Computing Intervals of Secure Power Injection

D. Georgiev * **E. Janeček** * **P. Voráč** *

* *New Technologies for the Information Society European Centre of Excellence, Faculty of Applied Sciences, University of West Bohemia in Pilsen, Univerzitni 8, Pilsen 30614, Czech Republic.*
`georgiev@kky.zcu.cz, janecek@kky.zcu.cz, vorac@ntis.zcu.cz`

Abstract: Existing tools used in many power system operations evaluate individual scenarios for power injection and network configuration but fail to consider nearby regions in the operating space. Such tools may lead to market transactions, preventive actions, or corrective actions that are nominally efficient but poor in general. Herein the foundations of an interval method are introduced. The presented results include an algorithm defined within a tractable optimisation framework that computes maximal power injection sets containing power injection profiles that are necessarily secure. The method is demonstrated on a simple 4 bus test system as well as on a medium sized IEEE 30 bus test system.

Keywords: Optimal operation and control of power systems, Constraint and security monitoring and control, Modeling and simulation of power systems.

1. INTRODUCTION

Present day transmission systems in the European Union are operated closer to their security limits. In part this mode of operation is a result of unforeseen power transfers caused by massive installations of renewable energy. In the global effort to curb carbon emissions, governments have proposed many ambitious renewable energy utilisation targets Zhou and Bialek (2007); Botterud et al. (2009); Zhou (2010) leading to installations of intermittent energy sources at geographical locations with promising energy potential but low energy demand. As a consequence, there is a greater need to evaluate risk associated with operations that may violate the network security limits.

TSOs ensure safe future operations by a priori reserving sufficient reserve energy to makeup for any forecasted imbalance between generation and demand. Current pricing mechanisms of ancillary services, however, are designed to purchase sufficient energy at the lowest price regardless of its origin Kirby (2007). Such transactions may lead to scenarios where reserved energy cannot be deployed before changing the system operational point through additional redispatch or reconfiguration.

Preventive and corrective redispatch and reconfiguration are yet another opportunity for potentially risky operations. In pursuit of most efficient system settings, various optimal power flow tools exist that propose changes in the system operating point either through reconfiguration or redispatch Platbrood et al. (2011); Hedman et al. (2009). Such tools often propose only the final settings and ignore the intermediate changes. In addition, such tools fail to incorporate security margins into the optimisation process yielding optimal but fragile states. In other words, the final state may satisfy security criteria but the operator has no idea by what margin.

In general, market and power flow optimisation tools are of the *what if* type. Optimal power flow tools used to clear intraday and spot electricity markets use simple models to price individual dispatch scenarios but fail to consider actual system safety, availability of regulation, and flexibility of corrective actions Ferrero et al. (1997); Litvinov et al. (2004). Price sensitivities may be computed using the approximate DC network model Bo and Li (2009) but the relevance to the security of the actual system is unclear. Security constrained optimal power flow tools used to propose reconfiguration and redispatch actions in order to increase system safety also compare individual scenarios but fail to consider nearby regions in the operating space Capitanescu et al. (2011). Stochastic load flow tools based on analytical probabilistic models or point estimate models can be used to investigate consequences of deviations from the proposed operating points Morales and Perez-Ruiz (2007); Janeček and Georgiev (2012). However, the complexity of these tools makes their integration into optimisation frameworks difficult.

Herein the foundations of a set based method are introduced. Given a general definition of network security, the method computes maximal interval sets of power injections that are necessarily secure. Intervals sets are chosen for computational and practical reasons. In real world applications, redispatch of different generators often lacks perfect coordination due to environmental conditions, ramp-up/down physical constraints, and generator de-bundling. Interval sets give information regarding operational margins for each network unit irrespective of other units' states.

⋆ This work was supported by the grant TA ČR TA01020865.

The method is formulated in terms of deviations from the nominal voltage, hence, even though the resulting sets are a conservative estimate, the suboptimality is negligible, as confirmed by Monte Carlo simulation performed on two test bus systems. The method algorithms are also based in a tractable optimisation framework suggesting its scalability and implementation robustness may be sufficient enough for market and operational deployment.

Set based tools do exist for evaluation of network transfer capabilities Greene et al. (2002). These tools, however, are not optimisation based. Instead, the boundaries of the operating region are approximated by their gradients. This can yield injections violating network security. Furthermore, combinatorial complexity typically associated with tracing boundaries suggests the methods are limited to modest sized problems. For approximate set-based tools formulated using linear network models see Liu (1986).

The remainder of the paper is organised as follows. The network model is given in Section 3. The method for computing the intervals of secure injection is then presented in Section 4. First, the general problem, which is too complex to solve but provides intuition regarding the end goals, is defined. Then, a simplified problem and its approximate solution algorithm are presented. Section 5 demonstrates and validates the results through two case studies. The paper concludes with Section 6.

2. NOMENCLATURE

$\mathcal{N}$: the set of nodes,
$\mathcal{L}$: set nodes with uncontrollable injections,
$\mathcal{G}$: set of nodes with controllable injections,
$\mathcal{B}$: set of branches,
Y: admittance matrix,
$X = (Re(V), Im(V)) = x_0 + \Delta$: nodal voltages,
$\mathcal{X}_S$: set of secure voltages,
$Z = (P, Q) = \bar{T}\left(\bar{Z} + W\right)$: power injections,
$\bar{T}$: rotational matrix,
$\bar{Z} = z_0 + A\Delta$: linear injections,
$\mathcal{Z}_S$: set of secure injections,
S: branch power flows.

