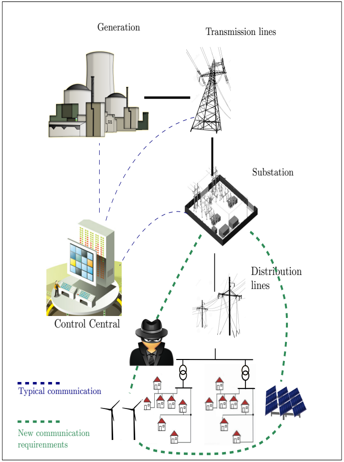
Security Assessment of Electricity Distribution Networks under DER Node Compromises

Devendra Shelar, Saurabh Amin

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

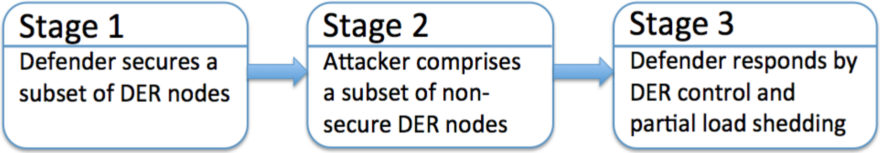
November 2, 2015

Model of DER disruptions



"Renewable electricity companies in Europe reportedly were targeted by cyberattackers at a clean power website from which malware was passed to visitors, thus giving the attackers access to the power grid."
- Richard J. Campbell, Cybersecurity Issues for the Bulk Power System.

Defender-Attacker-Defender Problem



Three-Stage Stackelberg Game

- Defender makes a security investment into a subset of DER nodes, making them non-vulnerable to compromise
- Attacker executes a resource-constrained interdiction plan (compromise DERs) to maximize the sum of loss of voltage regulation (LOVR), load shedding (VOLL), and line losses
- Defender optimally responds to attacker actions by:
  - Controlling non-compromised DERs to provide active and reactive power (VAR)
  - Partly satisfying demand at some consumption nodes;

Problem Statement

Find attacker's interdiction plan to maximize composite loss $\mathrm{L}(\psi, \phi)$, given that defender optimally responds

$$\max_{\psi=[\delta,\mathrm{sp^a}]\in\Psi} \quad \min_{\phi=[\gamma,\mathrm{sp^d}]\in\Phi} \quad \mathrm{L}(\mathrm{x}(\psi,\phi))$$

$$\text{s.t.} \quad \mathrm{x} = (\nu, \ell, sc, sg, S),$$

LOVR $\quad \mathrm{L_{VR}}(\mathrm{x}) := ||W \odot (\underline{\nu} - \nu)_+||_\infty$

VOLL $\quad \mathrm{L_{LC}}(\mathrm{x}) := ||C \odot (1-\gamma) \odot \mathrm{pc^{nom}}||_1$

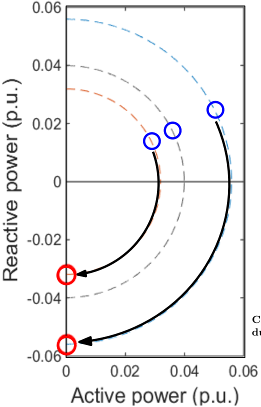
Attacker Model $\quad sg = \delta \odot \mathrm{sp^a} + (1-\delta) \odot \mathrm{sp^d}$

Defender Model $\quad sc = \gamma \odot \mathrm{sc^{nom}}$

$$S_j = \textstyle\sum_{k:(j,k)\in\mathcal{E}} S_k + s_j + z_j \ell_j$$

$$\nu_j = \nu_i - 2\mathbf{Re}(\bar{z}_j S_j) + |z_j|^2 \ell_j$$

$$\ell_j = \frac{|S_j|^2}{\nu_i}$$



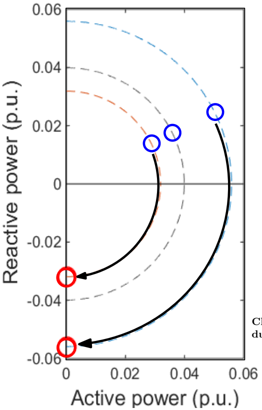
Change on set-points due to the attack

Main Results

Theorem

For a fixed defender action $\phi \in \Phi$, and a fixed attacker choice of DERs δ, the optimal attacker set-point sp^{a} is given by:

$$\mathrm{sp}^{\mathrm{a}} = \mathbf{0} - \mathbf{j}\overline{\mathrm{sp}}$$



Change on set-points due to the attack

Precedence Description

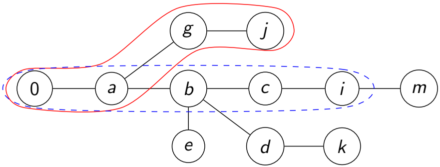


Figure : Precedence description of the nodes for a tree network. Here, $j \prec_i k$, $e =_i k$, $b \prec k$, $\mathcal{P}_j = \{a, g, j\}$, $\mathcal{P}_i \cap \mathcal{P}_j = \{a\}$.

