TCP再送信タイマ管理の変更による低量DoS攻撃被害の緩和効果

CSS2013

2013年10月23日（水）　発表：3A4－1

〇細井　琢朗　（東京大学）
松浦　幹太　（東京大学）

- TCP再送信タイマ
- 低量DoS攻撃
- 文献 [5] の提案方式
- 被害のモデル化
- 元の方式での被害見積り
- 提案方式の緩和効果
  - 解析的調査
- まとめ

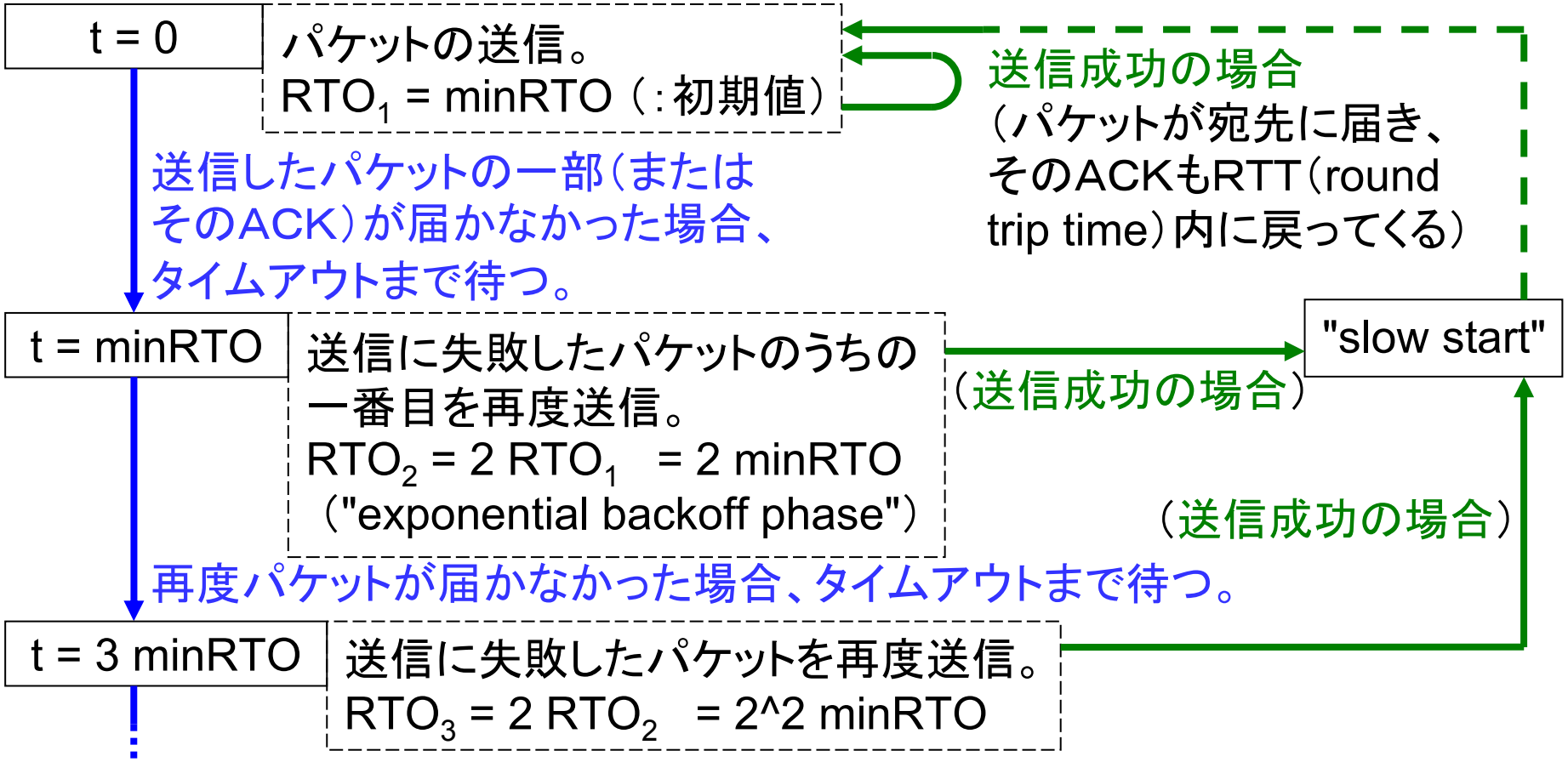
[5] 細井琢朗、松浦幹太、”低量DoS攻撃を緩和するTCP再送信タイマ管理の一検討”、第62回CSEC研究発表会、発表番号51（2013年7月）

