2008年10月24日
アラクサラネットワークス株式会社

高速通信トラヒックモニタリング技術を開発
～10Gbit/sを超えるトラヒックから異常通信フローをリアルタイムで抽出し ネットワーク障害解析などに利用可能～

アラクサラネットワークス株式会社（本社： 神奈川県川崎市 代表取締役社長 和田宏行 以下アラクサラ）は、10Gbit/s回線をモニタし、ネットワークの障害原因分析やコンピュータウィルスの活動検出などを容易に行える技術を開発しました。

今日、重要な社会インフラとなったネットワークにおいて、ネットワークを介してサーバやルータなどのサービスを妨害するDDoS攻撃(*1)、コンピュータウィルスやWorm(*2)によって発生する多量の異常フロー、P2Pファイル交換(*3)による帯域占有などが社会問題化しています。このためネットワークの管理運用を行う場合には、これらの異常フローをいち早く検知して、帯域制御やフィルタリングといった処理を実施し、ネットワークの正常な動作を確保することが重要となっています。

一方、ネットワークの高速大容量化の進展により、異常フローを検出するための解析処理自体の高速化が課題となっています。

アラクサラではこの課題に対処するために、以下の技術を開発しました。

- データマイニングの手法を応用し、IPアドレスやポート番号などといったパケットヘッダ情報のパターンをモニタし、頻出する組合せを抽出する「バスケット解析(*4)」と、出現するパターンが何種類あるかを高速で数える「異なり数計測(*5)」を組み合わせた、新たな異常フロー抽出技術(*6)。演算処理量が少なく、限られたメモリ容量で実行可能なことが特長。
- メモリアクセス量を最適化することにより高速処理を実現する「二段階集約方式(*7)」と「複数データー括更新方式(*8)」による高速回線対応技術。

この結果、約18Gbit/s（*9）のトラヒックをリアルタイムで解析し、異常フローを抽出できることをシミュレーションにより確認しました。

従来、ネットワーク上でのフロー解析には、インタフェース統計やsFlow、NetFlowといったフロー統計機能が利用されて来ましたが、高速回線ではフロー統計情報そのものが増大するため、回線上を流れるデータの全てを処理できず、一部分をサンプリングして処理をする必要がありました。このため、モニタリング精度の低下が懸念されています。10Gbpsを超える回線ではこの問題はさらに顕著になると見込まれますが、本方式では、前述の高速解析技術により、回線上を流れるデータの全てを対象に、リアルタイムのデータマイニング処理を行うため、高速回線でも精度の高い異常フロー検出が可能となります。

アラクサラネットワークスでは、今後本技術の実用化を進め、製品などに搭載して行くと共に、さらに40Gbit/sクラスのネットワークに適用すべく高性能化の研究開発を進める予定です。

なお、本技術については、10月23日～24日に沖縄県国頭郡恩納村の独立行政法人情報通信研究機構沖縄亜熱帯計測技術センターにて開催されております、インターネットコンファレンス2008にて発表を行います。

また、本開発の一部は、独立行政法人新エネルギー・産業技術総合開発機構が2007年度から実施している、「次世代高効率ネットワークデバイス技術開発」(プロジェクトリーダー:東京大学 浅見徹教授)により実施したものです。

別紙： 本技術によるトラヒック分析結果の例

*1 DDoS攻撃： Distributed Denial of Service 複数のPCやサーバから特定のターゲット（Webサーバなど）に対してパケットを集中的に送りつけることによって、ターゲットを高負荷状態にして、ターゲットのサービスを妨害する攻撃。攻撃源が複数のPCやサーバに分散するため、負荷が高く、また対処が困難になる。
*2 Worm： 自己増殖しながら、コンピュータを攻撃したり、情報漏えい行う不正プログラム。ネットワークや外部記憶媒体などを通じて別のコンピュータに入り込む。
*3 P2Pファイル交換： Peer to Peer ファイル交換。 特定のサーバなどを介さず、二つのコンピュータ間を直接接続し、ファイルの転送を行う技術。大量のファイル交換に利用された場合に、ネットワークに高い負荷が掛かりやすく、他の通信に影響を与える場合がある。
*4 バスケット解析：「商品Aと商品Bは一緒に購入されることが多い」といった組合せの傾向抽出を行う解析
*5 異なり数計測：サーバークライアント通信のように1対nの関係がある時にnがいくつであるかを計測する技術
*6 本技術は，筑波大学 吉田健一教授と共同の研究成果を活用したものです
*7 二段階集約方式：高速ハードウェア処理可能なフロー別の統計情報集約を行ってからデータマイニングによる集約を行う高速回線対応の処理方式
*8 複数データー括更新方式：キャッシュメモリのヒット率向上に配慮して高速化を図ったメモリ上の統計データ更新方式
*9 平均パケット長約580バイトで計算

