WIDE Technical-Report in 2007

WIDE-CNRS間の交換留学活動報告

wide-tr-mawi-widecnrs-masui-00.pdf

WIDE Project : http://www.wide.ad.jp/

WIDE–CNRS間の交換留学活動報告

益井 賢次 (kenji-ma@is.naist.jp)

2006年12月25日

1 概要

WIDE Projectとフランス国立科学研究センター（CNRS）の間での研究協力の一環として、両組織間で人的交流・学術的交流を目的とした、学生の交換留学制度を設けている。この交換留学生として、2006年9月14日から同年12月12日にかけて約3ヶ月間渡仏した。受入組織は、パリ第6大学情報処理研究所（Laboratoire d'informatique de Paris 6; LIP6）内のNetworks and Performance Analysis group（NPA）で、同組織のKavé Salamatian助教授を中心に受入体勢を整えていただいた。

滞在中は両組織間の研究協力関係に沿って、以下のような活動をした。まず、自身の研究活動の周知のため、CNRSに関連する研究イベントに参加し研究発表を行い、また人的交流も深めた。その上で、自身の研究に関連の深い研究者と直接議論することで、より具体的な研究協力関係の構築に努めた。

2 研究イベントへの参加

在仏中、いくつかの研究イベントに参加し、CNRS関係者との交流を深めるとともに研究内容について意見を交換した。ここでは、それらのイベントの内容について報告する。

2.1 CNRS/INRIA/WIDE Meeting

2006年9月18日・19日に、フランス・パリ市内のCNRS本部で行われたCNRS/INRIA/WIDE Meetingに参加した。本ミーティングには、CNRS・フランス国立情報学自動制御研究所（Institut National de Recherche en Informatique et en Automatique; INRIA）およびWIDE Projectのそれぞれの研究者らが参加し、measurementとmobilityの各セッションに分かれて研究発表を行った。

図 1: パリ第 6 大学・LIP6

このミーティングには先述の研究協力プロジェクトの関係者が多く参加することもあり、実質的に顔合わせのためのミーティングとなった。ミーティング中、CNRS 側の関係者の紹介を受けるとともに互いの研究内容について概説し合い理解を深めた。また、関連の深い研究に携わる研究者らとは後日個別に面談し、研究協力の体制について話し合うことを約束した。

2.2 NPA 内での研究発表

2006 年 10 月、フランス・パリ市内の LIP6（図 1）で行われた NPA によるミーティングに参加し、自身の研究発表を行った。NPA は、主にネットワークトラフィックの数学的な解析手法を研究対象とするメンバーから構成される。約 10 名の NPA メンバーが参加する中で、互いの研究内容について議論した。

自身の研究 [1] の中心となるテーマが、彼らの研究対象であるトラフィック解析手法を実装するための基盤であることもあり、互いに研究内容を補完できる関係で意見交換が行われた。こちら側の研究内容に関しては、基盤技術を利用する当事者から要望や意見が得られた点で有意義であった。

2.3 MetroSec Project での研究発表

MetroSec Project [2] は、ネットワークトポロジなどインターネットに関わる様々な特性を収集する手法について研究を行っている研究グループで、研究協力プロジェクトの CNRS 関係者も多く参加している。2006 年 10 月にフランス・リヨンの ENS Lyon 内で行われた MetroSec ミーティングで研究発表を行い、意見を交換した。

CNRS のコアメンバーも多く参加するミーティング内で研究発表を行いその内容を周知させるとともに、当該分野の第一線の研究者から指摘・意見をいただくことができた。

3 研究協力

前述の数回の研究イベントへの参加を経て、研究活動において具体的に協力していくため、自身の研究内容に関連の強い研究者と直接対話した。その上で、2 つの研究プロジェクトについて協力していくこととなった。