0. 今回の成果

- （前提）
  - 低量DoS攻撃の存在（文献 [1] ）。
    - 既存のTCP RTO (retransmission timeout) 管理（ [3] [4] ）。
  - RTO の増加方法の変更（文献 [5] ）。
    - 低量DoS攻撃被害の緩和の程度は不明。
- 今回の成果
  - 文献 [5] の提案方式の、低量DoS攻撃被害の緩和効果の検証。
    - 被害のモデル化。
    - 解析的調査。

1. TCP RTO（TCP再送信タイマ）

- TCP RTO (retransmission timeout) [3] [4]

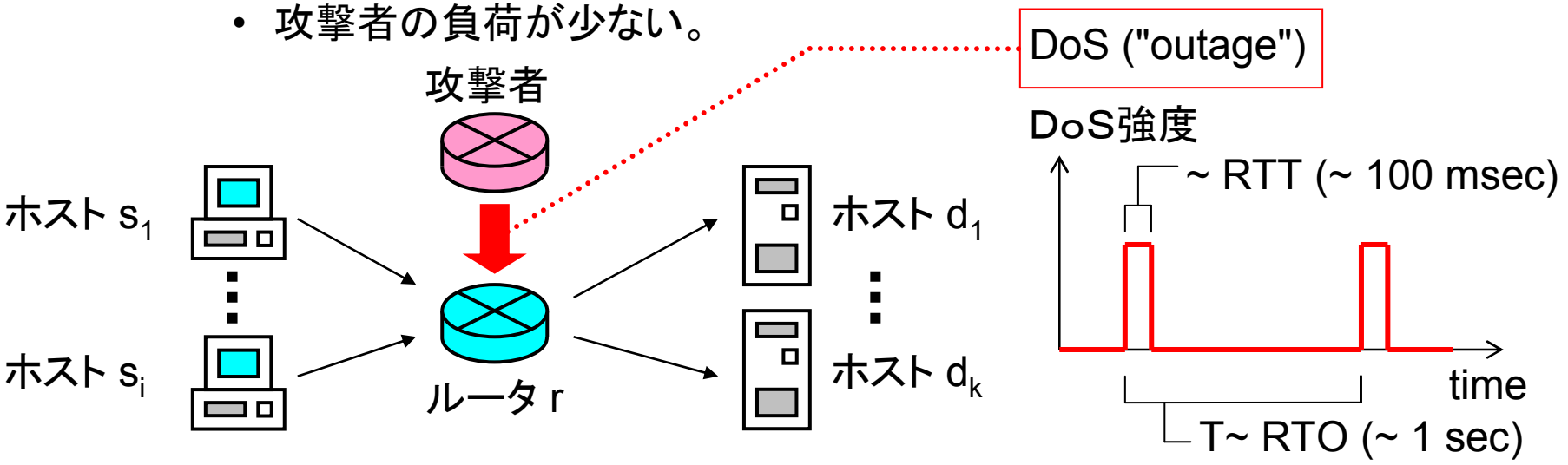


– RTO_i の値は上限（> 60 秒 [4]）に達するまで増やされる。

2. 低量DoS攻撃

– A. Kuzmanovic and E.W. Knightly
"Low-Rate TCP-Targeted Denial of Service Attacks: The Shrew versus the Mice and Elephants" [1]

