3D-tcpdump：3次元ネットワークブラウザ

―ネットワークをより身近に感じるユビキタスネットワーク・ブラウザ！―

1. 背景

計算機同士の大規模ネットワークであるインターネットなどのコンピュータネットワークは、計算機間通信インタラクションの OSI 7 層モデル通信プロトコル階層化によって、そのユーザに対して長くブラックボックス化されてきた。こういった状況は、ユーザにコンピュータ同士の接続関係であるネットワークを意識させるべきではない、というコンピュータネットワーク開発原理（End-to-End 議論）の観点からは利に適っている。むしろ、通信相手でさえ誰であるかの認識なくインターネットを利用しメールやウェブ閲覧などを行っているケースが一般的である。

しかし、近年のコンピュータウィルス増加や、オペレーティングシステム（OS）脆弱性攻撃型ワームソフトウェアの隆盛により、人々はコンピュータネットワークの存在を意識せざるをえない状況となっている。たとえ、コンピュータプログラムや OS を最新品質に保っていたとしても、膨大な量のサービス拒否攻撃を受ける可能性も存在する。ウィルス対策ソフトウェアなどにとって未知な攻撃は、通常の通信トラフィックとは異なるという意味の異常トラフィックとして検知することが可能であるが、異常であるかの決定は最終的にはその通信を担っているユーザに委ねられる必要がある。これらの攻撃に対処するには、一般ユーザであってもネットワークに関する簡単な知識獲得や攻撃状況目視を行う必要がある。

加えて、近年のユビキタス計算・ネットワーク環境の普及過渡期に見られるように、身の回りに存在するネットワークや計算機端末が増加することにより、一般家庭においても情報家電、小型センサ、無線接続端末などの複数計算機端末によってローカルネットワークを構成することが一般的になると考えられる。センサなどから構成されるネットワークは主に無線接続型であり、物理的にネットワーク配線が見えないため、より一段とその接続関係を視覚化することはネットワーク管理の観点から重要である。

2. 目的

我々の 3D-tcpdump プロジェクトでは人々がより直感的にネットワークというものを把握し興味を抱く助けとなることを目的に、単一計算機を基点としたネットワーク通信状態・トポロジの三次元グラフィカル視覚化ソフトウェア（3D-tcpdump）を提案する。本ソフトウェアがターゲットとする一般ユーザとは、コンピュータネットワークに関する知識は皆無であるが、メールやウェブなどを利用して計算機を扱っている人々までを指す。本ソフトウェアによって、こういったユーザが自分が扱っている計算機端末が危険な状況にさらされていないかの判断が行える、もしくはネットワーク管理者などに報告が可能になることが 3D-tcpdump プロジェクトの目的である。

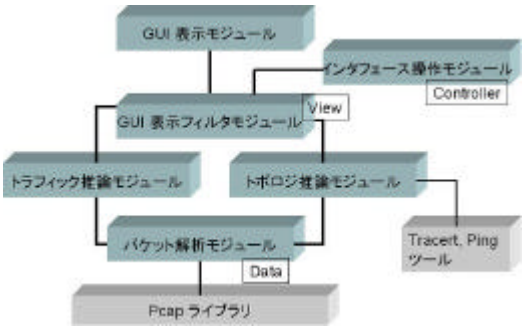
3. 開発の内容

3D-tcpdump におけるネットワーク情報視覚化では、通信トラフィックフローの視覚化に特に重点を置いている。一般ユーザにとっては、実際に自分が使用しているホストが関わっているトラフィックがどこから来ている、もしくはどこに向かっているのか、ということが最も重要だからである。ネットワークトポロジにおける途中経路ルータを把握する必要性があるのは、ネットワーク管理者や研究

者であり、一般ユーザにとっては自分のホストが存在する LAN やホームネットワークにおけるデフォルトルータを把握できれば十分だと考えられる。もちろん、より詳しく Traceroute 機能などの結果を知りたい一般ユーザも存在すると思われるので、ユーザの操作や要望に応じてネットワーク情報を開示していける視覚化ポリシのもとで 3D-tcpdump を構築する。つまり、最初の初期設定におけるネットワーク情報視覚化は自ホストと通信相手ホスト、デフォルトルータのシンプルなトポロジ上での、全ての通信トラフィック視覚化であるが、マウス操作や表示切り替えを行うことでネットワーク管理者の要望まで耐えられるように要求指向で視覚化表示フィルタの粒度を変更していく。

