論文内容の要旨

論文題目

A Study on Algorithms
for Efficient Multi-Point Communication
in Autonomous Distributed Networks
（自律分散ネットワークにおける効率的多地点間通信のためのアルゴリズムの研究）

氏　名　谷　誠一郎

IPネットワークの出現以来、データ通信は急速に人々の生活に浸透し、必須なものとなってきた。最近では、単純な1対1通信よりも、むしろ、WWW，ライブ放送、TV会議など多地点が関わる通信が主流となっている。このようなデータ通信が急速に普及した大きな理由の一つは、IPネットワーク上では、専門家以外の人々にとっても魅力的なアプリケーション、特に上記のような多地点間通信アプリケーションが簡単に実現できることである。他の大きな理由としては、IPネットワークは、自律分散的に動作し拡張できるためである。すなわち、ネットワークを構成する一つ一つの機器がネットワークの局所的情報によってのみ動作するため(自律分散的動作性)、ネットワークが巨大化しても対応でき、また、ネットワークに新たな機器・機能を導入する際に、他の機器・機能に与える影響が局所的である（自律分散的拡張性）であるため、ネットワークの各部分で独立に拡張していくことが可能である。

このような自律分散性は、パケットごとに宛先を持たせ、ルーターなどの各ネットワーク機器において、パケットごとに独立して処理することにより実現されている。しかし、皮肉なことに、このことが通信トラフィックの厳密な制御を困難にしている。この種のネットワークは、ユーザが増え、通信トラフィックが増えれば、輻輳が起こり、ネットワーク全体のサービス低下を招く問題を抱える。特に、多地点間通信では、特定の箇所に通信トラヒックが集中しやすいため、深刻である。このため、自律分散的性質を損なうことなく、多地点間通信を効率化することは極めて重要な研究課題となっている。単純な方法としては、多地点間通信を構成する一対一通信の効率性を向上させることが考えら

れる。しかし、多くの多地点間通信では、このような単純な手法では、必ずしも十分に効率を上げることが出来ない。このため、アプリケーションの動作を考慮することが必要となる。

多地点間でのデータ通信は、アプリケーションの動作に応じて、大きく、蓄積型データを時間差で多数の受信者に送るファイル配信型、と、蓄積型または非蓄積型データを同時に多数の受信者に送るストリーム型に分けることができる。

ファイル配信型多地点間通信に関しては、過去に送られたファイルのコピーをネットワーク内に保持(キャッシュ)しておき、後に、別の受信者から同じファイルへの要求があったときには、保持してあったコピーを送信することで、通信量、転送時間、コンテンツサーバー(ファイルを持つホスト)への負荷を低減する技術、すなわちネットワークキャッシュが代表的である。最も基本的な使われ方では、ネットワークキャッシュを行う各ノード(キャッシュサーバー)は、ネットワーク内の輻輳が起こりやすい箇所に設置され、自律分散的に動作する。このため、キャッシュサーバー個々の性能が、全体の通信効率に深く関係する。キャッシュサーバー単体の性能を、限られた記憶容量の下で、最大化するためには、どのファイルをキャッシュするかという判断が大変重要である。なぜなら、すべてのファイルをキャッシュに入れておくことはできないからである。この問題は、「ファイルキャッシュ問題」と呼ばれる。ファイルキャッシュ問題の困難さは、「各ファイルをキャッシュするべきかどうかは、将来、そのファイルが必要になるかどうかで決まるにもかかわらず、多くの場合、将来の情報は全く分からない」、という点にある。

本論文では、この種の問題に対するアルゴリズム解析によく使われる競合比解析に基づいた、ファイルキャッシュ問題に対する二つのアルゴリズムを提案する。提案アルゴリズムは、キャッシュ・ミスヒット時に起こるファイル転送に伴う通信コストに関して、その最悪値を競合比解析により理論的に保証しつつ、実際的場面でのヒット率向上または処理の高速化を目指したものである。具体的には、第一のアルゴリズムは、実験的には高いヒット率を達成するが理論的な性能が保証されていない発見的手法が与えられた場合に、その発見手法を基に理論的に性能を保証できるアルゴリズムを生成する汎用アルゴリズムである。また、第二のアルゴリズムは、ランダム化手法を取り入れることにより、既に提案されている最良の競合比を持つ決定性アルゴリズムと同等の性能を理論的に保証しながら、処理を高速化したアルゴリズムである。提案アルゴリズムに対して、実際のWWWの代理サーバのログを用いて実験を行い、その効果を確認した。

ストリーム型多地点間通信に関しては、リアルタイムな画像や音声データのように、多数の受信ホストに同時に送信する必要があり、また、データに切れ目がない場合があるので、ネットワーク内にコピーを保存することで対応することはできない。しかしながら、コンテンツサーバーが多数の受信者と一対一通信を行っていたのでは、ネットワークの帯域をいたずらに消費し、また、コンテンツサーバーにも、非常に大きな負荷がかかる。このため、ストリーム型多地点間通信に対しては、ネットワーク内に、必要に応じて、ストリームデータをリアルタイムにコピーする分岐点を設けることで、サーバを根とし、多数の受信ホストを葉とする、ツリー型配信経路を構成し、通信を効率化する手法「マルチキャスト」が一般的である。

