マルチメディア通信と分散処理 97－8
コンピュータセキュリティ 8－8
（2000．3．21）

ネットワーク動作情報の生成管理手法

金子 正和　齋藤 武夫　Glenn Mansfield　木下 哲男　白鳥 則郎

東北大学電気通信研究所 / 情報科学研究科

インターネットの普及やストリームデータを利用したアプリケーションの増加により，ネットワークのQoS制御などの高度で効果的なネットワークの運用の必要性が増加している．このようなネットワークの運用を実現するためには，ネットワークの輻輳状態を表すTCP再送パケット情報や，ネットワークの通信品質を表すディレイ情報などのネットワーク情報が必要になってくる．しかし，これらの情報に対する要求は，ユーザや状況により多岐に渡る．そこで我々は高度なネットワーク情報のアプリケーションに対する提供を目的とし，ネットワーク情報を収集・管理するネットワーク情報ウェアハウス(NIWH)について研究を進めている，本稿では，NIWHに対するユーザ・アプリケーションの要求記述言語である，ネットワーク情報コンフィグレーション・クエリー言語(NICQL)について述べる．

Network Information : Generation and Management

Masakazu KANEKO, Saitoh TAKEO, Glenn MANSFIELD, Tetsuo KINOSHITA, Norio SHIRATORI

Research Institute of Electrical Communication / Graduate School of Information Sciences, Tohoku University

The network applications on the Internet needs high level network information for better and effective operations. By high level information, we mean a "congestion state" of a network path (which can be obtained by monitoring TCP retransimissions, "quality of communication" (can be obtained by observing delay) etc. These information should be provided to the concerned applications and/or to users. To meet these requirements, we have already proposed a Network Information Ware House(NIWH) which gathers network information, analyses them and uses them for network management related activities. In this paper, we design NICQL (Network Information Configuration and Query Language) by which a user can set its query to the NIWH and gets back necessary high level network information.

1 序論

インターネットの普及やストリームデータを利用したアプリケーションの増加により，ネットワークのQoS制御などの高度で効果的なネットワークの運用の必要性が増加している．このようなネットワークの運用を行なうためには，ユーザやネットワーク状況により多岐

に渡る，例えばネットワークの輻輳状態を表すTCP再送パケット情報などのネットワーク情報が必要になってくる．現状のネットワークの運用や管理を目的とするシステムから得られる情報は，限られたものである．そこで我々は高度なネットワーク情報のアプリケーションに対する提供を目的とし，ネットワーク情報を収集・管理するネットワーク情報ウェアハウス(NIWH)について研究を進めている[1]，

本研究では，NIWHに対するユーザ・アプリケーションからの多様な要求を伝達する手法に，プログラミング言語による記述という手法を用いることにした．本稿では，ネットワーク情報の分析を目的とした，手続き型のプログラミング言語として，ネットワーク情報コンフィグレーション・クエリー言語(NICQL)の提案を行なう．この言語により，ユーザ・アプリケーションによる多様で高度なネットワーク情報の分析要求が実現されると考える．本稿の構成は，先ず本章で，本稿の概要を述べた．第2章で，現状で取得できるネットワーク情報と，NIWHについて述べる．第3章で，NICQLの扱うオブジェクトを示しながら分析手法を示し，設計を行なう．第4章に本稿のまとめを行なう．

2 NIWH

本章では，まず，従来のネットワーク情報モニタリングシステムに関して概観した後，NIWHのアーキテクチャの概要について述べる．

2.1 ネットワーク情報の取得

適切なネットワーク情報を得るためには，先ずデータ収集ノードでネットワーク情報が測定・収集され分析される必要がある．その測定，収集メカニズムを大きく次の2つに分類することができる．

(i) アクティブ・モニタリング

アクティブ・モニタリングは，ネットワークエージェントから操作情報を得るために計測トラフィックを生成したりSNMPなどの管理プロトコルを用いてポーリングを行なったりする．

tarceroute, ping, netperf, netstatなどはネットワークにテストパケットを送信することによって，ネットワークの性能を表す異なったネットワークのパラメータを測定する．例えば，traceroutは，round-trip-time, hop数,packetの損失を測定する．

(ii) パッシブ・モニタリング

パッシブ・モニタリングでは，ネットワークを通る通常のトラフィックをエージェントがモニタリングすることにより，測定を行なう．したがってトラトラフィックを生成することなく，トラフィックに関するより詳細な情報を提供する．また，ICMPのdestination unreachable packetを分析することによって，ネットワークサイトとルートの障害地点についての情報を得ることが出来る．

