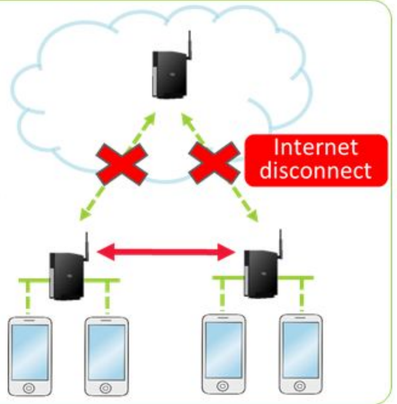
小口研究室　研究紹介　(2019年度)
(お茶の水女子大学理学部情報科学科)

避難所間における物資の共有のための運搬経路決定手法
(研究担当:佐藤　沙央)

研究背景

- 大規模災害時に、切断や遅延が発生するような劣悪なネットワークにおいても情報共有が可能なシステムの構築を行う
- 指定避難所に滞留する物資をニーズのある避難所へ送ることを考える。
- 避難所間で物資の過不足解消のための運搬経路決定手法の提案と比較を行った
- 端末側だけでもある程度動作可能にするか、あるいはローカルにサーバを設けて、非常時にはそちらへアクセスすることである程度の機能を利用可能にする。通信可能であればクラウドをそのまま利用し全てのデータアクセスと機能の利用が可能な多層構造にすることが理想的である。

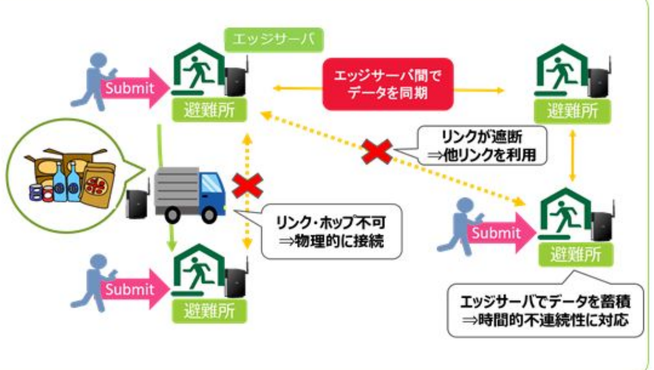


提案システム

利用形態

- 各避難所にエッジサーバが設置されており、ユーザは近くのエッジサーバにアプリからリクエストを登録
- 登録されたリクエストはお互いに張っているリンクを通して共有してアップデート

➢ リンクが一部遮断されてしまった場合
自動的に他のリンクを利用していずれデータが共有可能
➢ リンクの途絶、データのホップ不可の場合
フェリーノードで物理的に他のエッジサーバに共有
物資の運搬車をフェリーノードとすることで情報と物資を同時に運ぶことができる



運搬経路の決定手法

・一台の車が一種類の物資を積卸しを考慮しながら過不足を解消するような最短経路を考える

・巡回セールスマン問題に落とし込む
・グラフの頂点を避難所、移動時間/距離をエッジの重さ

コスト関数の定義

- Depo (物資が余っている避難所)からスタートし，他の避難所をすべて一度だけ通り最初のDepoに帰る
- Depo以外の避難所を一つ通ると荷物を一つ下す
- 車の最大積載量を設定し，それ以下であれば車に荷物がまだあってもDepoを通った時に車に載せる
- 車の荷物が無くなればそこから最寄りのDepoに取りに行く

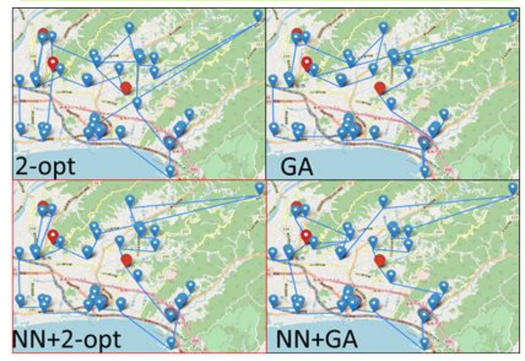
運搬経路の決定手法

高知県香南市の公開している情報をもとに指定避難所に限定して位置情報と各避難所間の距離・時間を取得

2-opt	ランダムな初期経路を与える2-opt法
GA	ランダムな初期経路を与える遺伝的アルゴリズム
NN+2-opt	Nearest Neighbor法で初期経路を与えた2-opt法
NN＋GA	Nearest Neighbor法で初期経路を与えた遺伝的アルゴリズム

