様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　元 年　 ６ 月 ２０ 日現在

機関番号：１２６１２
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ０６３４１

研究課題名（和文）通信ログからのTCP輻輳制御方式の推定および悪意の巨大TCPフローの抽出

研究課題名（英文）Estimation of TCP Congestion Control Algorithms Detection of Malicious Giant TCP Flow from Packet Logs

研究代表者
加藤　聰彦（KATO, Toshihiko）

電気通信大学・大学院情報理工学研究科・教授

研究者番号：９０３４５４２１

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：本研究は，パッシブに収集された通信ログから，ログに含まれるTCPセッションが使用している輻輳制御方式を推定する方法を確立する．具体的には，通信ログにデータセグメントとACKセグメントの双方の情報が含まれる双方向通信ログと，データセグメントの情報のみが含まれる片方向通信ログに対して，輻輳制御の推定方法を考案する．双方向通信ログに対しては，データとACKから往復遅延時間を推定し，その間のデータ量を輻輳ウィンドウとする．輻輳ウィンドウとその増加分の対応から推定する．片方向通信ログに対しては，シーケンス番号の時間変化を，一次式から四次式で近似し，そのグラフの一階微分と二階微分の対応から推定を行う．

研究成果の学術的意義や社会的意義
輻輳制御方式はTCPトラヒックを特徴づけるものである．このため，ネットワーク事業者にとっては，自分の運営するネットワークにおいてどのような輻輳制御方式がどの程度利用されているかを調査することは，重要な意味があると考えられる．しかしこれまでは，パッシブに収集された通信ログから，新たに提案された輻輳制御方式（HighSpeed TCPやCUBIC TCPなど）を推定する方法は，まったく提案されていなかった．本研究では，これまでにない手法により，双方向および片方向の通信ログから輻輳制御方式を推定することを可能とした．

研究成果の概要（英文）：Recently, various TCP congestion control mechanisms have been introduced. Since the TCP congestion control algorithms affect the performance of the Internet, it is important to analyze which algorithms are used widely. This research focuses on a passive scheme to infer a congestion control algorithm from passively collected packet traces by estimating congestion window at round-trip time (RTT) intervals, and inferring congestion control algorithms by correlating estimated window sizes and their increments. Specifically, two methods are proposed. One is a method for bidirectional packet traces that estimates congestion window sizes by mapping data and ACK segments. The other is a method for unidirectional traces including only data segments. It uses the curve fitting for sequence number vs. time graphs by applying the least squares method with linear through quartic functions, and maps the first-order and second-order differentiations.

研究分野：情報ネットワーク

キーワード：TCP　輻輳制御　通信ログ

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

TCP の輻輳制御は，TCP において重要な機能の一つであり，研究開始当時（および現在も）積極的に研究開発が行われている．Linux オペレーティングシステムにおいては 20 弱の方式が実装されており，このうちいくつかは実際に広く利用されている．

輻輳制御方式は TCP トラヒックを特徴づけるものである．このため，ネットワーク事業者にとっては，自分の運営するネットワークにおいてどのような輻輳制御方式がどの程度利用されているかを調査することは，重要な意味があると考えられる．しかし，輻輳制御方式は TCP のデータ送信側の内部動作として実現しているため，ネットワークを流れる TCP セグメントのヘッダなどを解析しても，明示的に方式の判定を行うことはできない．

