

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 13 日現在

機関番号：13701

研究種目：若手研究(B)

研究期間：2015～2017

課題番号：15K18092

研究課題名（和文）量子化制御理論に基づく暗号化通信制御

研究課題名（英文）Encrypted communication control based on quantized control theory

研究代表者

森田 亮介（Morita, Ryosuke）

岐阜大学・工学部・助教

研究者番号：00713801

交付決定額（研究期間全体）：（直接経費） 3,100,000 円

研究成果の概要（和文）：ディザリングとは、高解像な信号を低解像に変換する「量子化」を行なう際、ディザ信号と呼ばれる確率的な信号を用いて、量子化の影響を少なくする方法である。その方法の一つである、subtractive dither法をフィードバック制御系に用いたときの制御性能を、定量的に明らかにした。また、複数のサブシステムがネットワークを構成するマルチエージェントシステムにおいて、前述の結果を踏まえ、システムに異常が含まれている場合の検出方法について検討した。さらに、複数の車両ロボットを用いた実験を行ない、低スペックのセンサーを用いた空間認識と安価なモーターでの駆動によるフォーメーション制御を実現した。

研究成果の概要（英文）：Dithering is the method that decrease the performance degradation of the system when the high-resolution signals are transformed into the low-resolution signals. Subtractive dither is the one of the method and we have quantitatively clarified the control performance of feedback systems with subtractive dither. We have applied this result to multi-agent systems, which are composed of multiple subsystems, and presented how to detect malicious agents in the system. In addition, we have experimented with vehicle robots and achieved formation control with low-spec sensors and cheap motors.

研究分野：システム制御理論

キーワード：量子化制御 ディザリング 暗号化通信

1. 研究開始当初の背景

多くの制御理論は、制御系に含まれる信号は連続的であると見なせるほど、十分な解像度を有していることが前提となっている。しかし、実際には、アクチュエータの性能限界や、通信容量の制約などから、十分な解像度を確保することが難しいことがある。この場合、連続的な信号を前提としている制御理論では、意図した制御性能を得られないことがほとんどである。このため、離散的な信号を用いた制御系設計が必要となる。この方法の一つとして、制御系に「量子化器」と呼ばれる構造を取り入れ、連続的、すなわち高解像度の信号を低解像で離散的な解像度の信号に変換し、かつ、制御性能の劣化が起らないような変換を施すための方法が考案されている。

量子化の方法の一つであるディザリングは、画像・音声処理の分野では既に広く行なわれている。例えば紙幣などの印刷などでは、偽造防止技術として使われている。これを制御工学の観点で考えると、人間の目が制御対象に相当する。人間がその印刷を見ると、設計者が意図した画像が見えるが、コピー機などの異なる「制御対象」を通すと、元々の画像が再現されない。すなわち、人間の目にしか認識できないある種の暗号化ととらえることができる。逆にコピー機などを介すと、複写したことを表す文字が浮かび上がるが、人間の目ではじめからそれを確認することが難しい印刷もある。

このような技術はある特定の制御対象のみ、またはそれ以外においてのみ特徴的な出力が得られることから、本研究では制御理論の分野において研究されてきた量子化制御技術と、ディザリングを応用した暗号化を複合し、量子化制御理論に基づく暗号化通信制御を実現するための研究を行なう。

2. 研究の目的

本研究では、ディザリング技術を元にした量子化入力制御、すなわち、低解像な信号を用いて高解像な信号を用いた場合と同等の制御性能を実現するための理論を確立する。また、量子化制御の「入力される情報量が減少してもほぼ同じ出力が得られる」という点を応用し、情報の秘匿・暗号化を実現する。研究の最終的な目標として、ネットワーク通信を介した制御において、セキュリティの高いシステムの実現を目指す。

3. 研究の方法

本研究では、ディザリング技術に基づく量子化制御理論の確立と、量子化制御を応用した通信の暗号化を目的とする。この目的の達成のため、

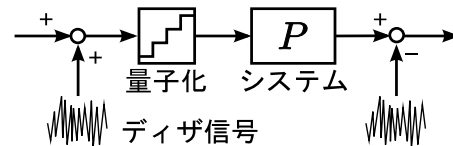
- (1) これまで研究を進めてきたランダムディザ量子化器を発展させた、システムのモデル情報に基づく、より強い制御性能の保証を与える量子化器を導出
- (2) 上記で確立したディザリング技術に基づ

