2005－OS－99（16）
2005／5／27

分散協調システムによるトラフィック測定システムの開発

小塚 雅洋
豊橋技術科学大学
情報工学系

岡部 正幸
豊橋技術科学大学
マルチメディアセンター

梅村 恭司
豊橋技術科学大学
情報工学系

概要　本学の各ゲートウェイ付近にトラフィックを測定する機能を持ったノードを配置し全学のトラフィックフローを観測するシステムを設計し、開発中である。トラフィックフローに異常が生じた場合は、これを検知し、直ちに報告する仕組みを作ることが目的である。本研究ではトラフィック測定機能を LiveCD 上で実現する。LiveCD を用いることにより、全学への配布と導入を容易にすることを意図してのものである。また LiveCD は、一旦全学に導入された後も、機能の追加が容易であり、全学的なネットワークセキュリティの向上のための土台となることが期待できる。

Distributed and Collaborative System for Network Traffic Measurement.

Masahiro Kozuka
Toyohashi University of Technology
Department of Information and Computer Sciences

Masayuki Okabe
Toyohashi University of Technology
Multimedia Center

Kyoji Umemura
Toyohashi University of Technology
Department of Information and Computer Sciences

Abstract　The system that observes the traffic flow of the entire university is designed, and being developed. The system will be set up beside each gateway. The purpose of this system is to make itself report at once if abnormality is caused in the traffic flow. In this research, the traffic measurement function is provided by LiveCD. Since LiveCD is used, it becomes easy to distribute and to introduce into the entire university. Moreover, because it is easy for LiveCD to introduce new function, LiveCD forms a foundation to improve the network security after system become in operation.

1　はじめに

近年、ネットワークを取り巻く環境は大きく変化しつつある。MS ブラスタに代表されるネットワーク感染型ワームによるセキュリティの脅威や、P2P 型ファイル交換ソフトウェアの出現により、当初のイントラネット構築段階での性能を発揮できない状況が発生し、ネットワーク管理者の頭を悩ませている。

大学のようなある程度以上の規模の組織において、ネットワークを健全な状態に保つには、日々変化するネットワークの状況を的確に把握することが必要である。本研究ではネットワークトラフィック測定システムの開発を目的とする。ネットワークは、異常トラフィックが発生すると、1 台のホストが原因であっても、その全体に深刻な影響を及ぼす可能性がある。トラフィックフローを観測し、トラフィックの異常をいち早く検知、改善することは、ネットワークの健全性を保つ上で、重要な事項である。

本論は、目的とするトラフィック測定システムの開発状況を報告し、本研究の今後の展望について論ずる。

2　ネットワークトラフィック測定

ネットワークトラフィックの測定は、ネットワークを管理・保守する上で重要な事項であり、そのための機器・サービスが様々なメーカから発売されている。その多くは、ネットワーク管理を簡単化するためのプロトコルである SNMP と、SNMP の拡張機能としての RMON を利用している。

2.1 SNMP(Simple Network Management Protocol)

SNMP は、ネットワーク上に存在する管理対象の機器と、その管理を司る機器 (管理ステーションと呼ばれる) の間で、管理情報をやり取りするための通信プロトコルである。日本語では「簡易ネットワーク管理プロトコル」と呼ばれる。通信には UDP を用いており、TCP/IP をベースとした管理プロトコルの標準といえる。SNMP は RFC1157 で規定されている。SNMP では、管理対象機器にはエージェント、管理ステーションにはマネージャと呼ばれるソフトウェアがそれぞれ常駐して通信を行う。管理されるのはネットワーク機器の性能や構成、障害、セキュリティ、アカウントの 5 種類である。マネージャやエージェントは、これらの管理情報を MIB(Management Information Base、「ミブ」) と呼ばれる独自のデータベースに保存する。エージェントはマネージャからの要求に応えて、MIB から必要な情報を送信する。

