

Isolation Forest を用いた IoT 向け異常検知手法に関する考察

菅田 大輔^{1,a)} 安全 花子^{1,2,†1}

概要：概要

キーワード：Isolation Forest, IoT, IDS, 異常検知

A Study on Anomaly Detection Method for IoT using Isolation Forest

DAISUKE SUGATA^{1,a)} HANAKO ANZEN^{1,2,†1}

Abstract: abstract

Keywords: Isolation Forest, IoT, IDS, Anomaly Detection

1. はじめに

以下のことを書く.

- 大目標：小規模な環境向けの IoT 向け異常検知手法の提案・「IoT 環境を考えたとき、iforest が軽量でうまくいきそうなので、～うまくいかないことも多かった。そこで、データセットの～を工夫して、そのやり方を報告する」→本研究の目的を最初に述べちゃう
- 大目標を実現する必要性：卒論と同じ
- 問題提起（大目標を達成するために必要なことを述べ、そのためにどのような問題があるのかを述べる（小目標に分割する）。）関連研究をリサーチしてみると参考にした論文が良さそうだ。しかし、いくつか課題もあるので改善したい 1. 特徴量エンジニアリング 2.

判定の組み合わせアルゴリズム

- （関連研究：問題を解決するための従来研究を紹介）
- 本研究の目的：1. 特徴量エンジニアリングの比較 2. 判定の組み合わせアルゴリズムの改善

2. 研究方法

2.1 Isolation Forest の説明

Isolation Forest の説明（卒論と同じ）かける

2.2 IDS の概要

IDS の概要をかく。採用した理由を述べる。

2.2.1 全体像

かける

2.2.2 特徴量エンジニアリング

3. 事前実験？

Isolation Forest を組み込んだ

4. 結果と考察

（本論文のメイン）

¹ 東京工業大学 情報理工学院 数理・計算科学系
Department of Mathematical and Computing Sciences,
School of Computing, Tokyo Institute of Technology

² 株式会社 YY セキュリティ研究所
Security Laboratories, YY Corporation

^{†1} 現在, 国立研究開発法人 ZZ 研究所
Presently with National Institute of ZZ

^{a)} sugata.d.aa@m.titech.ac.jp

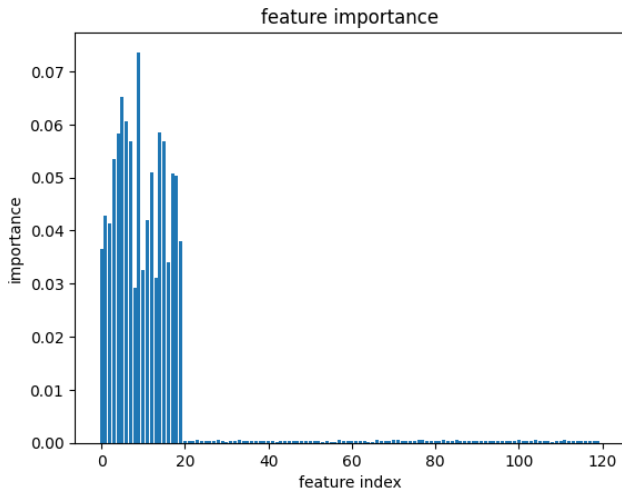


図 1 select_noise に関する図の説明 (和文)

Fig. 1 Description of the select_noise figure (English).

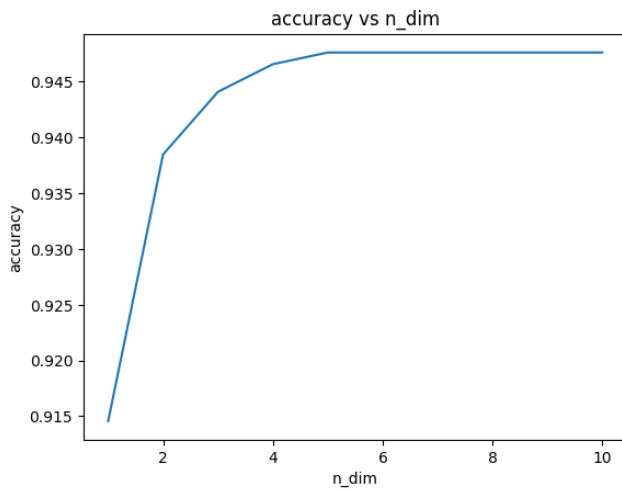


図 2 dim_vs_accu に関する図の説明 (和文)

Fig. 2 Description of the dim_vs_accu figure (English).

