様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　　６　日現在

機関番号：　１２６０８
研究種目：　基盤研究(B)（一般）
研究期間：　2015～2017
課題番号：　１５Ｈ０４０２０

研究課題名（和文）大規模ネットワーク化系のための制御論的セキュリティ対策の確立

研究課題名（英文）Security measures for large-scale networked systems based on a control theoretic approach

研究代表者

石井　秀明（Ishii, Hideaki）

東京工業大学・情報理工学院・准教授

研究者番号：５０３７６６１２

交付決定額（研究期間全体）：（直接経費）　　6,800,000円

研究成果の概要（和文）：本研究では，ネットワーク化された大規模制御系に対する悪意のあるサイバー攻撃とその情報セキュリティ対策を制御理論の観点に基づいて考える．攻撃として観測・制御信号の改ざんや無線通信に対するジャミングを想定し，危険な情報が及ぼし得る影響を抑制する制御・推定手法を構築した．主たる成果として，マルチエージェント系の合意問題において異常エージェントが含まれる場合にロバストに合意を達成するアルゴリズムの構築や，無線通信を介した線形制御系がジャミング攻撃やパケット損失の影響下にある場合の安定性解析が挙げられる．通信や計算量の面で制約される環境においても，セキュリティレベルや制御性能を保証する方法を導出した．

研究成果の概要（英文）：In this research, we have studied cyber security measures for large-scale networked control systems in the presence of malicious attacks from the viewpoint of control theory. As cyber attacks, we have considered data manipulation in measurement and control signals as well as jamming attacks in wireless communication. We have developed control and estimation techniques to mitigate the effects of such attacks. The main results include (i) resilient consensus algorithms for networks containing faulty/attacked agents which may prevent regular agents from reaching consensus and (ii) stability analysis for linear systems under jamming attacks and random packet dropouts. Our methods guarantee given security levels and control performance even when resources for communication and computation may be restricted.

研究分野：　制御工学

キーワード：　制御工学　ネットワーク化制御　サイバーセキュリティ　マルチエージェント系　分散アルゴリズム

１．研究開始当初の背景

大規模制御系において，インターネットや無線通信を介したオープンなネットワーク化は，情報セキュリティ面のリスクを著しく高めている．悪意のある攻撃により物理的な事故が起きれば非常に危険である．そうした攻撃は観測・指令信号の数値データ改ざんのみで可能であるため，汎用情報機器向けのセキュリティ対策では十分に対処できない．制御系の信頼性確保のために情報セキュリティは社会的にも非常に重要であり，その解決は急務である．本研究の目的は，制御システム論的な観点から，ネットワーク化された制御系のモデルや特性を考慮した上で，危険な情報が信号に含まれる場合にもロバストに制御や推定を可能とする手法の構築である．

こうした背景から研究代表者は最近，監視制御システムに対する侵入検知に関して，スマートグリッドと呼ばれ情報化が進む電力システムを対象に共同研究を進めてきた．例えば，電力系統の制御に欠かせない状態推定において，検知がとくに難しい系統パラメータの改ざんに対するロバスト推定法を提案した．また，より基礎的な課題として，自律移動ロボット群を想定したマルチエージェント系において，一部エージェントが故障・攻撃により異常に振舞う場合にも所望の協調制御を達成する分散アルゴリズムを構築した．

２．研究の目的

本研究では，こうした結果に共通して現れる，制御情報の改ざんや異常に対するロバスト化の手法に着目する．そこでは一定以上操作された情報は有用性の低い「外れ値」と見做し得るとして無視する．この手法は次のように説明できる．(i) 各時刻で観測データが冗長で十分な数が得られるとする．(ii) 改ざんされ得るデータ数に上限を設定する．(iii) 他のデータとの差や推定誤差が大きいデータを上限数だけ除外し，残りのデータで制御や推定を行う．これはセキュリティの観点から自然である上，小型センサを多数利用できるネットワーク化制御に適している．

本研究は，上記の外れ値や誤情報を検出・除去するセキュリティ対策のアプローチを，より一般的なダイナミクスを持つネットワーク化制御システムに対するレジリエントな制御・推定手法の枠組みとして展開することを目標とする．より複雑な動特性を持つ対象として，高次の状態方程式表現を持つシステムと，性能向上や困難なタスク達成のために補助的な変数を持つ等，高度化された分散アルゴリズムを考える．とくに通信・計算量に対する制約を考慮し，観測データの冗長性の低減化と，外れ値の選択時に生じる組合せ論的な計算の効率化を目指す．また，セキュリティに関わりが深い問題として，観測情報が匿名性やプライバシーを有する場合を考える．これは社会システムを扱うエージェント系では本質的な問題であるが，制御情報に匿名性を持たせることで攻撃に対するロバスト性を上げる可能性についても検討する．

