論 文 内 容 の 要 旨

博士論文題目　Improving Electricity Theft Detection for Smart Homes: Insights from Real and Synthetic Attack Scenarios

氏　名　Olufemi Abiodun Abraham

（論文内容の要旨）

Efforts to improve the security of electricity grids include both physical measures, such as detecting interference, and digital security methods, such as encryption. However, these measures alone are insufficient for addressing the full range of cyberattacks. To address these concerns, contemporary approaches that use data analytics, machine learning (ML), and predictive techniques are required. The rise in sophisticated statistical methods, particularly those involving machine learning, has led to an interest in developing models and algorithms, e.g., for smart homes, that can interpret smart meter data to quickly identify signs of tampering.

Smart home appliances, which are becoming increasingly integral to modern households, are also vulnerable to electricity theft. This can have a significant impact on both utility providers and consumers, as these appliances often connect to the internet and transmit usage data to utility providers for billing and monitoring. This data transmission can be intercepted or manipulated, leading to false readings and unauthorized electricity use. The ability to remotely control appliances also presents a risk of unauthorized access, which can lead to the misuse or manipulation of consumption data. To address these vulnerabilities, emerging technologies such as advanced ML algorithms and enhanced encryption methods are being developed to detect anomalies in usage patterns and secure data transmission.

This dissertation presents novel approaches to electricity theft detection (ETD) by introducing various classification algorithms to detect anomalies in non-intrusive appliance load monitoring (NIALM) or disaggregated smart meter networks. Our proposed framework utilizes ML knowledge-based synthetic attack data (KB- SAD) to train an attack classifier. The framework was validated using the Almanac of Minutely Power dataset version 2 (AMPds2), which contains fine-grained time-series data from a smart home. The Extreme Gradient Boosting algorithm performed best with an average area under curve (AUC) score of 98.74% and 98.69% for detecting and classifying anomalies in real and simulated attacks, respectively. These methods outperformed legacy unsupervised methods (LUM). By integrating the KBSAD, our approach eliminates the need for extensive data collection for real attacks and seamlessly combines synthetic attacks with genuine consumption readings, representing a significant advancement in the field of smart-home electricity theft detection.

氏　名	Olufemi Abiodun Abraham

（論文審査結果の要旨）

今日、スマートグリッドの登場により、エネルギー管理と効率の大幅な向上が期待されている。その一方で、スマートグリッドの完全性を損なう可能性のあるセキュリティ上の懸念も増大している。スマートメータが提供する高解像度のデータにより、動的なエネルギ価格設定、負荷予測、スマート家電の監視などの便益向上が期待される一方で、不正アクセスとデータ改竄のリスクがあるため、電力窃盗やその他の詐欺行為につながる可能性が懸念される。本論文では、既存知識に基づく合成攻撃データを用いて、スマートホーム向けの効果的な電力窃盗検出フレームワークを設計・開発することを目指している。実際の攻撃シナリオを模擬し、検証攻撃データを適用し、複数の機械学習アルゴリズムを用いて精度評価を行う。本論文の主な成果は、以下に要約される。

1. スマートメータの非侵襲型負荷監視システムにおける電力窃盗の検知を目的として、モデルを最適化して適切な検出精度を達成し、偽陽性と偽陰性の割合を減少させることに成功している。適切なハイパーパラメータの選択が堅牢な電力窃盗検知システムの開発に不可欠であることを実験結果から示している
2. スマートホームを想定した、5通りの攻撃シナリオと AMPds2 データセットに基づく合成攻撃データセットを作成し、さらに効果的な前処理方法を提案することで、スマートホーム向けの堅牢な電力窃盗検知システムを開発している。異なる機械学習モデルを調査し、検知に最適なアルゴリズムを特定している。提案方式は電力線ケーブルが容易に追跡できないアパート、混雑した建物複合体などで特に効果を発揮するとみられる。

以上のように、本論文はスマートホーム向け電力供給のセキュリティ向上に資するデータセット合成法を提案し、複数の機械学習アルゴリズムを用いた精度評価を実施し、発展途上国における電力窃盗の実情をふまえた実証的示唆を示すことでその有効性を検証している。それぞれの成果は1編の学術論文と2編の査読付き国際会議論文として発表されており、研究成果の有効性を見ることができる。よって本論文は、博士（工学）の学位論文としての価値があるものと認める。