実験結果

条件
・node数 : 48, item/Depo : 9, car capacity:16
・Depo数 : 5(3, 13, 21, 30, 41)　　Start Node :13



	2-opt	GA	NN+2-opt	NN+GA
実行時間(s)	49.6	3822.3	11.4	3774.8
コスト(mins)	186.9	170.7	164.3	169.5

・NN+2-optは短時間で小さいコストの経路を決定できる
→一方で局所的最適解に陥ることも多く、始点やDepoの位置、アイテム数等で変化すると考えられる

◆今後の課題
・距離データと所要時間データのどちらが有用かを調べていく
・各避難所で拾う物資の量や各避難所の必要な個数をバラバラにしてみる
・事前にGAで経路を決定しておき、それを初期経路として2-optで解いてみる

クラウド環境におけるゲノム秘匿検索に向けたシステムデザイン及び暗号スキームの比較と分析
(研究担当:山田　優輝)

研究背景

◆ ゲノムデータ委託システム

大型のストレージと計算機を所有するクラウドにデータと計算を委託
→ 膨大なゲノムデータを用いた統計処理を行うことができる
特定の文字列がゲノム配列に含まれているかどうか判定する問い合わせを行う

◆ プライバシ保護・計算量

ゲノムデータは住所などと異なり変更できない重要な個人情報
→ クラウドと相性の良い FHE によるプライバシー保護が必要
膨大なデータを暗号化して処理するため計算量が課題となる

研究内容

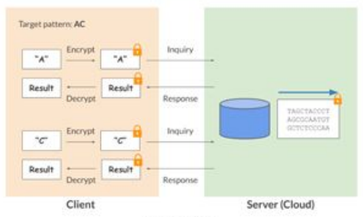
FHE を用いたゲノム秘匿検索システムの高速化及び実用化を目指し、以下の二つに関して比較・分析を行う

◆ システムデザイン

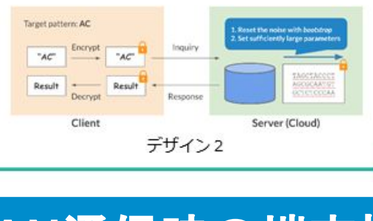
復号を保証するために三つのシステムデザインを比較する
1. 計算量の少ない問い合わせを文字数分繰り返して結果を得る
2. 一度の問い合わせで結果を得る
   2-1. Bootstrap を導入してノイズをリセットする
   2-2. 十分に大きなパラメータを指定する

◆ 暗号スキーム

以下の二つの暗号ライブラリ及び暗号スキームを比較する
- HElib により提供される BGV スキーム
- PALISADE により提供される BFV スキーム



デザイン 1



デザイン 2

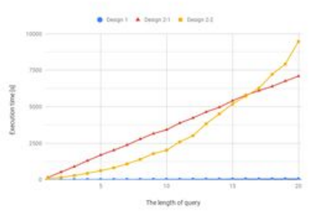
実験と分析

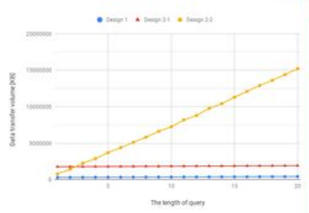
◆ 条件設定
- クエリ長:　1～8 もしくは 1～20
- ポジション数:　1～8（ダミーを含む）
- サンプル数:　1,000 サンプル
- サンプル長:　10,000 文字

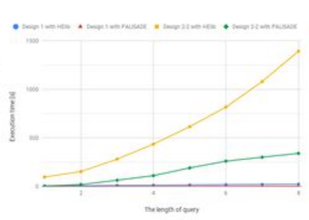
◆ 実験結果・分析

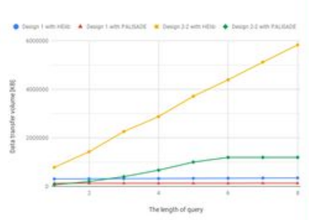
システムデザインによる比較
- 現時点で最も有力なのはデザイン2-1
- クエリ長によって適するデザインが異なる
  → デザインを切り替えることが望ましい
- 実用性のためにはより一層の高速化が必要

