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　５ 年　 ６ 月 １６ 日現在

機関番号：３２６１９
研究種目：若手研究
研究期間：2020～2022
課題番号：２０Ｋ１４７７１

研究課題名（和文）Stochastic Control-Theoretic Approach to Development of Simultaneously Cyber-Secure and Energy-Efficient Randomized Transmission Methods for Dependable IoT

研究課題名（英文）Stochastic Control-Theoretic Approach to Development of Simultaneously Cyber-Secure and Energy-Efficient Randomized Transmission Methods for Dependable IoT

研究代表者

ＣＥＴＩＮＫＡＹＡ　ＡＨＭＥＴ（CETINKAYA, AHMET）

芝浦工業大学・工学部・准教授

研究者番号：６０８５１７３０

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：このプロジェクトは、インターネット・オブ・シングス（IoT）のコンテキストにおけるネットワーク制御システムおよびマルチエージェントシステムのためにサイバーセキュアでエネルギー効率の高い制御と通信を開発することを目的としていました。プロジェクトの成果は、ネットワーク上での伝送時間をランダム化することというアイデアに基づいて構築されました。このアイデアは、ジャミングのモデリング、多目的最適化、予測制御、量子化、ゲーム理論の分析と設計、およびIoTテストベッドの開発を組み込むよう拡張されました。

研究成果の学術的意義や社会的意義
Wireless technologies are vital in smart cities and industrial applications for control and sensing data transmissions. Jamming attacks pose a major threat against them. We developed various techniques in networked control and multi-agent systems to counter jamming attacks.

研究成果の概要（英文）：This project aimed to develop secure and efficient techniques for control and communication components in network control systems and multi-agent systems within the context of the Internet of Things (IoT). The results were built upon the idea of randomizing transmission times over networks to achieve security and efficiency. This concept was expanded to incorporate modeling of jamming attacks, multi-objective optimization, predictive control, quantized control, game-theoretic analysis and design, and IoT testbed development.

研究分野：Stochastic control systems

キーワード：Control systems　Network attacks　Multi-agent systems　IoT　Jamming attacks　Control theory　Cyber security　Randomization

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

Nowadays, smart cities integrate the Internet of Things (IoT) into daily life by using wireless communication technologies like Wi-Fi, ZigBee, and Bluetooth Low Energy. These technologies offer many advantages, including easy set-up. However, in a wirelessly connected world, cybersecurity issues, especially jamming attacks, must be addressed carefully. Jamming attackers can block the delivery of crucial information packets by emitting strong interference signals. This poses a significant threat, leading to operational disruption and environmental harm in industrial settings.

Recent studies have explored jamming attacks from the perspective of communication systems. Investigating jamming attacks from the point of view of control theory and designing control and communication methods with security guarantees are also required. The principal investigator has been exploring the effects of jamming attacks in control systems, which presents several challenges.

One challenge is to model the occurrence and effects of jamming attacks in control systems. Typically, jamming attacks on wireless channels can be described using probabilistic models. Depending on the power of the jamming interference signal, the probability of transmission failure can vary. Another challenge involves designing control and communication protocols that provide security against jamming and maintain efficiency for battery powered IoT devices.

２．研究の目的

Considering the challenges mentioned above, the purpose of this project is two-fold.

1) The primary aim of this project is to develop novel control and communication methods that guarantee cybersecurity against jamming attacks in networked control systems, potentially representing the remote-control operation of an industrial plant. To achieve this, we first need to understand the effects of jamming attacks on such systems. In a networked control system, it is expected that an adversary with limited resources may carry out jamming attacks, as emitting jamming interference signals is energy-wise costly. In addition, attacks cause transmission failures on wireless channels probabilistically. Therefore, it is important to develop a model that captures these aspects. Equipped with this model, we plan to create new control and communication techniques and investigate the guarantees they provide.

2) Additionally, this project aims to achieve efficient operation in networked control systems and multi-agent systems, potentially representing IoT systems. This is crucial in IoT systems, as devices typically run on batteries. Although event-based operation is common for achieving energy savings, we will explore optimization-based and game-theoretic ideas to further improve efficiency. Particularly in the optimization-based approach, we intend to predict how a smart attacker may behave, which partially relates to machine learning approaches.

