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

令和　２ 年　 ６ 月　 ３ 日現在

機関番号：１４４０１
研究種目：若手研究
研究期間：2018～2019
課題番号：１８Ｋ１８０４０

研究課題名（和文）ヒトの脳の意思決定の仕組みに着想を得た攻撃傾向変化に適応的な異常検知の枠組み確立

研究課題名（英文）Anomaly detection adaptable to attack changes based on decision making of human brain

研究代表者
久世　尚美（Kuze, Naomi）

大阪大学・基礎工学研究科・助教

研究者番号：２０７７８０７１

交付決定額（研究期間全体）：（直接経費）　　1,900,000円

研究成果の概要（和文）：申請者は、ネットワークの大規模化、多様化に伴う、サイバー攻撃の多様化への対策のため、脳の意思決定、学習の仕組みの応用について研究を実施した。
申請者は、ヒトのグループにおける集団的行動選択においてみられるflexible leadershipの概念を無線センサネットワークにおけるチャネル選択手法に適用し、不確実な情報化で適切なチャネル選択が可能であることを示した。また、移動ロボットを対象として、QoSに基づいた強化学習を利用した無線通信を妨害するジャミング攻撃にロバストな移動制御手法を提案し、ジャミングを回避するよう移動方策の学習が可能であることを示した。

研究成果の学術的意義や社会的意義
申請者は、ネットワークの大規模化、多様化に伴う、サイバー攻撃の多様化への対策のため、脳の意思決定、学習の仕組みの応用について研究を実施した。
申請者は、ヒトのグループにおける集団的行動選択においてみられるflexible leadershipの概念を無線センサネットワークにおけるチャネル選択手法に適用し、不確実な情報化で適切なチャネル選択が可能であることを示した。また、移動ロボットを対象として、QoSに基づいた強化学習を利用した無線通信を妨害するジャミング攻撃にロバストな移動制御手法を提案し、ジャミングを回避するよう移動方策の学習が可能であることを示した。

研究成果の概要（英文）：Because of the rapid diversification of cyber attacks, it is important to consider novel approaches, which have high adaptability to attack changes, based on decision making and learning of brains.
First, we introduced collective decision making in animal groups to self-organizing systems. In detail, we adapted the concept of flexible leadership to channel selection in wireless sensor networks, and demonstrated that with the proposed mechanism, appropriate channels could be selected according to environmental changes. Next, we focused on a mobile robot with wireless communication, proposed QoS-based anti-jamming mobile control mechanism based on reinforcement learning. We revealed that with the proposed mechanism, the agent could learn mobile scheme that avoid jamming attacks.

研究分野：ネットワークセキュリティ

キーワード：セキュリティ　集団的行動選択　強化学習　移動制御　アンチジャミング

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

インターネットはデバイス技術、通信技術の発展により急速に浸透し、重要な社会基盤となっている。通信機器の増加、多様化に伴って、Web を介したサービスが数多く提供されるようになり、その形態も進化、多様化している。その一方で、Web サービスのぜい弱性などを利用したサービスを提供あるいは享受する個人や法人、政府などを対象とするサイバー攻撃が急激に増加し、サービスの妨害や個人情報・機密情報の漏洩、金銭の詐取などの被害が世界の各地、広範囲で起こっており、社会的に大きな問題となっている。また、Web サービスの浸透とともに正規な通信も含めたトラヒックが急激に増大していながら、サイバー攻撃への対策は未だ技術者、研究者の知識や経験に基づく手動解析による部分が大きく、サイバー攻撃の早期発見・対策およびその自動化が必須課題である。

しかしながら、Web サービスの形態の多様化とともに、サイバー攻撃も多様化・複雑化してきており、すべてのサービスやエンドユーザアプリケーションのぜい弱性を特定し、サイバー攻撃を防ぐことは困難になっている。そのため、もとより攻撃傾向が変化することを前提とし、サイバー攻撃の検知、対策システムそのものが自身を更新し（self-modeling、self-evaluation）[Fleming2017]、変化に適応していくことが重要な課題であり、本研究はその課題の解決を目的としたものである。

[Fleming17] Fleming, S. M and Daw, N. D., “Self-evaluation of decision making: a general Bayesian framework for metacognitive computation,” Psychological Review, vol. 124, no. 1, pp. 91-114, Jan. 2017.

