様式７号（第 12 条，第 31 条関係）
（様式７号）(Format No.7)　日本語版

学　位　論　文　要　旨
(Summary of the Doctoral Dissertation)

学位論文題目 (Dissertation Title)	Prediction Mechanism Using Adaptively Linked Composite Ensemble Networks to Enhance Robustness and Its Application in Smart Cities（堅牢性を高めるために適応連結する複合アンサンブルネットワークを用いた予測メカニズムとスマートシティへの応用）
氏　名(Name)	Mohd Hafizuddin Bin Kamilin

スマートシティのセンサーで収集される大規模で複雑なデータは、従来の方法では処理が難しく、機械学習が活用されている。機械学習により、都市運営の効率を上げ、住民の生活の質を向上させ、データに基づく意思決定を支援できる。応用例として、電力消費量や交通量の予測により電力負荷のバランスや交通の流れを改善し、大気汚染を減らせる。

これまでに提案された機械学習モデルは、品質に優れ、傾向が変わらない入力データと安定したシステムを前提に開発されてきた。しかし、分散型サービス拒否攻撃による入力データの欠損値、敵対的攻撃で予測を誤らせるために導入された小さな撹乱、季節やトレンドの変化でデータ分布が変わったことで予測が無効になる概念ドリフト、ホストサーバの不安定性の問題によって機械学習の予測精度が低下してしまう。

これらの問題を解決できる統合技術はまだ提案されていないため、本学位論文では、複数の独自の解決策を統一する新しい手法として、適応連結する複合アンサンブルネットワークを提案した。複合アンサンブルネットワークは、欠損値、敵対的攻撃、概念ドリフトなどの問題に対する解決策を、訂正および予測の強化という観点で分類する。複数の解決策を連結するために、解決策の優先順位に基づき、訂正用の解決策を順次連結し、予測を強化する解決策を並列に連結した。また、特定の問題に対する訂正用の解決策の出力を、予測を強化する解決策の入力に接続することで、予測モデルは訂正された欠損値、敵対的攻撃、そして概念ドリフトを把握し、継続的に予測精度を改善できる。単一障害点を防ぐために、複合アンサンブルネットワークの各ノードには異常検知、データのバックアップ、および投票メカニズムが組み込まれている。一部のノードに処理ができなくなる場合、投票メカニズムで選ばれたノードリーダーがノードの連結を再調整し、使用できなくなった解決策をバックアップデータから他のノードに復元することができる。

学位論文は 6 つの章から構成される。

第 1 章では、スマートシティにおける基本的なサービス運用の最適化と、サイバー攻撃からの防御について説明した。そして、これらの問題を統一的な方法で解決する必要性を示し、本学位論文の目的を示した。続いて、学位論文の位置づけを明確にするため、これまでの研究で提案された統一的な解決策に似た例を示し、解決策の相性で先行研究が簡単な解決に限られていたことを示した。そのうえで、学位論文に提案された複合アンサンブルネットワークはどのようにその弱点を解決することを示した。

第 2 章では、先行研究で扱われた欠損値、敵対的攻撃、概念ドリフト、および単一障害点に対する解決策と独自の研究を比較し、それらの解決策を 5 つのよく使われる機械学習モデルに適用して、回帰分析におけるそれぞれの解決策の不十分さと限界を明らかにした。

第 3 章では、提案された適応連結する複合アンサンブルネットワークが、スマートシティ管理システムから取得したデータの異常検知、適切な解決策の連結、および予測の流れを示した。さらに、シス

（和文 2,000 字程度 / 英文 800 語程度）
(about 800 words)

テム管理者から得たハイパーパラメータが機械学習モデルの設置と検知の流れにどのように影響するかを示した。続いて、分散システムアーキテクチャと解決策連結の条件のうえで、欠損値、敵対的攻撃、概念ドリフト、そして単一障害点の解決策を示した。

第 4 章では、ニューヨーク州の電力消費量を予測するために、適応的連結による複合アンサンブルネットワークを応用した。提案手法の有効性を示すために、実際の概念ドリフトのデータやランダムな欠損、および敵対的攻撃のシミュレーションを用いて、先行研究の第 2 章の結果と比較した。そして、低い電力消費量の予測精度により、経済的にどのような悪影響が与えられるかを議論した。

第 5 章では、適応連結する複合アンサンブルネットワークの一般性を示すために、カリフォルニア州の交通量を予測し、上記の問題に対する耐性を確認できた。また、第 4 章と同様に、不明確な予測がもたらす悪影響について議論し、交通車両の流れの悪化と燃料の無駄な消費との関係を示した。