３．研究の方法

To achieve the goals of this project, we follow several theoretical and practical research steps.

1) Security analysis and development of jamming attack models: We develop mathematical models that describe potential actions of a jamming attacker. Such models can take account of a) energy limitations of the attacker and b) probability of transmission failures depending on interference power used by the attacker at different times. Through such models, we address stability analysis of networked control systems and assess stabilizability.

2) Development of randomized transmission methods and game-theoretic approaches to achieve security in multi-agent systems: We propose randomized transmission methods for inter-agent transmissions in multi-agent systems. Furthermore, a game-theoretic approach is followed to understand inter-agent communications.

3) Development of predictive control methods data-quantization methods that are resilient against jamming and denial-of-service attacks: We address both linear and nonlinear control systems. In addition, we consider randomization of transmission times in the context of quantized systems to further improve security. Quantization approaches are necessary to enable data-efficiency.

4) Development of optimization-based, and game-theoretic control techniques: Genetic algorithms provide a method to do multi-objective optimization in the analysis of jamming in control systems. In addition, a multi-objective optimization and game-theoretic approaches can be used to guess potential attack strategies of an intelligent adversary and react accordingly.

5) Development of an IoT testbed and IoT software: We take an IoT development board and develop software to build a basis for testing our proposed communication methods (with randomized transmissions).

4．研究成果

The results of the project are multi-faceted, targeting the theoretical and practical development steps explained above. Major developments and publications are outlined as follows.

1) Development of randomized transmission methods: An analysis of optimal transmission times against potential jamming attacks was conducted. The analysis revealed the scenarios where the randomizing the transmission times is optimal. One way of randomizing transmission times is to divide the time axis into equal segments and choose a random time from each segment. This kind of randomized transmissions was used in a multi-agent system setting to achieve secure consensus among agents. A similar randomized transmission approach was later shown to improve security when systems use quantization.

- A. Cetinkaya, "Randomized Transmissions for Secure Networked Control", Presentation at INFORMS Annual Meeting 2020.
- A. Cetinkaya, H. Ishii, "Randomized Transmission Protocols for Secure Multi-Agent Consensus Under Jamming Attacks", Presentation at Workshop on Learning and Security for Multi-Agent Systems in IEEE Conference on Decision and Control, 2020.
- S. Feng, A. Cetinkaya, H. Ishii, P. Tesi, C. De Persis, "Resilient quantized control under Denial-of-Service: Variable bit rate quantization", Automatica, 2022.

2) Development of jamming attack models and a novel analysis method to investigate jamming attacks on control systems that face disturbance: In the context of networked control systems, a wireless channel model based on Signal-to-Interference-plus-Noise Ratio (SINR) was proposed. In this model, the likelihood of transmission failures at each time is influenced by the potentially time-dependent interference signal emitted by a jamming attacker. This model is probabilistic, and the overall system requires tail-probability techniques for analysis. A similar model was later used for investigating jamming attacks on wireless networked control systems with exogenous disturbances. The control input packets in such a system are assumed to be transmitted over an insecure wireless communication channel vulnerable to jamming attacks. It was demonstrated that stability can be compromised by jamming attacks in systems with disturbances, even if the system is stable without disturbances. However, it was also shown that stability can be achieved under specific restrictions related to the average jamming interference power.

- A. Cetinkaya, H. Ishii, T. Hayakawa, "Secure Networked Control Under Jamming

Attacks: An SINR-Based Approach", Chapter 3 in Security and Resilience of Control Systems, Springer, 2022.
- A. Cetinkaya, H. Ishii, T. Hayakawa, "Effects of Jamming Attacks on Wireless Networked Control Systems Under Disturbance", IEEE Transactions on Automatic Control, 2023.

3) Analysis of stabilizability of stochastic systems under constrained control: Constrained control of continuous-time linear stochastic systems was investigated with a problem structure that is motivated by the networked control problem with transmission failures. It was shown that constrained control can be impossible, if there are many transmission failures on average. The analysis technique expands those in existing stochastic control literature. This impossibility result is expected to be useful to characterize tolerable levels of jamming-related transmission failures in networks.
- A. Cetinkaya, M. Kishida, "Instabilizability Conditions for Continuous-Time Stochastic Systems Under Control Input Constraints", IEEE Control Systems Letters, 2022.

