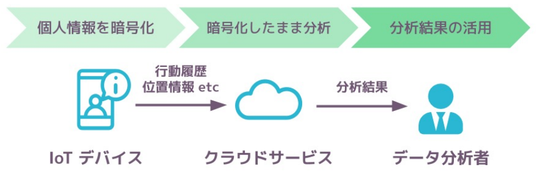
小口研究室　研究紹介 (2020年度)
(お茶の水女子大学理学部情報科学科)

IoTデバイスにおけるデータ活用のための準同型暗号を用いた暗号化の高速化
（研究担当：松本茉倫）

研究背景

- **クラウドと情報漏洩の危険**
  ユーザから取得したセンサデータを
  クラウドサービスで統計分析したい
  → クラウドサービスは安全とは限らない



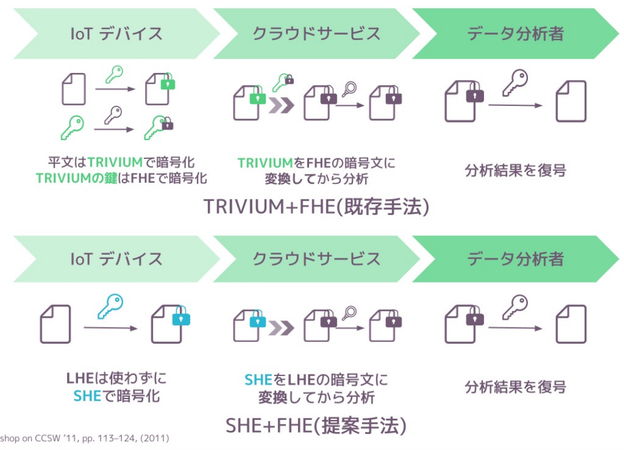
- **個人情報保護とデータ分析の需要**
  企業側　：データ分析結果が欲しい
  ユーザ側：個人情報を知られたくない
  → 完全準同型暗号 (FHE) が有用

- **完全準同型暗号 (FHE)**
  暗号文同士の加算・乗算が可能な暗号方式
  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

システムデザイン

- **FHE only (既存手法)**
  平文をFHEで暗号化する
- **TRIVIUM+FHE(既存手法)**
  FHEより軽量なTRIVIUM(共通鍵暗号)と
  FHEを組み合わせる [Lauter2011]
- **SHE+FHE (提案手法)**
  FHEより軽量なSomewhat 準同型暗号
  (SHE) とFHEを組み合わせる

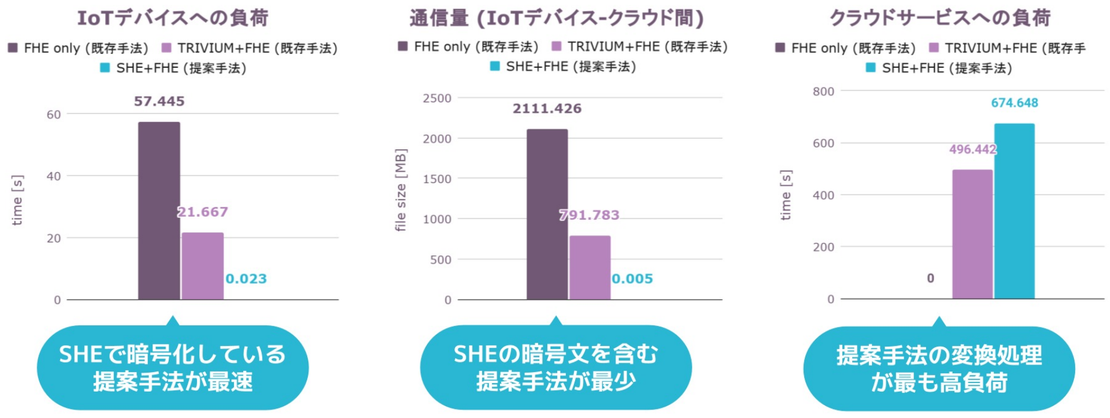
96Bを暗号化した場合の以下3つを比較
1. IoTデバイスへの負荷
2. IoTデバイス-クラウド間の通信量
3. クラウドサービスへの負荷



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

実験結果

IoTデバイス: Google Pixel 3　**クラウドサービス**: 6コア, 3.6GHz, 512GB



結論

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ため
IoTデバイスへの負荷を優先するべき

⇩

提案手法が最適

今後の課題

- SHEからFHEへの変換処理の高速化
- 具体的なアプリケーションを想定した実験
  ex) データマイニング，マシンラーニング
- セキュリティだけでなくプライバシを考慮した
  システムの設計

