インターネットワーク診断システム (2)
診断エキスパートシステムの試み

5T-6

菅原 俊治　　村上 健一郎
NTT Software Laboratories

1 はじめに

研究所・大学・企業等でLANで結合されたインターネットワークによるコンピュータ通信が盛んになってきた。インターネットワークは非常に有益なサービスを可能とする一方で、特に大規模なネットワークでは、多くのトラブルが発生しがちである。これらは、

(1) (大規模な) ネットワークの管理の難しさ

(2) 計算機・インターネット・LANの知識不足

(3) 通信ソフトウエア・インストレーションの問題

等に起因する。しかも障害が発生するとネットワークを共有している第三者に影響がおよぶばかりでなく、ゲートウエイ・ブリッジを越えて他のネットワークにも障害が伝染することもある。このようなネットワークの障害は、たとえば、通信が確立されない・転送が遅い・通信が不意に切れる、等が主な症状である。

障害が発生するとその原因究明にかなりの時間と労力を要する。これらは、ネットワークが物理的にも機能的にも分散されて原因個所の同定が難しいこと、管理の分散化に伴い一人のネットワークマネージャーが障害の解消に必要な情報をすべて持っていないこと、症状の再現が難しいこと等の理由がある。たとえば、他ネットワークから伝染した障害の真の原因をつかむことは不可能に近い。しかも、問題自体がnon-monotonic、つまり、正常なネットワークに新たなホストをつけ加えて障害が発生したとしても、真の原因がそれまで一見正常に動いていたホストにあることがある。

このようなインターネットワークの問題に対し、LANの状態を監視するとともに、異常が発生したとき速やかに障害の解消を行うインターネット監視・診断エキスパートシステム (Large Internetwork Observation and Diagnostic Expert System — LODES) を提案する。本システムはユーザからの申告に基づいて診断を行うばかりではなく、LANに流れているパケットを監視し、障害もしくは障害の兆候を検出し、発見された場合には診断システムが自動的に呼ばれてその原因の究明を行う。本論文では、エキスパートシステムの構成と概要および特徴を述べ、システムによる診断可能範囲を説明する。

2 システムの構成と特徴

図1は、ネットワークにおける本システムの配置を示している。各ネットワークセグメントごとに本システムが接続され、これらが通信をしあうことで診断が行われる。また図2は、各エキスパートシステムの構成である。本システムは4つのコンポーネントからなり、これらがお互いに通信・制御しながら診断を進める。それぞれのコンポーネントの役割を表1に記す。

本エキスパートシステムの特徴は以下の通りである。

1. TCP/IP関係とホスト情報を持ち、プロトコルに関連する障害に対し診断を行う。
2. ネットワークセグメントごとに本エキスパートシステムが配置され、障害に対し協調的に診断を行う。
3. 特定のパケットを監視することで、障害を未然にもしくは早期に解消する。

表1 LODESにおける各コンポーネントの役割

名称	役割
NOBS	ネットワークセグメントに流れているパケットの収集、Error パケット数とCollision数の収集を行う。通信により、Filter機能、Trigger機能を他のプロセスからコントロールできる。(作成言語: C)
NePS	任意のパケットを送出することができる。やはり通信により他のプロセスからコントロール可能である。(作成言語: C)
LAND	診断知識を持ち、診断と診断に必要な他コンポーネントへの命令を行う。知識は概ねプロダクションルールで記述されている。診断の状況・結果はBlackboardと呼ばれるメモリ領域に記述され、この部分はChalesとの共有メモリで、Chalesからも診断の状況を参照できる。(作成言語: KCL + C)
Chales	他のLODESとの通信を司るコンポーネント。協調診断の際に、他のLODESから要求された項目をチェック・スケージューリングし、可能であれば直ちに、必要ならLANに要請して要求に応答する。Chalesが中間に位置することで、LANDと他LODES間の通信を実現している。(作成言語: C)

3 分散診断の必要性

本システムを分散協調型診断システムとしたのは以下の理由からである。第一は診断にはパケットを収集・解析が必要である。たとえばLink levelの障害では、自ネットワークのほかに他のネットワークセグメント上のパケットを収集し解析する必要がある。このために二つの構成が考えられる。

- 各ネットワークにパケット収集装置を取り付け、それを特定の診断エキスパートシステムに転送し解析する。
- 各ネットワーク上にエキスパートシステムをもうけ、それぞれで解析を行い、その結果を交信する。

前者はコストは抑えられるが、次の問題点がある。まず、収集したパケットデータは多量で、それを他のネットワーク上のシステムに転送することは、途中のゲートウエイ・ネットワークに負担をかける。第二に、パケットにはパスワードやホスト情報等、重要なデータが含まれ、それらを他ネットへ転送することはセキュリティ上問題がある。後者では、解析結果だけを通信するため、これらの欠点は解消される。

分散協調型としたもう一つの理由は、ネットワーク管理の実態にそうためである。本システムが正常に動作するためには正しいホスト情報とルーティング情報が必要である。特に大きなネットワークでは、これらの管理は分散されており、これらのデータベース保持のためにも必要である。

Internetwork Observation and Diagnostic Expert System (2)
Toshiharu Sugawara, Ken-ichiro Murakami
NTT Software Laboratories