く量子化制御理論と既存の暗号化手法と融合させた、セキュリティの高い暗号化通信制御の実現について研究を進めた。

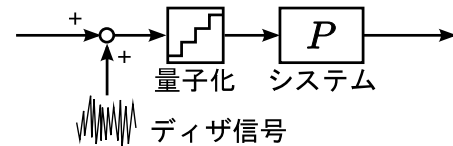
4. 研究成果

(1) フィードバック制御系における Subtractive dither の性能評価

信号の量子化の方法の一つとして、ディザリングと呼ばれる方法がある。その方法の一つである、Subtractive dither 法は、信号が量子化される前後において、ディザ信号と呼ばれる確率的信号をそれぞれ加算・減算する方法である（図 1(a)）。これに対し、量子化の前で加算するだけの、一般的なディザリングとして広く用いられている方法（図 1(b)）は、これと区別して Non-subtractive dither と呼ばれることがある。本研究では、フィードバック制御システムにおいて、subtractive dither を用いたときの制御性能を、ディザリングを行わない場合を基準とした評価指標によって、定量的に明らかにした。



(a) Subtractive dither



(b) Non-Subtractive dither

図1 ディザリングの手法

評価の方法は、ディザリングを行なう場合の出力を z_Q 、ディザリングを行わない場合の出力を z_I とし、双方のシステムに対して同じ初期値、同じ入力を与えた場合の出力の差の期待値の最悪値

$$J = \sup \mathbb{E} [(z_Q - z_I)^2]$$

を評価関数とした。subtractive dither を用いた場合、量子化の前後で用いられるディザ信号が一致している場合には、時刻 k でのシステムのインパルス応答行列 G_k 、量子化間隔 d を用いて $J \leq d^2/12 \cdot \sum_{j=0}^{\infty} G_k$ となることが得られた。一方、量子化の前後で用いるディザ信号が一致しない場合は $J \leq d^2/3 \cdot \sum_{j=0}^{\infty} G_k$ であり、ディザリングを行わないシステムを基準として、制御性能が4倍悪くなるという結果が得られた。数値シミュレーションの一例として、あるフィードバック制御システムに対し、subtractive dither 法を用いたとき、量子化の前後で同じデ

ィザ信号を用いた場合と異なるディザ信号を用いた場合のシステムの出力を比較したものが図2である。図中の赤線が前者、青線が後者である。なお、黒線は、評価の基準となる、ディザリングを行なわなかった場合の出力である。本シミュレーションの結果からディザ信号の一致・不一致が、システムの出力へ大きく影響を与えることが分かった。特に、量子化の前後において、ディザ信号が一致するときのみ高い制御性能が得られることが明らかとなった。

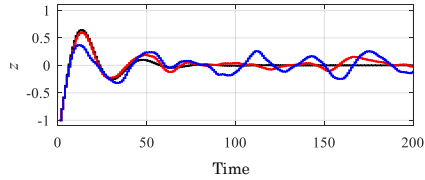


図2 subtractive ditherを用いた場合のシステムの出力

本研究におけるディザ信号を、暗号鍵に置き換えて考えれば、将来的な暗号化通信制御のための基礎理論となることが期待できる。

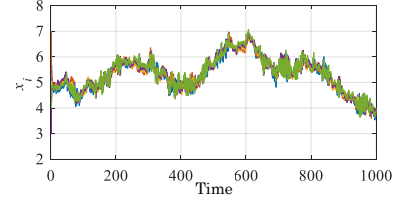
以上の内容は、「主な発表論文等」の雑誌論文②、学会発表⑥⑧⑨にて発表を行なっている。

(2) マルチエージェントシステムの合意制御における異常なエージェントの検出

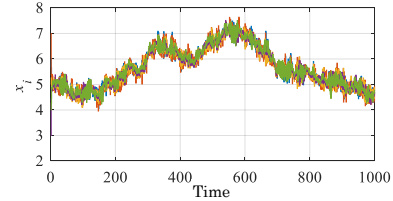
マルチエージェントシステムとは、複数の「エージェント」と呼ばれるサブシステムがネットワークをなし、システム全体で共通のタスクを実現するシステムである。そのなかでも、エージェントの状態変数を一致させる合意制御は、マルチエージェントシステムを考えるうえで基本的な問題の一つであるが、本研究では、前項の subtractive dither を利用し、合意制御において、異常検出を行なう方法について検討した。

合意制御では、エージェント間の情報交換が重要となるが、情報交換を行なう双方のエージェントに同一のディザ信号用いられるときのみ、量子化による制御性能の影響を受けにくい。しかし、何らかの異常により、ディザ信号が一致しないとき、もしくはシステムで用いられるディザ信号を知らない第三者により、ダミーのエージェントが設置された場合、制御性能が大きく低下することが、数値実験的に明らかとなった。図3は、システムが図4のようなネットワーク構造を持つときの、5つのエージェントの出力を表したものであり、(a)はすべてのエージェントに同一のディザ信号を与えたもの、(b)はエージェント2のみ異なるディザ信号を与えたものである。(a)では、すべてのエージェントの状態変数がおおよそ一致しているのに対し、(b)では、エー

