24 Sep 2007

Blueprint for Iteratively Hardening Power Grids Employing Unified Power Flow Controllers

William M. Siever

Ann K. Miller
Missouri University of Science and Technology

Daniel R. Tauritz
Missouri University of Science and Technology, tauritzd@mst.edu

Recommended Citation

W. M. Siever et al., "Blueprint for Iteratively Hardening Power Grids Employing Unified Power Flow Controllers," *Proceedings of the 2007 IEEE International Conference on System of Systems Engineering, 2007*, Institute of Electrical and Electronics Engineers (IEEE), Sep 2007.
The definitive version is available at https://doi.org/10.1109/SYSOSE.2007.4304291

Blueprint for Iteratively Hardening Power Grids Employing Unified Power Flow Controllers

William M. Siever[1], Ann Miller[1], Daniel R. Tauritz[2]
[1]Department of Electrical and Computer Engineering, [2]Department of Computer Science
University of Missouri–Rolla
E-mail: {bsiever,milleran,tauritzd}@umr.edu

Abstract— A stable electricity supply is vital for modern society. However, many parts of our power transmission grid are operating near their operational limits. Such stressed systems are vulnerable to cascading failures, where a few small faults can induce a cascade of failures potentially leading to a major blackout. The Unified Power Flow Controller (UPFC), the most powerful high-speed, semi-conductor based power flow device, can be used as a theoretical model to study how these devices can be used to improve power grid resilience. The blueprint presented here can be used to iteratively identify critical weaknesses in power grids and to recommend a means of fixing these weaknesses via the installation of UPFCs. This approach to hardening the power transmission grid will make it less prone to blackouts and better able to forestall or reduce the severity of unavoidable blackouts.

Keywords: Critical Infrastructure Protection, Power Grid, FACTS, UPFC, Evolutionary Algorithm

1 Introduction

Modern industrialized society has become dependent on electric power. In fact, in a report to the President of the United States, the U.S. Department of Energy said "Electricity is a cornerstone on which the economy and the daily lives of our nation's citizens depend. This essential commodity has no substitute" [7]. Not only does electric power directly provide heating, lighting and the power that drives manufacturing plants, but it is also a vital resource on which other infrastructures, including water distribution, sewage treatment and removal, emergency services, and traffic flow control, rely. Unfortunately, power grids all over the world are facing conditions which may jeopardize their ability to satisfy future demand for power as well as making them a target for terrorist attack.

Electric power is produced at large generating facilities and then "transmitted" over a system known as the transmission grid to regional distribution systems. The transmission grid, which consists of many long-distance, high-voltage lines and the buses to which they are connected, is really at the heart of the electric power industry. The transmission grid is the fundamental link between power producers and consumers, and, unfortunately, is becoming increasingly overburdened. Over the past decade demand for electricity has steadily increased and deregulation has spurred increased power transfers, but due to environmental, economic, and social concerns, the transmission grid has had relatively few upgrades. As a result, many of the components are operating near their intended capacity. Prior to deregulation a top-down approach could be used to distribute power evenly through the entire system, however, due to deregulation there is incentive for transmission operators to operate as near capacity as possible. This allows excess power to be purchased from distant markets, but at the expense of reduced system stability margins. For the foreseeable future the power industry will be able to produce enough power to meet customer demands, however, the current transmission grid may be operating so close to its limits that a small fault could cause a blackout [7].

Transmission grids have two features which make them prone to catastrophic failure. First, because transmission lines often cross vast, unmonitored space, they are susceptible to both natural failures (ice, wind damage, tree contact) and intentional disruption (terrorist attack). Second, when a transmission line fails, the power which it was carrying flows over other lines. In a system where many components are already operating near their limits, the additional demands following a failure can cause other components to fail. The induced failures can, in turn, induce additional failures that eventually lead to a domino effect that causes a blackout.

Power flow in the transmission grid today is largely dictated by Ohm's laws: power flows along the path of least resistance. Historically, the flow of power has been controlled by adjusting where the power is being generated and by "compensating" the lines, where electromechanical devices physically add or remove components to change line impedances. Although this was satisfactory when the grid was operating well below its maximum capacity, as the grid becomes increasingly overburdened it becomes vital to have better control over the flow of power to help mitigate cascading outages by directing power flow away from components that are near their failure point. By using automatic control algorithms and high-speed, accurate power flow control in key locations, it may be possible to mitigate or at least reduce the severity of cascading outages. Having this additional control may also be a vital element for defending power systems against deliberate physical and cyber attack.

