第 V 部

ネットワーク管理とセキュリティ

第５部
ネットワーク管理とセキュリティ

第１章　はじめに

The Internet is growing in all respects. New types of devices are getting connected, newer applications are emerging and newer security threats are looming. Most important of all, the Internet is permeating into every facet of our lives. Monitoring, managing and securing this Internet have become a task of utmost importance. The WIDE-NetMan-WG has been working to expand the scope of network monitoring for effective management and security.

The IETF-MIPv6-WG is working on a Mobile-IPv6 standard that will allow IPv6 communication between entities which may be moving across networks. Designing the standard framework for monitoring and managing mobile entities is a challenge. The WIDE-NetMan-WG has been working in this direction — as a first step the requirements are analyzed and a preliminary MIB is defined. The internet-draft has been posted in the archives it is being discussed in the IETF-MIP6-WG. This work is described in Section 2.

Along with monitoring, network security has always been found lagging behind the protocol developments. The security threats that exist in an IPv6 network are still not fully understood and analyzed and there are few IDS systems that are offering IPv6 security monitoring features. We have been working on studying potential threats that may exist in IPv6 networks. We have implemented the IPv6 signature based security monitoring features in one of the most widely used IDS systems — Snort. This work is described in Section 3.

Network monitoring and management have always taken a backseat in protocol development. Though IPv6 devices are commercially available and operational in networks, few of these devices offered any monitoring capability. This problem plagued the JGN-IPv6 testbed. To cope with this problem we developed and extended our passive monitoring technology to monitor multiprotocol networks. This system is now being used to monitor the JGN-IPv6 network. It has proved effective and useful. This work is described in Section 4.

Knowing how the network links are being used and who is using them has been a requirement since the early days networking. But with the spread of the Internet and it dynamic nature, this is a challenging task. We extended our passive monitoring technology to aggregate and synthesize flows based on network information. We then served the information in the context of a network map. To obtain the network map related to context information we peered with a local BGP-router. That makes the system dynamic and self-sufficient. This proved to be a powerful media of conveying the usage of the network at a given point of time, graphically and online. This work is described in Section 5.

Continuing our search to characterize Internet traffic we have analyzed the traffic seen on the WIDE backbone. On the one hand, we have used this opportunity to characterize the usage of the network in terms of secure protocols and insecure protocols. On the other hand, we have attempted to study and understand the stability characteristics of the traffic. This work is described in Section 6.

As an example of the technique of data collection from mobile devices, we have experimented with monitoring automobiles. We have used the data-aggregation technique to gather bulk data at small intervals. A wide spectrum of interesting

applications of this technology is emerging. This work is described in Section 7.

第 2 章　Development of MIP6mib

2.1 Introduction

The Internet has become an indispensable part of the infrastructure that supports modern society. The move now is to make it ubiquitous. It should be available, anywhere, anytime, to anybody stationary or on the move. The emphasis is on mobile networking. The IETF-MIPv6-WG is working on a Mobile-IPv6 standard that will allow IPv6 communication between entities which may be moving across networks. Designing the standard framework for monitoring and managing MIPv6 entities is a challenge.

In this section we describe the work that we are doing towards defining a portion of the Management Information Base (MIB), the Mobile-IPv6 MIB, for use with network management protocols in the Internet community. Mobile-IPv6 MIB will be used to monitor and control Mobile Node, Home Agent and Correspondent Node functions of a MIPv6 entity.

2.2 The Mobile IPv6 Protocol entities

Mobile IPv6 (mipv6)[142] specifies a protocol which allows nodes to remain reachable while moving around in the IPv6 Internet. An entity which implements the mipv6 protocol is a mipv6 entity. There are three types of entities envisaged by the mipv6 protocol.

mobile node (MN): A node that can change its point of attachment from one link to another, while still being reachable via its home address.

correspondent node (CN): A peer node with which a mobile node is communicating. The correspondent node may be either mobile or stationary. [Note that a correspondent node does not necessarily require mipv6 support.]

home agent (HA): A router on a mobile node's home link with which the mobile node has registered its current care-of address. While the mobile node is away from home, the home agent intercepts packets on the home link destined to the mobile node's home address, encapsulates them, and tunnels them to the mobile node's registered care-of address.

2.3 Mobile IPv6 Monitoring and Control Requirements

For managing a MIPv6 entity it is necessary to monitor the

- capabilities of MIPv6 entities
- traffic due to MIPv6
- binding related statistics (at HA, CN, MN)
- binding details (at HA, CN)
- history of binding updates (at HA, CN, MN)

The MIPv6 protocol document stipulates that several MIPv6 related parameters should be manually configurable. The MIPv6 MIB should define managed objects that can be used to configure the related parameters.

2.4 MIB Design

The basic principle has been to keep the MIB as simple as possible and at the same time to make it effective enough so that the essential needs of monitoring and control are met. It is envisaged that wherever possible existing MIBS will be used (e.g. IPsec MIB, Neighbor Discovery MIB, Tunnel MIB..) for monitor and control of MIPv6 entities.

The MIPv6MIB is comprised of following sets of groups

mipv6IP: a generic group containing objects that are common to all the mobile IPv6 entities.

mipv6HA: this group models the Home Agent service. It is comprised of objects specific to the services and associated advertisement parameters offered by the Home Agent on each of its links. It also contains objects pertaining to the maintenance of the Home Agent list on each of the links on which the

service is offered.

mipv6MN: this group models the Mobile Node service. It is comprised of objects specific to the Dynamic Home Agent discovery function and related parameters. It also contains objects that record the movement of the mobile node.

mipv6CN: models the Correspondent Node and is primarily scoped to its participation in the Return Routability procedure for achieving Route Optimization triggered by the mobile node.

mipv6Notifications: defines the set of notifications that will be used to asynchronously monitor the mobile IPv6 entities.

The tables contained in the above groups are as follows —

mipv6BindingCacheTable: contains the BindingCache.

mipv6BindingHistoryTable: the history of the Bindings.

mipv6NodeTrafficTable: the mobile node-wise traffic counters.

mipv6MnBLTable: contains information about the registration requests sent by the mobile node and the corresponding results.

mipv6CnCounterTable: contains the mobile node-wise registration statistics.

haAdvConfTable: contains the configurable advertisement parameters for all the interfaces on which the home agent service is advertised.

haCounterTable: contains registration statistics for all mobile nodes registered.

haListTable: contains the list of all routers that are acting as home agents on each of the interfaces on which the home agent service is offered by this router.

