小口研究室　研究紹介　(2016年度)
(お茶の水女子大学理学部情報科学科)

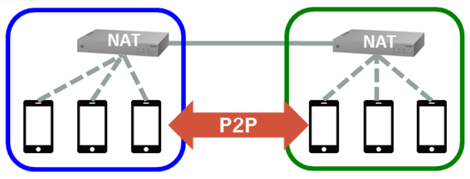
インターネット非接続時における複数NAT越えP2P通信方式の検討
（研究担当:田中 有彩）

研究背景

平常時のネットワークは
クライアント・サーバ型通信であり、NAT配下にある
⇒しかし…災害時には被災域外への通信の遮断・輻輳より情報共有ができない

災害時にも情報共有可能なアプリケーションに必要な接続環境を用意したい

研究目的



NATであるルータに仕組みを作り、ルータ同士のMANETを構築しP2P型通信によりデータを共有する

研究概要

平常クライアントはNAT配下にあり、
NATからインターネットへつながっている
しかし逆に、インターネットからNAT配下の端末へは直接通信できない

⇒NAT越えという技術を使用する

◆ NAT越え
NAT配下の端末やネットワークへ、インターネット側からダイレクトに到達可能にする技術のこと
多くの技術があるが、今回は「ICE」を使用

◆ ICE(Interactive Connectivity Establishment)
STUNやTURNなどによるNAT越えの手順をまとめたもの
具体的には通信できそうな候補を集め、シグナリングにより相手とその候補を交換し相手との通信を試みる仕組み
これによりクライアント同士のP2P通信を可能にする

◆ STUN(Session Traversal Utilities for NATs)
通信するホストがSTUNサーバにUDP接続を行い、NATが割り当てたグローバルIPアドレスとポート番号を取得する
フルコーン型・制限コーン型・ポート制限コーン型に対応

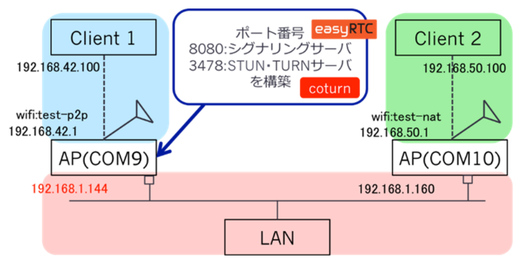
◆ TURN(Traversal Using Relay NAT)
すべての通信をTURNサーバ経由で行う
そのためシンメトリック型にも対応するが、P2P通信ではなくなり、サーバ的にも高負荷となる

◆ シグナリング
Peerの情報であるSDPと通信経路の情報であるICE candidateを仲介する役割
これによりP2P通信を可能にする

これらの技術を用いた「WebRTC」という
ブラウザでリアルタイムコミュニケーションを実現するための仕組みを利用する

ローカルでの実験

プライベートネットワーク内で情報共有ができるかどうかを試すため、以下の通りに環境を構築



◆既存技術ではNATとサーバが分かれていたが、NATであるAPにサーバが含まれている
◆APは無線LANを搭載したDebian GNU/Linux8 ubilinux サーバ2 台にそれぞれhostapdをインストールし、Wi-Fi AP兼NATルータとして動作

Client1から2へ2MBのファイルを送信できるかを試す

実験結果

◆Client1でのパケットキャプチャ

Source	Destination	Protocol	Info
192.168.42.100	192.168.1.144	DTLSv1.2	Application Data
192.168.42.100	192.168.1.144	DTLSv1.2	Application Data
192.168.1.144	192.168.42.100	DTLSv1.2	Application Data
192.168.42.100	192.168.1.144	DTLSv1.2	Application Data
192.168.42.100	192.168.1.144	DTLSv1.2	Application Data
192.168.42.100	192.168.1.144	DTLSv1.2	Application Data
192.168.42.100	192.168.1.144	DTLSv1.2	Application Data

プロトコルDTLSでClient1とサーバ間でP2P通信している

◆Client2でのパケットキャプチャ

Source	Destination	Protocol	Info
192.168.1.144	192.168.50.100	STUN	ChannelData TURN Message
192.168.1.144	192.168.50.100	STUN	ChannelData TURN Message
192.168.1.144	192.168.50.100	STUN	ChannelData TURN Message
192.168.1.144	192.168.50.100	STUN	ChannelData TURN Message
192.168.1.144	192.168.50.100	STUN	ChannelData TURN Message
192.168.50.100	192.168.1.144	STUN	ChannelData TURN Message

Client2 とサーバ間でTURNによる情報共有が行われている
このときプロトコルが「STUN」となっているが、これは Wiresharkの仕様による表記であり、本来はTURNプロトコルが使用されている

TURNでの情報共有に成功(NAT越え可能)