Linear power flow (LPF)
State vector:
$\widehat{\mathrm{x}} = [\widehat{\nu}, \widehat{\ell}, sc, sg, \widehat{S}] \in \widehat{\mathcal{X}}$

$$\widehat{S}_j = \sum_{k:(j,k)\in\mathcal{E}} \widehat{S}_k + s_j + \cancel{z_j \ell_j}$$

$$\widehat{\nu}_j = \widehat{\nu}_i - 2\mathbf{Re}(\bar{z}_j \widehat{S}_j) + \cancel{|z_j|^2 \ell_j}$$

- (Linear) LPF lower bounds already investigated in Steven Low *et. al.*
- What about linear upper bounds?

$\epsilon-$Linear power flow (ϵ-LPF)

Net power consumed at node j: $s_j = sc_j - sg_j$

$\epsilon-$Linear power flow (ϵ-LPF)

State vector: $\check{\mathrm{x}} = [\check{\nu}, \check{\ell}, sc, sg, \check{S}] \in \check{\mathcal{X}}$

$$\check{S}_j = \sum_{k:(j,k)\in\mathcal{E}} \check{S}_k + (1+\epsilon)s_j$$

$$\check{\nu}_j = \check{\nu}_i - 2\mathbf{Re}(\bar{z}_j \check{S}_j)$$

Assumptions

- **Safety:** Safety bounds are always satisfied, i.e., $\forall\ (\psi, \phi) \in \mathcal{U}_B \times \Psi \times \Phi,\ \forall\ \mathrm{x}(\psi, \phi) \in \mathcal{X},\ \underline{\mu}\mathbf{1} \leqslant \nu \leqslant \overline{\mu}\mathbf{1}$.
- **No reverse power flows (NRP):** Power flows from the substation node towards the downstream nodes, i.e., $\widehat{S} \geqslant 0$. This implies that $\forall\ \widehat{\mathrm{x}} \in \widehat{\mathcal{X}},\ \widehat{\nu} \leqslant \nu_0\mathbf{1}$; similarly, for NPF model.
- **Small line losses (SL):** The line losses are very small compared to the power flows, i.e., $\forall\ \mathrm{x} \in \mathcal{X},\ z \odot \ell \leqslant \epsilon_0 S$, where ϵ_0 is a small positive number.

Attacker-Defender Problem (ADNPF)

$$[\mathrm{AD}] \quad \mathcal{L} := \max_{\psi \in \Psi} \min_{\phi \in \Phi} \mathrm{L}(\mathrm{x}(\psi, \phi)) \quad \text{s.t.} \quad \mathrm{x} \in \mathcal{X}$$

Attacker-Defender Problem (ADLPF) Lower bound

$$[\widehat{\mathrm{AD}}] \quad \hat{\mathcal{L}} := \max_{\psi \in \Psi} \min_{\phi \in \Phi} \mathrm{L}(\hat{\mathrm{x}}(\psi, \phi)) \quad \text{s.t.} \quad \hat{\mathrm{x}} \in \hat{\mathcal{X}}$$

Attacker-Defender Problem (ADUPF) Upper bound

$$[\widetilde{\mathrm{AD}}] \quad \check{\mathcal{L}} := \max_{\psi \in \Psi} \min_{\phi \in \Phi} \mathrm{L}(\check{\mathrm{x}}(\psi, \phi)) \quad \text{s.t.} \quad \check{\mathrm{x}} \in \check{\mathcal{X}}$$

Theorem

Let (ψ^*, ϕ^*), $(\widehat{\psi}^*, \widehat{\phi}^*)$ *and* $(\check{\psi}^*, \check{\phi}^*)$ *be optimal solutions to* $[\mathrm{AD}]$, $[\widehat{\mathrm{AD}}]$ *and* $[\underbrace{\mathrm{AD}}]$, *respectively; and denote the optimal losses by* $\mathcal{L}$, $\widehat{\mathcal{L}}$, $\check{\mathcal{L}}$, *respectively. Then,*

$$\widehat{\mathcal{L}} \leqslant \mathcal{L} \leqslant \check{\mathcal{L}} + \frac{\underline{\mu} N}{2\underline{\mu} + 4}.$$

- All the results that are applicable to the LPF model are also valid for the ϵ-LPF model.
- The optimal attacker strategy computed under both LPF and ϵ-LPF model can be shown to be the same.