For the specific MOs in each of the tables, please refer to *draft-ietf-mip6-mipv6-mib-01.txt*[1].

2.5 Security Considerations

There is a number of management objects defined in this MIB module with a MAX-ACCESS clause of read-write and/or read-create. Such objects may be considered sensitive or vulnerable in some network environments. The support for SET operations in a non-secure environment without proper protection can have a negative effect on network operations. These are the tables and objects and their sensitivity/vulnerability:

mipv6Enable: This value of this object is used to enable or disable the mipv6 functionality on a mipv6 entity. Access to this MO may be abused to disrupt the mipv6 communication.

haAdvLifetime: Access to this object may be abused to set the advertised lifetime to incorrect values. That will have an adverse impact on the mipv6 communication.

haAdvPreference: Access to this object may be abused to force MNs into selecting the wrong HA.

Some of the readable objects in this MIB module (i.e., objects with a MAX-ACCESS other than not-accessible) may be considered sensitive or vulnerable in some network environments. It is thus important to control even GET and/or NOTIFY access to these objects and possibly to even encrypt the values of these objects when sending them over the network via SNMP.

The address related objects in this MIB may be considered to be particularly sensitive and/or private. The care of address related objects reveals the location and movement of the mobile node. This information may be considered to be private and sensitive and must be carefully handled.

- mipv6BindingHstCOAType
- mipv6BindingHstCOA
- mipv6MnBLCOAType
- mipv6MnBLCOA

The mobile node's home address and home agent related information may be considered to be sensitive too as these may provide clues to a malicious party on ways to disrupt the mobile nodes communication channels.

- mipv6BindingHstHomeAddressType

1 http://www.cysol.co.jp/contrib/draft-ietf-mip6-mipv6-mib-01.txt

- mipv6BindingHstHomeAddress
- mipv6MnHomeAddressType
- mipv6MnHomeAddress

The Correspondent node's addresses related MOs will reveal the nodes with whom the MN is corresponding. This information may be considered private and sensitive.

- mipv6MnBLNodeAddressType
- mipv6MnBLNodeAddress

SNMP versions prior to SNMPv3 did not include adequate security. Even if the network itself is secure (for example by using IPsec), even then, there is no control as to who on the secure network is allowed to access and GET/SET (read/change/create/delete) the objects in this MIB module.

It is important that implementers consider the security features as provided by the SNMPv3 framework (see RFC 3410[24], section 8), including full support for the SNMPv3 cryptographic mechanisms (for authentication and privacy).

2.6 Status

The MIB definition is undergoing discussion in the IETF-MIPv6-WG[152]. The first revision of the draft is ready. A preliminary prototype implementation is slated for March 2004. A MIPv6 network is being set up to experiment with the MIB.

第 3 章　Snort-IPv6

本章では、我々が行っている IPv6 ネットワークにおけるネットワーク侵入検知システム（NIDS）の実装の方針について説明する。

3.1 方針

我々は IPv6 ネットワーク用の NIDS を実装するに当たり、オープンソフトウェアとして広く普及している snort（バージョン 2.0.2）を基に行った。snort の実装状況から、我々は以下の項目について IPv6 対応が必要であると判断した。

1. ルールヘッダの IPv6 対応
2. 検知機能の IPv6 対応
3. ログ出力の IPv6 対応

最初の項目は、snort がホームネットワークアドレス、および外部ネットワークアドレスを把握するために必要である。2 番目の項目は、snort が観測した IPv6 トラフィックを解析する上で必要である。最後の項目は、snort が IPv6 トラフィックを解析した結果を出力する上で必要である。以後、上で挙げた項目の実装の方針について説明する。

3.2 実装

最初に、ルールヘッダの IPv6 対応における実装の方針について説明する。ルールヘッダの一例を図 3.1 に記す。

ルールヘッダの第 2 項目は、監視対象となるネットワークプロトコルについて指定することができる。snort-2.0.2 では ip、icmp、tcp、udp を指定することができる。そこで、我々は、新たに IPv6 トラフィックを対象とする ip6、ICMPv6 トラフィックを対象とする icmp6 を指定できるように拡張する。

ルールヘッダの第 3 項目、第 5 項目では送信元アドレス、到達先アドレスを指定することができる。そこで、我々は以下の機能を備えるように拡張する。

- IPv6 ネットワークアドレスを、ネットワークアドレス/ネットワークアドレス長の書式で指定することができる（例 2001:200::/35）。
- 複数のネットワークアドレスを指定することができる。この場合、IPv4 アドレス、IPv6 アドレス両方とも同時に指定することができる（例 [192.168.0.0/24, fe80::/12]）。
- any で指定した場合は、IPv4 ネットワーク、IPv6 ネットワーク両方を監視対象とする。

次に、検知機能の IPv6 対応における実装の方針について説明する。まず、snort の検知機能、Decode Engine、Preprocessor、Detection プラグインについて説明する。

Decode Engine では、pcap ライブラリにより捕捉された第 3 層パケットの情報を snort で定義しているパケット構造体に引き渡す。IPv6 対応において我々は、snort-2.0.2 では実装されていない IPv6 ヘッ

```
alert ip any any -> any any
```

図 3.1.　ルールヘッダの一例

ダ情報、ICMPv6 情報をパケット構造体に引き渡すことができるように拡張する。

Preprocessor に関しては、IPv4 パケットを前提とした実装がされているのが現状である。従って、各 Preprocessor の実装について IPv4 パケットを前提として実装された箇所を IPv6 に対応するよう見直すことが必要である。今回は表 3.1 に挙げた Preprocessor を対象とする。

Detection プラグインに関して、TCP や UDP、パケットペイロードに関するものは、Decode Engine において適切にパケット構造体に情報を引き渡すことによって、IPv6 対応は行える。しかし、ttl や icmp type など IPv4 ヘッダ、ICMPv4 に特定した Detection プラグインも幾つか存在する。我々はこのようなプラグインを参考にして、IPv6 ヘッダ、ICMPv6 に対応した Detection プラグインを実装する。表 3.2 に実装予定の IPv6 ヘッダ、ICMPv6 に対応した Detection プラグインの一覧を記す。

3.3 まとめ

本章では、snort を基にしたネットワーク侵入検知システムの IPv6 対応の方針について、および現状の実装状況について説明した。今後の予定として、試験版を一般に公開し、不具合状況や改善要望などの意見を広く求める。試験版の公開先として
`http://www.cysol.co.jp/conrtib/snortv6/`
を予定している。また現在の snort のリリース版 2.1.0 への対応も今後の検討課題である。