最後に、第 6 章では、学位論文の全体をまとめた。

以上の成果により、適応連結する複合アンサンブルネットワークは欠損値、敵対的攻撃、そして概念ドリフトを統一的に解決できた。さらに、分散システムアーキテクチャとデータと機械学習モデルデータのバックアップにより単一障害点の問題も解決できた。統一された解決策は、都市機能の根幹を支えるサービスの品質向上と、サイバー攻撃に対する強靭なシステム構築を両立させ、市民が安心して暮らせる安全で持続可能なスマートシティの実現に大きく貢献することが期待される。

様式７号（第 12 条，第 31 条関係）
（様式７号）(Format No.7) 英語版

学 位 論 文 要 旨
(Summary of the Doctoral Dissertation)

学位論文題目 (Dissertation Title)	Prediction Mechanism Using Adaptively Linked Composite Ensemble Networks to Enhance Robustness and Its Application in Smart Cities（堅牢性を高めるために適応連結する複合アンサンブルネットワークを用いた予測メカニズムとスマートシティへの応用）
氏　名(Name)	Mohd Hafizuddin Bin Kamilin

Machine learning is often suggested to help with the processing of huge and intricate datasets collected by sensors in smart cities, which are challenging to process or compute using conventional approaches. In addition to improving the efficiency of urban operations, it also enhances the quality of life for the residents and provides actionable insight to help with decision-making. Machine learning has various applications in smart cities, such as forecasting electricity loads to balance supply and demand and estimating traffic volume to enhance traffic flow and minimize air pollution.

Most of the proposed machine learning techniques for forecasting were created with the assumption that the input variables are clean with consistent data distribution and running on a stable system. However, the accuracy of machine learning forecasts is compromised by problems such as missing values in input data due to distributed denial-of-service attacks, small disturbances introduced by hostile attacks to make predictions erroneous, conceptual drift that invalidates predictions due to changes in data distribution caused by seasonal or trend changes, and system instability that could bring the servers or Internet of Things devices that are hosting the forecasting models to be offline.

Because a true unified method that could solve these problems by combining multiple solutions not yet been proposed, this thesis proposes a novel approach called Adaptively Linked Composite Ensemble Networks to combine multiple original works into one. To link multiple solutions into one, Composite Ensemble Networks classify solutions to problems such as missing values, adversarial attacks, and concept drift in terms of correction and enhanced forecast. Then, it sequentially links the solutions for correction and solutions for enhanced prediction in parallel based on the priority of the solutions. After that, by connecting the inputs and outputs of the corrective solutions for a particular problem to the inputs of the prediction-enhancing solutions, it can capture corrected missing values, adversarial attacks, and concept drift to continuously improve prediction accuracy.

The thesis consists of six chapters.

Chapter 1 describes the optimization of essential service operations in smart cities and protection against cyberattacks. It then indicated the need to solve these problems in a unified way and stated the purpose of this dissertation. To clarify the position of the dissertation, the previous study similar to the unified solutions was compared, and the limitations of why it is limited to simple solutions due to the compatibility of the solutions is explained. Then, the countermeasures taken to solve the compatibility issues in this thesis are defined.

Chapter 2 compares the solutions to missing values, adversarial attacks, concept drift, and single point of failure addressed in prior work with original work, applies those solutions to five commonly used machine learning models, and reveals the inadequacies and limitations of each solution in regression analysis.

Chapter 3 presented the Adaptively Linked Composite Ensemble Networks to detect anomalies in data obtained from a smart city management system, link appropriate solutions, and predict the flow of prediction. In addition, it was shown how hyperparameters obtained from the system administrator

affect the system initialization. Then, the distributed system architecture, conditions for linking solutions, anomaly detection, and anomalies detection were presented.

Chapter 4 demonstrated the proposed ensemble learning network implementation and application for forecasting the electricity load in New York State and its resiliency against missing values, adversarial attacks, and concept drift. Then, the accuracy of the proposed method was compared with the previous methods in Chapter 2, highlighting their weaknesses and how they could negatively affect economies.

Chapter 5 showed the adaptability of the proposed method application to forecast the traffic volume in California against the problems previously mentioned. Similarly, the effect of an accurate traffic volume forecast is discussed, especially the reduced fuel consumption due to car idling during congestion.

Finally, Chapter 6 summarized the works done in this thesis.

These results highlight the effectiveness of Adaptively Linked Composite Ensemble Networks to solve missing values, adversarial attacks, and concept drift. In addition, the implementation shows its robustness against the single point of failure by distributing the essential components with redundancy. As the society is becoming deeply integrated with cyberspace, the unified solution is not only necessary to improve the essential services but also to protect them against the cyberattacks.