Theorem

In an optimal security strategy, over a balanced, homogeneous tree network:

- *If a node is secure, all its children nodes must be secure.*
- *At most one level containing secure and non-secure nodes can exist.*
- *Nodes in such a level are uniformly secured.*

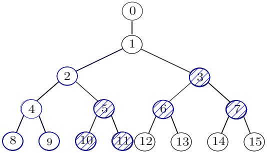


Figure : Security strategy u^1.
$\mathcal{N}_s(u^1) = \{3, 5, 6, 7, 10, 11\}$.

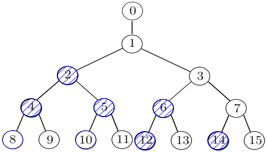


Figure : Security strategy u^2.
$\mathcal{N}_s(u^2) = \{2, 4, 5, 6, 12, 14\}$.

Concluding Remarks

- Tractable ways to do the computations using linearized models
- Guarantees on the structural properties of the solutions
- Results applicable to $[\widehat{\text{AD}}]$ and $[\widetilde{\text{AD}}]$ can be intra-polated.

Other applications

The LPF and ϵ-LPF model may be used for:

- Placement of voltage regulators
- Other loss functions such as loss of frequency regulation
- Placement of storage devices
- Optimal DER set-points in terms of active power curtailment
- Other systems with small second-order non-linearities, e.g., water distribution networks.

We first prove the following result that relates $\mathrm{x}(\psi, \phi)$, $\widehat{\mathrm{x}}(\psi, \phi)$, and $\check{\mathrm{x}}(\psi, \phi)$:

Proposition

For a fixed strategy profile $(\psi, \phi) \in \Psi \times \Phi$,

$$\widehat{S} \leqslant S \leqslant \check{S}, \quad \widehat{\nu} \geqslant \nu \geqslant \check{\nu}, \quad \widehat{\ell} \leqslant \ell \leqslant \check{\ell}.$$

Hence,

$$\left.\begin{array}{l} \mathrm{L_{VR}}(\widehat{\mathrm{x}}) \leqslant \mathrm{L_{VR}}(\mathrm{x}) \leqslant \mathrm{L_{VR}}(\check{\mathrm{x}}) \\ \mathrm{L_{LC}}(\widehat{\mathrm{x}}) = \mathrm{L_{LC}}(\mathrm{x}) = \mathrm{L_{LC}}(\check{\mathrm{x}}) \\ \mathrm{L_{LL}}(\widehat{\mathrm{x}}) \leqslant \mathrm{L_{LL}}(\widehat{\mathrm{x}}) \leqslant \mathrm{L_{LL}}(\check{\mathrm{x}}) \end{array}\right\} \implies \mathrm{L}(\widehat{\mathrm{x}}) \leqslant \mathrm{L}(\mathrm{x}) \leqslant \mathrm{L}(\check{\mathrm{x}}).$$

Lemma

For a fixed $(\psi, \phi) \in \Psi \times \Phi$,

$$\forall \quad (i,j) \in \mathcal{E}, \quad S_j \leqslant \frac{\widehat{S}_j}{(1-\epsilon_0)^{H-|\mathcal{P}_j|+1}}. \tag{3}$$

Proof.

We apply induction from leaf nodes to the root node.
Base case: For any leaf node $k \in \mathcal{N}_L$,

$$z_k \ell_k \overset{SL}{\leqslant} \epsilon_0 S_k \quad \overset{PC}{=} \epsilon_0 (s_k + z_k \ell_k)$$
$$\therefore z_k \ell_k \leqslant \tfrac{\epsilon_0 s_k}{1-\epsilon_0} \quad \overset{PC}{=} \tfrac{\epsilon_0 \widehat{S}_k}{1-\epsilon_0}.$$

□

Now, for any $j \in \mathcal{N} \backslash \mathcal{N}_L$,

$$z_j \ell_j \overset{SL}{\leqslant} \epsilon_0 S_j \overset{PC}{=} \epsilon_0 \Big[\sum_{k:(j,k)\in\mathcal{E}} S_k + s_j + z_j \ell_j \Big]$$
$$\therefore z_j \ell_j \leqslant \tfrac{\epsilon_0}{1-\epsilon_0} \Big[\sum_{k:(j,k)\in\mathcal{E}} S_k + s_j \Big].$$

Adding $\sum S_k + s_j$ on both the sides:

$$\underbrace{\sum_{k:(j,k)\in\mathcal{E}} S_k + s_j + z_j \ell_j}_{S_j} \leqslant \tfrac{1}{1-\epsilon_0} \Big[\sum_{k:(j,k)\in\mathcal{E}} S_k + s_j \Big].$$