２．研究の目的

本研究は、サイバー攻撃を早期に発見、また攻撃への対策を行うための攻撃情報の収集のために重要な攻撃の検知技術に着目し、サイバー攻撃の形態や傾向の変化に適応的な攻撃検知の枠組みの確立を目的とする。

申請者は、多様かつ多量なデータの扱いに長けた群知能の仕組みなどを応用して通信の傾向の学習を行い、多様な通信から、攻撃の準備動作であるぜい弱性スキャンを高い精度で識別することが可能であることを示した[4,5]。しかし、常に変化し続けるネットワーク環境においてサイバー攻撃に対して早期対処を行うためには、攻撃の傾向の変化への適応性を内包、つまり傾向の変化に合わせて検知モデル自身を逐次的に学習、更新する機構が必要となる。そこで、本研究課題においては、過去の知覚情報およびその蓄積から学習（知識の抽出）を行うとともに、リアルタイムで得られる情報から逐次的に学習を行い、状況に応じて柔軟な意思決定を行うヒトの脳の認知・意思決定の仕組みをサイバー攻撃の検知へと応用する。このような脳の意思決定における特性に関して、近年、ベイジアンネットワークとの高い類似性が指摘される。申請者は、このような脳の意思決定の仕組みをサイバー攻撃の検知へと応用し、攻撃の傾向の変化に適応的な攻撃検知の枠組みを確立する。

３．研究の方法

（１） Effective leadership model の導入

自己組織化制御における、各ノードの観測可能な情報が不確実な環境下でのネットワーク全体としての適切な制御の実現のため、生物の群れにおける集団的な行動選択の仕組みを応用する。生物の群れにおいては、各個体の知覚可能な情報は、その個体の知覚・身体能力の制約や周囲の環境の影響により不確実なものとなる。しかし、群れの中で、個体同士の協調を通して群れ全体として適切な行動の選択を実現している。本研究では、特に、鳥などの群れにおける集団的な行動選択の仕組みをモデル化した Effective leadership model [Couzin05]に着目し、ネットワーク制御へと応用する。

Effective leadership model において、個体は informed individual と non-informed individual の二種類に大別される。Informed individual は、他の個体よりも豊富な知識などの情報を有し、それらの情報に基づいて行動の選択を行う。一方、non-informed individual は周囲の個体に追従して行動を行う。結果として、informed individual が群れのリーダーとしての役割を持ち、他の個体をけん引し、群れ全体を適切な行動選択へと導く。

本研究課題では、無線センサネットワークを対象とした経路制御手法であるポテンシャルルーティングを対象として、Effective leadership model を応用した。ポテンシャルルーティングは自己組織型の経路制御手法であり、各ノードがデータパケットの経路を決定するためのスカラー値“ポテンシャル”を保有しており、各ノードはポテンシャルに基づいてデータパケットの転送を行う。ポテンシャル値の更新、およびポテンシャル値に基づいたデータパケットの転送が局所的に行われるため、ネットワークサイズに対する高い拡張性を有する。申請者は、さらに、[Kuze16]において、コントローラを導入し、制御入力を与えることにより、ポテンシャル値の収束速度が向上することを示した。一方で、故障などの環境変動の影響についての情報をコントローラが取得できない状況では、コントローラからの制御入力は信頼できず、ノード間の協調のみに基づいてポテンシャル値の更新を行うことが望ましい。

そこで、ポテンシャル値の更新規則の選択を題材として、Effective leadership model の仕組みを応用した手法を提案した。ネットワーク内の各ノードを Effective leadership model における individual（個体）とみなす。提案手法では、ノードを、自身の保有する情報に基づいて行動選択を行う傾向の強い leader node と他ノードに追従して行動選択を行う傾向の強い follower node に大別する。結果として、leader node は自身の観測可能な情報に基づいて、環境に応じた適切なポテンシャル値の更新規則を選択する。

[Couzin05] I. D. Couzin, J. Krause, N. R. Franks, and S. A. Levin, “Effective leadership and decision-making in animal groups on the move,” Nature, vol. 433, pp. 513-516, Nov. 2005.