The power grid is considered to be a significant target for terrorist attack because, due to its large scale, it is susceptible to a number of different attacks including: physical destruction of lines, physical control of a substation or generating facility, and cyber attacks on control and communication systems. Due to the sheer size of the system it is impossible to effectively protect all the physical components, and due to the complex

control interactions of the different companies and components in the system a comprehensive cyber defense is also infeasible. In addition to being vulnerable, the power grid makes a tantalizing terrorist target due to the havoc that follows even a short disruption. This was particularly evident following the August 2003 blackout that effected a significant region of North America. In addition to the financial losses incurred due to business closings, a number of vital services including 911 service, sewage treatment, and water service were lost due to their reliance on electricity. Moreover, there is evidence that grid attacks are actively being investigated by terrorist organizations. In a statement to the joint subcommittee of the House of Representatives, Christopher Cox, a representative from the state of California, reported that "Al-Qaida computers seized in Afghanistan in 2001 had logged on to sites offering that offer [sic] software and programming instructions for the distributed control systems (DCS) and Supervisory-control and Data-acquisition (SCADA) systems that run power, water, transport and communications grids. [6]"

1.1 Unified Power Flow Controllers

In an effort to help better control power flow, the Electric Power Research Institute (EPRI) sponsored an initiative to develop a new class of power control devices called Flexible AC Transmission System (FACTS) devices. These devices, which are based on recent improvements in semi-conductor technology, can be used to help solve a variety of power control problems. By using the latest semi-conductor technology, these devices are able to control AC power in a substantially new way which is both faster and more precise than previous techniques.

One of the most powerful forms of FACTS device is the Unified Power Flow Controller (UPFC). As its name suggests, its primary role is to provide control over power flow. A UPFC is installed on a specific power line and provides almost total control over the power flowing through that line. Due to the nature of electric power flow, increasing or decreasing the flow through one line has an ancillary effect on the lines to which it is connected. This allows a single UPFC to have significant impact: it can be used to increase power flow through a line and potentially draw excess power away from "upstream" lines that are operating over capacity, or it can restrict power flow and reduce the load on "down stream" lines. Due to high installation cost it is impractical to install more than a few UPFCs in a system, but a few devices cooperatively using their ancillary impact may provide enough regulation to redirect power flow and avoid or at least reduce the overload on critical lines.

Although UPFCs can be used to mitigate a variety of operating conditions, the work here focuses on finding ways to relieve or at least reduce the severity of cascading outages. The most significant cascading outages are a direct result of transmission lines carrying higher-than-normal amounts of current, which causes the metal to expand and sag. A failure occurs when the line either sags into contact with a ground source, such as a tree, or weakens to the point of its own weight causing it to break, much like a fuse. Either of these failures is due to carrying above average current for a sustained period (several seconds to hours). Sagging into trees was the most significant contributor to the North American blackout of 2003 [7]. In that case, failure to maintain properly trimmed trees, rather than excessive line sag, was the major cause of failure.

UPFCs are studied here primarily because they offer a comprehensive means of power flow control, being able to control both real and reactive power flow as well as being able to regulate bus voltage. UPFCs have a total of twelve different forms of control [8] and represent a super set of the capabilities of other devices in the FACTS family as well as high speed versions of more traditional electromechanical means of control. For the work proposed here, the ideal control mode is unknown *a priori*, and, more importantly, may be different for different system vulnerabilities. I.e., under one type of failure the UPFCs may be best used for power flow regulation and in another scenario additional voltage support may be more important. A theoretical UPFC provides an ideal model of control capabilities because, with the appropriate control algorithm, it can seamlessly change control modes to suit the current situation. The plan presented here can be used to indicate where system vulnerabilities exist and further studies can easily identify the specific form of device (UPFC, other FACTS, or traditional means) to provide the best cost benefit for system defense.