まとめ・今後の課題

◆まとめ　ローカルにおけるNAT越え実験を行い、TURNによる情報共有を確認した

◆今後の課題
・STUNを用いてP2P通信を可能にする
・複数サーバがあった場合、どう情報共有するかの検討

完全準同型暗号を用いたゲノム秘匿検索の分散処理による高速化
（研究担当:山本 百合）

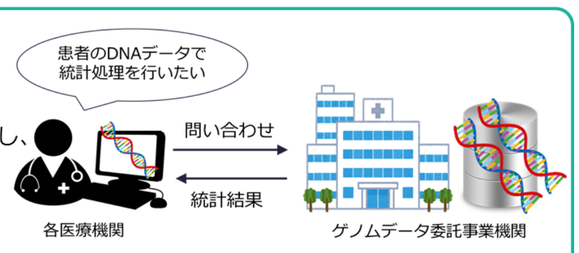
研究背景

◆ ゲノムデータ委託システムの必要性

膨大なゲノムデータを用いた統計処理を行うために大型の計算機を所有する機関にゲノムデータを委託し、計算結果の問い合わせを行うシステム

◆ ゲノムデータは個人を特定する識別子

暗号化によるデータのプライバシー保護が必要
問い合わせ内容とゲノムデータを暗号化した状態で計算



双方の情報を相手に秘匿しながら統計処理が可能な委託システム

提案手法

◆ 完全準同型暗号の利用

加法と乗法で準同型性が成立する完全準同型暗号を利用し、サーバ・クライアント双方のデータを秘匿

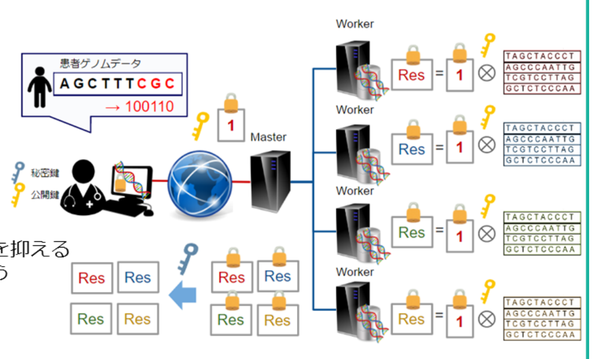
完全準同型暗号は**計算量が大きい**ため、サーバ側の計算時間が長い ⇨ **サーバ側の処理の分散化で高速化を目指す**

◆ マスタ・ワーカ型分散

マスタとワーカに役割を分担し、クライアントとの通信回数を抑える
今回はサンプルごとのデータ分割による分散処理で実験を行う

◆ プログラム実装方法

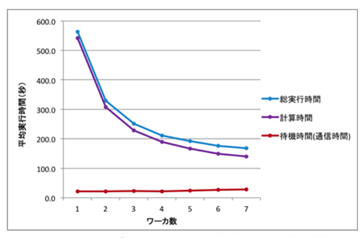
C++で実装、マスタとワーカの制御にOpen MPIを使用
完全準同型暗号計算にHElibライブラリを使用



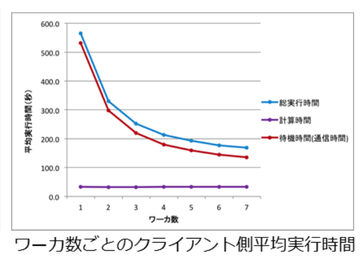
実験と考察

◆ 平均実行時間測定実験

- 分散台数が増えるにつれて平均実行時間が減少
- 実行時間は徐々に横ばいになる
- クライアント側の復号計算はワーカ数による変化は小さい
- 各ワーカ間の計算時間のばらつきは小さい



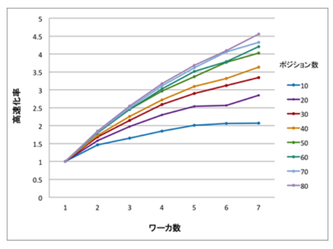
ワーカ数ごとのマスタ側平均実行時間



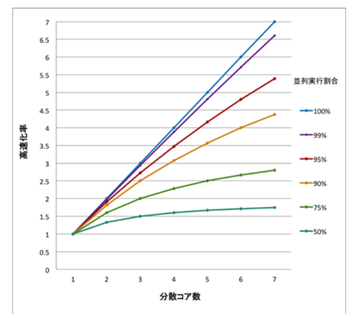
ワーカ数ごとのクライアント側平均実行時間

◆ 各ポジション数における高速化率測定実験

- 高速化率＝逐次実行時間/並列実行時間
- ダミー検索を含めたポジション数ごとの実験
- ポジション数が多いほど分散化効果が大きい



ポジション数におけるワーカ数ごとの高速化率



Amdahlの法則に基づいた
並列実行時間割合別高速化率予測曲線

◆ Amdahlの法則による考察

- 高速化率 $\leqq \dfrac{1}{(1\text{-並列実行時間の割合}) + \dfrac{\text{並列実行時間の割合}}{\text{分散コア数}}}$
- ポジション数80の時の理想的な最大高速化率は10倍程度

今後の課題

◆ 計算手順やデータ構造に着目した分散処理による高速化
◆ クラウドコンピューティングを想定した環境での実験
◆ 複数回通信を必要としないゲノム秘匿検索システムへの適用

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