[Kuze16] N. Kuze, D. Kominami, K. Kashima, T. Hashimoto, and M. Murata, "Controlling large-scale self-organized networks with lightweight cost for fast adaptation to changing environments," ACM Transactions on Autonomous and Adaptive Systems, vol. 11, no. 2, pp. 9:1-9:25, June 2016.

（2） Flexible leadership の概念の導入

（1）で提案した手法は、各ノードの持つ情報が動的に変化することについては考慮していなかった。実際のネットワークでは、常に状態が変化し続けており、また外部環境の影響を受けるため、適切な制御を行うために必要な情報を有する、つまりリーダーとして適切なノードは時間的・空間的に変動する。そこで、ヒトのグループにおける集団的な行動選択においてみられる flexible leadership の概念[Kurvers15]をネットワークに応用した。ヒトのグループにおいては、意思決定者は、自身の選択に対する信頼度に基づいて、自身の役割を柔軟（flexible）に変化させる。具体的には、自身の選択に対する信頼度が高い際には自身の情報に基づいて選択を行う傾向が強く、一方で自身の選択に対する信頼度が低い場合には他者の選択に追従する傾向が強くなる。その結果として、自身の選択に対する信頼度が高い意思決定者が他の意思決定者をけん引し、グループ全体として適切な行動選択が達成される。

信頼度に基づいた協調を実現するために、既存研究[Park17]において提案されている信頼度に基づいた individual、social information の統合手法を導入する。Individual information は自身の観測情報に基づく選択を、social information は他の意思決定者から受け取った情報に基づく選択を示す。文献[Park17]の手法においては、individual、social information がそれぞれ正規分布に従うと仮定しており、正規分布の平均がそれぞれの情報に基づいた判断結果あるいは指標、分散がその不確実さ（信頼度の低さ）を示す。そして、各ノードは individual、social information をそれぞれの不誠実さに基づいて統合した結果を最終的な選択とする。

本研究課題では、無線センサネットワークにおけるチャネル選択を題材として、信頼度に基づいた集団的な行動選択の仕組みを応用した手法を提案した。提案手法においては、各ノードが一定間隔で一部のチャネルの状態を観測し、観測状態に基づいてそのチャネルの通信品質の推定、およびその推定結果に対する不確実さ（individual information）を計算する。そして、各ノードは隣接ノードの individual information を収集し、隣接ノードの情報に基づいてチャネルの通信品質の推定とその推定結果に対する不確実さ(social information)の計算を行う。最後に、各ノードは individual information と social information を、それらの不確実さに応じて統合し、得られた結果から最も通信品質が高いと推定されるチャネルを選択する。

[Kurvers15] R. H. J. M. Kurvers, M. Wolf, M. Naguib, and J. Krause, “Self-organized flexible leadership promotes collective intelligence in human groups,” Royal Society Open Science, vol. 2, no. 12, Dec. 2015.

[Park17] S. A. Park, S. Goïame, D. A. O’Connor, and J.-C. Dreher, “Integration of individual and social information for decision-making in groups of different sizes,” PLoS Biology, vol. 15, no. 6, pp. 1-28, Jun. 2017.

（3） アンチジャミング移動制御の導入

本研究課題では、通信機能を有する移動ロボットを対象とし、妨害電波を発することにより無線通信を妨害するジャミング攻撃に耐性のあるシステムの構築について検討を行う。従来のジャミング対策では、スペクトラム拡散技術を利用したものが主流であったが、根本的な解決とはなっていない。一方、移動ロボットからなるシステムにおいては、移動ロボット自身が移動することにより、ジャミング攻撃を回避することで対策を行うことができる。既存研究[Xiao18]においては、強化学習に基づいて、ジャミングを回避するための移動ロボットの移動方策を学習する手法が提案されている。既存研究[Xiao18]においては、信号雑音比（SNR 比）を報酬関数の計算に用いることにより、ジャミング攻撃を回避する移動方策の学習が行われている。しかしながら、実世界でシステム、サービスを運用する際には、ユーザの要求を満たし、アプリケーションレベルでの品質を向上させることが重要となる。そこで、Quality of Service (QoS)を、品質を評価するための指標として採用する。QoS はユーザの観点からシステムの品質を評価するための指標である。QoS を報酬関数の計算に用いることにより、アプリケーションレベルでシステムの品質を向上しつつ、ジャミング攻撃を回避するような移動方策の学習を達成する。

[Xiao18] L. Xiao, et al., “Two-dimensional anti-jamming mobile communication based

on reinforcement learning," IEEE Transactions on Vehicular Technology, vol. 67, no. 10, pp. 9499-9512, October 2018.

