Robustness of Microgrid Control Mechanisms Against Cyber Attacks

Pelle de Greeuw
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands
p.c.a.degreeuw@student.utwente.nl

ABSTRACT

In our society the power grid is one of the most important systems which we cannot do without. The rise of local renewable energy production results in localized smart grids which can govern themselves, also known as micro grids. To keep the grids stable, control mechanisms are used. These can be localized, centralized or a combination of both. Due to the high availability requirement of these grids and control mechanisms they are a likely target for cyber attacks. This paper shows the weaknesses and strengths of an auction control mechanism and a control mechanism based on local voltage measurements during attacks such as DDoS and data injection.

Keywords

control mechanism, microgrid, cyber attack, powermatcher, data injection

1. INTRODUCTION

Traditionally the grid[1] is made out of consumers and producers which have no overlap with one another. The producers govern the grid stability manually by operator and automatically with a droop controller as explained by [8]. This works well as the droop controller handles smaller changes in load in the grid and the operator handles larger changes such as a tea time energy spike in the UK after the end of a popular program. In this type of grid, it is controlled almost locally in on the producers side. While the operator can control multiple producers, their droop controllers only have a limited form of communication through grid frequency and the consumers are never contacted.

With the rise in renewable energy sources and them being available for consumers to place locally the grid changes, consumers can now also be producers. All of the producers have to work together to keep the grid stable and with so many possible producers a need for more control and communication arises. The smart grid solves this by having every consumer and produces communicating with each other via for example the internet. More and more devices have smart controllers which allows them to be controlled by a different controller. These controllers in turn communicate with one another or are controller by an even higher up controller. The smart grid thus can be viewed as a tree structure and a sub part of such a tree (e.g. a housing block) is a microgrid.

Electricity is one of the, if not the, most important things in our society and therefore a large target for attackers. Smart grid controllers therefore must be able to withstand attacks from different angles. This paper shows the weaknesses and strengths of an auction control mechanism and a control mechanism based on local voltage measurements during attacks such as DDoS and data injection.

[1]Throughout this paper, "network" will refer to a communication network and "grid" will refer to the power network

32nd Twente Student Conference on IT Jan. 31st, 2020, Enschede, The Netherlands.

2. RELATED WORK

Liu et al.[7] combined research on injection attacks on a microgrid. Attackers are injecting control signals to several devices; solar photovoltaic and energy storage systems and inverters. The attacks can significantly disrupt the stability of the microgrid. Some attack identification methods are shown to identify these types of attack.

Li et al.[6] Studies undetectable line outages in a local or microgrid. First power lines are estimated in a local grid after which the rest of the grid is modeled. Then cyber attacks are carried out to mask physical attacks on the transmission lines which cause the controller to be unaware of the physical attack while the cyber attack in underway.

D'hulst et al.[1] Tests a control mechanism for households where no communication with the other controllers are necessary. Only communication with the smart appliances within the household are used, together with local voltage measurements of the grid provided by the smart meter.

Hartmanns et al.[2] Studies the oscillating effect photovoltaic micro-generation can have on the grid and proposes an communication design approach similar to TCP to prevent the effect.

The last 2 are used by Hoogsteen [3] where they are combined to test if the can provide a greater defense together than alone.

3. METHODOLOGY

Using the software simulation tool DEMKit [4] a microgrid can be simulated. The controllers and device agents are programmable / editable which allows for different control mechanisms and attacks to be implemented. The first part of the research is identifying and implementing multiple control mechanisms to compare against each other and multiple attack vectors.

The control mechanisms are divided in 2 types, localized and centralized. A localized controller controls its device(s) by taking measurements from the grid (e.g. volt-

age). It may control a few devices below it with other communication methods but cannot communicate with any other controller above or beside it (e.g. droop controller). The centralized controller communicates with its peers and agents via a means other than the grid itself (e.g. the internet) to control its devices. It can communicate upwards and with its peers to decide strategies for stabilizing the grid.

For each control mechanism one or more simulations are run for each attack vector. With the metrics from the simulation it is compared against the other mechanisms and other attack vectors. These metrics are grid voltage, frequency and user comfort level. The first 2 are easily measurable with the simulation but the third can turn out to be to hard to quantify and therefore not to be considered.