1.2 Using UPFCs for Critical Infrastructure Protection

The remainder of the paper looks at three inter-connected problems: 1) identifying the kinds of attacks the power grid is susceptible to, 2) finding installation locations that allow a few UPFCs to substantially reduce the likelihood of cascading failures, and 3) modeling the elements necessary to simulate both simple cascading failures and the control capabilities of UPFCs. Each of these topics alone presents a complex problem and the approach presented here is not intended to be a panacea to solve all power grid vulnerabilities. Instead, a simplistic approach is outlined to explore the feasibility and potential impact of the use of FACTS devices for a specific type of system vulnerability. Following the feasibility study, detailed analysis can be performed to determine the real-world applicability of the results. Essentially the technique can be used to provide some recommended solutions to a very complicated problem, which system engineers can then evaluate and refine.

The approach presented here is based on a game-theory model of attackers and defenders and requires iterative cycles of simulated attacks. As such, a power system simulation that models the most significant features of both cascading failures and UPFCs is required. The simulation will be used in two ways: the first will identify the attacks to which the system is highly vulnerable and the second is used to find ways for UPFCs to mitigate the attacks. By repeating the two cycles it will be possible to incrementally harden the system against the most probable attacks and failures.

2 Iterative Hardening

The proposed technique for identifying system vulnerabilities and potential ways to rectify them is based on a basic game theory approach similar to that proposed in [1]. In this approach, two distinct games are played: one by an attacker and one by a defender.

2.1 The Attacker's Game

The goal of the attacker's game is to identify the brittle areas in the network. The actual goal of the attacker is to cause the most damage with the least effort. Ideally the attacker will select a few lines that will cause a total blackout. The attacker's game can be thought of as a simple discrete maximization problem, such as:

$$\arg\max_{\alpha} F(\emptyset,\beta) - F(\alpha,\beta) + G(\alpha,\beta) \qquad (1)$$

where:

- α is the attack plan, a schedule of what lines to remove and when to remove them
- β is a set of parameters for the power system, including load profiles
- $F(\alpha,\beta)$ is a function that simulates the power system and determines the total amount of power delivered
- $G(\alpha,\beta)$ is a reward function for encouraging the simpler attacks. β is included so that parameters of the power system, such as line length and location, may be used evaluate the complexity.

The term $F(\emptyset,\beta) - F(\alpha,\beta)$ measures the amount of power delivery lost due to the attack. The reward function, $G(\alpha,\beta)$, may also be dependent on the degree of power loss, so a three step plan may be preferred to a two step plan if the increase in damage is substantial. This maximization problem represents the typical intent of a malicious attack (maximal damage with minimal effort). (Note that the value of $F(\emptyset,\beta)$ is constant)

Power system parameters and operating conditions are nearly impossible to predict in advance, so the game can either assume that: 1) the attacker will try to take advantage of a peak load time and assume a specified worst case β, or 2) that β can be considered a random variable and, at the expense of considerably more computation, the expectation can be used:

$$\arg\max_{\alpha} E[F(\emptyset,\beta) - F(\alpha,\beta) + G(\alpha,\beta)] \qquad (2)$$

Exhaustive search can be used to find the most significant attacks on small systems, but unfortunately the problem search space grows exponentially with the attack size, so it is infeasible for large systems. At this time, there are no efficient techniques known for optimal search of this problem; however, some important observations can be made: 1) It is expected that changing a single element of an attack may make the attack incrementally better, but there is no known method of identifying which change is optimal without exhaustive search and 2) It is expected that mixing elements of two good attacks may yield a better attack

A technique known as an Evolutionary Algorithm (EA) is an ideal candidate for searching large combinatorial search spaces that exhibit these properties. EAs are loosely based on the concept of Darwinian evolution. Problem solutions are encoded in individuals (in our case a list of line outages). A population of several individuals is "evolved" by iteratively applying a fixed cycle of evolutionary operations. At each iteration, the fitness of all members of the population is determined by measuring how good each member is relative to the others using (1). The evolutionary operators are: (1) selecting individuals for reproduction with a bias towards fitter individuals, (2) applying variation mechanisms inspired by biological systems such as recombination (implements II) and mutation (implements I), (3) selecting individuals to survive to the next cycle from the combined "adult" individuals and their offspring, with a bias towards fitter individuals, The evolutionary cycle continues until a suitable termination condition has been achieved, such as reaching a performance plateau.