表 3.1. IPv6 に対応予定の Preprocessor

Preprocessor 名	機能
conversation	プロトコルの通信状況把握用
portscan2	ポートスキャン検知用

第 4 章 JGN-IPv6 ネットワークのモニタリング環境構築とモニタリング

4.1 概要

IPv6 による次世代インターネットの普及を促し、その潜在能力を最大限引き出すためには、ネットワーク管理技術も次世代に対応した新しい技術が必要になる。しかし、IPv6 ネットワークにおける管理技術の整備は大幅に立ち遅れており、早急な整備が必要となっている。そこで我々は、通信・放送機構（TAO）直轄研究「分散型ネットワーク監視システムの構築」を東北大学および(株)サイバー・ソリューションズの共同研究として行い、IPv4/IPv6 ネットワークに対応した SNMP エージェントとパッシブ型ネットワーク情報収集プローブの研究開発を行った。この研究開発により、管理プロトコルの IPv6 対応が実現し、IPv6 管理の基盤技術の確立と、これまでできていなかった IPv6 情報の汎用的な収集方式を確立し、結果として、IPv6 ネットワーク上での IPv6 プロトコルのみによる管理と IPv6 トラヒック情報の詳細な収集が実現した。

そこで我々は、この研究成果を基に、広域にわたる IPv6 ネットワークを安全で効率的かつ容易に管理できる管理技術の確立を目的とし、IPv6 セキュリティ管理技術の確立と監視システムのスケーラビリティの向上、IPv4 に比較して複雑性が増している IPv6 の構成管理を容易にする技術についての研究を継続して行ってきた。当初計画では、

1. パッシブ型ネットワーク情報収集プローブのセキュリティ関連機能の拡張
2. インターネット標準プロトコルである SNMP と LDAP（ディレクトリアクセスプロトコル）を基盤とした分散配置されたネットワーク情報収

表 3.2. IPv6 ヘッダ、ICMPv6 に対応した Detection プラグイン

Detection プラグイン名	機能
ip6_proto	IPv6 ヘッダの Next Header 値を検知
i6type	ICMPv6 ヘッダの type 値を検知
i6code	ICMPv6 ヘッダの code 値を検知
icmp6_id	ICMPv6 ヘッダの ECHO ID 値を検知
icmp6_seq	ICMPv6 ヘッダの ECHO sequence 値を検知

集プローブの活用技術の開発

3. IPv6 ネットワークマップの自動生成と活用技術に関する研究開発を実施し、JGN IPv6 ネットワーク上での実運用と、その評価の実施

を目標として掲げた。

1. に関しては、不正検出型侵入検知システム（IDS）の事実上の世界標準である snort パッケージの IPv6 化を行った（3 章参照）。

2. に関しては、分散プローブにおけるネットワーク情報ラベルの変更を隠蔽し、それと管理者が定義するネットワーク情報ラベルとのマッピングを保持して継続的な情報収集を可能にするシステムを、LDAP を用いて実現する（現在も開発を継続中）。

3. に関しては、ルーティングプロトコルのパケットをパッシブモニタリングしてネットワークマップを自動生成する手法を開発した。

本節では特に、JGN-IPv6 ネットワークにおけるネットワーク情報収集インフラストラクチャの構築と、2. の成果について詳説する。

4.2 JGN-IPv6 ネットワークのモニタリング環境

研究開発と平行し、JGN IPv6 ネットワークにおける実運用実験を行うための IPv6 分散プローブ環境の構築を進め、平成 15 年 3 月末までに全国 15 サイト、のべ 40 箇所のギガビットおよびファーストイーサネットリンクのモニタリング環境が実現した（表 4.1）。

モニタリングの結果は Web で公開されており、NetGrapher および MRTG を用いて可視化されている[2]。

4.3 分散プローブを用いたモニタリングの問題点

モニタリングシステムによって観測される、リンクのトラフィック量といった「観測対象」は、ネットワークのトポロジなどが大きく変化しない限りは変更されることは少なく、また変更時にはオペレーションの観点から対応が行われることが多いため、その変更の発生はそれほど問題になることはない。しかし、モニタリングシステムそのものの設定、構成の変更は、分散プローブメカニズムを採用している本システムでは比較的頻繁に起こりうるだけでなく、オペレーションに直接関係がないことからその変更が必ずしも認知されて適切に対処されるとは限らない。結果として、データ収集に支障を来す場合が多くなるという問題点がある。

具体的には以下の 3 つが挙げられる。

表 4.1.　JGN-IPv6 ネットワークのモニタリング環境の配置

	サイト名	モニタ可能リンク数		マネジャ
		100baseTX	1000base-SX	
1	東北大学情報シナジーセンター	1		
2	東北大学電気通信研究所	6		1
3	名古屋大学	2	1	
4	ソフトピアジャパン	3		
5	京都大学		1	1
6	広島大学	2	1	
7	広島市立大学	1		
8	九州大学	8	1	
9	佐賀大学	3		
10	TAO 北九州リサーチセンター	3		
11	TAO 大手町 IPv6 システム運用技術開発センター	2	1	1
12	堂島	2	1	
13	TAO 高知通信トラフィックリサーチセンター	2		
14	大阪大学	2	1	
15	東京大学	3		

2　http://cpmanager.shiratori.riec.tohoku.ac.jp/traffic.html

1. ディスクスペースの不足：
   継続的なモニタリングと情報蓄積の結果として発生する。遠隔地のプローブ群の残ディスク容量の管理が比較的容易でないことと、モニタリングシステム専用のディスクを用いている場合が多く、その場合はディスクが溢れてもオペレーションに影響が出ないため、発見が遅れることが多い。
2. MO（プローブ）へのリーチャビリティ変化：
   プローブの動作している PC のダウンや、中間ネットワークの障害によって発生する。突発的要因のため事前の予測と対処が難しいことと、1. 同様モニタリングシステムのダウンが通常のオペレーションに影響を与えないことが発見を遅らせる原因となる。対策としてプローブの稼動状況をチェックし、遠隔において行われているモニタリングの成否を逐一確認する必要が生じる。またより信頼性を高めるために、複数のマネジャを設置して同一観測対象のモニタリングを行い冗長性を確保する、といった方策が考えられる。
3. MO マッピングの変化：
   モニタリングシステムは、内部的にはネットワーク情報とネットワーク・インタフェースの情報を結びつけて管理しているため、たとえば元と異なるネットワーク・インタフェースを持つプローブに置き換えたり、ネットワーク・インタフェースの故障による交換を行ったりすると、それまでのマッピングが意味のないものに変化する可能性がある。この場合、モニタリングそのものは継続できる場合が多いため、途中からデータの意味がまったく異なってしまうといった問題が生じる。構成変更時の適切な対処および、変更前のデータとの連続性の維持などが必要となる。