（様式９号）

学位論文審査の結果及び最終試験の結果報告書

山口大学大学院創成科学研究科

氏　　名	Mohd Hafizuddin Bin Kamilin
審査委員	主　　査：山口　真悟
	副　　査：間普　真吾
	副　　査：中村　秀明
	副　　査：佐村　俊和
	副　　査：王　　元元
論文題目	Prediction Mechanism Using Adaptively Linked Composite Ensemble Networks to Enhance Robustness and Its Application in Smart Cities （堅牢性を高めるために適応連結する複合アンサンブルネットワークを用いた予測メカニズムとスマートシティへの応用）

【論文審査の結果及び最終試験の結果】

スマートシティは、センサーネットワークから収集される大量のデータを活用し、都市運営の効率化や住民の生活の質向上を目指す都市形態である。このデータ利活用において、機械学習は重要な役割を果たしている。しかし、従来の機械学習モデルは、高品質で傾向が変わらない入力データと安定したシステムを前提に開発されてきたため、現実のスマートシティ環境では様々な課題に直面している。具体的には、分散型サービス拒否攻撃による入力データの欠損値、敵対的攻撃による予測の誤り、季節やトレンドの変化によるデータ分布の変化（概念ドリフト）、そしてサーバの不安定性などが挙げられる。これらの問題は、機械学習の予測精度を低下させ、都市サービスの提供に支障をきたすおそれがある。先行研究では、これらの問題に対する統一的な解決策が検討されてきたが、処理の順序に制約があり、外乱の訂正誤差が蓄積してしまうという課題があった。

そこで、本学位論文では、これらの課題を解決するために、複数の解決策を統一するための新しい手法として、適応連結する複合アンサンブルネットワーク（ALCEN）を提案した。ALCENは、欠損値、敵対的攻撃、概念ドリフトといった問題に対する解決策を、訂正と予測の強化という観点から分類し、複数の解決策を連結する。具体的には、解決策の優先順位に基づき、訂正用の解決策を順次連結し、予測を強化する解決策を並列に連結する。さらに、特定の問題に対する訂正用解決策の出力を、予測を強化する解決策の入力に接続することで、予測モデルは訂正された欠損値、敵対的攻撃、そして概念ドリフトを把握し、継続的に予測精度を改善することが可能となる。

また、サーバの不安定性に対応するため、ALCENの各ノードには他のノードの解決策がバ

（様式９号）

ックアップされている。一部のノードがダウンした場合でも、投票メカニズムで選ばれたノードリーダーがノードの連結を再調整し、ダウンした解決策をバックアップデータから他のノードに復元することができる。

以上の成果により、ALCENは欠損値、敵対的攻撃、そして概念ドリフトを統一的に解決し、分散システムアーキテクチャとデータのバックアップにより単一障害点の問題も解決した。この統一された解決策は、都市機能の根幹を支えるサービスの品質向上と、サイバー攻撃に対する強靭なシステム構築を両立させ、市民が安心して暮らせる安全で持続可能なスマートシティの実現に大きく貢献することが期待される。成果はその有効性を裏付けるものである。

公聴会における主な質問内容は、提案手法における再学習の必要性とその実装方法に関するもの、敵対的攻撃の検知方法に関するもの、実際の攻撃とシミュレーションの間のパラメータ設定に関するもの、提案手法の適用限界に関するものなどについてであった。いずれの質問に対しても発表者から的確な回答がなされた。

以上より本研究は独創性、信頼性、有効性、実用性ともに優れ、博士（工学）の論文に十分値するものと判断した。

論文内容及び審査会、公聴会での質問に対する応答などから、最終試験は合格とした。

なお、主要な関連論文の発表状況は下記のとおりである。（関連論文 計８編、参考論文 計０編）

1) Mohd Hafizuddin Bin Kamilin, Mohd Anuaruddin Bin Ahmadon, Shingo Yamaguchi, “Multi-Task Learning-Based Task Scheduling Switcher for a Resource-Constrained IoT System,” Information, vol. 12, no. 4, 150, 2021.
2) Mohd Hafizuddin Bin Kamilin, Shingo Yamaguchi, “Resilient Electricity Load Forecasting Network with Collective Intelligence Predictor for Smart Cities,” Electronics, vol. 13, no. 4, 718, 2024.
3) Mohd Hafizuddin Bin Kamilin, Shingo Yamaguchi, Mohd Anuaruddin Bin Ahmadon, “Radian Scaling and Its Application to Enhance Electricity Load Forecasting in Smart Cities Against Concept Drift,” Smart Cities, vol. 7, no. 6, pp. 3412-3436, 2024.
4) Mohd Hafizuddin Bin Kamilin, Shingo Yamaguchi, Mohd Anuaruddin Bin Ahmadon, “Fault-Tolerance and Zero-Downtime Electricity Forecasting in Smart City,” Proceedings of 2023 IEEE 12th Global Conference on Consumer Electronics, pp. 298-301, 2023.