TCP トラフィック解析ツール: tcpillust

西田佳史
ソニーコンピュータサイエンス研究所
nishida@csl.sony.co.jp

1 背景

近年の TCP の細かい改善により、TCP の転送制御アルゴリズムはより複雑になっている。このため、新しい機能が実際に有効に機能していることを確認することや、実装が標準に準拠していることを検証することは重要である。また標準に正しく準拠している TCP 間の通信においても、実装の微妙な差異から問題が生じる可能性もある。この様な背景から、より正確に TCP トラフィックの挙動の解析し、かつ解析作業の効率を改善するツールとして tcpillust の開発を行った。

2 tcpillust の概要

2.1 ２地点によるトラフィック観測

tcpillust は、より正確な解析を行うため、TCP を用いて通信する２つのノードの近くに、それぞれ観測ポイントを設置することを想定する。そして、２つの観測ポイントから得られたトラフィックログファイルを比較し、パケットがそれぞれの観測ポイントを通過した時刻を検査する。２つのデータを利用することにより、パケットの喪失などを的確に検出し、正確な TCP コネクションの挙動の解析を行うことができる。

2.2 トラフィック情報の視覚化

tcpillust は、パケットが観測ポイントを通過した時間の情報を視覚化して表示することにより、正確で直観的な解析を可能にする。図1に tcpillust が採用している情報の視覚化の例を示す。図1は、３つのパケットの２つの観測ポイントにおける記録時刻を視覚化して表示したものである。各観測ポイントの記録時刻は、２本の直線A,B で示され、記録時刻は、上から下に向かって経過している。パケットの記録時刻 a, b, c は、直線 A 上、a', b', c' は、直線 B 上にそれぞれの時間関係に対応した間隔でプロットされる。そして、観測ポイントにおける同一のパケットの記録時刻 a-a',b-b',c-c' の間は直線で結ばれる。時刻の経過を直線で表し、パケットの時間関係に対応した間隔でプロットすることにより、各観測ポイントにおけるパケットの間隔を直観的に把握できる。また観測ポイントにおける同一のパケットの記録時刻の間を直線で結ぶことにより、パケットの転送方向を把握することができる。

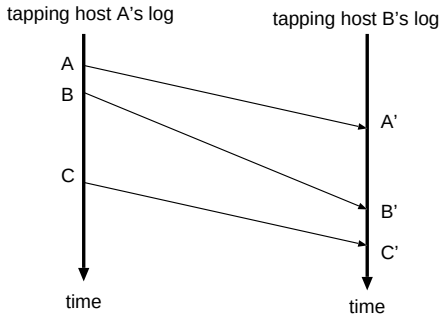

図 1: トラフィックログの情報の視覚化

2.3 観測データの同期

２つの観測ポイントで時刻同期が取られていない場合、観測ポイント間の時刻のずれから解析結果に問題が生じることがある。この様な問題に対処するため、tcpillust はトラフィックデータを比較し、２つの観測ポイントの時刻のずれを推測し自動的に補正する機構を備えている。

3 ツールの取得方法

tcpillust のソースコードは以下の url より取得できる。
http://www.csl.sony.co.jp/person/nishida/tcpillust.html
また、FreeBSD と NetBSD の ports コレクションからインストールすることも可能である。