以上の問題点をまとめると、おおよそ以下の 2 つに集約することができる。

1. MO-Index の変更による情報の一貫性の欠落
2. 分散マネジャ・プローブ群の適切な管理の必要性

1. に関しては 4.4 節で詳しく述べる。2. に関しては、必要なチェック機構をプローブやマネジャに実装していく形で対処を進めている。プローブの稼動状況に関しては、IPv6 Ping を用いてネットワークの接続性も同時に計測し、障害を検知する仕組みを実現している。これは Unreachable を検出すると、メールによる障害報告を送信するものとなっている。しかし Ping には応答しても SNMP による情報の取得はできないケースもあり、改善の余地があるといえる。

また、当初 TAO 大手町に設置したマネジャのみによる情報収集を継続してきたが、これに加えて京都大学に設置したマネジャを同様の設定で動作させ、情報収集の冗長化を図っている。データは 1 日毎の単位で分割して保存する仕組みとし、データの不連続がどちらか一方で発生した場合にマージを行いやすくしている。

ディスク溢れの検出など、検出システム全体の改善が今後とも課題となる。

4.4 LDAP を用いた情報ラベル同期手法の実現

本節では、4.3 節で指摘した問題点 1. について詳細に述べる。

まずは、プローブの構成変化が発生してもデータをもらさず取得することを保証できなければならない。分散プローブの特性として、プローブの管理者がサイト毎に異なっている。この場合、各サイトでの変更をマネジャに反映する統一的な手段がないことが問題の本質であるといえる。

プローブの構成情報で、上記のような変更によって変化するものは、IP Address、SNMP community のような認証情報、そして、プローブ上で収集ポイントを認識するために用いられるインタフェース番号やデバイス名などである。これらの変化を登録し、マネジャはその情報を参照して変化に対応することで、継続的なモニタリングが可能になる。このため、LDAP（Lightweight Directory Access Protocol）を活用した構成情報管理の手法に関して、現在設計を行っている。

第 5 章　BGP 情報の蓄積とそれを活用したトラフィック分析手法

5.1 ネットワークのコンテキスト情報

ネットワーク情報をモニタリングする際には、その情報が、いつ、どのような状況で、どのリンクをモニタして得られたのかという「コンテキスト情報」

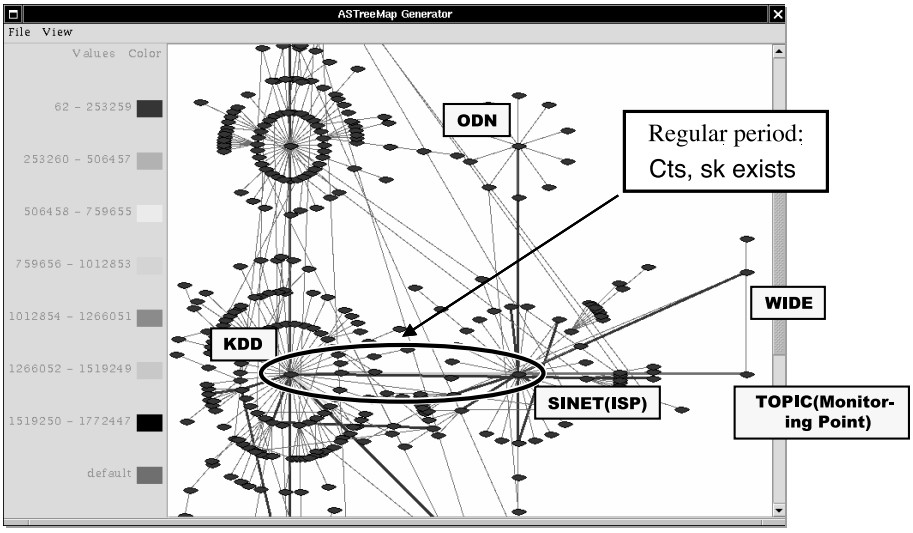

図 5.1.　Traffic tree visualization at regular period

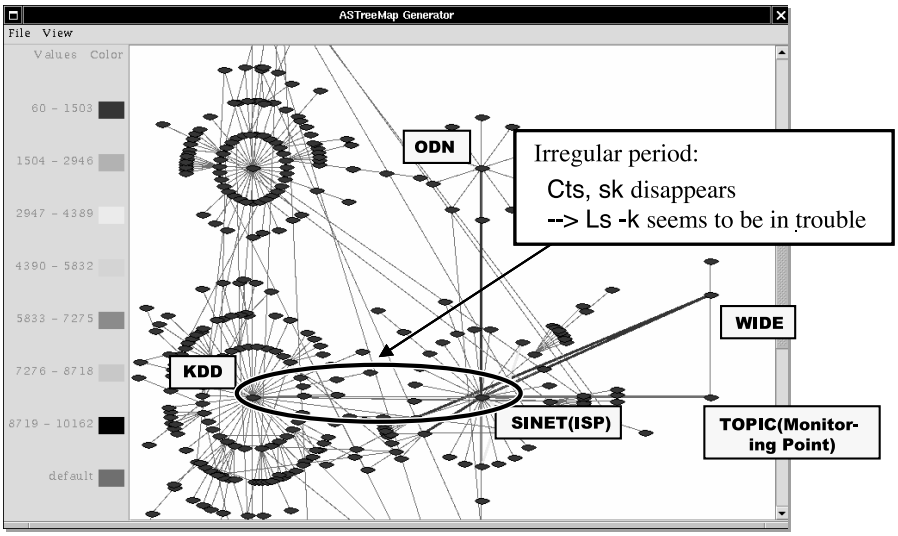

図 5.2.　Traffic tree visualization at irregular period

は欠かせない要素となる。モニタしたリンクが同一であっても、時間によってその意味は異なるものとなり、またルーティングの状態によって流れるトラフィックの性質も変化するからである。

ネットワークエンティティの接続状態を表すネットワークマップや、ルーティングの状態、すなわちルーテイングテーブルやルーティングプロトコルの内部状態は有用なコンテキスト情報である。したがって、これを収集し、そしてネットワーク情報と組み合わせることで、さらに有用な情報を得ることができる。

