戦略的創造研究推進事業　CREST
研究領域「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」

研究課題「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」

研究終了報告書

研究期間　平成24年10月～平成27年3月

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）

§1 研究実施の概要

(1)実施概要
(チームとしてまとめた研究実施内容や経緯、得られた成果等の研究全体概要を、簡単に分かり易く、概ね1ページ程度でまとめてください。それぞれの研究グループの研究が、どのようにチーム全体の成果につながったのかを中心に記載してください。)

再生可能エネルギーの大量導入や需給状況に応じた電力料金の変動制度等により，電力システムの大規模化や複雑化が進んでいる．その実現には，情報通信技術を広く活用した新たなエネルギー管理システムの開発が不可欠である．将来的な電力システムは電力系統と制御通信の 2 階層からなるネットワーク系とみなすことができる．両ネットワーク間は監視・制御信号を介して相互作用しており，悪意のある攻撃者による外部からのサイバー攻撃は，物理的な設備の誤動作や事故を引き起し得る．本研究では，セキュリティ技術の中でも「侵入検知」と呼ばれる手法に焦点をあてた．これは制御通信ネットワーク内のトラフィックを監視し，異常や故障による不正な通信を検知するものである．

本研究で想定する攻撃は，通信自体は正常だが，監視・制御情報を直接改ざんすることで機器操作を行うものである．例えば，センサ情報のデータ部が攻撃者によってすり替えられることが考えられる．こうした攻撃は一般のセキュリティ対策では検知されない可能性が高い．そこで監視制御システムの特性を考慮した上で，システム理論に基づいたモデルベースのアプローチによる手法を開発した．すなわち，電力系統と通信の 2 つのネットワークのモデルを構築した上で，制御・学習・最適化の手法を応用して，両ネットワークから得られる情報を統合した侵入検知を考えた．

電力系統側では，意図的な機器操作による電力の変動，あるいは不正な情報操作による観測データの変化に対する検知システムの構築を目指し，以下の研究課題に取り組んだ．まず，送電系統を対象として，系統内のバスをグループ化した上で，システムモデルを用いた状態推定機構を準備し，観測データと推定値間の誤差に基づく攻撃検知手法を開発した．システムモデルとしては，静的な場合と動的な場合を考えた．本研究の成果として，従来の偶発的な故障を想定した手法では検知不可能な高度に協調された攻撃に対するロバスト推定法や，検知性能や耐故障性を高めるためにセキュアなセンサを最適に配置するための方法等を導出した．また，機械学習的な観点から，センサ情報の時間的変化に着目した手法についても，基礎的な成果が上がっている．

他方で，配電系統について，系統内の電圧を一定に保持するための電圧制御システムを対象として，センサ情報の改ざんを防止・検知するためのアルゴリズムを構築した．とくに実データに基づいた詳細なシミュレーションを行い，攻撃の影響を解析すると共に，検知アルゴリズムの有効性を確認した．

制御通信ネットワークについては，正規の運転下における設備情報や機器の制御指令の通信パターンや制御情報に対する確率的モデルを用いた機械学習に基づく検知手法を開発した．これによりネットワーク上のパケットやその動作に関して不審なものがないかの確認が可能となる．制御通信に固有のプロトコルを用いた通信データを解析し，攻撃を模した異常データを高い精度で検知できることを示した．

また，本研究で開発する分散型検知手法の有効性を検証するために，テストベッドとしてのシミュレータの開発も進めてきた．そこでは，数値計算ソフトウェア MATLAB を用いて系統のダイナミクスや制御機器，検知アルゴリズム等を模擬し，通信シミュレータ QualNet 上で無線・有

線を介した制御通信ネットワークでのトラフィックや攻撃シナリオのモデル化を行うことが可能となった．両者を連携させたフレームワークを開発し，統一的にデータを扱えるスケーラブルな実験環境が完成した．今後，ネットワーク化された大規模な電力システムにおけるセキュリティの課題を検討することが可能となった．

本チームは，制御工学，機械学習，最適化，信号処理，無線通信等を専門とするメンバーから構成される．また FS 活動を通じて，配電系統や HEMS 等の研究者と深く交流する機会を持つことができた．電力システムのセキュリティ対策に関連する課題は学際的な側面が強く，上記の成果はいずれも複数の専門家による共同研究から生まれたものである．

(2)顕著な成果

(CREST 研究で得られた最も顕著な成果を＜優れた基礎研究としての成果＞と＜科学技術イノベーションに大きく寄与する成果＞各々3 点まで挙げ、それぞれについて 200 字程度で説明してください。研究成果の科学技術上のインパクトや国内外の類似研究の研究動向・状況に対する位置づけについても説明してください。成果は論文、特許、試作品、展示などが挙げられます。)

＜優れた基礎研究としての成果＞

(先導的・独創的であり国際的に高く評価され、今後の科学技術に大きなインパクトを与える成果など)