3. NETWORK MODEL

3.1 Notation

Capital letters are used to denote matrices and vector variables. Lower case letters are reserved for constants and parameter vectors. Script letters are reserved for sets. Any vector $x \in \mathbb{R}^n$ can be written as $(x_1, \ldots, x_n)$, as $(x_k)_{k\in\{1,\ldots,n\}}$, or as $x_{\{1,\ldots,n\}}$. The set of real numbers is denoted by $\mathbb{R}$ and the set of complex numbers is denoted by $\mathbb{C}$. Real and imaginary parts of a complex vector y are given by $Re(y)$ and $Im(y)$, respectively. The letter i is reserved for the imaginary unit. Transpose and complex conjugates of a complex vector y are given by y^T and y^*, respectively. The absolute value of a complex number y is given by $|y|$ and the p-norm of a vector x is given by $||x||_p$. For a set $\mathcal{X}$, the volume of the set is given by $\mu(\mathcal{X}) = \int_{\mathcal{X}} dx$ and, for two sets $\mathcal{X}_1, \mathcal{X}_2 \subseteq \mathcal{X}$ and mappings $T_1, T_2 : \mathcal{X} \to \mathcal{Y}$, $T_1\mathcal{X}_1 + T_2\mathcal{X}_2 = \{y \in \mathcal{Y} | y = T_1x_1 + T_2x_2, x_1 \in \mathcal{X}_1, x_2 \in \mathcal{X}_2\}$. A closed interval, a cartesian product of 1-dimensional closed intervals from x_k^- to x_k^+, is denoted by $[x^-, x^+]$.

3.2 Network parameters

The network is described by a directed graph where each node harbours a potential load or a generator unit and each branch corresponds to a power line or a transformer. The set of nodes is given by the finite set $\mathcal{N} = 1, \ldots, n$ and the set of branches is defined by the set $\mathcal{B} \subset \mathcal{N} \times \mathcal{N}$. Node 1 is reserved for the slack bus, where the voltage is held constant and the injected power is adjusted to meet the network demand. The set of nodes with controllable injections (e.g. generators providing ancillary services) but excluding the slack is denoted by $\mathcal{G} \subset \mathcal{N}$ and has the cardinality g. The set of nodes with uncontrollable injections (e.g., standard loads or renewable energy sources) including the slack bus is denoted by $\mathcal{L} \subseteq \mathcal{N}$ and has the cardinality ℓ. The two sets $\mathcal{G}$ and $\mathcal{L}$ satisfy $\mathcal{L} \cap \mathcal{G} = \emptyset$ and $\mathcal{L} \cup \mathcal{G} = \mathcal{N}$. The network admittance matrix is denoted by $Y \in \mathbb{C}^{n\times n}$.

3.3 Network variables

It is assumed the network is operating under normal conditions under which the single phase model is applicable. Each node $k \in \mathcal{N}$ is associated with a voltage $V_k \in \mathbb{C}$ and an injected power $P_k + iQ_k$. It is often more convenient to list the real and imaginary parts of V separately in a real vector $X = (Re(V), Im(V))$ and the real and imaginary parts of the injected powers in a real vector $Z = (P, Q)$. Each branch $b \in \mathcal{B}$ is associated with a power flow $S_b \in \mathbb{C}$.

Distinction is made between free injections (those that are not controllable) and controllable injections. Uncontrollable injections at nodes in $\mathcal{L}$ are assumed to be contained in a known set

$$\mathcal{Z}_L = \left\{(P_{\mathcal{L}}, Q_{\mathcal{L}}) \,|\, (P_k, Q_k) \in T_k[z_k^-, z_k^+], k \in \mathcal{L}\right\},$$

where the bounds $z_k^-, z_k^+ \in \mathbb{R}^2$ as well as the orthonormal matrix $T_k \in \mathbb{R}^{2\times 2}$ are known. By the definition of the slack bus, $z_1^- = -\infty, z_1^+ = \infty$.

Definition 1. (Nominal Operating Point). The network has a nominal operating point x_0 representing the expected network state for the planning horizon. The realised state at the end of this horizon is defined in terms of deviations from this operating point, $X = x_0 + \Delta$. By the definition of the slack bus, $\Delta_1 = \Delta_n = 0$.

Definition 2. (Network Security Domain). Let the state of the network be described by $X = (Re(V), Im(V))$. The network security domain is the set $\mathcal{X}_S \subseteq \mathbb{R}^{2n}$ such that, for all $X \in \mathcal{X}$, the network satisfies the following physical constraints:

$$\begin{aligned} v_k^- \leq |V_k| \leq v_k^+, \forall k \in \mathcal{N}, \\ |S_b| \leq s_b^+, \forall b \in \mathcal{B}. \end{aligned} \tag{1}$$

The exact formulation of the network security domain is not important for the results of this paper. Hence, the above defined conditions can be easily expanded to account for other physical constrains or contingency scenarios, e.g., $N - 1$. Power injection limits are also omitted as they are part of the problem formulation.

4. OPTIMIZATION

Power injections, for all $k \in \mathcal{N}$, are computed from X by the formula Lavaei and Low (2012)

$$P_k = Z_k = X^T Y_k X, Q_k = Z_{k+n} = X^T Y_{k+n} X, \quad (2)$$

where the matrices Y_k are defined as

$$Y_k = \begin{pmatrix} e_k Re(y_k) & -e_k Im(y_k) \\ e_k Im(y_k) & e_k Re(y_k) \end{pmatrix}, \quad (3)$$

$$Y_{k+n} = \begin{pmatrix} -e_k Im(y_k) & -e_k Re(y_k) \\ e_k Re(y_k) & -e_k Im(y_k) \end{pmatrix}, \quad (4)$$

with $\{e_k\}_{k\in\mathcal{N}}$ being the set of standard basis vectors in $\mathbb{R}^n$ and y_k being the kth row of the admittance matrix Y. Note the matrices are not symmetric. This is intentional for reasons that will be made clear below.

