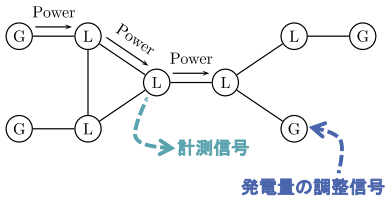
電力ネットワークシステムにおける分散的サイバー攻撃検知

橋本英明 (NTT環境エネルギー研究所)
早川朋久 (東京工業大学)

背景

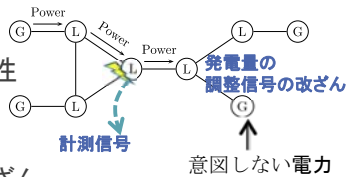
- 電力網
  - 発電機 (G) と負荷 (L) が複雑な接続関係を持つ，大規模なネットワークシステム

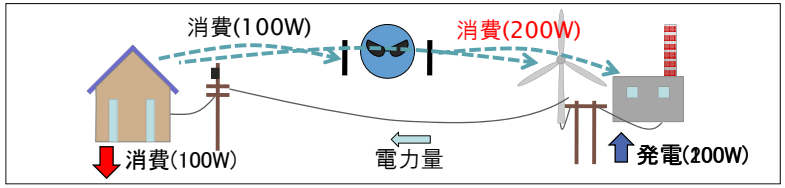


- 電力網の高度化 ➡ スマートグリッド
  - IT技術を利用して情報の共有や通信が行われる
    - 消費電力などの計測情報
    - 発電機に対する，発電量の調整信号

電力網高度化に伴う新たな課題

- 共有された情報の改ざんや悪用の可能性
  - 消費電力などの計測情報の悪用
    公称値と異なる電力消費 [1]
  - 発電機に対する，発電量の調整信号の改ざん
    発電機が余分な電力を発電・電力網に流入 [2]





- IT技術を用いた電力網への悪意のある攻撃が物理現象に影響

サイバー攻撃 → 意図しない電力消費，電力流入

- サイバー攻撃を分散的に検知

[1] Pasdar and Mirzakuchaki, “A solution to remote detection of illegal electricity usage based on smart metering,” 2007.
[2] Esfahani *et al.* “A robust policy for automatic generation control cyber attack in two area power network,” 2010.

電力ネットワークシステム

ノード→ 発電機/負荷

- 動揺方程式：
  ノード i の複素電圧の位相 δ_i の時間変化

ノード i での発電電力

ノード i から
ノード j に流れる電力

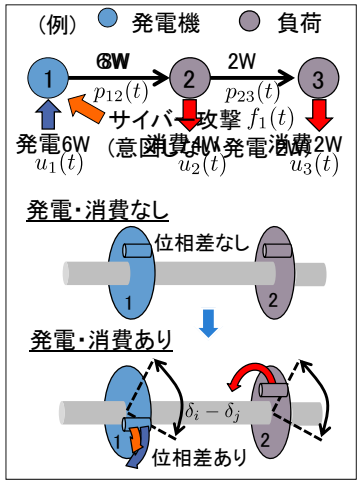
$$m_i\ddot{\delta}_i(t) + d_i\dot{\delta}_i(t) - u_i(t) = -\sum_{j\in\mathcal{N}_i} p_{ij}(t) + f_i(t)$$

ノード i の減衰定数

ノード i の質量定数

ノード i に対するサイバー攻撃
$f_i(t) = 0$ → サイバー攻撃なし
$f_i(t) \neq 0$ → サイバー攻撃あり

- ノード i からノード j に流れる電力
  $p_{ij}(t) = w_{ij}(\delta_i(t) - \delta_j(t))$
- ノード i での計測量 $y_i(t)$
  ノード i に接続しているノードに流れる電力
  $y_i(t) = [p_{ii_1}, \ldots, p_{ii_{n_i}}]^{\mathrm{T}}$ ➡ 位相差がわかる