2.2 The Defender's Game

Since the end goal is to demonstrate that UPFCs can defend the system against the weaknesses identified by the attacker, the defender's goal is to minimize the system's brittleness, which can also be expressed as a discrete maximization problem:

$$\arg\max_{\beta} E[F(\alpha,\beta) + H(\beta)] \qquad (3)$$

Where $H(\beta)$ is a reward function that encourages using as few UPFCs as possible, the expectation is taken over a set of likely attacks, and only the components of β that correspond to UPFC locations can be changed. By maximizing (3), the defender is selecting places to install UPFCs that maximize the amount of power delivered over all the attacks to which the system was the most vulnerable.

The set of potential attacks will be taken directly from the best solutions to the Attacker's Game, and the probability of their incidence can be based on the same ranking used by the attacker (their complexity, $G(\alpha,\beta)$) or may assume that the probability of attack is related to the amount of damage incurred ($F(\emptyset,\beta) - F(\alpha,\beta)$). The latter corresponds to a mini-max game, where the defender minimizes the damage done by the attacker's best possible attacks.

Selecting installation locations for UPFCs is also a combinatorial problem with no known, optimal solution, but, as with selecting attacks, random variation and combination of good solutions may yield better solutions, so, again, an EA is a good mechanism to select installation configurations. This assumes that all the installed UPFCs operate optimally with respect to the performance criteria, which will be covered in Section 3.3.

2.3 Iterative Hardening

Defending against a single attack alone does not provide any significant improvement in fault tolerance if there are other attacks of nearly equal complexity and damage. The real goal is to demonstrate that a few well placed UPFCs can substantially harden power grids.

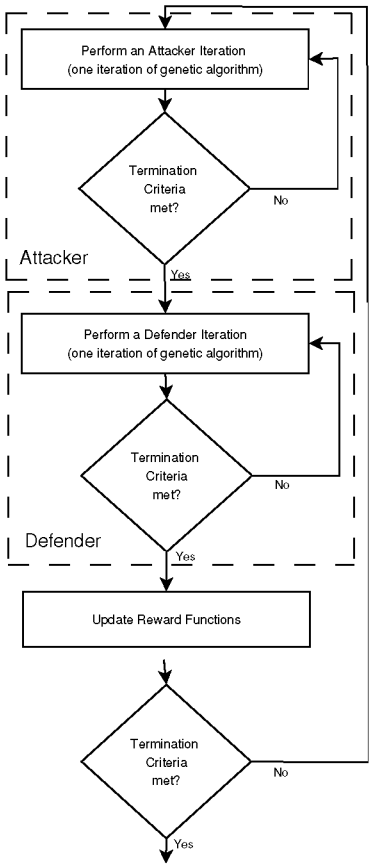

Fig. 1. Computational Flow Chart of Attacker and Defender Algorithms

The attacker's EA is designed to find the simplest significant faults, while the defender's EA is designed to install the fewest number of devices necessary to significantly harden the grid against those attacks. Since the attacker's choices will change based on the system configuration, these two algorithms need to be run in an iterative cycle to incrementally improve the system.

The attacker's algorithm will provide an adequate source of attacks for each potential system configuration, while the defender's algorithm will continually improve the system defenses in order to escalate the complexity of significant attacks. As such, it is expected that both the reward functions will need to be "cooled" as the two algorithms alternate back and forth to allow for increasingly complicated attacks and increasing numbers of FACTS installations. Fig. 1 shows a flow chart of the sequence in which the two algorithms will be used and Fig. 2 shows the basic data flow.

3 Simulation

An accurate simulation of the power system, represented by the function $F(\alpha, \beta)$ above, is vital in order to achieve meaningful results. To be useful, the simulation must:

1) Be fast enough for repeated evaluations needed by a EA
2) Be able to simulate line failures
3) Be able to simulate all twelve UPFC control modes as well as install and remove UPFCs

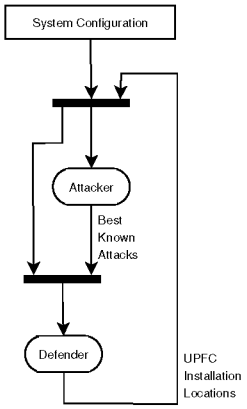

Fig. 2. Data Flow of the Attacker and Defender Algorithms

4) Provide a distinct means of comparing the quality of different attacks and different defenses
5) Be as accurate a model as an actual attacker would be likely to use

The first four criteria can be met via modification to a traditional power system technique known as Loadflow. The fifth criteria is subjective, however the form of simulation presented here is based on common analysis techniques used by power engineers to determine system faults and is one of the most likely starting places for a vulnerability assessment. Moreover, all the information required for this type of attack simulation would be readily available to a potential attacker.