３．研究の方法

セキュリティの観点から制御系のレジリエント性向上を目指し，具体的に以下の課題に取り組む．

(1) マルチエージェント系の合意問題

本研究の中心的な課題として，エージェント系に対する協調制御の基本的課題の 1 つである合意問題を考える．そこでは各エージェントが自身の持つ状態量を近傍のエージェントと交換しながら更新し，最終的にそれが同一の値に到達することを目指す．一部の異常エージェントが誤情報を発信し，合意を妨害する状況を考える．外れ値に基づくアルゴリズムで達成可能な防護レベルと必要な通信や計算量の間のトレードオフを解明する．ネットワークが持つ接続構造やダイナミクスに関して一般化を図ると共に，より高度な協調制御問題へと発展させる．

(2) サイバー攻撃下のネットワーク化制御

通信路を介してフィードバック制御系を遠隔制御する際にサイバー攻撃を受けた場合の制御システムへの影響を解析する．攻撃として無線ネットワークに対するジャミング攻撃や通信量の変動，センサ情報の改ざんを検討し，制御性能に対する影響の解析やロバストな制御器設計を考える．

(3) 匿名情報に基づく推定

エージェント系の出力が個々のエージェントに関連付けられず，データのプライバシーが問題となる状況を考え，可観測性や状態推定等の未解決な課題を検討する．

(4) 統一的な枠組みの構築：上記の課題で得られる知見や手法を統合させることで，よりセキュリティレベルの高い制御系を実現するための枠組みと解析法を確立する．

これらの課題に対し，主に理論研究を進めるが，その有効性の検証は，数値実験およびセンサネットワーク系の実験を通じて行う．後者では実際の攻撃の在り方についても検討する．

４．研究成果

本研究で得られた成果のうち主たるものを以下にまとめる．

(1) レジリエントな合意アルゴリズム構築

大規模なネットワーク化されたエージェントシステムにおいて，エージェント間の相互作用を通じて各エージェントが持つ状態値が一致するための合意アルゴリズムを考える．ここでは一部のエージェントが悪意を持って，正常なエージェントの合意を妨害すべく行動する場合を扱う．正常エージェントは近傍の情報の内，非常に大きな値もしくは小さな値を外れ値として無視する単純なアルゴリズムを採用する．合意達成のために必要十分なネットワーク構造に関する条件を導出した．

エージェントが持つ値に関して，実数の場合および整数値の場合を検討した．前者では各エージェントが高次のダイナミクスを持つ場合として自律移動ビークルを扱った．後者については，各エージェントが更新を行う時刻を確率的に決定するゴシップ通信の仕組みを導入し，グラフのロバスト性に関するタイトな条件を導出した．さらに最大値ベースの更新則を導入することで，従来法よりも高速な合意達成を可能とした．

(2) 無線センサネットワークでのレジリエントな分散型時刻同期アルゴリズム

上記のレジリエントな合意問題の応用として，無線センサネットワークにおける時刻同期アルゴリズムを考えた．センサノードの時計が故障や攻撃によって異常を示す場合にも，影響を受けずに同期する手法を開発した．とくに情報交換に時刻遅れが伴う場合を扱った．センサネットワークの実機を用いた検証も行った．

(3) ジャミング攻撃下における線形制御システムの安定性解析

無線通信を介したネットワーク化制御システムに対してジャミング攻撃がなされた場合を考え，その安定性解析を行った．攻撃に要する消費エネルギーに制約を設け，また正常時にも生じるランダムなデータ損失を考慮した．システムは確率的となるが，攻撃に関しては確率分布が未知となるため，解析が困難である．とくに攻撃パターンが無数にあるため，解析に必要な計算効率が問題となるが，従来法よりも精度の高い手法を開発した．