1．電力システムの状態推定における観測関数に対するサイバー攻撃の解析

概要：送電系統の制御や異常検知，需要予測等のために重要な状態推定機構に対するサイバー攻撃およびその検知手法を検討した．系統内のセンサ情報が悪意のある攻撃者により改ざんされると，従来の故障検知では対応できないが，とくに検知が難しい系統トポロジーや送電線パラメータの改ざんを考えた．外れ値を含む観測データに有効なロバスト推定手法を適用し，分散的な推定・検知の実現のために，系統のグループ化や局所的な情報のみ用いる手法を考案した．

2．配電系統の電圧制御に対する攻撃と検知

概要：本研究では，配電系統における変電所で行われる電圧制御に着目し，系統内のセンサ情報が改ざんされた場合に引き起こされる制御系の異常な振舞いを解析し，その検知のための対策を考案した．検証は，実データに基づいて簡単な配電系統モデル上で数値シミュレーションを通じて行った．とくに情報改ざんにより，系統の一部で電圧逸脱が起き得ること，および単純な検知アルゴリズムにより攻撃が検知可能であることを示した．また，PV 発電の出力抑制に対する影響も評価した．

3．電力システムへのセンサ配置による状態推定のロバスト化

概要：送電系統におけるセンサ情報が攻撃者によって操作された場合にも，監視制御システムにおいて状態推定機構が十分に機能するための方策として，センサ自体が攻撃に強いセキュアなものを配置することが考えられる．本研究では，コスト面を考慮した上で配置するための最適化問題を扱った．とくに一定数のセンサが乗っ取られたとしても残りのセンサでシステムの可観測性を維持するために必要な最小のセンサ数およびその配置箇所を，従来研究に比べて効率的に求めるアルゴリズムを導出した．

＜科学技術イノベーションに大きく寄与する成果＞
（新産業の創出への手掛かりなど出口を見据えた基礎研究から、企業化開発の手前までを含め、科学技術イノベーションに大きく貢献する成果など）

1．電力制御通信ネットワークシミュレータの構築

概要：電力システムにおけるサイバー攻撃によって発生する異常およびその検知を模擬するために，電力系統ネットワークと制御通信ネットワークが適切に連携させたフレームワークを開発し，正常時の運用データや，サイバー攻撃時の運用データ等を生成することを目指した．本フレームワークを用いて，送電系統へのサイバー攻撃を想定したシミュレータおよび Advanced Metering Infrastructure (AMI)シミュレータを構築し，攻撃のシナリオ，攻撃によって起こりうるシステムへの影響について検討が可能となった．

§２ 研究実施体制

(1)研究チームの体制について

① 「東京工業大学」グループ

研究参加者

氏名	所属	役職	参加時期
石井 秀明	東京工業大学　大学院総合理工学研究科	准教授	H24.10～
小野 功	同上	准教授	H24.10～
寺野 隆雄	同上	教授	H24.10～
早川 朋久	東京工業大学　大学院情報理工学研究科	准教授	H24.10～
杉山 将	東京大学 大学院新領域創成科学研究科	教授	H24.10～
Yacine Chakhchoukh	東京工業大学　大学院総合理工学研究科	博士研究員	H25.10～
Ahmet Cetinkaya	東京工業大学　大学院情報理工学研究科	博士研究員	H24.10～
岡野 訓尚	東京工業大学　大学院総合理工学研究科	博士研究員	H24.10～
Seyed Mehran Dibaj	同上	D2	H25.4～
益富 和之	同上	D2	H24.10～
西垣　貴央	同上	D2	H24.10～
小林 雄太	同上	M2(H26 修了)	H24.10～H26.3
磯﨑 保徳	同上	M2	H25.4～
西野 宏亮	同上	M2	H24.10～
楊 航	同上	M2	H24.10～
Samratul Fuady	同上	M1	H26.1～
明石 茂	同上	M1	H25.4～
Lukas Frannek	東京工業大学　大学院情報理工学研究科	D3	H24.10～
岡本　有司	同上	M2(H26 修了)	H24.10～H26.3
Muhamad Bintang Hadi Prayoga	同上	M2(H26 修了)	H24.10～H26.3
庄村　啓	同上	M2	H24.10～
傍島　駿介	同上	M2	H24.10～
Vu Loc Dui	同上	M1	H26.4～
Yao Ma	同上	D2	H26.4～H26.8
Hao Zhang	同上	D2	H26.4～H26.8
Hyunha Nam 南　賢河	同上	D3 (H26 修了)	H25.5～H26.3
Gang Niu	同上	D3 (H26 修了)	H25.5～H25.9

研究項目: 系統情報に基づく検知

・定常アプローチ
・動的アプローチ
・統合化
・ロバスト化：観測装置の最適配置，複数個所への同時攻撃
・通信・計算の負荷軽減
・配電系統の電圧制御
・系統ネットワークのテストベッド構築

② 「電力中央研究所」グループ

研究参加者

氏名	所属	役職	参加時期
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	H24.10～
二方　厚志	同上	上席研究員	H24.10～H25.11
渡邉　勇	同上	主任研究員	H24.10～
木内　舞	同上	主任研究員	H24.10～25.9
宮下　充史	同上	主任研究員	H25.10～
三浦　輝久	同上	主任研究員	H26.4～