3.1 Power System Steady-State Model

The most straight forward approach to steady-state power system simulation is a technique known as Loadflow. Loadflow models a power system as a collection of buses, which can be either a generator, a power customer, or both, and a set of power lines connecting the buses together. At each bus there are four state variables, and, depending on the specific combination of generators and power consumers at the bus, two of the state variables are known and the other two are unknown. Loadflow is merely a technique that solves for the unknown state variables. The four state variables are:

P_j	the real power load at bus j
Q_j,	the reactive power load at bus j
$v_{e,j}$	the real component of the voltage at bus j, $Re\{V_j\}$
$v_{h,j}$	the reactive component of voltage at bus j, $Imag\{V_j\}$

Note that the voltage is a sinusoidal signal and can be represented in polar form with a magnitude, $|V_j|$, and a phase angle (relative to a reference bus), $\angle V_j$. For the version of Loadflow used here the voltage is converted to rectangular form, $v_{e,j} + iv_{h,j}$. There are three types of buses in the system, and the type of bus indicates which variables are known and which are unknown:

Generator Buses are directly connected to a large generator. It is assumed that the power, P_j, and voltage, v_j, at these buses is constant due to the generator. The reactive power supplied by the generator, Q_j, and the phase angle of the

voltage, δ_j, are unknown. Note that there are practical limits on the amount of reactive power a generator can supply, which are enforced by the simulation described here.

Load Buses represent the bulk of the buses in a system, which have a known real power load, P_j, and a known reactive power load, Q_j. Generally these represent the load being used by customers but may also represent power being injected into the system that cannot be explicitly represented as a generator (discussed later). The voltage, v_j, and phase angle of the voltage, δ_j, are unknown.

The Slack Bus is a special generator in the system which is used: 1) as a reference against which all other phase angles are measured ($\delta_j = 0$ by definition), and 2) as a supply for additional real power to make up for system losses. At all other buses a known power is either injected or withdrawn, however the power lines themselves require power to operate. The slack bus represents a "free" source of real power (the slack) to make up for the power consumed by the transmission system itself, known as system losses.

Power systems are governed by Kirchhoff's power laws, which ensure that the sum of the power at a bus is zero. I.e., the power that enters the bus must also leave the bus. Kirchhoff's laws for an AC transmission grid can be represented as one set of equations for the real component of power and a second set for either the reactive component or voltage depending on the type of bus. All buses except the slack bus must have balanced real power:

$$\begin{aligned} P_j \quad & -v_{e,j} \sum_{k}^{buses} \left(g_{j,k} v_{e,k} - b_{j,k} v_{h,k}\right) \\ & v_{h,j} \sum_{k}^{buses} \left(g_{j,k} v_{h,k} + b_{j,k} v_{e,k}\right) \quad = 0 \end{aligned} \tag{4}$$

$$\begin{aligned} Q_j \quad & +v_{e,j} \sum_{k}^{buses} \left(g_{j,k} v_{h,k} + b_{j,k} v_{e,k}\right) \\ & +v_{h,j} \sum_{k}^{buses} \left(g_{j,k} v_{e,k} - b_{j,k} v_{h,k}\right) \quad = 0 \end{aligned} \tag{5}$$

while the generator buses have a constant voltage:

$$|V_j| - \left(v_{e,j}^2 + v_{h,j}^2\right) = 0 \tag{6}$$

where:

$g_{j,k}$ the conductance from bus j to bus k
$b_{j,k}$ the susceptance from bus j to bus k

Note that subscript e indicates the real component of a complex variable and the subscript h indicates the imaginary component of a complex variable. (4) assures everything but the slack bus meets Kirchhoff's law for real power. (5) ensures that load buses meet Kirchhoff's law for reactive power as well, while (6) ensures that generators, which generate an unknown amount of reactive power and thus violate (5), operate at a fixed voltage.

