

2D-2

異常な通信シーケンスを生成可能な TCP 試験システムの設計

大岸 智彦 長谷川 亨 加藤 聡彦

KDDI 研究所

1. はじめに

インターネットの普及に伴い、TCP/IP を用いた通信が盛んに行われている。このうち、TCP は、エンドエンドでフロー制御や輻輳制御を行うことにより、ネットワークの帯域や混雑度に応じた通信を可能とする。しかしながら、相手側のシステムが異常な振舞いを行った場合に、スループットの低下やコネクションの異常切断などを引き起こす場合がある^[1]。そこで筆者らは、故意に異常な通信シーケンスを生成することにより、各種 OS に実装された TCP の振舞いを試験するシステムを設計した。本システムは、本来のプロトコル手順に従わない振舞いを行う箇所を記述したテストシナリオを実行することにより、異常な通信シーケンスを生成する。本稿では、TCP 試験システムの設計について述べる。

2. 要求条件

TCP 試験システムは、各種 OS の TCP の実装の違いや、正常な通信シーケンスにおいて検出し難い実装上の不具合、一定長以上の不連続なセグメントを続けて受信した場合や TCP の状態や内部変数がある条件を満たす場合にのみ発生する不具合などを検出することを目的とする。そこで、本システムは、以下に示すようなテストシナリオを記述可能とする。

- (1) 通常の通信シーケンスと異なる振舞いを行う箇所のみをテストシナリオ (以降、シナリオと呼ぶ) に記述する。
- (2) 任意のタイミングで、任意のパラメータを持つ TCP セグメントを生成可能とする。TCP セグメントは、以下のタイミングで生成する。
 - 特定のシーケンス番号や応答確認番号を持つ TCP セグメントを受信した場合
 - 特定のシーケンス番号や応答確認番号を持つ TCP セグメントを送信しようとした場合
 - 予め設定したタイマが終了した場合
- (3) ネットワーク上での TCP セグメントの紛失を想定するため、送受信したセグメントに対して状

Design of TCP Test System Generating Misbehaving Communication Sequences
Tomohiko Ogishi, Toru Hasegawa and Toshihiko Kato
KDDI R&D Laboratories

態/内部変数を更新するか否かを設定可能とする。

(4) SACK^[2]や拡張ウィンドウなどの新しい TCP の実装を試験するため、これらの仕様に対応する。

3. システム設計

3.1 シナリオ記述方法

シナリオの記述例を図 1 に示す。シナリオは、ヘッダ部分とコンテンツ部分に分けて記述する。ヘッダ部分には、試験対象とする TCP コネクションを指定する発着の IP アドレスおよびポート番号、および、コネクション確立時に使用する TCP オプションを記述する。図中のシナリオでは、MSS を 10、ウィンドウスケールを 0 とし、SACK、TIMESTAMP のオプションを使用可としている。

```

<header>
src-addr=192.168.0.1
dst-addr=192.168.0.2
dst-port=20
syn-opt=mss(10), sack, timestamp, ws(0)

<content>
① recv seq=1 var-upd=ON : send seq=1 ack=11 flag=(ack) win=20 var-upd=ON
② recv seq=11 var-upd=OFF : ignore
③ send seq=1 ack=11 var-upd=yes : ignore
④ wait 1 : send seq=1 ack=11 flag=(ack) win=30 var-upd=OFF
⑤ recv seq=11 var-upd=ON : ignore
⑥ recv seq=21 var-upd=OFF : ignore
⑦ recv seq=31 var-upd=ON : send seq=1 ack=21 sack=(31-41) flag=(ack) win=30 var-upd=ON
: send seq=1 ack=21 sack=(31-41) flag=(ack) win=30 var-upd=ON
: send seq=1 ack=21 sack=(31-41) flag=(ack) win=30 var-upd=ON
: send seq=1 ack=21 sack=(31-41) flag=(ack) win=30 var-upd=ON
⑧ recv seq=70 var-upd=ON : send seq=1 flag=(rst) win=30 var-upd=ON

```

図 1 シナリオの記述例

コンテンツ部の各行には、セグメントの送受信などの個々のイベントにおいて実行される異常な振舞いを記述する。各行には、シナリオが実行される条件と、条件に合致した場合のアクションを記述し、それらの間を";"で区切る。①は、シーケンス番号が 1 のセグメントを受信した場合、seq=1 (シーケンス番号が 1)、ack=11 (応答確認番号が 11)、win=20 (ウィンドウサイズが 20) の ACK を送信する。シーケンス番号および応答確認番号は、初期値からの相対値で示す。図中の var-upd は、条件またはアクションに伴う内部変数の更新を行う (ON) か否 (OFF) かを示す。②は、seq=11 のセグメントを受信した場合、内部変数の更新を行わず、それに伴うセグメントの送信を行わないことを示す。従って、seq=11 のセグメントがネットワーク上で紛失し、試験システムに届かなかった場合と等価となる。③は seq=1, ack=11 のセグメ