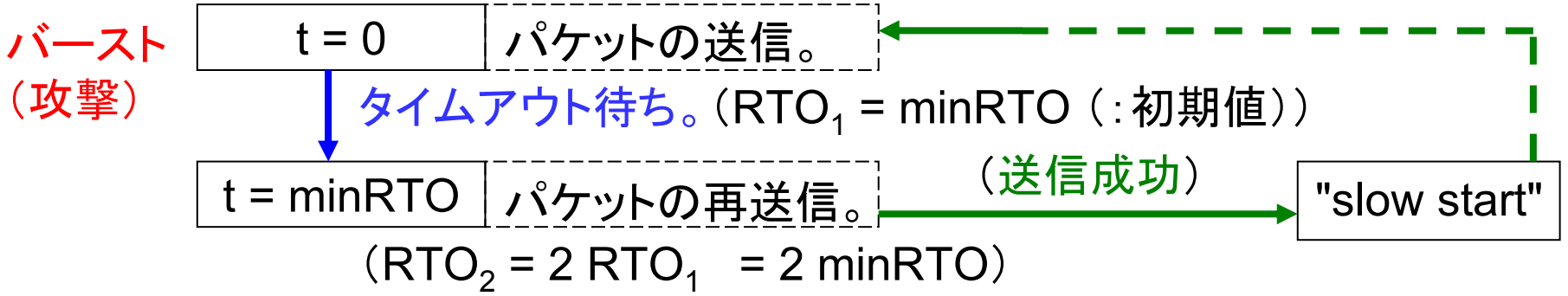
- TCPのタイムアウト機構を悪用したDoS攻撃
  – 低量
    - RTT（round trip time）程度の短時間のDoSバーストの繰り返し。
    - 攻撃が検知しにくい。
    - 攻撃者の負荷が少ない。



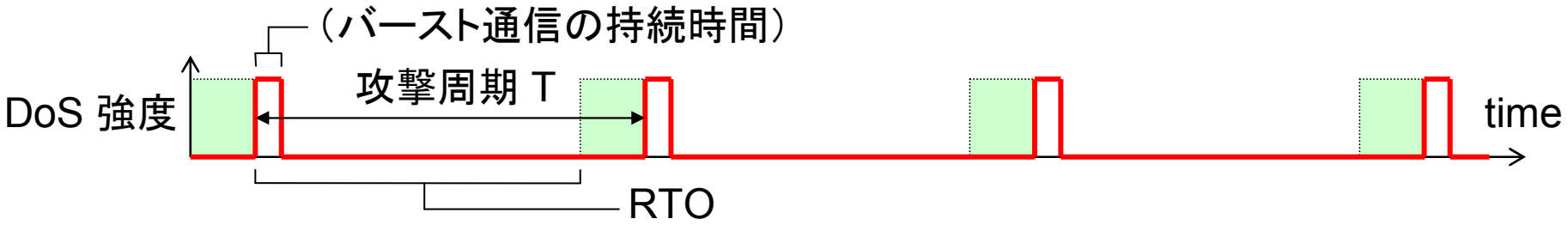
  – DoSの被害は攻撃周期 T ~ minRTO （＝1秒 [2]）のところで最大。

2．1　長期TCP通信への攻撃例

- バーストによる攻撃が完全に成功する場合。
  （T > minRTO）



  - タイムアウトから次の攻撃（バースト）まで通信できる。
    - →　平均回線容量
  - T = minRTO で通信不能。
  - 最初のバースト通信以降に始まった通信も同じ攻撃に同様に捉まる。