4.1 General Problem

The problem addressed in the remainder of the paper is defined next.

Problem 3. (General ISI). Consider the network security domain $\mathcal{X}_S$ and the set of injections from the free buses $\mathcal{Z}_L$. Find a set of secure injections $\mathcal{Z}_G^*$ satisfying

$$\begin{aligned} &\mathcal{Z}_G^* = \max \mu(\mathcal{Z}_G), \text{ subject to} \\ &\quad \mathcal{Z} = \{(P,Q) \,|\, (P_\mathcal{G}, Q_\mathcal{G}) \in \mathcal{Z}_G, (P_\mathcal{L}, Q_\mathcal{L}) \in \mathcal{Z}_L\}, \\ &\quad \mathcal{Z}_G = \left\{(P_\mathcal{G}, Q_\mathcal{G}) \,|\, (P_k, Q_k) \in T_k[z_k^-, z_k^+], k \in \mathcal{G}\right\}, \\ &\quad \mathcal{Z} \subseteq \left\{Z | Z_k = X^T Y_k X, k \in \{1, ..., 2n\}, X \in \mathcal{X}_S\right\}. \quad (5) \end{aligned}$$

The matrices T_k are rotation matrices satisfying $T_k^T T_k = I$. The set $\mathcal{Z}_S = \{(P,Q) \,|\, (P_\mathcal{G}, Q_\mathcal{G}) \in \mathcal{Z}_G^*, (P_\mathcal{L}, Q_\mathcal{L}) \in \mathcal{Z}_L\}$ is referred to as the interval of secure injections.

The input to the general ISI problem is the network security domain $\mathcal{X}_S$ and the network topology given by the admittance matrix Y. The output is the set of secure injections $\mathcal{Z}_G$, the Cartesian product of intervals $[z_k^-, z_k^+] \subset \mathbb{R}^2$ in the range space of the orthonormal matrix T_k. Hence, $\mathcal{Z}_G$ is itself an interval in $\mathbb{R}^{2g}$. The choice of intervals for the set of secure injections has both computational and practical reasons. In real world applications, operation of different generators is often hard to coordinate. Generators may be renewable energy sources, whose power injections are influenced by environmental conditions. Generators may be ancillary service providers or sources re-dispatched in corrective actions, whose operation is limited by complex physical constraints dependent on internal hardware limitations. Coordination of such actions may be difficult in practice and unsafe in case of communication failures. Note, the intervals are not defined in the standard basis. Instead, they are defined in a rotated coordinate frame to capture potential power factor settings of different devices.

The above problem seeks to find the limits of injection in all directions and hence is more general than the well known AC OPF problem with a linear criterion, which seeks to maximise injections projected in a single direction. The AC OPF problem is known to be NP hard Lavaei and Low (2012) suggesting the general ISI problem is not easily solvable. A simpler version of the general problem is formulated below and is solved in Section 4.3.

4.2 Simplified Problem

The simplified problem (simply referred to as ISI) is defined next.

Problem 4. (ISI). Solve Problem 3 under the following assumptions:

- A1: $\mathcal{X}_S = \{X | X = x_0 + \Delta, D\Delta \leq d, d \in \mathbb{R}^m\}$: the network security domain is taken to be a bounded convex polytope, where $\Delta_{\{1,n\}} = 0$,
- A2: the transformation mappings $T_k, k \in \mathcal{G}$, are fixed,
- A3: $Z = \bar{T}(z_0 + A\Delta + W)$: the injections are expanded around the nominal point x_0 and separated into affine terms (referred to as the linear injections) and purely quadratic terms. The quadratic terms W are treated as a disturbance acting to violate Condition 5 in the definition of Problem 3.

A1 is a technical assumption. One may consider unions of polytopes to expand the domain. A2 is a conservative assumption supposing coordination of injections is absent. In practice, coordination is possible but often limited due to environmental conditions, physical constraints, and decentralised operation caused by de-bundled architectures. Power factor characteristics of generator units are described by the known rotation matrices T_k. In A3, the power vector is expanded around the nominal point so that $Z_k = x_0^T Y_k x_0 + x_0^T Y_k \Delta + x_0^T Y_k^T \Delta + \Delta^T Y_k \Delta$. The expression is then separated into affine and quadratic terms expressed in the rotated coordinate frame, where $\bar{T}_{\{k,k+n\},\{k,k+n\}} = T_k$. The quadratic term is then taken to be a disturbance reducing network security. In practice, $||\Delta||_\infty < 1$ in the per unit scale, implying the quadratic terms are likely to be small. One of the key problems resolved in this paper is finding tight bounds on Δ.

In the next section, an approximate solution of ISI is presented. The solution involves three basic steps, each solving one of the following two subproblems. The first subproblem considers a set of nodes $\mathcal{C} \subseteq \mathcal{N}$ and sets out to find limits on the injections Z with the disturbance W set to zero, i.e., limits on the linear injections $\bar{Z} = z_0 + A\Delta$.