図 1 に 3D-tcpdump ソフトウェアのモジュール構成を示す。「Pcap ライブラリ」から全パケット情報を取得し、そのパケット情報を「パケット解析モジュール」がプロトコルごとのヘッダ解析を行う。ヘッダ解析されたパケット情報は、トラフィック推論モジュールとトポロジ推論モジュール（この二つを統合して「ネットワークパケット情報解析モジュール」とする）に渡され、通信トラフィックのプロトコル情報把握や通信レート計算、通信相手情報をもとにした Traceroute 機能と Ping 機能実行による途中経路、デフォルトルータ把握、相手先ホストへの遅延情報把握が行われる。次いで、GUI 表示フィルタモジュールを通して、これらのネットワーク情報結果が 3D & 2D GUI 表示を行う「3D グラフィック視覚化モジュール」において三次元グラフィカル表示される。フィルタモジュールの命令インプットは、3D-tcpdump の初期設定や XML 設定ファイル、マウスやキーボード操作による「GUI インタフェース操作モジュール」から行われる。

図 1：ソフトウェアモジュール構成



3D-tcpdump ソフトウェアのプロトタイプ実装には、通信トラフィック取得に libpcap 標準ライブラリを利用し、三次元表示系には Java3D を使用している。libpcap 標準ライブラリに関しては、Windows や Linux、FreeBSD などの現在使われている汎用 OS のほとんどにおいて使用可能であるために採用を決定した。三次元表示系で選択した Java3D は、実行プラットフォーム OS に依存しないという Java の利点を享受できるのにくわえ、3D 表示機能が実行マシン上のグラフィックデバイス性能に大きく依存することを避けるためである。個々の OS やグラフィックデバイスへの依存部分を可能な限り、Java3D ライブラリに吸収してもらうという方針である。Java3D の採用はまた、現在の二次元的なコンピュータデスクトップ環境が完全三次元される近未来を想定してのことでもある。既に、UNIX の X ウィンドウ環境で動作する完全三次元デスクトップシステムである、Project Looking Glass が開発されオープンソース化されようとしている。

libpcap によってネットワークインタフェースに到着する全てのパケット情報が取得可能であるが、現在のプロトタイプ実装では NetBIOS や DHCP などのブロードキャスト通信とマルチキャスト通信を非表示にしている。これはマルチキャスト通信の最も適切な表示方法が考案できていないことにくわえ、主要なソフトウェアターゲットが一般ユーザであるということを考慮すると、マルチキャスト通信のフロー情報はエンドホストにとってそれ

ほど重要ではないと判断したからである。また、現在の実装では OS で提供される/etc/services 情報を利用して 1 通信フローのトランスポートプロトコル区別を行っているが、これだけの情報では例外フローとして判断されてしまう通信が多くなってしまう。そのため、トランスポートポート番号情報からマッピング可能なアプリケーションをプログラム的に判断し、それをユーザに情報提供してフローが例外であるかの最終判断をユーザに委ねている。アプリケーション情報の取得は、netstat や ps プログラムなど OS 依存になってしまう面があるために、現在は Windows プラットフォームに依存した実装となっている。OS に依存しない形での汎用的なアプリケーション情報取得機構の試案は今後の課題である。

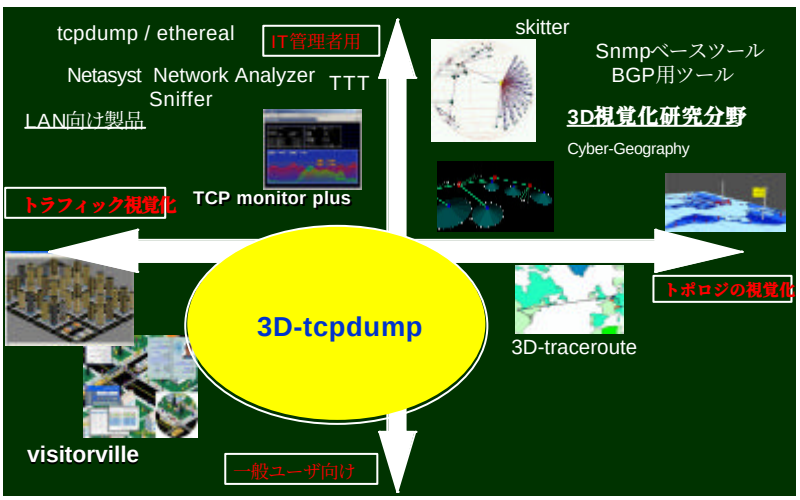
libpcap は C 言語実装の OS 標準ライブラリであるために、Java から Java Native Interface (JNI) を利用して三次元表示 Java3D モジュールに統合させている。図 4 における、「パケット解析モジュール」が JNI 部である。