w_{ij} : ノードi, j間のサセプタンス
とノードi, jの電圧の積

$\mathcal{N}_i$: ノード i に接続している
ノードの集合
$\{i_1, \ldots, i_{n_i}\}$

電力ネットワークシステム全体

- ネットワークを表すグラフ(ノードの数 N)
  - 重み付きグラフラプラシアン L
- 電力ネットワーク全体のダイナミクス

$$\dot{x}(t) = (A + (L \otimes D))x(t) + Bu(t) + Bf(t)$$
$$y(t) = Cx(t)$$

- ノード i の状態　$x_i \triangleq [\delta_i, \dot{\delta}_i]^{\mathrm{T}} \in \mathbb{R}^2$
- 状態　$x \triangleq [x_1^{\mathrm{T}}, \ldots, x_N^{\mathrm{T}}] \in \mathbb{R}^{2N}$
- 入力　$y \triangleq [y_1^{\mathrm{T}}, \ldots, y_N^{\mathrm{T}}]^{\mathrm{T}} \in \mathbb{R}^{\sum_{i=1}^{N} n_i}$
- サイバー攻撃　$f \triangleq [f_1, \ldots, f_N]^{\mathrm{T}} \in \mathbb{R}^N$
- 発電電力　$u \triangleq [u_1, \ldots, u_N]^{\mathrm{T}} \in \mathbb{R}^N$

$$m_i\ddot{\delta}_i(t) + d_i\dot{\delta}_i(t) = -\sum_{j\in\mathcal{N}_i} p_{ij}(t) + u_i(t) + f_i(t)$$

$$L_{(i,j)} \triangleq \begin{cases} -\sum_{j\in\mathcal{N}_i} \frac{w_{ij}}{m_i}, & i = j, \\ \frac{w_{ij}}{m_i}, & j \in \mathcal{N}_i, \\ 0, & \text{otherwise} \end{cases}$$

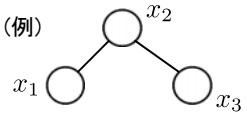
$$A_i \triangleq \begin{bmatrix} 0 & 1 \\ 0 & -\frac{d_i}{m_i} \end{bmatrix}, \quad B_i \triangleq \begin{bmatrix} 0 \\ \frac{1}{m_i} \end{bmatrix}$$

$$A \triangleq \begin{bmatrix} A_1 & & \\ & \ddots & \\ & & A_N \end{bmatrix} \in \mathbb{R}^{2N\times 2N}$$

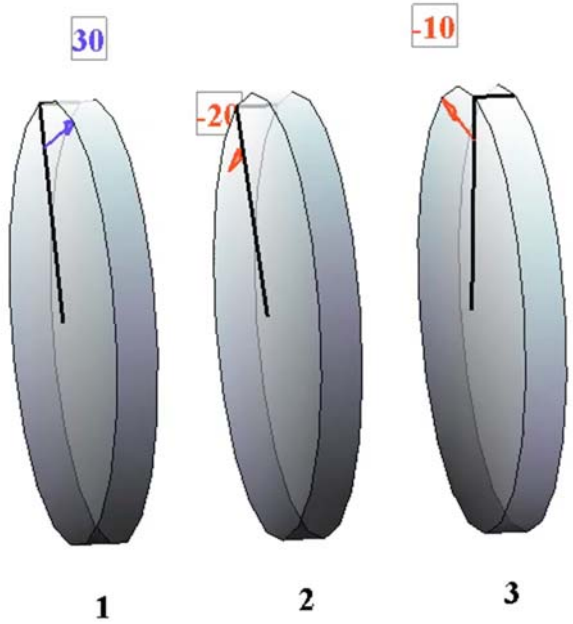
$$B \triangleq \begin{bmatrix} B_1 & & \\ & \ddots & \\ & & B_N \end{bmatrix} \in \mathbb{R}^{2N\times N}$$

$$D \triangleq \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad C \triangleq [\bar{C}_1^{\mathrm{T}}, \ldots, \bar{C}_N^{\mathrm{T}}]^{\mathrm{T}}$$

(例)



$$\dot{x}(t) = \begin{bmatrix} A+D & -D & 0 \\ -D & A+2D & -D \\ 0 & -D & A+2D \end{bmatrix} x(t) + \begin{bmatrix} B & 0 & 0 \\ 0 & B & 0 \\ 0 & 0 & B \end{bmatrix} u(t)$$