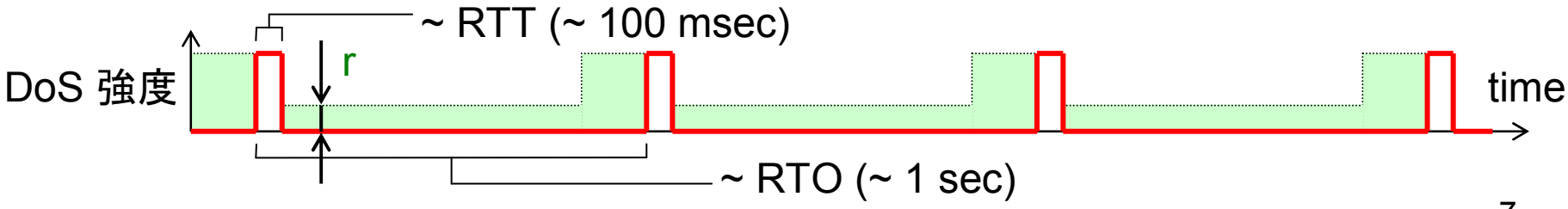


3. 提案方式 [5]

- 既存の被害緩和策
  - minRTO を一定範囲内でランダムに変更（文献 [1] ）。
    - 範囲の枷のため、僅かな緩和効果。
  - RTO の初期値（minRTO）を大きく変えると、ホスト間で不公平。
    → 初期値（minRTO）はそのままにしたい。
- 提案： RTO の増加方法の変更（文献 [5] ）
  - 要件：
    - 連続するタイムアウト待ちで指数的に増加すること。
      （TCP の輻輳制御の一環として）
  - $RTO_i = (1 + u)\, RTO_{i-1}$　　$(0 < u < 1)$
    - RTO_i （i 回連続するタイムアウト待ち）
      $= (1 + u)^{(i - 1)}\, minRTO$
  - minRTO の整数倍でない系列。
  - 連続するタイムアウト待ちが明けたときに、それまで受けていた周期 T = minRTO の低量DoS攻撃に重ならない機会がどこかで生まれる。
    → DoS攻撃の被害緩和。

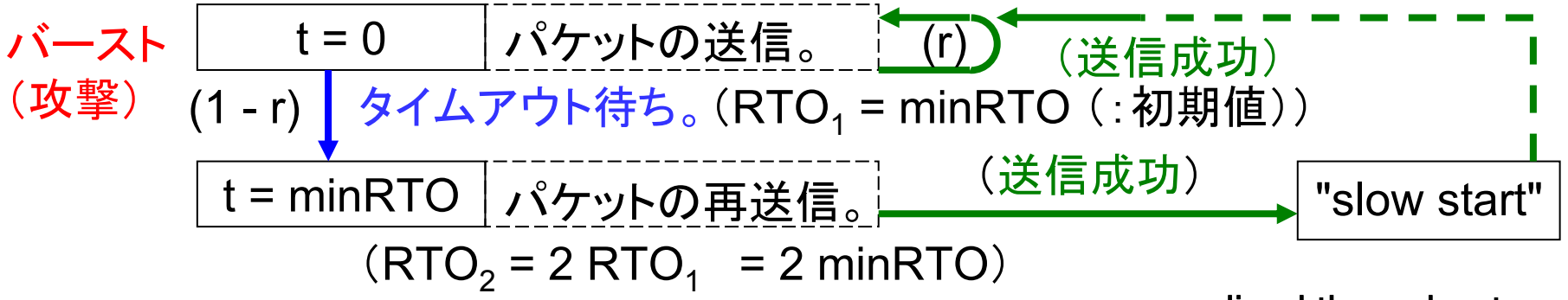
4.　被害のモデル化

- 低量DoS攻撃の被害の簡単化（モデル化）
  - 各バースト通信の際、全TCP通信のうちの一定の回避率（r）の分だけが攻撃を逃れて、パケットの送信に成功する。
    - 各バースト通信は RTO の時間スケールに較べて非常に短いと見なす。
  - 残りの通信はパケット送信に失敗し、タイムアウトが明けるのを待つ。
  - バースト通信がないときには、全てのパケット送信は成功する。
- 低量DoS攻撃のバーストを避ける要因：
  - 攻撃者が「低量」を志向。
    - 検知を逃れるために、攻撃の強度（バーストの強さ、持続時間）を抑制。
  - 計時の粒度
    - RTO の計時の粒度が粗いと、攻撃周期を逃れることがある。
  - 文献 [1] で提案された対策：
    - minRTO を（一定の範囲内で）ランダムに設定。