これらのメカニズムは，ネットワーク情報をモニタリングするにあたり非常に優れたフレームワークを提供している．

2.2 従来のモニタリングシステム

提供される情報は，事前に設定された一連のオブジェクトに限られている(in MIBs)．RMON-MIB[2]は，設定したfilterによって1次ネットワーク情報をモニターするが，('1次'というパラメータは個々のパケットの性質に基づいている．ことと定義する．)2次ネットワーク情報('2次'というパラメータはパケット間の関係に基づく．これは異なったネットワークコンポーネントを関係づけるのも用いられる)はサポートしていない．MeterMIBで実装されたNeTraMetは，1次ネットワーク情報をモニターするが，'2次'ネットワーク情報に関してはサポートしない．[3][4]

2.3 NIWH

本節では，我々が，提案しているネットワーク情報ウェアハウスのアーキテクチャの概略について説明する．ネットワーク情

報は，各ノード(図1:N3とN6)でtcpdump[5]などによりtimestampのついたpacketが収集されより意味のある('2次')ネットワーク情報を生成するために，注意深く分析される．過去の情報はネットワークの特徴の統計的傾向を調べるために非常に役にたつ．将来使うために，このデータはNIWH内に生もしくは，分析された結果として保持される．図1にNIWHの概要を示す．

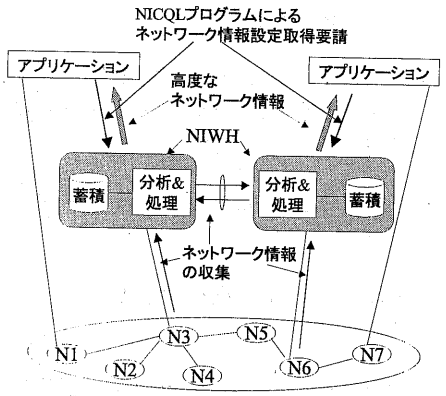

図 1: NIWH:アーキテクチャ

(i) データの収集　NIWHはネットワーク(インターネットまたは他のネットワーク)上の異なった地点に分散的に配置され運用される．1次ネットワーク情報はアクティブ・モニタリングシステム(SNMPポーリング，ping，traceroute など)と，パッシブ・モニタリングシステム(packet dump など)の両方を用いて，収集を行なう．

(ii) アクセスコントロール・プライバシーコントロール　多様な要求を持った広範囲なユーザに対して，その権限，必要なネットワーク情報に応じたネットワーク情報を提供するために，NIWHではネットワーク情報自体に対するプライバシーレベルと，ユーザに対して与えられるユーザレベルという2つのアクセス権限レベルを導入する．これを用いて誰がどの情報に対してアクセスできるかのアクセスコントロールを実現する．

(iii) ネットワーク情報のコンフィグレーションおよび要求記述　NIWHにおいては，ユーザが，ネットワーク情報コンフィグレーション・クエリー言語(NICQL)を記述しNIWHに送ることによってNIWHの情報管理機構を設定し，ネットワーク情報を分析する．このNICQLについては次章で詳しく述べる．

3 NICQL

本章では，ネットワーク情報コンフィグレーション・クエリー言語(NICQL)の扱うデータと分析要素を示し，次にそれらを用いた，ネットワーク情報の分析手法について述べる．

3.1 データ形式と分析要素

NICQLでは，ネットワーク情報をpacketおよびfield，そしてpacketstreamとして扱う．また分析中に用いる分析要素としてfilterおよび，tableを使う．次にこれらの定義とそれらの使われかたを示す．

[packet]

NIWHで扱う最も基礎となるネットワーク情報とは，packetdumpなどを用いて収集したpacketである．

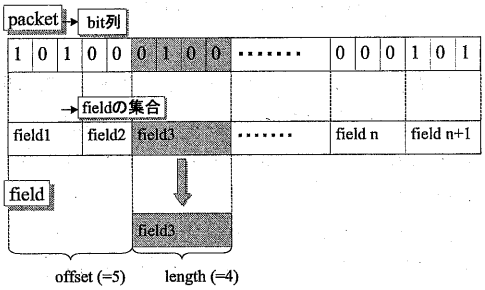

図 2: packetとfieldの関係

ここで図2で示すように，packetを有限の長さを持つbit列であると定義する．またpacketとは複数のfieldに分けることができる，fieldの集合である．

[field]

図2に示すようにfieldとは，packetの先頭からのoffsetと，その領域幅を示すlengthか

ら成る．

[packetStream]