SNMP の特徴は、その名が示すようにプロトコルが単純なことである。たとえば、マネージャとエージェントの間でやり取りされる SNMP のコマンド (命令) やレスポンス (応答) は、基本的に 6 種類だけと少ない。特にエージェント側は、障害発生などのイベントをマネージャに通知することを除けば、すべてマネージャからの要求に応じて MIB から情報を引き出して送信するという受け身の動作だけなので、プログラムはコンパクトで実装も容易である。そのためハブやルータなど、プログラム サイズが限定されるネットワーク機器にも SNMP はよく実装される。逆にマネージャ側は、エージェントが担わない仕事をすべてこなす必要があるので、複雑になりやすい [1]。

2.2 RMON(Remote network MONitoring)

SNMP から利用できるモニタリングエージェントとして RMON(Remote network MONitoring) が存在する。RMON MIB はパケットをモニタリングするのに有効な MIB が定義されており、特定パケットのみを観測する Filter 機能、パケット数に対して閾値を設け検出を行う Alarm 機能、発生したイベントを NMS に伝える Event 機能、パケットのキャプチャを行う Capture 機能などが挙げられる。RMON MIB を実装した専用機器を RMON エージェント・RMON プローブ等と呼ぶ。RMON を利用することにより SNMP を介して遠隔地のネットワークのパケットモニタリングが実現可能になると共に、専用ハードウェアで構成された RMON は高い観測性能を実現する [2]。

RMON プローブが作成する統計情報は RMON MIB と呼ばれ、IETF(Internet Engineering Task Force) によって RFC(Request For Comments) として規定されている。RMON MIB は RMON1 と RMON2 の 2 つのグループに分けられており、RMON1 グループは物理層、データリンク層、RMON2 グループはネットワーク層からアプリケーション層までの統計情報である [3]。

以下に、RMON プローブの特長を示す。

(1) 遠隔監視
RMON プローブは RMON マネージャーと IP(Internet Protocol) に基づいた通信機能を持つ。このため、遠隔地にある RMON マネージャーから RMON プローブの設定を行ったり、プローブが作成した統計情報を読み出すことができる。また RMON マネージャーは複数の RMON プローブの統計情報を読み出すことによりシステム全体の監視が可能となる

(2) 詳細統計情報作成
RMON プローブは、RMON MIB に基づいた非常に詳細な統計情報を作成する。また、RMON プローブは、パケット解析の専用機であるため一般的に処理能力も高い。

(3) 常時監視
RMON プローブは RMON マネージャーから収集条件を設定されたあとは自動で統計情報を作成し続ける。また、統計情報を長期間格納するための十分なメモリを備えており、常設することによってネットワークの異常を検知後、過去にさかのぼって調査することができる。

(4) マルチベンダ環境対応
RMON プローブと RMON マネージャーの間で行われる RMON MIB のやり取りは、ネットワーク管理プロトコルとして一般的な SNMP を用いて IP ネットワーク上で行われる。RMON MIB、SNMP、IP ともすべて業界標準であるため、マネージャーとプローブのベンダが異なっても使用可能である。

3 LiveOS

FD(フロッピーディスク)、CD-ROM など、ハードディスク以外の媒体にシステムをインストールし、ハードディスクレスで起動・動作するオペレーティングシステムを、ここでは LiveOS と呼ぶこととする。LiveOS には、古くは FD を利用したルータから、最近では CD-ROM や DVD-ROM を利用して、本格的な Linux を体験できるものなどが存在する。LiveOS には、CD-ROM による Linux が数多く存在し、KNOPPIX などが有名であるが、Microsoft Power Pointer を搭載した、プレゼンテーション用の Live Windows なども存在する。また、Windows や Linux な

どの OS のインストール CD も、CD-ROM から起動する LiveOS の一種である。

LiveOS の機能を有した CD-ROM は LiveCD と呼ばれる。LiveCD による Linux は、1CD Linux と呼ばれることが多いが、Live Linux と呼ばれることもある。