そこで，ネットワークを流れるパケットの記録（通信ログ）から，TCP セッションごとの輻輳制御方式を推定する方法が多く研究されてきた．パッシブ方式を用いた初期の研究[1-3]では，通信ログの情報から，TCP の送信側の内部状態や内部変数（輻輳ウィンドウサイズ(cwnd)やスロースタート閾値(ssthresh)など）を推定し，使用されている輻輳制御を類推する．これらの研究では Tahoe, Reno, NewReno などの限られた輻輳制御アルゴリズムのみを対象としている．近年の研究である[4]も同様なアプローチを用いており，NewReno を対象とし cwnd と ssthresh をリアルタイムに推定する方法を提案している．[5, 6]では，Linux に実装されている 13 の輻輳制御アルゴリズムの識別を対象としているが，13 のアルゴリズムのうち任意の 2 つの組を対象として，そのどちらが実装されているかを区別することを目的としている．推定に当たっては，RTT ごとの cwnd を推定し，その値の増加率，1 セグメント分だけ増加した回数の割合などの特徴量を求め，その特徴量をクラスター分析するという手法を用いている．以上の提案では双方向の通信ログの使用を前提としている．

一方，[7]は，片方向の通信ログを用いたもので，輻輳制御アルゴリズムとは別の視点からの研究である．具体的には，cwnd の初期値，再送中に輻輳ウィンドウを減少させない不当なフローの識別，データ転送の動作周期（フロークロック）の抽出によるアプリケーションの識別を行う方法を提案している．

このように，本研究の開始時点においては，パッシブに収集された通信ログから，新たに提案された輻輳制御方式（HighSpeed TCP や CUBIC TCP など）を推定する方法は，まったく提案されていなかった．

２．研究の目的

本研究は，パッシブに収集された通信ログから，ログに含まれる TCP セッションが使用している輻輳制御方式を推定する方法を確立することを目的とする．具体的には，通信ログにデータセグメントと ACK セグメントの双方の情報が含まれる場合（双方向通信ログ）と，データセグメントまたは ACK セグメントの情報のみが含まれる場合（片方向通信ログ）のそれぞれに対して，輻輳制御の推定方法を考案する．

３．研究の方法

(1) 双方向通信ログに対する輻輳制御の推定方法については，次の方法で行う．

① まずログに含まれるデータセグメントと ACK セグメントをシーケンス番号，受信確認番号，タイムスタンプオプションを用いて対応付け，データセグメントの送出からその受信確認までの時間を推定し，それを RTT（往復遅延時間）とする．

② RTT 間に新たに送信されたデータ量（パケット単位）を cwnd と推定する．

③ cwnd とその増加分（以降⊿cwnd と呼ぶ）に対して，⊿cwnd を輻輳制御アルゴリズム固有の cwnd の関数として定めることを提案する．具体的には，通信ログから求めた cwnd と⊿cwnd に対して，$(cwnd, \Delta cwnd)$をプロットし，その結果がどの関数に相当するかを調べることで，輻輳制御方式を識別する．

(2) 片方向通信ログに対する輻輳制御の推定方法に対しては，まず片方向の通信ログから RTT を推定し，その RTT に基づいて RTT の間に転送されたデータ量（パケット単位）を cwnd とし，双方向通信ログで採用した方法を流用するという方法を試みた．そこで，片方向通信ログから RTT を推定する手段として，ピリオドグラム法[8]に基づく方法と，単位時間当たりのデータ送信量の自己相関に基づく方法の 2 つを検討する．

(3) 片方向通信ログに対する第 2 の方法として，シーケンス番号の時間遷移のみを対象とする（すなわち RTT に依存しない）以下のような方法を採用した．

① シーケンス番号の時間変化に対して，再送が行われていない範囲（シーケンス番号が単調増加している範囲）を選ぶ．

② その範囲のデータを，時間の 1 次から 4 次の範囲の関数として，最小二乗法を用いて近似する．その際，途中から近似関数が変更される場合も考慮する．具体的には，一定の時間（本論文では 0.5 秒）の刻みで，近似関数の境界を仮定し，その前後で異なる関数を用いることにより，より誤差の少ない近似ができるかどうかを確認する．

③ 得られた近似関数を時間で微分した関数を⊿seq，さらにそれを再度時間で微分した関数を⊿^{2}seq とする．

④ ⊿²seq を⊿seq の関数としてグラフ化する．⊿seq と⊿²seq が 3 章の手法における cwnd と⊿cwnd に対応すると想定し，その形態から 3.2 節と同様な方法で，輻輳制御アルゴリズムを推定する．