5.2 ネットワーク情報の集約手法

ネットワークのリンクを流れるトラフィックは多種多様で量も膨大であり、パケットを全てキャプチャして分析するような伝統的なトラフィックモニタリングの手法の適用は既に不可能であり、分析のリアルタイム性も失ってしまう。ネットワーク情報を活用するためには、似た性質の情報を集約し、サマライズした結果を出力する機能が重要である。しかし従来の集約手法は細かな設定を必要としたり、出力結果が必ずしも現実のネットワークの構成とマッチしない、などの問題があった。そこで我々は、ネットワークの構成情報を IRR（Internet Routing Registry）

から自動取得し、現実のネットワーク構成に基づいて、IP アドレスをキーとして動的にトラフィック情報を集約する手法を開発した [160]。また、前述のコンテキスト情報として traceroute の結果から生成したネットワークマップと、集約したトラフィック情報を組み合わせることで、ネットワークの障害検出と診断を可能にする手法を提案した（図 5.1、図 5.2）。

5.3 BGP 情報の収集

BGP ルータの情報は、コンテキスト情報やネットワーク構成情報として有用であり、これをパッシブモニタと組み合わせる手法の開発がこれからの課題である。このため、BGP ルータと peering を行い、情報を収集するサーバの構築を行った。詳細は mawi-WG の報告書を参照して頂きたい。

第 6 章　WIDE バックボーントラフィックの解析

ネットワーク管理を行う上で、ネットワークの利用状況の把握やトラフィックの傾向の分析は欠かすことのできない要素である。特に、WIDE バックボーンのように大量のトラフィックが流れ続けるネットワークでは、如何に効率的にこれらの分析を行うかが鍵となる。

今年度我々は、WIDE のバックボーンで観測したトラフィックデータを対象として、以下の項目について解析を行った。

1. セキュアなプロトコルの利用状況
2. トラフィックの安定性

6.1 セキュアなプロトコルの利用状況調査

この調査の目的は、セキュアなアプリケーションの利用状況および、現在のインターネット利用者のセキュリティ意識を把握することである。まず、想定するユーザを管理者等の比較的スキルのあるユーザと、アプリケーション利用が主である一般のユーザに大別して考える。そして、前者についてはリモートログインに使用するプロトコル、後者についてはメールの取得に使用するプロトコルについて、暗号化などを採り入れたセキュアなプロトコルの使用状況を調査した。

図 6.1 に、リモートログインに使用される TELNET と SSH のトラフィックが全トラフィック中に占める割合について調査した結果を示す。対象としたデータは、WIDE バックボーンの観測点 B で採取したデータ（2002/10/20〜2002/10/25 分）である。送受信ポート番号のいずれかが 23 番である TCP パケットを TELNET に関連するパケット、22 番である TCP パケットを SSH に関連するパケットと判断した。TELNET は通信が暗号化されないセキュアでない通信とみなし、SSH は暗号化を行うセキュアな通信と考えた。

図 6.1 より SSH のトラフィックが大半を占めていることが分かるが、TELNET のトラフィックも常に一定以上流れていることが分かる。TELNET のトラフィック全てがセキュアでないとは断定できないが、リモートログインが比較的スキルのあるユーザが利用するアプリケーションであることを考えると、スキルのあるユーザの一部にもセキュリティ意識の低いユーザがいることが伺える。また、このことから一般のユーザでは更にセキュリティ意識の低いユーザの割合が増えるであろうことが予想できる。

次に、同じトラフィックデータを対象として、メール取得に使用する POP について、セキュアな通信とセキュアでない通信の割合を調査した。送受信ポート番号のいずれかが 109 番または 110 番である TCP および UDP パケットを、通信路が暗号化されない POP2 または POP3 の通信によるパケットと考え、セキュアでない通信とみなした。また、送受信ポート番号のいずれかが 995 番の TCP パケットを、暗号化を利用する POP over SSL を使用した通信のパケットであるとし、セキュアな通信とみなした。結果を図 6.2 に示す。結果より、通信路を暗号化して

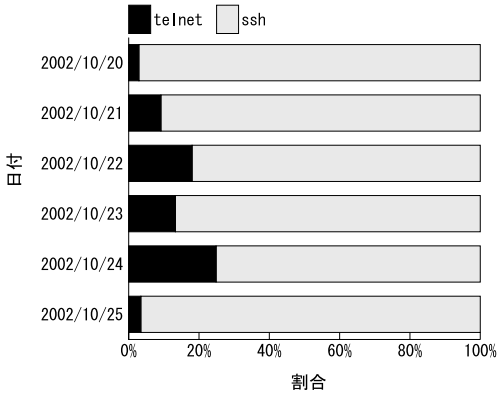

図 6.1.　TELNET と SSH のトラフィックの割合

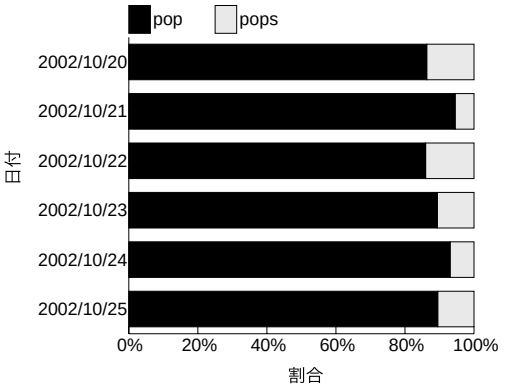

図 6.2. セキュアでない POP とセキュアな POP のトラフィックの割合

いない通信が大部分であることが分かる。これらの中にはパスワードを暗号化する APOP を利用しているものも含まれているが、メールの本文自体が暗号化されるわけではないため、セキュアでない通信とみなした。

以上の結果から、ネットワーク管理者などの比較的スキルのあるユーザと比較すると、一般の利用者のセキュリティ意識が大きく立ち後れていることがわかる。このひとつの原因としては、POP over SSL のような技術が、一般ユーザにとってまだ敷居の高いものであることが考えられる。ネットワーク全体のセキュリティレベルの引き上げを図るためには、こういった技術の存在の啓蒙と共に、より使いやすい形で一般ユーザに提供することが急務であるといえる。

他の観点からの分析については、情報処理事業振興会（IPA）の調査研究の一環として、「インターネット情報インフラ防護のための技術調査　調査報告書」に記載してあるので参照して頂きたい。