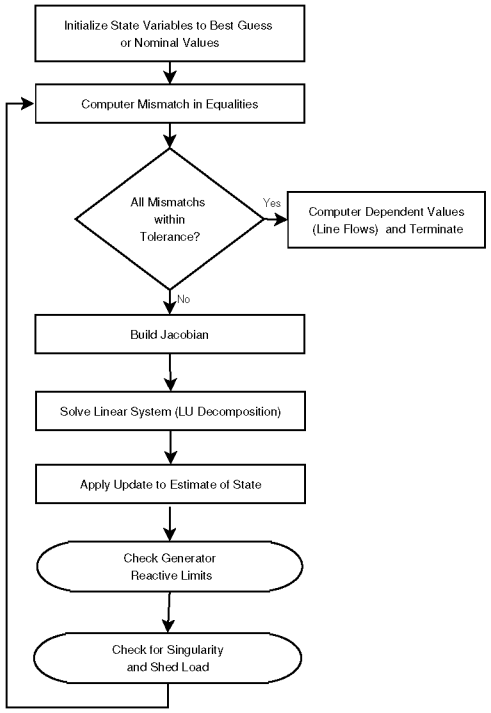

Fig. 3. The Newton-Raphson Loadflow Estimation Process

Since each bus has an equation for real power (P_j) and either an equation for reactive power (Q_j) or an equation for voltage magnitude ($|V_j|$), there are a total of $2N$ quadratic equations and $2N$ unknowns for a system with N buses. The system of equations is generally solved via the Newton-Raphson method, which uses the first-order Taylor series approximation of (4), (5), and (6) to iteratively update an estimate of the values of the unknown variables.

The Newton-Raphson method starts with an initial guess of state variables, which is either based on a prior known state or specified nominal values. The iterative process then updates these values until the error in the equalities of (4), (5), and (6) are within an appropriate error tolerance.

A basic Loadflow algorithm which relies on the Newton-Raphson technique is shown in Fig. 3. The Newton-Raphson technique is commonly used in power systems for a variety of reasons:

1) State variables are generally close to either a known or a nominal value, so it is easy to select an "initial guess" for state variables,
2) the technique generally has quadratic convergence, and hence only requires a few iterations,
3) the power flow equations are sinusoidal in nature and are well behaved with regard to minor perturbations,
4) in the Newton-Raphson method, the power flow equations are a sparse, linear system and the underlying techniques, such as using LU decomposition, are computationally efficient.

Generators produce both real power, which can be used for real work, and a form of oscillating power called reactive power.

Reactive power is a vital component of AC power systems and may be either consumed or produced by the power lines themselves, as well as by generators or customers. As power lines fail, other lines begin to transfer the excess power and may require additional reactive power to do so. The generators in the system both produce or consume reactive power to ensure that the total reactive power in the system is balanced, however each generator has a limit on the amount of reactive power it can supply or absorb. Since reactive power demands change as the system loading changes during outages, it is vital to be able to honor the reactive generation limits of the system's generators. A common method to enforce these limits is to monitor the reactive power each generator is supplying on each iteration of the Newton-Raphson loop. If a generator exceeds either the minimum or maximum reactive generation limit, the generator bus is changed to a load bus with P_j set to correspond to the power injected by the generator, Q_j set to correspond to the maximum amount of reactive power that the generator can absorb or consume depending on which limit was exceeded and the voltage. The voltage v_j then becomes an unknown variable.

3.2 Detecting and Enforcing Convergence

As lines are removed from the system, two significant problems may occur, either of which can prevent traditional Loadflow techniques from working: islanding and exceeding system capacity.

Islanding is where separate "islands" develop which effectively separate the system into multiple independent systems. Typically when this occurs at least one of the newly formed systems will be unable to meet the equality constraints. There are three possible cases: 1) islands that lack a swing bus and have no mechanism to compensate for the real-power losses in the lines, 2) islands that have load but no generation can not satisfy customer demand, and 3) islands that have generation but no load have a surplus of power with no consumers.

Islanding can be easily detected and corrected via graph traversal. A simple mechanism starts from an arbitrary bus and recursively visits all unvisited buses to which it is connected, marking each as visited. If, upon completion, any unvisited buses exist then the visited group represents a new island, and the process is repeated with the first unvisited bus. This process is repeated until all nodes are assigned to islands. When complete, islands with only generators or only loads are discarded. Any remaining islands that lack a slack bus are modified so that the largest generator in each becomes a slack bus.