3.1 大規模トポロジ収集プロジェクト（traceroute@home）

traceroute@home Project [3] は、インターネット上に分散配置されたエンドノードが各々IP ネットワークトポロジを収集し、得られた情報を統合することによりインターネット全体のトポロジ情報を構築することを目的としている。このプロジェクトには CNRS のメンバーである Timur Friedman 助教授も関わっており、現在も活動が続いている。traceroute@home Project の研究課題は大きく 2 つに分けられる。1 つは、大規模・広域に展開するインターネットにおいてトポロジ情報を収集するために有効な計測手法を研究することである。もう 1 つは、そのような手法を実際にインターネット上で適用できる計測基盤のアーキテクチャについての研究である。

前者の計測手法については、Doubletree [4] と呼ばれるトポロジ情報の収集手法が traceroute@home Project から提案されている。この協調計測アルゴリズムでは、各計測ノードがトポロジ情報の収集のために IP パケットの TTL 値を漸増させる手法（いわゆる traceroute の方式）を用いる。その上で、ある計測ノードは他の計測ノードが収集したトポロジ情報のグラフの中から共通部分を抽出し、自身が行うトポロジ情報の収集範囲をその共通部分に重複しないように調節する。このようにして重複したトポロジ収集活動を避けることで、収集活動に伴うネットワーク資源の消費を押さえ、トポロジ情報の収集の効率化を図っている。重複部分の開始点を示すデータセットは stop set と呼ばれ、各計測ノードが収集結果に基づいて協調して構築していく。

また、Doubletree のような協調計測アルゴリズムを適用できる計測基盤についての研究も行われている。traceroute@home v1 と呼ばれる計測基盤で

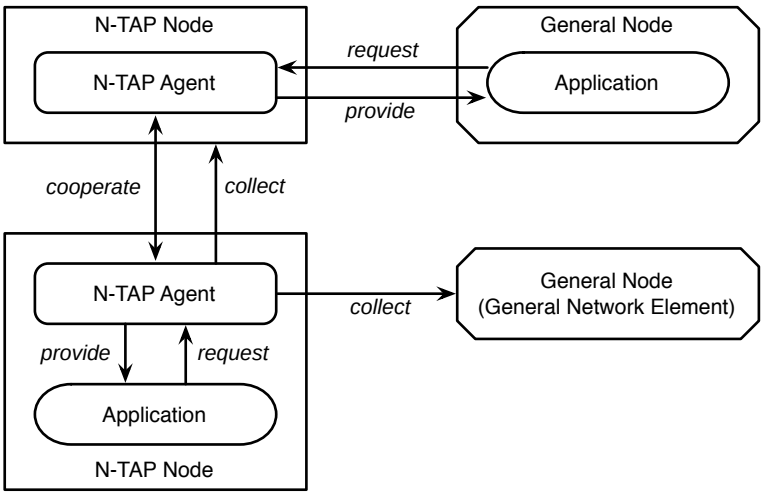

図 2: N-TAP とそれを利用するアプリケーションとの関係

は、計測ノード間で片方向リング状の計測ネットワークを構築し、stop set を含むデータを回覧・修正していくことで Doubletree を実際に適用していた。この基盤の問題点として、リング状ネットワークに属するホストが 1 台でも故障すると stop set の回覧が途切れ計測ネットワークが機能しなくなる点、次第に大容量化する stop set を計測ノード間で交換する際のネットワーク負荷の高さ、リングネットワーク中の各ノードの性能が計測ネットワーク全体の性能に直接影響する点などが挙げられている。

そこで、traceroute@home v1 の改善版として traceroute@home v2 が現在策定中である。traceroute@home v2 では、分散ハッシュテーブル（Distributed Hash Table; DHT）の一実装である OpenDHT [5] ベースの共有ストレージに stop set を含むデータを蓄積することで、先述の問題の解決を図ろうとしている。共有ストレージの構成ノードは、必ずしも計測ノードである必要はない。

