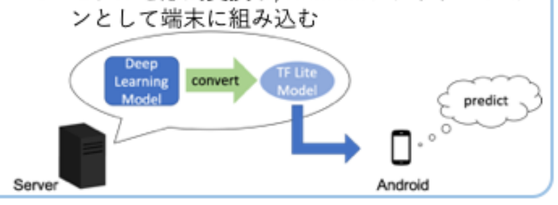
小口研究室　研究紹介　(2021年度)
(お茶の水女子大学理学部情報科学科)

深層学習を用いた輻輳予測モデルのAndroidへの実装と性能評価
（研究担当:佐藤 里香）

研究概要

◆ 研究背景
- 無線環境下でのトラフィックの輻輳は突発的に生じ，一度起こると制御が難しい上制御を試みるとさらに悪化
  ⇒輻輳を事前予測することが理想
- 予測にあたりデータを端末外に出す安全上の問題やデータ転送に要する時間等が課題に
  ⇒端末内処理が理想

◆ 研究方針
- サーバで深層学習を用いたトラフィックデータの解析，学習モデルを作成
- モデルを形式変換し，Androidアプリケーションとして端末に組み込む



サーバでの学習モデルの作成・形式変換

◆ 端末での無線LAN通信時のスループットデータから同一AP接続端末台数をLSTMで予測
- TensorFlowのKerasを使用
- 端末1, 3, 5, 7, 9台，各500秒間の通信データを使用
- 各端末でt－9秒 ～ t 秒の10秒間のスループット値からt秒における接続端末台数が設定した閾値を超えているか否かを予測
- 400秒分で学習，100秒分でテスト

◆ 正解率
⇒9割超の高い正解率での予測に成功

閾値	Training Data	Test Data
1台or3台以上	100%	100%
3台以下or5台以上	99.2%	98.4%
5台以下or7台以上	94.9%	93.0%
7台以下or9台	98.6%	93.5%

◆ 作成した学習モデルをAndroid端末に導入するため、TensorFlow Lite対応形式に変換
- 変換前の学習モデルによる予測結果と変換後の学習モデルによる予測結果を比較
  ⇒100%一致

学習モデルのAndroid端末上への導入・性能評価

◆ 形式変換後の学習モデルを組み込んだAndroidアプリケーションを制作
・ t－9秒 ～ t 秒の10秒間のスループットを入力し，t秒における接続端末台数が閾値を超えているか否かを予測

◆ 予測精度の比較
- サーバ上と端末上の予測結果を比較
  ⇒100%一致，端末上でもサーバとほぼ同等の精度であることが確認できた

◆ 予測時間の比較
- サーバ上と端末上の予測時間を比較
  ⇒端末上ではサーバに比べ3倍程度要しているが，想定する輻輳制御周期(0.3秒)を考えると十分な速度

	サーバ上	端末上
予測時間	1.00ms	3.14ms

◆ CPU使用率の比較
- 端末上での予測処理時のCPU使用率を計測
  ⇒10%を切り十分低い値

	検証用アプリ
CPU使用率	7%

今後の課題

・より早い段階での高精度な予測を実現
・端末上で完結する輻輳制御システムの実現

Neural Architecture Searchを取り入れた時系列予測モデル運用手法の検討
（研究担当:高橋 佑里子）

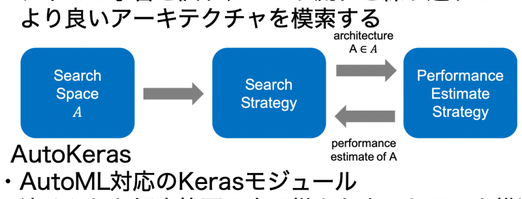
研究概要

◆ 背景
・仮想環境において、計算資源のオーバーコミットに由来するVMの性能低下を防ぐことを目的として、VMのCPU使用率を予測し、その結果に基づいて制御を行う技術が知られている
・VMとそこで実行されるアプリケーションは時々刻々と変化するため、環境の変化に合わせて予測モデルを継続的に学習し、モデルを更新することで予測精度を担保する
・従来は学習させるデータを変えるのみで、予測モデルのネットワーク構造を変えることはなかったが、学習させるデータによって最適な予測モデルのネットワーク構造は異なる

