

「分散協調型エネルギー管理システム構築のための理論及び基盤技術の
創出と融合展開」

H24 年度 実績報告

平成24年度採択研究代表者

石井 秀明

東京工業大学 大学院総合理工学研究科・准教授

電力システムにおける系統・制御通信ネットワークに対する
分散型侵入検知手法の構築

§1. 研究実施体制

(1)「東京工業大学」グループ

① 研究代表者:石井 秀明 (東京工業大学・大学院総合理工学研究科・准教授)

② 研究項目

- ・系統情報に基づく侵入検知手法の構築
- ・センサノードの最適配置問題
- ・耐故障性を有する分散型アルゴリズム
- ・ネットワーク化大規模システムの分散型学習
- ・テストベッドの構築

(2)「電力中央研究所」グループ

① 主たる共同研究者:小野田 崇 (電力中央研究所・システム技術研究所・領域リーダー)

② 研究項目

- ・制御通信情報に基づく侵入検知手法の構築
- ・時系列データのノンパラメトリック変化点検知手法の開発
- ・テストベッドの構築

§2. 研究実施内容

本研究では、電力系統と制御通信という2つの大規模なネットワーク構造を持つ電力システムを対象とし、電力系統と制御通信に対する悪意のある攻撃を検知する分散型システム機構の開発を目的とする(図 1)。本年度は、電力系統と制御通信の両ネットワークの研究を並行して行い、基礎的な研究を行った。また、両研究の背景や成果について研究者間で情報を共有することで、最終的な目標である統合されたハイブリッドな検知システム構築に向けてチームの体制を整えた。研究内容として以下を実施した。

(1) 系統情報に基づく検知(担当:石井 秀明)

電力系統では、その状態推定を通じて異常や外部からの侵入を検知する分散型システムを開発することが目的である。とくにネットワーク上の各バス・ノードで、トポロジーに関する情報および観測データを基に、リアルタイムに周辺バスの電圧や位相角を推定した上で、局所的なネットワークモデルを構築する検知機構を設計する。

本年度は、まず定常的な系統モデルを用いた状態推定アプローチに関する研究を行った。高度なサイバー攻撃を受ける場合を想定し、あり得る多様なシナリオを検討しながら、検知システムの分散的な構成法を考えた。また、よりリアルタイム性や精度が高い検知を実現するために、電力系統のダイナミクスを陽に考慮した動的なアプローチも検討した。各ノードにおける挙動をモデル化した上で、ネットワーク化された系統のダイナミクスを構成し、検知手法はオブザーバを用いた状態推定器に基づく手法をベースとすることとした。

上記の定常的なアプローチの枠組みで、検出の精度やロバスト性を向上するために、セキュアな環境下にある観測装置(位相計測装置(PMU)等)を系統内に最適に配置する問題を

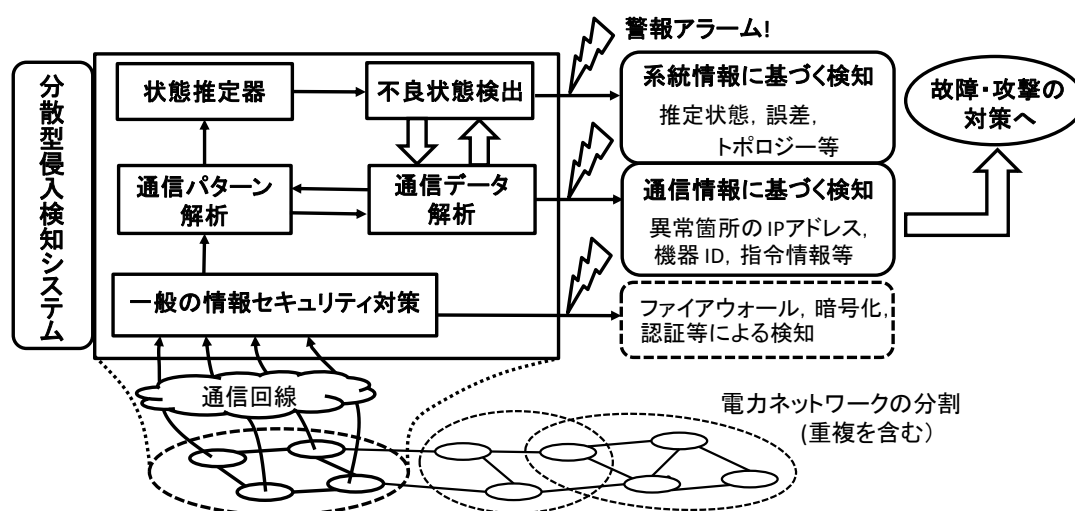


図 1: 分散型侵入検知システムの概要

考えた。既存のモデルが解析のために置いている仮定，問題設定等の様々な観点から既存のモデルを検討し，新たなモデルを構築する上での知見を集積した。

また，分散制御に関する基礎的な課題として，ネットワーク化された動的システムの入出力関係を分散的に学習する手法について検討を行った。

(2) 通信情報に基づく検知(担当:小野田 崇)

制御通信では，ネットワーク上の通信パターンに基づき異常や外部からの侵入を検知する分散型侵入検知システムを開発する。制御機器間の通信や制御情報および観測データを基に，定常状態の通信パターンをモデル化し，異常や侵入を検知する技術を構築する。

本年度は，大規模な電力システムにおける制御系システム内で行われる制御通信の現状を調べ，より効率的な検知を実現するためのシステム構成について検討を行った。現状の制御機器間で行われる制御通信のデータやその通信パターンを整理・分析した。

また，確率モデルに基づく検知モデルの分析についても基礎的な検討を進めた。主に制御システム内における通信が定常状態にある場合を想定し，特徴的な通信パターンに対する数理モデルを構成する。とくに確率モデルとして **Conditional Random Field** と **Hidden Markov Model** を採用し，各々のモデルが持つ検知能力に関する特徴を分析した。攻撃パターンに応じた適切なモデルを検討し，そのための評価指標についても議論した。

他方，これまでに開発してきた時系列データのノンパラメトリック変化点検知手法の電力システムにおける系統・制御通信ネットワークに対する侵入検知への適用可能性を検討した。

(3) テストベッドを用いた統合検知システムの検証(担当:小野田 崇, 石井 秀明)

将来のスマートグリッドで想定される系統や通信のデータを模擬するテストベッドを通じて，攻撃検知システムをシミュレートできる環境を構築する。本年度は，実験環境の整備に向けて，システムの基本的な仕様を設計した。制御機器間の通信を模擬する通信系シミュレータ，および系統ダイナミクスを分散的にシミュレートするために数値計算ソフトウェアを連携させた構成とすること，制御通信プロトコルは国際規格に基づくものとする事等を議論した。