研究項目： 通信情報に基づく検知

・ 通信パターンの分析
・ 検知モデルの分析
・ 統合化
・ ロバスト化： 検知システムの最適配置，複数個所への同時攻撃
・ HEMS 通信データの解析
・ スマートメータの通信解析
・ 制御通信ネットワークにおけるテストベット構築

(2)国内外の研究者や産業界等との連携によるネットワーク形成の状況について

本研究領域のFS活動を通じて，他チームとの連携を図った．とくに早稲田大学の林泰弘チームとは，配電系統に対するサイバー攻撃に関して具体的な課題検討を継続的に行い，研究期間内に国際会議で発表できる成果が挙げられた．また，名古屋大学の鈴木達也チームとは，HEMSに関連するセンサ情報をネットワークを介してアグリゲータに送信する際のデータ解析およびサイバー攻撃の可能性について検討を行った．いずれのチームとも引き続き共同研究を進めることとなっている．

また，海外研究協力者との連携については，東工大チーム側に参加しているCNR及びトリノ工科大のロベルト・テンポ先生と制御通信において重要な分散制御について基礎的な研究を進めた．また，本CRESTを通じて電力システムの制御におけるサイバーセキュリティについて議論を深め，定常アプローチの状態推定問題に用いるアルゴリズムに関する共同研究に着手している．

§3 研究実施内容及び成果

3.1 系統情報に基づく検知(東京工業大学グループ)

(1)電力システムの状態推定における観測関数に対するサイバー攻撃

本研究では，送電系統の制御や異常検知，需要予測等のために重要な情報を提供する状態推定機構に対するサイバーセキュリティ向上を目指す．そこでは発電所や変電所をバスとするネットワークを考え，各バスの発電・消費電力，電圧や位相の関係式から，センサでは計測されない状態の推定値を計算する．センサ情報が悪意のある攻撃者により改ざんされると，従来の故障検知手法では検知されずに推定値が変更され得ること指摘され[Liuら 09]，注目されている．

本研究では，推定機構に対する攻撃の中でも検知が難しいシナリオの 1 つである，系統のトポロジーや送電線の特性パラメータが改ざんされる場合を検討した．このような攻撃は，トポロジー解析に用いられる観測値が改ざんされる，あるいは監視制御システムへ直接侵入されることにより，データが操作されて生じ得る．通常の状態推定で用いられる最小二乗法による状態推定での残差に基づく異常検知では，こうした攻撃を見つけることは不可能であり，推定結果が攻撃者によって操作され得る．

そこで本研究では，観測データの一部に外れ値が含まれる場合に有効なロバスト推定手法の 1 つである最小刈込み二乗法(Least trimmed squares) [Miliら 94]を適用した．これは一定数の観測値を無視した上で二乗誤差を最小化する方法である．とくに推定状態により計算される残差が大きい観測値を無視することで，例外的なデータの影響を除去できる．分散的な状態推定および攻撃検知を実現するために，系統を効率的に分割・グループ化した上で，局所的なデータを用いる手法を考案した．

文献：・Y. Chakhchoukh and H. Ishii, Coordinated cyber-attacks on the measurement function in hybrid state estimation, IEEE Transactions on Power Systems, to appear, 2015.
・Y. Chakhchoukh and H. Ishii, Cyber attacks scenarios on the measurement function of power state estimation, Proc. American Control Conference, to appear, 2015.
・Y. Chakhchoukh and H. Ishii, Robust estimation for enhancing the cyber security of power state estimation, Proc. IEEE Power & Energy Society General Meeting, to appear, 2015.
・石井秀明， 電力系統へのサイバー攻撃に対する分散型侵入検知， 計測と制御, vol. 53, no. 10, pp. 916-921, 2014.

(2) 動的な系統モデルを用いた攻撃検知

本研究では，系統のダイナミクスを陽にモデル化した上で，センサ情報に対する改ざん攻撃の在り方やその検知手法を考えた．

有効電力潮流のモデルとして，系統上の発電機のネットワークで生じる同期現象を解析する上で基本的な表現である，動揺方程式に基づくものを用いた[Doerflerら 13]．これは各発電機のダイナミクスや各バスでの注入電力および電力網のトポロジーを考慮するものである．攻撃としては，センサ情報が通信を介して送られる際に悪意のある攻撃者によって改ざんされるケー

スを想定した. このような攻撃により, 例えば消費電力を実際よりも少なく見せることが可能となる.

検知する側は, 時々刻々変化する系統ダイナミクスや電力潮流に関する情報に着目することで, 一部のセンサ情報がその挙動と整合しない場合に, 異常もしくは故障が起きたと判断できる. 本研究では, 幾何学的なアプローチに基づく動的な故障検知フィルタを用いる手法を考えた. とくに, 従来法[Hashimoto ら 12]では扱い困難であった, 複数のバスに対する同時攻撃を検知することを実現した.

文献: H. Nishino and H. Ishii, Distributed detection of cyber attacks and faults for power systems, Proc. 19th IFAC World Congress, pp. 11932-11937, August 2014.