さらに同様なジャミング攻撃がマルチエージェント系の合意問題に与える影響についても検討し，その抑制を確率的な通信により実現する手法を提案した．

(3) アンサンブル系に対する状態推定

多数の同一のダイナミクスを持つ線形システムから構成されるアンサンブル系に対する初期状態の推定問題を考えた．アンサンブル系においてはシステムが匿名性を有しており，出力値を観測した際に，各出力とシステムの添え字を結びつけることが出来ない．そのため組み合わせ論的な問題が生じる上，どの程度観測を行えば推定が可能となるかという問題が生じる．本研究ではシステム間で情報交換がある場合，およびシステムのダイナミクスが異なる場合を検討した．

(4) 情報理論に基づくネットワーク制御系の性能限界解析

制御システムの性能評価において，通信に関する基礎分野である情報理論を活用して解析する．とくに信号のエントロピーや相互情報量を見ることで，非線形システムの解析が容易になることが知られる．本研究では，制御理論における古典的な結果であるボードの定理を通信ネットワークを含む場合に拡張した．制御器や符号器・復号器に関して因果性のみを仮定した一般的な理論を構築し，通信量が制御性能限界に与える影響を陽に表すことに成功した．そこでは通信量を特徴づける新たな情報論的な測度 blurredness を導入した．本研究の集大成となる研究書が出版された．その一部は本研究課題の中で進められたものである．

(5) サイバーフィジカルシステムのための連成シミュレータの性能評価

ネットワーク化制御系を高精度にシミュレーションするために以前に開発したツールの性能評価を進めた．これは数値計算ソフト Matlab/Simulink と通信シミュレータ QualNet の連成シミュレーション環境である．両シミュレータ間の時刻同期を効率的かつ高精度に実現している．とくに無線センサネットワークのように多数のデバイスから成るシステムをシミュレートする場合に有用であり，時刻同期アルゴリズムのケーススタディを行い，有効性を確認した．

(6) 自己駆動制御に基づく通信低減化

ネットワーク化制御系のために用いる通信量を削減する手法として注目されている自己駆動型制御について新たな手法を提案した．これは線形システムに対して 2 次評価関数を導入し，制御性能を保証しつつ通信を低減化するものとなっている．とくに制御信号の送信時刻をリアルタイムに決定する際に必要となる計算を効率的に行う特徴を持つ．

数値シミュレーションを通じて，本手法と既存法の詳細な比較を行い，計算量と通信量の間にあるトレードオフを確認した．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 24 件）

1. Cetinkaya, H. Ishii, and T. Hayakawa, Networked control under random and malicious packet losses, IEEE Transactions on Automatic Control, 62: 2434-2449, 2017. （査読有）
2. S. M. Dibaji and H. Ishii, Resilient consensus of second-order agent networks: Asynchronous update rules over robust graphs, Automatica, 81: 123-132, 2017. （査読有）
3. S. Fang, J. Chen, and H. Ishii, Fundamental error bounds in state estimation: An information-theoretic analysis, Proc. 56th IEEE Conference on Decision and Control, pp. 357-362, 2017. （査読有）
4. S. Fang, J. Chen, and H. Ishii, Intrinsic limits of power reduction in MIMO networked control systems, Proc. 56th IEEE Conference on Decision and Control, pp. 4759-4764, 2017. （査読有）
5. K. Kikuchi, A. Cetinkaya, T. Hayakawa, and H. Ishii, Stochastic communication protocols for multi-agent consensus under jamming attacks, Proc. 56th IEEE Conference on Decision and Control, pp. 1657-1662, 2017. （査読有）
6. Y. Kikuya, S. M. Dibaji, and H. Ishii, Resilient clock synchronization over unreliable channels in WSNs, Proc. 56th IEEE Conference on Decision and Control, pp. 996-1001, 2017. （査読有）
7. A. Cetinkaya, H. Ishii, and T. Hayakawa, Wireless control under jamming attacks with bounded average interference power, Proc. 20th IFAC World Congress, pp. 8735-8740, 2017. （査読有）
8. K. Takijiri and H. Ishii, Networked control of uncertain systems via the coarsest quantization and lossy communication, Proc. 20th IFAC World C ongress, pp. 6570-6575, 2017. （査読有）
9. S. M. Dibaji, H. Ishii, and R. Tempo, Resilient randomized quantized consensus with delayed information, Proc. 55th IEEE Conference on Decision and Control, pp. 3505-3510, 2016. （査読有）
10. A. Cetinkaya, H. Ishii, and T. Hayakawa, Enhanced stability analysis for networked control systems under random and malicious packet losses, Proc. 55th IEEE Conference on Decision and Control, pp. 2721-2726, 2016. （査読有）
11. S. Zeng, H. Ishii, and F. Allgower, State estimation of interconnected ensembles with anonymized outputs, Proc. 6th IFAC Workshop on Distributed Estimation and Control in Networked Systems (NecSys'16), pp. 109-114, 2016. （査読有）
12. A. Cetinkaya, H. Ishii, and T. Hayakawa, Random and malicious packet transmission failures on multi-hop channels in networked control systems, Proc. 6th IFAC Workshop on Distributed Estimation and Control in Networked Systems (NecSys'16), pp. 49-54, 2016. （査読有）
13. S. Akashi, H. Ishii, and A. Cetinkaya, Self-triggered control for communication reduction in networked systems, Proc. 6th IFAC Workshop on Distributed Estimation and Control in Networked Systems (NecSys'16) pp. 280-285, 2016. （査読有）
14. Y. Kikuya and H. Ishii, A fault tolerant protocol for clock synchronization in sensor networks, Proc. 6th IFAC Workshop on Distributed Estimation and Control in Networked Systems (NecSys'16), pp. 181-186, 2016. （査読有）
15. S. M. Dibaji, H. Ishii, and R. Tempo, Resilient randomized quantized consensus, Proc. American Control Conference, pp. 5118-5123, 2016. （査読有）
16. J. M. Maestre and H. Ishii, A cooperative game theory approach to the PageRank problem, Proc. American Control Conference, pp. 3820-3825, 2016. （査読有）
17. S. M. Dibaji and H. Ishii, Resilient consensus of double-integrator multi-agent networks with communication delays, Proc. 54th IEEE Conference on Decision and Control, pp. 4290-4295, 2015. （査読有）
18. S. Zeng, H. Ishii, and F. Allgower, Sampled observability of discrete heterogeneous ensembles from anonymized output measurements, Proc. 54th IEEE Conference on Decision and