（4） フォールバック制御の導入

サイバーフィジカルシステムの発展に伴い、物理システムを対象とした攻撃が増加傾向にある。本研究課題においては、特に false injection 攻撃に着目する。False injection 攻撃は、ネットワークを介してリモートコントローラが物理システムの制御を行うネットワーク化制御を対象とした攻撃であり、物理システムに対して、悪意のある制御入力を与えることにより、不正な操作を行う。False injection 攻撃は、システムの機能停止や、システム自体の破壊につながるため、対策が重要となる。False injection 攻撃に関する従来の研究として、攻撃の検知を行う手法が多く提案されているが、物理システムのセキュリティにおいては、攻撃を検知するだけでなく、システムの可用性を維持することが重要である。

本研究課題においては、false injection 攻撃へロバスト性とシステムの可用性の両立を実現するため、フォールバック制御の導入を行う。フォールバック制御は、異常が検知された際に、機能の一部を制限したり、制御系を切り替えたりすることにより、システムの機能を維持する技術である。既存研究[Sasaki17]において、ボールソーティングシステムを対象としてフォールバック制御が提案されている。本研究課題においては、リモートコントローラが WiFi 通信を介してドローンの制御を行うドローン制御システムを対象として、フォールバック制御を導入することにより、false injection 攻撃へのロバスト性とシステムの可用性の両立を達成する。また、フォールバック制御においては、異常検知の精度も重要となる。本研究課題においては、false injection 攻撃を検知するための動的制約に基づいた異常検知手法の導入を行う。

[Sasaki17] T. Sasaki, K. Sawada, S. Shin, and S. Hosokawa, “Model based fallback control for networked control system via switched Lyapunov function,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. 100, no. 10, pp. 2086-2094, Oct. 2017.

4．研究成果

（1） Effective leadership model のネットワーク制御への応用

ポテンシャル値の更新規則の選択を題材として Effective leadership model を応用した手法を提案し、ネットワークシミュレーションを通して評価を行った。提案手法では、Effective leadership model の仕組みを利用して、局所的な協調を通して、コントローラの信頼度の評価を行い、信頼度が高い場合にはコントローラからの制御入力を考慮してポテンシャル値の更新を行い、信頼度が低い場合にはコントローラからの制御入力を無視して、ノード間の協調のみに基づいてポテンシャル値の更新を行う。

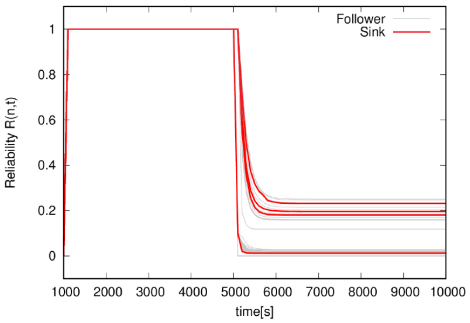

図 1 信頼度の時間変動

本評価では、ネットワーク内でノードの故障が生じ、コントローラがその故障に関する情報を観測できない状況を想定し、各ノードにおける信頼度の変動の評価を行った。故障が生じた際、その隣接ノードが leader node としてコントローラの信頼度を下げる。その他のノードは follower node として隣接ノードの情報に基づいてコントローラの信頼度の計算を行う。

シミュレーション開始から 5,000s 経過後に呼称が生じた場合の、各ノードにおけるコントローラに対する信頼度の変動を図 1 に示す。図より、故障が生じた 5,000s 経過後、コントローラに対する信頼度が低下し、環境に応じたコントローラへの信頼度の評価が適切に行えることを示した。これにより、適切なポテンシャル値の更新規則の選択が可能になると考えられる。

