

プロトコル言語 PROMELA の時間特性の拡張

2D-1

太田 賢* 中野 宣政** 渡辺 尚* 水野 忠則*

* 静岡大学工学部 ** 三菱電機(株)名古屋製作所

1 はじめに

プロトコルは通信媒体を介して、ネットワーク内の計算機の間で並列に動作するものであり、効率的であまいでない通信プロトコルの設計が必要となる。この目的のため通信サービス、プロトコルの記述には形式記述技法(FDT)が開発され、その記述言語として LOTOS、Estelle、SDL、ベトリネット、Z、代数記述などがある。^[1]

一方、マルチメディア、FA等の分野が「要求する所定時間以内での通信サービスの保証」すなわちタイムクリティカル通信^[2]の実現を要求している。これまでの通信サービスというのは実時間というよりも時間順序を主体としたものであった。

本研究は形式記述法の言語の一つである PROMELA^[3]を時間特性について拡張し、仕様記述に対し絶対時間を形式的に規定可能とするものである。仕様記述はシミュレータにより、動作のトレースや検査が可能である。本稿では PROMELA とそのシミュレータ SPIN^[4]について概観した後、時間を拡張した T-PROMELA と T-SPIN^[5]について報告する。

2 PROMELA/SPINの特徴

PROMELA (PROtocol MEta Language)はプロトコル設計用の言語であり、送受信や非確定処理の記述のためのガードコマンド、セレクトコマンドなどはコンカレントプログラミング言語 CSP、変数の宣言や式などはC言語の影響を受けている。

○プロセス定義内に、記述対象を有限状態機械として記述する。

○変数の型は、チャンネル型、整数型、バイト型、

ビット型、メッセージ型が用意されている。

SPINはPROMELAにより記述されたプロトコル検証モデルをシミュレーション、バリデーションするものである。シミュレータは高速にプロトコル動作を参照でき、バリデータは全数探索(可達性解析)を行なう。検証の種類としては、表明、進行性(デッドロック)、時間的要求、終了状態の有効性がある。

3 T-PROMELAのシンタックス

PROMELAに時間の概念を取り入れて、T-PROMELAへと拡張することにより、以下のよな記述を可能とした。

○時間型の変数

実数型で、時間を記述するための変数

例 `time timeout = 5.0`

時間型変数 `timeout` を初期値 5.0 として宣言する。

○時間変数 `gtime`

シミュレーション開始からの時間経過を示すシステム予約型の変数

例 `cur_time = gtime;`

現在の経過時間を `cur_time` に代入する。

○文実行時間記述

明示的な実行時間の記述

例 `channel !data @ 10`

チャンネルに `data` を送信するのに 10ms かかる。

この拡張に基づき、次のような記述が可能である。

○タイムアウトなどの明示的な記述

例 `chout ! data;`

`st_time = gtime;`

`/* タイマのスタート */`

`do`

`:: chin ? ack` 確認応答受信

`:: (gtime - st_time > 5000)`

`/* タイムアウトした`

Time Oriented Protocol Language T-PROMELA

Ken Ohta* Nobumasa Nakano#

Takashi Watanabe* Tadanori Mizuno*

*Shizuoka University, Faculty of Engineering

3-5-1 Johoku, Hamamatsu 432, Japan

#Mitsubishi Electric Corp. NAGOYA WORKS

5-1-14 Yada-minami, Higashi-ku, Nagoya 451,

Japan

5000(ms)=5(s)待った */

o d

チャンネルchoutにdataを送信した後チャンネルchinよりackを受信するがそのタイムアウトを5秒に設定する。

○表明文による、ある実行列がある時間以内に完了しなければならないというような実時間要求の記述

```
例 st_time = gtime ;
    chout! req; /*トランザクション*/
    chin? ack ;
    assert( gtime-st_time < 2000 );
    トランザクションが2000(ms)=2(s)以内に終了
    しない場合表明違反としてユーザに通知する。
```