◆ 目的
Neural Architecture Searchを取り入れることで
環境の変化に応じて予測モデルの構造を変化させながら予測モデルを運用する手法の検討

関連技術

◆ Neural Architecture Search (NAS)
・ニューラルネットワークの構造自体を最適化すること
・探索戦略によって選ばれた探索空間に含まれるアーキテクチャでの学習を行い、作成されたモデルのパフォーマンスを推定した結果を元に別のアーキテクチャでの学習を試す、という流れを繰り返すことで、より良いアーキテクチャを模索する



◆ AutoKeras
・AutoML対応のKerasモジュール
・決められた探索範囲の中で様々なネットワーク構造やハイパーパラメータで学習を行い、複数回の試行の後最も精度が良いモデルを出力する機能を持つ

予備実験

◆ 概要
・最適なNASの探索範囲を定めるために、モデルのネットワーク構造と学習時間/精度の関係を、以下の表から得られるすべての組み合わせ(3*30=90通り)で調べた

パラメータ	範囲
LSTM の層数	1-3
LSTM のユニット数	1-30

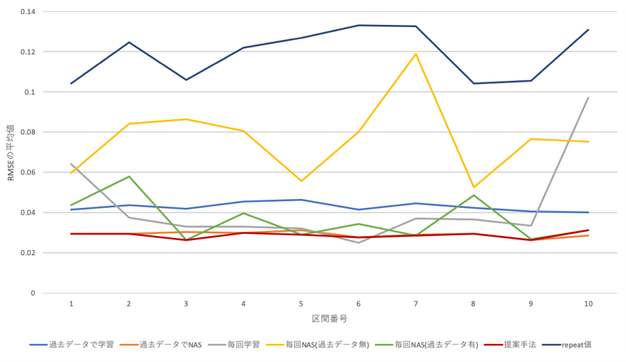
・2種類の実験を行った結果、以下の範囲に絞るのが良いと考えた→提案手法で適用

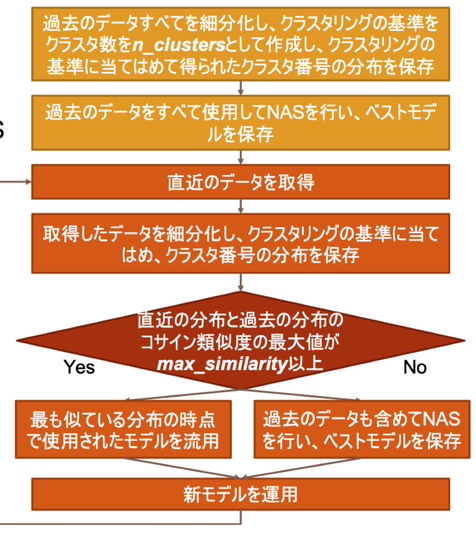
パラメータ	範囲
ラーニングレート	0.01 または 0.001
LSTM の層数	2(固定)
LSTM のユニット数	20-30

実験

◆ 方法
・Microsoft社が提供しているAzureのVMデータセットの一部を使用し、100種類の波形を抽出した後、それらを異なる割合で含むデータを20種類作成し、10種類を準備段階、10種類を運用段階として行った
・提案手法(画像右)におけるパラメータは、n_clusters: 50, max_similarity: 0.94とした
→NASの回数は4/10回となった

◆ 結果(画像左)から読み取れること
・NASを行う場合は、過去のデータを使用することが精度を向上させるために必要
・過去データでNASを行い出力されたモデルの精度が良い
・提案手法では適切なタイミングでNASを行っており、NASを取り入れることでより高精度な予測モデルの運用が可能