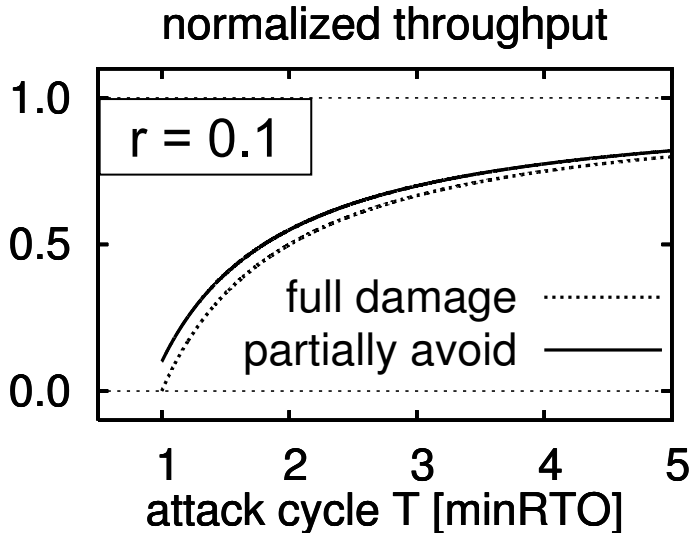


5．1　元の RTO 管理での被害（1）

- （T > minRTO）



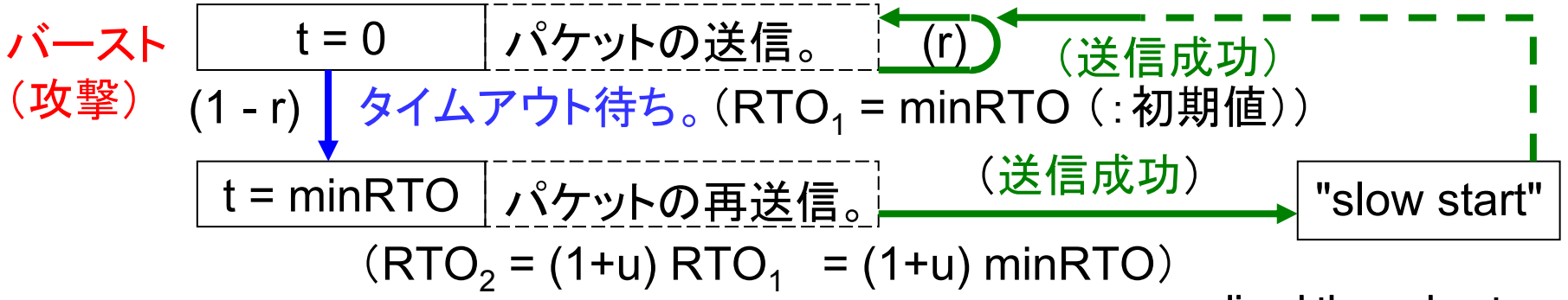
– 正規化平均回線容量：
$q = (T - (1 - r)\,\mathrm{minRTO}) / T$