3.1 FD ルータ (floppyfw)

floppyfw は、Linux で動作するファイアウォール機能付きのスタティック・ルータである。ここでいうファイアウォール機能とは、一般的なファイアウォールではなく、パケットフィルタリングによるものであることを断っておく。

floppyfw の特徴を以下に示す。

- 全システムが 1 枚の FD に収まるので、HDD が必要ない
- 386SX 以上の CPU、8MB 以上の RAM で動作する
- NAT(IP マスカレード) をサポート
- DHCP クライアント (外部向け) と DHCP サーバ (内部向け) 機能をサポート
- ポートフォワード機能をサポート
- klogd/syslogd によるログ保存機能をサポート
- VPN 機能をサポート

floppyfw のシステムは、1.44MB の FD に収まる。FD にアクセスするのはブート時だけで、運用は RAM ディスク上で行われる。起動時間も、HDD にインストールしたフルシステムの Linux と同程度で、シャットダウンは電源をオフにするだけでよい [4]。

3.2 1CD Linux(KNOPPIX)

KNOPPIX とは CD のみでブート可能な Linux ディストリビューションである。ドイツの Klaus Knopper 氏が Debian パッケージを元に開発を行っている。KNOPPIX は現在、様々なカスタマイズが施され、教育用、実用の両面で広く利用されている。日本語 KNOPPIX は産業技術総合研究所による [5]。

KNOPPIX の特徴は、オープンソースソフトウェアで構築されていることである。オープンソースソフトウェアのみを利用することで、再配布・カスタマイズが可能となっている。また、CD からの起動であるので、同様の内容の CD を複数用意することで、簡単に環境の統一を図れるだけでなく、どこでも環境を再現することが可能となる。さらに、1CD Linux の利点として、システムを CD に格納することから、ハードディスクにすでにインストールされている Windows 環境を損なうことなく、Linux を利用でき、またシステムに異常を来たした場合は再起動することで、再度 CD-ROM から正常な状態のシステムを復旧することが可能である点が挙げられる。

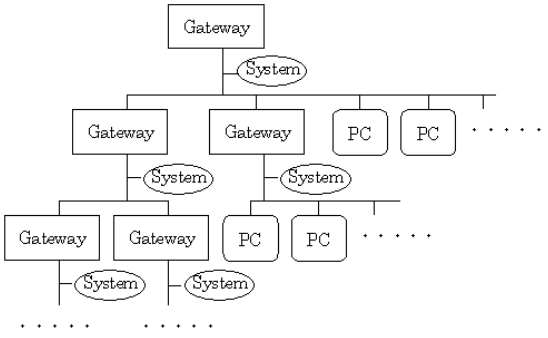

図 1: ネットワーク構成例

4 システム仕様

目的とするシステムの仕様について説明する。

目的とするシステムは、ゲートウェイを出入りするネットワークトラフィックを測定するシステムである。

4.1 ネットワーク構成

システムは、何らかの形でネットワークを流れるトラフィックの流量を取得する必要がある。本システムは、RMON プローブのように、測定対象となるゲートウェイ付近に設置し、直接 IP パケットを取得することで、流量を計測するものとする。

図 1 に、ネットワークの構成例を示す。

4.2 システム構成

システムは、測定対象であるゲートウェイ付近に設置され、パケットを取得するトラフィック測定エージェントと、全トラフィック測定エージェントを管理・制御する管理マネージャとで構成される。

4.2.1 トラフィック測定エージェント

トラフィック測定エージェントは、以下の 3 つの機能を有する。

(1) LiveCD
システムは、LiveCD 上で実現する。LiveCD を用いることで、測定対象となるゲートウェイの数が大量であっても、配布と導入を容易に行うことができる。また、LiveCD 上でシステムを開発することで、配布先のシステム環境を考慮する必要がなくなることから、開発効率の向上にもつながる。

(2) パケットキャプチャ
システムは、ゲートウェイを出入りするパケットの総量を測定するために、パケットキャプチャを有する。本システムは、トラフィックの測定を目的とするので、IP パケットのヘッダ部分のみを参照する機能の