4) Development of linearized control and quantized communication methods: Both the stability and the security properties of nonlinear systems with linearization-based controllers were investigated. This investigation was later extended to include systems that involve quantization. For systems that incorporate data-quantization, bitrates of transmission were explicitly analyzed.
- R. Kato, A. Cetinkaya, H. Ishii, "DoS-Aware Quantized Control of Nonlinear Systems via Linearization", Proc. IFAC World Congress, 2020.
- R. Kato, A. Cetinkaya, H. Ishii, "Security Analysis of Linearization for Nonlinear Networked Control Systems Under DoS", IEEE Transactions on Control of Network Systems, 2021.
- S. Feng, A. Cetinkaya, H. Ishii, P. Tesi, C. De Persis, "Networked Control Under DoS Attacks: Tradeoffs Between Resilience and Data Rate", IEEE Transactions on Automatic Control, 2021.
- R. Kato, A. Cetinkaya, H. Ishii, "Linearization-Based Quantized Stabilization of Nonlinear Systems Under DoS Attacks", IEEE Transactions on Automatic Control, 2022.

5) Development of model predictive control techniques to counteract jamming attacks: The technique of solving linear matrix inequalities was expanded to target optimal control problems for networked control systems that face transmission failures. In addition, a tree-based multi-scenario approach was developed to achieve so-called "model predictive control" of networked systems under potentially malicious packet losses. Multi-scenario approach allows considering all possible situations regarding successful or failed transmissions of control commands.
- T. Arauz, J. M. Maestre, A. Cetinkaya, E. F. Camacho, Proc. European Control Conference, 2021.
- T. Arauz, J. M. Maestre, A. Cetinkaya, C. Stoica Maniu, Proc. IFAC Workshop on Control Applications of Optimization, 2022.

6) Development of multi-objective search-based approach to achieve secure and efficient control and data transmission methods: State-dependent attack and defense mechanisms in a wireless networked control system was investigated. In this system, the controller's transmission of control commands to a remote plant via a wireless channel is subject to jamming attacks. The attacker was assumed to have general access to state information of the system. In this setting, stability of the networked control system is shown to be achievable under certain interference power level conditions. Due to the complex wireless channel model, a multi-objective search-based approach using genetic algorithms is proposed for identifying dangerous attacks and effective defense policies, with the controller regulating transmission signal power based on the plant's state information. This regulation achieves not only security but also efficiency in the sense that control commands do not need to be transmitted with highest possible signal power levels. Via genetic algorithms, the search-based approach can be a useful

method of predicting what jamming attackers may do. The development of multi-objective approach had practical consequences. The software for the simulation was later used in evaluating other approaches through benchmark studies.

- A. Cetinkaya, P. Arcaini, H. Ishii, T. Hayakawa, "A Search-Based Approach to Identifying Jamming Attacks and Defense Policies in Wireless Networked Control", Proc. IEEE Conference on Decision and Control, 2020.

7) Game theoretic analysis of jamming attacks in multi-agent systems: A game-theoretic approach was proposed to study cybersecurity in networked systems. This approach relies on the so-called "resilient graph problem". The attacker disrupts the connectivity of the network by removing edges from the graph, while the defender restores them. Both sides face energy constraints that limit their actions. Optimal strategies for each player are characterized by edge connectivity and the graph's connected components. The game is applied to a multi-agent consensus problem, examining how attacks and recovery actions affect consensus over time. This is important to guess strategic attackers' potential actions and to counteract them optimally. The approach was later extended so as to consider a rolling horizon method for players. This method captures the notion that attacker and defender can adjust their strategies as they obtain new insights into the overall process.

- Y. Nugraha, A. Cetinkaya, T. Hayakawa, H. Ishii, Q. Zhu, "Rolling Horizon Games for Cluster Formation of Resilient Multiagent Systems", Proc. IEEE Conference on Decision and Control, 2021.

- Y. Nugraha, A. Cetinkaya, T. Hayakawa, H. Ishii, Q. Zhu, "Cluster Formation in Multiagent Consensus via Dynamic Resilient Graph Games", Proc. IEEE Conference on Control Technology and Applications.

