, one should not only be concerned about message latencies and connection loss, but also about malicious behaviour. In this section, some fault scenarios are studied in order to assess the resilience of distributed control systems based on MAS and p2p networks.

Simulation setup

The distribution grid shown in Figure 2 is used in these simulations. There are three branches containing loads and DG units. It is presumed that point 'F' near the feeding transformer is constantly at nominal voltage (230V). In the simulations, both the electrical and ICT-part are simulated. Agents controlling generators communicate over a virtual IP-network by setting up a p2p-network and iteratively communicating with one another as in the real-world implementation. When a generator adjusts its power output, new power flows and voltages are calculated.

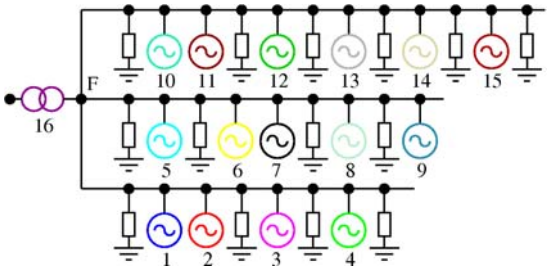

Figure 2: Distribution net layout

Normal behaviour

The first simulation shows the microgrid behaviour under normal circumstances. Both secondary and tertiary control are operational and no faults have occurred in the system. In the simulation graphs (Figure 4), strong fluctuations are seen in DG power outputs at time t=1, t=20 and t=120 (load changes). After a while power output remains constant. The reason for the fluctuations is the combination of secondary

and tertiary control converging to a Pareto optimal point that equalizes marginal costs while taking voltage into account. Following the large load increase at t=20, voltage near generators 14 and 15 drops very low. Secondary control subsequently brings this voltage closer to the nominal value. In the production cost graph, it is seen how marginal production costs converge to a system wide value, which is the economic optimum. Only some divergences from this uniform cost are seen, namely generator 15 which produces at a higher cost to mitigate the voltage dip and generators 6 and 9 which produce at a lower cost because they already reached their maximum output capacity.

Accidental ICT fault scenarios

IP-package loss and network latency

Latencies on public IP-based networks are unpredictable and packets can get lost. Due to TCP abstraction packet loss is seen as a longer latency to the application and can thus be treated in a similar way. In the microgrid, secondary and tertiary control are optimization protocols and by no means time-critical. Large message latencies will only lead to slower convergence and less optimal behaviour. Under expectable Internet delays the slower convergence would be barely noticeable, and thus negligible.

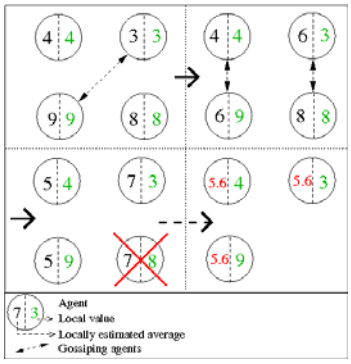

Figure 3: Node failure influence on averaging

Agent crash or communication network failure

When dealing with random agent or node crashes, or communication failures, the impact on both the p2p network and the application itself can be studied. The p2p-network is designed to deal with the dynamism of public networks and can deal with regular entering and leaving of nodes, or random communication link failures [7]. On application level, loss of a single agent simply implies its DG unit operates less optimal, which should not be too much of a problem. There is however one less obvious problem with secondary control, more specifically the averaging algorithm. When a node is lost, the estimated average diverges from the real average, and this divergence can not be detected or restored (see Figure 3). When only a small number of nodes fail, this will result in quite marginal divergences, and a regular reset of the averaging algorithm restores the system to a valid state. The problem may become serious when failures are no longer random, which is discussed later on.

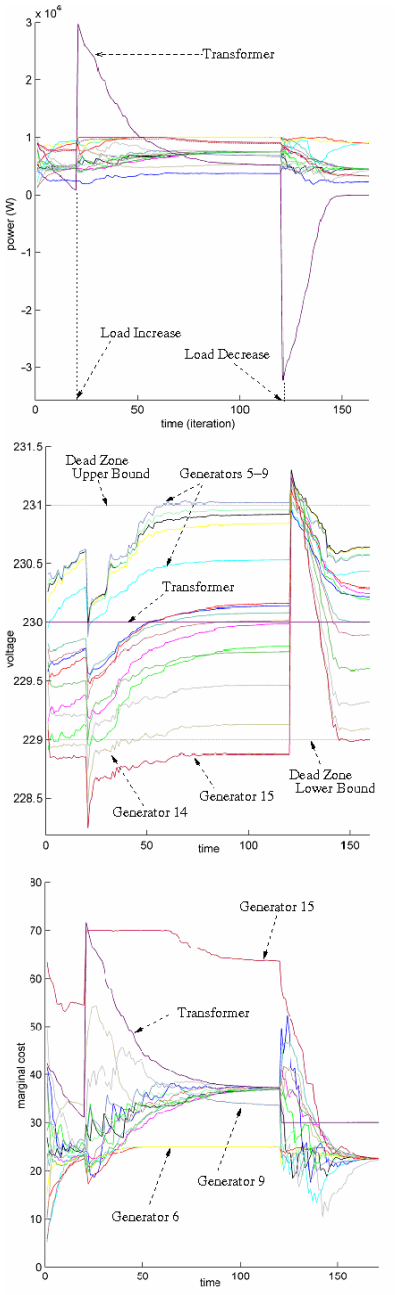

Figure 4: Power output, voltages and production costs

Malicious ICT faults

General security threats

In an open environment security threats such as worms, viruses or hackers exploiting application or operating system vulnerabilities may be expected. For this, especially when using off-the-shelf systems, best practices for security have to be deployed, such firewalls, virus-scanners and intrusion detection systems.