Problem 5. ($\text{ISI}_1 : \mathcal{C}$). Consider a set $\mathcal{C} \subset \mathcal{N}$ and the network security domain $\mathcal{X}_S$ described by the pair (D, d). Suppose the parameters $\bar{z}_k^-$ and $\bar{z}_k^+$ are given for all $k \in \mathcal{N} \setminus \mathcal{C}$. Find the limits $\bar{z}_\mathcal{C}^{-,*}, \bar{z}_\mathcal{C}^{+,*}$ that solve the following optimisation problem:

$$\max_{\bar{z}_\mathcal{C}^-, \bar{z}_\mathcal{C}^+} \prod_{k\in\mathcal{C}} \mu([\bar{z}_k^-, \bar{z}_k^+]), \text{ subject to } \mathcal{D}_Z \subseteq \mathcal{D}_D,$$

$$\mathcal{D}_Z = \left\{\Delta | \bar{z}^- \leq z_0 + A\Delta \leq \bar{z}^+\right\} \quad (6)$$

$$\mathcal{D}_\Delta = \{\Delta | D\Delta \leq d\}, z^- \leq z_0 \leq z^+. \quad (7)$$

ISI_1 is not trivial if the injection intervals are generalised to polytopes. The problem is then equivalent to finding a maximal polytope embedded in another polytope. Solution to such a problem requires using an exponentially increasing number of constraints.

The second subproblem considers a set $\mathcal{D}$ of admissible Δ together with a set of nodes $\mathcal{C}$ and sets out to find limits on the quadratic terms W.

Problem 6. ($\text{ISI}_2 : \mathcal{C}, \mathcal{D}$). Consider a set $\mathcal{C} \subseteq \mathcal{N}$ and a convex bounded polytope $\mathcal{D}$. Find the limits $w_k^{-,*}$ and $w_k^{+,*}$ that solve the following optimisation problem:

$$\min \mu \left(\left[w^-_{\{k,k+n\}}, w^+_{\{k,k+n\}} \right] \right) \text{ subject to}$$
$$W_{\{k,k+n\}} \in \left[w^-_{\{k,k+n\}}, w^+_{\{k,k+n\}} \right], \forall \Delta \in \mathcal{D}.$$

The structure of the matrices Y_k is used in the next section to approximate the bounds. Finding the exact bounds requires maximising a nonconvex quadratic function over a polytope, an NP hard problem.

4.3 Solution

The ISI solution algorithm presented in this section is outlined in Figure 1. The individual steps as well as some facts useful for efficient solutions of ISI_1 and ISI_2 are described next.

Compute bounds on $\bar{Z}_{\{k,k+n\}}, k \in \mathcal{L}$ One of the inputs is the set of injections from the free buses $\mathcal{Z}_L$. This set constraints the possible values of Δ through Equation 2. These constraints, however, are not amenable to efficient optimisation methods. Hence, the first step is to map the bounds on the injections Z_k into bounds on the linear injections $\bar{Z}_k$ (see previous section for definition) without tightening the constraints on Δ. Note, there is no need to consider the slack bus since its injections are unlimited.

Any number of ways may be used to approximate the bounds on the linear injections. The following fact yields upper and lower bounds on the quadratic terms and hence can be used to over-approximate the set of linear injections produced by the free buses.

Fact 7. Consider a polytope $\mathcal{D}$, and, for any $k \in \mathcal{N}$ and $\ell \in \{k, k+n\}$, the set

$$\mathcal{D}_\ell = \left\{ \Delta | h^-_\ell \leq \bar{Y}_\ell \Delta \leq h^+_\ell \right\} \supseteq \mathcal{D},$$

where

$$\bar{Y}_k = (T_k)^{-1}_{1,1} Y_k + (T_k)^{-1}_{1,2} Y_{k+n},$$
$$\bar{Y}_{k+n} = (T_k)^{-1}_{2,1} Y_k + (T_k)^{-1}_{2,2} Y_{k+n}.$$

Then, $\forall \Delta \in \mathcal{D} \cap \mathcal{D}_\ell, W_\ell$ is bound by

$$W_\ell \geq \left(\Delta^-_{\{k,k+n\}} \right)^T h^+_\ell + \left(\Delta^+_{\{k,k+n\}} \right)^T h^-_\ell$$
$$W_\ell \leq \left(\Delta^-_{\{k,k+n\}} \right)^T h^-_\ell + \left(\Delta^+_{\{k,k+n\}} \right)^T h^+_\ell,$$

where

$$\Delta^-_{\{k,k+n\}} = \min \left(\Delta_{\{k,k+n\}}, 0 \right),$$
$$\Delta^+_{\{k,k+n\}} = \max \left(\Delta_{\{k,k+n\}}, 0 \right).$$

Computation of the smallest set $\mathcal{D}_k \supseteq \mathcal{D}$ is a linear program. It follows from Fact 7 that an approximate solution to ISI_2 is also a linear program. The computed bounds $w^{-,*}_k, w^{+*}_k$ may subsequently be transformed into bounds on the linear injections for all nodes $k \in \mathcal{L}$.

$$\left[\bar{z}^{-,*}_k, \bar{z}^{+,*}_k \right] = \left[z^-_k, z^+_k \right] + \left[w^-_{\{k,k+n\}}, w^+_{\{k,k+n\}} \right]. \quad (8)$$

Optimise bounds on linear injections for nodes $k \in \mathcal{G}$ The second step is to take known bounds on linear injections and maximise the bounds on the remaining linear injections. This is done by solving ISI_1 using the following fact.