■ アラクサラネットワークス株式会社について

アラクサラネットワークス株式会社は、「快適で安心して使えるネットワークを世界の人々に提供し、豊かな情報通信社会の実現に貢献」を企業理念としています。情報ライフラインを支える概念としてギャランティード・ネットワークを提唱し、ネットワーク構築に必要な基幹系ルータおよびスイッチの開発から設計、製造、販売、保守のサービスを提供しています。

会社名	アラクサラネットワークス株式会社
設立日	2004 年 10 月 1 日
代表者	代表取締役社長 和田宏行
資本金	55 億円
所在地	神奈川県川崎市幸区鹿島田890 新川崎三井ビル西棟
従業員数	約 320 名 （2008 年 3 月末現在）
URL	http://www.alaxala.com/

■ 商標名称等に関する表示

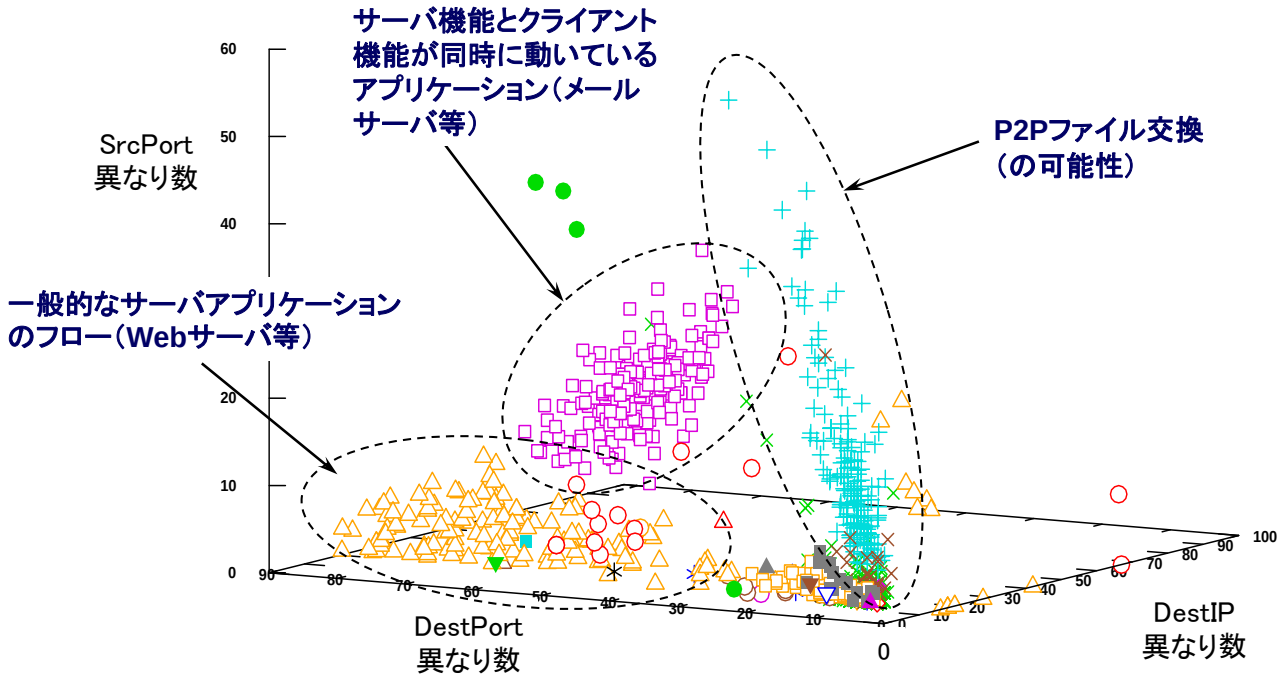
■ 技術に関するお問い合わせ先

アラクサラネットワークス株式会社 先端技術企画部
〒212-0058 神奈川県川崎市幸区鹿島田 890 新川崎三井ビル西棟
URL： http://www.alaxala.com/jp/contact/

■ 報道機関お問合わせ先

アラクサラネットワークス株式会社 広報担当 【担当： 新井】
〒212-0058 神奈川県川崎市幸区鹿島田 890 新川崎三井ビル西棟
電話：044-549-1706(ダイヤルイン)
URL： http://www.alaxala.com/jp/contact/

【別紙】



本技術によるトラヒック分析結果の例　～リアルタイムで分析が可能～