(3) False Data Injection 攻撃に対するロバストなメータ配置に関する検討

近年, 同時に 2 か所以上のメータを攻撃することにより, 状態推定に検知されない攻撃方法 (False Data Injection; FDI) の存在が指摘されている [Liu 09]. そのため, 攻撃に強いセキュアなメータを配置する必要があるが, すべての観測地点にセキュアなメータを配置しようとするとコストが非常に高くなる 問題がある. そこで, k 個のメータが乗っ取られたとしても, 残りのメータで FDI を検知するための最小のメータ数とそれらの配置を求めることが重 要となる. 本問題は, 任意の k 個のメータに異常があったとしても, 残りのメータでシステムが可観測となる最小のメータ数とそれらの配置を求める問題として扱えることが知られている [Bobba 10]. Castillo らは, このメータ配置問題を数理計画問題として定式化する方法を提案している [Castillo 08]. しかし, Castillo らの定式化は非線形であり, 最適化のための計算コストが高いため, k=2 までの問題までしか扱えていない. k=2 の場合においても, 300 バスの問題では, メータの配置箇所を 90 か所に限定することにより, 15.3 分かけて最適解を求めている.

本研究では, Castillo らの計算コストの問題を解決するため, 新しく線形の定式化を提案し, Castillo らの結果に比べて, よりロバス トなメータ配置をより早く発見することに成功した. 具体的には, k=2, 300 バスの問題において, 全てのメータ設置可能箇所 412 か所を対象にした場合でも, 6.7 分で最適解を発見できることを確認した. さらに, Castillo らの手法が扱っていない k=3 の場合においても, 57 バス の問題まで最適解の発見に成功した.

Castillo らのモデルは, 必須メータのみに異常が起こると仮定しており, 冗長メータに異常が起こることは想定できていない. そこで, 現在, 冗長メータに異常が起きたとしても FDI 攻撃を検知するための数理計画モデルの検討を進めている.

文献: Isamu Watanabe, Kazuyuki Masutomi and Isao Ono, Robust Meter Placement against False Data Injection Attacks on Power System State Estimation, Neural Information Processing, Lecture Notes in Computer Science, Vol. 8226, pp.569-576 (2013).

(4) 配電系統の電圧制御に対する攻撃と検知

本研究では, より需要家に近く, 系統および通信網の規模が大きい配電系統を対象として, サイバーセキュリティの問題を扱った. とくに配電系統内の電圧を一定に保つための電圧制御に着目し, 系統内に配置された電圧センサが発信する情報が通信路内で改ざんされた場合を考

えた. その場合に系統が被る影響, およびその検知・防止のための対策を検討した. 配電系統を対象とした従来研究は殆どなく, これは非常に新しい研究課題である.

配電系統のレベルでは, PV 等の再生可能エネルギーの出力が変動することで逆潮流をもたらすため, 電圧制御を通じて系統の地点電圧を適正範囲に維持する制御が必要となる. 複雑化する配電系統の状態を把握するために, 配電線の自動区分開閉器をセンサ内臓型とすること等が検討されている. その開閉器における計測情報を活用した集中的な電圧制御手法も多く提案されている[Hanai ら 10]. 集中型制御を用いた簡単な配電系統モデルを用いて, 限られた数のセンサが攻撃された場合を考える.

本研究では, 実データに基づく数値シミュレーションをベースとする解析を行った. 配電系統モデルとして, 住宅地区を模擬した1 フィーダから成るシンプルなものを用いた, また各需要家に PV が導入されていると仮定した. センサ情報の改ざんにより引き起こされ得る電圧逸脱をクラス分けし, 単純な検知アルゴリズムを用いることで一定程度攻撃を検知できることを示した. また, PVの出力抑制に対する影響の評価も行った.

文献: Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda, and Y. Hayashi, On detection of cyber attacks against voltage control in distribution power grids, Proceedings of the IEEE International Conference on Smart Grid Communications, pp. 848–853, November 2014.

(5) マルチエージェント系の合意問題に対する攻撃にロバストな分散型アルゴリズム

本研究では, 悪意のある攻撃に対してロバストな制御系の基礎的な課題として, マルチエージェント系の合意問題を考えた. 合意問題では, 各エージェントは自身の周りから得る局所的な情報を用いて自分の状態を更新するが, 全エージェントの状態が一致するというシステム全体の目的を達成させることが課題である[Bullo ら 07]. とくに, 一部のエージェントが故障もしくは攻撃により異常な挙動をした場合を扱う. 他の通常のエージェントが影響されずに必ず合意に至ることを保証する分散型アルゴリズムを導出した.

計算科学の分散型アルゴリズムの分野[Lynch 96]の問題設定を踏襲し, 異常エージェントの総数に対する上界が既知であると仮定した. また更新則としても MSR (mean subsequence reduced)アルゴリズムと呼ばれる標準的なものを採用した. そのため各エージェントは更新する毎に, 自身の値から最も差が大きい値を持つエージェントを無視し, 異常エージェントの影響を回避する.

本研究の特徴は, 自律移動型ビークルの合意を想定し, 各エージェントが 2 次系のダイナミクスを持つ場合を扱っている点, およびエージェント間の情報交換を決定するネットワーク構造が備えるべき必要条件・十分条件をグラフのロバスト性と呼ばれる性質[LeBlanc ら 13]で表現した点である.

