構成発見の問題

2C－8

村山 優子
広島市立大学情報科学部

1　はじめに

この１５年ほどの間のインターネットに代表されるコンピュータ通信網の発展における最も顕著な点は，その拡大度であろう．初期の網の階層構造についての研究 [6] やそれに基づいた開放型アーキテクチャ [4] [2]，また，パケット交換技術 [1] により，単にひとつの網の構築だけでなく，それらをつなぎ合わせた網間網の形成により，インターネットは地球規模の通信網を成すまでに至った．この結果として，網は期待された以上に拡大し，限られた範囲での網環境のためにしか設計されていない既存の管理システムでは対処できない問題点が浮上してくる．そうした問題の一つに，現在の網環境内に存在するオブジェクトとそれらの位置をどのように知るかという問題がある．これを構成発見と呼び，本稿では，ホストやルータといった網オブジェクトの構成発見における問題点を論じ，それらの問題から派生する安全性などの問題点を示す．

2　構成発見の定義とその問題

インターネットの古典である Shoch[7] の表現で言えば，コンピュータ通信網の動作においては次のような知識が必要とされる；

どのようなものが存在し，
それらがどこに位置し，
それらにどのようにして到達できるか．

これらの知識を以下で構成情報と呼ぶことにする．網管理システムでは，どのノードを管理し，それらがどこにあるか，また，それらが管理装置からどのように監視および制御することができるかという知識が必要である．電子メイル・システムにおいては，どこかにメッセージを送信する場合，受信者とそのアドレスを知ることが必要である．経路制御では，各ノードは使用可能な他のノードの存在とそれらを通してどの宛先まで到達可能かなどの情報が必要である．

構成情報は，従来，網管理システムと情報システムで管理されてきたと考えられる．網管理システムは，網管理作業 のために網の構成情報を保持している．情報システムとは，ここでは，運用のための情報を提供するシステムを指す．ノード名を網アドレスに変換するネームサーバや様々な資源についての名前や位置などの情報を提供するディレクトリは，比較的変化の少ない情報を扱うので静的なタイプの情報システムと言えよう．これに対し，経路情報交換システム，網アドレスを下層網アドレスに変換するアドレス変換システム，ブリッジシステムなどは，動的情報システムとみなすことができよう．

静的な情報システムは環境規模の拡大問題について，階層的な分離型 (decentralised) 管理方式 [3] を導入することで各管理域を小さくすることで解決してきた．これは，上記の網管理システムも同様の解決法に進みつつある．動的情報システムでは，動的学習によって拡大問題にある程度対処している．

構成発見は拡大する環境下で問題となるのであるなら，この小域分離や動的学習で解決できるのであろうか．階層的分離型や動的学習で得られた情報には，実は，２つの問題が潜在する．それは，情報が現状に則していないことからおこる一貫性の問題 *inconsistency* と，情報自体が始めから間違って登録されてしまう不正確さの問題 *invalidity* である．これら２つの問題は，様々な波及効果を網環境に及ぼす．

3　誤った下層アドレスによる問題

インターネット・プロトコル (Internet Protocol: IP) 環境下で，あるノードの下層アドレスが放送アドレスに誤って設定された時に網の嵐 (network storm) と呼ばれる現象が起こる．網の嵐とは，パケットが網上に過剰に溢れ，各ノードのインターフェースがそれ以上何も出力できなくなるような状態を指す．この問題は特定な環境だけに起こるわけではなく，IP のようなパケット交換が放送型の網メディア上で使われる時に起こる普遍的な問題として考えることができる．

ひとつの部分網において，２つの異なるルータが，同じ下層メディア・アドレスを持つと，各ルータ宛のトラヒックは倍増される．ある部分網上に存在する３台以上のルータが同じ下層アドレスに設定されてしまった場合，網の嵐が引き起こされる．一般に，部分網上の n 個のルータ機能のあるノードが，同じ下層プロトコル・アドレスに設定された場合，寿命（TTL）の値が t に設定さ

Configuration Detection and Its Problems
Yuko Murayama
Faculty of Information Sicences, Hiroshima City University

