L-021

パケットスコープの開発
Development of Packet Scope

鎌田 知男† 武田 利浩† 平中 幸雄†
Tomoo Kamata Toshihiro Taketa Yukio Hiranaka

1. はじめに

近年，インターネットなどの普及やネットワーク技術の進展とともに，アプリケーションやトラフィックが増大する一方で，ネットワークのトラブルや障害などの影響が大きくなり，ネットワークを分析する機能の重要性が高まっている．ネットワークの保守や管理には，ネットワークケーブル上を流れるパケットをキャプチャし，それを解析する方法が挙げられる．しかし，キャプチャしたパケットの分析結果はバイナリ形式やテキストベースで表示され，一般ユーザにとっては直感的に理解できるとは言い難い．

本研究では，ネットワークで送受信されるパケットをモニタし，ウェブブラウザ上でグラフィカルな表示を行ったうえで，任意のパケットを固定することのできるトリガ機能をもつ「パケットスコープ」の開発を行った．

2. 既存のパケットモニタ

既存のパケットモニタリングソフトについて具体的な例を挙げ説明する．

1) WireShark (Ethereal)[1]

以前は Ethereal という名前で開発が進められていた．非常に高性能ながら無償で利用できるパケットモニタリングソフトである．（図 1）また，Linux で一般的な tcpdump などのキャプチャデータを解析することもできる等，多様なフォーマットに対応している．さらにフィルタリング解析能力も高く，使用ユーザも多い．このソフトはオープンソースであり，現在も世界中の開発者によって改良が進められている．

2) PacketViz[2]

パケットログ「.pkt」ファイル形式をラダーチャートで視覚化する．図 2 のようにサーバやクライアントを複数指定することができる．パケットの説明やコントロールパネルが別窓で開く．開発言語として Java5.0 を使用しておりファイル形式が対応していれば，どんなプラットフォームでも動作すると記述してある．

現状のパケット視覚化ツールの特徴として，表示方法に文字をベースとしたテキスト形式を用いている．これでは通信内容を直感的に理解することは困難である．また，矢印でパケットの通信方向を表示している．しかし，矢印が重なりみにくくなっている．また，任意のパケットに対する連続した対応がわからないといったことが挙げられる．

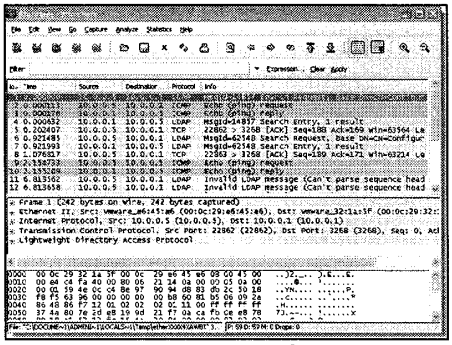

図 1 WireShark 実行画面

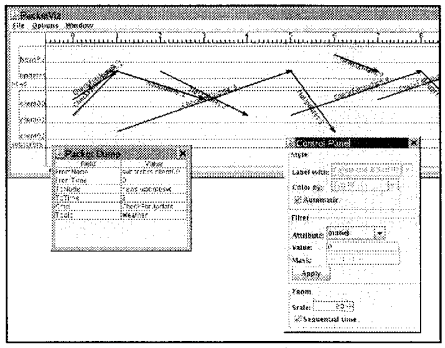

図 2 PacketViz 実行画面

3. パケットスコープの開発

3.1 開発目標

パケットスコープとは，ウェブブラウザ上にスコープ画面を表示し，操作も可能とするシステムである．ネットワークトラフィックを時間軸上にパケットを表示することで時間変化をわかりやすく表示する．パケットの送信から受信までの時間とその変動，パケットサイズとパケット列の関係を視覚化し，ネットワーク機能やトラフィックの分析を行えるようにする．本研究で開発するパケットスコープの機能として，さらにオシロスコープのようなトリガ機能の実装を行う．

オシロスコープのトリガ機能とは，オシロスコープに入力される信号の電圧が，ある一定の電圧(トリガレベル)を横切ったとき，その時刻の前後の電圧の変化(波形)を画面に表示し固定する機能のことである．

本研究では，任意のパケット(トリガ)を選択し前後の時刻のパケットとともに画面に固定する．次にトリガのパケットが現れたら，そのパケットの周囲の変化とともに画面に表示するといった機能である．

† 山形大学 Yamagata University

3.2 開発環境および開発言語

本研究のシステム概要を図 3 に示す．WireShark を使用し，ネットワーク上に流れるパケットデータを抽出する．抽出したデータを perl で作成したプログラムを使用しウェブサーバ上でデータファイルにする．

作成したデータファイルを，パケットスコープのメイン画面の HTML と同じディレクトリに置き，Ajax を用いて，クライアントのウェブブラウザにパケットスコープ画面を出力する．グラフの描画には JavaScript プラグイン Flot を使用した．