これまで、多くのマルチキャスト方式が提案され、またその一部は、標準化され、 IP マルチキャス

ト と呼ばれている。IP マルチキャストは、同一ストリームデータの受信ホスト集合を、グループアドレスと呼ばれる特殊なアドレスにより識別している。ホスト毎に割り振られるアドレス（ユニキャストアドレス）と比べて、グループアドレスは、受信ホストの「集合」に付与される点に加え、いくつかの全く異なる点がある：（1）時間とともに、同じグループアドレスを付与されているホストの集合が変化する点、(2) 同じグループアドレスを付与されているホストの位置は、一般に、ネットワーク内の物理的位置に無関係である点、である。このため IP マルチキャストは、独自のアドレス管理機構や複雑な経路制御プロトコルを必要とする。結果として、自律分散性の点で問題があり、研究が始まって数十年たつが、実験網や単一組織で管理するネットワークの中だけの使用に留まっている。このような状況に対し、近年、マルチキャストのツリーの各枝をユニキャスト（一対一通信）として実現することで、これらの問題を解決する手法が注目されている。

本論文では、この手法を用いた、新たなマルチキャストプロトコルを提案する。提案プロトコルは、キャッシュサーバー同士の動作と非常に良く似た仕組みを取り入れることにより、極めて自律分散的にツリー型配信経路（マルチキャストツリー）を構築・管理する。例えば、ユニキャストの経路の変化や、送信者・受信者の移動に対応して、自律分散的にマルチキャストツリーを再構築することができる。ところで、この種のマルチキャストプロトコルは、多くの場合、端末から送信されるパケットによりネットワーク内で分岐点となるノードの内部状態を変化させる。しかし、悪意のある受信者・送信者を仮定した場合、このような性質は、ネットワークを危機的状況に陥れる可能性をはらむ。本論文では、多少の自律分散性と引き換えに、悪意のある受信者・送信者からの攻撃に対する耐性がある改良型プロトコルも合わせて提案する。また、提案プロトコルの実装を行い、日米間での実証実験によりその動作を確認した。

これまで、現在のネットワークにおいて、二つの代表的なタイプの多地点間通信に対して効率化手法を述べてきた。これらの手法のアイデアは、将来のネットワークが現在のネットワークと同様の基本動作をもつ限り、将来にも有効であろう。しかし、将来の多地点間通信に備えるためには、新しいタイプのネットワーク、とりわけ、全く異なった原理に基づくネットワークについても、多地点間通信という観点から、検討しておくことが必要である。そのような新たなネットワークを実現する技術として、量子通信技術（データ処理を行う量子計算技術を含む）が近年注目されている。これは、量子力学的効果を利用する通信技術であるため、現在とは全く異なる多地点間通信を実現する可能性がある。

実際、量子通信は、一対一通信でさえ、現在の通信とは非常に異なる性質を持つことが知られている。 一対一量子通信における、最も顕著な成果は、暗号における、量子鍵配送プロトコルであろう。このプロトコルを用いることにより、無限の計算能力を持つ盗聴者に対してさえ、二者間で安全に秘密鍵を共有することができる。このような方法は、量子通信を使わない「現在のネットワーク」で実現する方法は知られていない。つまり、量子通信を用いることにより、秘密鍵暗号を利用する際の安全性を飛躍的に高めることができる。一方で、1994 年に発見された、素因数分解を行う多項式時間量子アルゴリズムは、現在広く使われている公開鍵暗号であるRSA暗号の安全性を脅かした。なぜなら、RSA暗号は、素因数分解の困難性に安全性の理論的根拠を置いているからで

ある。すなわち、もし量子計算機ができれば、RSA暗号が破られ、現在の安全な多地点間通信を脅かすことになる。悪意を持った通信者を仮定しない、純粋に効率的通信を追求する研究では、通信複雑さの理論を中心に多くの研究が行われている。 例えば、一対一量子通信においては、ある種の人工的な分散計算問題に対して、非量子通信に比べて、量子通信は指数倍効率的であることが明らかになっている。しかし、多地点間通信における量子通信の能力は、まだ不明な点が多い。

本論文では、多地点間通信を要し、かつ、極度に自律分散性が求められる代表的な分散計算問題である、匿名リーダ選挙問題を取り上げ、量子通信可能なネットワーク上で解くための効率性について理論的に検討する。匿名リーダ選挙問題は、量子効果を使わない現在のネットワークでは、誤りが許されない場合、有限時間では解けないことが良く知られている。すなわち、最悪ケースでの通信量を保証することはできない。本論文では、量子通信ネットワークを仮定した場合に、匿名リーダ選挙問題を有限時間かつ誤り無しで解くアルゴリズムを提示する。すなわち、量子通信を用いることができれば、誤りが許されない場合でも、最悪ケースでの通信量を保証できることを示す。