適切なアクセス制御状態にあるネットワークシステムの特徴抽出

金岡 晃 †　　藤堂 伸勝 †　　加藤 雅彦 ‡　　岡本 栄司 †

† 筑波大学大学院システム情報工学研究科
305-8573 茨城県つくば市天王台 1-1-1

{kanaoka,okamoto}@risk.tsukuba.ac.jp toudou@cipher.risk.tsukuba.ac.jp
‡ 株式会社アイアイジェイテクノロジー
101-0051 東京都千代田区神田神保町 1-105 神保町三井ビルディング

masa@iij-tech.co.jp

あらまし　アクセス制御が適切にされているネットワークシステムでは、利用されるネットワーク機器にかかわらず出線数分布がほぼ一定になることがわかっている。本研究では、得られた分布からの関数近似を行い、ノード数に依存しない共通パラメータの抽出に成功し、適切なアクセス制御状態下にあるネットワークシステムの次数分布の関数表現を実現した。

Extraction of Parameters for Networked System with Well Managed Access Control

Akira KANAOKA†　　Nobukatsu TOUDOU†　　Masahiko KATO‡
Eiji OKAMOTO†

†University of Tsukuba
1-1-1, Tennodai, Tsukuba, 305-8573, Ibaraki, Japan

{kanaoka,okamoto}@risk.tsukuba.ac.jp toudou@cipher.risk.tsukuba.ac.jp
‡IIJ Technology Inc.
1-105 Kanda Jinbo-cho, Chiyodaku, Tokyo 101-0051, Japan

masa@iij-tech.co.jp

Abstract　Integration of a networked system (NS), which consists of various network equipments and uses LAN technology to provide a service, has become increasingly important. However, there have been few studies on the integration of secure NS. Our previous study suggests that a well-designed NS from an access control viewpoint has a fixed link distribution, regardless of connection restriction. In this paper, we find an approximation function of its distribution using GA algorithm. Found parameters show well approximation result in all type of networked system.

1　はじめに

インターネットを通じてサービスを提供するシステムでは、1 台のサーバのみでサービスを提供していることは稀であり、多くは様々なネットワーク機器を組み合わせ、LAN 技術を利用することで 1 つのサービスが提供されている。このようなシステムをネットワークシステ

ム（Networked System:NS）と呼ぶこととする。

近年 NS の重要性は高くなっており、コスト、冗長性、拡張性、そしてセキュリティなど多くの性質が求められている。これらの性質を満たすために、単純な NS でさえ設計構築は複雑なものとなる。しかし NS の構築や運用はその重要性にもかかわらず、熟練した技術者の経験に依存しており、学術的視点から見た構築・運用方法論や理論などはほとんどなされていない。

NS は様々な機器が様々な機能を提供しているものであり、単一機能での効率化や最適化を図る既存研究を直接適用することは難しい。

また複数機能を集約可能とするモデルも検討されてこなかったが、金岡らにより 1 つの表現上に集約可能とする NS の表現モデルが提案され [1] 、さらにアクセス制御が適切に行われている NS では次数分布が一定の分布形状を取ることがわかり、その形状は特定機器の有無にかかわらず現れることが示された [2]。

本論文では、一定の分布形状を取る次数分布の近似を実現する。近似された関数 $f(x)$ の存在を見つけることで、あらためて適切にアクセス制御された NS には次数分布で共通の特徴を持つことが示され、構築方法論の実現へ向けた有用なパラメータを得た。

第 2 章では、本研究の関連研究について紹介をする。また第 3 章において、NS の次数分布がもつ特徴を述べる。遺伝的アルゴリズムを用いた次数分布の近似関数パラメータ取得についてを第 4 章で述べ、最後に第 5 章でまとめる。

2 関連研究

ネットワークやシステムの設計では、デザイン要件などのもとでネットワークアーキテクチャの最適化やスループットの効率化などが実現されてきた [3] [4] [5] [6] [7]。これらは要件を満たす適切な解決法を提供するが、多くが単一機能をもつ機器によるネットワークやシステムの最適化を行うものとなっている。