４．研究成果

以下，３節に述べた方法について，TCP Reno と CUBIC TCP を例にとり解説する

(1) 双方向通信ログに対する輻輳制御推定方法

① TCP Reno に対する方式提案と結果

TCP Reno では，輻輳回避フェーズにおいて cwnd が RTT の間に 1 セグメントだけ増加するように，ACK セグメントを受信するごとに 1/cwnd セグメントずつ cwnd を増加させる．しかし実際には，連続したデータ転送における遅延 ACK により，2 データセグメントに 1 つの ACK セグメントが送信されるのみである．このため cwnd の RTT ごとの増加分は 1/2 セグメントとなる．通信ログから推定される cwnd は MSS の整数倍となるため，TCP Reno における RTT 毎の cwnd の増加状況は cwnd の値に関係なく．⊿cwnd=1or 0（パケット） となる．

TCP Reno の推定結果結果を図 1 に示す．通信ログに含まれるデータセグメントと ACK セグメントのヘッダ中のシーケンス番号と応答確認番号から，cwnd の値を推定した結果を図 1(a)に示す．この内で，丸印で示した，cwnd が増加し続ける部分に対して，(cwnd, ⊿cwnd)の関係をグラフしたものが図 1(b)である．前章で示した通り，⊿cwnd が 0 と 1 を交互に取っていることがわかる．

② CUBIC TCP に対する方式提案と結果

CUBIC TCP では，cwnd は直前の輻輳事象からの経過時間の関数として以下の 3 次式で与えられる．

$$cwnd = C\left(T - \sqrt[3]{\beta \cdot \frac{cwnd_{max}}{C}}\right)^3 + cwnd_{max} \qquad (1)$$

ここで $cwnd_{max}$ は直前の輻輳発生時の cwnd の値，C は定数，β は減少パラメータ，T は直前の輻輳事象からの経過時間である．RTT 間の cwnd の変化は，以下のように，$cwnd$ を T で微分した値に RTT をかけたもので近似できる．

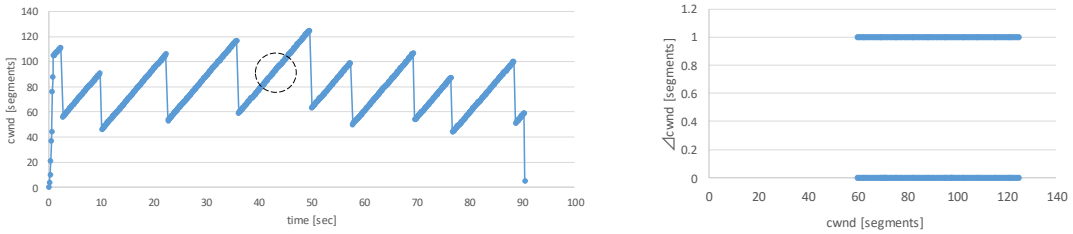
$$\Delta cwnd = RTT \cdot \frac{d(cwnd)}{dT} = RTT \cdot 3C\left(T - \sqrt[3]{\beta \cdot \frac{cwnd_{max}}{C}}\right)^2 \quad (2)$$

ここで $cwnd$ の定義式を用いて，$\Delta cwnd$ を $cwnd$ の関数で表すと以下のようになる．

$$\Delta cwnd = 3RTT \cdot \sqrt[3]{C}\left(\sqrt[3]{cwnd - cwnd_{max}}\right)^2 \qquad (3)$$

