1K－1

分散オブジェクトを用いたコンピュータネットワークのトラフィック収集・分析技術の一考察*

池上 聡† 浜田 雅樹† 小松原 重之† 三上 博英†

NTTソフトウェア研究所‡

1 はじめに

インターネットのトラフィック管理においては、アプリケーションの種類、パケットの発信地、着信地などの統計情報と、パケットのTCP/IPヘッダが必要である。統計情報は、設備投資、トポロジの再構成、ユーザ管理などを行うために用いられ、パケットのヘッダはパケット欠落やルーティングの確認などに用いられる。今日、これらのトラフィックデータ収集の標準として、RMON (Remote Network Monitoring) [1]、RMON 2が存在する。これらは、SNMP(Simple Network Management Protocol)のMIB2 (Management Information Base 2)を拡張したRMON-MIBと、それらにアクセスするためのインターフェースを定義したものである。

RMONを用いた実際のトラフィック収集では、ルータやハブ等のネットワーク機器で収集する方法やプローブで収集する方法が存在する。プローブとは、セグメント上の全てのパケットを調査し、それを分析して統計情報を作成したり、後から分析できるようにパケットを保存しておくことができる専用ハード、WS、PC等である。これら2つの方法は一長一短であるが、RMONでは負荷の高い処理を必要とすることから、プローブを用いる方法が将来的に有望である。しかしながら、プローブを用いる際には多くのコストがかかるという問題がある。その理由は、インターネットではトラフィックが特定箇所に集まることがないためにプローブの設置数が多くなること、RMONは負荷の高い処理を要求するためにバックボーンなどの広帯域な伝送路では高性能なプローブを用いる必要があることである。

そこで本稿では、処理能力の低い安価なマシンを複数協調させてRMONとして高い処理能力を実現することを目的とし、複数のマシン間での負荷分散方法について検討する。

2 分散オブジェクトを用いたRMON

分散オブジェクトを用いたRMONを構築する際の方針について述べ、その処理方式を構成する要素について述べる。

2.1 方針

コストを含めた多様なニーズに対応するために以下の方針をとるものとする。

1. PCで動作する
2. 分散オブジェクトパッケージとして実現する

1はコストを軽減することを目的としている。そのため、特殊なハードやOSの改造などは最小限に留めることが望ましい。

2は、分散オブジェクトを用いることで、スケーラビリティを向上させることを狙いとしている。また、分散オブジェクトの部品として実現することで、他のソフトウェア(NMS等)との結合などが可能となり、適用範囲が広がることが期待できる。

2.2 処理方式の構成要素

分散オブジェクトを用いたRMONの処理方式は以下の要素より成る。

1. トラフィックを分散オブジェクトに割り振る方法(負荷分散方法)
2. 分散オブジェクトが協調を実現するために必要な情報を交換したり、調整する機構の実現方法(分散、協調のメカニズム)
3. 各収集オブジェクトの収集したトラフィックデータを集め、重複などがある場合にはそれを除き、そのセグメントのトラフィックデータを作成する方法(データ回収、整理方法)

本稿では、Ethernetを例にして、1の負荷分散方法を中心に検討する。

3 負荷分散方法の検討

負荷分散方式としては、以下の方法が考えられる。

1. 時間で分担する方法
   複数のPC間で時間を同期させ、それぞれのオブジェクトにトラフィックを収集する時間を割り当てることで分担する方法である。
2. ヘッダの属性で分担する方法
   パケットの属性(プロトコルetc)から、各オブジェクトが取り込むパケットを選択する方法である。
3. 到着順序で分担する方法
   各オブジェクトでセグメント上での順序情報を用いて分担する方法である。つまり、各オブジェクトが順番にパケットを処理する。

以下、それぞれの方法の実現可能性を検討する。

3.1 時間で分担する方法

この方法の場合、各オブジェクトは収集する時間が割当てられるので、その割当てられた一定時間はとりこぼしなく収集(連続収集)可能である必要がある。それを調べるため、10M Ethernet上でbeholder [2]というRMON Agentを用いて実験を行った。その結果、起動時は連続して収集することができたが、その後、収集できたりできなかったりという現象が発生した。この結果より、beholderは図1のような構成で動作していると考えられる。このことから、それぞれのオブジェクトで、一次バッファに取り込む時間(連続収集時間)を分担し、連続収集時間以外の時間(処理時間)でデータを処理して統計データ等を作成する方法が有効であると考えられる。

---

*A Study of RMON Implementation using Distributed Object

†Satoru IKEGAMI, Masaki Hamada, Shigeyuki Komatsubara, Hirohide Mikami

‡NTT Software Laboratory

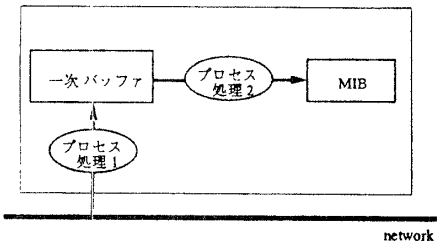

図 1: beholder の仕組み

この場合、連続収集時間と同期の精度が問題となる。例えば、図2のように3つのオブジェクトで分担して収集する場合、それぞれのPC間の時間の同期が正確でないと、切り換え時にとりこぼしが発生する。それを防ぐため、同期の精度の分だけ、互いの収集時間に余裕を持たせる必要がある。その際、少くとも以下の条件を満たす必要がある。