一方で、NS 内部で形成されるネットワークは様々な機能より構成されており、そこにはサーバ以外にもハブ、スイッチ、ルータなど多くの機能が存在している。金岡らはそれら異なる機器の特徴を失うことなく NS を表現するモデルを提案した [1]。本稿ではこのモデルを NSQ（**N**etworked System **S**ecurity **Q**uantification）モデルと呼ぶこととする。さらに金岡らの研究結果により、適切にアクセス制御が施された NS は機器の有無や接続の制限にかかわらず、そのモデルにおける次数分布が一定の形状をとる性質を持つことが示された [2]。

表 1: レイヤ定義

Layer 5	抽象サービス (WWW, DNS など)
Layer 4	TCP/IP ポート番号
Layer 3	IP
Layer 2	MAC アドレス空間
Layer 1	物理的接続

3 ネットワークシステムの次数分布

3.1 NSQ モデル

NSQ モデルではサーバやスイッチ、ルータなどの機器はモジュールとして表現される。モジュールは機能に従い、各レイヤ上の複数ノードから構成される。例えば、ルータモジュール（レイヤ 3 中継器：L3R）は複数のレイヤ 3（L3）ノードを持つが、レイヤ 4（L4）以上ではノードを持たない。レイヤ定義は表 1 の通りである。

モジュールは 6 つの種類から成る。WWW や DNS などのサービスを提供するサービスモジュール（S)。そしてサービス要求者の代理を示すインターネットモジュール（I) がある。そしてレイヤ 1 から 4 の各レイヤでの中継を行う中継器がそれぞれ L1R、L2R、L3R、L4R として定義される。たとえばシェアードハブは L1R であり、L2 スイッチは L2R として表される。

各ノードはリンクにより接続される。リンクは、異なるモジュールを同じレイヤで接続するリンクと、同じモジュール内で異なるレイヤを接続するリンクの 2 種類がある。前者は当該レ

イヤ上での直接通信が可能であるかを表現するものであり、後者はモジュール内のノード間の関係を示すものである。図 1 に従来表現の NS 例、そして図 2 に NSQ モデルによる同 NS の表現を示す。

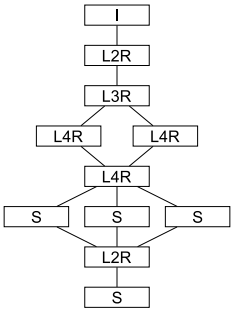

図 1: NS の従来表現

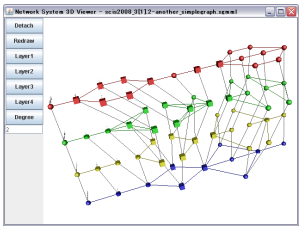

図 2: NSQ モデルでの NS 表現

3.2 効率的な NS 構築アルゴリズム

NS への最適なネットワークアクセス制御を実現するには、モデル内のノードが孤立することなくノード間リンク数を最小化することが必要となる。最適性には議論の余地があり、他の要件を加えた上での最適性を定義することもできよう。例えばコストや冗長性を加えることでのアクセス制御の最適性などが考えられる。しかし本稿ではアクセス制御だけに焦点を当て「リンク数の最小化」を最適の定義とした。

最小リンク数を実現するアルゴリズムの実現は大きな課題であるが、本稿ではアルゴリズム開発に焦点は置いていないため、リンク数を減少させる単純なアルゴリズムを示すに留める。

まず最初に、システム要件より抽出された必要サービスを L5 ノードとし、そのサービス関係を L5 ネットワークとする。各サービスは複数の機器より構成されるため、機能である L5 ノードに対応した部分的なネットワークを最下位レイヤ L1 に持たせる。そして L5 ノードの接続に応じて L1 ノード同士が接続をさせる。L2 ネットワークは L1 ネットワークの接続により一意に設定される。

L3 と L4 のネットワークでは、各ノード間の接続はアクセス制御のルールにより接続の可否が定められる。

アクセス制御のルールがなく、すべての通信が許可されているケース（以後 Loose ケースと呼ぶ）では、各セグメント内にあるモジュール間はすべて通信可能、つまり L3 あるいは L4 ネットワークにおいて部分的な完全グラフを形成する。

一方、金岡らにより L3 と L4 における単純な効率的ネットワーク構築アルゴリズムが提案されている [2]。そこでは、L5 接続に従って L4 接続をされる候補ノードを抽出し、候補ノード間を最小リンク数で接続する。その後、L4 接続にしたがって同様に L3 接続が決定される。以後そのアルゴリズムで接続された NS を「Efficient ケース」と呼ぶ。

