Methodology for Identifying Near-Optimal Interdiction Strategies for a Power Transmission System

Vicki M. Bier  
*University of Wisconsin–Madison*, bier@engr.wisc.edu

Eli R. Gratz  
*University of Wisconsin–Madison*

Naraphorn J. Haphuriwat  
*University of Wisconsin–Madison*

Wairimu Magua  
*University of Wisconsin–Madison*

Kevin R. Wierzbicki  
*University of Wisconsin–Madison*

Follow this and additional works at: [http://research.create.usc.edu/published_papers](http://research.create.usc.edu/published_papers)

Recommended Citation

[http://research.create.usc.edu/published_papers/119](http://research.create.usc.edu/published_papers/119)

This Article is brought to you for free and open access by CREATE Research Archive. It has been accepted for inclusion in Published Articles & Papers by an authorized administrator of CREATE Research Archive. For more information, please contact gribben@usc.edu.
Methodology for identifying near-optimal interdiction strategies for a power transmission system

Vicki M. Bier\textsuperscript{a,\,*}, Eli R. Gratz\textsuperscript{a}, Naraphorn J. Haphuriwat\textsuperscript{a}, Wairimu Magua\textsuperscript{a}, Kevin R. Wierzbicki\textsuperscript{b}

\textsuperscript{a}Department of Industrial and Systems Engineering, University of Wisconsin-Madison, Madison, WI 53711, USA
\textsuperscript{b}Department of Electrical and Computer Engineering, University of Wisconsin-Madison, Madison, WI 53711, USA

Available online 18 October 2006

Abstract

Previous methods for assessing the vulnerability of complex systems to intentional attacks or interdiction have either not been adequate to deal with systems in which flow readjusts dynamically (such as electricity transmission systems), or have been complex and computationally difficult. We propose a relatively simple, inexpensive, and practical method ("Max Line") for identifying promising interdiction strategies in such systems. The method is based on a greedy algorithm in which, at each iteration, the transmission line with the highest load is interdicted. We apply this method to sample electrical transmission systems from the Reliability Test System developed by the Institute of Electrical and Electronics Engineers, and compare our method and results with those of other proposed approaches for vulnerability assessment. We also study the effectiveness of protecting those transmission lines identified as promising candidates for interdiction. These comparisons shed light on the relative merits of the various vulnerability assessment methods, as well as providing insights that can help to guide the allocation of scarce resources for defensive investment.

\textcopyright{} 2006 Elsevier Ltd. All rights reserved.

Keywords: Vulnerability assessment; Transmission systems; Greedy algorithm; Interdiction; Hardening

1. Overview

Electric power transmission grids are an important component of the modern economy [1]. We rely on electricity for communications, light, water, transportation, heating, and industry, among other critical uses of power. As a result, numerous researchers have studied the risk of electric blackouts. For example, Carreras et al. [2] and Chen et al. [3] studied blackouts in the North American electric power transmission system from 1984 to 1999 and found that blackout sizes show a power law distribution. At a more theoretical level, Carreras et al. [2] and Liao et al. [4] studied the probability of cascading failures in simple models of electric power networks; Mili et al. [5] proposed methodologies and algorithms to assess the conditional probability of catastrophic failure in electric transmission systems; and Phadke [6] described possible mechanisms of hidden (i.e., undetected or latent) failures in electric power systems.

Vulnerability studies have been recognized as being important in assessing the reliability of critical infrastructure and helping to guide defensive investments since even before the terrorist attacks on September 11, 2001 [7]. See for example Guzic [8] for an application of vulnerability analysis to military systems, and Ezell et al. [9–11] for applications to water systems. Methods for assessing and improving the vulnerabilities of critical infrastructure have also been the focus of substantial government research programs; see for example Los Alamos National Laboratory [12].

One of the most promising approaches for vulnerability assessment is that proposed by Apostolakis and Lemon [13], who present a methodology to identify critical locations in infrastructure. In particular, this methodology explicitly takes into account the complex networked structures of many infrastructure systems. However, their
approach is limited to distribution systems (with one-directional flows), in which the consequences of interdicting a given line can be determined in a straightforward manner.