文献: ・S. M. Dibaji and H. Ishii, Resilient consensus of double-integrator multi-agent systems, Proc. American Control Conference, pp. 5139–5144, June 2014.
・S. M. Dibaji and H. Ishii, Resilient consensus of second-order agent networks: Asynchronous update rules over robust graphs, Proc. American Control Conference, to appear, 2015.
・S. M. Dibaji and H. Ishii, Consensus of second-order multi-agent systems in the presence of locally bounded faults, Systems & Control Letters, to appear, 2015.

(6) ネットワークを介した分散型確率アルゴリズム

分散的な構造を持つネットワーク化されたシステムにおいて，各ノードが自身で得たセンサ情報および近傍との情報交換を通じて得た情報に用いて，系全体で最小二乗法に基づく計算を行う状況を考える．こうした課題は，上記の合意問題とも関連が深いが，電力システムの状態推定問題をはじめ，無線センサネットワークにおける時刻同期や位置推定問題等，合意とは異なる応用がある．本研究では，ノード間の通信が非同期に行われる状況を想定して，通信時刻が確率的に決まる場合の分散型アルゴリズムと，その性能解析を行った．

文献：C. Ravazzi, P. Frasca, R. Tempo, and H. Ishii, Ergodic randomized algorithms and dynamics over networks, IEEE Transactions on Control of Network Systems, vol. 2, no. 1, pp. 78–87, 2015.

(7) 機械学習によるノンパラメトリック異常検知

本研究では，パラメトリックなモデルを用いずに，得られるデータだけからノンパラメトリックに異常や侵入を検知する機械学習技術を構築した．このようなノンパラメトリックな異常検出アプローチは，電力網の定常的な系統モデルを用いた状態推定に基づくアプローチと相補的な関係にあるため，これらを組み合わせることによって様々な種類の変化に対応できる技術が開発できると期待される．

従来の統計的な変化検知では，あらかじめ生成されるデータの確率分布を仮定したもとで，変化前と変化後のデータからそれぞれパラメータ推定し，それらを比較することによって変化の有無を判定していた．しかし，このようなアプローチでは，データ生成確率分布のモデルを事前に仮定するため，想定していない変化を捉える事ができないという問題がある．また，変化前と変化後の確率分布をそれぞれ推定するため，それぞれの確率分布が精度良く推定できたとしても，必ずしも変化が精度良く推定できるとは限らないという原理的な弱点もある．更に，従来の手法では変数間の相関関係の変化のみを調べるため，高次の相関に関わる変化は捉えられないという問題もある．

そこで本研究では，変化前と変化後の確率分布を推定するのではなく，「変化」そのものを直接ノンパラメトリックに推定する機械学習手法を開発した．これにより，ネットワークの構造を反映したパラメトリックモデルが不要となる．更に変化を直接データから学習することにより，変化検出の精度の大幅な向上が期待される．計算機実験により，少数のデータから従来法よりも高精度に変化が検出できることを実証した．また，変化のパターンがスパースな場合に，従来法よりも少ない標本数で正しく変化が検出できることを理論的にも証明した．更に，従来手法では計算量の爆発のため高次の相関関係の変化を検出することが著しく困難であったが，変化そのものを直接推定するという定式化の特徴を生かすことで克服し，現実的な計算時間で高次相関の変化を捉えられることを計算機実験により示した．

文献：S. Liu, J. Quinn, M. U. Gutmann, M. Sugiyama, Direct learning of sparse changes in Markov networks by density ratio estimation. Neural Computation, vol.26, no.6, pp.1169–1197, 2014.

3．2 通信情報に基づく検知（電力中央研究所グループ）

(1) 制御通信データにおける異常検知に対する機械学習アプローチ

近年，遠隔制御に用いられる制御通信ネットワークは，効率化のために外部に接続された業務用ネットワークに繋がれるようになった．そのため，制御通信ネットワークに対するサイバーセキュリティが注目されている．本研究では，制御システムに対するサイバー攻撃の検知を目指すが，とくに制御データを解析することで行った．このような攻撃は過去の事例が少なく，正規通信のみを利用した手法が重要となる．ここでは，制御通信の特徴を考慮した上で，教師なし機械学習の手法を用いた検知を考える．

先行研究[木内ら 12]では，制御系の運転時に生じる一定の順序にしたがう制御や観測信号の送信等を検知のための学習に用いた．本研究では，通信データに限定せずに，制御入力や目標値等，制御機器に直接関わる情報を用いることで学習精度が向上することを示した．公開されている，攻撃データを含む実験データに基づき，本手法の有効性を確認した．

文献：明石茂，小野田崇，石井秀明，「制御通信データにおける異常検知に対する機械学習アプローチ」，計測自動制御学会 制御部門マルチシンポジウム，電気通信大学，2014年3月6日．

3．3 テストベッドを用いた統合検知システムの検証（東工大グループ・電中研グループ）

(1)電力制御通信ネットワークシミュレータの構築

電力系統と監視制御用通信の双方の情報を利用したサイバー攻撃によって発生する異常の検知手法を開発するためには，電力系統ネットワークと制御通信ネットワークが適切に連携させた環境で，正常時の運用データに加えて，サイバー攻撃時の運用データを取得がある．しかし，現在，そのようなデータを容易に取得できるオープンテストベッドは存在しない．そのようなデータを取得するためには，実機を組み合わせて模擬環境を構築するしかなく，さまざまな状況を想定して研究を推進することは非常に困難である．