Control, pp. 5683-5688, 2015. （査読有）
19. S. M. Dibaji and H. Ishii, Resilient multi-agent consensus with asynchrony and delayed information, Proc. 5th IFAC Workshop on Distributed Estimation and Control in Networked Systems (NecSys'15), pp. 28-33, 2015. （査読有）
20. A. Cetinkaya, H. Ishii, and T. Hayakawa, Event-triggered output feedback control resilient against jamming attacks and random packet losses, Proc. 5th IFAC Workshop on Distributed Estimation and Control in Networked Systems (NecSys'15), pp. 270-275, 2015. （査読有）
21. S. Fuady and H. Ishii, Alignment forming in source seeking for multi-agent systems, Proc. 1st Int. Symposium on Swarm Behavior and Bio-Inspired Robotics (SWARM'15), pp. 162-165, 2015. （査読有）
22. 淺間一，石井秀明，原辰次，「わ」のコンセプトに基づく新しいシステム理論構築に向けて，計測自動制御学会「計測と制御」，57: 69-72, 2018. （査読無）
23. 石井秀明，サイバーセキュアシティを支えるシステム，計測自動制御学会「計測と制御」，57: 101-105, 2018. （査読無）
24. 石井秀明，マルチエージェント合意問題におけるセキュリティ対策，計測自動制御学会「計測と制御」，55: 936-941, 2016. （査読無）