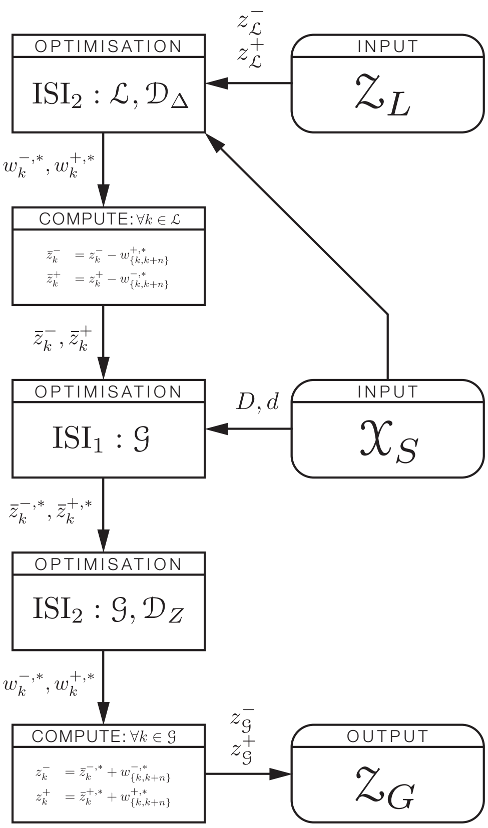

Fig. 1. ISI solution algorithm flowchart.

Fact 8. Define the submatrices

$$D_{-1} = D_{\mathcal{N},\mathcal{N}\backslash\{1\}}, A_{-1} = A_{\mathcal{N}\backslash\{1\},\mathcal{N}\backslash\{1\}}$$

and consider the two sets $\mathcal{D}_Z$ and $\mathcal{D}_D$ defined in Problem 4. The condition $\mathcal{D}_Z \subseteq \mathcal{D}_D$ holds if and only if

$$D^+ \left(\bar{z}^+ - z_0 \right) + D^- \left(\bar{z}^- - z_0 \right) \leq d, \quad (9)$$

where

$$D^+ = \max \left\{ 0, D_{-1} A^{-1}_{-1} \right\}, D^- = \min \left\{ 0, D_{-1} A^{-1}_{-1} \right\}.$$

Fact 8 expresses the polytope inclusion constraints in ISI_1 as linear constraints on the limits $\bar{z}^-$ and $\bar{z}^+$. Subsequently, if we take the logarithm of the utility function, ISI_1 is converted into a convex optimisation problem. Note, the inverse of A_{-1} exists if the nominal voltages are different from zero and the network is connected, which is always the case in real world systems.

Estimate bounds on quadratic injections for nodes $k \in \mathcal{G}$ The computed set $\mathcal{D}_Z$ is used in this step to bound the quadratic terms of the controllable nodes. The procedure is the same as in Step 1, with the input set being $\mathcal{D}_Z$ instead of the larger set $\mathcal{D}_\Delta$. Note, the bounds on all the quadratic terms could have been computed at the outset to yield a greater overapproximation. Similarly, the bounds on the quadratic terms of the free buses could be recomputed to yield a lesser overapproximation.

Contract bounds on injections for nodes $k \in \mathcal{G}$ The algorithm terminates once the appropriate bounds on linear injections of controllable nodes are found. The final step is to contract the injection sets of the controllable nodes to obtain conservative bounds on the actual injections.

$$\left[z^-_k, z^+_k \right] = \left[\bar{z}^{-,*}_k + w^+_{\{k,k+n\}}, \bar{z}^{+,*}_k + w^-_{\{k,k+n\}} \right]. \quad (10)$$

The final bounds $z_{\mathcal{G}}^-$ and $z_{\mathcal{G}}^+$ approximate the solution to ISI while ensuring that any injection $Z_{\{k,k+n\}} \in T_k[z_k^-, z_k^+], k \in \mathcal{G}$, does not produce an unsafe network state, as long as the injections at the other nodes (free nodes and controllable nodes) are also within their prescribed bounds.

Theorem 9. Consider the set

$$\mathcal{Z}_S = \left\{ (P,Q) \,|\, (P_k, Q_k) \in T_k[z_k^-, z_k^+], k \in \mathcal{N} \right\},$$

where z_k^-, z_k^+ are given for $k \in \mathcal{L}$ and computed by following Steps 1- 4 for $k \in \mathcal{G}$. Then, for any $Z \in \mathcal{Z}_S$, the resulting voltage lies in the network security domain $\mathcal{X}_S$ defined in Problem 4.

Proof. Define the following sets:

$$\mathcal{X}_{L1} = \{X |\, (P_{\mathcal{L}}, Q_{\mathcal{L}}) \in \mathcal{Z}_L\},$$
$$\mathcal{X}_{L2} = \left\{X | \bar{Z}_{\{k,k+n\}} \in \left[\bar{z}_k^{-,*}, \bar{z}_k^{+,*}\right], k \in \mathcal{L}\right\},$$
$$\mathcal{X}_{G1} = \left\{X | \bar{Z}_{\{k,k+n\}} \in \left[\bar{z}_k^{-,*}, \bar{z}_k^{+,*}\right], k \in \mathcal{G}\right\},$$
$$\mathcal{X}_{G2} = \{X |\, (P_{\mathcal{G}}, Q_{\mathcal{G}}) \in \mathcal{Z}_G\}.$$

To prove the theorem, it must be shown that $\mathcal{X}_{L1} \cap \mathcal{X}_{G2} \subseteq \mathcal{X}_S$. It follows from Fact 7 and ISI$_2$, that $\mathcal{X}_{L2} \supseteq \mathcal{X}_{L1}$ and that $\mathcal{X}_{L2} \cap \mathcal{X}_{G1} \supseteq \mathcal{X}_{L2} \cap \mathcal{X}_{G2}$. Hence, $\mathcal{X}_{L2} \cap \mathcal{X}_{G1} \supseteq \mathcal{X}_{L1} \cap \mathcal{X}_{G2}$. The theorem follows from Fact 8 and ISI$_1$ since $\mathcal{X}_{L2} \cap \mathcal{X}_{G1} \subseteq \mathcal{X}_S$.