ジェント2の出力を示す赤い線がスパイク状に表れており、断続的に他のエージェントとは異なる振る舞いとなっており、合意制御が達成できていないことが確認できる。



(a) 全てのエージェントに同一のディザ信号を与えたときの出力



(b) 異なるディザ信号を持つエージェントが含まれる場合の出力

図3 マルチエージェントシステムに対して subtractive dither を用いた場合のシステムの出力

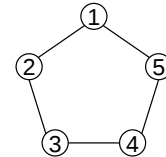


図4 システムのネットワーク構造

さらにこの結果を発展させ、その制御性能を定量的に評価できる基準を明確化し、システムに異常があるかどうかを判定できるようにした。全てのエージェントの状態変数の平均値と、エージェントの実際の状態変数の値との差を δ とすると、これがエージェントの散らばり具合を評価する指標となる。しかし、 δ の値をあらかじめ予測することは難しいため、「ディザリングを用いない場合に予想される、平均値と実際の値との差」を δ' とし、評価関数を、その差の2ノルムの期待値、すなわち、 $J = \mathbb{E}[\|\delta - \delta'\|_2^2]$ とすることで、あらかじめ見積もることを可能にした。なお、ディザリングを用いない合意制御では、十分な時間が経過した場合には状態変数の値は、エージェント間で完全に一致し、 $\delta' = 0$ となるので、この評価関数で、システムの妥当な評価ができる。

図5において、青線は、評価関数に基づいて見積もられた期待値の概算値を示しており、黄線と赤線は、それぞれ異常なエージェントを含んだシステム、全て正常なエージェントで構成されるシステムについて、シミュレーションを行なった結果から、その散らばり具合を評価関数に準じて、求めたものである。全てのエージェントが正常なシステムでは、あらかじめ見積もった値に近づいている

のに対し、異常なエージェントを含んだシステムでは、その差が大きくなっていることから、システムの異常判定が可能であると考えられる。

現状の結果では、異常判定が可能な概

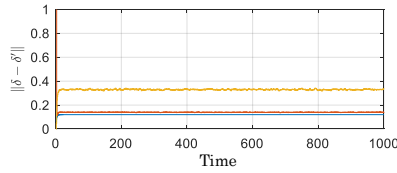


図5 合意制御における異常検出の指標

算値までは求められているものの、正確な値、すなわち、システムに異常がない場合に期待できる制御性能を示す評価値までは得られてはいない。また、システムに異常なエージェントが含まれているかどうかの判定は可能ではあるが、どのエージェントが異常かまでは特定できないに至っていない。そのため、期間終了後も引き続き研究を継続する予定である。

以上の内容は、「主な発表論文等」の学会発表②④⑤にて発表を行なっている。

(3) 低ビット通信による合意制御の制御性能とネットワーク構造の関係の解明

マルチエージェントシステムでは、エージェント間の情報交換があるため、システムが大きくなるほど通信量が飛躍的に増大する。本研究では、ディザリングなどの高度な量子化手法を用いないで低ビット通信による合意制御アルゴリズムを構築し、その制御性能と、システムのネットワーク構造との関係を解明した。

本研究で用いたアルゴリズムは、エージェント i がエージェント j と情報交換をするとき、エージェントの状態変数をそれぞれ x_i, x_j とすると、時刻 $k+1$ の状態変数を

$$x_i(k+1) = x_i(k) + \sum_j u_{ij}(k)$$

のように更新する。ここで入力 $u_{ij}(k)$ は

$$u_{ij}(k) = \begin{cases} b & \text{if } x_j(k) - x_i(k) > a \\ -b & \text{if } x_j(k) - x_i(k) < -a \\ 0 & \text{otherwise} \end{cases}$$

と定める。すなわちエージェント i と j の差が、しきい値 a 以上であれば状態変数を更新幅 b だけ更新し、そうでなければ更新しない。これにより、入力は3ビットしか用いないでよい。本研究では、このアルゴリズムを用いたときのシステムの定常状態の最悪値を求め、その結果、十分に時間が経過しても、エージェントの状態変数がばらついたままである場合に、エージェント間の状態変数の最大の差が $2(b(n-1) - (a+b))$ となることを示した。また、そのような最悪値となりうるネットワーク構造の一つとして、図6のような、スター型構造を二つ重ねたものがあることを示した。