本研究では，安価かつ容易に電力システムを模擬して，サイバー攻撃時を含むさまざまな状況下における運用データを生成するため，我々のグループで構築している電力系統ネットワークと制御通信ネットワークの連成シミュレーションフレームワークの開発を行った．本フレームワーク は，MATLAB の API を提供している．通信 NW シミュレータとの通信は，本研究で提案したオープンな通信プロトコル Simple Network Simulator Protocol (SNSP)を用いて行われる．SNSP は，最も標準的な通信プロトコルである TCP/IP 上に実装されている．一方，電力系統 NW シミュレータとの通信 は，MATLAB の関数呼び出しを用いて行うことができる．通信 NW シミュレータの実装としては，定評のある商用の QualNet を採用し，QualNet に対して SNSP を解釈するラッパプログラムを作成した．電力系統 NW シミュレータの実装としては，無償の MATPOWER8)をベースにして，指定した時間だけ時刻を進めて一時停止するようなメソッドをもつシミュレータを作成した．本フレームワーク を用いて，送電系統へのサイバー攻撃を想定したシミュレータおよび Advanced Metering Infrastructure (AMI)シミュレータを構築し，それぞれにおいて攻撃のシナリオ，攻撃によって起こりうるシステムへの影響について検討を行った．

文献：小野功，益富和之，西野宏亮，西垣貴央，石井秀明，三浦輝久，宮下充史，小野田崇：電力系統ネットワークと制御通信ネットワークの連成シミュレーションフ

§4 成果発表等

(1)原著論文発表 （国内(和文)誌 0 件、国際（欧文）誌 17 件）

1. Watanabe, K. Masutomi and I. Ono, ``Robust meter placement against false data injection attacks on power system state estimation,'' Neural Information Processing, Lecture Notes in Computer Science, Vol. 8226, pp. 569-576, 2013. (DOI:10.1007/978-3-642-42054-2_71)
2. S. Liu, J. Quinn, M.U. Gutmann, and M. Sugiyama, Direct learning of sparse changes in Markov networks by density ratio estimation. In Proceedings of European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML-PKDD2013), pp.596-611, Prague, Czech Republic, Sep. 23-27, 2013.
3. C. Ravazzi, P. Frasca, R. Tempo, and H. Ishii, Almost sure convergence of a randomized algorithm for relative localization in sensor networks, Proc. 52nd IEEE Conference on Decision and Control, pp. 4778-4783, 2013.
4. T. Onoda, Probabilistic Models Based Intrusion Detection Using Sequence Characteristics in Control System Communication, EANN 2014, CCIS 459, pp. 155-164, 2014.
5. S. M. Dibaji and H. Ishii, Resilient consensus of double-integrator multi-agent systems, Proc. American Control Conference, pp. 5139-5144, June 2014.
6. H. Nishino and H. Ishii, Distributed detection of cyber attacks and faults for power systems, Proc. 19th IFAC World Congress, pp. 11932-11937, August 2014.
7. Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda, and Y. Hayashi, On detection of cyber attacks against voltage control in distribution power grids, Proceedings of the IEEE International Conference on Smart Grid Communications, pp. 848-853, November 2014.
8. S. Liu, J. Quinn, M. U. Gutmann, M. Sugiyama, Direct learning of sparse changes in Markov networks by density ratio estimation. Neural Computation, vol.26, no.6, pp.1169-1197, 2014.
9. S. Nakajima, and M. Sugiyama, Analysis of empirical MAP and empirical partially Bayes: Can they be alternatives to variational Bayes? In Proceedings of Seventeenth International Conference on Artificial Intelligence and Statistics (AISTATS2014), pp.20-28, Reykjavik, Iceland, Apr. 22-24, 2014.
10. Y. Ma, T. Zhao, K. Hatano, and M. Sugiyama, An online policy gradient algorithm for continuous state and action Markov decision processes. In Proceedings of European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML-PKDD2014), pp.354-369, Nancy, France, Sep. 15-19, 2014.
11. S. Suzumura, K. Ogawa, M. Sugiyama, and I. Takeuchi, Outlier path: A homotopy algorithm for robust SVM. In Proceedings of 31st International Conference on Machine Learning (ICML2014), pp. 1098-1106, Beijing, China, Jun. 21-26, 2014.
12. C. Ravazzi, P. Frasca, R. Tempo, and H. Ishii, Ergodic randomized algorithms and dynamics over networks, IEEE Transactions on Control of Network Systems, vol. 2, no. 1, pp. 78-87, 2015.
13. Y. Chakhchoukh and H. Ishii, Coordinated cyber-attacks on the measurement function in hybrid state estimation, IEEE Transactions on Power Systems, to appear, 2015.
14. Y. Chakhchoukh and H. Ishii, Cyber attacks scenarios on the measurement function of

power state estimation, Proc. American Control Conference, to appear, 2015.