複数のpacketとtimestampの組の集合である．このtimestampは，NIWHがネットワークから収集された時点で，測定ツールにより付加される．

[filteset・filter]

filtersetとはpacketもしくは複数のfieldに対する適合条件を規定したものである．これは複数のfieldに対する適合条件をfilterと論理演算子を用いて規定する．

filterとは個々のfieldに対する適合条件を規定する．filterは次の要素，(field名,関係演算子,値) もしくは，((offset,length),関係演算子,値) によって構成される．field名により，比較対象部を規定し，関係演算子により，関係を規定し，値により，比較対象の値が幾つのときという条件を規定する．

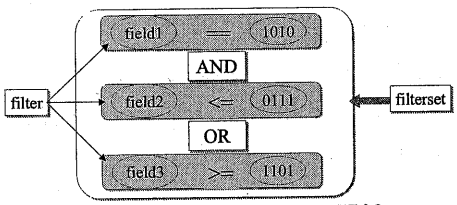

図 3: filtersetとfilterの関係

NICQLを用いたネットワーク情報の分析では，これらのfiltersetおよびfilterを用いて，意図した情報を検出し，検出した情報を基に分析を行なう．

packet1がIP -versionの値として4を持つかどうかを調べたいときは，(IP -version, ==, 4) というfilter1を設定し，paket1がfilter1の比較条件に適合するかどうか判別する．

[table]

NIWHはデータ構造としてのtableを持ち，それをNICQLを用いて操作する．tableとはfieldで指定したデータをtimestamp順に格納するデータ構造である．ネットワークから収集した1次ネットワーク情報をNIWH上に蓄積したり，ネットワーク情報を分析する過程で用いたり，また分析した結果を再利用できるようにNIWH上に蓄積するために用いる．

tableは次の2つの要素から成る．

- 行:timestampによりインデックス付けされ，timestampの順に並んでいる．
- 列:field記述子によりインデックス付けされる．

またtableは次のようなテーブル固有の属性値を持ち，これらを設定変更することにより，tableを管理する．

- sizeout: rowサイズで規定したスライディングウインドウのrowサイズを規定する．
- max-rows: tableの最大rowサイズを規定する．
- owner: tableを操作できるユーザを規定する．
- table-row-size: 現在table中に存在している，rowの数を示す．

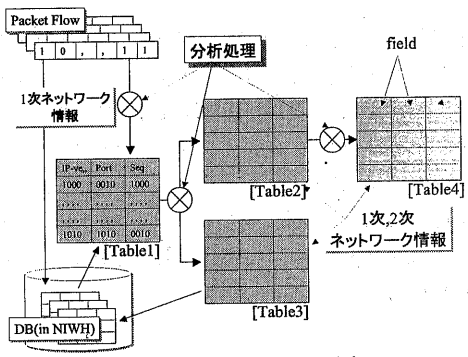

図 4: tableを用いた分析

tableを用いた分析では，一旦ネットワーク情報を貯えることにより，より高度な分析を行なうことが出来る．

図4では測定packetflowや，NIWH内のDataBaseなどに蓄積された，ネットワーク情報を基に，tableを用いて．それに対して，分析処理を加えることにより，多様なネットワーク情報が生成される様子を示す．

3.2 基本操作の記述

以下に，NICQLの基本的操作の記述について示す．

(1) ネットワーク情報の入出力

ネットワーク情報源を選択し，ネットワーク情報源を開き，packetを取得し，分析したネットワーク情報をユーザに送信もしくは，NIWH内に蓄積し，ネットワーク情報源を閉じる操作が含まれる．

```
ih = ni_open(PacketStream-name)
packet=ni_get(ih)
output(table-name[packet-name,
fields-name])
```

(2)field データの取得

bit列として存在するpacketから，offsetとlengthの情報を基に，必要なfieldのデータを抜き出す．

```
packet-name.field-name
```

(3)filtersetとfilterを用いた，packet field(s)の比較

filtersetおよびfilterと，それを用いた比較操作により自分の必要とする情報をpacket-streamなどから検出するのに用いる．図5は，2つのpacketの同じfieldが同じ値を持つかどうかという操作を，NICQLにおいてfilterを用いてどのように行なうかについて示す．

ここでは，2つのpacket1とpacket2のfield–IP-version同士を比較したい場合，一旦packet1のfield–IP-versionの値を引き出した後，それを用いてfilter1を設定し，packet2との比較操作を行なっていることを示す．

```
makeFilter(field-name, operator, data)
makeFilterset(filter-name operator
filter-name)
Match(filter-name,packet-name)
```