4. 従来の技術（または機能）との相違

3D-tcpdump ソフトウェアが対象とするのは、tcpdump などと同じローカルネットワークや自ホストにおける通信トラフィックとネットワークトポロジ情報の視覚化である。既存のネットワーク情報視覚化研究や関連ツールと 3D-tcpdump ソフトウェアとの位置関係を図 2 に示す。縦軸には、コンピュータネットワークに関する習熟度として上側が IT 管理者、下側に一般ユーザ層を位置づけ、3D-tcpdump を含めた関連ソフトウェア群の対象ユーザ層を示している。横軸には、ネットワーク情報として大きく通信トラフィック情報と通信トポロジ情報の二つに大別し、その二つを両端に位置づけた。

3D-tcpdump ソフトウェアは、単一計算機、つまり自分が利用するコンピュータホストで行われているコンピュータ通信と、通信に関わる計算機ネットワークトポロジの三次元視覚化を行う。その対象ユーザ層は、ネットワーク管理者やコンピュータ科学研究者などのネットワークに関する知識が既に十分な人々ではなく、コンピュータを利用しているがネットワークというものはよく分からない、もしくは意識したことがないといった人々である。

図 2：3D-tcpdump 関連ツールの相関図



コンピュータネットワーク視覚化を行うソフトウェアは大きく分けて、通信トラフィック視覚化とネットワークトポロジ視覚化の二つに分類することができる。3D-tcpdump と同じ一般ユーザ層向けであるが、ウェブの HTTP トラフィック視覚化のみに特化した VisitorVille や不正侵入検知に特化したネットワーク視覚化ソフトウェア研究などが 3D-tcpdump に特に関連するソフトウェアである。しかし、これらのツールは用途が特定化されているために、一般ユーザの日常的なコンピューティング環境での使用には適していない。また、三次元情報視覚化手法を用いたネットワークトポロジ視覚化ツールとして、3d Traceroute ツールが開発されているが、通信トラフィック解析には向いていない。ネットワーク情報の視覚化に関する研究自体は新しいものではなく、情報視覚化の研究となればアニメーションや三次元化などその歴史は長い。既存のネットワーク情報視覚化研究はインターネットや WWW 構造の大規模視覚化が主要であり、インターネット運用の観点からはパケットプローブを利用した大規模ネットワークトポロジ・接続性視覚化などの研究が主要である。もちろん、これらの研究やツールは、ネットワーク管理者や研究者用途である。一方、ローカルネットワークや自ホストを対象として、通信トラフィック情報の視覚化を行うツールや研究も多く存在する。いくつか例を挙げれば、ネットワークトラフィック表示ツールとして最も有名な tcpdump やその GUI 操作解析ツールである Ethereal、tcpdump のリアルタイムグラフ表示ツールである ttt などが存在する。また、ネットワーク運用管理を目的としたトラフィック解析製品として Netasyst Sniffer など多くの解析ソフトウェア製品が存在する。しかし、これらのソフトウェアは全てネットワーク管理者と研究者向けのものである。

5. 期待される効果

コンピュータを利用しているがネットワークというものはよく分からない、もしくは意識したことがないといった人々がネットワークをより身近に感じてもらえることにより、来るべきユビキタスネットワーク社会に向けて人々の IT リテラシー向上の礎となり得る。

3D-tcpdump ソフトウェアが、パーソナルファイアオールなどのネットワーク制御機構と連携し、ADSL や FTTH 経由のインタネットサービスを提供するプロバイダなどが、我々の 3D-tcpdump フィルタリングソフトウェアを顧客に配布し使用してもらうことでより円滑なネットワーク管理、顧客対応が可能になると考えられる。

さらに、本ソフトウェアの使用用途には、異常トラフィック視覚化検出やコンピュータウィルス発生源ホストの特定、家庭内ネットワークにおける通信フィルタリング設定補助ツール、ネットワーク・通信プロトコルの教育などが挙げられ、ユビキタスネットワーク社会のいたるところ活用される可能性がある。

6. 普及（または活用）の見通し

可能な限り多くの方々に使ってもらえるよう普及活動を行っていきたい。

7. 開発者名（所属）

斉藤匡人　慶應義塾大学大学院 政策・メディア研究科）
山下勝司　慶應義塾大学 総合政策学部）
金田裕剛　慶應義塾大学大学院 政策・メディア研究科）
青柳禎矩　慶應義塾大学大学院 政策・メディア研究科）

参考）プロジェクトURL：http://www.3d-tcpdump.org
開発者URL：http://www.ht.sfc.keio.ac.jp/~masato