15. Y. Chakhchoukh and H. Ishii, Robust estimation for enhancing the cyber security of power state estimation, Proc. IEEE Power & Energy Society General Meeting, to appear, 2015.
16. S. M. Dibaji and H. Ishii, Resilient consensus of second-order agent networks: Asynchronous update rules over robust graphs, Proc. American Control Conference, to appear, 2015.
17. S. M. Dibaji and H. Ishii, Consensus of second-order multi-agent systems in the presence of locally bounded faults, Systems & Control Letters, to appear, 2015.

(2)その他の著作物(総説、書籍など)

1. 石井秀明,「講座:マルチエージェントシステムの制御 ― Ⅰ 総論」, システム/制御/情報, vol. 57, no. 5, pp. 221-228, 2013.
2. 石井秀明, 電力系統へのサイバー攻撃に対する分散型侵入検知, 計測と制御, vol. 53, no. 10, pp. 916-921, 2014.

(3)国際学会発表及び主要な国内学会発表

① 招待講演 (国内会議 6 件、国際会議 4 件)

(主要な国際会議への招待講演の前に*を付記してください)

1. H. Ishii, Distributed Intrusion Detection Methods for Power Grids and Control Communication Networks in Electric Power Systems, 計測自動制御学会, 第 13 回制御部門大会, 福岡市, 2013 年 3 月 7 日
2. 石井秀明,「電力系統に対する分散型侵入検知」, 計測自動制御学会 産業応用部門 2013 年度大会, 東京工業大学, 2013 年 10 月 22 日.
3. 小野田崇,「監視制御通信シーケンスに基づく侵入検知の研究構想」, 計測自動制御学会 産業応用部門 2013 年度大会, 東京工業大学, 2013 年 10 月 22 日.
4. 渡邊勇, 益富和之, 小野 功,「電力系統へのサイバー攻撃を考慮したロバストなメータ配置に関する基礎検討」, 計測自動制御学会 産業応用部門 2013 年度大会, 東京工業大学, 2013 年 10 月 22 日.
5. 早川朋久,「動的ネットワーク符号化の定式化」, 計測自動制御学会 産業応用部門 2013 年度大会, 東京工業大学, 2013 年 10 月 22 日.
6. 杉山将,「機械学習による変化検知」, 日本鉄鋼協会 計測・制御・システム工学部会シンポジウム, 和歌山, 2013 年 11 月 29 日.
7. H. Ishii, ``Distributed intrusion detection for power grids and control communication networks,'' Workshop on Cooperative Distributed Control for Energy Management Systems, 52nd IEEE Conference on Decision and Control, Florence, Italy, Dec. 9, 2013.
8. M. Sugiyama, ``Machine learning with density ratio estimation,'' Japan-Britain Workshop on Big Data Research, Tokyo, Feb. 6, 2014.
9. H. Ishii, Distributed detection of cyber attacks against power grids, Brainstorming Session on Systems, Control and Networks, CNR-IEIIT, Politecnico di Torino, Italy, Nov. 27, 2014.
10. H. Ishii, Detection of coordinated cyber attacks on state estimation in power systems, Oberwolfach Workshop on Control Theory: A Mathematical Perspective on Cyber-Physical Systems, Feb. 23, 2015.

② 口頭発表　　（国内会議 7 件、国際会議 2 件）

1. 西野宏亮, 電力系統におけるサイバー攻撃・故障の分散的検知, 計測自動制御学会, 第 13 回制御部門大会, 福岡市, 2013 年 3 月 8 日
2. Takashi Onoda, “Analysis of intrusion detection in control system communication based on outlier detection with one-class classifiers,” 19th International Conference on Neural Information Processing (ICOMP 2012), Doha, Qatar, November 2012.
3. M. Kiuchi and T. Onoda, “Analysis of intrusion detection in control system communication based on outlier detection with one-class classifiers,” 26th European Conference on Operations Research, Rome, Italy, July 2, 2013.
4. 磯﨑保徳, 芳澤信哉, 藤本悠, 石井秀明, 小野功, 小野田崇, 林泰弘,「配電系統電圧制御におけるサイバー攻撃検知に関する考察」, 計測自動制御学会 制御部門マルチシンポジウム, 電気通信大学, 2014 年 3 月 5 日.
5. Y. Chakhchoukh and H. Ishii, “Cyber attack detection in power state estimation,” 計測自動制御学会 制御部門マルチシンポジウム, 電気通信大学, 2014 年 3 月 5 日.
6. 明石茂, 小野田崇, 石井秀明,「制御通信データにおける異常検知に対する機械学習アプローチ」, 計測自動制御学会 制御部門マルチシンポジウム, 電気通信大学, 2014 年 3 月 6 日.
7. M. Dibaji and H. Ishii, “Resilient consensus of double-integrator multi-agent systems,” 計測自動制御学会 制御部門マルチシンポジウム, 電気通信大学, 2014 年 3 月 7 日.
8. S. M. Dibaji and H. Ishii, “Multi-agent consensus under asynchronous update rules in the presence of malicious agents,” SICE International Symposium on Control Systems, Tokyo, Mar. 6, 2015.
9. Y. Chakhchoukh and H. Ishii, “Redundant LTS-based detection of cyber-attacks on the measurement function,” SICE International Symposium on Control Systems, Tokyo, Mar. 7, 2015.