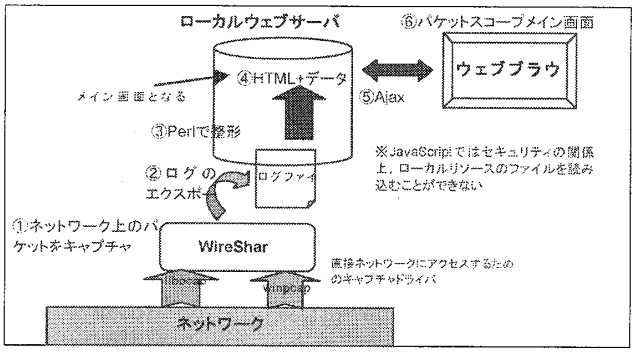

図 3　システム概要

3.3 主要機能

グラフ上をドラッグすることでズームし，パケットの IP 情報をマウスホバー時に表示させる機能の実装を行った．グラフをクリックした際に，パケットスコープ内 HTML にパケットの詳細説明を出力する．

フィルタ機能として，データファイルをロードする際に，チェックボックスを作成する．チェックを外すと対応したグラフが非表示になる．

パケットスコープの実行画面を図 4 に示す．

3.4 トリガ機能

オシロスコープのようなトリガ機能の実装をした．任意のパケットをトリガとして固定し，その前後の時刻のパケットとともに変化を繰り返して表示するといった機能である．

例えば，ping のような繰り返されるパケットの場合，前回との応答時間の変化がわかりやすくなる．

オシロスコープのトリガ機能の実行画面を図 5 に示す．

4. まとめ・課題

本研究では，WireShark のログファイルを加工し，パケットの流れをぱっと見てわかるような「パケットスコープ」を作成した．パケットモニタとしての主要機能および，パケットスコープのトリガ機能の動作を確認した．

X 軸は時間軸であるが，ズームした際に目盛が重なってしまい見づらい場合がある．表示方法をラダー形式にした場合と比べる必要がある．

トリガ機能であるが，リアルタイム表示のときにより有効な機能であり，パケットの対応や変化，応答分布といったものがより判断しやすくなる．そのためには，パケットキャプチャドライバから直接データを取り込めるようにする必要がある．

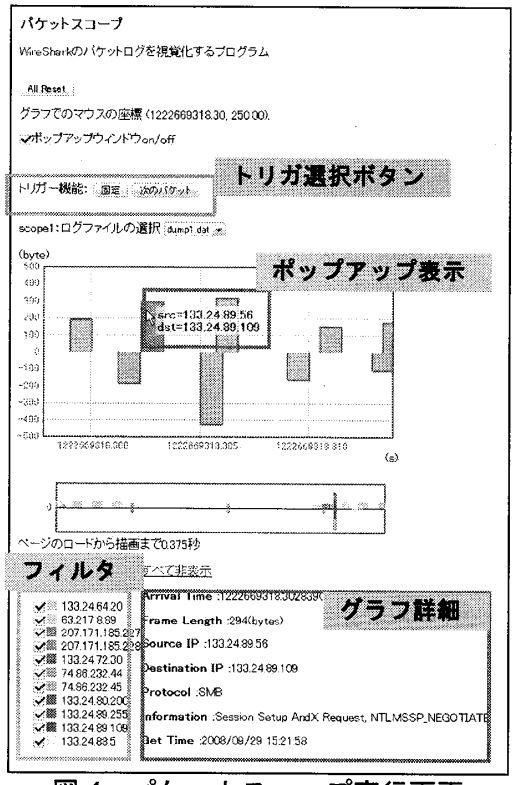

図 4　パケットスコープ実行画面

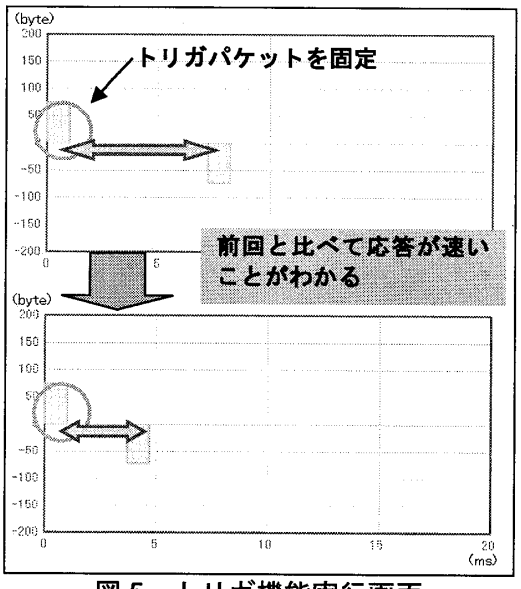

図 5　トリガ機能実行画面

参考文献

[1]Wireshark, http://www.wireshark.org/

[2]PacketViz Packet Visualization, http://packetviz.sourceforge.net/