6.2 トラフィックの安定性解析

トラフィック分析は、ネットワークを観測して得られたトラフィックデータを分析し、その結果を管理者に提示するという役割を担っており、ネットワーク管理に欠かすことのできない要素である。管理者への負荷を軽減するためには、より高度な分析を行い、詳細かつ有用な情報を管理者に提供することが必要となる。しかし、高度な分析は、分析対象が膨大になる大規模ネットワークにおいては大きな負荷を伴うことも多い。このことから、大規模ネットワークにおけるトラフィック分析では、高度な分析を行う前段階として、シンプルな手法による簡易分析を行い、高度な分析の対象を限定するといった段階的な分析が必要になると考えられる。そこで我々は、この簡易分析の 1 つのアプローチとして、定常的なトラフィックの存在に着目し、トラフィックの安定性の解析実験を行った。

ネットワークトラフィックには、ある一定の種類のトラフィックが常に支配的であるという安定性と呼ばれる性質があると言われている [301]。このことから、ある観測点で一定期間トラフィックを観測する場合、プロトコルによって規定されるような情報項目は、通常時には特定の範囲の値しか取り得ないことなどが予想される。そこで、実際に WIDE バックボーンのトラフィックの安定性を調査した。

まず、トラフィックをある長さのスロットに区切り、対象とする情報項目（例えば送信元 IP アドレス等）のパケット数をカウントし、パケット数の多い順にソートする。そして、その上位 N 位までを考えた場合のパケット数が全体に対して占める割合を、TopN 支配率 $D(N)$ として式 (6.1) のように定義し、安定性を示す指標の 1 つとして考える。

$$D(N) = \frac{(Number\ of\ packets\ in\ TopN\ group)/slot}{(Number\ of\ packets)/slot}\ [\%] \tag{6.1}$$

情報項目として送信元 IP アドレスを考えたとすれば、全体に対して特定の送信ホストが占める割合であり、Top3 で $D(3)$ が 90%となったとすれば、3 つのアドレスが全通信の 9 割を占めていることになる。

WIDE バックボーントラフィックの連続する 5 日分のデータについて、以下の情報項目の安定性を調査した。

1. 送信元 IP アドレス
2. TCP のフラグの組合わせ

送信元 IP アドレスは母集団の数とその変動が大きくなり得る情報項目であり、TCP のフラグの種類は基本的に母集団が少ない数であり、ほぼ一定となる情報項目である。

送信元 IP アドレスについての TopN 支配率 $D(N)$ の分析結果を図 6.3 から図 6.7 にそれぞれ示す。パケット 10000 個分を 1 スロットとし、スロット毎の $D(N)$ の推移を示している。各線が 1 スロット分の $D(N)$ の推移に対応している。スロット毎に $D(N)$ の増加傾向に差はあるものの、ほぼ全てのスロットで上位 70 位から 80 位までで全体の 5 割を占めてい

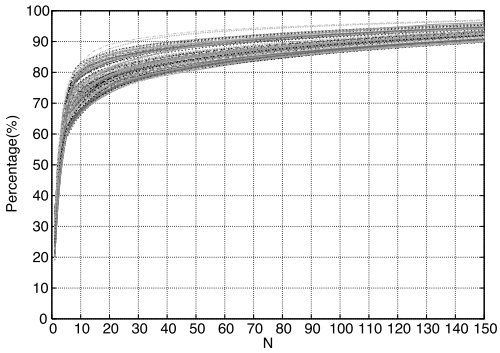

図 6.3. 2001/5/27（送信元 IP アドレス）

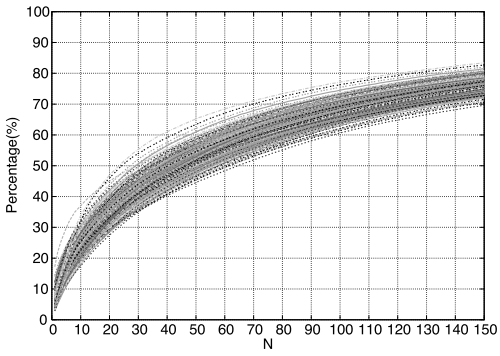

図 6.4. 2001/5/28（送信元 IP アドレス）

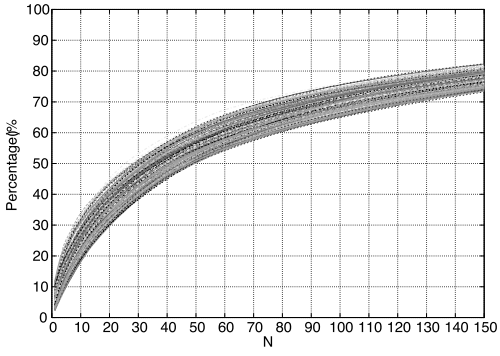

図 6.5. 2001/5/29（送信元 IP アドレス）

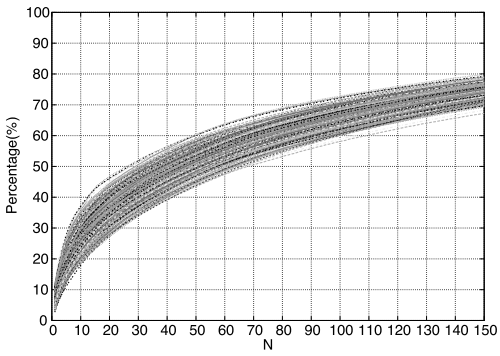

図 6.6. 2001/5/30（送信元 IP アドレス）

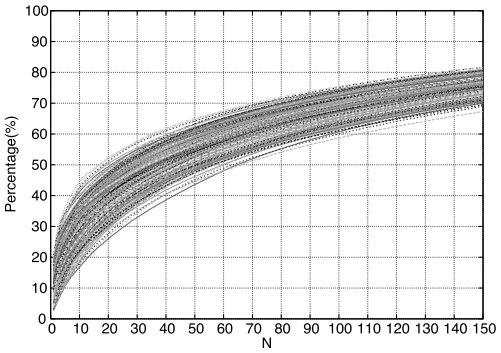

図 6.7. 2001/5/31（送信元 IP アドレス）

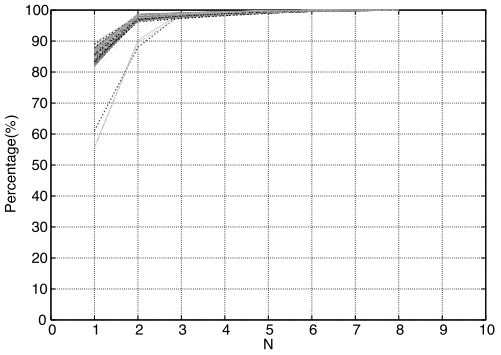

図 6.8. 2001/5/27（フラグの組合わせ）

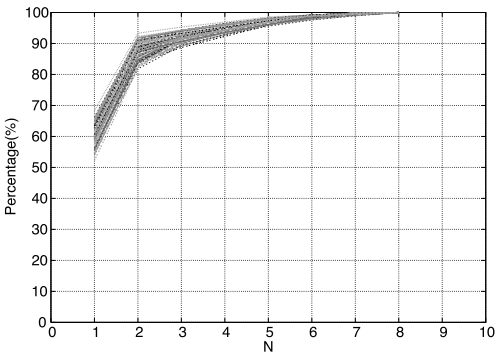

図 6.9. 2001/5/28（フラグの組合わせ）

ることが分かる。これはどの日付でも基本的に同様である。また、2001/5/27 のデータについては特殊な傾向を示しており、上位 5 位で全体の 5 割が占められている。このことから、特定の数個のホストから連続的にある程度の量のパケットが送信されていることが分かる。つまり、この日は他の日に比べて特別に安定性が高くなっているため何らかの異常と考えることができる。