一方で、我々が研究・開発を進めている計測基盤 N-TAP [1] は、計測ノード間の通信と分散共有ストレージの機能を提供する、協調計測・分散計測の実現を目的とした計測基盤である。N-TAP では、計測ノード間で DHT ベースのオーバレイネットワークを構築し、その上に協調分散計測アルゴリズムで最も重要となる、共有ストレージおよび計測ノード同士のランデブーを実現する機構を備えている。図 2 のように、N-TAP では計測エージェントがエンドノード上で動作し、計測活動を行う。また、エージェントはアプリケーションからの要望に応じてネットワーク特性の提供も行う。図 3 は、N-TAP エージェントの内部コンポーネントとそれらの間の関係を示している。エージェントは、アプリケーションからの要求を受付けネットワーク特性を提供

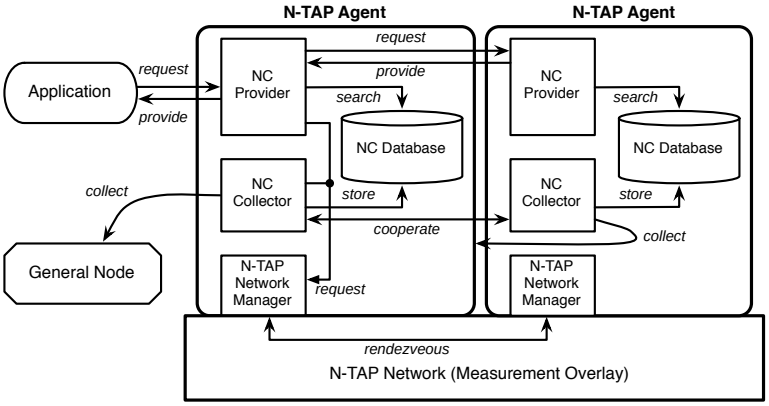

図 3: N-TAP のコンポーネント間の関係

する provider、実際の収集活動を行う collector、計測オーバレイネットワークを構成し計測ノード間の協調活動を管理する network manager、分散共有ストレージの一片となる database から構成され、それぞれが連携しつつ全体として動作する。現在、N-TAP は PlanetLab [6] を始めとした数種のプラットフォームで動作することが確認されている。

traceroute@home v2 の根幹となる機能要件は、先述したとおり規模拡張性をもった共有ストレージを用意することである。さらに、従来通り計測ノード間の通信機構も必要となる。これらの機能は N-TAP 上で実現可能であると判断したため、将来の研究活動において互いに補完し合うことのできる事項があるかについて、Timur Friedman 助教授と直接議論した。議論では、traceroute@home v2 での要件の洗い出しと N-TAP ですでに実現可能である機能の列挙を行い、traceroute@home v2 が N-TAP 上で実現可能であることを確認した。また、双方のシステムについての改良すべき点について議論した。ただし、traceroute@home v2 の開発において、議論の時点ですでに開発者の雇用が完了している段階でその取り消しが難しい状況であったので、早急に traceroute@home のプラットフォームを N-TAP のみに移行することは難しいという。このような事情を考慮し、当面は独立して各々のシステムの研究・開発を続け、双方のマイルストーンに達した時点で成果を統合することで合意した。そのため、日本帰国後も互いに連絡を取り続ける体勢をとっている。現時点（2006 年 12 月）で、双方での開発作業が続行中である。

3.2 TCP トラフィックの初動分析によるアプリケーション識別手法の研究

Kavé Salamatian 助教授らが関わる研究の一つに、TCP トラフィックのセッション初期の傾向を分析することで、そのトラフィックがどのプロトコルに準じたものであるかを識別する手法 [7] がある。TCP トラフィックに含まれるポート番号を判断基準にした従来の識別法では、通常使用されるものとは異なるポート番号で運用されているサービスに起因するトラフィックを判別することができない。また、パケットのペイロードを逐一検査してプロトコル判別を行う手法は CPU 資源などの消費が大きく、大量のトラフィックの判別が必要な場合に規模拡張性がない。さらにどちらの手法も、Peer-to-Peer アプリケーションなどに起因する暗号化された任意のポート間のトラフィックについては、識別が難しい。このような従来の手法の欠点をふまえた上で、この研究は TCP トラフィックの数パケットの特性を分析することで、高速にトラフィックの識別を実現することを目的としている。