The method of Apostolakis and Lemon [13] has a different purpose than ours, since it is designed to identify the geographic locations of key vulnerabilities in numerous collocated infrastructures. Still, it would be worthwhile to extend this methodology to transmission systems, since Zimmerman et al. [14] (in a study of the risks, consequences, and economic impacts of electricity system problems) state that the majority of electricity outages and terrorist attacks on electricity systems involve damage to transmission equipment. This will require some method of accounting for the fact that transmission systems can have bi-directional flows, and that flows can therefore be reconfigured dynamically after one or more transmission lines have been removed.

Salmeron et al. [15] model interdiction of lines and/or nodes in an electricity transmission system using a non-linear program. However, their formulation of the problem is difficult to solve, since it involves a nested optimization (minimization of costs to determine power flows on the network, with maximization of damage to identify an interdiction strategy), with the outer loop entailing maximization of a convex rather than a concave function. They are able to solve their model only using a heuristic algorithm, so the resulting interdiction strategies are not known to be optimal. The non-linear programming approach also seems impractical for use on large problems, so we based our methodology on that of Apostolakis and Lemon [13].

In extending the work of Apostolakis and Lemon [13] to transmission systems, we initially considered the option of taking out transmission lines randomly, in an approach similar to that applied by Schaefer and Bajpai [16,17] (see also [18]) in the context of load-bearing members of buildings or other structures. However, while potentially useful in anticipating “unforeseen hazards” in general, that approach did not seem adequate for modeling the effects of terrorist actions or other intentional malevolent acts, where presumably some intelligence is devoted to determining which elements to attack. It also had the potential to be computationally costly, if large numbers of random “attacks” were needed to identify a few that were seriously damaging. Therefore, we decided to take out transmission lines in decreasing order of load. Albert et al. [19] indicated that “connectivity loss is significantly higher” when interdiction of transmission-system components is in decreasing order of load rather than random.

The resulting method offers a viable way of identifying strategies that result in substantial unmet demand for electricity. Our method extends the work of Apostolakis and Lemon [13] from distribution networks to transmission networks, yielding results that compare favorably to those of Salmeron et al. [15]. The methodology reflects the dynamic nature of transmission grid power flow, but is simple enough to implement in practice even for relatively complex systems. We use the same nested optimization approach as Salmeron et al. [15], but our method avoids their computational difficulties, since in our method the outer maximization loop is trivial and can be solved by inspection.

2. Case study and approach

We apply our method to the IEEE Reliability Test System—1996 [20], which is designed to be representative of typical transmission systems. We analyze both the IEEE One Area RTS-96, and the IEEE Two Area RTS-96 (which combines two separate areas using three interconnections). We model the IEEE One Area RTS-96 using 24 nodes and 38 arcs, and the IEEE Two Area RTS-96 as a network consisting of 48 nodes and 79 arcs.

We base our analysis on DC power flow, with optimal dispatch of the generators. DC power flow is a linearized, static model of the real power flows on the network; this is a standard and useful simplification. Generators, loads, transformers, transmission lines, and other specialized devices have more elaborate models that are needed in some situations; actual power networks also exhibit reactive power flows, manual and automatic control actions, nonlinear and transient dynamics, and hybrid system effects due to protection and control system limits that can affect the consequences of network attacks. For example, an attack on a highly stressed network could lead to loss of an equilibrium solution, collapsing voltages, and a widespread blackout. We do not model these more elaborate effects in this paper. One might expect terrorists to also begin their analysis with the most essential and basic system model.

Our approach is based on three nested algorithms: a load-flow algorithm; a Max Line interdiction algorithm; and a hardening algorithm. The load-flow algorithm is used to determine optimal DC power flow dispatch on the transmission network, both before and after any interdiction of transmission lines. The Max Line interdiction algorithm identifies the transmission line transporting the most DC flow (to be removed from the network by supposed malevolent attackers), after which flows are re-optimized using the load-flow algorithm. We refer to each cycle of interdiction and re-optimization as an iteration. The hardening algorithm then simulates a system upgrade by hardening (making invulnerable) some of the transmission lines identified for interdiction by the Max Line algorithm. After hardening has been implemented, the Max Line algorithm can then be applied in successive iterations to identify “next best” interdiction strategies. These algorithms are described in Sections 3–5, respectively.