暗号スキームによる比較
- 総じて HElib が提供する BGV よりも PALISADE が提供する BFV の方が高パフォーマンス
- PALISADE は bootstrap をサポートしていないため、システムデザインによっては HElib を用いなければならない場合もある


システムデザインによる
サーバ上での実行時間の比較


システムデザインによる
クライアントからサーバへの
データ転送量の比較


暗号スキームによる
サーバ上での実行時間の比較


暗号スキームによる
クライアントからサーバへの
データ転送量の比較

今後の課題

- 分散環境下での比較実験
- より多くの暗号ライブラリ及び暗号スキームの比較
- デザイン1とデザイン2を組み合わせた新しいデザインの提案と比較
- 通信帯域を限定した際のデータ転送に要する通信時間の測定実験

深層学習を用いた無線LAN通信時の端末情報を考慮したパケット解析に基づく輻輳の予測
(研究担当:山本　葵)

研究背景

- スマートフォン、タブレット端末などのワイヤレスデバイスの普及によるトラフィックの増加
- 帯域の取り合いによる輻輳の発生

→
- 無線LANのトラフィックの深層学習による解析
- 解析によるトラフィックの予測
- →輻輳の極めて早期な検出、予兆の発見

帯域をコントロールして使うことが必要　　輻輳が起こることを予想して制御

実験概要

アクセスポイントに接続した複数のAndroid端末からiperfによってデータをサーバに送信、データの取得

- カーネルモニタ
通信時におけるLinuxシステムのカーネル内部の処理を解析するシステムツールで、カーネル内部のパラメータ値の変化を記録可能

実験①
カーネルモニタで通信中の各端末のTCPパラメータを出力、輻輳状態の観察
実験②
深層学習を用いて輻輳発生時のAPまわりのパケットの解析、予測実験

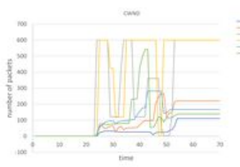
実験結果

実験1 通信中の各端末のTCPパラメータの観察

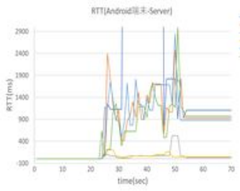
- データ通信(3600秒)
- 端末5台で同時通信

出力
- 各端末のCWNDサイズ
- 各端末のスループット

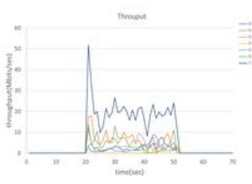
学習に用いるデータ



端末3と端末4の2台が帯域の大部分を圧迫している



通信開始直後から値は大幅増加
キューが溜まるのが早くパケットの処理が追い付かなかったと考えられる



CWND値が小さくなるときにスループット値も減少
→十分なスループットを確保できていない

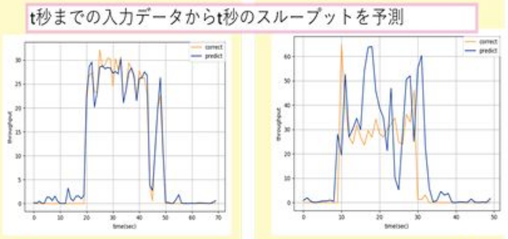
実験2 深層学習を用いた予測実験

学習に用いるデータ

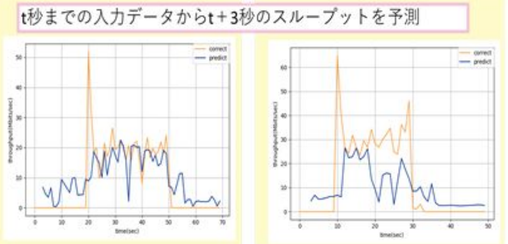
入力データ(特徴量)		正解データ
1秒間	[length sequence_number … etc …cwnd1 … cwnd N]（1パケット+cwnd）	スループット
	[length sequence_number … etc …cwnd1 … cwnd N]	
	…	
	[length sequence_number … etc …cwnd1 … cwnd N]	

学習データ(70秒)(20-50秒で通信)を用いた予測
テストデータ(70秒)(10-30秒で通信)を用いた予測

t秒までの入力データからt秒のスループットを予測



t秒までの入力データからt+3秒のスループットを予測



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

oguchi@is.ocha.ac.jp