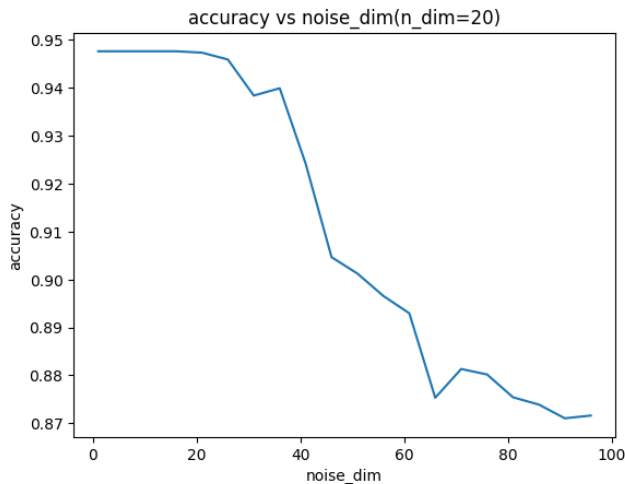


図 3 noise_accu に関する図の説明 (和文)

Fig. 3 Description of the noise_accu figure (English).

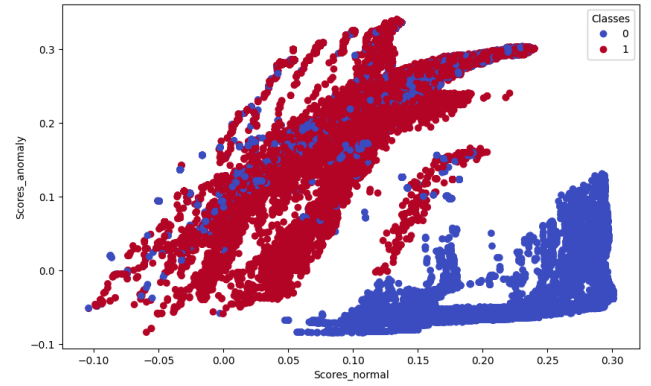


図 4 FLUNSW に関する図の説明 (和文)

Fig. 4 Description of the FLUNSW figure (English).

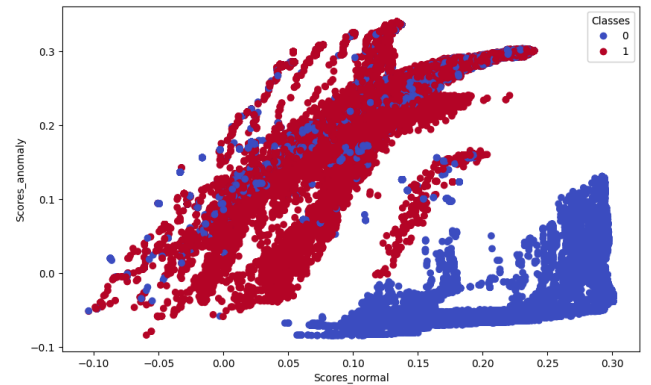


図 5 classes_UNSW に関する図の説明 (和文)

Fig. 5 Description of the classes_UNSW figure (English).

4.1 実験方法

4.1.1 実験環境

他の人が再現できるように実験環境を書く. 1. 特徴量エンジニアリングの比較 2. 判定の組み合わせアルゴリズムの比較

4.1.2 データセット

使用したデータセットの概要と, その妥当性について述べる.

4.1.3 評価指標

使用した評価指標と, その妥当性について述べる.

4.2 結果

実験の結果, 得られるデータから読み取れる客観的事実を書く. この時, 論文の目的を達成するためにどのような主張をどのような結果(データ)に基づいて説明すべきかを考える.