4 T-SPINの特徴

T-PROMELAで記述した仕様をシミュレーションするツールがT-SPINである。これにより、動作の確認や、実行時間の評価、実時間要求の検査ができる。T-SPINの構造を図1に示す。

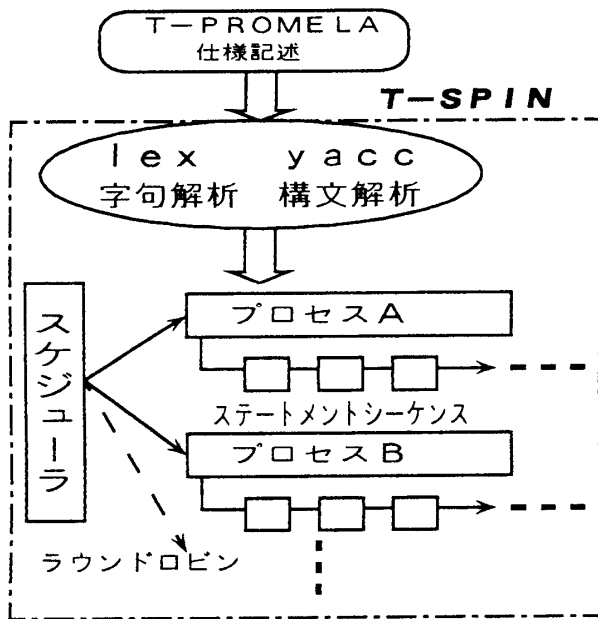


図1 T-SPINの構造

T-SPINは以下を仮定している。

○ラウンドロビン方式

T-PROMELAは並行プロセスを扱うが、プロセスのスケジューリングはラウンドロビン方式で行なう。

○対象モデル

1マシン(1CPU)内の通信サービスに限定する。

○プロセス間通信

通信は1マシン中のプロセス間通信を扱う。

○実行時間の内部計測

各文に実行時間が記述してあった場合はその値を実行時間とし、記述のない場合はシミュレータが実際の実行時間を計測して、その値を用いる。図2にその計測方法を示す。

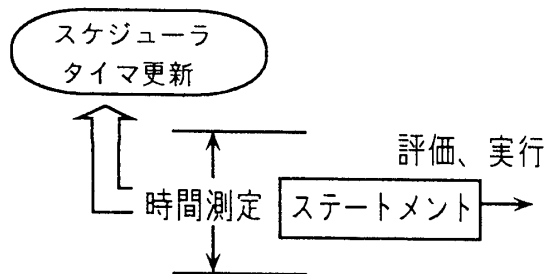


図2 実行時間計測

5 おわりに

実時間の要求を含んだ通信サービスの仕様を、T-PROMELAで形式的に記述する方法、及びその仕様記述のシミュレータT-SPINについて報告した。仕様記述内にタイムアウトの時間などを明示的に記述でき、またその仕様の時間的検査、評価ができるようになった。現在の対象モデルは1マシン内の通信サービスである。今後の課題は、これを分散システム上での通信サービスに発展させることであり、そのための構文拡張及びシミュレータの実現方式を検討中である。

参考文献

[1]水野忠則編：通信システムの形式記述技法の標準化、情報処理、Vol.31, No.1, PP.2-81(1990).
 [2]Nobumasa Nakano: Time Critical Communication Architecture in Factory Automation, JSPE-IFIP WG5.3 Workshop on THE DESIGN OF INFORMATION INFRASTRUCTURE SYSTEMS FOR MANUFACTURING, PP.241-252(1993)
 [3]厚井、妹尾、高田、井手口、石坂： LANにおけるタイムクリティカル通信プロトコルの提案と評価、信学論、Vol.J76-B-1, No.8, PP.882-891 (1993).
 [4]Gerard J. Holzmann: Design and Validation of Computer Protocols, PRENTICE HALL(1991).