- バーストによる攻撃が完全に成功する場合は、上式で r = 0 としたものになる。

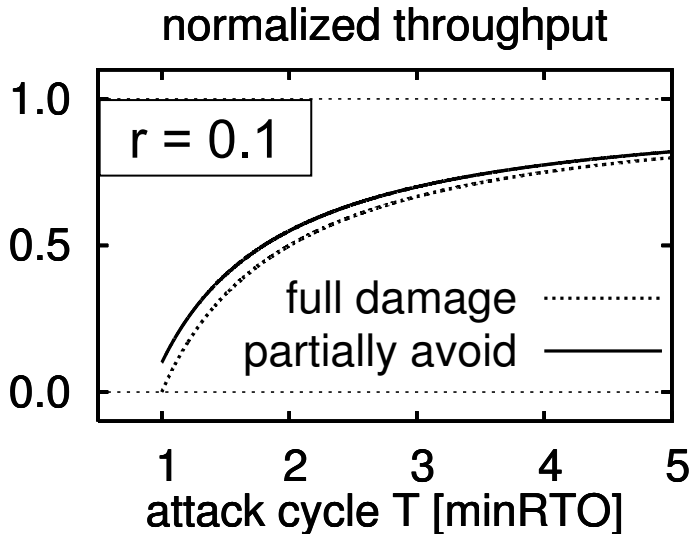
５．２　緩和効果の評価（１）

- （T > minRTO）



– 正規化平均回線容量：
  q = (T - (1 - r) minRTO) / T

– 元の RTO 管理の場合と同じ。
（効果はないが、悪影響もない。）



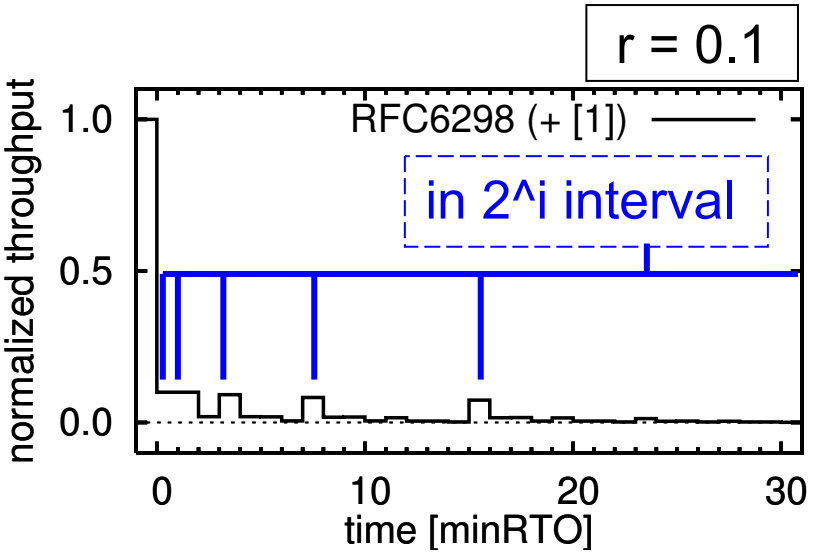
6．1　元の RTO 管理での被害（2）

- （T = minRTO）

– パケット送信に連続失敗　／　成功　／　その他（多数）。

6．2　元の RTO 管理での被害（2）（続き）

- （T = minRTO）
  - 正規化平均回線容量の上限：　q ≤ r
  - オーダーの見積り
    - 最初のバースト通信から i 回連続してパケット送信に失敗し、タイムアウトを待っている通信のタイムアウト時刻：
      t(i) = $\Sigma_{k=0}^{i-1}$ 2^k * minRTO　= (2^i - 1) minRTO
    - 次の（連続した）タイムアウト待ちをしている割合　~ o(1)
      パケットの送信に成功した割合　~ o(r)
    - その次のバースト通信の際、送信に成功する割合　~ o(r^2)
      （．．．　t(i+1) まで）
    - 正規化平均回線容量（ t(i) から t(i+1) まで）　~ o(r)/2^i + o(r^2)