3.3 次数分布

2 つのノード間が通信可能である場合、モデル上ではそのノード間にリンクが存在する。アクセス制御ポリシーが NS 間で異なる場合、リンクの数も異なってくるためノードの出線数分布（次数分布）が異なってくる。

この節では、Loose ケースと Efficient ケースでの次数分布を比較する。対象となる NS は Web によるサービスを提供する一般的なものとした。さらに、機能の要件として 4 つのサービスを置く。Internet（I）と Web サーバ（W）、アプリケーションサーバ（AP）そしてデータベース（DB）がその 4 つであり、それぞれ L5 ノードとして割り当てられる。これら 4 つのノードから構成される L5 ネットワークの種類数は 27 となる。そして、前節の構築法により得られた 10764 種類の NS より次数分布を得た。図 3 はノード数が 58 である NS の次数分布を示したものである。

双方ともリンク数が 3（L=3）の時に最大のノード数を持つが、Efficient ケースのほうがノード数が多くなっている。L=4 では、ノード数がほぼ同等になり、L>5 では Loose ケースのほうが多くなる。Loose ケースのほうがより平坦な分布となっていることがわかる。

紙面の問題により本稿では 1 例のみの提示で

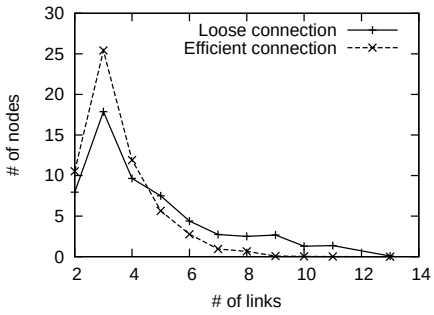

図 3: 次数分布:N=58

あるが、他のノード数においても同様の結果が得られる。

次に、モジュールの有無が Efficient ケースの次数分布に影響を与えるかを調査した。図 4 はノード数 63 の NS での L1R の有無による各次数分布を示したものであり、図 5 はノード数 63 の時の L3R の有無による次数分布を示したものである。これらの結果は、モジュールの有無では次数分布に差が現れないことを示し、アクセス制御が適切にされている NS においてはその次数分布が一定の分布を取ることを示唆していると言えよう。

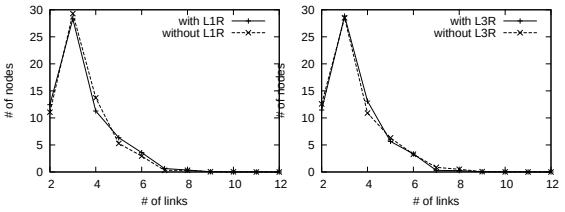

図 4: L1R 有無による 図 5: L3R 有無による
次数分布の差:N=63　次数分布の差:N=63

4　次数分布の関数近似

複雑ネットワークやグラフ理論の分野における近似の多くは指数分布やべき乗則分布ではあるが、NSQ モデルによる NS の次数分布ではその形状からこれら 2 つの分布は当てはまらない。

そこで本節では、統計において用いられているいくつかの分布タイプを用いて次数分布の近似を試みる。

4.1　関数近似の対象

本研究では 6 種類の分布タイプを対象とする。タイプ A は F 分布に近い形のものであり、タイプ B は指数 $\exp(x)$ とべキ x^{α} で決まるタイプのものである。そして最後に離散値の分布としてタイプ C を挙げた。

各タイプは、ポワソン分布やカイ 2 乗分布など統計学においてよく知られている分布を基としているが、そのものではなく、それらに似た構成でよりパラメータの自由度を高めた。

- Type A : F 分布タイプ

Type A : $f(x) \propto \frac{x^{\alpha}}{(1+\beta x)^{\gamma}}$

- Type B : 指数とべキの積

Type B-1 : $f(x) \propto x^{\alpha}\exp(\beta x)$
Type B-2 : $f(x) \propto x^{\alpha}\exp(\beta x^2)$
Type B-3 : $f(x) \propto x^{\alpha}\exp\left(\beta x + \frac{\gamma}{x}\right)$
Type B-4 : $f(x) \propto x^{\alpha}\exp\left\{(\beta \log x + \gamma)^2\right\}$