For simplicity, we consider only the interdiction of electric transmission lines (arcs), not nodes (such as transformers). We compare our methods and results to those of Salmeron et al. [15] and Apostolakis and Lemon [13].
We now introduce the following notation used in describing our algorithms:

- **B**: set of nodes in the network, indexed by \( i \)
- **L**: set of lines in the network, indexed by \( k \)
- **\( G_i \)**: generation at node \( i \)
- **\( L_i \)**: load supply at node \( i \)
- **\( L_i, \text{demand} \)**: load demand at node \( i \)
- **\( F_k \)**: negative or positive power flow on line \( k \) (to reflect bi-directional flow)
- **\( F_{k, \text{max}} \)**: maximum power flow permitted on line \( k \) (in absolute value)
- **\( F \)**: vector of \( F_k \) for all \( k \in L \)
- **\( P_i \)**: total power at node \( i \) (given by \( G_i - L_i \))
- **\( P \)**: vector of \( P_i \) for all \( i \in B \)
- **\( W_{\text{gen}, i} \)**: cost of generation at node \( i \)
- **\( W_{\text{shed}, i} \)**: cost of load shedding at node \( i \)
- **\( M \)**: DC load flow matrix relating the line flows \( F \) to the power levels \( P \)
- **\( k^*(t) \)**: index of the line with the highest absolute value of power flow at iteration \( t \) of the Max Line algorithm
- **\( K(t) \)**: set of lines attacked in iteration \( t \) of the Max Line algorithm
- **\( A \)**: ordered set of (sets of) attacked lines
- **\( A(s) \)**: ordered set of (sets of) attacked lines after iteration \( s \) of the hardening algorithm
- **\( H \)**: set of hardened lines

### 3. Load-flow algorithm

To simulate power flows on the network, we use a DC load-flow model (Salmeron et al. [15]; Carreras et al. [2]). This optimization problem minimizes the cost function

\[
\sum (G_i W_{\text{gen}, i} - L_i W_{\text{shed}, i})
\]

subject to the following constraints:

1. \( 0 \leq G_i \leq G_{i, \text{max}} \) (2)
2. \( -L_i, \text{demand} \leq -L_i \leq 0 \) (3)
3. \( -F_{k, \text{max}} \leq F_k \leq F_{k, \text{max}} \) (4)
4. \( F = MP \) (5)

For any given set of available lines, both generation and load flows are assumed to be determined as the solution to the above optimal dispatch problem. The objective is to minimize the combined cost of generation and unmet demands. Constraint (2) ensures that no generator exceeds its maximum power output. Constraint (3) ensures that the load supplied at any given node does not exceed the corresponding demand. Constraint (4) ensures that power flows on the lines remain within safe margins. Constraint (5) is a matrix equation relating the vector of power levels at each node with the vector of power flows on each line through the constraint matrix \( M \). For details, consult Carreras et al. [2] or Salmeron et al. [15].

In general, the costs or weights, \( W_{\text{gen}, i} \) and \( W_{\text{shed}, i} \), can take on different values at each node, representing different prices at each generator and different levels of importance of each load respectively. However, in our case, we set each generator price to 1 and each load importance to 100, as in Carreras et al. [2].

### 4. The Max Line interdiction algorithm

We assume that the attacker uses a greedy algorithm where, at each iteration, the line with the maximum flow is effectively disabled or removed from the system. The load-flow algorithm is then run to compute the optimal power dispatch on the revised system. The interdiction algorithm is terminated after a predetermined number of steps. The algorithm can be summarized as follows:

Step 1: The system is initialized at iteration \( t = 0 \), at which time the sets \( A \) and \( K(t) \) are empty. The set \( H \) is also empty, unless the hardening algorithm has already been run one or more times, in which case \( H \) contains the lines selected for hardening as a result of that algorithm.

Step 2: The load-flow algorithm is run, and optimal dispatch is determined. The resulting load shed or unmet demand (which may be zero), \( L_i, \text{demand} - L_i \), at each bus \( i \in B \) is recorded.

Step 3: The line \( k^*(t) \) whose absolute value of power flow is given by \( \{ \max | F_k(t) : k \in L - H \} \) is found, and \( k^*(t) \) is added to \( K(t) \). In the case where there is more than one such line, \( k^*(t) \) is chosen at random from those lines whose absolute value of power flow is equal to \( \{ \max | F_k(t) : k \in L - H \} \). Any lines in close geographical proximity to \( k^*(t) \) are also added to \( K(t) \).

Step 4: The lines in \( K(t) \) are removed from the network by setting \( F_{k, \text{max}} \) to zero for all \( k \in K(t) \). These changes remain in effect through all subsequent iterations of the interdiction algorithm. The set \( K(t) \) is also added as the \( t \)th element of the ordered set \( A \).