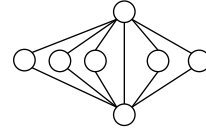


図6 エージェントの状態変数がばらついたままになってしまう場合のネットワーク構造の例

本研究の結果によって、所望の制御性能を得るためのネットワーク構築の指針となることや、暗号化通信制御のための通信帯域・計算リソースの確保へとつながることを期待している。

以上の内容は「主な発表論文等」の学会発表①③にて発表を行なっている。

(4) 簡易的な車両ロボットを用いたフォーメーション制御実験

本研究では、近年 IoT デバイスとして注目されている arduino をベースとした車両ロボットを製作し、フォーメーション制御の実験を行なった。製作したロボット(図7)には、低スペックの距離センサーと安価なモーターを搭載し、限られたリソースで実際にフォーメーション制御が可能かどうかの検証を行なった。図8はモーションキャプチャにより計測した実験の様子を示している。初期状態(a)では青・黄・橙・赤の4台のロボットがばらばらに配置されているが、時間経過とともに、(b)のように、あらかじめ設定しておいた正方形のフォーメーションを形成できていることがわかる。

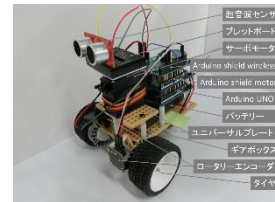
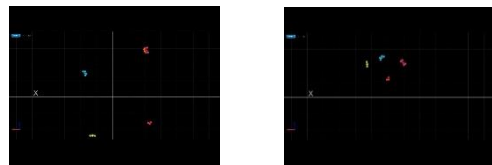


図7 製作した車両ロボット



(a) 初期状態 (b) 最終状態

図8 フォーメーション実験の結果

本ロボットの製作中に、センサーを一つしか搭載できず、一定の方向しか空間の認識ができないなど、想定以上に低性能なものになってしまうことが分かったが、それでも所望の制御が可能であった。

本研究では基本的な制御実験しか実施できていないが、同様のデバイスを用いてさらなる実験を実施できる見通しが得られたといえる。

以上の内容は「主な発表論文等」の学会発表⑦にて発表を行なっている。

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2件)

- ① Ryosuke Morita, Shun-ichi Azuma, and Toshiharu Sugie, “Optimal Random Dither Quantizers for Positive Systems,” Asian Journal of Control. (印刷中) DOI: 10.1002/asjc.1744
- ② 森田亮介, 「Subtractive Dither を用いた量子化器のフィードバック制御系における効果」, システム制御情報学会論文誌, Vol. 29, No. 5, pp. 225–230, 2016. DOI: 10.5687/iscie.29.225

〔学会発表〕(計9件)

- ① Ryosuke Morita and Satoshi Ito, “Weak Consensus with Discrete-Valued Input and the Performance Dependency on Its Network Topology,” The 23rd International Symposium on Mathematical Theory of Networks and Systems, 2018. (発表予定)
- ② 堀江風哉, 森田亮介, 伊藤聡, 「ランダムディザを用いた合意問題における異常エージェントの検出」, 第62回システム制御情報学会研究発表講演会, 114-4, 2018.
- ③ 森田亮介, 伊藤聡, 「多数決型コンセンサスアルゴリズムとネットワーク構造の関係」, 第5回計測自動制御学会制御部門マルチシンポジウム, Sa52-4, 2018.
- ④ 森田亮介, 「Subtractive dither を使った合意制御に関する考察」, 第59回自動制御連合講演会, pp. 235–236, 2016.
- ⑤ Ryosuke Morita, “Multi-Agent Consensus by Quantized Communication with Subtractive Dither,” 22nd International Symposium on Mathematical Theory of Networks and Systems, pp. 385–387, 2016.
- ⑥ Ryosuke Morita, “Performance Analysis of Feedback Control Systems with Subtractive Dither,” 2016 American Control Conference, pp. 5112–5117, 2016. DOI: 10.1109/ACC.2016.7526164
- ⑦ 辻村光, 森田亮介, 渡辺昌宏, 「超音波センサーを搭載したマルチロボットのフォーメーション制御」, 第3回計測自動制御学会制御部門マルチシンポジウム, PS-35, 2016.3
- ⑧ 森田亮介, 「Subtractive Dither を用いたフィードバック系の制御性能」第58回自動制御連合講演会, 1D2-3, 2015.
- ⑨ 森田亮介, 「Subtractive Dither を用いた量子化器のフィードバック制御系における暗号化通信への有用性について」, 第59回システム制御情報学会研究発表講演会, 344-2, 2015.

6. 研究組織

(1) 研究代表者

森田 亮介 (MORITA Ryosuke)
岐阜大学・工学部・助教
研究者番号：00713801