通信プロトコルにおける状態遷移表現の生成法

3H-4

斉藤 誠*、 光永 聖**、 田代 勤*、 鷹田 憲久*
*(株)日立製作所 システム開発研究所 ** 同・大森ソフトウェア工場

1．まえがき

コンピュータネットワークの高度化、高信頼化が進むにつれ、システムの高信頼化機能を含む大規模かつ複雑な通信プロトコルを効率的かつ高信頼に設計することが重要な課題となっている。通信プロトコルの設計における問題は、その仕様にあいまいさ、矛盾が含まれていることにより後戻り作業が生じ、開発が遅れること、あるいは上記仕様不備によって製品が事故を起こすことである。このため、通信プロトコルの仕様を厳密かつ完全に記述するための仕様記述法の確立が重要となる。現在、通信プロトコルの設計においては、理解が容易な通信シーケンス図から網羅的記述に向く状態遷移表を生成するということが行われている。ところが、通信シーケンス図からの状態遷移表の生成は設計者の経験に依存しており、非効率的かつ品質にばらつきが出る作業となっている。本稿では、通信プロトコルの通信シーケンス図による表現から状態遷移表現を生成する一方法を提案する。

2．通信プロトコルのモデル化

一般に通信機能は階層化されている。そこで、ここでは通信プロトコルは階層構造を成すものとし、各階層の通信プロトコルを実行するプロセスの動作を以下の有限状態機械Mでモデル化する。

$M = (X, Q, Z, \delta, \omega, q_0)$

X：入力集合、Q：状態集合、Z：出力集合

δ：$X \times Q \rightarrow Q$なる状態遷移関数

ω：$X \times Q \rightarrow Z$なる出力関数

q_0:初期状態

但し、入力は、各時点でただ一つ与えられるものとする。ここで、Mにおける入出力は上位階層、下位階層およびタイマーとの間に存在し、Mからタイマーへはタイマー起動、停止指示、タイマーからMへはタイムアウト通知が与えられるものとする。

3．通信プロトコルの状態遷移表現の生成手順

本稿では、通信シーケンス図から状態遷移表現を生成する手順を提案する。この手順は、応答を要求するメッセージに着目し、これを基に状態を決定するところに特徴がある。以下に、与えられた一連の通信シーケンス図から状態遷移表現を生成する手順を示す。但し、ここでは上位階層および下位階層からの不当なプリミティブは無視する。

＜ｓｔｅｐ１＞応答を要求する送信メッセージに対応させて状態を設定する。

＜ｓｔｅｐ２＞応答待ち以外のタイミングで応答を要求するメッセージを受信した場合には、その前状態として、そのメッセージ対応の状態を設定する。但し、障害発生による割込み入力を除く。

＜ｓｔｅｐ３＞＜ｓｔｅｐ１＞、＜ｓｔｅｐ２＞で状態の設定が行なわれていない場合について、入力後の状態として、別状態を設定する。

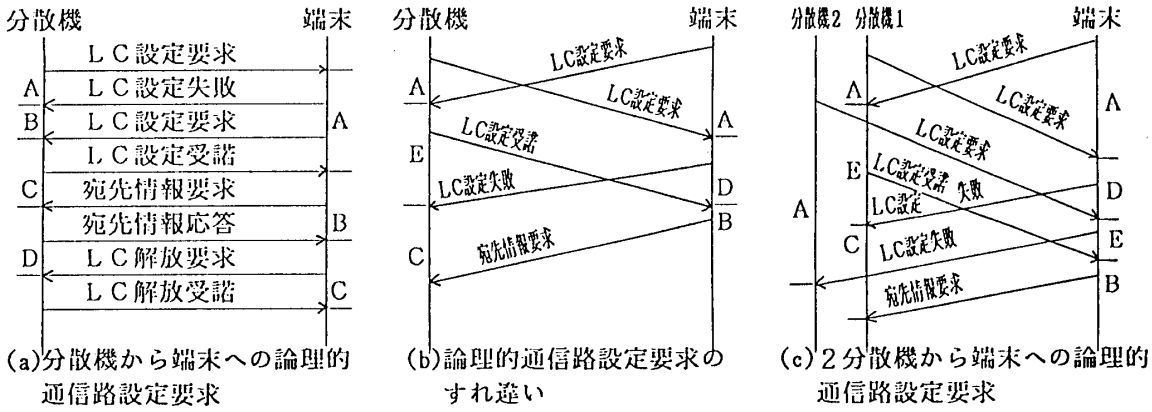
＜ｓｔｅｐ４＞各状態におけるアクションを調べ、等価とした状態においてアクションが異なる場合には、その都度別状態として設定する。また、アクションが同じになる状態は統合する。