この手法では、ひとつの TCP セッションについて、その開始からの数パケットを分析対象とする。分析の指標となる項目は、トラフィックの方向（2 ノード間通信であるので、2 方向のいずれか）とパケットサイズである。これらの指標を用い、K 平均法・ガウス混合分布などにもとづくトラフィックのクラスタリングを行ってプロトコル別に分類する。現在、この手法は Early Application Identification と呼ばれている。

本研究では、識別可能なトラフィックの種類の拡充を図る一方で、人間の動作により生じるトラフィックとボット（bot）のようなプログラムにより機械的に生じるトラフィックの識別が可能であるかについても、検証の課題としている。ボットを利用した、ネットワークおよびホストを対象とする DoS 攻撃およびネットワークゲームにおける不正行為など、機械的に生じるトラフィックに起因するセキュリティ上・サービス展開上の問題・妨害は後を絶たない。対策の第一歩として、このようなトラフィックを識別することは重要である。本件に関して、Kavé Salamatian 助教授より研究協力の要請を受け、研究へ荷担することとなった。

まず、先述の対象トラフィックの拡充という点で、ゲームトラフィックの識別を行うことになった。現時点で Early Application Identification が適用されたアプリケーション（プロトコル）は、NNTP・POP3・SMTP・SSH・HTTPS・POP3S・HTTP・FTP・eDonkey・Kazaa であり、ゲームトラフィックの識別は未検証である。Early Application Identification がゲームトラフィックに対して適用可能であるかを検証するために、ゲームトラフィックを含むトラフィックデータセットを用意する必要がある。そのため、既存のネットワークゲームの調査から実験環境の構築までを引き受け、行った。現時点（2006 年 12 月）で、ゲームサーバ環境の整備が完了し、参加者数人程度で小規模なゲームプレイを試行し、その結果を解析する体勢までが整った。

今後、フランス国内の各所から実験協力者を募り、可能であれば日本からも協力者を用意して大規模な実験を行う。本実験では、正規のプレイヤに加えて、ボットプログラムが操作するプレイヤもゲーム内に参加させる。その上で、取得したデータセットを解析して Early Application Identification のゲームトラフィックへの適用可能性を検証するとともに、機械的に生じるトラフィックの識別手法についての検討も並行して進めていく。本実験は 2007 年 1 月に実行予定で、今後も Kavé Salamatian 助教授との協力関係のもと、ネットワークオペレーションおよびトラフィック分析の両面から共同で研究を進める。

4 まとめ

WIDE Project と CNRS との間の交換留学生として渡仏し、研究発表と研究者との議論を通じて、2 つの研究プロジェクトについて協力することとなった。研究協力の 1 つは、traceroute@home Project に対するネットワーク計測基盤技術の提供、もう 1 つは Early Application Identification と呼ばれる手法に関する実験協力である。これらの研究協力関係は、これからも継続される。

参考文献

[1] K. Masui and Y. Kadobayashi, *N-TAP: A Platform of Large-Scale Distributed Measurement for Overlay Network Applications*, DAS-P2P 2007.

[2] MetroSec Project
http://www.laas.fr/METROSEC/

[3] traceroute@home Project
http://traceroutеathome.net/

[4] B. Donnet, P. Raoult, T. Friedman and M. Crovella, *Efficient Algorithms for Large-Scale Topology Discovery*, ACM SIGMETRICS 2005.

[5] S. Rhea, B. Godfrey, B. Karp, J. Kubiatowicz, S. Ratnasamy, S. Shenker, I. Stoica and H. Yu, *OpenDHT: A Public DHT Service and Its Uses*, ACM SIGCOMM 2005.

[6] PlanetLab
http://www.planet-lab.org/

[7] L. Bernaille, R. Teixeira and K. Salamatian, *Early Application Identification*, CoNext 2006.