Inductive step: By inductive hypothesis (IH) on $\mathcal{C}_j$,

$$S_j \overset{\text{(IH)}}{\leqslant} \tfrac{1}{(1-\epsilon_0)^{H-|P_k|+2}} \Big[\sum_{k:(j,k)\in\mathcal{E}} \widehat{S}_k + s_j \Big]$$
$$= \frac{\widehat{S}_j}{(1-\epsilon_0)^{H-|P_j|+1}} \quad (\because |\mathcal{P}_j| = |\mathcal{P}_k| - 1).$$

From Lemma 4, for any $(i,j) \in \mathcal{E}$,

$$S_j \leqslant \frac{\widehat{S}_j}{(1-\epsilon_0)^{H-|\mathcal{P}_j|+1}} \leqslant \frac{\widehat{S}_j}{(1-\epsilon_0)^{H}} = (1+\epsilon)\widehat{S}_j = \breve{S}_j. \tag{4}$$

For nodal voltages,

$$\begin{aligned} \nu_j &\overset{VE}{=} \nu_i - 2\mathbf{Re}(\bar{z}_j S_j) + |z|_j^2 \ell_j \\ &\geqslant \nu_i - 2\mathbf{Re}(\bar{z}_j S_j) \\ &\overset{(4)}{\geqslant} \nu_i - 2\mathbf{Re}(\bar{z}_j \breve{S}_j). \end{aligned} \tag{5}$$

Applying (5) recursively from the node j till root node:

$$\nu_j \geqslant \nu_0 - 2\sum_{k\in\mathcal{P}_j} \mathbf{Re}(\bar{z}_k \breve{S}_k) \overset{VE}{=} \breve{\nu}_j.$$

Thus, $\widehat{S}_j \leqslant S_j \leqslant \breve{S}_j$ and $\widehat{\nu}_j \geqslant \nu_j \geqslant \breve{\nu}_j$. Furthermore,

$$\begin{aligned} \widehat{S}_j \leqslant S_j \leqslant \breve{S}_j &\overset{NRP}{\Longrightarrow} |\widehat{S}_j|^2 \leqslant |S_j|^2 \leqslant |\breve{S}_j|^2 \\ &\Longrightarrow \frac{|\widehat{S}_j|^2}{\widehat{\nu}_j} \leqslant \frac{|S_j|^2}{\nu_j} \leqslant \frac{|\breve{S}|^2}{\breve{\nu}_j} \Longrightarrow \widehat{\ell} \leqslant \ell \leqslant \breve{\ell}. \end{aligned}$$

Proof of **Theorem**.

For any $\mathrm{x} \in \mathcal{X}$,

$$\mathrm{L}_{\mathrm{LL}}(\mathrm{x}) = \sum_{(i,j)\in\mathcal{E}} \frac{r_j(P_j^2+Q_j^2)}{\nu_i} \overset{HLBV,SI}{\leqslant} \frac{2}{\underline{\mu}} \sum_{(i,j)\in\mathcal{E}} r_j \overset{SI}{\leqslant} \frac{\underline{\mu}N}{2\underline{\mu}+4} \tag{6}$$

Hence,

$$\begin{aligned}
\check{\mathcal{L}} &= \check{\mathrm{L}}(\check{\mathrm{x}}(\check{\psi}^*, \check{\phi}^*(\check{\psi}^*))) \\
&\geqslant \check{\mathrm{L}}(\check{\mathrm{x}}(\psi^*, \check{\phi}^*(\psi^*))) && \text{(by optimality of } \check{\psi}^*\text{)} \\
&\geqslant \check{\mathrm{L}}(\mathrm{x}(\psi^*, \check{\phi}^*(\psi^*))) && \text{(by Proposition)} \\
&\overset{(6)}{\geqslant} \mathrm{L}(\mathrm{x}(\psi^*, \check{\phi}^*(\psi^*))) - \frac{\underline{\mu}N}{2\underline{\mu}+4} \\
&\geqslant \mathrm{L}(\mathrm{x}(\psi^*, \phi^*(\psi^*))) - \frac{\underline{\mu}N}{2\underline{\mu}+4} && \text{(by optimality of } \phi^*\text{)} \\
&= \mathcal{L} - \frac{\underline{\mu}N}{2\underline{\mu}+4}.
\end{aligned}$$

Similarly, one can show $\mathcal{L} \geqslant \widehat{\mathcal{L}}$. □

Concluding Remarks

- First (known) successful attempt to upper bound the power flows.
- Results are applicable for other type of questions like placement of voltage regulators or DERs, other loss functions including loss of frequency regulation, etc.
- The analysis can possibly be extended to other systems that have second-order non-linear losses as a bounded tiny fraction of the network flows, e.g., water networks.