また、TCP のフラグの組合せについての $D(N)$ 分析結果を図 6.8 から図 6.12 にそれぞれ示す。送信元 IP アドレスと比べ、母集団自体が小さいため最上位

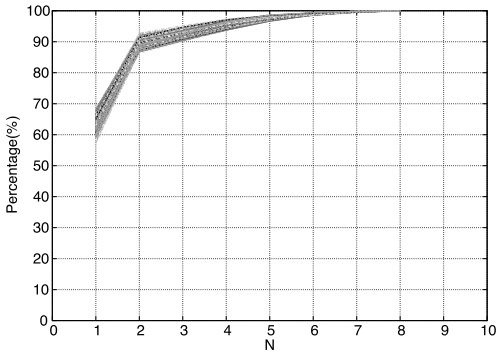

図 6.10.　2001/5/29（フラグの組合わせ）

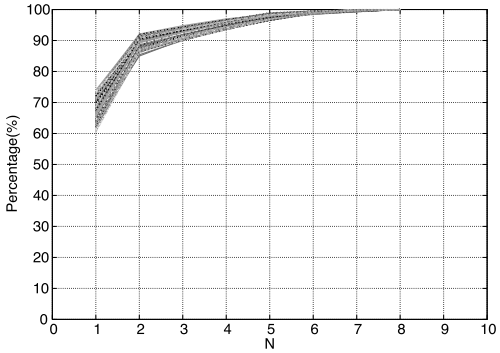

図 6.11.　2001/5/30（フラグの組合わせ）

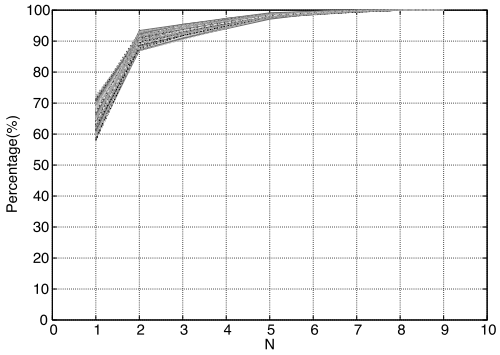

図 6.12.　2001/5/31（フラグの組合わせ）

のみで全体の 5 割を占めていることがわかり、トラフィックの安定性が顕著に現れているといえる。ほぼ全てのスロットで最上位となっているのは、Ack フラグであり、プロトコルの観点から考えても妥当な結果である。また、送信元 IP アドレスでの結果と同様に、2001/5/27 のデータは他の日と大きく異なった特性を示し、最上位のみで全体の 8 割以上を占めている。

この 2 つの結果を合わせて考えると、特定のホストが Ack フラグの立ったパケットを送信し続けている可能性が示唆される。これらの結果から、安定性の分析がネットワークの異常を捉える上で有用な手法となる可能性が高い。

第 7 章　Cooperation with InternetCAR WG

7.1 Monitoring framework for Internet Car

In 2003, we cooperated with InternetCAR WG, defined the car monitoring framework and implemented it on the car.

In the following we abstract the process of information collection as the act of monitoring the value of an “information object” or object. A standard and open framework is required for Information Collection from automobiles. The framework should provide

- a means for defining objects which will be monitored

  It is not possible to enumerate the list of objects that will or may be of monitoring interest. Also, the objects of interest will vary depending on the monitored object. The list of objects will grow in step with time and technological developments. The object definitions
  - must be unique and unambiguous
  - must be ‘pluggable’ in the monitoring framework
- a message protocol for transferring information (the value of the objects)

  The information will be carried from the car to the monitor (person or machine) by a standard protocol which will be independent of the car or the monitor machine or person. The message protocol
  - should be lightweight.
  - must have security mechanisms built in to provide privacy, authentication, and integrity.
- mechanism for controlling access to the objects

  Not all information will be accessible by all

users. A standard mechanism must be there to control 'read' and 'write' access to these objects.

The Simple Network Management Protocol (SNMP)[99] meets these requirements very nicely. It is comprised of

- Mechanisms for describing and naming objects and events for the purpose of management.

  This is called the Structure of Management Information (SMI). The current version (SMIv2) is described in RFC 2578[174], RFC 2579[173] and RFC 2580[172].
- Message protocols for transferring management information.

  The current version of the message protocol is called SNMPv3 and is described in RFC 3412[23], RFC 3414[16] and RFC 3417[235].
- A view-based access control mechanism described in RFC 3415[324].

A more detailed introduction to the current SNMP Management Framework can be found in RFC 3410[24].

The objects which are the target of monitoring and control are called Managed Objects. Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. Objects in the MIB are defined using the mechanisms defined in the SMI.

7.2 Problems and solutions

The general data collection framework for vehicle network is ready with SNMP, but specific problems are raised through the field test. Vehicles are connected with wireless data link, so it has following specific problems for data collection.

- The bandwidth is narrow due to the limitation of cellular phone system
- The data link is likely to be disconnected by shadowing and/or physical condition

Those means the reliability and effectiveness are critical issues of the communication. The bandwidth problem may be solved with 3G cellular service or 802.11a/b/g like infrastructure in future, but it will be costly compared with existing wired link. And shadowing and physical condition problem are essential with wireless communication.

Also, disconnection problem of mobile network requires bulk transport during a short period when the connectivity is stable.

So, the techniques for compaction of the amount of data and transport it within small time window is important.

On the other hand, vehicles are moving everywhere on the road. So we can collect followings as basic information from vehicles.