Denial of Service (DoS) attacks
On the Internet bandwidth is shared with other users. This means anyone can flood a part of this network, as long as his bandwidth is large enough to insert this packet flow. A typical DoS attack would trick a large number of PCs into sending messages to a single network section, denying legitimate traffic. In case of a DoS attack, the microgrid would experience similar problems as with network latency or failures, but maybe on a larger scale.

Malicious agent intrusion
For an agent to be accepted as a legitimate agent some sort of certification and authentication is needed. Nevertheless, one should keep in mind that even a trusted agent may misbehave, or an intruder may claim to be a trusted agent. This scenario studies the influence of a malicious agent injecting false values into the secondary control loop, falsifying the estimated average voltage divergence (similar to Figure 3). It tricks other agents into believing there is a voltage dip in the grid, stimulating them to increase active power production. The simulation shows the voltage increasing all over the system (Figure 5), possibly leading to equipment damage or disconnections of generators and grid segments by protection equipment.

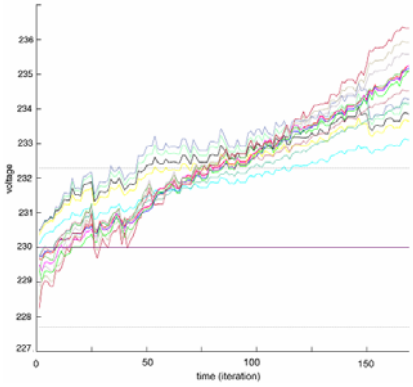

Figure 5: Grid voltage levels due to malicious agent

P2P network vulnerabilities
The p2p-network topology depends on the rules for a node to choose its direct neighbours. In one scenario a malicious node could attack this topology by sending false replies to nodes searching new neighbours as to make himself the new neighbour. After some time, the malicious node can become the overlay network centre. This may give the malicious node the power to partition the network and falsify power cost in one partition which may render the attacker financial gain.

CONCLUSIONS

Low cost solutions for coordinated DG operation are needed to make it economically feasible. Therefore we propose the Internet as a communication medium and a control system design which does not need an expensive dedicated server. The design has been built to deal with unreliable communications and agent failures. This resilience to **accidental faults** is validated using fault injections in simulations. On the other hand, in a public network **malicious behaviour** can also be encountered. Simulations show two scenarios in which attacks cause serious inconveniences for the microgrid operation. The root of this problem lies within the openness and boundlessness of the MAS. A notion of **mutual trust** is needed, and monitoring can be an important tool to strengthen or weaken this trust.

ACKNOWLEDGMENTS

This work is partially supported by the K.U.Leuven Research Council (project GOA/2007/09) and by the European Commission (projects IST-4-27513 CRUTIAL and IST-4- 026923 GRID).

REFERENCES

[1] T. Ackermann, G. Andersson, and L. Söder, 2001, "Distributed Generation: a Definition", *Electric Power Systems Research*, **57**, p. 10.

[2] M. Scheepers, M. van Werven, et al., 2006, "Distributed Generation in Electricity Markets, its Impact on DSOs, and the Role of Regulatory and Commercial Arrangements", *International Journal of Distributed Energy Resources*, **2**(1), p. 4.

[3] A.L. Dimeas and N.D. Hatziagyriou, 2005, "Operation of a Multi-Agent System for Microgrid Control", *IEEE Transactions on Power Systems*, **20**(3), p. 1447-1455.

[4] J.K. Kok, C.J. Warner, and I.G. Kamphuis, 2005, "Powermatcher: Multiagent Control in the Electricity Infrastructure", *Proceedings Autonomous Agents and Multi-Agent Systems*, Utrecht, Netherlands.

[5] T. Rigole, K. Vanthournout, and G. Deconinck, 2006, "Distributed Control Systems for Electric Power Applications", *Proceedings 2nd Workshop on Networked Control Systems*, Rende, Italy.

[6] K. Vanthournout, G. Deconinck, and R. Belmans, 2005, "Agora: Distributed Tertiary Control of Distributed Resources", *Proceedings 15th Power Systems Computation Conference*, Liege, Belgium.

[7] K. Vanthournout, G. Deconinck, and R. Belmans, 2004, "Building Dependable Peer-to-Peer Systems", *Proceedings International Conference on Dependable Systems and Networks*, Florence, Italy.

[8] K. De Brabandere, B. Bolsens, et al., 2004, "A Voltage and Frequency Droop Control Method for Parallel Inverters", *Proceedings IEEE Power Electronics Specialist Conference*, Aachen, Germany.

[9] M.N. Marwali, J.W. Jung, and A. Keyhani, 2004, "Control of Distributed Generation Systems - Load Sharing Control", *IEEE Transactions on Power Electronics*, **19**(6), p. 1551-1561.