（2） Flexible leadership の概念に基づいたチャネル選択手法

無線センサネットワークを対象としたチャネル選択を題材とし、flexible leadership の概念を応用した手法を提案し、ネットワークシミュレーションを通して評価を行った。図 2 に、ノード間の協調に伴う、適切なチャネルが選択できているノードの数の変動について評価した結果を示す。比較手法として、各ノードにおける individual information の信頼度を考慮しない場合の結果を示す。図より、信頼度を考慮しない場合と比較して、提案手法においては、多くのノードが適切な（品質の高い）チャネルの選択が達成できていることが確認できる。この結果から、情報の信頼度を考慮することにより、より適切な情報を持ったノードが leader node としての役割を持って他のノードをけん引し、ネットワーク全体として、適切なチャネルの選択が実現できていると

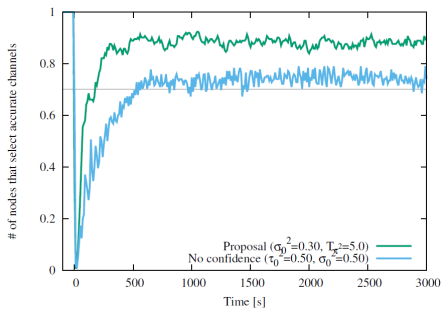

図 2 適切なチャネルを選択するノードの数の変動

考えられる。

（3） QoS を考慮した強化学習に基づいたアンチジャミング移動制御

移動ロボットを対象として、QoS を考慮した強化学習に基づいたアンチジャミング移動制御手法を提案し、シミュレーションを通して評価を行った。提案手法においては、移動ロボットは、はじめホームポイントを出発し、センシングポイントへ移動してデータのセンシングを行い、アクセスポイントへ移動して収集データをサーバへ送信し、ホームポイントへ帰還する、という一連のタスクを行う。通信の成功率を報酬関数の計算を行うことで、QoS を考慮しつつ、ジャミングを回避するような移動方策の学習を行う。

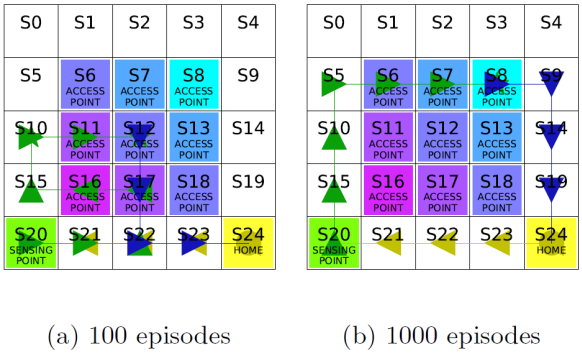

図 3　移動ロボットの経路の例

図 3 に、学習によって得られた経路の例を示す。図において、S24 がホームポイント、S20 がセンシングポイント、S6-8,11-13,16-18 がアクセスポイントを示す。アクセスポイントにおいては、左下ほどジャミング攻撃の影響が大きく、通信の成功率が低くなる。100 エピソードの時点では、ジャミング攻撃の大きいアクセスポイント S12 において通信が行われており、また学習された経路も冗長である。一方で、1,000 エピソードの時点では、ジャミング攻撃の影響が最も小さいアクセスポイント S8 において通信が行われているとともに、経路の冗長さも解消されており、ジャミング攻撃を回避するような移動方策が学習されていることが確認できる。

（4） フォールバック制御に基づいた False injection 攻撃に耐性のあるネットワーク化システム

ドローン制御システムを対象とし、フォールバック制御を導入したシステムを提案した（図 4）。提案システムにおいては、通常時、リモートコントローラがネットワークを介してドローンの制御を行う。一方で、異常発見時には、リモートコントローラの代わりにローカルコントローラがネットワークを介すことなくドローンの制御を行う。また、静的、動的制約に基づく異常検知方式の提案を行い、シミュレーションを通して評価を行った。異常検知方式においては、システムの状態値を観測し、制約を満たさない場合に異常が生じたと判断を行う。静的制約は、高度制限などを考慮して設定している。しかし、システムは、環境の変動に応じて、過渡状態、安定状態をとるため、静的制約だけでは異常検知を適切に行うことが困難である。そこで、システムの過渡、安定状態間の移行を考慮した動的制約を導入している。

