インターネットにおける経路制御監視方式とネットキーパーへの実装

2U－1

福田 晴元　小松原 重之　鈴木 亮一　三上 博英
NTT ソフトウェア研究所

1 はじめに

大きなLANを所有するユーザを多数収容したインターネットバックボーンでは，ユーザが所有する数多くのアドレスを経路制御する．また，インターネットバックボーンで利用されるルータでは，動的に経路制御が行なわれ，常に経路テーブルが更新されている．この場合に，ユーザに対する通信経路を保証するためには，経路テーブル上にあるユーザアドレスを監視し，ユーザアドレスへの経路が不到達となった場合や，ネットワーク管理者が想定した経路と異なっている場合には，ネットワークの管理者にその状態を知らせることが重要となる．

本稿では，動的に経路制御されているネットワークにおける，経路の状態監視を可能とするRTCHK(*Routing Table Checker*)と呼ぶ経路テーブル検証プログラムの検証方法と手順，そして動作状況について述べる．

2 従来のパケット伝送経路確認方法

従来より，パケット伝送経路を確認するために，traceroute[1]コマンドが広く利用されている．この方法は，検査用のパケットが経路テーブルに従って伝送される際に，通過したルータ名，もしくは，ルータのアドレスを表示する．これにより，検査用のパケットが検査先に到達しない場合には，何処のルータで不到達となるかを確認することが可能となる．

しかし，本方法では，ネットワーク管理者の思惑と異なった経路を通ってパケットが伝送されたとしても，パケットの伝送上問題がなければ，その経路を異常として検出しない．また，試験パケットと各ルータからの返信パケットは，実ネットワーク上を転送するため，例えば，試験装置への返信パケットが届かない場合には，ユーザアドレスへの伝送経路が正常であっても，異常として検出する可能性がある．この場合には，異常の内容を把握するために，繰り返し異なる箇所からの経路確認が必要となる．しかし，tracerouteを実行するホストが複数箇所にない場合には，内容の把握が困難となる．

3 RTCHKでのパケット伝送経路の検証確認

3.1 経路の検証方法

RTCHKでは，ひとつの検証装置上で一度の経路確認により経路テーブルの検証を行なうために，ルータの経路テーブルを直接参照してルータの接続関係を求めることによって，異常状態を検出する手法を用いた．

この際に，パケットがネットワーク管理者の思惑と異なった経路を伝送する状態を検出するために，RTCHKでは，ユーザアドレスと，そのアドレスを利用するユーザネットワークを収容したルータ（以降はソースルータと呼ぶ）の組からなるデータベースを利用する．ひとつのユーザアドレスに対してソースルータが複数ある場合には，ユーザが希望するパケット配送経路に従った優先度を属性として与えて，全てのソースルータを登録する．これにより，ユーザアドレスに向けたパケットが，ユーザネットワークを収容していないルータや，優先度の低いルータに向けて伝送されるような異常状態を検出可能とした．なお，RTCHKでは，パケットが延々と同じ箇所を伝送するような，ループの状態も異常状態として検出可能である．

3.2 経路の検証手順

RTCHKでは，以下の手順で経路確認を行なう．

1. 監視対象ネットワーク内にあるルータであり，経路テーブルの監視を行なうルータを定める．
2. 検証対象ネットワークアドレス(以後Aとする)を選択する．
3. SNMP(*Simple Network Management Protocol*)[3]を利用して，全ての監視対象ルータにおける，アドレスAの経路テーブルを参照する．
4. ブール接続行列[2]と呼ばれる接続行列Cを用いて，経路テーブルに従った監視対象ルータの接続関係を表現する．さらに，監視対象ルータ数をmとすると，$C, C^2, \cdots, C^{m-1}$と$M = C+C^2+\cdots+C^{m-1}$を求める．ここで，C^n_{ij}は，ルータr_iからr_jへの長さnの経路があれば1であり，M_{ij}は，ルータr_iからr_jへの経路があれば1となる．
5. $M_{ii} = 1$の場合には，パケットがルータiからルータiへもどる経路があることを意味する．したがって，M_{ii}を調べることによってループの存在を知ることが出来る．

   ルータkにおいて，$M_{ik} = 0 (i = 1, 2, \cdots, m)$の場合には，ルータ$k$からは，他のルータへの経路が存在しない．このため，ルータkはソースルータであると考えられる．また，$l_i = \sum_{j=1}^{m} M_{ij}$を計算した場合に，$l_i$の値が大きいほど，ルータ$i$は他のルータからの経路が多いことを示す．そこで，$l_i$の値が大きいほど，優先度が高いと考える．このようにして求めたアドレスAのソースルータとその優先度について，データベースと比べることにより，検証を行なう．

4 動作状況

RTCHKのプロトタイプを作成し，省際研究情報ネットワーク[4]上で動作確認を行なった．プロトタイプでは，

An Approach and Impremention for Routing Table Checking with RTC on NetKeeper
Harumoto FUKUDA, Shigeyuki KOMATSUBARA, Ryoichi SUZUKI, Hirohide MIKAMI
NTT Software Laboratories

第3.2節で示した手順の2番目以降を定期的に繰り返すことにより，連続して検証を行なっている．

なお，ソースルータ別に，また，多くのネットワークアドレスを持つユーザネットワーク別にアドレスのグループを作成し，そのグループの中から任意にひとつのアドレスを選択し，それを検証対象のアドレスとしている．従って，一回の検証により，グループ数だけのアドレスについて，第3.2節の手順2番目以降を繰り返した検証が行なわれる．以下に，プロトタイプを実行した結果，検出した異常状態の2例を示す．

