



CPHSにおけるサイバーセキュリティ

-Cyber Security for Cyber-Physical-Human Systems-

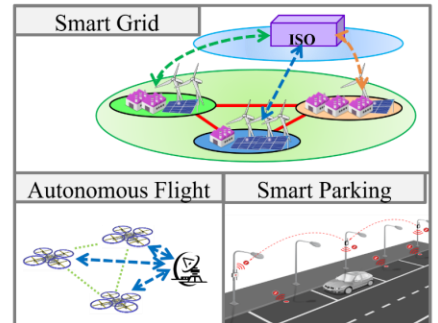
サイバーフィジカルヒューマンシステム (CPHS)

■ 現実世界に点在する「もの」がIoTの技術革新により「システム化」

▶ ICT・IoT技術を最大限活用し、サイバー空間と実空間との融合

■ CPHSに対するサイバー攻撃 → **実システムの破壊**に繋がる恐れ

▶ CPHSにおけるサイバー攻撃に対する頑健性の確立



分散オブザーバセキュア状態推定問題

■ 大規模システムは複数のローカルシステムから構成 → 本質的には**分散システム**

■ 各オブザーバは**局所観測値**のみ観測可能 → 他のオブザーバと**通信**することでシステム全体の状態を推定

■ 攻撃が存在する環境における**状態推定問題**

アプローチ → **仮想状態(Virtual-State)** + **グラフィカル分散オブザーバ**

■ あるオブザーバ e を除外した上での**状態推定値** $\hat{x}^{\setminus e}$

■ 各分散オブザーバ上に複数の**仮想状態**を生成

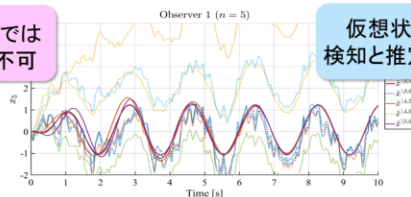
■ 仮想状態を比較することで**被攻撃オブザーバの特定**と**状態真値の推定**

■ **オブザーバ通信構造**と**可観測性**をグラフで一括表現

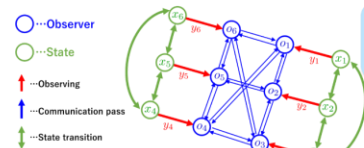
■ 分散オブザーバ問題をグラフ連結性に落とし込むことが可能

■ 状態行列と出力行列によって状態パスと観測パスが決定

通常推定値では
検知・推定不可



仮想状態により
検知と推定を可能に



グラフ上の連結性
議論に帰着

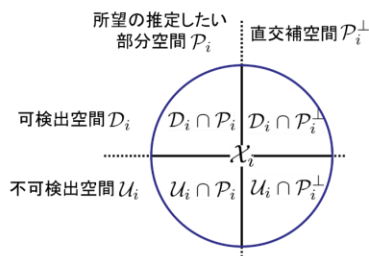
Graphical Distributed Observer

仮想状態 $\hat{x}^{\setminus 2,5}$, $\hat{x}^{\setminus 3,5}$, $\hat{x}^{\setminus 4,5}$, $\hat{x}^{\setminus 5,6}$ が一致 → **被攻撃オブザーバの特定(攻撃検知)**と**セキュア状態推定**を達成

■ 大規模システムや、グラフ連結度が小さいシステム(不可検出なシステム) → 状態ベクトル全体の推定が**困難**

■ グラフ連結度が小さい場合にも近傍のエージェントの情報を元に、部分的に状態ベクトルを推定したい

アプローチ → **可検出分解** + **制限写像 P_i による推定空間の制限**

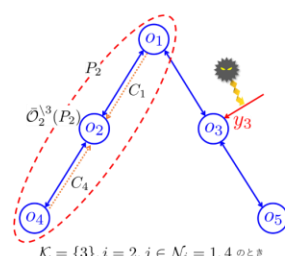


従来の仮想オブザーバ
では推定不可能

不可検出なシステム

抽出された状態空間に
ついてオブザーバを設計

可検出空間を抽出



分散システムのもと
で仮想オブザーバが
構成可能

$$\mathcal{K} = \{3\}, i = 2, j \in \mathcal{N}_i = 1, 4 \text{ のとき}$$

研究者名

システムデザイン工学科 / 総合デザイン工学専攻 教授 滑川 徹

大学院生 滑川 諒 / 学部生 柘植 涼太

お問合せ先

E-mail : namerikawa@sd.keio.ac.jp TEL : 045-566-1731

URL : http://www.namerikawa.sd.keio.ac.jp/