情報処理学会第39回(平成元年後期)全国大会

インターネットワーク診断システム(1)

障害診断の技法

5T-5

村上健一郎　　菅原俊治

(NTT ソフトウェア研究所)

1. はじめに

近年、ワークステーションの普及に伴い、それらをLAN(Local Area Network)で結合した分散処理システムの構築が行われるようになった。これらのシステムの特徴は、さまざまな製造メーカの装置から構成される点である。このようなマルチベンダシステムでは、通信プロトコルとして、PCからメインフレームまでサポートされているTCP/IP(Transmission Control Protocol/Internet Protocol)が、使用される。最近では、このような独立したネットワークを、ルータなどのネットワーク結合装置によって接続し、全体をあたかも一つのネットワークのごとく動作させる、インターネットワークの構築も行われるようになった。

インターネットワークは、膨大な数、および多種多様な要素から構成され、しかも、それらは地理的に分散している。このため、一旦、事故が発生すると、その原因の追求が極めて困難であり、解決までに長い時間を要する。これに加え、大規模ネットワークにおける複雑な問題を解決できるエキスパートが少数であるということも、問題をますます困難なものとしている。このような問題を解決するため、我々は、ネットワークを監視し、異常の発生や、その兆候を発見して、速やかに問題を解決するインターネットワーク監視・診断エキスパートシステム(Large Internetwork Observation and Diagnostic Expert System - LODES)を開発中である。本論文では、障害診断に用いられる技法とエキスパートシステムのアーキテクチャとの関係について説明する。

2. 診断方法の特徴

診断の対象となるプロトコルは、インターネットワークを構築するために米国のARPANETで開発され、さまざまなコンピュータ上でインプリメントされているTCP/IPプロトコル群である[1]。インターネットワークでは、個々のLANは、ルータにより、相互に接続されている。ルータとは、パケットをネットワーク間で中継する装置である。地理的に離れた場所にあるLAN上のルータどうしは、専用回線やX.25などによって結合されている。この構成を図1に示す。インターネットワークを構成する各ネットワークは、独立した組織によって運営されている。このため、トポロジやネットワーク装置に関する知識は、中央の管理機構によって掌握されているものではなく、個々のネットワークの管理組織によって分散して管理されている。従って、診断は、しばしば複数のエキスパートの協力により進められる。

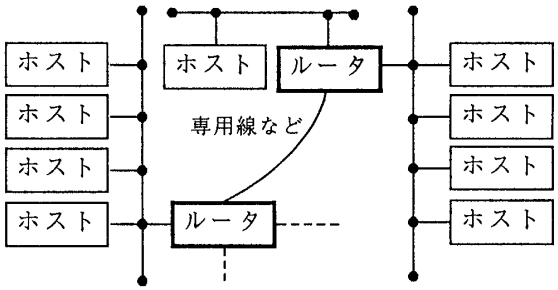

図1インターネットワークの構造

ユーザからの障害の申告があいまいなことも、診断を進めるうえでの特徴である。実際、一般のユーザは、ネットワークのエキスパートではないので、障害を報告する場合には、表面的な症状しか報告しないうえ、この報告が、しばしばあいまいであったり、誤っていたりする。このため、診断を進めていくうちに報告された症状と観測結果との間に矛盾が発生する。この場合には、ユーザの申告を疑い、再度、仮定を変更して、診断を進めてゆく。これらの診断方法の特徴は、エキスパートシステムのアーキテクチャに大きな影響を及ぼしている。

3. 障害診断の技法とシステムアーキテクチャ

本エキスパートシステムのアーキテクチャ上の特徴は、(1)基本システム内部は、診断エキスパートサブシステムと監視エキスパートサブシステムから構成される複合型エキスパートシステムであること、(2)各LAN上の基本システムどうしが、通信しながら推論をすすめてゆく分散協調型エキスパートシステムであること、そして、(3)エキスパートシステム自体が、流れているパケットから情報を抽出して診断を行ったり、場合によっては、ネットワークへパケットを流してその応答から情報を取り出しながら診断を行う、能動型リアルタイムエキスパートシステムであることである。以下では、これらの特徴を診断の技法の側面から説明する。

3.1 複合型エキスパートシステム

人間が診断を行う場合には、障害を申告したユーザとのインタラクションによって診断を進めてゆくばかりではな

Internetwork Observation and Diagnostic Expert System(1)
Ken-ichiro MURAKAMI, Toshiharu SUGAWARA
NTT Software Laboratories

く、プロトコルアナライザによってパケットを監視しながら診断を進めてゆく。時には、ユーザからの申告を受ける前に異常もしくは、その徴候を発見し、診断を行う場合もある。従って、これをエキスパートシステムとして実現するためには、ユーザとのインタラクションによって推論をすすめ、診断そのものを行うエキスパートサブシステムと、問題の発生につながるパケットを発見したり、多数のパケットのなかから特定のパケットをフィルタをかけて取り出すのための知識を持つエキスパートサブシステムの2つが必要となる。これらは、完全に独立したものではなく、内部では協調して動作する。これを図2に示す。