みがあれば、要件を満たす。

(3) 異常検知・通知機能

システムはさらに、異常なトラフィックを検知し、その事態が発生した場合は直ちに管理マネージャへと異常を通知する機能を有する。

本システムは、ネットワーク管理の補助ツールとなるべくして開発を進めている。異常トラフィックの発生は、その原因が 1 台のホストにあったとしても、それが所属するネットワーク全体に深刻な影響を与えかねない重要な問題である。異常トラフィックが発生した際には、迅速に管理者へと報告する仕組みは必須であると考える。

4.2.2 管理マネージャ

管理マネージャは、稼動中の全エージェントのリストを保持するなど、エージェントの動作を補助する機能を有する。

5 開発状況

現在の開発状況とシステムの仕様を報告する。

5.1 LiveCD

LiveCD は現在、「Red Hat Linux 7.3(カーネル 2.4)」OS に最新パッチをあてたものを元に開発されている。

5.2 トラフィック測定エージェント

トラフィック測定エージェントは、起動と同時に自身の測定対象であるゲートウェイの MAC アドレスを管理マネージャに報告し、自分以外のエージェントが測定対象としているゲートウェイの MAC アドレスのリストを、管理マネージャからダウンロードする。この MAC リストは、異常を検知した際、異常を報告すべきかどうかの判断に利用される。

5.3 パケットキャプチャ

パケットキャプチャは、パケットキャプチャ用ライブラリ「pcap」を用いて作成した。

作成したパケットキャプチャの仕様を以下に示す。

- バックグラウンドで動作しパケットを取得する
- ゲートウェイから出入りするパケットのみ参照する
- パケットのヘッダ情報のみを参照する
- 時間、送信元ホスト、送信先ホスト、ポート番号、バイト数を記録する

5.4 異常検知・通知機能

システムは、パケットキャプチャで取得したトラフィックを時系列で記録し、以下のアルゴリズムにより、異常を判断する。

アルゴリズム 1

過去 1 分間のトラフィックが X 以上で、かつ過去 10 分間の平均トラフィックの Y 倍以上であれば、異常と判断する (ただし、X, Y は実験によって定まるパラメータ)

また、異常が検知された場合、システムは管理マネージャに対して異常を通知する。ただし、図 1 のように、システムは再帰的に設置されており、下層で異常トラフィックが発生した場合、その異常は上層へ向かって伝播し、結果複数のシステムが異常トラフィックを検知することとなる。そこでシステムは、予め各システムの測定対象であるゲートウェイの MAC アドレスのリストを、管理マネージャから取得しておき、異常トラフィックを発生させているノードの MAC アドレスが、MAC リストにあれば異常を報告せず、MAC リストになければ異常を報告する。

6 問題点と解決提案

6.1 問題点

本システムは、現状いくつかの問題点が存在する。そのひとつが、パケットをどの位置でどのように取得するかである。

パケットキャプチャを利用したネットワーク管理は伝統的な手法であるが、スイッチングハブが存在するネットワークでは、パケットキャプチャの動作に障害を及ぼすことが一般に知られている。旧来のリピータハブが、取得したパケットを全てのポートへ一律に転送するのに対し、スイッチングハブは、必要最低限のポートへしか、パケットを転送しない。そのため、スイッチングハブが存在するネットワークでは、パケットキャプチャを設置する位置によって、取得できるパケットに差異が生じる。

もうひとつの問題点は、ネットワークのセキュリティポリシーから、ネットワークカードのプロミスキャスモードでの動作を許可しない場合があることである。ネットワークカードは本来、自分宛のパケット以外のパケットを無視することで、動作を効率化している。しかし、パケットキャプチャを使用する場合、全てのパケットを取得する必要があることから、自分宛以外のパケットも取得するようネットワークカードの動作を変更しなければならない。そのために用意されているのが、プロミスキャスモードである。しかし、パケットの中には、個人的な情報や、パスワードなど、本来隠匿すべき重要な情報が含まれており、プロミスキャスモードの利用は、他のユーザのセキュリティを損なってしまう。そのため、プロミスキャスモードの使用を制限したネットワークや、プロミスキャスモード