③ ポスター発表　　（国内会議 2 件、国際会議 1 件）

1. 石井秀明, 小野功, 早川朋久, 杉山将, 小野田崇, 二方厚志, 渡邊勇,「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」, 計測自動制御学会 システム・情報部門 学術講演会, 大津, 2013 年 11 月 19 日.
2. M. Dibaji and H. Ishii, ``Resilient consensus of double-integrator multi-agent systems,'' 3rd International Symposium on Innovative Mathematical Modelling, University of Tokyo, Nov. 14, 2013.
3. 小野功, 益富和之, 西野宏亮, 西垣貴央, 石井秀明, 三浦輝久, 宮下充史, 小野田崇:電力系統ネットワークと制御通信ネットワークの連成シミュレー ションフレームワークの構築, 第 57 回自動制御連合講演会講演集, 7 pages, 2014.

(4)知財出願

①国内出願 (0 件)
②海外出願 (0 件)

③その他の知的財産権
・特になし

(5)受賞・報道等

① 受賞

・石井秀明, 計測自動制御学会 制御部門研究賞(木村賞), 2013 年 3 月

・木内舞, 小野田崇, 第 69 回電気学術振興賞 論文賞, 2013 年 5 月,「監視制御通信におけるシーケンスを考慮した侵入検知」, 電気学会論文誌 C, Vol.132, No.1, pp.14-20, 2013.

② マスコミ(新聞・TV等)報道

特になし

③ その他

特になし

(6)成果展開事例

・特になし

②社会還元的な展開活動

・特になし

§５ 研究期間中の活動

主なワークショップ、シンポジウム、アウトリーチ等の活動

年月日	名称	場所	参加人数	概要
2012 年度	チーム内ミーティング：進捗報告（キックオフミーティング他，計 6 回，非公開）	東京工業大学すずかけ台キャンパス他	20 人程度	
2012 年度	チーム内ミーティング：シミュレータ作成のための業者との打ち合わせ（計 3 回，非公開）	東京工業大学すずかけ台キャンパス他	8 人程度	
2013 年 3 月 7 日	計測自動制御学会 第 13 回制御部門大会 CREST 企画	ACROS 福岡，福岡市	200 人	海外からの招待講演者 4 名，および本 CREST の研究代表者 5 名による講演 学会セッションを 4 つオーガナイズ，日本学術会議 IFAC 分科会と共催
2013 年度	チーム内ミーティング：進捗報告（計 9 回，非公開）	東京工業大学すずかけ台キャンパス他	20 人程度	
2013 年度	チーム内ミーティング：シミュレータ作成のための業者との打ち合わせ（計 10 回程度，非公開）	東京工業大学すずかけ台キャンパス他	8 人程度	
2014 年度	チーム内ミーティング：進捗報告（計 6 回，非公開）	東京工業大学すずかけ台キャンパス他	20 人程度	

§６ 最後に

本課題を通じては，電力システムのサイバーセキュリティという将来的かつ重要な課題に，異分野の研究者が協同して挑戦するという得難い機会が与えられた．研究代表者としては電力システムに関する知識も十分にない状況でプロジェクトを立ち上げたが，この分野における研究が国際的に活発になりつつあるタイミングでもあったこと，また適度に異なる分野のメンバーが揃っていたことから，チーム全体で本格的に取り組むのにはさほど時間はかからなかった．さらに，本 CREST 内でセキュリティに対する関心が高く，またこの研究分野に焦点を当てているチームが他にないこともメンバーの動機づけを後押ししたように感じる．

立ち上げ当初から見た場合の目標の達成度を測るのは必ずしも容易でないが，2.5 年間の研究期間を通じて，一定の成果は得られたと考えている．基本的なことから挙げると，電力システム，そ

の制御・監視等の理論や実際に関する基礎知識を得て，この分野の研究状況が把握できるようになった．これは今後の研究課題や方針を立てる上で欠かせない．また，本チーム内あるいは FS 活動を通じて共同研究がいくつも行われ，ディスカッションを通じて取り組むべき課題の検討から試みを始めた．実際に，電力系統に対する攻撃の検知手法，制御通信ネットワークのモデル化と解析，学習手法の開発と検知への応用等の課題において，既に具体的な成果も上がっている．当初予想もしていなかった広がりをもった横の展開があった．これは本 CREST の運営に負うところも大きい．今後，最強チームに再編がなされた後にも繋がる長期的な研究活動が期待できるものも多く，メンバー一同楽しみにしている．

当初予期していなかったことの１つは，主要なチームメンバー2 名が抜けることを余儀なくされたことである．プロジェクト開始当時には，本チームの研究課題が直接関わる分野の研究者はこの 2 名だけであったため，取り組む課題や進捗，他メンバーの担当エリア等に変更が生じた．

謝辞：本研究課題を進めるにあたり，ご指導ご支援くださった，研究総括の藤田政之先生，アドバイザーの先生方にこの場を借りて感謝の意を表したい．また，JST の職員の方々のサポートにも多くの場面で助けられた．合わせて謝意を表する．