L-001

組織内ネットワーク可視化ツールの開発
Development of Internal Network Visualization Tool

脇村 亜衣 † Ai Wakimura
青木 茂樹 † Shigeki Aoki
宮本 貴朗 † Takao Miyamoto

1. まえがき

近年，クラウドコンピューティングサービスに代表されるネットワークサービスの多様化により，ネットワーク環境は複雑化を続けている．ネットワーク管理者にはトラフィックの状況を迅速かつ正確に把握することが求められるが，膨大なデータの分析は文字と数値だけでは困難である．そのため昨今，ネットワークトラフィックを視覚的に把握可能な可視化システムの開発が進んでいる [1][2].

本研究では，組織内ネットワークの管理者がネットワークの状況を適確に把握するために有用な，組織内ネットワークのトラフィックを可視化するツールを開発した．このツールでは，サブネット毎に設置した計測機器から取得した情報を用いるため，端末そのものにエージェントを仕込む必要がない．管理者はツールの出力を確認することで，組織内ネットワーク内にマルウェアに感染した端末が存在する場合などに，通常とは異なる状態にあることを容易に把握することができる．

2. 研究手法

2.1. トラフィックデータの収集

ネットワークのトラフィックデータを，可視化対象となるサブネットのエッジスイッチに計測機器を設置することで収集する．これにより，SNMP の MIB などでは不可能なパケット単位での情報の収集が行える．また，組織内部の相互の通信についても把握することができる．具体的な収集手順として，まずエッジスイッチのアップリンクにミラーポートを設定し，そのポートにトラフィック計測機器を接続する．各トラフィック計測機器で tcpdump によりパケットを監視し，必要情報を抽出して単位時間ごとに保存し，サーバへ転送する．

2.2. 可視化手法

抽出した情報は，画像上の送信元座標から宛先座標に向けて立体を斜方投射するように描画することで三次元的に表示する．トラフィック状況の表現手法として，パケットの送信元と宛先を示す立体の発着点に加え，各トラフィックの状態を表す立体の種類・大きさ・色，また斜方投射の高さを用いる．各表現方法に対応する可視化パラメータは，表 1 に示す通りである．複数の可視化パラメータが含まれている表現方法については，管理者が GUI による操作で自由に変更できる．なお，初期値として*印の項目を設定している．

可視化機能として，リアルタイムにトラフィックデータをアニメーションで描画するほか，日時を入力することにより過去のトラフィックを描画できる．さらにフィルタ機能として，プロトコルや IP アドレス・ポート番号を指定することにより，特定の通信だけの描画または除外が可能である．また，描画のスピード変更や画像を回転・拡大縮小・軸移動する操作も，マウスとキーボードで操作できる．

表 1: 表現方法と可視化パラメータ

表現方法	可視化パラメータ
出発点と着地点	送信元 IP アドレスと宛先 IP アドレス
立体の種類 (立方体/球体)	TCP/UDP
立体の色	*計測機器の識別番号，単位時間あたりの合計パケットサイズ，単位時間あたりのパケット数
立体の大きさ	*単位時間あたりの合計パケットサイズ，単位時間あたりのパケット数
斜方投射の高さ	*単位時間あたりのパケット数，単位時間あたりの合計パケットサイズ，送信元ポート番号，宛先ポート番号

図 1 に本手法を用いた可視化の例を示す．図 1 では描画の表現方法として初期値を用いており，アニメーションでトラフィック状況が描画されている．また，図 1 に示したような可視化手法と連動し，受信ポート番号・送信ポート番号ごとのパケット数と，送信元サブネット・送信先サブネットごとのパケット数を，それぞれ棒グラフで出力する．これらは，組織内ネットワークの全パケットをサブネットで色分けし，単位時間毎に比較できるよう複数個並べて表示している．また，同一内容の通信のパケット数に一つ前の単位時間と比べて 50 %以上の変化があった場合，その対象となるサブネットを個別に自動表示する．

3. 実験及び考察

3.1. 実験環境

大阪府立大学のキャンパスネットワークにおいて，開発したツールを用いた実験を行った．大阪府立大学内の 10 個のエッジスイッチに対して計測機器を設置してトラフィックデータを収集した．本実験では計測機器に Raspberry Pi を，サーバには Mac mini を用いている．また，単位時間は 1 分とした．

3.2. 実験結果

可視化結果の例を，図 1〜図 4 に示す．図 1 では，黄色の丸で示した棟のサブネットと，水色の丸で示した棟のサブネット間での一部の TCP 通信が，合計パケットサイズ・パケット数ともに他の通信と比べて大きかったため，トラフィックの量を示す立方体が大きさ・斜方投射の高さともに最大となっている．