ネットワークシステムにおける故障検知

サイバー攻撃 → 広義の故障

- 集中的な動的システムに対する故障検知
  - 故障検知ができるための必要十分条件 [3]
- ネットワークシステムに対する分散的故障検知

	先行研究[4]	本研究	先行研究[5]
ネットワークシステム	非均一(電力ネットワークシステム)	非均一(電力ネットワークシステム)	均一
相互作用項	あり	あり	なし
情報	位相の絶対値	位相差(電力量)	同左
	全体の使用電力	局所的な使用電力	同左

[3] Massoumnia, "A geometric approach to the synthesis of failure detection filters," 1986.
[4] Teixeira *et al.*, "Networked Control Systems under Cyber Attacks with Applications to Power Networks," 2010.
[5] Meskin *et al.*, "Actuator fault detection and isolation for a network of unmanned vehicles," 2009.

本研究の目的

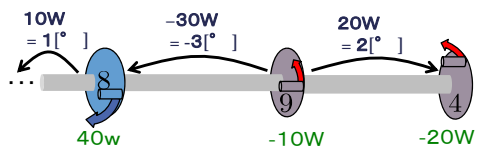
$$m_i\ddot{\delta}_i(t) + d_i\dot{\delta}_i(t) - u_i(t) = -\sum_{j\in\mathcal{N}_i} p_{ij}(t) + f_i(t)$$
$$p_{ij}(t) = w_{ij}(\delta_i(t) - \delta_j(t))$$

- 各ノード i において分散的に
  - ノード iとその近傍の計測量
  - ノード iとその近傍の発電電力

$$\bar{y}_i \triangleq [y_i^{\mathrm{T}}, y_{i_1}^{\mathrm{T}}, \ldots, y_{i_{n_i}}^{\mathrm{T}}]^{\mathrm{T}}$$
$$\bar{u}_i \triangleq [u_i, u_{i_1}, \ldots, u_{i_{n_i}}]^{\mathrm{T}}$$

を用いて，サイバー攻撃の検知を行う

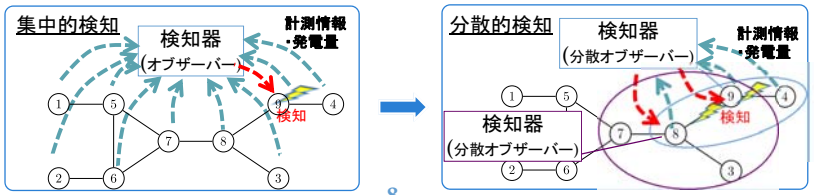
(例: ノード $i = 9$分散的サイバー攻撃検知を行うとき使用する情報)



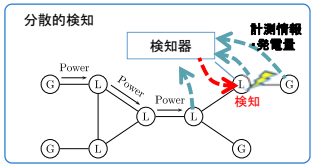
← 計測量 $y_9 = [p_{98}, p_{94}]^{\mathrm{T}}$

$\bar{y}_9 = [y_9^{\mathrm{T}}, y_8^{\mathrm{T}}, y_4^{\mathrm{T}}]^{\mathrm{T}}$

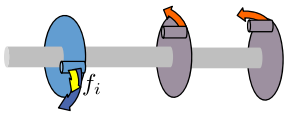
←発電電力 $\bar{u}_9 = [u_9, u_8, u_4]^{\mathrm{T}}$



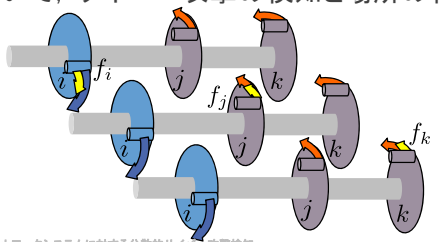
本研究の目的



- サイバー攻撃 f_i ＝ 意図しない
  電力消費・電力流入



- ノード i において分散的に
  ・接続しているノードに流れる電力　$\bar{y}_i \triangleq [y_i^{\mathrm{T}}, y_{i_1}^{\mathrm{T}}, \ldots, y_{i_{n_i}}^{\mathrm{T}}]^{\mathrm{T}}$ ← 観測
  ・自分と接続しているノードの発電電力　$\bar{u}_i \triangleq [u_i, u_{i_1}, \ldots, u_{i_{n_i}}]$ ← 入力
  を用いて，サイバー攻撃の検知と場所の特定を行う