- Type C : 離散分布

Type C-1 : $f(x) \propto \sum_{k=0}^{x} \frac{\lambda^k \exp(-\lambda)}{k!}$
Type C-2 : $f(x) \propto \sum_{k=0}^{[x/2]} \frac{\lambda_1^{x-2k}\lambda_2^k}{(x-2k)!k!}$

4.2　近似方法

近似は遺伝的アルゴリズム（GA）を用いて行う。GA は各個体を評価関数により評価し、選択・交叉・突然変異を確率的に行う。

評価関数には平均 2 乗誤差などが用いられるが、平均 2 乗誤差はノード数に依存して値が変わるため、ノード数の依存を排除した以下の S を評価関数として用いた。

$$S = \frac{\sum_i (y_i - \hat{y}_i)^2}{\sum_i \hat{y}_i^2} \qquad (1)$$

ここで $\hat{y}_i = f(x_i)$ である。

各個体のパラメータは、各タイプに依存したものとスケール係数 Θ より構成される。例えば、TypeA（$f(x) = \Theta\frac{x^{\alpha}}{(1+\beta x)^{\gamma}}$）の個体は $g = (\Theta, \alpha, \beta, \gamma)$ となる。

	Avg.(> 35)
Type A	0.0133
Type B-1	0.0166
Type B-2	0.0232
Type B-3	0.0161
Type B-4	0.3102
Type C-1	0.3963
Type C-2	0.0476

表 2: GA による各近似の S 値（平均）

4.3 近似結果

GA による近似関数パラメータ取得は、各分布タイプにおいて行う。また各タイプでのパラメータ取得においても、ある NS の特徴ごとで分布に特徴が著しく異なる場合を考慮して、ここではすべての NS をノード数ごとに分割したグループに対してそれぞれ行う。

54 のグループ数と 7 種の対象分布より合計 378 回の GA による近似を行った。結果比較にあたり、まず NS 数が少ないノード数 35 以下のケースを除いた。次に、S 値が他グループの結果と比較して大きく外れているものを GA 近似の失敗として除いた。得られた S 値を図 6 に、またその時の平均を表 2 に示す。

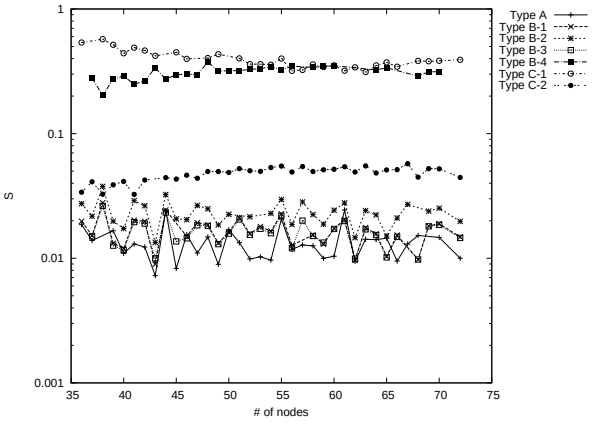

図 6: GA による各近似の S 値

$S = 0$ であるとき、次数分布は近似関数に一致することを示しているため、S 値は 0 に近いほど良い近似結果を示していることとなる。表 2 から、タイプ A が良い近似を示していることがわかる。

次に、グループごとでの分布の差を固定パラメータで吸収されるかを調べるため、近似パラメータをグループによらず固定した近似結果を調査する。ただし、スケール係数 Θ はノード数の変化に対応させるために固定しない。固定パラメータは、上記近似で得た各パラメータを平均することで得る。この際、表 2 で近似精度の低かったタイプ B-4、C-1、C-2 は対象から除いた。

スケール係数 Θ は、ノード数により決定される。それぞれの次数で最大値をとる L=3 の時、それぞれの値は NS のノード数 N と関係があることを示す。図 7 は $L = 3$ を持つノード数の N に対する割合を示したグラフであり、平均の割合は 0.43859 となる。Θ は以下の式を解くことで得られる。

