

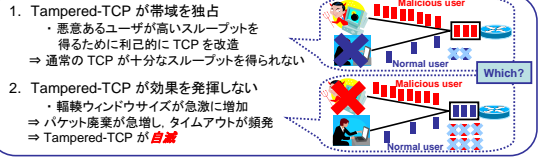
III-effects of Tampered-TCP Flows and Protection Mechanisms for Well-behaved TCP Flows

改造 TCP がネットワークに与える影響とその検出・制御方法に関する研究

大阪大学 大学院情報科学研究科
 情報ネットワーク学専攻
 中野研究室 博士前期課程2年
 丸山 純一

研究背景と目的

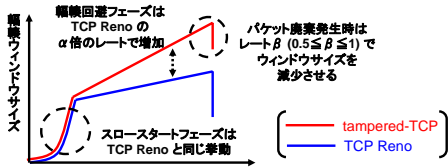
- 現在のインターネットトラフィックの大半は TCP で送信される
 - TCP の輻輳制御によって公平性が保たれる
 - 各 OS は RFC に沿って TCP の輻輳制御を実装
- 悪意あるユーザに改造された TCP が存在 **"tampered-TCP"**
 - TCP はエンド端末で動作するため、改造により高いスループットを得ようとするユーザが存在



研究目的 : tampered-TCP がネットワークに与える影響を明らかにし、その制御手法を提案する

評価対象とする tampered-TCP

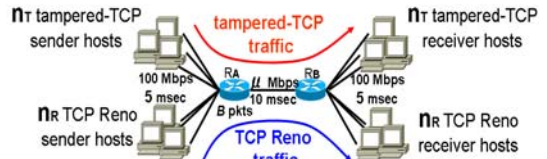
- 輻輳ウィンドウサイズの上げ幅 α ・下げ幅 β を変更した tampered-TCP に着目
 - TCP Reno は $(\alpha, \beta) = (1, 0.5)$



- Selective ACK (SACK) オプションが有効な場合と無効な場合を評価

評価モデルと評価指標

- 評価モデル

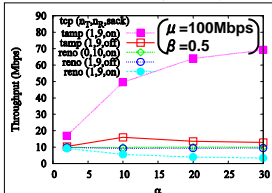


- 評価指標

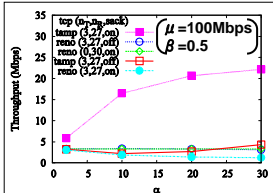
- tampered-TCP コネクションと TCP Reno コネクションのスループット

tampered-TCP の有効性

コネクション数 10 本



コネクション数 30 本

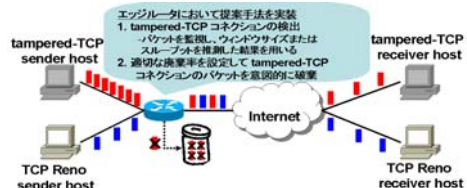


- tampered-TCP コネクションが無い場合は公平性が保たれる
- SACK を無効にした tampered-TCP コネクションは効果がほぼ無い
- SACK を有効にした tampered-TCP コネクションは TCP Reno を圧迫して帯域を獲得

ネットワーク内において tampered-TCP を制御する仕組みが必要

tampered-TCP の検出・制御手法

- エッジルータにおける tampered-TCP 検出・制御手法の提案
 - コアルータより監視するコネクションが少なく、負荷が小さい
 - コアネットワークに余計なパケットが送出されることを防ぐ

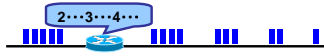


- 2つのアプローチ

- ウィンドウサイズ監視手法とスループット監視手法

ウィンドウサイズ監視手法

- TCP コネクションを監視してウィンドウサイズを推測
 - パケット間隔が開いたところをウィンドウの切れ目と判断



TCP がウィンドウ単位でパースティックにパケットを送信することを利用

- ウィンドウサイズの増減幅 (α , β) を推測
 - α : 連続する2つのウィンドウサイズの推測値の間の増加量
 - β : ウィンドウサイズが低下した時の減少量

- タンパリング性の判定
 - 誤差を許容
 - $\frac{4(1-\beta^2)}{3\alpha} < (1-\gamma_w), (0 < \gamma_w < 1) \dots (1)$
 - TCP Reno との公平性を満たさない α , β を持つコネクションを tampered-TCP と判定

- tampered-TCP コネクションの制御
 - TCP の動きを考慮して設定された p' を満たすように意図的にパケットを破壊
 - $p' = \frac{(1+\beta)}{3(1-\beta)} \alpha p \dots (2)$

2007/2/20

修士論文発表会

7

スループット監視手法

- 制御区間 i ごとにスループットの観測値 $T_o(i)$ を算出
 - sFlow や NetFlow といったトラフィック監視ツールを用いて測定

- 制御区間 i ごとにスループットの推測値 $T_e(i)$ を算出

$$B = \frac{s}{RTT \sqrt{\frac{2bp}{3}} + T_o \min\left(1, 3\sqrt{\frac{3bp}{8}}\right)} p(1 + 32 p^2) \dots (3)$$

- タンパリング性の判定
 - 誤差を許容
 - $\frac{T_o(i)}{T_e(i)} > (1+\gamma_i), (0 < \gamma_i) \dots (4)$
 - 推測値より推測値が大きいコネクションを tampered-TCP と判定

- tampered-TCP コネクションの制御

$$p'(i) = \left(\frac{T_o(i-1)}{T_e(i-1)}\right)^2 p'(i-1) \dots (5)$$

TCP の動きを考慮して設定された $p'(i)$ を満たすように意図的にパケットを破壊

2007/2/20

修士論文発表会

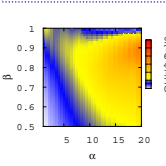
8

提案手法を用いた場合のスループット比の変化

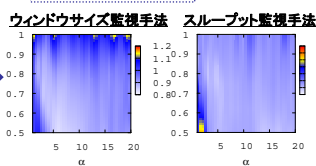
評価指標: スループット比

$$\text{スループット比} = \frac{\text{(tampered-TCP のスループット)}}{\text{(TCP Reno のスループット)}} \dots (6)$$

提案手法を用いない場合



提案手法を用いた場合



(tampered-TCP 1本, TCP Reno 20本, ボトルネックリンク 50Mbps)

広いパラメータ領域でスループット比を1に保つことが可能

2007/2/20

修士論文発表会

9

まとめ

まとめ

- tampered-TCP がネットワークに与える影響を評価
 - SACK オプションを無効にした tampered-TCP は効果がほとんど無い
 - SACK オプションを有効にした tampered-TCP は効果が高い
- エッジルータにおける tampered-TCP の検出・制御手法を提案
 - ウィンドウサイズ監視手法
 - スループット監視手法
 - ⇒ スループット比をほぼ1に保つことが可能

今後の課題

- 提案手法の実装方法の検討
- 実ネットワークにおける提案方式の性能評価

2007/2/20

修士論文発表会

10