〔学会発表〕(計 21 件)
1. H. Ishii, Tradeoffs in networked control systems: An information theoretic approach, Mini-Workshop on Entropy, Information and Control (Mathematisches Forschungsinstitut Oberwolfach, Germany)(招待講演),2018 年 3 月
2. 鈴木敦之，石井秀明，新たな PageRank 分散アルゴリズム：指数収束性と性能検証，第 5 回計測自動制御学会制御部門マルチシンポジウム(東京都市大学，東京)，2018 年 3 月
3. 岡本貴之，石井秀明，ネットワーク化制御系に対する攻撃検知システムの最適設計，第 5 回計測自動制御学会制御部門マルチシンポジウム(東京都市大学，東京)，2018 年 3 月
4. A. Cetinkaya, H. Ishii, and T. Hayakawa, Wireless networked control systems subject to jamming and disturbance, SICE Int. Symposium on Control Systems (東京都市大学，東京)，2018 年 3 月
5. Hideaki Ishii, Resilience against malicious agents in quantized consensus, Seminar at CNR-IEIIT and Politecnico di Torino (Torino, Italy)（招待講演），2017 年 11 月
6. Hideaki Ishii, Fault tolerant clock synchronization in wireless sensor networks, Seminar at Otto-von-Guericke-Universitaet Magdeburg (Magdeburg, Germany)（招待講演），2017 年 11 月
7. 石井秀明，サイバーセキュアシティを支えるシステム，第 60 回自動制御連合講演会(電気通信大学，調布市)（招待講演），2017 年 11 月
8. 中村将大，石井秀明，最大値に基づくレジリエント合意アルゴリズム，第 60 回自動制御連合講演会(電気通信大学，調布市)，2017 年 11 月
9. S. M. Dibaji, H. Ishii, R. Tempo, Resilient randomized quantized consensus, 2nd Symposium on the COntrol of NEtwork Systems (Boston USA)，2017 年 10 月
10. 瀧尻和哉，石井秀明，不確かなネットワーク化制御系における通信制約の限界導出，第 4 回 制御部門マルチシンポジウム，計測自動制御学会，岡山大学（岡山市），2017 年 03 月
11. 鈴木惇之，石井秀明，小野功，動的システムと制御通信の連成シミュレータ構築： Simulink による連携，第 4 回 制御部門マルチシンポジウム，計測自動制御学会，岡山大学（岡山市），2017 年 03 月
12. S. Fang, J. Chen, and H. Ishii, Power gain bounds of networked feedback systems: An information-theoretic approach, SICE Int. Symposium on Control Systems, 岡山大学（岡山市），2017 年 03 月
13. A. Cetinkaya, H. Ishii, and T. Hayakawa, Wireless networked control resilient against jamming attacks with bounded average power, SICE Int.n Symposium on Control Systems, 岡山大学（岡山市），2017 年 03 月
14. Hideaki Ishii, Resilience against Malicious Agents in Quantized Consensus Half a Century of Progress in Teams, Games and Control: A workshop dedicated to Tamer Basar's 70th birthday, IEEE Conf. on Decision and Control（招待講演），Las Vegas, USA, 2016 年 12 月
15. 石井秀明，マルチエージェントシステムの制御：総論，SICE セミナー「マルチエージェントシステムの制御 ― IoT 時代の制御理論」（招待講演），北陸先端大東京サテライト，2016 年 09 月
16. 瀧尻和哉，石井秀明，不確かなネットワ

ーク化制御系における通信制約の限界導出，第 60 回システム制御情報学会研究発表講演会(SCI'16)，京都テルサ（京都市），2016 年 05 月

17. Hideaki Ishii, Cyber security and attack detections for power systems, Seminar at the Systems and Automation Department（招待講演）, University of Seville, Spain, 2016 年 03 月
18. 石井秀明,「マルチエージェントシステムの制御」概論，SICE 第 3 回制御部門マルチシンポジウム，ワークショップ：マルチエージェントシステムの制御―IoT/CPS 時代の制御理論（招待講演），南山大学（名古屋市），2016 年 03 月
19. S. M. Dibaji, H. Ishii, and R. Tempo, Quantized randomized consensus over networks with adversaries, SICE Int. Symposium on Control Systems, 南山大学（名古屋市），2016 年 03 月
20. 石井秀明，マルチエージェントシステムの制御（1）総論，第 58 回自動制御連合講演会，ＯＳチュートリアル（招待講演），神戸大学（神戸市），2015 年 11 月
21. Hideaki Ishii, Resilient consensus of multi-agent networks in the presence of malicious attacks, Seminar at the Department of Electronic Engineering（招待講演），City University of Hong Kong, Hong Kong, China, 2015 年 10 月

〔図書〕（計 1 件）

1. S. Fang, J. Chen, and H. Ishii, Towards Integrating Control and Information Theories: From Information-Theoretic Measures to Control Performance Limitations, Springer, Berlin, 2017.（ページ数： XII, 190）

〔その他〕

・ホームページ
http://www.sc.dis.titech.ac.jp/ishii/

・受賞
手島精一記念研究賞（若手研究賞），東京工業大学，2017

・国際ワークショップ開催
7th IFAC Workshop on Distributed Estimation and Control in Networked Systems (NecSys'16)，東京国際交流館プラザ平成（東京・お台場），2016 年 09 月 08 日～2016 年 09 月 09 日

６．研究組織

(1)研究代表者

石井 秀明 （Ishii Hideaki）
東京工業大学・情報理工学院・准教授
研究者番号：50376612