$$0.43859N = f(3) \tag{2}$$

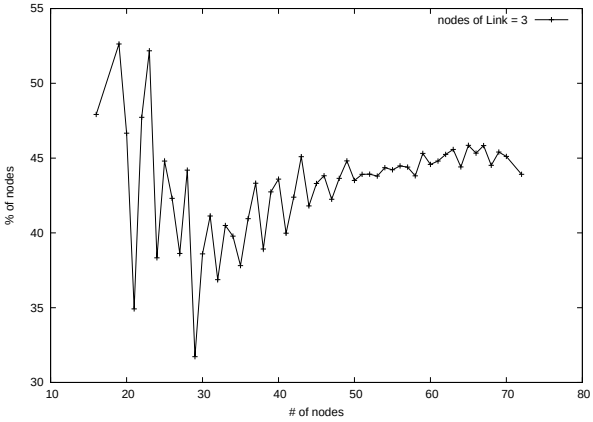

図 7: L=3 を持つノード数の割合

図 8 はは固定パラメータで近似をした時の S 値を示したものであり、表 3 はその平均を示したものである。

この結果より、タイプ A が固定パラメータでも最も良い近似を示していることがわかる。

固定パラメータの値は以下の通りである。

- $\alpha = 29.526$
- $\beta = 0.518$
- $\gamma = 50.019$

	Avg.	Avg.(> 35)
Type A	0.0212	0.0143
Type B-1	0.0268	0.0182
Type B-2	0.0317	0.0238
Type B-3	0.0269	0.0173

表 3: 固定パラメータでの S 値（平均）

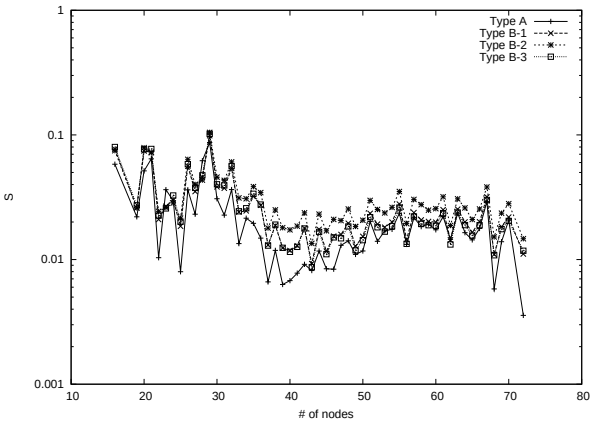

図 8: 固定パラメータでの S 値

5 まとめ

本研究では、アクセス制御が適切にされたネットワークシステムでは NSQ モデル上の次数分布が一定になるという金岡らの結果 [2] を用いて、その近似関数を求めた。

次数分布は、複数の候補を選びそれぞれで遺伝的アルゴリズムを用いて近似した。最もよく近似されている候補を選択し、そのパラメータを抽出した。得られた近似関数は $f(x) = \Theta x^{\alpha}/(1+\beta x)^{\gamma}$ であり、パラメータはそれぞれ $\alpha = 29.526, \beta = 0.518, \gamma = 50.019$ である。

近似関数の存在は、アクセス制御が適切であるネットワークシステムが一定の性質を持つことをあらためて示すものであり、固定パラメータを利用することで、任意のネットワークシステムのアクセス制御状態の適切性の判断指標が得られるであろう。

今後は、本研究の結果から得られたパラメータと数式を用いて、任意のネットワークシステムの状態評価を行う手法を検討する。

参考文献

[1] 金岡晃, 藤堂伸勝, 加藤雅彦, 岡本栄司, ネットワークシステムの安全性定量化に向けた新たな表現モデルとアクセス制御解析, 2008 年暗号と情報セキュリティシンポジウム（SCIS2008）, 2008

[2] 金岡晃, 加藤雅彦, 藤堂伸勝, 岡本栄司, アクセス制御の違いによるネットワークシステムの特性変化に関する考察, 情報通信システムセキュリティ時限研究会（ICSS）, 2008

[3] A. Hayrapetyan, C. Swamy, E. Tardos, Network Design for Information Networks. Proc. of 16th annual ACM-SIAM symposium on Descrete Algorithms, 933-942 (2005)

[4] N. Sadagopan, M. Singh, B. Krishnamachari, Decentralized Utility-based Sensor Network Design. Mobile Networks and Applications 11, 341-350 (2006)

[5] C. Chekuri, Routing and Network Design with Robustness to Changing or Uncertain Traffic Demands. ASM SIGACT News, 106-129 (2007)

[6] L.C. Lau, J. Naor, M. R. Salavatipour, M. Singh, Survivable Network Design with Degree or Order Constraints. STOC'07, (2007)

[7] T. Wolf, Design of a Network Architecture with Inherent Data Path Security. ANCS'07 (2007)