Exceeding capacity is when the system is not physically able to transmit power in a way that satisfies all the constraints (the power flow constraints of (4), (5), and (6) as well as the generator reactive limits).

In many cases the constraint equations cannot be met because the system no longer has the physical ability to carry enough power to satisfy the load being demanded. When this happens the original assumptions about the known variables are incorrect and no values of state variables can meet the constraint equations, so the original assumptions on load and generation must be changed to bring the system back to a solvable state. In systems losing transmission facilities the most common problem is having a load bus who's lines can not carry enough power to satisfy the specified demand, P_j. To bring the system back to a solvable state some of the load must be shed (reduce P_j). In the framework devised here, the attackers must assume, as in typical min-max game theory, that the defender will make optimal choices with the resources available. Thus ideally both the attackers and defenders will assume that only the minimum amount of load necessary will be shed to bring the system back to a solvable state.

A mechanism for optimal updates of the state variables, which can also be used to detect an ill-conditioned system, was proposed in [2]. The authors noticed that, when using the rectangular formulation of power flow as given previously, the complete Taylor series expansion only requires three terms. Moreover, these terms have a particularly efficient form and, most importantly, an exact solution can be found via the use of an appropriately chosen scalar multiplier. The optimal multiplier is easy to compute and provides a substantial improvement in system solvability.

In [3], Overbye notes that the solvable region of the state space is separated from the unsolvable region by a border on which the Jacobian used in the Newton-Raphson process becomes singular. When the system is solvable, the optimal multiplier remains near unity. Overbye also shows that infeasible systems can be detected by monitoring the magnitude of the optimal multiplier [3] . When it is sufficiently small, no state assignments will be able to satisfy the load demands of the system and load shedding must be performed.

In [4], an extension of [3], a technique was proposed to bring the system back to an optimal solvable point with a load shedding technique that maximizes the amount of demand that can be met. This optimal load shedding relies on the use of the optimal multiplier technique to bring unsolvable systems back to the solvable boundary.

Although this optimal form of load shedding may not be in use on a given power system, it is unlikely that an attacker would know the exact load shedding capabilities and procedures, so they would assume a conservative case. By using the optimal load shedding, the attacker's mini-max perception, i.e., that the system will be as well defended as possible, is maintained.

3.3 UPFC Model

A perfect model of a UPFC consists of a voltage source connected to a bus in shunt and another voltage source connected in series with a line. The only constraints imposed on the model are the magnitude of the shunt voltage source, which is typically near the magnitude of the source bus, and that the real power injected or consumed by the series source must be supplied by the shunt source, which ensures there is no net real power injected into the system.

The typical UPFC model has twelve unique forms of control and typical Loadflow implementations assume that

one particular mode will be used [8]. In the plan presented here, the desired control mode is unknown and may change depending on the conditions of the system, so a simpler model is used in which the shunt voltage, series voltage, and series phase angle are specified directly. The shunt phase angle is left free to ensure that the shunt can meet the power consumption demands of the series source.

The UPFC model used here is novel in two respects: 1) it does not assume the control mode, allowing for the UPFC to change operating modes in different simulated scenarios to achieve optimal control for each, and 2) the rectangular coordinate system is used to comply with the optimal multiplier method, which is used to allow for optimal load shedding.

The optimal settings for the UPFCs can be found via simple optimization of a metric that will ensure maximal power delivery prior to failure. Prior work has shown that sequential quadratic programming is sufficient to directly find UPFC settings for a simpler model [5], however it is expected that the same technique will apply to this more general model.

3.4 Line Failure

Line failures, the prime component of cascading outages, occur because of excessive current overheating power lines, which eventually sag to the point that they either contact a ground source or physical failure. A simple line model has two parameters for each line: 1) a maximum current rating which it can safely carry and 2) a maximum ampacity, or cumulative current, that can be carried when the current rating is exceeded. The time until a line fails can be calculated based on the results of the Loadflow. For each line which is exceeding its current rating, the failure time is the amount of "remaining ampacity" divided by the current through the line. The "remaining ampacity" continually diminishes until either the line fails, or the line is no longer exceeding capacity and has had suitable time to "cool" to relieve the excess heat generated.

