2R-05

ネットワーク障害解析支援機構

－統計情報型ネットワーク障害解析方式－

小坂 哲也　　坪根 宣宏

三菱電機(株)情報技術総合研究所

1. はじめに

近年、情報ネットワークの大規模化、高速化が進み、社会システムにおけるネットワークへの依存度は急速に高まっている。これに伴い、ネットワーク障害による被害は社会的に非常に大きな影響を及ぼすため、障害の原因解析を高速に行うことが求められている。従来、これらの障害解析作業は熟練作業者による手作業に依存する部分が多く、昨今の大規模化するネットワークへの対応が困難になってきている。本発表では、実際の ATM ネットワークを対象に、各通信ノードが持つ統計情報を利用してネットワーク障害原因を自動的に解析する方式（統計情報型ネットワーク障害解析方式）について述べる。

2．障害解析における問題点

一般にネットワーク上で障害が発生した場合、その原因特定のための代表的な手法として以下のような方法がある。

① 各通信ノードからネットワーク管理装置に寄せられるログ（トラップ）情報を解析し原因となる交換機などの通信機器（ノード）を推測する。その後ネットワーク管理装置から直接ノードの状態等を調べる。

② プローブやアナライザなど計測装置をネットワークに接続し、試験用のパケットを送信することにより、原因個所の特定を行う。

①の方法はネットワーク上の全てのノードから寄せられるさまざまな情報から特定の障害の原因解析に必要な情報を抽出し、それらから原因個所を特定する作業を行う。この方式は障害が起こった時点での状況をある程度推測することが可能である反面

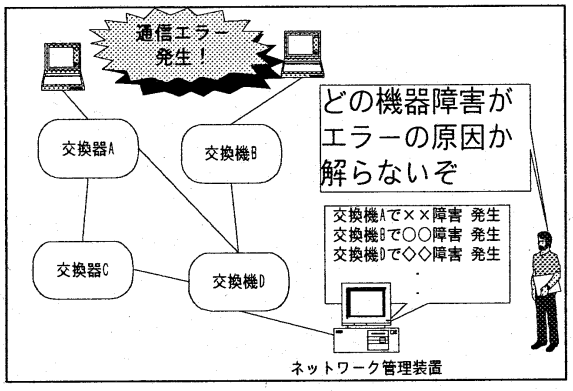

図１トラップによる障害解析の問題点

・必ずしも障害に関連した情報（トラップ）が送信されるとは限らない。

・ネットワーク全体から送られる大量の情報の中から解析しようとしている障害原因に関連する情報を抽出しなければならない。

・１つのノード障害はネットワーク上の他ノードからの障害情報（トラップ）を誘発するため、管理装置に寄せられた情報のうちどれが障害原因に直結する情報なのか分からない。

など、障害原因を解析する上でさまざまな問題がある。（図１）

一方②の計測装置をネットワークに配置して、試験用パケットを利用することにより解析する方式は、詳細な情報が収集できる反面、

・セグメント毎に計測装置を配置しなければならず、コスト高になる。

などの問題点が挙げられる。

Network Trouble Shooting Support Mechanism

Tetsuya Kosaka, Nobuhiro Tsubone

Information Technology R&D Center, MITSUBISHI Electric Corp

5-1-1 Ofuna, Kamakura, Kanagawa 247, Japan

３．統計情報型ネットワーク障害解析方式

以上の問題点を解消するために、統計情報型ネットワーク障害解析方式を検討した。統計情報型ネットワーク障害解析方式はある通信のEnd To End でデータの欠落等の障害が起きた際にその通信のネットワーク上での経路（呼）情報を取得し、呼を構成するノード内の構成機器が保持している統計情報（入出力セル数）を収集、解析することにより障害原因個所の特定を行なう方式である。実際の統計情報型ネットワーク障害解析装置はネットワーク管理装置上ソフトウェア的にアドオンされる形で実装される。

図３に示す通り、統計情報型ネットワーク障害自動解析機構は４つのモジュールから構成される。

(1)通信経路解析部
(2)解析処理用スクリプト生成部
(3)スクリプト実行部
(4)障害原因解析部

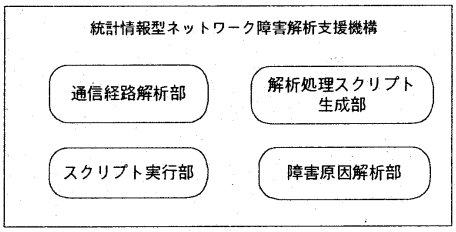

図２ 機能ブロック図

解析処理例として ATM ネットワークのある呼上でセルが欠損する障害発生時の解析処理の手順を以下に示す。

・通信経路解析部が問題の呼の通信経路を解析し、呼の構成機器リスト（ポート、VC など）を作成。
・解析処理用スクリプト生成部は生成された構成機器リストに基づき、統計情報が収集可能な構成要素を発呼側から順に並べ、「入出力セル数統計情報」を収集する制御コマンドリストを生成する。
・スクリプト実行部は生成された制御コマンドリストを実行し、結果（入出力セル数の統計情報）を取得する。
・障害原因判定部は取得した情報を基に入出力セルの差がある構成要素を「障害原因となる可能性が高い要素」として判定する。

上記の方式により、呼を構成する（統計情報を持つ）全ての機器の統計情報が取得、解析され、セル欠損の原因個所が自動的に特定される。この方式の利点として

・トラップ情報だけでは判定できない呼障害の原因判定を自動的に行なうことが可能
・従来の管理装置にソフトウェア的にアドオンする構成のため、コストの抑制が可能

が挙げられる。

４．課題と解決策

本方式では呼の構成要素すべてから統計情報を取得する。このため、大規模なネットワークに適応した場合、呼の構成要素が膨大になり、「通信量が大きくなる」、「収集に時間がかかる」等の問題点がある。これを解決するために、従来のトラップによる障害原因解析方法を利用し、予め情報を収集すべき（障害原因の可能性が高い）構成要素を絞り込む方法が考えられる。具体的には、障害が起きた時点で各装置から寄せられたトラップを解析し、呼を構成する要素と関係のある（呼構成要素そのものからのトラップではなく、その要素が含まれる上位の）装置からのトラップを抽出する。その後、トラップが存在する呼構成要素に絞り込んで統計情報を収集する。これにより、障害原因の可能性の高い構成要素に絞り込んで、情報を収集できるため、上記の問題点を回避することが可能と考えられる。

参考文献

[1]浅野正一郎,大規模ネットワーク構築上の課題;情報処理 Vol.39 1998.10