4 知識の種類と役割

- データとプロトコル知識
  - **IP アドレスとルーティング情報**
    前者はホストの identification を正確に行うため、後者は他のネットワークセグメントとの通信のために使われるもので、診断には不可欠である。
  - **ホスト情報**
    他のホストからパケットを受けたときの応答は通信ソフトに依存する。これらの応答を平常時に自動的に調べその情報を蓄える。Media Access Control Number もホスト情報として収集される。これから製造会社が確定でき、正常な応答が推定できる。最終の診断結果・対処方法の出力にも反映できる。
  - **プロトコル知識**
    収集されたパケットの解析に、各レイヤのプロトコル知識が使われる。本システムでは、Ether Packet, ARP, IP, TCP, UDP, ICMP の他 TELNET, SMTP, FTP, NNTP, RSHELL などのよく使われるアプリケーションレベルの知識も持つ。
  - **平常時のネットワーク状態**
    平常時の LAN の状態を知り、何が異常なのかを推定する。たとえば、LAN の負荷状況を知れば、busy 状態になったときに、平常時にもあることか真に輻輳なのかを推定できる。
- 診断知識
  - **パケット収集・送出のための知識**
    診断・障害の状況に応じてフィルター・トリガ等を指定し、不要なパケット情報を排除する。NOBS を制御するための知識である。
  - **協調診断のための知識**
    他の LODES と通信をするための知識で、診断中に必要な情報の他、システムのインストール、診断の開始・終了、他の LODES のコントロール等の知識を含む。
  - **障害診断のための知識**
    障害発生時に使われる診断知識である。他のネットワークの障害は他の LODES が発見するため、基本的に Local なネットワークの診断知識のみを持つ。
- 監視の知識
  - **障害監視のための知識**
    Ethernet meltdown, Broadcast storm 等の障害が発生するときにその引金となりやすいパケットがある。これらを我々の経験からリストアップし、発見されたると必要なフィルタ機能を働かせ必要な情報を収集し、これを LAND に知らせる。
  - **診断時の監視の知識**
    診断時に、特殊なパケットがどこかのホストから送出され、ネットワークの状態が変わったことを認識する知識。この知識がないと、たとえば、RIP が送出され通信が正常に戻ると、以降は異常を発見できない。

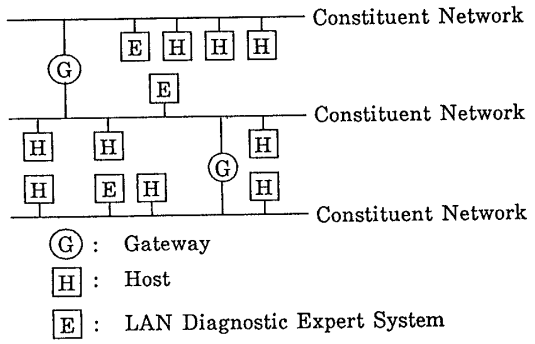

Fig.1 Network Organization with Diagnostic Expert System

5 診断の流れ

診断はユーザからの苦情または NOBS による監視機構からの情報によって開始される。ユーザからの申告は表面的な症状を訴えるもので、通常 (1) つながらない、(2) 通信が遅い、(3) ときどき通信が切れる、(4) ときどき通信が遅くなる、等である。

診断開始後は診断ルールに従い、通常は以下のテスト・解析を行う。

(1) 流れているパケットを収集し、

(1–1) パケット数、パケット長、パケットの種類に関し、統計的な処理を行う。

(1–2) Ether Header, IP, TCP, UDP, およびアプリケーションレベルのプロトコルの解析を行う。

(2) ホストに対し特定のパケットを送出し、その応答を解析する。

6 本システムの効果

以下の本システムで診断が可能である障害の例を提示する。但し、現状では障害がホストにあるときは、そのホストが UNIX machine であることを仮定する。

- **ホストの異常**
  ホストテーブルのミス、ルーティングの誤り、電源 OFF 等、通信関係の daemon の異常、アドレスの設定ミス、
- **ゲートウエイの異常**
  ルーティングの異常、電源 OFF 等、過負荷、
- **ネットワークに関する異常**
  LAN の短絡、Error rate の異常、輻輳状態 (ACKing ACK, broadcast storm, etc.)、
- **プロトコル違反**
  ほとんどすべての診断が可能、

自動検出できる障害

- 輻輳状態
- Multiple ARP reply
- Collision Rate, Error rate の異常
- Ethernet の短絡

そのほか必ずしも異常を起こすとは限らないが、RIP, Hello, 特定の Broadcast が流れた後では、LAN やルーティングの異常の監視を強化する。

7 終わりに

LAN の状態を監視し、障害を診断するエキスパートシステム LODES について述べた。本システムは、現在、NTT においてテストの段階であり、さらに必要な診断ルール等を追加している。また、NOBS の部分を、監視機能付きのプロトコルアナライザーとして、独立化させる方針である。

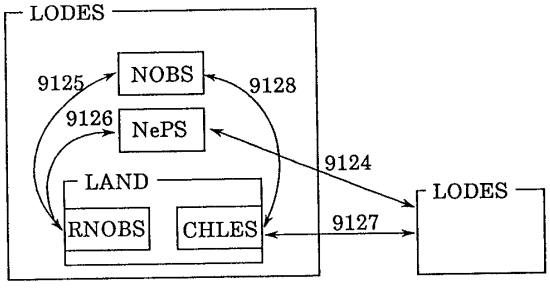

Fig.2 LAN Diagnostic Expert System Configuration and Communication port numbers