3.5 Simulation Overview

The full power system simulation overview can be seen in Fig. 4. As can be seen, there are a variety of nested loops for selecting optimal UPFC settings, removing naturally failing lines, and removing attacked lines. In addition, the Loadflow itself is a loop performing a significant amount of computation.

4 Conclusions and Future Work

By combining a simplistic UPFC model, which is amenable to optimal control, with a simulation that is capable of simulating the power system's state as components fail, a simple line failure estimate, and EAs, it should be possible to provide a rudimentary plan for significantly improving the robustness of power grids. EAs will use the simulation to both identify and repair weaknesses in the system. This combined approach uses the super set of functionality provided by a general model of the UPFC to identify and fix weaknesses.

Preliminary testing of the blueprint presented here with a more simplisitic injection model of the UPFC has shown that the basic ideas presented are sound. Future work will focus on utilizing more realistic models of the UPFC and qualitative analysis of the results.

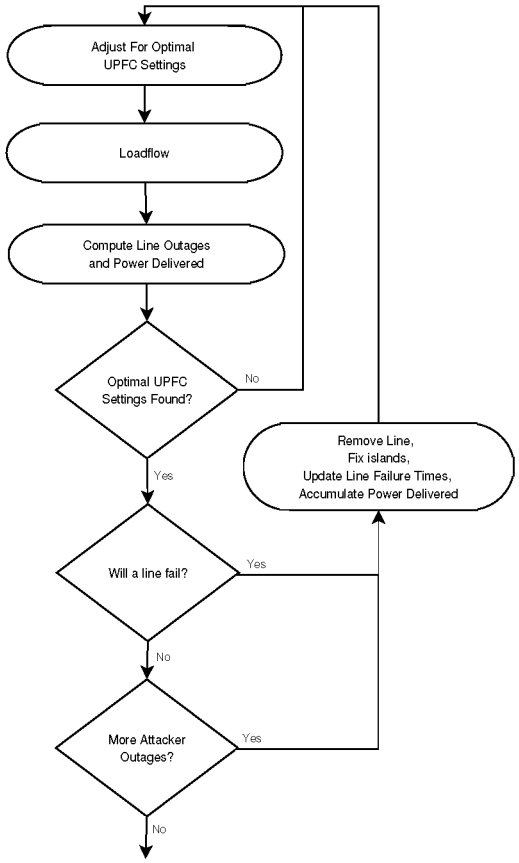

Fig. 4. Power System Simulation for Cascading Failures

References

[1] V. M. Bier. *Game-Theoretic and Reliability Methods in Counter-Terrorism and Security*, chapter 3, pages 23–42. World Scientific Publishing Co, 2005.

[2] S. Iwamoto and Y. Tamura. A load flow calculation method for ill-conditioned power systems. *IEEE Transactions on Power Apparatus and Systems*, PAS-100(4):1736–1743, April 1981.

[3] T.J. Overbye. A power flow measure for unsolvable cases. *IEEE Transactions on Power Systems*, 9(3):1359–1365, 1994.

[4] T.J. Overbye. Computation of a practical method to restore power flow solvability. *IEEE Transactions on Power Systems*, 10(1):280–287, 1995.

[5] William M. Siever, Daniel R. Tauritz, and Ann Miller. Improving grid fault tolerance by optimal control of FACTS devices. *Proceedings of Artificial Intelligence in Energy Systems and Power, 2006*, 1, February 2006.

[6] United States. Congress. House. Select Committee on Homeland Security. Subcommittee on Cybersecurity, Science, and Research and Development. *Implications of power blackouts for the nation's cybersecurity and critical infrastructure protection : joint hearing of the Subcommittee on Cybersecurity, Science, and Research and Development and the Subcommittee on Infrastructure and Border Security of the Select Committee on Homeland Security, House of Representatives, One Hundred Eighth Congress, first session, September 4, 2003 and September 23, 2003.* U.S. G.P.O., 2005.

[7] United States Department of Energy. National transmission grid study, May 2002.

[8] Xiao-Ping Zhang and K.R. Godfrey. Advanced unified power flow controller model for power system steady state control. In *Proceedings of the 2004 IEEE International Conference on Electric Utility Deregulation, Restructuring and Power Technologies*, volume 1, pages 228–233, 2004.