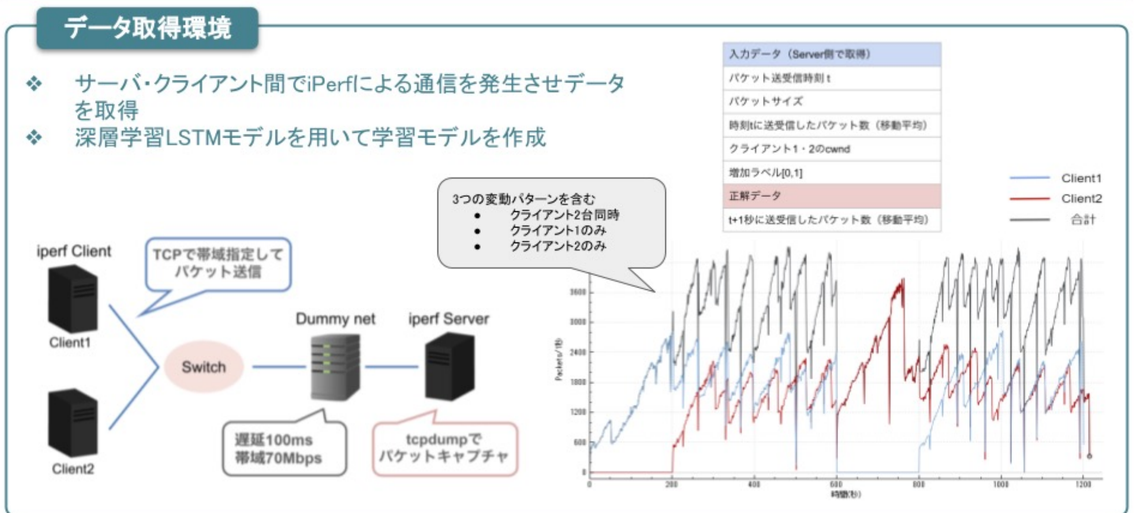
深層学習を用いた有線通信におけるネットワークトラフィック変動の予測と評価
（研究担当：明石 季利子）

研究背景

- 突然発生する通信障害の対応
  大規模災害による通信過多・DDos攻撃・同時に起こるOS アップデート等の原因で引き起こされる
  従来手法では輻輳の検知後に経路・システムの切り替えが行われる
  → サーバ・基地局が故障する可能性がある
  → 復旧に時間やコストがかかる
- TCP輻輳制御アルゴリズム
  ネットワークの輻輳によるパケットロスのようなイベントが発生してから制御するシステム
  → 早期検知により効率的なトラフィック制御を実現できることは明らか
- → トラフィックのモニタリングデータから数秒先のトラフィックの振舞いを深層学習を用いて予測する手法の提案

データ取得環境

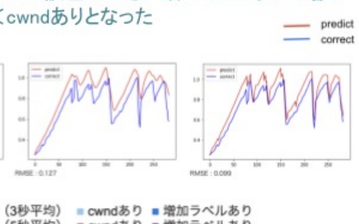
- サーバ・クライアント間でiPerfによる通信を発生させデータを取得
- 深層学習LSTMモデルを用いて学習モデルを作成



入力データ（Server側で取得）
パケット送受信時刻 t
パケットサイズ
時刻tに送受信したパケット数（移動平均）
クライアント1・2のcwnd
増加ラベル[0,1]
正解データ
t+1秒に送受信したパケット数（移動平均）

バリデーションデータを用いた予測結果

- バリデーションデータ
  学習データに含まれる3つの変動パターンでそれぞれ通信しtcpdumpを用いてサーバ側でデータを取得した

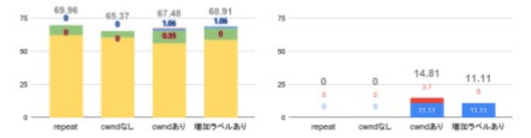


- 予測結果
  目視においてはパケット数の増減変動を予測可能であることが確認できる
  正解値とのRMSE誤差は小さい順に cwndなし＜増加ラベルあり＜cwndありとなった

性能評価

- 他手法との性能比較
  repeat：直前の状態を繰り返すことで、ある程度の予測精度ができてしまうモデル
- → 変動の内訳を用いて正解値と予測値で一致する割合（MATCH）を算出・比較する

直前の変動＼現在の変動	増加	減少
増加	変動①	変動②
減少	変動③	変動④



- cwndありのモデルはrepeatが当たらない箇所②③も予測できている
- 増加ラベルありのモデルは全体の予測精度はrepeatと並び、当たらない箇所においても優位性が見られた

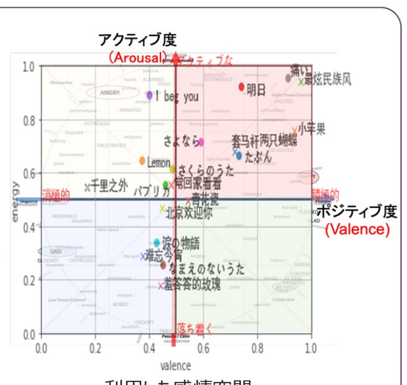
まとめと今後の課題

- MATCHの観点から提案手法の有効性を確認
- 実験環境の複雑化の検討
  （クライアント数の増加）

利用者の印象に基づく音楽レコメンドサービス
（研究担当：韓 語佳）

研究背景

- 本研究現在では、利用者の印象に基づき適切な音楽の推薦を行うことを目的とし、適切な印象語を得るためのユーザインタフェースについて考察を行っている
- 近年、音楽配信サービスが普及し、インターネット上には数百万曲以上の楽曲が配信され、また新曲も多数発表されている。一方で、音楽は単なる趣味に留まらず、音楽療法からショッピングセンターの背景まで生活の中で様々に利用されている。多数の楽曲を利用されるシーンに併せて適切に選ぶことは難しい。そこで、音楽の利用に合せた音楽推薦手法が期待されている
- 本研究現在では、一人暮らしの後期高齢者や幼い子供視覚障害者などインターネットの利用は難しいユーザを対象に、そのときの気分（印象）に合せた音楽推薦の実現をめざしている