ントを送信しようとした場合に、それを中止することを示す。④は、1タイムスロット (=500 ミリ秒) 経過した場合に行われるアクションを示す。⑦では、受信セグメントの条件により、複数のアクションが実行される場合を示す。⑧では、seq>70 の場合に、RST セグメントを送信し、TCP コネクションを解放することを示す。

3.2 シナリオインタプリタの動作

シナリオは、シナリオインタプリタに基づき実行される。シナリオインタプリタは、実行中の行(カウンタ)を管理する。シナリオインタプリタの基本的な動作を図2に示す。シナリオインタプリタは、検出した送受信セグメントが、試験対象のTCPコネクションかどうか、カウンタの条件に合致するかどうかを判断し、双方が真ならシナリオに記述されたアクションを実行し、そうでなければ通常の振舞いを実行する。条件に合致した場合はカウンタを更新する。シナリオが終了している場合には、常に通常の振舞いを実行する。

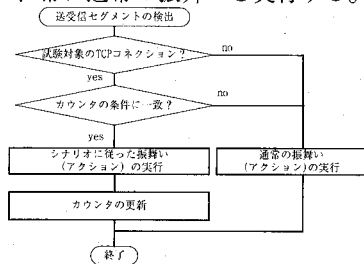


図2 シナリオインタプリタの基本動作

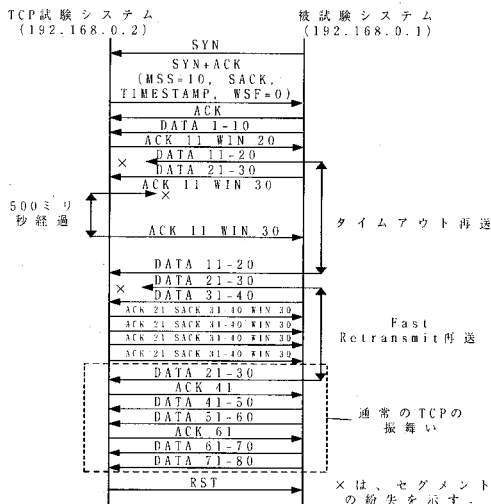


図3 シナリオ実行時の通信シーケンス

図1のシナリオを用いて、TCP試験システムから数100バイト以上のデータを送信した場合に、実際に発生する通信シーケンスを図3に示す。被

試験システムには、TCPが持つ輻輳制御により発生するセグメントと、シナリオに従って送信されるセグメントがテスト入力として与えられる。これにより、被試験システムにおいてタイムアウト再送やFast Retransmit再送を意図的に発生させ、これらの動作を試験することが可能となる。

3.3 システム構成

本システムの全体構成を図4に示す。TCPプロトコル処理部は、通常の振舞いおよびシナリオに従った振舞いを含むTCPのプロトコル処理を行う。検出したセグメントのTCPコネクションやシナリオの条件に基づき、上記のいずれを行うかを判断する。試験実行プログラムは、TCP上で動作する試験用のアプリケーションプログラムを表す。本システムでは、ftpやtcpなどの汎用のアプリケーションを用いることを想定している。試験環境設定プログラムは、シナリオのアップロードや参照などの機能を提供する。TCPプロトコル処理部では、実際に行われた通信シーケンスを通信ログとして記録する機能を持つ。通信ログには、送受信されたセグメントの発生時刻とパラメータに加え、セグメント発生時のカウンタ、内部変数を更新したか否かなどの情報を記録する。また、シナリオに従ったため、送受信されなかったイベントも記録する。

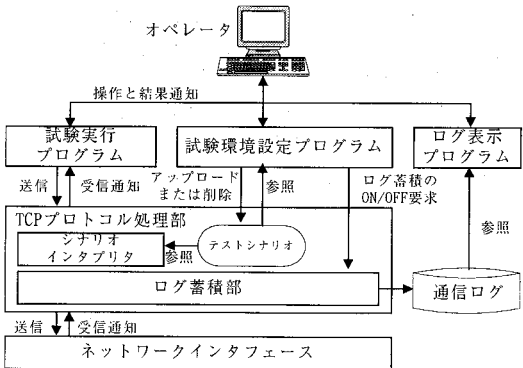


図4 システム構成

4. まとめ

本稿では、TCP試験システムの設計について述べた。本システムは、異常な振舞いを行う条件を記述したシナリオと、それを実行するシナリオインタプリタにより、異常な通信シーケンスを生成可能とする。最後に日頃ご指導頂く KDDI 研究所 浅見所長に感謝する。

参考文献

- [1] S. Savage et al., "TCP Congestion Control with a Misbehaving Receiver," SIGCOMM CCR, October, 1999.
- [2] M. Mathis et al., "TCP Selective Acknowledgment Options," RFC 1818, October 1996.