自分のところで故障

隣で故障

自分と隣では
故障は起こっていない

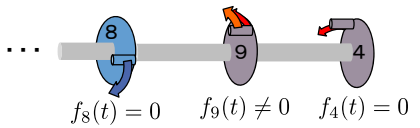
サイバー攻撃の検知手法

- 分散オブザーバーを設計し，実システムと比較
  - 一致 → サイバー攻撃なし，　異なる → サイバー攻撃発生

計測量が相対値のみ → 絶対量を推定するオブザーバーは設計できない

→ 相対量を推定する分散オブザーバーを設計
$f_j(t) - f_k(t) \neq 0$を検知する

ノード9に対するサイバー攻撃が発生



$f_9(t) - f_8(t) \neq 0$
$f_9(t) - f_4(t) \neq 0$
$f_8(t) - f_4(t) = 0$

オブザーバーにより $f_j(t) - f_k(t) \neq 0$ を検出

$f_9(t) - f_8(t) \neq 0$　ノード8, 9のどちらかに攻撃
$f_9(t) - f_4(t) \neq 0$　ノード9, 4のどちらかに攻撃
$f_8(t) - f_4(t) = 0$　ノード8, 4には攻撃が起こっていない

($f_9(t) \equiv f_4(t)$ を除く)
→ ノード9に攻撃が発生

問題

$\bar{y}_i \triangleq [y_i^{\mathrm{T}}, y_{i_1}^{\mathrm{T}}, \ldots, y_{i_{n_i}}^{\mathrm{T}}]^{\mathrm{T}}$　$\bar{u}_i \triangleq [u_i, u_{i_1}, \ldots, u_{i_{n_i}}]^{\mathrm{T}}$

ノード iと接続しているノードの出力 $\bar{y}_i$と入力 $\bar{u}_i$を用いて
オブザーバー変数 $w_{jk}(t)$ と誤差変数 $r_{jk}(t)$ を以下のように定義するとき，

$$\dot{w}_{jk}(t) = F_{jk} w_{jk}(t) - E_{jk} \bar{y}_i(t) + G_{jk} \bar{u}_i(t)$$
$$r_{jk}(t) = M_{jk} w_{jk}(t) - H_{jk} \bar{y}_i(t) + K_{jk} \bar{u}_i(t)$$
$$j = i, i_1, \ldots, i_{n_i}, \quad k = i, i_1, \ldots, i_{n_i}, \quad j > k$$

サイバー攻撃の差が $f_j(t) - f_k(t) \neq 0$ であるときのみ，$r_{jk}(t) \neq 0$
となるような設計パラメータ $F_{jk}, E_{jk}, G_{jk}, M_{jk}, H_{jk}, K_{jk}$を探す問題
→ ノードi における $\bar{y}_i, \bar{u}_i$を用いた分散的サイバー攻撃検知問題

定理

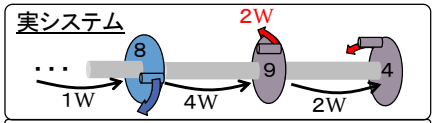
$$\dot{x}(t) = (A + (L \otimes D))x(t) + Bu(t) + Bf(t) \quad (1)$$