4．適用例

分散機とそれに接続される端末との間の論理的通信路設定方式の通信シーケンス図から状態遷移表現を生成した例を示す。

A Generation Method of State Transition Representation for Communication Protocols

Makoto SAITOH, Satoshi MITSUNAGA, Tsutomu TASHIRO, Norihisa KOMODA, HITACHI Ltd.



(a)分散機から端末への論理的通信路設定要求　(b)論理的通信路設定要求のすれ違い　(c)2分散機から端末への論理的通信路設定要求

ＬＣ：論理的通信路　　分散機２：分散機１の予備機
Ａ～Ｅ：状態

図１　分散機－端末間における論理的通信路設定手順の例

４．１分散機－端末間における論理的通信路の構成

分散機－端末間の論理的通信路は、端末とそれが接続される複数の分散機との間に一本ずつ設定される。また、分散機には通常用いる分散機とこれらの分散機の予備の分散機が存在し、通常用いる分散機と端末との間の論理的通信路は、システムの起動時に設定される。予備の分散機と端末の間の論理的通信路は、通常用いている分散機がダウンした時点で設定される。

表１　分散機の状態遷移表（一部）

入力＼状態	A ＬＣ 未設定	B ＬＣ設定 要求待ち	C 宛先情報 待ち	D ＬＣ解放 要求待ち	E LC設定要求 すれ違い
ＬＣ設定 要求	ＬＣ設定 受諾送信 E	ＬＣ設定 受諾送信 C	－	－	－
ＬＣ設定 失敗	B	－	－	－	C
宛先情報 要求	－	－	宛先情報 送信 D	－	－
ＬＣ解放 要求	－	－	－	ＬＣ解放 受諾送信 －	－

注）－：未定義，ＬＣ：論理的通信路

４．２分散機－端末間における論理的通信路設定方式の状態遷移表の生成

分散機－端末間の論理的通信路設定方式の通信シーケンス図による表現(一部)および３節に示した手順に従って設定した状態を図１に示す。図１(a)において、応答を要求するメッセージは、論理的通信路設定要求、宛先情報要求および論理的通信路解放要求であり、これらのトリガーとなる入力後の送信側の状態は、これらの要求対応にとられている。但し、図１(b)の端末では、論理的通信路設定要求を送信してからその応答が得られるまでに論理的通信路設定要求を受信したため、その入力後の状態として入力前とは異なる状態が設定されている。また、図１(a)の分散機では、応答待ち以外のタイミングで宛先情報要求を受信したため、これを受信する前の状態として宛先情報要求対応の状態が設定されている。図１の通信シーケンス図から生成した分散機、端末の状態遷移表をそれぞれ表１、表２に示した。

表２　端末の状態遷移表（一部）

入力＼状態	A ＬＣ 未設定	B 宛先情報 待ち	C ＬＣ解放 待ち	D LC設定要求 すれ違い	E ＬＣ設定 要求競合
ＬＣ設定 受諾	宛先情報 要求送信 B	－	－	宛先情報 要求送信 B	宛先情報 要求送信 B
宛先情報	－	ＬＣ解放 受諾送信 C	－	－	－
ＬＣ設定 要求	ＬＣ設定 失敗送信 D	－	－	ＬＣ設定 失敗送信 E	－
ＬＣ解放 受諾	－	－	－	－	－

注）－：未定義，ＬＣ：論理的通信路

５．おわりに

本稿では、通信シーケンス図から状態遷移表現を得る手順を提案した。本方式は、上記作業の計算機支援のために有効である。