6．3　緩和効果の評価（2）

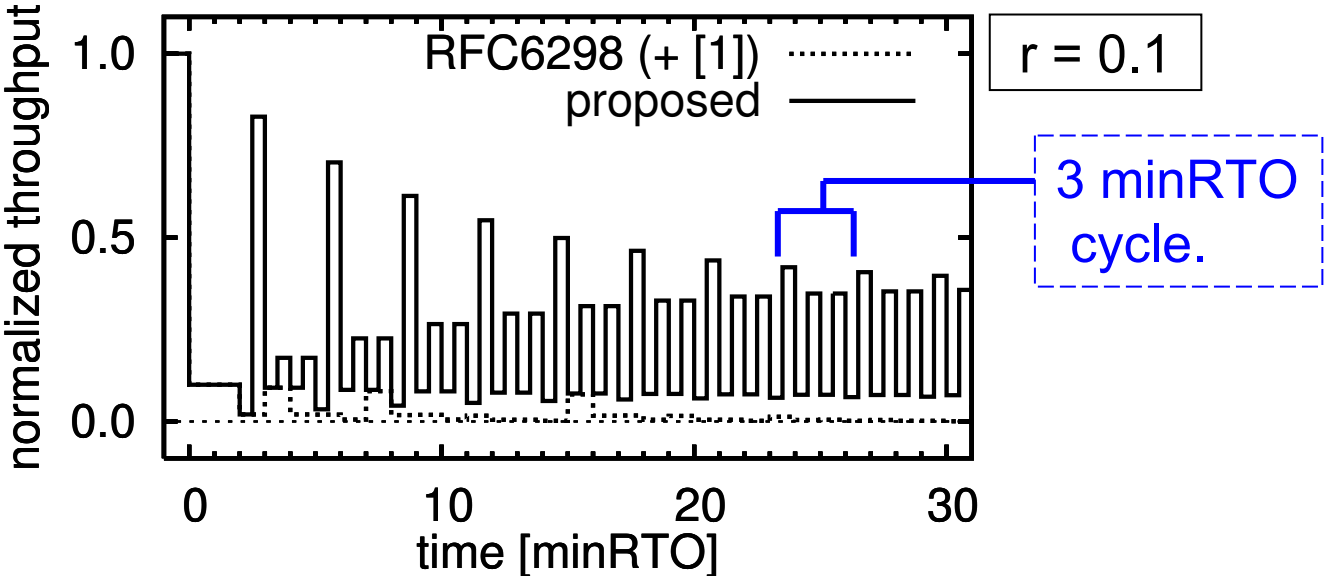
- （T = minRTO）

– 攻撃被害の連続から逃れる。

６．４　緩和効果の評価（２）

（続き1）

- （T = minRTO）



– 上側（バースト後、+u）と下側（バースト直後）の値がそれぞれ収束しているように見える。
– それぞれ 3*minRTO 周期で変化。

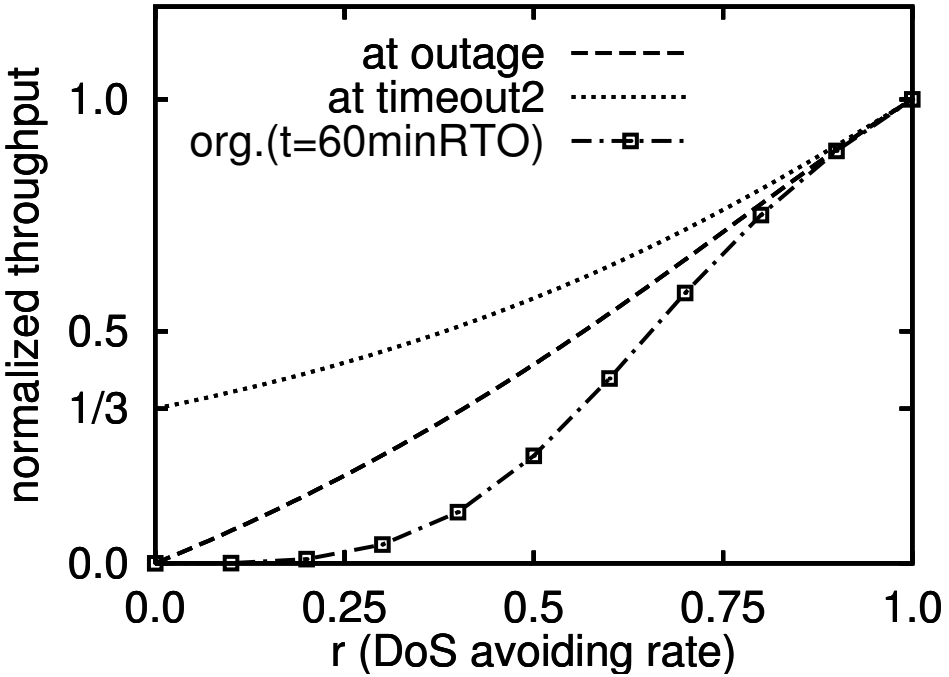
６．５　緩和効果の評価（２）　（続き2）

- （T = minRTO）
  - それぞれの状態にある割合を定義。
    - t = k*minRTO のバースト通信直後（ k ≥ 0 ）
      A_k　:通常の通信をしている割合。
      B_k　:一回目のタイムアウト待ちに入った割合。
      C_k　:二回連続のタイムアウト待ちに入った割合。
      D_k　:二回連続のタイムアウト待ちを続けている割合。
    - t = (k+u)*minRTO でのそれぞれの割合:
      A_(k+u) 、B_(k+u) 、C_(k+u) 、D_(k+u)
  - 解析的に以下を証明した。
    - 0 ≤ (A_0 , B_0 , C_0 , D_0) ≤ 1 , 0 ≤ r ≤ 1 のとき、
      正規化平均通信量
      q_(3k, 3) = (1/3) [u A_(3k+1) + (1-u) A_(3k+1+u)
      + u A_(3k+2) + (1-u) A_(3k+2+u)
      + u A_(3k+3) + (1-u) A_(3k+3+u)]
      が単調に変化し、[0,1] の間に収束する。
      （増／減は、初期条件と、(1-u) と r の大小の関係で決まる。）

６．６　緩和効果の評価（２）

（続き3）

- （T = minRTO）
  - 収束値：



  - 正規化回線容量
    - バースト通信直後（"at outage"）
      q = A_k　　→ [1 - (1-r)^2] / [1 + (1-r) + (1-r)^2]
    - バースト通信後 +u（"at timeout2"）
      q = A_(k+u) = A_k + D_k　→ 1 / [1 + (1-r) + (1-r)^2]
    - 回避率 r = 0 の場合でも回線容量は 0 にならない。
      q = [u A_k + (1-u) A_(k+u)] / 2　　→ **(1-u) / 3**