Step 5: The index \( t \) is incremented by 1, and the algorithm returns to Step 2, unless it has reached the predetermined maximum number of iterations.

### 5. Hardening algorithm

The hardening algorithm can be run after the Max Line interdiction algorithm to simulate an “improvement” of the system to reduce the consequences of an attack. In this case, the interdiction algorithm is rerun after each successive run of the hardening algorithm to investigate the effectiveness of the postulated system hardening.
The hardening algorithm is summarized below:

Step H-1: The system is initialized at iteration $s = 0$, with the set $H$ empty.

Step H-2: The Max Line interdiction algorithm is run for some number of iterations $t$, resulting in an ordered set $A(s)$ consisting of $t$ sets of attacked lines.

Step H-3: The first $n$ elements of $A(s)$, $K(1)$ through $K(n)$, are chosen for hardening, and added to the set of hardened lines $H$. (In the application of this algorithm in Section 6, we choose $n = 5$ for the one-area network and $n = 10$ for the two-area network.) The hardened lines are no longer candidates for interdiction, as shown in Step 3 of the Max Line interdiction algorithm.

Step H-4: The hardening index $s$ is incremented by 1, and the program returns to step H-2, unless it has reached the maximum number of hardening iterations.

6. Results

In Fig. 1, we graph the load shed pattern that would result from the first 14 iterations of the Max Line algorithm applied to the one-area system. Each of the iterations on the horizontal axis represents the removal of a line or two or more lines in close geographical proximity as described in RTS-96 from the network. The corresponding value on the vertical axis shows the unmet load after optimal re-dispatch of power flow on the remaining lines.

In our proposed interdiction plan, the first three iterations of the algorithm (leading to the interdiction of four transmission lines) in the one-area system result in a 44% loss of load, indicating that attacking only 11% of the transmission lines in the system would result in significant unmet demand. The first nine iterations (corresponding to 11 transmission lines, and roughly a third of the lines in the system) result in a 56% loss of load. Removing additional lines does not result in substantial additional loss of load, because the system is already largely unconnected and serving primarily local loads by this point.

We now compare the results of our methodology with those obtained by Salmeron et al. [15], who developed two candidate interdiction plans for the IEEE One Area RTS-96. Since we do not consider the interdiction of substations in our method, we therefore compare our results only to the line interdiction strategy (Plan 2) developed by Salmeron et al. [15]. Nine lines are interdicted in Plan 2 (corresponding to six sets of lines in close geographical proximity).

As illustrated in Fig. 1, Plan 2 of Salmeron et al. [15] results in shedding about 48% of the total system demand after six sets of lines have been removed (Salmeron et al. [15] do not provide intermediate results showing the load shed when smaller numbers of lines are removed). By contrast, the Max Line algorithm results in a 50% load shed after six iterations (corresponding to eight lines). Note that the transmission lines interdicted in the strategy proposed by Salmeron et al. [15] differ somewhat from those interdicted by our strategy.

We also study the IEEE Two Area RTS-96. Plan 3 proposed by Salmeron et al. [15] sheds approximately 44% of the system load after the removal of 11 sets of lines in close geographical proximity (corresponding to 17 transmission lines). By contrast, the Max Line algorithm results in 45% load shed after 11 iterations (corresponding to 15 lines) (Fig. 2).

Thus, the Max Line interdiction strategy reasonably approximates the load shed by the near-optimal attack plan developed by Salmeron et al. [15]. Note, however that Salmeron et al. [15] do not weight all transmission-system components equally. Therefore, it is possible that their
algorithm would perform better than ours if both algorithms were applied using the same weights. However, Salmeron et al. [15] specifically state that the weights are chosen to improve the efficiency of their algorithm. In any case, we find the performance of the two approaches to be remarkably close.

We now compare the Max Line strategy against random removal of lines from the one-area transmission system. In this example, the first five iterations (corresponding to seven randomly chosen transmission lines) shed only 9% of the total system demand. By contrast, the first five iterations of the Max Line algorithm (corresponding to seven transmission lines) result in a loss of approximately 46% of the total system demand, as shown in Fig. 3. We conclude that random interdiction appears to be an inefficient strategy for identifying vulnerabilities (although even random interdiction can have a significant effect on system connectivity if a sufficiently large number of lines are interdicted, as shown in Fig. 3).