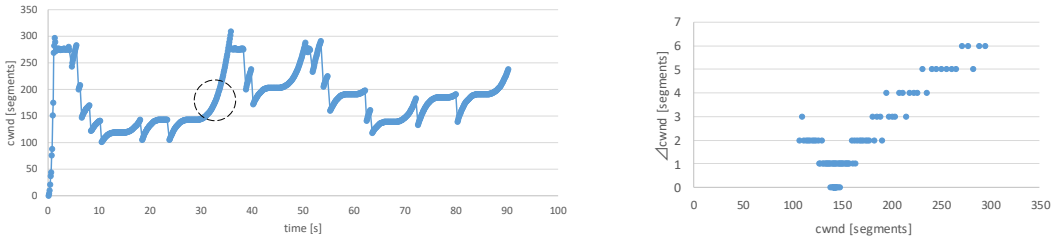
すなわち，CUBIC TCP の場合，$\Delta cwnd$ は $cwnd$ の 2/3 乗の関係にあると考えられる．この関数は，$cwnd_{max}$ の時に 0 となり，その値を中心に対称な形をとる．

CUBIC TCP の実験結果を図 2 に示す．使用した通信ログはイーサネット接続を使用したものである．図 2(a)が通信ログの情報から推定した cwnd の時間的変化である．図 2(b)が丸印で示



(a) 推定された cwnd の時間変化　　(b) ⊿cwnd と cwnd の対応（(a)の丸印の部分）

図 1　TCP Reno の結果（双方向通信ログ）



(a) 推定された cwnd の時間変化　　(b) ⊿cwnd と cwnd の対応（(a)の丸印の部分）

図 2　CUBIC TCP の結果（双方向通信ログ）

した部分に対する(cwnd, ⊿cwnd)のグラフである．この結果は，式(3)に対応していると判断できる．すなわち，cwnd=150 付近で⊿cwnd が 0 となり，それを中心に⊿cwnd が対称なグラフを示している．また⊿cwnd のグラフは上に凸の形になっている．(cwnd, ⊿cwnd)のグラフがこのような形をとる場合は，CUBIC TCP が使用されていると判断できる．

(2) 片方向通信ログに対する輻輳制御推定方法（RTT の推定による方法）

片方向通信ログに対して，人為的に追加した遅延を想定される RTT として，双方向通信ログに対する推定方法を適用した結果，ネットワークに無線 LAN リンクが存在する場合など，RTT が微妙に変動する場合に，推定がうまくいかないことが判明した．また，ピリオドグラム法により，データセグメントのみを含む片方向通信ログから RTT を推定したところ，以下の結果を得た．イーサネットリンクのみを含み遅延変動が少ないと思われるネットワークで得られたログに対しては，実際の値に比べて推定 RTT 値の変動が大きくなった．一方で，ネットワークの一部に無線 LAN を含む場合は，実際の RTT 値は変動があったものの，推定 RTT 値では変動が少なくなってしまった．いずれにせよ，この研究で提案する方法は，厳密な RTT の推定が必要となり，ピリオドグラム法を用いた RTT 推定では不十分であるという結論を得た．追加で，自己相関を用いた RTT の推定も行ったが，その性能はあまりよくなかった．これらの検討の結果から，RTT の推定に基づく片方向通信ログからの輻輳制御方式の推定は，現状では有効でないという判断を得た．

(3) 片方向通信ログに対する輻輳制御推定方法（シーケンス番号の時間変化のによる方法）

① TCP Reno に対する方式提案と結果

双方向通信ログに対する推定方法で RTT ごとに推定された⊿cwnd では，0 また 1 セグメントとなったが，片方向通信ログからの識別では，それらが平均化され，一定値となる．Δ^2seq の値は一定値をとるものの，(1)に示したように MSS（最大セグメントサイズ）の値に相当するわけではない．これは片方向通信ログに対する方法が，RTT を考慮していないためである．