- Y. Nugraha, A. Cetinkaya, T. Hayakawa, H. Ishii, Q. Zhu, "Rolling horizon games of resilient networks with non-uniform horizons", European Journal of Control, 2022.

8) Development of an IoT testbed and IoT software: During the project, an IoT system (called RandomizedTransmissions) was developed. RandomizedTransmissions provides code for communication between several clients and a server running on IoT devices with Contiki-NG operating system. More specifically, the code enables transmission of sensor data at random time instants. The code was written in C for the communication part and Python for data analysis and plotting.

５．主な発表論文等

〔雑誌論文〕　計13件（うち査読付論文　4件／うち国際共著　5件／うちオープンアクセス　0件）

１．著者名 Feng Shuai、Cetinkaya Ahmet、Ishii Hideaki、Tesi Pietro、De Persis Claudio	４．巻 141
２．論文標題 Resilient quantized control under Denial-of-Service: Variable bit rate quantization	５．発行年 2022年
３．雑誌名 Automatica	６．最初と最後の頁 110302～110302
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.automatica.2022.110302	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Cetinkaya Ahmet、Kishida Masako	４．巻 66
２．論文標題 Impossibility Results for Constrained Control of Stochastic Systems	５．発行年 2021年
３．雑誌名 IEEE Transactions on Automatic Control	６．最初と最後の頁 5974～5981
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TAC.2021.3059842	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Kato Rui、Cetinkaya Ahmet、Ishii Hideaki	４．巻 8
２．論文標題 Security Analysis of Linearization for Nonlinear Networked Control Systems Under DoS	５．発行年 2021年
３．雑誌名 IEEE Transactions on Control of Network Systems	６．最初と最後の頁 1692～1704
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TCNS.2021.3078130	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Cetinkaya Ahmet、Kishida Masako	４．巻 6
２．論文標題 Instabilizability Conditions for Continuous-Time Stochastic Systems Under Control Input Constraints	５．発行年 2022年
３．雑誌名 IEEE Control Systems Letters	６．最初と最後の頁 1430～1435
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/LCSYS.2021.3105452	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Cetinkaya Ahmet、Ishii Hideaki、Hayakawa Tomohisa	4．巻 3
2．論文標題 Secure Networked Control Under Jamming Attacks: An SINR-Based Approach	5．発行年 2022年
3．雑誌名 Security and Resilience of Control Systems, Chapter 3	6．最初と最後の頁 63～91
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-83236-0_3	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Cetinkaya Ahmet、Kikuchi Kaito、Hayakawa Tomohisa、Ishii Hideaki	4．巻 117
2．論文標題 Randomized Transmission Protocols for Protection against Jamming Attacks in Multi-Agent Consensus	5．発行年 2020年
3．雑誌名 Automatica	6．最初と最後の頁 108960～108960
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.automatica.2020.108960	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Feng Shuai、Cetinkaya Ahmet、Ishii Hideaki、Tesi Pietro、Persis Claudio De	4．巻 66
2．論文標題 Networked Control Under DoS Attacks: Tradeoffs Between Resilience and Data Rate	5．発行年 2021年
3．雑誌名 IEEE Transactions on Automatic Control	6．最初と最後の頁 460～467
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TAC.2020.2981083	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Nugraha Yurid、Cetinkaya Ahmet、Hayakawa Tomohisa、Ishii Hideaki、Zhu Quanyan	4．巻 8
2．論文標題 Dynamic Resilient Network Games With Applications to Multiagent Consensus	5．発行年 2021年
3．雑誌名 IEEE Transactions on Control of Network Systems	6．最初と最後の頁 246～259
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TCNS.2020.3016839	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Wakaiki Masashi、Cetinkaya Ahmet、Ishii Hideaki	4．巻 65
2．論文標題 Stabilization of Networked Control Systems Under DoS Attacks and Output Quantization	5．発行年 2020年
3．雑誌名 IEEE Transactions on Automatic Control	6．最初と最後の頁 3560～3575
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TAC.2019.2949096	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Nugraha Yurid、Cetinkaya Ahmet、Hayakawa Tomohisa、Ishii Hideaki、Zhu Quanyan	4．巻 68
2．論文標題 Rolling horizon games of resilient networks with non-uniform horizons	5．発行年 2022年
3．雑誌名 European Journal of Control	6．最初と最後の頁 100693～100693
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.ejcon.2022.100693	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Kato Rui、Cetinkaya Ahmet、Ishii Hideaki	4．巻 67
2．論文標題 Linearization-Based Quantized Stabilization of Nonlinear Systems Under DoS Attacks	5．発行年 2022年
3．雑誌名 IEEE Transactions on Automatic Control	6．最初と最後の頁 6826～6833
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TAC.2021.3133180	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Kishida Masako、Cetinkaya Ahmet	4．巻 68
2．論文標題 Risk-Aware Linear Quadratic Control Using Conditional Value-at-Risk	5．発行年 2023年
3．雑誌名 IEEE Transactions on Automatic Control	6．最初と最後の頁 416～423
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TAC.2022.3142131	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Cetinkaya Ahmet、Ishii Hideaki、Hayakawa Tomohisa	4．巻 68
2．論文標題 Effects of Jamming Attacks on Wireless Networked Control Systems Under Disturbance	5．発行年 2023年
3．雑誌名 IEEE Transactions on Automatic Control	6．最初と最後の頁 1223～1230
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TAC.2022.3153275	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計25件（うち招待講演　1件／うち国際学会　17件）