5. CASE STUDY

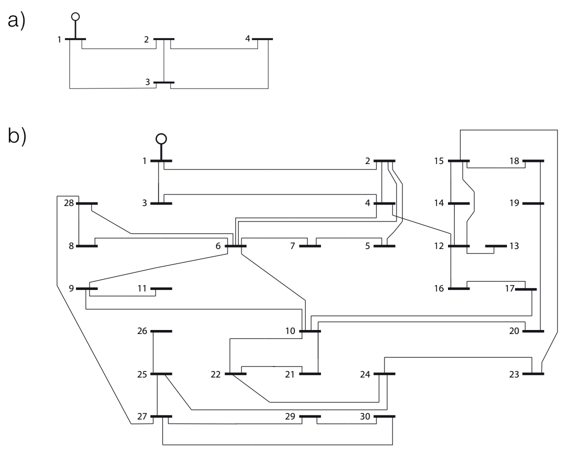

Fig. 2. Test system topologies. The slack bus is always located at node 1 and all other nodes are taken to be controllable. a) The truncated IEEE 14 bus test system containing only nodes 1,2,4, and 5 with their respective branches. b) The IEEE 30 bus test system.

The purpose of the case study is to show possible applications of the ISI method on two widely used IEEE test systems 30 Bus Power Flow Test Case. For easy visualisation, the first test system is the IEEE 14 bus test system truncated to 4 nodes. The IEEE 30 bus test system is used to demonstrate the applicability and computation tractability for a medium sized power system. Figure 2 illustrates the topologies. The slack bus is always located at node 1 and all other nodes are taken to be controllable, e.g., providers of ancillary services supplying both positive or negative injections to meet system demands (i.e., $\mathcal{L} = 1$ and $\mathcal{G} = \{2, ...n\}$). While, allowing all nodes to be controllable is an exaggeration, it provides a comprehensive study giving properties of all nodes in the system.

The test systems are considered in the p.u. scale with the base of 100 MVA. Power injections, impedances, line flow constraints, and topologies are taken from 30 Bus Power Flow Test Case; Kodsi and Canizares (2003). The case study is divided into two parts. First the intervals of secure injection for the 4 node the 30 node systems are computed and plotted. Second the results are verified by Monte Carlo simulation. All optimisation was performed in Matlab using the tool CVX CVX Research (2012).

5.1 *Network Security Domain*

The network security domain given in Definition 2 is, for the purposes of this case study, simply approximated from the test system line flow constraints f^+ and voltage constraints x^-, x^+. For the sake of simplicity, the standard DC approximation is used to model line flow constraints. Line flows, rewritten using the DC approximation for some branch $b = (k, \ell) \in \mathcal{B}$, is written as $|Im\,(Y_{k,\ell})\,(\theta_k - \theta_\ell)| \leq f_b^+$, where θ_k and θ_ℓ are the voltage phase angles at nodes $k, \ell \in \mathcal{N}$. For small phase angles differences

$$\theta_k - \theta_\ell \approx R\left(X_{\{k,k+n\}} - X_{\{\ell,\ell+n\}}\right),$$
$$R_{k,\ell} = ||\bar{x}||_2 \begin{pmatrix} \bar{x}_1 & -\bar{x}_2 \\ \bar{x}_2 & \bar{x}_1 \end{pmatrix}^{-1}, \bar{x} = X_{\{k,k+n\}}.$$

The voltage constraints are approximated by an interval $\pm 5\%$ of the nominal state x_0 computed from the published power injections using the deterministic Gauss-Seidel load flow method Kirtley (2003). In other words, $x_{\{k,k+n\}}^- = -0.05\left|x_{0,\{k,k+n\}}\right|$ and $x_{\{k,k+n\}}^+ = 0.05\left|x_{0,\{k,k+n\}}\right|, \forall k \in \mathcal{N} \setminus \{1\}$. These approximations of the voltage and flow constraints are in no way maximised as this is not the objective of this paper.

Hence, the network security domain $\mathcal{X}_S$ is taken to be all vectors X satisfying $X \in [x^-, x^+]$ and

$$\left|Im\,(Y_{k,\ell})\,R\left(X_{\{k,k+n\}} - X_{\{\ell,\ell+n\}}\right)\right| \leq f_{(k,\ell)}^+, (k,\ell) \in \mathcal{B}.$$

5.2 *Secure injection sets and weighed distance maps*

The computed intervals of secure injection for the 4 and 30 node systems are shown in Figures 3 and 4. The injection sets are filled with weighed distance maps, generated through Monte Carlo simulation, that illustrate the relative security of the given injection pair for all simulated values. The distances are normalised so that the maximum distance is equal to 1.

For example, take an injection (P_2, Q_2) in the plotted interval $T_k\left[z_2^-, z_2^+\right]$ with a weighed distance of 0.05. Then there exist injections (P_k, Q_k), in the plotted intervals $T_k\left[z_k^-, z_k^+\right], k = 3, 4$, such that (P, Q) the corresponding to a voltage $X \in \mathcal{X}_S$ and is spaced 5% of the cross-width from the border of $\mathcal{X}_S$. Therefore, the uniformly shaded intervals suggest the corresponding injections are not main determinants of security. Whereas, intervals with large gradients suggest there are settings for that node that yield a generally more secure network regardless of the other injections. Note that all three intervals contain points within five percentage points away from the border. In the next section, the mapped voltages corresponding to the secure sample injections of the Monte Carlo simulation are plotted with respect to the network security domain to provide a more visual verification of the algorithm.