電力ネットワークシステム(1)に対する，
ノードiにおける $\bar{y}_i, \bar{u}_i$ を用いた分散的サイバー攻撃検知問題は可解である

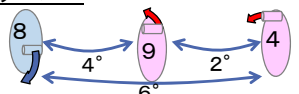
偏差システムを $x(t) - w_{jk}(t)$, その出力を $r_{jk}(t)$としたとき，
・サイバー攻撃 $f_{\alpha\beta}$, $\alpha \neq j$, $\beta \neq k$ の入力ベクトル値空間が
　不可観測部分空間に含まれる
・サイバー攻撃 f_{jk}の入力ベクトルの値空間がを可観測部分空間に含まれる
ようなパラメータ $F_{jk}, E_{jk}, G_{jk}, M_{jk}, H_{jk}, K_{jk}$ が存在すれば可解
→不可観測性部分空間の概念を利用すると，存在性を確認できる

提案手法のイメージ　ノード9で分散的にサイバー攻撃を検知

実システム

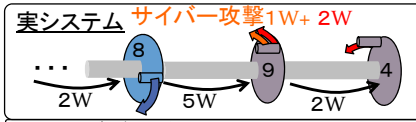


分散オブザーバー

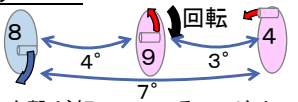


サイバー攻撃が起こっていないときは
位相の推定が正確にできる

実システム　サイバー攻撃1W+ 2W



分散オブザーバー



サイバー攻撃が起こっているノードは
位相を推定が正確にできない

位相差の誤差から攻撃を検知

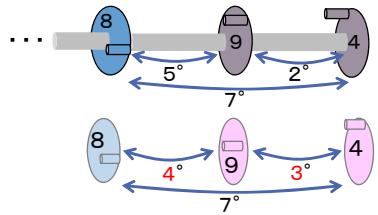
r_{jk}: 実システムと分散オブザーバーの
ノード j, k位相差の誤差を表す変数

$r_{98}(t) = 5^\circ - 4^\circ \neq 0$ → ノード8, 9の
どちらかに攻撃

$r_{94}(t) = 2^\circ - 3^\circ \neq 0$ → ノード9, 4の
どちらかに攻撃

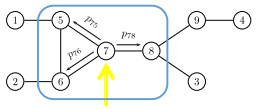
$r_{84}(t) = 7^\circ - 7^\circ = 0$ → ノード8, 4には攻撃
が起こっていない

実システムと分散オブザーバーの比較

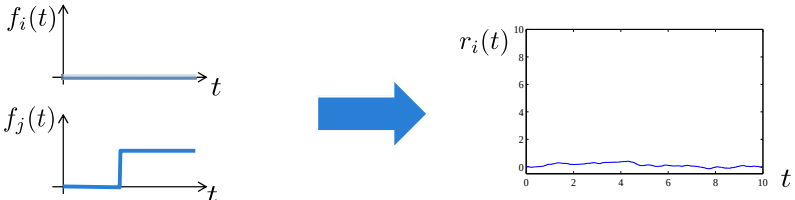


位相は直接測定できないので，
位相差を比べる

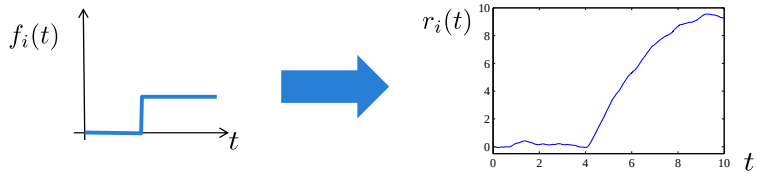
提案手法のイメージ



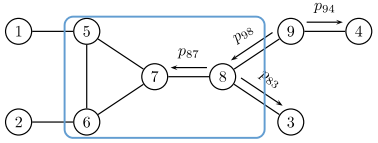
- ノード iに対するサイバー攻撃が起こっていない(つまり $f_i(t) \equiv 0$)
  ときは，他のノードにおいてサイバー攻撃が起こっても
  (つまり $f_j(t) \neq 0,\ j \in \{1,\ldots,N\}\backslash\{i\}$)，検知信号 $r_i(t)$ は0に収束する



- ノード iに対するサイバー攻撃が起こっている(つまり $f_i(t) \neq 0$)
  ならば，検知信号 $r_i(t)$は0以外の値を持つ(つまり $r_i(t) \neq 0$)