- GPS information
- Geographical position
- Direction of movement
- Moving information
- Velocity
- Acceleration
- Start/Stop
- Winker status
- Vehicle equipments
- Wiper status
- Road surface sensor
- ABS workload

This information is useful for various players like driver/owner, car vender, road service provider, public transportation, traffic control, and many car related information service providers.

Drivers can obtain IP access from the car with his position and destination information. Car vendors can obtain information for usage and maintenance. Public transportation service can be improved with precise traffic information. Traffic control can be improved also for signal deployment and the control. It is possible to realize many types of car related information service provider.

To realize the mobile node imitated information collection, the design of notification data is important. Useful notification can reduce the risk of data collection failure due to the link stability problem. Useful notification is that it can notify the changes of mobile node status.

We define the following notifications to collect the vehicle information,

- Short Stop/Short trip
  - This can notify distinct car movement, suppressing slight movement in traffic jam.
  - This is defined as threshold values for the combination of velocity and duration.
- Winker status
  - This is usefulness to notify the intention of driver, which also indicates the change of car direction.
  - This is useful to evaluate the effectiveness of PTPS at Yokohama public bus.
- Wiper status
  - This can notify the whether condition of car location.

We can define many other notifications like this. Important point is that those notifications have to be defined application by application. So, the definition and standardization should be done carefully.

7.3 Application development

We are trying some of applications like below,

- Load surface monitoring with JH
- PTPS evaluation with Yokohama city bus organization
- Load maintenance monitoring with Nagoya load management service

7.4 Future work

We are continuing developing,

- Standardization of overall MIB structure for vehicle network
- Standardization (on going) Aggregation MIB
- Build concrete architecture of Mobile node initiated data collection

to build more reliable, efficient and useful system for the Internet Cars.

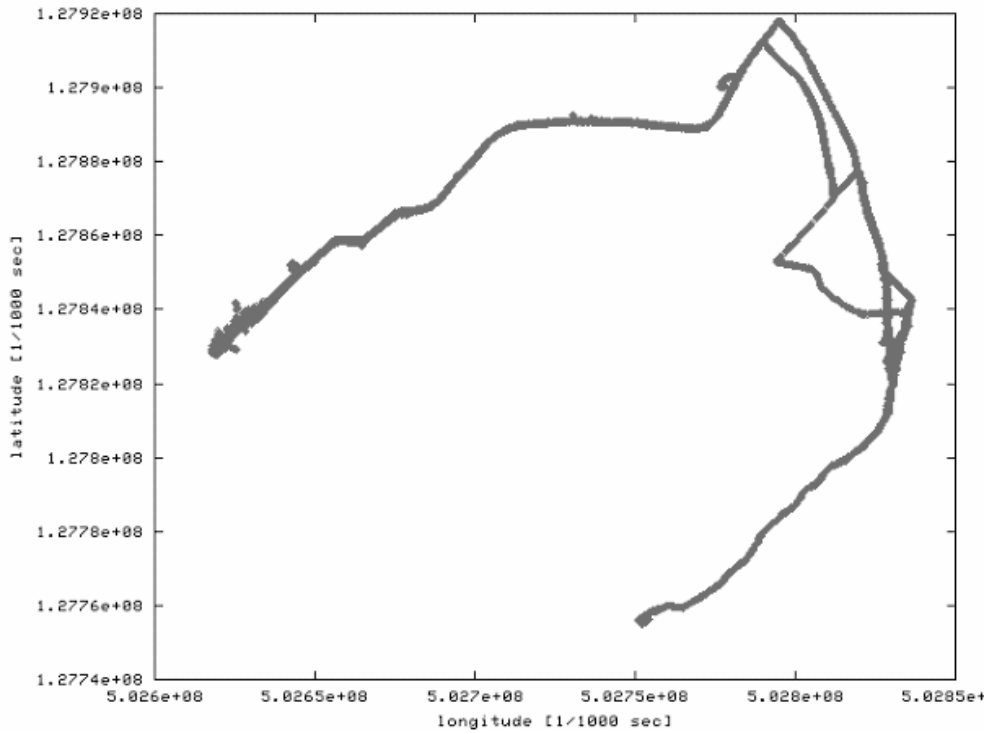

図 7.1. Longitude-Latitude plot

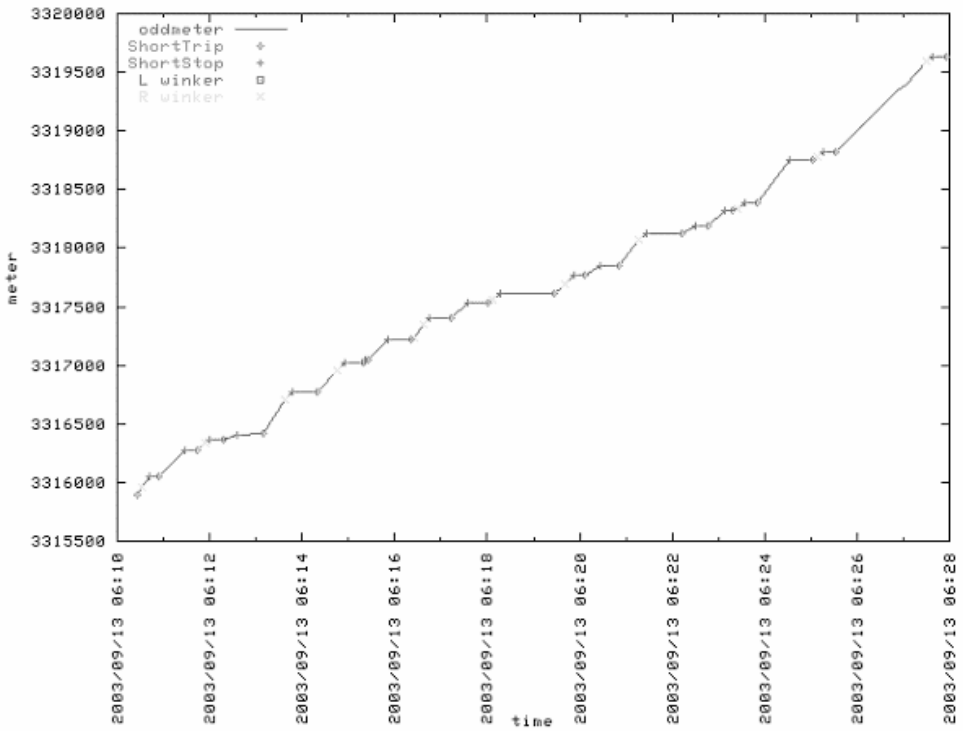

図 7.2. Time-Event occurrence

図 7.3. Traffic JAM is caught by this system