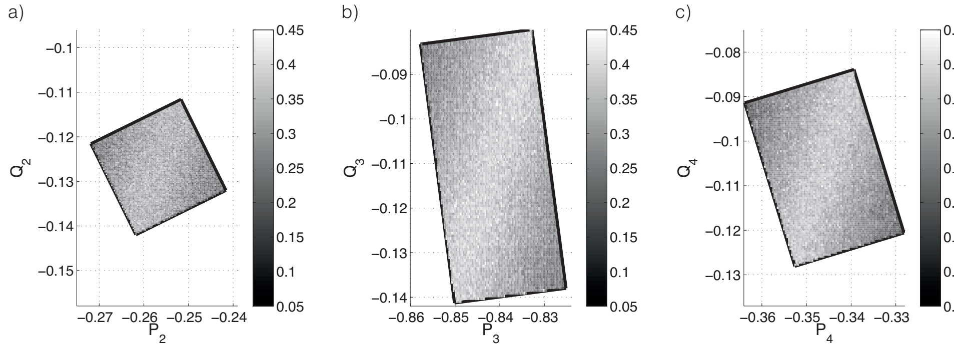

Fig. 3. Computed intervals of secure injection for the controllable nodes of the IEEE 4 bus test system overlaid with the corresponding weighed distance map, where the colours indicate the minimum distance from the boundary of the network security domain $\mathcal{X}_S$ computed by Monte Carlo simulation. The distances vary between 0.05 and 0.45 (i.e., approximately 5% and 45% of the network security domain cross-width). Lighter bands running down the middle illustrate areas of increased security. Axis of all plots have equal scales indicating node 3 is clearly most robust to injection variation.

To verify the applicability to larger power systems, ISI was implemented for the IEEE 30 bus test system. Figure 4 shows the computed intervals of secure injection filled with the weighed distance maps. The computation time for the 30 node system scaled approximately linearly when compared to the 4 node system (computer time of 24.8sec for the 4 node system and 224.4sec for the 30 node system on a desktop PC with an AMD Athlon(tm) 64 X2 Dual Core Processor 4400+ 2.3 GHz 4GB of Ram).

5.3 Network security domain verification

The ISI solution algorithm was verified through Monte Carlo simulation using 100 thousand and 10 thousand points for the 4 and 30 node systems, respectively. Samples are taken from the computed intervals of secure injection and mapped to voltages using the deterministic Gauss-Seidel load flow method. Membership of the resulting vectors X in the network security domain $\mathcal{X}_S$ was then tested by computing the normalised minimum distance to the border. For a voltage vector X, the distance was computed by $\min\{d - D(X - x_0)\}$, where each constraint defined by the pair (d, D) is normalised so that the maximum distance of interior points is equal to 1.

Figure 5 displays the results in the voltage vector space. For the 4 node system, the security domain is approximately a Cartesian product of sets containing $Re(V)$ and $Im(V)$. Hence, by leaving out the slack bus, the location of the mapped voltages within $\mathcal{X}_S$ can be shown in two separate three-dimensional plots. Furthermore, for the 4 node system, $Re(V)$ and $Im(V)$ are also approximately proportional to the voltage magnitude and phase, respectively. Figure 5, therefore, shows injection variation has little effect on the voltage magnitudes but great effect on voltage phase.

6. CONCLUSION

A framework and a sufficient solution algorithm for computing intervals of secure injection was presented. Given a nominal operating point, the method parametrises sets

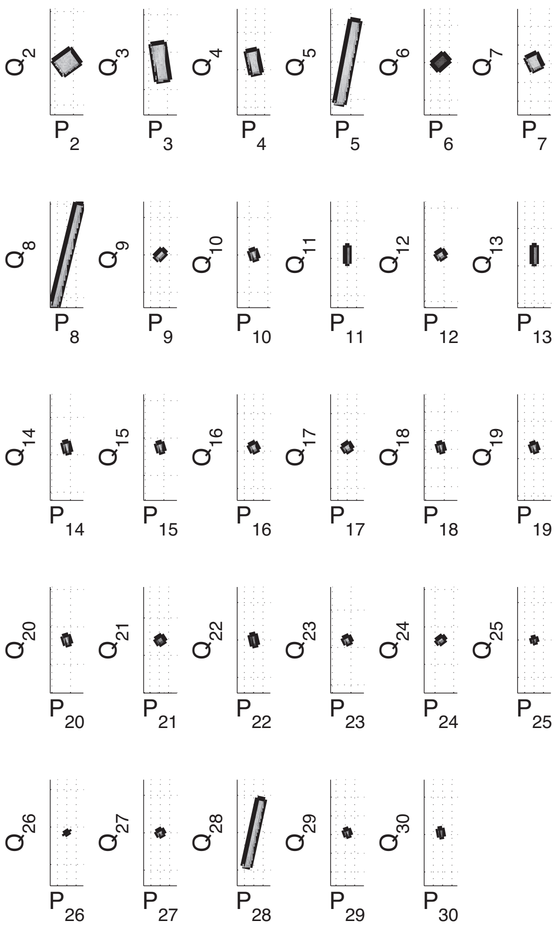

Fig. 4. Computed intervals of secure injection for the IEEE 30 bus test system. All axis have equal scale. Results indicate network security robustness, e.g., nodes 5,6, and 28 are major hubs where large injection variations are possible. Nodes 9-27 and nodes 29, 30 are located on the medium voltage portion of the network. Monte Carlo simulation was used to validate all regions. The normalised distances ranged from 0.02 to 0.5 (i.e., approximately 2% to 50% of the network security domain cross-width).

