3ZC-1

TCP/IP の可視化ツールの開発 -TCP の順序制御とトランスポート層における コネクション/コネクションレス型の違いの可視化ツール

高橋祥吾　荒井正之

帝京大学大学院理工学研究科

1. はじめに

インターネットの普及に伴い，情報の専門教育において TCP/IP プロトコルの教育が重要になってきた．我々は，従来の TCP/IP プロトコルの学習方法の問題点を解決するために，ネットワークの可視化ツールを開発・提案してきた[1]．本論文では，開発した TCP の制御方式の 1 つである順序制御の可視化ツールと，現在開発中のトランスポート層におけるコネクション/コネクションレス型の違いを可視化するツール(以下 TCP/UDP 可視化ツールと呼ぶ)について述べる．

2. TCP の順序制御の可視化ツール

2.1. 順序制御の学習上の問題点　順序制御とは，送信側がパケットにシーケンス番号を付けて送り，受信側がパケットを受け取りシーケンス番号どおりに並べ，送信側に確認応答番号を送り返す制御である．途中でパケットの順番が入れ替わっても，受信側でシーケンス番号どおりに並べ替えデータを復元する．シーケンス番号とは，送信するデータに，順番を付けるための番号である．送信するデータ 1byte ごとにシーケンス番号を 1 ずつ増やして行く．また，確認応答番号とは，送られたデータがどこまで受信できたか，そして次のデータがどこからかを表している．

従来の学習方法である参考書や講義によって，TCP の順序制御を学習するには次のような問題点があると考える．

- 教科書や講義では，様々な通信パターンの提示が難しい．また実感がわきにくい．
- シーケンス番号や確認応答番号の増分，および 2 つの番号の関係の理解が難しい．(参考書には，番号が 1 ずつ増えるように説明されている場合が多い)
- パケットキャプチャリングツールなど，汎用的なソフトウェアを用いることも考えられるが，このようなツールはユーザインターフェースが優れていない．

2.2. ツールの概要　本ツールは，実行している PC の IP アドレスとポート番号をキーにパケットをキャプチャする．複数セッションのパケットをキャプチャした場合は，最初のセッションのパケットだけが表示される．

図 1 は，開発した TCP 順序制御の可視化ツールの実行画面の一例である．①プロトコル/ポート番号の選択部 ②データ表示部 ③画像表示部 ④/⑤画像操作部から構成される．

図 1①に示したチェックボックスまたはポート番号を入力することにより，取得するアプリケーションプロトコルを選ぶことができる．

図 1②は，キャプチャしたパケットを表示する．左から「取得した順番」「送信側(Local)の IP アドレス」「受信側(Remote)の IP アドレス」」「確認応答番号」「シーケンス番号」「次のシーケンス番号」「データ量」「送信元(src)ポート番号」「宛先(dst)ポート番号」を表示する．1 行が 1 つのパケットに対応しており，選択したパケットに関連のあるデータを使って③に可視化した図を表示する．パケットの取得中は，本ツールを操作できない．

図 1③には，図 1②で選んだパケットを可視化した図を表示する．描画する内容は「取得した順番」「データ量」「シーケンス番号」「確認応答番号」，矢印は「通信方向」を表している．図 1⑥を例に表記すると「取得した順番:No5」「データ量:1460」「シーケンス番号:8488147」「確認応答番号:8489607」，矢印は「通信方向:上」となる．

図 1④「size」は，パケットデータの長さの幅を可変できる．シーケンス番号，確認応答番号の上位数桁はあまり変化しないので，図 1⑤「Digit」で表示桁数を決めることにより，数値の桁を変更することができる．選んだパケットの中にアプリケーション層のデータがある場合塗りつぶされた四角の中にパケットデータの数値(図 1⑦)，データサイズが 0 で Ack を返している部分を選択した場合は空白の四角(図 1⑧)で表示する．

2.3. 実装方法　本研究では Jpcap というクラスライブラリを使用している．これは WinPcap という Windows にパケットキャプチャの機能を追加するドライバを使用して Java 言語でのパケットキャプチャを実現している．Jpcap による開発・実行には管理者権限が必要である．また，JRE Version5 以下の場合，OS 上で Java や Jpcap のファイルが置いてあるディレクトリの指定をす

「TCP/IP Visualization Tools for the Control Method of Packet Arrival Order and Differences between Connection and Connectionless of the Transport Layer Protocol」Shogo TAKAHASHI, Masayuki ARAI, Graduate School of Sciences and Engineering, Teikyo University

る環境変数を設定しなければならない.

3. トランスポート層におけるコネクション/コネクションレス型の違いの可視化ツール

3.1. TCP/UDP の学習上の問題点　コネクション型である TCP とコネクションレス型である UDP の大きな違いはデータ転送の信頼性の有無と転送するパケットの量である. TCP はコネクションを張るためのオープン処理(3 way hand shake), データのやり取りが正確に行われたかを確認する応答確認, 通信相手とのやり取りを正確に終了させるクローズ処理などを行い, データ転送の信頼性を確立している. 本ツールではオープン処理, 応答確認, クローズ処理等を可視化することを目的としている.