4.3 考察

4.3.1 本論文における目的に即した結論を導く

- 本結果を一般化したどのような結論を導き出せるかを, 論文の目的に即して述べる. 1. このくらい有効特徴量あればいける 2. iforest ではうまくいく

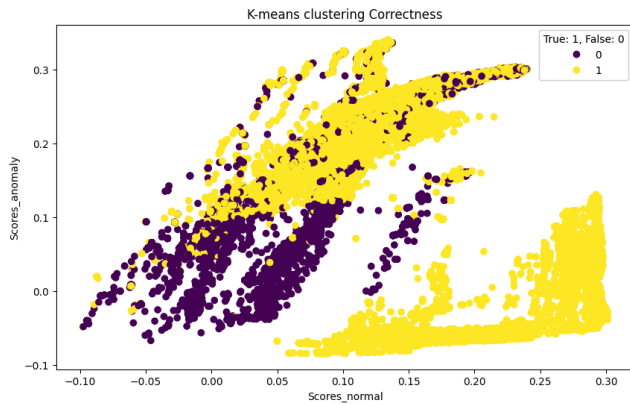


図 6 collectness_UNSW に関する図の説明 (和文)

Fig. 6 Description of the collectness_UNSW figure (English).

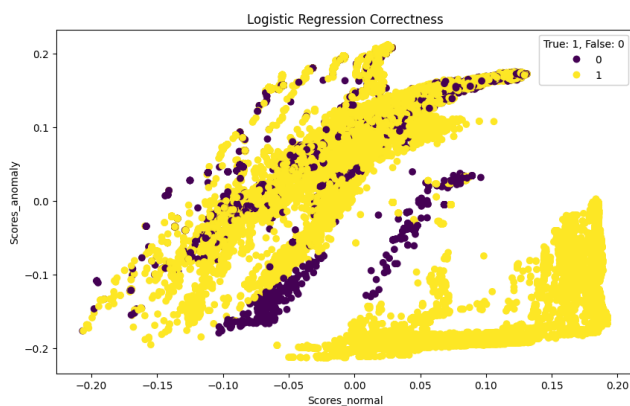


図 7 collectness_UNSW2 に関する図の説明 (和文)

Fig. 7 Description of the collectness_UNSW2 figure (English).

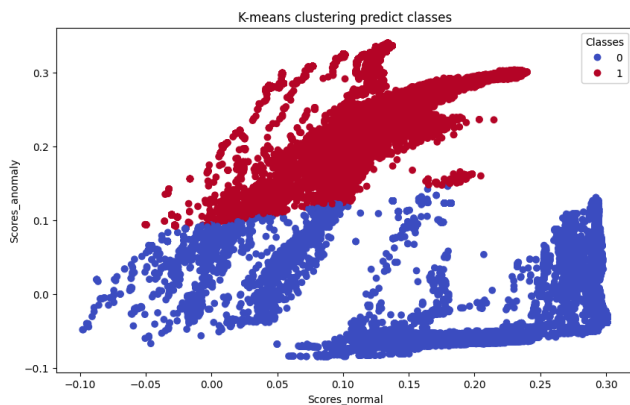


図 8 predict_classes_UNSW に関する図の説明 (和文)

Fig. 8 Description of the predict_classes_UNSW figure (English).

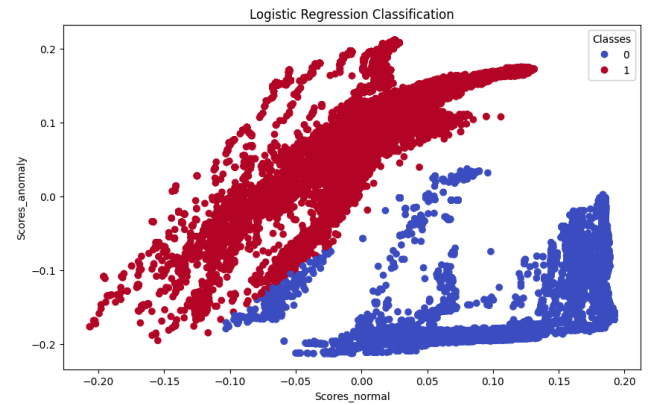


図 9 predict_classes_UNSW2 に関する図の説明 (和文)

Fig. 9 Description of the predict_classes_UNSW2 figure (English).

良いアルゴリズムがあるかも

5. おわりに

おわりにを書く.

謝辞 謝辞を書く.

参考文献

- 実験結果の妥当性を説明する.

4.3.2 結果から予測される問題を提起する.

- 結果が生じた理由について考察する. 1. 2. グラフの分布を見ると、縦横で切るより斜めで切ったほうがいい
- 本実験結果を認めると、どのような現象の予測や応用可能性があるかを述べる. 1. 2. より良い局面、より