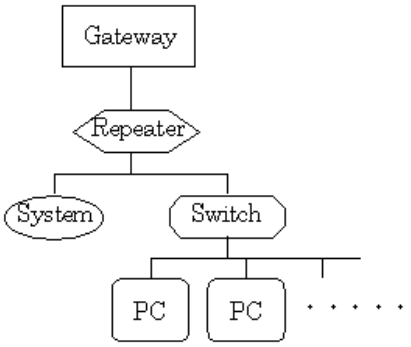

図 2: リピータを利用したパケット取得方法

で動作しているネットワークカードを検出する技術も存在している。そのようなネットワークで本システムを稼動させるには、プロミスキャスモードを利用しないパケット取得方法を実現させる必要がある。

6.2 解決提案

6.2.1 システムの接続方法

ネットワークにスイッチングハブが存在する場合は、システムを接続する位置を考慮する必要がある。本システムは、ネットワークから出入りするトラフィックを測定することが目的なので、取得したいパケットは、ゲートウェイから出入りするパケットに限定できる。ゲートウェイから出入りするパケットを取得するためのネットワーク構成としては、以下の 3 つが考えられる。

(1) リピータハブを利用する方法
図 2 のように、ゲートウェイの直下にリピータハブを接続し、そのリピータハブの直下に本システムを設置する。他のホストはリピータハブ以下に接続することで、システムはゲートウェイを通過するパケット全てを取得できるようになる。

(2) ポート・ミラーリング機能を利用する方法
高価なインテリジェントハブには、あるポートから出入りするパケットを、特定のポートへも転送するポート・ミラーリング機能を有する製品が存在する。図 3 のように、ゲートウェイの直下にインテリジェントハブを接続し、インテリジェントハブのポート・ミラーリング機能を利用して、ゲートウェイのパケットをシステムが接続されたポートへも転送すれば、システムはゲートウェイを通過するパケットの全てを取得できるようになる。

(3) PC ルータ
図 4 のように、本システムにルーティング機能を追加し、本システムをゲートウェイとして設置することで、ゲートウェイを通過するパケットの全てを取得できるようになる。

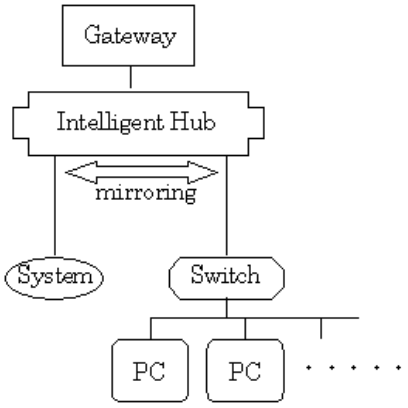

図 3: ポート・ミラーリングを利用したパケット取得方法

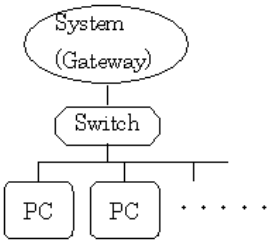

図 4: PC ルータを利用したパケット取得方法

6.2.2 プロミスキャスモード不許可の場合

プロミスキャスモードが許可されていないネットワークにおいて、ゲートウェイを通過する全てのパケットを取得するためには、プロミスキャスモードを使用しなくても、それらのパケットが本システムへ転送される仕組みが必要となる。これを実現するための提案としては、以下の例が挙げられる。

(1) PC ルータ
図 4 のように、本システムにルーティグ機能を追加し、本システムをゲートウェイとして設置することで、システムはプロミスキャスモードを使用することなく、ゲートウェイを通過する全てのパケットを取得することができる。

7 今後の課題・展望

7.1 実用規模での運用試験

現状では、最大 5 台の PC と、1 台のルータのみという極小規模なネットワーク内での動作試験を行っているのみなので、今後はより大きな規模での運用試験を行っていき