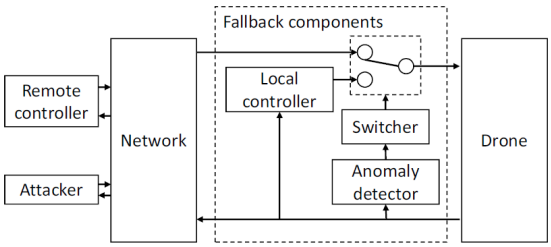

図 4　フォールバック制御に基づいたドローン制御システム

図 5 において、0s の時点で DoS 攻撃が発生した際のある状態値の変動を示す。本評価では、以上が検知された場合、コントローラがローカルコントローラに切り替えられ、安全のため、ドローンが着地状態となるよう制御を行う。図において、緑色の破線は静的制約、赤色の破線は動的制約を示しており、黒色の実践がある状態値の値を示す。DoS 攻撃が発生に伴い、動的制約を満たしていない状態となり、約 8s の時点で状態値が 0 へと収束し、ローカルコントローラにより着地状態へ移行したことが確認できる。以上の結果から、提案したシステム、異常検知手法により、攻撃時に異常を検知し、ローカルコントローラによる制御への移行が達成できることを確認した。

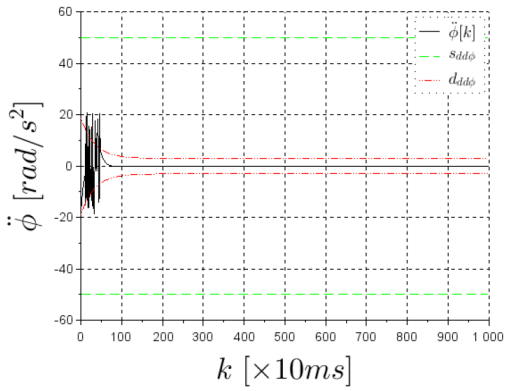

図 5　DoS 攻撃発生時の異常検知

５．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　2件／うち国際共著　0件／うちオープンアクセス　2件）

１．著者名 Naomi Kuze, Daichi Kominami, Kenji Kashimaa, Tomoaki Hashimoto, Masayuki Murata	４．巻 13
２．論文標題 Self-organizing control mechanism based on collective decision-making for information uncertainty	５．発行年 2018年
３．雑誌名 CM Transactions on Autonomous and Adaptive Systems	６．最初と最後の頁 7:1-7:21
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3183340	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Kuze Naomi、Nakashima Taishi、Ushio Toshimitsu	４．巻 8
２．論文標題 Anti-jamming mobile control using QoS-based reinforcement learning	５．発行年 2019年
３．雑誌名 IEICE Communications Express	６．最初と最後の頁 501～506
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/comex.2019GCL0025	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計6件（うち招待講演　0件／うち国際学会　2件）

１．発表者名 Naomi Kuze, Daichi Kominami, Kenji Kashima, Masayuki Murata
２．発表標題 Self-organizing control mechanisms according to information confidence for improving performance
３．学会等名 IEEE Global Communication Conference (GLOBECOM 2018)（国際学会）
４．発表年 2018年

１．発表者名 中嶋 大志, 久世 尚美, 潮 俊光
２．発表標題 強化学習を用いたQoSベースのアンチジャミング移動制御
３．学会等名 IEICE総合大会
４．発表年 2019年

１．発表者名
Sota Takashima, Naomi Kuze, Toshimitsu Ushio

２．発表標題
Hierarchical taxi dispatch system with local coordination among micro-level components: WIP abstract

３．学会等名
The 10th ACM/IEEE International Conference on Cyber-Physical Systems（国際学会）

４．発表年
2019年

１．発表者名
志垣沙衣子，久世尚美，小南大智，加嶋健司，村田正幸

２．発表標題
生物の集団的行動選択に基づく不確実な情報を用いた自己組織型ネットワーク制御手法の一検討

３．学会等名
電子情報通信学会情報ネットワーク研究会

４．発表年
2020年

１．発表者名
高島相太，久世尚美，潮俊光

２．発表標題
需要変動を考慮した非同期型タクシー経路支援システム

３．学会等名
IEICE総合大会

４．発表年
2020年

１．発表者名
Mi Jian，久世 尚美，潮 俊光

２．発表標題
An application of reinforcement learning in anti-jamming mechanism of mobile robot path planning with co-safe temporal logic specifications

３．学会等名
複雑コミュニケーションサイエンス研究会

４．発表年
2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考