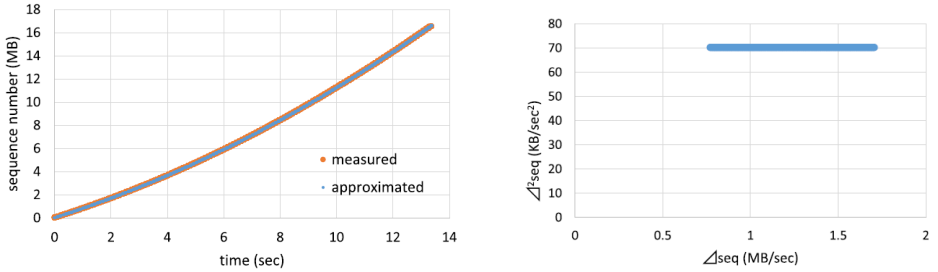
図 3 に実験結果を示す．この実験では，図 1(a)に示した cwnd の時間変化において，丸印を付けた部分に対応するシーケンス番号の時間変化を対象として，多項式近似を行った．図 3(a)はその結果を示す．この図ではオレンジのグラフが通信ログから得られたシーケンス番号の時間変化，青のグラフがそれに対する多項式近似である．なお時間およびシーケンス番号の値は，0 からの相対値としている．この例では 2 次式による近似が最適となっており，図に示すように類似性の高い近似が可能となっている．

近似した多項式から，その一階微分（⊿seq）と二階微分（Δ^2seq）の対応を示したものを図の(b)に示す．結果はΔ^2seq が⊿seq によらず一定値となっており，前節で示した TCP Reno の特徴を示している．このようにΔ^2seq が一定値をとる場合は，その TCP フローが Reno を採用している可能性が高いと判断できる．

② CUBIC TCP に対する方式提案と結果

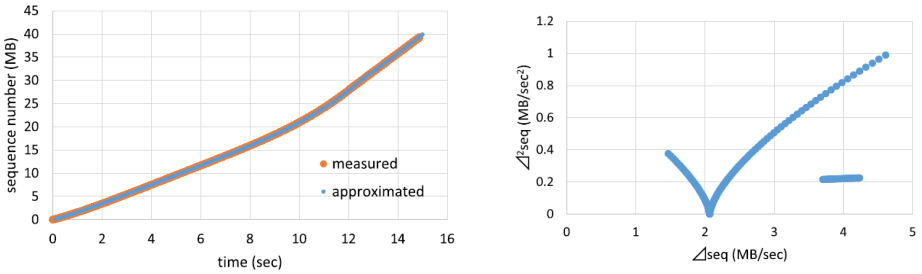
CUBIC TCP においては，Δ^2seq の値は特定の⊿seq の値で 0 となり，その値を中心として線対称な形態をとる．またΔ^2seq は⊿seq の 2/3 乗の関係になる．

図 4 に実験結果を示す．この図でも，図 2(a)の丸印に対応するシーケンス番号の時間変化を対象とした．図 4(a)が多項式近似の結果である．この場合は 12.5 秒までが 4 次式で，それ以降が 3 次式で近似された．その結果を微分することにより得られた⊿seq とΔ^2seq の対応関係を図 4(b)に示す．この結果は 2 つの部分から構成される．1 つは，⊿seq が 2M バイト/秒付近で 0 となり，それを中心に線対称となるグラフである．これは 4 次多項式で近似されたシーケンス番号の変化に対応するもので，上述の CUBIC TCP の特徴を反映している．他は，Δ^2seq の値が約 0.2M バイト/秒 ^{2} でほぼ一定となっているもので，これは 3 次多項式で近似された部分に対応する．後者については，実際の通信で cwnd が増加した結果，RTT の間に cwnd のすべてが送信できなくなった部分に相当する．すなわち，片方向通信ログに対する手法では，cwnd が大きい場合に正しく輻輳制御アルゴリズムのふるまいを推定できない場合があることを示している．いずれにせよ，前者のグラフにより，この TCP フローが CUBIC TCP を採用していることは推定可能である．



(a) シーケンス番号の多項式近似　　(b) Δ^2seq と⊿seq の対応

図 3　TCP Reno の結果（片方向通信ログ）



(a) シーケンス番号の多項式近似　　(b)　⊿²seq と⊿seq の対応

図 4　CUBIC TCP の結果（片方向通信ログ）

＜参考文献＞

[1] Paxson, V.: Automated Packet Trace Analysis of TCP Implementations. ACM Comp. Commun. Review, 1997, vol. 27, no. 4, pp.167-179.