3.1 Network model

The DEMKit tool has no true network modelling in it, however, most function calling, getting and setting of values is done through a single method going all the way back to the simulation host. Through these functions a network simulation could be implemented relatively easy.

The network simulation consist of a simulator host similar to the flow simulator host which can hold an amount of switches and edges. An edge can connect a controller to a switch or a controller to another controller. When a call is made to any number of receivers, it is intercepted when the controller has a network edge connected to it. For each receiver which is found in the network of the edge, either through a switch or directly, the call is handed off to the network edge instead of the simulation host. For the receivers not in the network the call is handed off to the simulation host as usual.

When initializing the simulation controllers can be assigned to a switch, which automatically creates a network edge if not provided. By using different switches isolated networks can be simulated, a controller to controller edge can simulate a very local connection.

3.2 Control mechanisms

3.2.1 No Control

The first control mechanisms used in testing is no control mechanism at all. The modeled network then has no form of smart controllers for any of the devices in it. The measurements from this setup servers as a basis to compare the other control mechanisms against. They should, preferably, never be worse than this measurement as that would mean the controller is actually working towards making the grid unstable.

3.2.2 Auction control

The second control mechanism that will be considered is the auction controller presented by Kok [5]. This control mechanism consist of a master controller called an auctioneer which takes bids from its devices and calculates a price at which power generation and production are in balance. This mechanism can have multiple layers of aggregators, each collecting bids from a increasingly smaller set of sub controllers or devices and sending the combined bid upwards. In this research we will only look at a single layer, 1 auctioneer overseeing several houses with smart meters as aggregators which are talking with that auctioneer.

3.2.3 Local voltage measurements

The third and last type of control mechanism is control based on local voltage measurements as seen in D. Hulst et. al.[1]. The smart meter of each house has access to voltage measurements and based on that measurement can make decisions on power consumption and generation of the devices in the house. If the voltage drops below a certain point it will aim to generate more power and consume less and if the voltage comes above a certain point it will aim towards the opposite.

While Hulst only uses on or off devices, DEMKit offers more flexibility for charging devices such as EV's and to keep the test fair between control mechanisms we cannot change the EV to just on or off. Therefor a adaptation of the control mechanisms has to be made to allow different charging rates of a device.

Just like the auction control mechanism, all devices send options to the controller. These options specify if the device wants to turn off or on and how urgent it wants to do so so on a scale of 0 to 100, at 100 it has to turn on or off directly or the user comfort level will be impacted. If the voltage is within the desired limits (229 - 231) the controller does not interfere and the devices continue their current behaviour. If below or above this "deadzone" the controller will respectively turn devices off or on.

3.3 Attacks

3.3.1 Physical disconnect

The first type of attack that will be simulated is a physical disconnect of a network cable or DDoS of a controller. In this type of attack the controller cannot communicate anymore with other controllers or a controller higher up on the chain. This type of attack is easily detectable as the hardware layer will notice there is no active connection anymore and the controller can change it behaviour based on the knowledge.

Smart devices and controllers have to be connected to a network to communicate with each other, either a designated network from the supplier or the internet. Both can be brought down through not only by an attacker cutting cables or buying a DDoS attack but also by a ISP network outage or a construction crew accidentally hitting lines.

3.3.2 Data injection

The second type of attack is injecting false data into the communication between controllers. This type of attack can be very hard to detect, in this research it is therefore simulated as completely undetectable for the controller. The data is injected when coming from the controller going to a sub controller. With an auction controller the price sent back to a controller is changed, with the local voltage controller the control signal to the deivce is changed.

While not as likely in a supplier owned network, through the openness of the internet anyone can send anything to anyone, including your smart controllers. If not properly secured they can be susceptible to data injection from attackers.

3.3.3 Rogue devices

The previous two types of attack are both attacks on the controller of a house (e.g. a smart meter), the third and last type of attack focuses on devices in a household itself.

Because of the increasing amount of IOT devices controlling appliances and their often lack of security, it is very realistic that an attacker would gain access to such a controller. They can then turn on all those devices at once for example, not much unlike a DDoS attack on the network but targeted at the grid.