3.2. ツールの概要　本ツールではアプリケーションプロトコルの 1 つ DNS の通信内容のパケットをキャプチャし TCP と UDP の信頼性の有無と, 通信パケット数の違いを可視化するツールを考えている. 図 2 は, 本研究で提案する TCP/UDP 可視化ツールの実行画面の一例である. ①TCP 通信表示部②データ表示部③UDP 通信表示部から構成される.

図 2①には TCP のキャプチャした DNS 通信データを元に「Local」「Remote」, Syn,Ack,Push,Fin 等のフラグの表記, 通信方向を矢印で表している. オープン処理やクローズ処理などは, 矢印の色を変えて, どこからどこまでがその処理に該当するのかをわかりやすく表示したいと考えている. 図 2 では④がオープン処理, ⑤がクローズ処理を行っている箇所に該当する.

図 2②はアプリケーションプロトコルのデータを表示する. トランスポートプロトコルは, TCP, UDP と異なるが, アプリケーションプロトコルは同じ DNS を用いているので, 同じメッセージが表示される. 図 2⑥は, Local 側からリクエストメッセージを送信していることを表し, 図 2⑦では Remote 側が Local から受けたリクエストメッセージに対するレスポンスを表している.

図 2③は UDP のキャプチャした DNS 通信データを元に「Local」「Remote」, 矢印は通信方向を表している.

4. おわりに

本論文は, 開発した TCP 順序制御の可視化ツールの概要と, 開発予定の TCP/UDP 可視化ツールの概要を述べた. 順序制御の可視化ツールは通信の際に発生するパケットのサイズ, シーケンス番号, 確認応答番号の可視化機能, データのやり取り, 通信方向が視覚的にわかりやすく見せる機能を持つ. TCP/UDP 可視化ツールは, TCP と UDP の信頼性の違いが分かりやすい可視化を行いたいと考えている. 今後の課題として TCP/UDP 可視化ツールの開発及び両ツールの評価実験が挙げられる.

参 考 文 献 [1] M.Arai, S.Takahashi and G.Kitamura:"Visualization Tools for Learning TCP/IP",2010 IEEE RIVF.

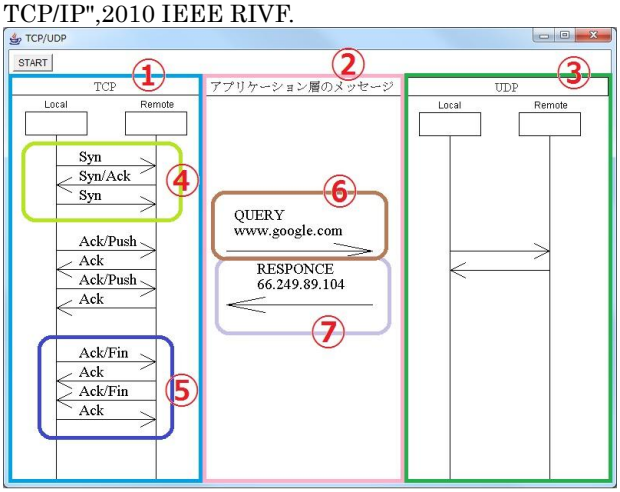

図 2.コネクション/コネクションレス型の違いの可視化ツール実行画面(予定)

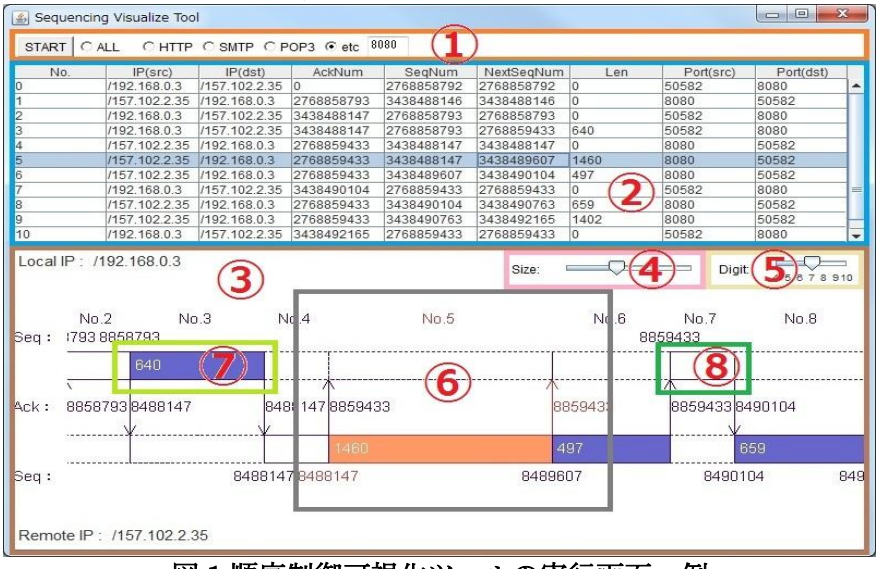

図 1.順序制御可視化ツールの実行画面一例