利用した感情空間

感情空間適切さの考察

- すでに、音楽DBとしてのSpotifyが提供する音楽の定量的評価値（Arousal、Valence等）を利用し、印象語（楽しい、悲しい等）等の感情空間と音楽の関係について詳細に検討を行っている
- Spotifyは数十万曲の楽曲を提供しているが、全ての音楽を調べることには限界があるため、研究では中国語及び日本語の曲を十曲選び、Spotifyが提供する音楽データの数値により感情空間上にマッピングを行った。中国人と日本人にそれぞれアンケート調査を実施し、該当する楽曲と感情空間の関係について尋ねた
- アンケートの結果に基づき、感情空間における楽曲の位置及び印象語に関しての考察を行い、Spotifyが提供するEnergyとValenceの値を用いた感情空間上の位置として適切であることを確認した

中国曲の曲名	対応する印象語
X 套马杆/Horse Pole - Namka Tso	light hearted, convinced, enthusiastic
X 两只蝴蝶/Two Butterflies - Pang Long	light hearted, convinced, enthusiastic
X 小苹果/Little Apple - Chopstick Brothers	elated
X 最炫民族风/The Most Dazzling Folk Style - Luo Yan Si	high power/control, excited
X 常回家看看/Often Go Home to Have a Look - Gong Yue	a little active
X 难忘今宵/Can't forget tonight - Gong Yue	feel guilt
X 青花瓷/Blue and White Porcelain - Jay Chou	a little positive, impressed
X 盖答答的玫瑰静悄悄地开/A Shy Rose Is Silently Blooming - Hu Xia	melancholic
X 千里之外/Far Away - Jay Chou	distrustful
X 北京欢迎你/Beijing Welcomes You - Gong Yue	a little low power/control
日本曲の曲名	**対応する印象語**
● たぶん - YOASOBI	enthusiastic, light hearted
● Lemon - 米津玄師	impatient, suspicious
● パプリカ - 米津玄師	a little active and a little negative
● 明日はきっといい日になる - 高橋優	triumphant
● I beg you - Aimer	afraid
● なまえのないうた - DATEKEN	languid
● さよならごっこ - amazarashi	convinced
● とても痛い痛がりたい - EZFG, TOUYU	high power/control, excited
● さくらのうた - 高橋優	a little active
● 涙の物語 - 有里知花	worried

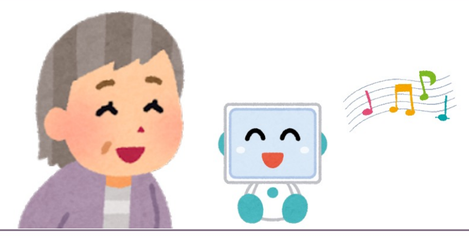
選択した中国と日本曲と対応する印象語

適切な印象語を得るためのユーザインタフェースの考察

感情空間上にマッピングされた音楽DBから利用したいシーン、気分に合せた推薦を行うためには、ユーザから適切な印象語を得ることが重要である
しかしながら、新しい技術を使えにくい後期高齢者等から情報を得るためには、ユーザインタフェースの工夫が必要となる。スマートスピーカや対話型介護ロボットが家庭内で普及し始めている現在、対話を楽しみながらその場の雰囲気に合せた、あるいは、気分に合せた印象語を得るたい
そこで、対話型介護ロボットなどにおける短い対話の中から、適切な印象語を引き出し、利用できるような対話エージェントの開発、特に数回の対話で有用な印象語を得る工夫を検討したい
既存の対話型エージェントなどをベースに、感情空間上にマッピングされた音楽ＤＢを検索するための印象語の獲得および利用時の範囲等を検討し、より少ない対話でより適切な印象語を得るための仕組みを検討したい
また、得られた印象語をより詳細な範囲に限定するための対話方法等について考察を行う
さらに、個人の嗜好を反映するために、対話中に現れる音楽への好みなどを収集し、気分を表す印象語に加え、個人の趣味を反映することで、さらに適切な音楽の推薦に向けた情報収集の工夫を検討している

今後の課題

これらの気分（印象語）に関わる入力方法を容易かつ自然に行えうことで、「楽しい音楽を聞きたい」、「誰々の曲を聴きたい」と言って、お年寄りが簡単に好きな音楽を視聴できることが期待される



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

oguchi@is.ocha.ac.jp