今後の課題

・モデルの重みの再利用の検討
・提案手法に沿った予測モデルの運用を行い、どの程度の改善が見込まれるかのシミュレーション

IoTデバイスのためのLeveled準同型暗号システムの提案
（研究担当:松本 茉倫）

研究背景

❑ **クラウドと情報漏洩の危険**
IoTデバイスから取得したセンサデータ等をクラウドサービスで活用したい
→ 暗号化したままで活用できるのが理想

❑ **Leveled 準同型暗号 (LHE)**
暗号文同士の加算・乗算が可能な暗号化方式
処理に時間がかかり、暗号文サイズが大きい
→ 低性能マシン (IoTデバイス) において
暗号化時間・通信量を減らしたい

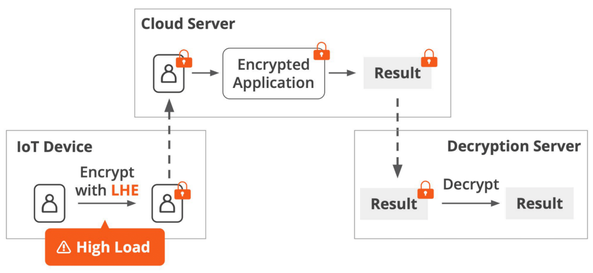


図1: LHE暗号化の課題

システムデザイン

❑ **想定**
IoTデバイス: 個人データを暗号化
クラウドサーバ: 暗号化されたアプリケーションを実行
復号サーバ: アプリケーション実行結果を復号

❑ **Baseline**
IoTデバイスが平文をLHEで暗号化.

❑ **HomAES**[Lauter2011]
IoTデバイスが平文をAES，AES鍵をLHEで暗号化.
クラウドサーバがAESをLHEの暗号文へ切り替える.

❑ **提案手法**
IoTデバイスが平文をRLWE暗号で暗号化.
クラウドサーバがRLWEをLHEの暗号文へ切り替える.
→IoTデバイスでLHEを使う必要がない

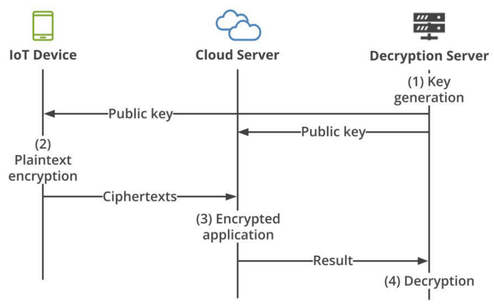


図2: システムデザインの概要

[Lauter2011] Kristin Lauter and others, "Can homomorphic encryption be practical?", Proc. of the 3rd ACM workshop on CCSW '11, pp. 113–124, (2011)

評価実験

IoTデバイスが100KiBを暗号化する場合で評価 (100KiB→CIFAR-10なら33枚相当)

❑ **実験環境**
IoTデバイス: Google Pixel 3, Raspberry Pi 3 Model B+
クラウドサーバ: 6コア, 3.6GHz CPU, 512GB RAM

❑ **評価指標**
IoTデバイスの暗号化時間・クラウドサーバのLHEへ切り替える時間・通信量

表1: IoT・CSへの負荷と通信量

	Encryption time on the IoT [s]	Switching time on the CS [m]	Ciphertext size (IoT→CS) [MiB]	Public key size (DS→IoT) [MiB]
Baseline	57.578 275.493	Switching is unnecessary	1014.613	154.082
HomAES	19.303 Memory error	227	316.933	2400.233
Ours	0.63 1.73	351.87	4.357	0.001

結論

❑ **Baseline**
クラウドサーバにとっては楽だが，IoTデバイスには最も負担が大きい

❑ **HomAES**
IoTデバイスはBaselineよりも速く暗号化できるがメモリの小さなデバイスでは実行不可能

❑ **提案手法**
クラウドサーバには負荷をかけるが最もIoTデバイス向き

一般にIoTデバイスの性能はクラウドサービスよりも低い
提案手法が最適

http://ogl.is.ocha.ac.jp/
oguchi@is.ocha.ac.jp