図 2 では，同一時刻のトラフィックにおいて描画の表現

†大阪府立大学 大学院人間社会システム科学研究科

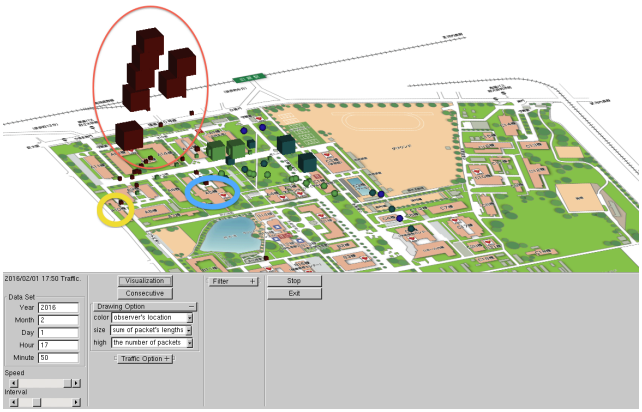

図 1: 可視化の例

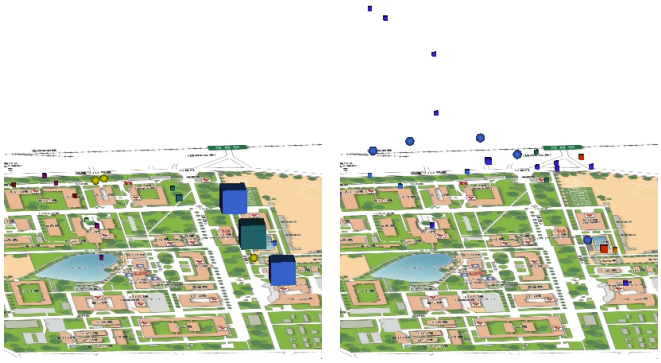

図 2: 表現方法の比較例

方法を変更して描画している．左図は各種表現方法を初期値としているため，合計パケットサイズが大きい通信が三種類発生していることが分かる．右図では斜方投射の高さを送信元のポート番号に設定しているため，多種類のプロトコルが利用されていることが分かる．このように描画の表現方法を変更することにより，管理者が見たい情報を提示することができる．

図 3 は，送信ポート番号ごとのパケット数を棒グラフとして出力した例である．左図は全サブネットがほぼ均等に各ポート番号を利用している時のグラフであり，右図は二つのサブネットに利用率が偏っている時のグラフである．右図のように偏った出力ではネットワーク利用状況の推移の特徴が掴み辛いため，一つ前の単位時間に比べて特定の

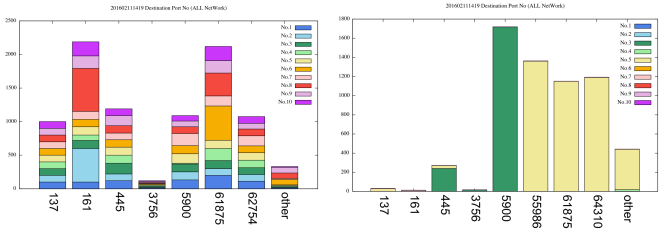

図 3: 送信ポート番号ごとのパケット数のグラフ出力例

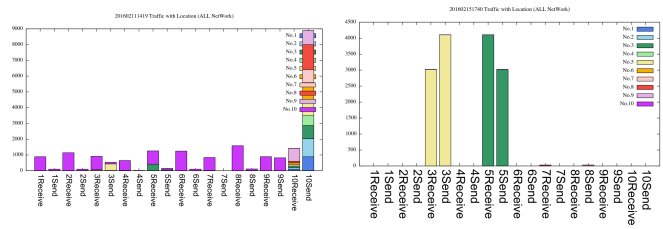

図 4: 通信先サブネットごとのパケット数のグラフ出力例

ポートを利用するパケットの増減がしきい値を超えた場合，そのサブネットのグラフのみを個別出力する機能を付加している．この機能により，特定のポートにおいて異常にパケットが増加した場合などを一目で把握することができる．

図 4 は，通信先サブネットごとのパケット数を棒グラフとして出力した例である．左図はサブネット No.10 が他のサブネットとほぼ均等に通信している時のグラフであり，右図はサブネット No.5 とサブネット No.3 の間での通信量が多い時のグラフである．

3.3. 考察

実験により，開発したツールによってサブネット間のトラフィックを視覚的に分かりやすく把握可能であることを確認できた．通常と異なる状態になるとグラフを出力することにより，アニメーションだけでは分からなかったサブネット間の通信量の推移も簡単に把握できる．さらに，異常なパケット数やパケットサイズを観測した場合には，アニメーションとグラフの出力によりトラフィックが通常とは異なる状態にあると視覚的に判断することができた．

4. まとめ

本研究では，組織内ネットワークにおけるトラフィックを，エッジスイッチに設置した計測機器で観測・解析してアニメーションとグラフで表現することにより，管理者に対して情報を視覚的に分かりやすく提示することができる可視化システムを開発した．また，GUI による直感的な操作で，管理者が得たい情報に合わせて描画の表現方法を変更したり，得たい情報のみを抽出した描画を可能にした．

今後の展開として，可視化と連動して異常を自動的に検知し警告する機能や，利用している OS の情報などをオンデマンドで取得できるシステムの構築など，より管理者の目線に立った新たな機能の検討が考えられる．

参考文献

[1] 鈴木 和也，馬場 俊輔，和田 英彦，中尾 康二，高倉 弘喜，岡部 寿男，“ 迅速な障害対応を支援するトラヒック可視化システムの構築と評価，”電子情報通信学会（B），Vol.J92-B，No.7，pp.1072-1083，2009.

[2] 鈴木宏栄，衛藤将史，井上大介，“ ネットワークトラフィック可視化システム NIRVANA の開発と評価，”情報通信研究機構，Vol.57，pp.63-80，2011.