1．発表者名 A. Cetinkaya, M. Kishida
2．発表標題 Nonlinear Data-Driven Control for Stabilizing Periodic Orbits
3．学会等名 IEEE Conference on Decision and Control（国際学会）
4．発表年 2021年

1．発表者名 Y. Nugraha, A. Cetinkaya, T. Hayakawa, H. Ishii, Q. Zhu
2．発表標題 Rolling Horizon Games for Cluster Formation of Resilient Multiagent Systems
3．学会等名 IEEE Conference on Decision and Control（国際学会）
4．発表年 2021年

1．発表者名 A. R. Ibrahim, A. Cetinkaya, M. Kishida
2．発表標題 Timed Congestion Games with Application to Multi-Fleet Platoon Matching
3．学会等名 IEEE Conference on Decision and Control（国際学会）
4．発表年 2021年

１．発表者名
Y. Nugraha, A. Cetinkaya, T. Hayakawa, H. Ishii, Q. Zhu

２．発表標題
Cluster Formation in Multiagent Consensus via Dynamic Resilient Graph Games

３．学会等名
IEEE Conference on Control Technology and Applications（国際学会）

４．発表年
2021年

１．発表者名
S. Feng, A. Cetinkaya, H. Ishii, P. Tesi, C. De Persis

２．発表標題
Resilient Quantized Control under Denial-of-Service with the Application of Variable Bitrate Quantization

３．学会等名
European Control Conference（国際学会）

４．発表年
2021年

１．発表者名
T. Arauz, J. M. Maestre, A. Cetinkaya, E. F. Camacho

２．発表標題
Model-Based PI Design for Irrigation Canals with Faulty Communication Networks

３．学会等名
European Control Conference（国際学会）

４．発表年
2021年

１．発表者名
E. Castellano, A. Cetinkaya, P. Arcaini

２．発表標題
Analysis of Road Representations in Search-Based Testing of Autonomous Driving Systems

３．学会等名
IEEE International Conference on Software Quality, Reliability and Security（国際学会）

４．発表年
2021年

１．発表者名
E. Castellano, A. Cetinkaya, C. Ho Thanh, S. Klikovits, X. Zhang, P. Arcaini

２．発表標題
Frenetic at the SBST 2021 Tool Competition

３．学会等名
IEEE/ACM 14th International Workshop on Search-Based Software Testing（国際学会）

４．発表年
2021年

１．発表者名
T. Pierron, T. Arauz, J. M. Maestre, A. Cetinkaya, C. Stoica Maniu

２．発表標題
Tree-Based Model Predictive Control for Jamming Attacks

３．学会等名
European Control Conference（国際学会）

４．発表年
2020年

１．発表者名
A. Cetinkaya, M. Kishida

２．発表標題
An Impossibility Result Concerning Bounded Average-Moment Control of Linear Stochastic Systems