提案手法のイメージ



- ノード7で分散的にサイバー攻撃検知
  ノード7に接続しているノード5, 6, 8

ノード8に対するサイバー攻撃が発生

$f_8(t) \neq 0$ ➡ $r_{87}(t), r_{86}(t), r_{85}(t) \neq 0$
$r_{76}(t), r_{75}(t), r_{65}(t) = 0$

r_{jk}：実システムとオブザーバーのノード j,k の位相差の誤差を表す変数

サイバー攻撃が加わったノードと位相差の誤差の関係
(誤差が生じる組み合わせを○で示した)

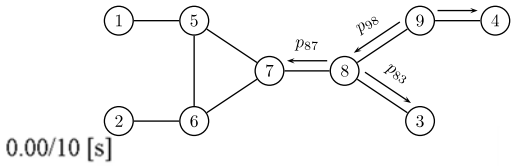
	Cyber attacked nodes								
	8	7	6	5	8,7	8,6	8,5	7,6	7,6,5
r_{87}	○	○			○	○	○	○	○
r_{86}	○		○		○	○		○	○
r_{85}	○			○	○	○	○		○
r_{76}		○	○		○	○	○	○	○
r_{75}		○		○	○		○	○	○
r_{65}			○	○		○	○	○	○

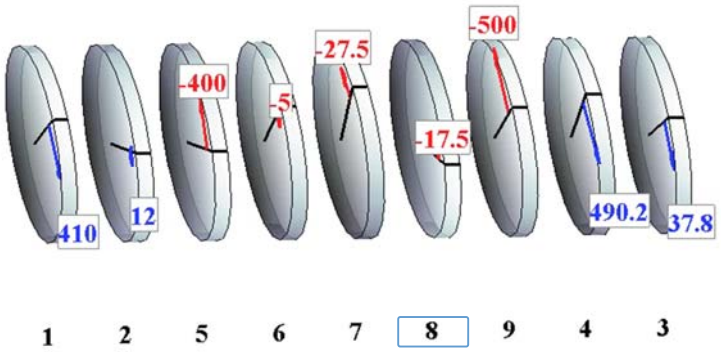
サイバーアタックが起こったノード(同時に $n_i - 1$ 個まで)と，それにより誤差が生じる位相差の組が唯一に決まる