3.4 Environment

The simulation consist of a street of 20 houses. Each of these houses has a static load assigned to it to simulate uncontrollable devices such as lights and entertainment setups. The following devices are distributed to the houses, meaning not all houses have such a device. Dishwashers and washing machines both have a availability window set in which they can run their program, once started it cannot be stopped. Solar panels (PV's) can be disconnected but not further regulated. Electrical vehicles (EV's) have an availability window in which they should be charged. During this window they can charge at any rate between 0 and their assigned maximum charge speed. Batteries are similar to EV's but have no availability window and can also discharge at any rate between 0 and their assigned maximum discharge rate.

Because the batteries have no other use than provide a buffer in the network, an uncontrolled network cannot actually use them. There is no controller to decide if the battery should charge or discharge.

3.5 Attack simulation

All three types of attacks can be simulated through the network edge class. When setting the simulation up, edges are created for the controllers with a certain type of attack and timestamps for when the attacks are to happen. When time ticks are propagated through the switch to the edge it will set its attack status and either let the communication through untouched or do something with it based on the type of attack.

Disconnecting attacks will simply do not execute the call and data injection attacks can change the arguments of a call or a result returned by one. With rogue devices the attacks will be given to the device classes themselves. Regardless of the type of controller attached to a device it will then perform the attack and there is nothing the controller can do about it.

To get results which can fairly be compared to each other only the controllers and network edges are changed for each simulation. Devices are fed with the same profiles and static loads remain the same through each simulation.

3.6 Quantifying results

Performances of a control mechanism under a type of attack are measured with line voltages and overall power usage. The goal is to have lower and less power peaks and lower and less voltage deviations from 230V than the no control simulations. The less and lower power peaks and voltage deviations the better.

The line voltage may deviate 10% from 230 [2], above or below that threshold is a over- or under-voltage and mean a failure of the grid. Because of the size of the test environment, a maximum load will not see a voltage drop of more than 23V. Therefore a 10V maximum deviation was chosen for the supposed failure of the grid.

4. RESULTS

4.1 Baseline

Table one shows limits reached by the controlling mechanism during the simulation in normal operation. Limits are the extremes reached by the grid at one time, while they do not represent the whole simulation it sheds light on the performance of the control mechanisms on dividing the power available.

[2]NEN-EN 50160:2010

Table 1. Baseline performance

Control	Voltage (min / max)	Power peak
No control	219 V / 232 V	47 kW
Auction	224 V / 232 V	20 kW
Local	225 V / 232 V	22kW

As expected, a large difference is seen between no control and the 2 controlled simulations. The 2 controlled simulations are very close in keeping the power peaks low. This is also expected as both control mechanisms aim to keep the voltage as stable as possible through different means.

4.2 Physical disconnects

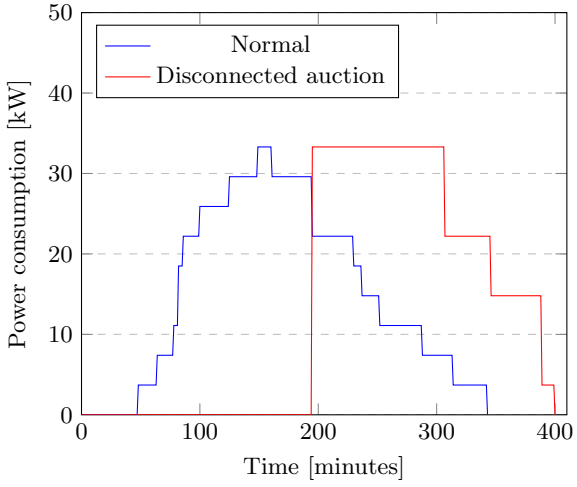
The localized voltage control mechanisms is completely unphased by this attack type as it does not require a connection to other controllers apart from the devices within the household it is controlling. It therefore maintains exactly the same performance as the baseline simulation. While it is possible that those remaing connections could be severed it does not hold any new information as there are no more controllers which can do any work and thus the grid is in a no control state.

The auction controller is however affected by this type of attack as it relies on communication with other controllers to device a strategy. When the connection is severed the default behaviour of the devices take over, which is to start as soon as possible within its availability window. This means a perfectly timed attack can hold worse results than an uncontrolled grid as this can cause large loads to stack fully on top of one another instead of just overlapping.

As seen in figure 1, without any control the devices start their cycle as soon as they enter their window which causes a pyramid as all come online one after another. The auction controller actually prevents the devices from starting until much later in the simulation when the other loads are less. By disconnecting the controllers all devices start their cycle at the same time which causes a huge load on the grid for a substantial amount of time.