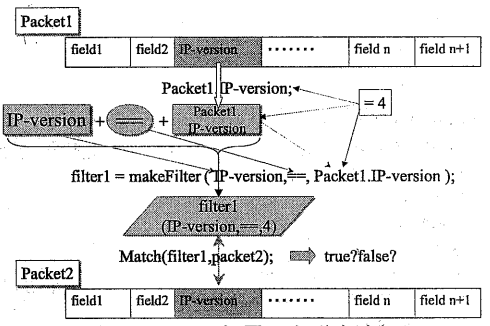

図 5: filterを用いた分析例

(4)table

- tableの生成
  table本体を生成し，属性値を設定する．

```
makeTable(table-name)
setAttribute(table-name,attribute,
value)
```

- tableの操作
  table操作はrowのキーとしてのtimestampを中心に，tableへの入出力を行なう．filterやfiltersetを用いて，必要な情報だけに対して，分析を行なうといった操作を行なう．

```
pushtoTable(table-name,packet-name)
row=readTable(table-name)
MatchTable(filter-name,table-name)
SearchTable(filter-name,table-name)
row-size=getTablerowsize(table-name)
```

- tableの消去
  tableの必要でないrowやtable本体の消去を行なう．

```
matchremoveTable(filter-name,
table-name)
removeTable(table-name)
```

3.3 実装と現在の状況

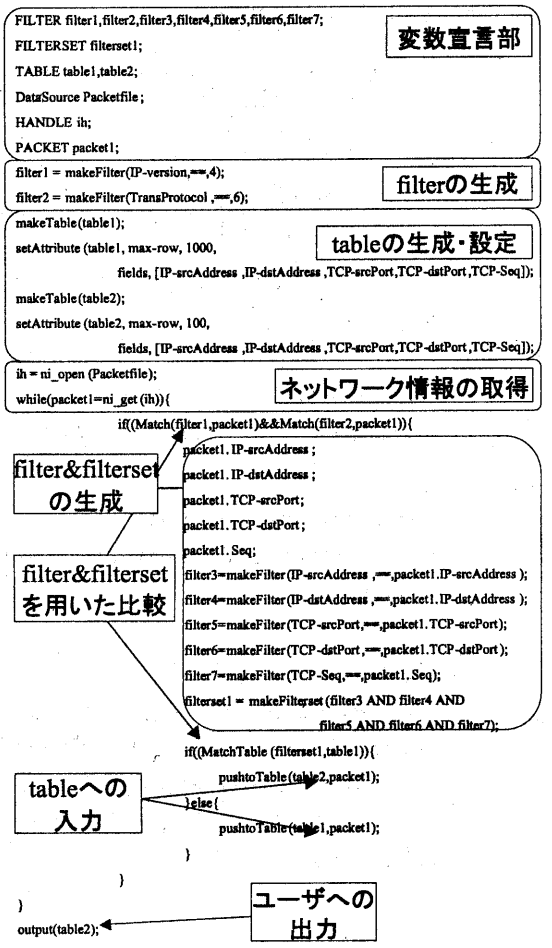

図 6: NICQLによる再送検出プログラム

ネットワーク情報が必要なユーザ・アプリケーションはNICQLプログラムをNIWH送信する．NIWHでは，NICQL処理部がNICQLプログラムを受け，解析し実行し，probeもしくは，NIWH内のDBから要求を実現するために必要なネットワーク情報を収集し，分析が行なわれる．図6にNICQLによる，TCP再送検出プログラムを示す．現在は，検証実験を行なっている．

4 結論

ネットワーク情報の取得に関して考察し，我々が提案するネットワーク情報ウェアハウスのアーキテクチャの概略を示した．次に，そのネットワーク情報の設定および分析を行なう，NICQLについて述べ，packet，filterset(filter)，tableを明確にし．またそれらを用いたネットワーク情報の分析における基本操作ついて示した．これにより，2次ネットワーク情報を含む高度なネットワーク情報の記述が実現できた．

NICQLに関する今後の課題としては，更に検証実験を進め，NICQLにおけるネットワーク情報の分析を行なうためのより高い記述性を図るとともに，複数のネットワーク情報源に対して，シームレスなアクセスの実現を図って行く必要がある．

参考文献

[1] Ahmed Ashir,Glenn Mansfield,Takeo Saitoh,Masakazu Kaneko,Norio Shiratori,"AnOpen and Configurable Network Information Warehouse Service,"Passive and Active Measurements - PAM-2000 NewZealand April 2000 [forth coming]

[2] S. Waldbusser,"Remote Network Monitoring Management Information Base Version 2 using SMIv2,"RFC2021,Jan.1997.

[3] N. Brownlnee,"Traffic Flow Measurement: Experiences with NeTraMet,"RFC2123,Mar.1997.

[4] N.Brownlee,"Traffic Flow Measurement: Meter MIB,"RFC2720,Oct.1999.

[5] Tcpdump: fttp://ee.lbl.gov/