⬇

誤差が生じている位相差の組からサイバー攻撃を検知

数値実験

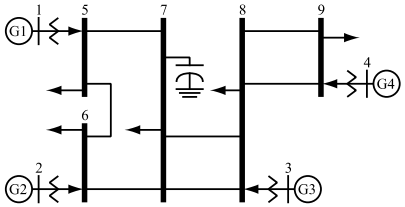




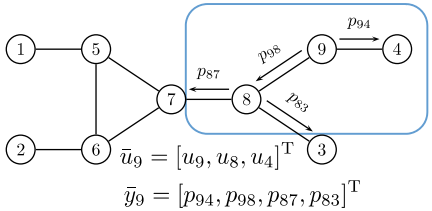
数値実験

- $t = 4$ [s] でノード8に対するサイバー攻撃が発生
- ノード9 (接続ノード4,8) で分散的サイバー攻撃検知

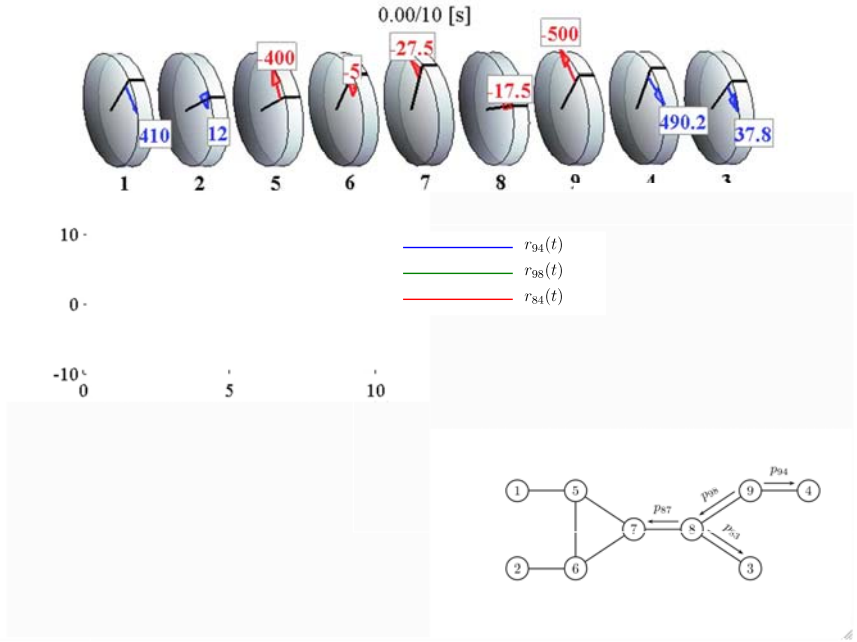
定理より
オブザーバー w_{94}, w_{98}, w_{84} と誤差変数 r_{94}, r_{98}, r_{84} が設計可能



電力ネットワーク

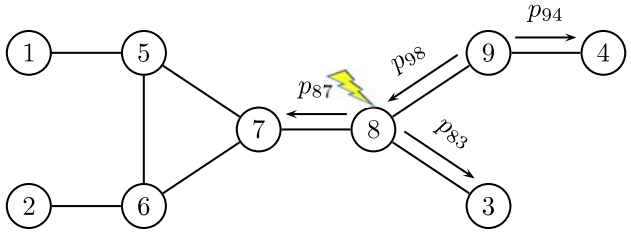


電力ネットワークの接続関係



ノード8に対するサイバー攻撃

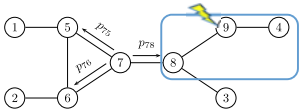
- ノード9, 8, 7で検知できる
- ノード1, 2, 5, 6では検知しない(できない)が，誤検知もない
- ノード3では，ノード8でサイバー攻撃が起こったのか
  ノード3でサイバー攻撃が起こったのか区別できない



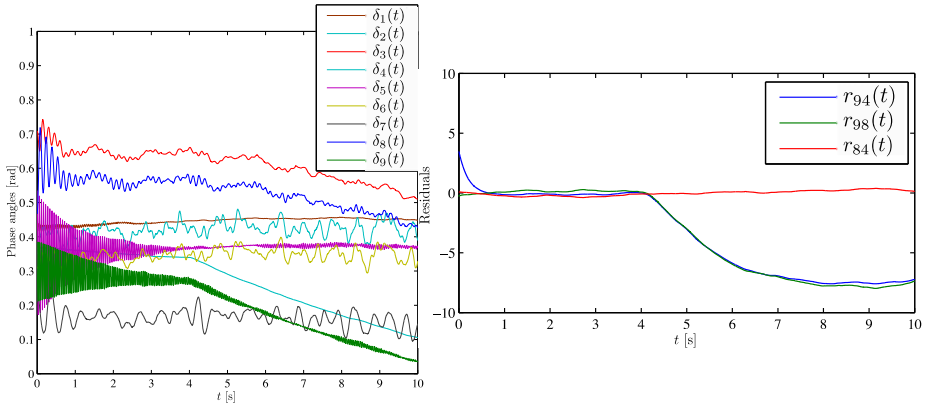
複数の分散的サイバー攻撃検知を行うことで，
電力ネットワーク全体でロバストな故障検知を行える

数値実験

- ノード9における，間接的分散サイバー攻撃検知



$t = 4$ [s] でノード9に対するサイバー攻撃が起こったとき



r_{94}，r_{98} のみ0以外の値を持つ → ノード9に対するサイバー攻撃

まとめ

- 電力ネットワークシステムに対する，分散的サイバー攻撃(故障)検知手法を提案した．
- 一般的に提案手法が適応可能であることを理論的に確かめ，数値実験でその有効性を示した．

今後の課題

- モデル誤差，や外乱に対するロバスト性を陽に考慮した分散的サイバー攻撃(故障)検知手法の提案