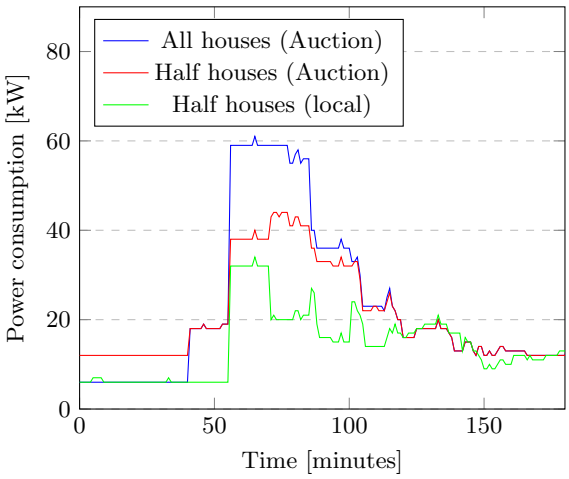
While the peak power usages are about the same, the attack causes a high load for a long time under the auction controller. The auction controller performance is thus worse than no control at all. Without a controlling mechanisms the devices space themselves naturally through the need of their users which is negated by having a central controller.

Fig. 1: EV power usage



4.3 Data Injection

Fig. 2: Power consumption during injection



4.3.1 Auction controller

When injecting between the auctioneer and a house controller a result similar to the disconnecting attack can be achieved. The controller is fed a false price, first a very high one in order to fully deplete any storage left in the batteries and prevent the EV's from charging. Secondly a very low price to trick the controller into fully charging both batteries and EV's at the same time. The result is a power spike of almost 60kW and a voltage drop to 219 V.

As seen in figure 2 when all houses are injected with the above strategy it causes a large spike in power usage. When only half of the houses are under attack the spike is lower as would be expected. What is not expected is the power increase at minute 71. Intuitively the power should decrease instead of increasing when the controller is in control of some of the devices. This highlights a problem with the auction controller, it bases its view of the grid only on the data provided by the bids devices send in. As the injection happens when the price is going back to the household, the auctioneer assumes that the devices conform to the calculated price when they do not. At minute 71 it calculates a price which allows some controlled EV's to start charging when they clearly should wait.

4.3.2 Local controller

Because there is no communication with anything ouside the household, injection can only happen between the house controller and each individual controller. This results in exactly the same profile of batteries and EV's charging at the same time, however the controller is still able to use the other devices to compensate for the huge power draw. As seen in figure 2 the initial power spike is less than the auction controller and after it only declines and does not increase appart from some peaks.

The reason why the controller compensates with other devices is that it has an accurate state of the grid through its local voltage measurements. These cannot be injected and thus the controller will send signals to its devices to turn off. Even if some do not comply it will still turn of others and only allow them to turn back on if the grid is more stable again.

4.4 Rogue devices

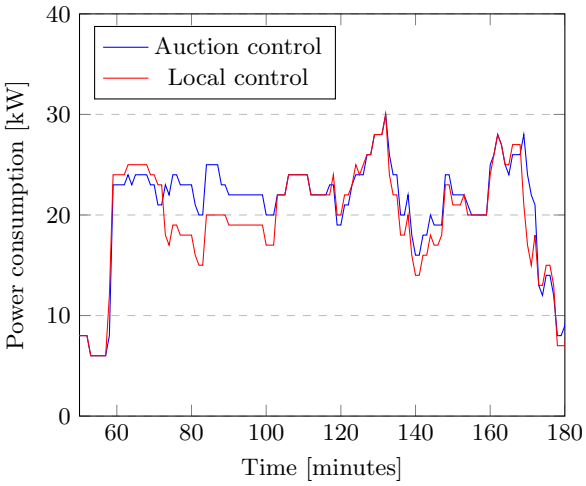
The attack with the most potential is when the devices themselves are at full control of an attacker. In the previous two types of attack, the attacker was always limit by the availability windows put in by the user. The devices would always turn on regardless of price or command from the controller if staying off meant the user specified time could not be reached otherwise. This requires the attacker to know when each devices availability window is in order to pick the best possible time to attack. This is not required when you have full control over a device.