れていたとすると，ひとつのノードに向けて送り出されたパケットがその部分網上に再生されるパケットの総数 S は：

$$S = \frac{(n-1)\{(n-2)^{t-1}-1\}}{n-3}$$

となる．

この状況は，実は，ひとつのホストが下層プロトコルの放送アドレスに設定されてしまうだけで，すぐに，作り出されてしまう．“連鎖反応” (chain reaction) と呼ばれる現象のひとつである [5]．網の嵐状態を解除するには，誤った設定をされたホストやルータだけでなく，問題のない他のルータも停止しなければならないところが重大な点である．

4 網層の安全性に対する脅威

情報の非一貫性と不正確さの問題は，様々な層での安全性に影響を及ぼす．一般に，網層より上位の層ではそれぞれのアプリケーションごとに，通信相手同士 (end-to-end) での対策がとられる．しかし，そのような上位層での対策がこうじられても，なお，網層における安全性に対する脅威は存在する．

網層における安全性に対する脅威には次のようなものがある:

1. 改竄
2. 網資源不正使用 (資源泥棒)
3. トラヒック生成による上位層サービス否認拒否
   a. 連鎖反応による網の嵐攻撃
   b. 目標ホスト宛の多量トラヒック生成攻撃
4. 不正な網情報監視

改竄攻撃では，経路情報交換プロトコルにより不正情報を流し，パケットが偽ルータへ転送されるようにする．アプリケーション層での encryption などの安全対策により，網レベルでのデータ 改竄の脅威は減るが，偽ルータでは，受け取ったパケットの一部を故意に落すような形での情報改竄も可能である．

網資源不正使用攻撃では，未使用の網アドレスを偽ホストに設定し，正規の登録手続きをふまずに網を使用し，他の偽ホスト群と通信し合う．

トラヒック生成によるサービス却下攻撃には，2種類ある．ひとつは，前節で説明した連鎖反応を使用したもので，もうひとつは，多量のメッセージを被害者ホスト宛に向け発信するものである．このトラヒック生成攻撃では，偽ホストは自分の網アドレスや下層アドレスを時によって変えてしまうであろうから，その監視は不可能に近い．

網情報の不正監視は，網のトラヒックを監視することで，他に気づかれずに他のノードのアドレスや非一貫性などの網構成情報が読みとられ，攻撃者に役立つ情報入手の機会を与えてしまう．

5 おわりに

構成発見の延長上には以上のような重大な問題が存在し，それらの解決なしには，本当の構成発見の問題解決はありえない．しかし，これらすべての問題に対する対策を行なおうとすると，それぞれの対策の最大公倍数になってしまい，膨大な制御システムの構築が必要となる．従って，その環境に応じた対策がとられるべきである．

一方で，対策を立てるより，監視装置で充分ではないかという議論がある．しかし，地球規模に広がったインターネット環境などをみると，すでに各ホストやルータさえも，熟練した管理者の制御下にあることは少なくなり，また，そのような管理者がいる場合にはその求められる管理範囲が大きく，監視装置からの情報の有効な活用を人間レベルの管理者に要求することは難しくなりつつある．また，パーソナル・コンピュータの世界では，“接続即稼働 (plug and play)” と呼ばれるような，より安易な網接続の方向へと進んでいる．このような状況では，網自体が解決していくようなメカニズムが望ましいと思われる．

References

[1] V. G. Cerf andP. T. Kirstein. Issues in packet-network interconnection. *Proceedings of the IEEE*, Vol. 66, No. 11, pp. 1386–1408, November 1978.

[2] V. G. Cerf and E. Cain. The dod internet architecture model. *Computer Networks*, pp. pp.307–318, July 1983. North-Holland.

[3] D. R. Cheriton and T. P. Mann. Decentralizing a global naming service for improved performance and fault tolerance. *ACM Transactions on Computer Systems*, Vol. 7, No. 2, pp. 147–183, May 1989.

[4] ISO. Iso 7498 information processing systems - open systems interconnection - basic reference model. International Standard ISO 7498, 1984.

[5] U. Manber. Chain reactions in networks. *IEEE COMPUTER*, Vol. 23, No. 10, pp. 57–63, October 1990.

[6] L. Pouzin. Internetworking. In W. Chou, editor, *Computer Communications*, volume Volume 2: systems and applications, chapter 15. Prentice-Hall, 1985.

[7] J. Shoch. Inter-network naming, addressing, and routing. *Conf. Proc. of IEEE COMPCON Fall 1978*, pp. 72–79, 1978.