7. まとめ

- 低量DoS攻撃 [1] の被害緩和を目指した、TCP 再送信タイマの管理方法の変更の提案 [5] について、その効果を調査。
  - 被害のモデル化（一定の回避率 r ）。
  - 解析的に調査。
    - 攻撃のバースト通信の周期 T が再送信タイマの最小値 minRTO よりも大きい場合： 提案方式での被害は元の場合と同じ。
      - 緩和効果は無いが、悪影響も無い。
    - 攻撃のバースト通信の周期 T が再送信タイマの最小値 minRTO に一致する場合： 有意な緩和効果。
      - 特に、バースト通信で全てのパケット送信が失敗する場合（回避率 r = 0）でも、平均回線容量が 0 にならない。
- ＜今後の課題＞
  - 既存のネットワーク環境への適合性の確認。
    - 特に輻輳制御との適合性。
  - 実験による性能評価。

A. 参考文献

- [1]（TCP RTO を悪用したDoS攻撃）
  A. Kuzmanovic and E.W. Knightly, "Low-Rate TCP-Targeted Denial of Service Attacks: The Shrew versus the Mice and Elephants", Proc. ACM SIGCOMM '03, pp.75-86 (August 2003).
- [2]（TCP minRTO = 1 秒）
  M. Allman and V. Paxson, “On Estimating End-to-end Network Path Properties”, Proc. ACM SIGCOMM ‘99, pp.263-274 (September 1999).
- [3]（TCP）
  J. Postel (Ed.), "Transmission Control Protocol", Internet RFC 793, IETF (September 1981).
- [4]（TCP 再送信タイマ管理）
  V. Paxson, M. Allman, J. Chu, M. Sargent, "Computing TCP's Retransmission Timer", Internet RFC 6298, IETF (June 2011). (This obsoletes RFC 2988.)
- [5]（TCP 再送信タイマ管理の変更の提案）
  細井琢朗、松浦幹太、”低量DoS攻撃を緩和するTCP再送信タイマ管理の一検討”、第62回CSEC研究発表会、発表番号51（2013年7月）