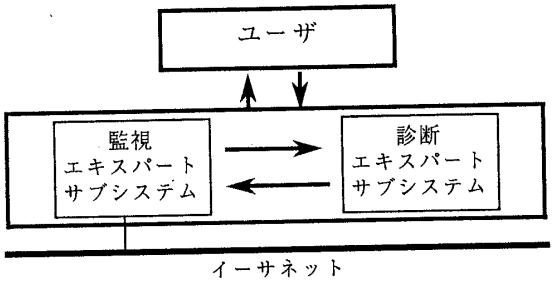

図2 複合型エキスパートシステム

3.2 分散協調型エキスパートシステム

インターネットワークは、独立した管理組織によって運営されるネットワークの共同体と考えられる。また、ネットワークが地理的な広がりを持つことから、診断のために必要な情報(知識)は分散しているのが普通である。更に、あるLANで問題が発生しても、その原因が別の遠隔にあるLAN上の装置にあるというきわめて特異な性質もある。このため、インターネットワークの診断は、それぞれのLANに詳しい複数のエキスパートによって進められる。この場合、各LAN上で、プロトコルアナライザによる多数のパケットを収集したあと、その結果から原因のしぼりこみをある程度行い、それをもとに、別の場所にいる複数のエキスパートと連絡して問題の切り分けを行う。収集されるパケットの量が膨大なうえ、解析にはローカルな知識を必要とするだけに、それをそのまま転送してひとりのエキスパートが診断するのは、不可能に近い。

本エキスパートシステムにおいても、各LANセグメント上にあるエキスパートシステムが、推論の経過や途中結果をブラックボードモデルに基づいて互いに共有し、その診断の確度を高めたり、診断を修正したりする。この意味で、本システムは、分散協調型エキスパートシステムである。これを図3に示す。各LANにエキスパートシステムが接続されるので、イーサネットケーブルに関するショートやターミネータの欠落などの物理的障害も正確に検出できるという利点もある。

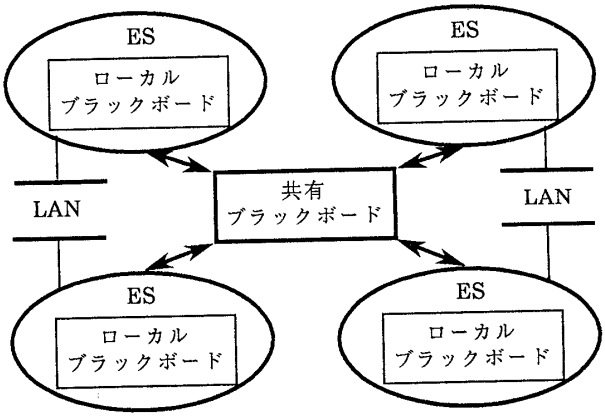

図3 分散協調型エキスパートシステム

3.3 能動型リアルタイムエキスパートシステム

ネットワーク診断では、プロトコルアナライザや、ワークステーション上にあるネットワーク状態を把握するツールを使用して障害場所や原因の切り分けを行う。本エキスパートシステムは、ワークステーション上でインプリメントされており、エキスパートシステムが直接、パケットをダンプしたり、任意のパケットを出したりすることが可能である。このため、システムは、推論に必要な情報を自動的に収集し、リアルタイムに診断を進めることができる。

また、ユーザとのインタラクションを行うことなく、ICMP (Internet Control Message Protocol) ECHO やSNMP (Simple Network Management Protocol) などのネットワーク管理用の標準プロトコルを使用しながら、能動的に診断を進めてゆくこともできる。SNMPプロトコルでは、ルータやホストのコンフィギュレーションを変更する機能をサポートしているため、これを使用して、自動的に問題を解決したり、障害の範囲を最小に押さえ込むことも可能となる。

4. おわりに

インターネットワーク監視・診断エキスパートシステムの診断技法の特徴について述べ、それが、エキスパートシステムのアーキテクチャにどのように反映されているかについて説明した。現在、SUNワークステーション上にプロトタイプシステムが実現され、NTT研究所内でテスト中である。今後、このテストに基づいて、ルールの高度化などを行う予定である。

参考文献

[1]Jonathan B. Postel: "Internetwork Protocol Approaches" IEEE Trans. on Commn. Vol.COM-28, No.4, PP.604-611 (April,1980)

[2]L. Bosack and C. Hedrick: "Problems in Large LANs" IEEE Network, Vol.2, No.1,PP.49- 56 (January, 1988)