たい。

7.2 本システムによるサブネット管理補助

本システムは、全学のあらゆるネットワーク内で稼動させることを目指している。一般に、ファイアーウォール機能を持つゲートウェイ以下の情報は、セキュリティの確保のために隠匿されるのが常であるが、これは全体ネットワークの管理者にとって、内部の各サブネット内の情報が隠されてしまうという弊害ももたらす。サブネットにおけるセキュリティホールは、全学のセキュリティを脅かすものであり、全体ネットワークの管理者にとって、サブネットのセキュリティには決して無関心ではいられない。しかしながら、上述のような事情から、サブネットの管理は手間がかかる。また、本学では研究室・部署ごとに Web・メールサーバを構築・運用しており、全学のネットワーク管理者が、これら全てのサーバについてセキュリティ面のサポートを行うのは不可能である。そこで本研究は、LiveCD の特長を活かし、サブネットの管理を補助する仕組みを提供することを考えている。

本研究で作成した LiveCD は Linux OS で構築されており、現在 Web サーバとメールサーバがすでに含まれている。サブネット内においては、この LiveCD 付属の Web・メールサーバを利用してもらうことで、全体ネットワークの管理者は、LiveCD に含まれた Web・メールサーバに関するセキュリティ情報にのみ注目すればよくなり、個々のサーバへの不安を解消できる。

またさらに、作成した LiveCD には、サブネット内で稼動中のホストのリストを自動作成する機能が含まれている。この情報は、異常トラフィックが検知された際や、他のシステムにより、ウイルスの感染や不正侵入などが検知された際に、どのホストに原因があるのかを、より詳細に検証するために利用できると考えている。

LiveCD の環境構築は、基本的に CD-ROM の製作者に委ねられており、それを利用するユーザの労力はほとんどない。例えば、LiveCD に含まれている Web サーバの新バージョンがリリースされた際、LiveCD の Web サーバをバージョンアップさせるには、CD-ROM の製作者は、新しいバージョンの Web サーバをインストールした上で LiveCD を作り直す作業が必要であるが、ユーザは、ただ CD-ROM を新しいものに差し替えて PC を再起動するのみでよい。

このように、LiveCD によって、それ以降の機能拡張は大変容易に行える。著者らは、豊橋技術科学大学でのネットワーク管理を担当しているので、LiveCD を普及させることは実際に可能であり、本研究は全学のネットワークセキュリティ向上のための土台作りとしての側面を持つと言え、今後はこの点も踏まえて開発を進めていきたい。

8 おわりに

本論は、分散協調システムによる、異常トラフィック検知・通知システムを設計し、その開発状況を報告した。本システムは複数のゲートウェイから出入りするトラフィックを測定することを想定したものであるが、これを LiveCD 上で実現することで、配布と導入を効率化しつつ、LiveOS の特長を利用することで、今後の機能向上の優位性を持たせることを試みた。

LiveCD の特長は、CD を複製することでシステムを複数用意でき、専用の機器を必要とせず、一般的な PC を流用することでシステムを導入できること、さらに、システムを稼動させる PC の環境別対応を考慮しないシステム開発ができること、などである。

本論はまた、これらの特長を活かし、開発中のシステムが、全学的なネットワークセキュリティの向上のための土台となり得る可能性を示唆した。

参考文献

[1] @IT:Insider's Computer Dictionary SNMP
http://www.atmarkit.co.jp/icd/root/42/5784442.html (*2005.4.8*)

[2] WIDE PROJECT
第 14 部 ネットワーク管理とセキュリティ
http://www.wide.ad.jp/project/document/reports/pdf2000/part14.pdf (*2005.4.8*)

[3] 遠隔ネットワーク監視プローブ (RMON プローブ)
青島健次, 大貫泰照, 栗山勝, 越前谷孝嗣, 大江慎一
日立電線,*No.19(2001-1).*

[4] ゼロ円でできるブロードバンド・ルータ
北浦訓行, @IT Linux Square
http://www.atmarkit.co.jp/flinux/special/router/router00.html (*2005.4.8*)

[5] KNOPPIX 3.7 日本語版
http://unit.aist.go.jp/itri/knoppix/index.html
(*2005.4.8*)

[6] Recovering Latent Time-Series from their Observed Sums: Network Tomography with Particle Filters.
Edoardo Airoldi, Christos Faloutsos.
SIG-KDD,2005-1