連続収集時間 > 同期の精度 ×2

また、一回の最大連続収集時間は、

連続収集時間 = バッファの容量 / 伝送路の帯域

として計算されるため、必要なバッファ容量は

バッファ容量 > 伝送路の帯域 × 同期の精度 ×2

となる。例えば、NTP(Network Time Protocol)[3]等で $10ms$ の同期精度が得られたとした場合、100 Mbps の伝送路に対応するには 250 Kbyte 以上のバッファを確保できれば実現可能であると考えられる。

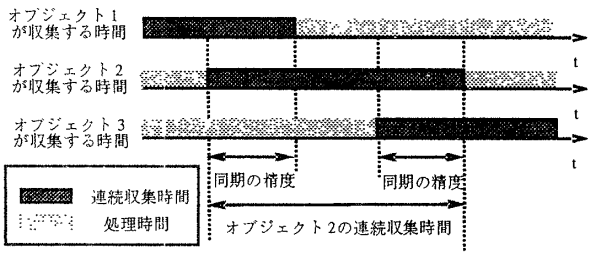

図 2: 連続収集時間と同期の精度の関係

3.2 パケットの属性で分担する方法

この方法では、負荷を分散させることのできるパケットの属性があるかどうかが課題となる。インターネットでは単一のユーザによる負荷が発生することがあるため、プロトコル、ソース、デェスティネーションアドレスなどで分担した場合には負荷が大きく偏ることが考えられる。これに依存せず分担する属性値には、ID識別子、ヘッダチェックサムが考えられる。しかし、短時間で偏りが発生しないことを保証できる属性はなく、実用上の問題があると考えている。

3.3 到着順序で分担する方法

この方法では、各オブジェクト間で同一のパケットを収集しないための協調機構が不可欠である。その理由は、パケットには順序情報がないので、それぞれのオブジェクトが収集するパケットがわからないためである。例えば、2つの収集オブジェクトが互いに1パケットおきに収集した場合に、同一のパケットを収集している様子を図3上に示す。これらを調整する方法としては、図3のように調整オブジェクトを設け、それぞれのオブジェクトが収集しているパケットを監視し、同一のパケットを収集している場合には片方のオブジェクトに収集するパケットをずらすように指示する方法が考えられる。

この方法を実現するには、各収集オブジェクトが同一のパケットを収集していることの識別方法、及び、オブジェクト間の通信方法の確立が必要である。各収集オブジェクトが同一のパケットを収集していることの識別方法は現在検討中であるが、以下の方法で可能であると考えられる。

1. 調整オブジェクトが各収集オブジェクトに対して制御用パケットを送出し、そのパケットが到着してからの一定時間に収集したパケットを送り返す
2. 各収集オブジェクトから送り返されたパケットを比較し、同一のパケットを収集していることを識別する

上記の一定時間は、制御用パケットが各収集オブジェクトに到着するまでの時間のずれ、比較に必要なパケット数から決定される。今後、これらの数値を検討していく必要があるが、同一のパケットを収集している場合にはパケットの到着順序までが同一であることを利用すれば、識別は可能である。また、オブジェクト間の通信方法としては、制御用パケットに目印を付与して送出し、各PCで制御用パケットと監視対象パケットを区別して処理する方法や、専用の制御回線を設ける方法などが考えられる。これらの方法を比較し、最適な方法を選択する必要があると考えている。

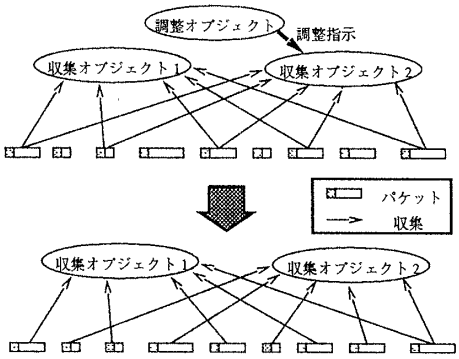

図 3: 協調の仕組み

4 まとめ

本稿では、複数のマシンを協調動作させてRMONの処理を行う方法について、負荷分散方法を中心に検討した。検討の結果、時間で分担する方法と到着順序で分担する方法が有望と考えられる。今後は、分散、協調のメカニズム、データ回収、整理方法を中心に検討を進め、さらに、対象を広帯域な伝送路に拡張し、実際のネットワークに適用していく予定である。

参考文献

[1] S.Waldbusser, 'Remote Network Monitoring Management Information Base', RFC 1757, Feb 1995

[2] ftp://dnpap.et.tudelft.nl/pub/btng
http://dnpap.et.tudelft.nl/DNPAP/Documents/cookbook/bibliography1_4.html

[3] David L.Mills,'On the Accuracy and Stability of Clocks Synchronized by the Network Time Protocol in the Internet System' Computer Communication Review, vol.20, No.1, pp65-75, 1990