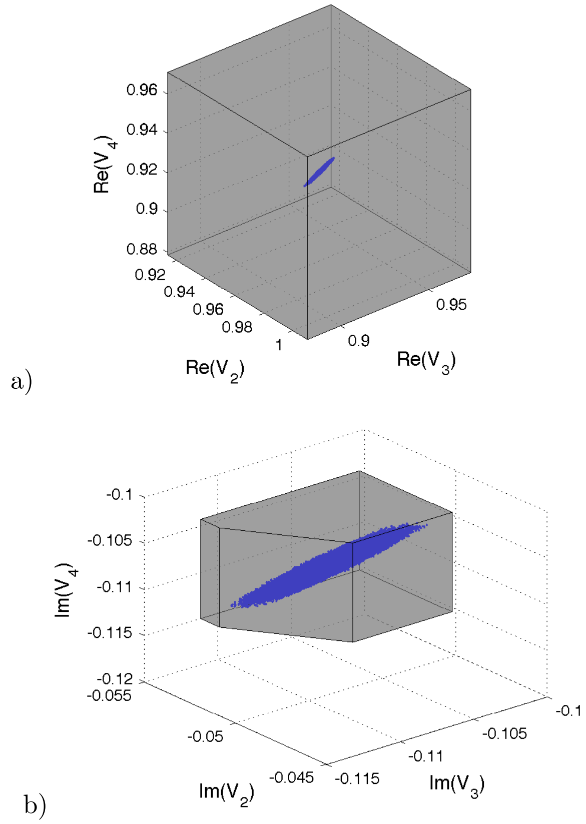

Fig. 5. Monte Carlo verification of the ISI algorithm for the 4 node system. The plotted points indicate samples from the intervals of secure injections mapped to voltages. All points lie in $\mathcal{X}_S$. a) The network security domain projected onto the real parts of nodal voltages. b) The network security domain projected onto the imaginary parts of nodal voltages.

of injections that necessarily comply with general network security criteria for AC systems. Monte Carlo simulation was subsequently used to validate the algorithm on two IEEE test systems. The injection sets were shown to be close to maximal and the algorithm was shown to scale linearly with the number of nodes. The method has the potential to be foundational for a new set of market and operational tools mindful of security margins and operational flexibility.

REFERENCES

30 Bus Power Flow Test Case (1993). Power systems test case archive.

Bo, R. and Li, F. (2009). Probabilistic LMP forecasting considering load uncertainty. *IEEE Trans. on Power Systems*, 24.

Botterud, A., Wang, J., Moteiro, C., and Miranda, V. (2009). Wind power forecasting and electricity market operations. In *Proc. of the IAEE Int. Conf.*

Capitanescu, F., Ramos, J.L.M., Panciatici, P., Kirschen, D., Marcolini, A.M., Platbrood, L., and Wehenkel, L. (2011). State-of-the-art, challenges, and future trends in security constrained optimal power flow. *Electrical Power System Research.*

CVX Research, I. (2012). CVX: Matlab software for disciplined convex programming, version 2.0. `http://cvxr.com/cvx`.

Ferrero, R.W., Shahidehpour, S.M., and Ramesh, V.C. (1997). Transaction analysis in deregulated power systems using game theory. *IEEE Trans. on Power Systems*, 12(3).

Greene, S., Dobson, I., and Alvarado, F.L. (2002). Sensitivity of transfer capability margins with a fast formula. *IEEE Trans. on Power Systems.*

Hedman, K.W., O'Neill, R.P., Fisher, E.B., and Oren, S.S. (2009). Optimal transmission switching with contingency analysis. *IEEE Trans. on Power Systems.*

Janeček, E. and Georgiev, D. (2012). Probabilistic extension of the backward/forward load flow analysis method. *IEEE Trans. on Power Systems.*

Kirby, B. (2007). Ancillary services: Technical and commercial insights. Technical report, Wartsila.

Kirtley, Jr., J.L. (2003). Introduction to load flow - introduction to power system, class notes chapter 5. Technical report, Massachusetts Institute of Technology, `http://ocw.mit.edu/courses/electrical-engineering-and-computer-science`.

Kodsi, S.K.M. and Canizares, C.A. (2003). Modeling and simulation of IEEE 14 bus system with facts controllers. Technical report, University of Waterloo.

Lavaei, J. and Low, S.H. (2012). Zero duality gap in optimal power flow problem. *IEEE Trans. on Power Systems.*

Litvinov, E., Zheng, T., Rosenwald, G., and Shamsollahi, P. (2004). Marginal loss modeling in LMP calculation. *IEEE Trans. on Power Systems*, 19(2).

Liu, C.C. (1986). A new method for the construction of maximal steady-state security regions of power systems. *IEEE Trans. on Power Systems.*

Morales, J.M. and Perez-Ruiz, J. (2007). Point estimate schemes to solve the probabilistic power flow. *IEEE Trans. on Power Systems.*, 22(4).

Platbrood, L., Crisciu, H., Capitanescu, F., and Wehenkel, L. (2011). Solving very large-scale security-constrained optimal power flow problems by combining iterative contingency selection and network compression. In *Power system computation conference.*

Zhou, J. (2010). *20% Wind Generation and the Energy Markets: A Model and Simulation of the Effect of Wind on the Optimal Energy Portfolio.* Master's thesis, Princeton University, Dep. of Operations Research and Financial Engineering.

Zhou, Q. and Bialek, J. (2007). Generation curtailment to manage voltage constraints in distribution networks. *IET Generation, Transmission & Distribution*, 1.