Next, we apply the hardening algorithm to simulate an upgrade of the system, as described in Section 5. This examines the impact of protecting attractive targets in both the IEEE One Area RTS-96 and the IEEE Two Area RTS-96. H0 represents the original interdiction strategy, as shown in Figs. 4 or 5, as appropriate. Strategies H1, H2, and H3 show the interdiction strategies obtained after each of three iterations of the hardening algorithm.

For the IEEE One Area RTS-96, strategy H0 (with no hardening) results in a loss of 56% of the total system demand. By contrast, strategy H3, after hardening 15 sets of transmission lines in close geographical proximity (approximately 39% of all lines in the system) still results in a loss of 42% of the total system demand.

We now study the same cycle of hardening and interdiction for the IEEE Two Area RTS-96. The results are shown in Fig. 5. Strategy H0 results in a loss of 56% of total system demand. Strategy H3, after hardening 39% of the transmission lines in the system, results in a loss of 39% of total system demand.

In fact, hardening can even have a negative impact on the system, resulting in slight increases in the amount of load shed for a given number of iterations. Presumably, this is because the greedy nature of our Max Line algorithm does not always identify the optimal interdiction strategy. Thus, applying the Max Line algorithm to a hardened transmission network may fortuitously result in identification of a better interdiction strategy than that found by applying the algorithm to the original non-hardened network.

Overall, our results cast doubt on the observation by Salmeron et al. [15] that “By considering the largest possible disruptions, our proposed plan will be appropriately...
conservative.” In fact, we observe that hardening even a significant percentage of the transmission lines in the system does not dramatically diminish the load that can be shed as the result of an intelligent attack. Thus, while our results compare favorably with those of Salmeron et al. [15], it is not clear that either approach will be a helpful guide to system hardening, mainly because hardening of lines seems unlikely to be cost effective.

7. Conclusions and directions for future research

In this paper, we developed a relatively simple, inexpensive, and viable method of identifying promising attack strategies. The impacts of our Max Line interdiction strategies for two sample transmission grids are comparable to interdiction strategies developed by Salmeron et al. [15]. However, our method and that developed by Salmeron et al. [15] identify different sets of vulnerable transmission lines. Therefore, a single run of either method will likely not be sufficient to identify all critical vulnerabilities. Moreover, our results suggest that hardening transmission lines is not likely to be cost effective, since interdiction can still cause substantial unmet demand even after significant system hardening.

Our work so far does have some important caveats. First, we considered transmission lines to be the only vulnerable components of a transmission system. Moreover, our interdiction and load-flow algorithms consider only power flows, and not the criticality of particular loads or demands.

In future research, this method could be extended to address other components of transmission systems, such as transformers (which would be represented as nodes rather than arcs). This is an important extension, since Zimmerman et al. [14] note that transformers are especially difficult and time consuming to replace. It would also be desirable to extend the algorithm to identify additional complexities of transmission networks (such as reactive power), and the possibility that some types of interdiction strategies may trigger cascading power failures. The possibility of cascading power failures was not considered in our algorithm, but could obviously amplify the effectiveness of line interdiction, as shown in the blackout of August 2003 [1].

Finally, it would be helpful to adapt our algorithm to take into account the importance of different loads, as done by Salmeron et al. [15]. In particular, Zimmerman et al. [14] note that disrupting electrical supply to certain demand sectors (for example, transportation, or other types of critical infrastructure that depend on electricity) could have disproportionate impacts. Such prioritization of customers, which we have not yet considered, could well provide greater justification for hardening lines serving high priority loads.

We also believe that the general approach outlined in this paper (the Max Line greedy interdiction algorithm) could be extended to identify critical components in other types of systems, such as structures [16, 17]; see also [18], water distribution systems [21], and ground transportation systems. Of course, the algorithm for re-optimizing load (in structures) or flow (in water or transportation systems) would be different from the load-flow algorithm used here for electricity transmission systems. However, we believe that the general approach embodied in the Max Line algorithm could still be applied to such systems with reasonable results.

Acknowledgements

This material is based upon work supported in part by the US Army Research Laboratory and the US Army Research Office under grant number DAAD19-01-1-0502, the US National Science Foundation under grant number ECS-0214369, and the Department of Homeland Security under grant number EMW-2004-GR-0112. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the sponsors. The authors would also like to acknowledge Prof. Ian Dobson of the Department of Electrical and Computer Engineering at the University of Wisconsin-Madison for his guidance and helpful contributions to this study.

References