This is also the only type of attack where a uncontrolled grid is affected as the other 2 types of attack need a controller to perform the attacks on.

When all devices are infected it produces the largest power spike of all simulations of about 70kW. Because all devices are infected the grid is basically uncontrolled as the controllers cannot control any devices. When only a subset of the devices are infected a difference can be spotted between the local controller and the auction controller. After the initial spike the local controller decreases in power consumption for a bit where the auction controller does not.

This is caused by the same problem identified in 4.3.1, the auction controller will not take advantage of the batteries which can still produce some power because it does not "know" more generation is needed. The local controller again will turn on the batteries as it detects when it detects a lower voltage.

Fig. 3: Power consumption during rogue devices



5. CONCLUSION

Rogue devices are definitely the most disruptive attack of all considered when all devices are infected. Both controllers fair similarly against that attack so not much can be said about them at this point. It is also an attack which is increasingly more likely to be viable because more and more of the appliances can be controlled through the internet with little to no protection.

The weak spot of the auction controller is the main auctioneer which is is control of the house controllers. It means there is a single point (or at least less points) of failure in the system where an attack can happen. An attack or failure of that point is very realistic, if connected to the internet it requires only the push of a button to conduct a DDoS attack and bring it down.

The local voltage controller, while slightly worse than the auction controller in normal conditions, performs better when under the tested types of attack. Its greatest strength comparing to the auction controller is its lack of single point of failure.

6. DISCUSSION

6.1 Default behaviour

The default behaviour of some devices has effect on the results of the simulation. The devices with the most load are the EV's which can be charged at a variable rate, their default behaviour however is to charge at full speed as soon as possible. While this is in the users best interest, they can use their car sooner if needed, from a grid point of view it is much more logical to let the EV charge for the average amount through it's entire availability window. The load would be longer on the grid but would be a lot less demanding than a full charge speed load.

7. FUTURE WORK

7.1 Frequency

At time of writing DEMKit is missing the simulation of grid frequency. The frequency is commonly used by generators to govern the voltage, lower frequency will give more voltage and vice versa. When a smart grid gets disconnected from the main grid and still has such a generator connected it would mean voltage is not a good representation of the grid status anymore. The local controller would need a frequency variable incorporated into its calculations to correctly control its devices.

7.2 Larger network model

The network implementation used, consists of a single layer switch to which all devices are connected. To better reflect reality switches should be able to connect to each other to allow failures to occur in other localized parts of the system.

7.3 Combining control mechanisms

A better controller would most likely be a combination of the 2 mentioned here, the auction controller performs better when in normal operation but is very vulnerable to attacks on the communication network. When a network outage outage or DDoS attack is happening it could easily switch over to a the local controller to continue sending control signals instead of staying silent. While data-injections will be much harder to detect it could then also switch over to the local controller.

8. REFERENCES

[1] R. D'hulst, K. Vanthournout, and F. Hoornaert. Lv distribution network voltage control mechanism: Experimental tests and validation. In *IECON 2014 - 40th Annual Conference of the IEEE Industrial Electronics Society*, pages 3504–3509, Oct 2014.

[2] A. Hartmanns, H. Hermanns, and P. Berrang. A comparative analysis of decentralized power grid stabilization strategies. In *Proceedings of the Winter Simulation Conference*, WSC '12, pages 158:1–158:13. Winter Simulation Conference, 2012.

[3] G. Hoogsteen. *A Cyber-Physical Systems Perspective on Decentralized Energy Management*. PhD thesis, University of Twente, Netherlands, 12 2017.

[4] G. Hoogsteen, J. L. Hurink, and G. J. M. Smit. Demkit: a decentralized energy management simulation and demonstration toolkit. In *2019 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, pages 1–5, Sep. 2019.

[5] K.Kok. In *The PowerMatcher: smart coordination for the smart electricity grid*, July 2013.

[6] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah. Analyzing locally coordinated cyber-physical attacks for undetectable line outages. *IEEE Transactions on Smart Grid*, 9(1):35–47, jan 2018.

[7] X. Liu and Z. Li. False data attack models, impact analyses and defense strategies in the electricity grid. *Electricity Journal*, 30(4):35–42, may 2017.

[8] R. Wright. In *Understanding modern generator control*, pages 453–458, 1989.