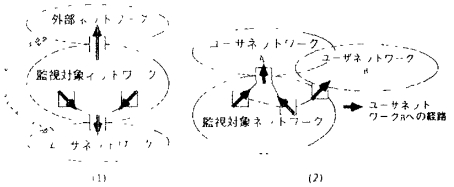

図 1: 異常状態の例

- 二つのAS(*Autonomous System*)に対してマルチホーム接続[5]したユーザが，回線帯域の有効利用といった観点から，外部ネットワークより管理対象ネットワークを経由する経路を主経路として利用すると決めていた．ところがある時点より，BGP[6]による経路制御の結果が外部ネットワークを向くこととなった状態（図1の(1)），つまり，外部ネットワークからは管理対象ネットワークが副経路となっている状態を検出した．

- 図1の(2)に示すように，他のユーザ（ユーザネットワークB）へのパケットが，管理対象ネットワークを経由して伝送するべきところを，ユーザネットワークAを経由するように経路制御された状態を検出した．これは，ユーザネットワークAから誤った経路情報を受取ったことが原因であった．

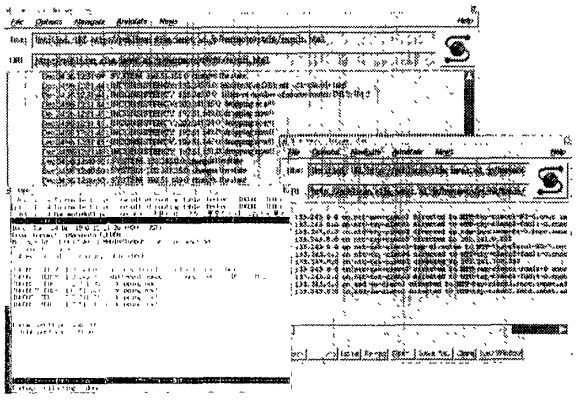

図 2: プロトタイプによる経路テーブルの確認状態

プロトタイプでは，異常を検出した際のログを，HTML(*Hypertext Markup Language*)を用いて作成する．また，異常となったアドレスの経路テーブルを確認できるようにHTML形式で経路テーブルを保存している．さらに，異常をメイルにてネットワーク管理者に伝えている．従って，RTCHKによりユーザアドレスの経路制御に異常が発見されると，ネットワーク管理者は，メイルにて異常を認識し，その内容と経路テーブルをHTMLブラウザを用いて確認することが可能である．プロトタイプにより作成されたログと経路テーブルを確認している画面を図2に示す．現在，ネットキーパー[8]と呼ぶネットワーク監視ツール上へ，RTCHKを実装した．現在は，省際ネットワーク上で動作確認をしている．RTCHKのネットキーパーでの動作画面を図3に示す．

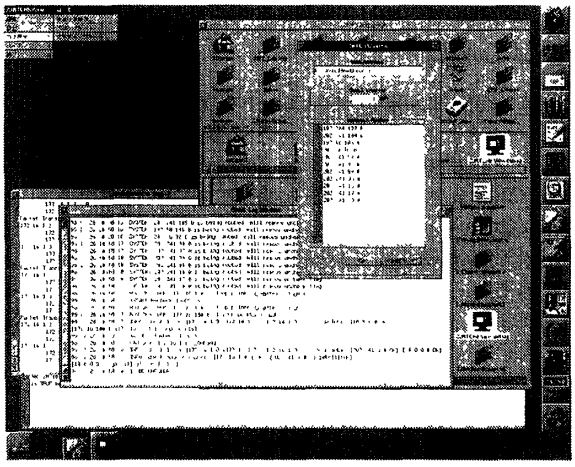

図 3: ネットキーパーでの動作画面

5 おわりに

本稿では，RTCHKと呼ぶ経路テーブルの検証プログラムについて，検証方法と検証手順について述べた．さらに，作成したプロトタイプの動作について述べた．本プログラムはネットキーパーへの実装を行なった．

RTCHKは，経路制御の異常をメイルを利用してネットワーク管理者に伝える．プロトタイプでは，その情報をHTML形式で保存しており，ネットワーク管理者は，HTMLブラウザを利用することにより情報を参照できる．

今後は，ネットキーパの動作確認をさらに進めていく予定である．

最後に，貴重な御意見を頂いた宮川晋氏を始め，IMnet NOCの皆様，早稲田大学後藤滋樹教授，そして我々を御支援下さるNTTソフトウエア研究所広域コンピューティング研究部市川晴久部長に深謝します．

参 考 文 献

1) Daniel C. Lynch, Marshall T. Rose, "Internet System handbook", ADDISON-WESLEY PUBLISHING COMPANY INC., Jan. 1993.

2) 甘利俊一, 金谷健一, 嶋田晋 共訳, "計算機科学入門", pp189-214, サイエンス社.

3) M. Schoffstall, M. Fedor, J. Davin, J. Case, "A Simple Network Management Protocol (SNMP)", RFC1157, May. 1990.

4) 鈴木亮一, 福田晴元, 三上博英, "省際研究情報ネットワークの構築について", 第51回全国大会予稿集 2E-9, Sep 1995.

5) 福田晴元, 鈴木亮一, 三上博英, "省際研究情報ネットワークの接続形態", 第51回全国大会予稿集 2E-8, Sep 1995.

6) Y. Rekhter, T. Li, "A Border Gateway Protocol 4 (BGP-4)", RFC1771, May 1995.

7) Christian Huitema, "ROUTING IN THE INTERNET", Prentice Hall PTR.

8) Takashi Arano at el. "A Computer Network Management System Platform based on Distributed Objects", Sixth IFIP/IEEE International Workshop on Distributed Systems: Operations & Management, Oct 1995.