[2] Kato, T., et al.: Design of Protocol Monitor Emulating Behaviors of TCP/IP Protocols. Proc. 10th Int. Workshop on Testing of Communicating Systems (IWTCS '97), Sep. 1997, pp. 416-431.

[3] Jaiswel, S., et al.: Inferring TCP Connection Characteristics Through Passive Measurements. Proc. INFOCOM 2004, Mar. 2004, pp. 1582-1592.

[4] 茂木重憲, 渡邊晶: 輻輳制御パラメータのリアルタイム推定. 情報処理学会論文誌, 2011, vol. 52, no. 3, pp. 1308-1322.

[5] 大塩純平, 阿多信吾, 岡育生: クラスター分析に基づく各種 TCP バージョンの識別手法. 信学技報, 2009, vol. 108, no. 457, NS2008-179, pp. 205-210.

[6] Oshio, J., Ata, S., and Oka, I.: Identification of Different TCP Versions Based on Cluster Analysis. Proc. 18sth Int. Conf. on Computer Communications and Networks (ICCCN 2009), Aug. 2009, pp. 1-6.

[7] Qian, F., Gerber, A., and Mao, Z.: TCP Revisited: A Fresh Look at TCP in the Wild. Proc. Internet Measurement Conference 2009 (IMC '09), Nov. 2009, pp. 76-89.

[8] Carra, D., et al.: Passive Online RTT Estimation for Flow-Aware Routers Using One-Way Traffic. NETWORKING 2010 LNCS6091, May 2010, pp. 109-121.

５．主な発表論文等

〔雑誌論文〕（計　２件）

① Toshihiko Kato, Xiaofan Yan, Ryo Yamamoto, Satoshi Ohzahata, A Study on Round-trip Time Estimation from Unidirectional Packet Traces Using Different TCP Congestion Algorithms, International Journal On Advances in Networks and Services (peer reviewed), vol. 12, no. 1&2, pp. 1-9, 2019.

② 加藤　聰彦, 小田　淳, 厳　笑凡, 山本　嶺, 大坐畠　智, 輻輳ウィンドウとその増加分に着目したパッシブな TCP 輻輳制御アルゴリズムの推定方式, 情報処理学会論文誌（査読あり）, 第 60 巻, 第 2 号, 479-490, 2019 年 2 月.

〔学会発表〕（計　３件）

① Toshihiko Kato, Xiaofan Yan, Ryo Yamamoto, Satoshi Ohzahata, Identification of TCP Congestion Control Algorithms from Unidirectional Packet Traces, Proc. 2nd International Conference on Telecommunications and Communication Engineering (ICTCE 2018) (peer reviewed), pp. 22-17. doi:10.1145/3291842.3291922, Sept. 2018.

② Toshihiko Kato, Xiaofan Yan, Ryo Yamamoto, Satoshi Ohzahata, Applying Lomb Periodogram to Round-trip Time Estimation from Unidirectional Packet Traces with Different TCP Congestion Controls, Proc. 13th International Conference on Internet Monitoring and Protection (ICIMP 2018) (peer reviewed), pp. 1-6, Jul. 2018.

③ Toshihiko Kato, Leelianou Yongxialee, Ryo Yamamoto, Satoshi Ohzahata, A Study on How to Characterize TCP Congestion Control Algorithms from Unidirectional Packet Traces, Proc. 11th International Conference on Internet Monitoring and Protection (ICIMP 2016) (peer reviewed), pp. 23-28, May 2016.

〔図書〕（計　０件）

〔産業財産権〕

○出願状況（計　０件）

○取得状況（計　０件）

〔その他〕

ホームページ等　特になし