３．学会等名
21st IFAC World Congress（国際学会）

４．発表年
2020年

１．発表者名
R. Kato, A. Cetinkaya, H. Ishii

２．発表標題
DoS-Aware Quantized Control of Nonlinear Systems via Linearization

３．学会等名
21st IFAC World Congress（国際学会）

４．発表年
2020年

１．発表者名
Y. Nugraha, A. Cetinkaya, T. Hayakawa, H. Ishii, Q. Zhu

２．発表標題
Dynamic Resilient Graph Games for State-Dependent Jamming Attacks Analysis on Multi-Agent Systems

３．学会等名
21st IFAC World Congress（国際学会）

４．発表年
2020年

１．発表者名
S. Pruekprasert, T. Takisaka, C. Eberhart, A. Cetinkaya, J. Dubut

２．発表標題
Moment Propagation of Discrete-Time Stochastic Polynomial Systems Using Truncated Carleman Linearization

３．学会等名
21st IFAC World Congress（国際学会）

４．発表年
2020年

１．発表者名
A. Cetinkaya, P. Arcaini, H. Ishii, T. Hayakawa

２．発表標題
A Search-Based Approach to Identifying Jamming Attacks and Defense Policies in Wireless Networked Control

３．学会等名
IEEE Conference on Decision and Control（国際学会）

４．発表年
2020年

１．発表者名
Y. Nugraha, A. Cetinkaya, T. Hayakawa, H. Ishii, Q. Zhu

２．発表標題
Dynamic Resilient Network Games Considering Connectivity

３．学会等名
IEEE Conference on Decision and Control（国際学会）

４．発表年
2020年

１．発表者名
A. Cetinkaya

２．発表標題
Randomized Transmissions for Secure Networked Control

３．学会等名
INFORMS Annual Meeting（国際学会）

４．発表年
2020年

１．発表者名
A. Cetinkaya, H. Ishii

２．発表標題
Randomized Transmission Protocols for Secure Multi-Agent Consensus Under Jamming Attacks

３．学会等名
IEEE Conference on Decision and Control, Workshop on Learning and Security for Multi-Agent Systems（招待講演）（国際学会）

４．発表年
2020年

１．発表者名
A. Cetinkaya, M. Kishida

２．発表標題
Impossibility Results for Stochastic Constrained Control

３．学会等名
SICE International Symposium on Control Systems

４．発表年
2021年

１．発表者名
A. Cetinkaya, P. Arcaini, H. Ishii, T. Hayakawa

２．発表標題
A Search-Based Approach for Designing Defense Policies Against Jamming Attacks in Wireless Networked Control Systems

３．学会等名
第49回 制御理論シンポジウム

４．発表年
2021年

１．発表者名
P. Arcaini, A. Cetinkaya

２．発表標題
CRAG at the SBFT 2023 tool competition-Cyber-physical systems track

３．学会等名
16th IEEE/ACM International Workshop on Search-Based and Fuzz Testing

４．発表年
2023年

１．発表者名
A. R. Ibrahim, A. Cetinkaya, M. Kishida

２．発表標題
Complexity and Efficiency of Nash Equilibria in Noncooperative Simple Platoon Games

３．学会等名
EEE Conference on Decison and Contro

４．発表年
2022年

１．発表者名
C. Eberhart, J. Haydon, J. Dubut, A. Cetinkaya, S. Pruekprasert

２．発表標題
Logic for Timed Agent Network Topologies

３．学会等名
IEEE Conference on Decison and Contr

４．発表年
2022年

１．発表者名
T. Arauz, J. M. Maestre, A. Cetinkaya, C. Stoica Maniu

２．発表標題
A Tree-Based Multi-Scenario Approach to Networked MPC under Packet Losses and Disturbances

３．学会等名
18th IFAC Workshop on Control Applications of Optimizati

４．発表年
2022年

１．発表者名
E. Castellano, S. Klikovits, A. Cetinkaya, P. Arcaini

２．発表標題
FreneticV at the SBST 2022 Tool Competition

３．学会等名
IEEE/ACM 15th International Workshop on Search-Based Software Testi

４．発表年
2022年

１．発表者名
A. R. Ibrahim, A. Cetinkaya, M. Kishida

２．発表標題
Modeling Heterogeneous Transportation Services by Two-Stage Congestion Games

３．学会等名
European Control Conferenc

４．発表年
2022年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

Website of Principle Investigator: https://www.ahmet.ac

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

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関