SCIS 2008 The 2008 Symposium on Cryptography and Information Security
Miyazaki, Japan, Jan. 22-25, 2008
The Institute of Electronics, Information and Communication Engineers

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

Network Analysis Model for Security Measurement on Network System and its Access Control Analysis

金岡 晃* 藤堂 伸勝* 加藤 雅彦† 岡本 栄司*
Akira Kanaoka Nobukatsu Toudou Masahiko Katoh Eiji Okamoto

あらまし インターネットを通じて1つのサービスを提供する場合、現在は1つのサーバですべてを行うことはされておらず、各機能をそれぞれの機器で行い全体として1つのサービスを提供するネットワークシステムとなっていることが一般的である。このようなネットワークシステムの設計を行う場合にはセキュリティ面で考慮すべき点が多く、小規模なシステムでさえ設計が複雑となる。本論文では複数機能を表現可能なあらたなネットワーク表現モデルを構築し、ネットワークシステムを構成するさまざまな機能に対し機能ごとの特性判定や論理的整合性を1つのネットワークの中に表現可能とした。さらに、モデルにより表現されたさまざまなネットワークシステムが持つ特性を解析した。その結果アクセス制御に関してネットワークシステムの特性への変化を捕らえることに成功し、さらなる発展としてネットワークシステムが持つ共通特性に関する検討を行った。

キーワード ネットワークシステム、アクセス制御、脆弱性対策、複雑ネットワーク

1 はじめに

インターネットを通じて1つのサービスを提供する場合、現在は1つのサーバですべてを行うことは稀であり、ルータ・ファイアウォール・スイッチ・Webサーバ・アプリケーションサーバ・データベース・侵入検知システム等、各機能をそれぞれの機器で行い全体として1つのサービスを提供するネットワークシステムとなっていることが一般的である。このようなネットワークシステムの設計を行う場合には機能以外に「コスト」「通信量」「拡張性」などの最適化が行われるが、さらに「アクセス制御」「耐障害性」「脆弱性による影響」などセキュリティ面でも考慮すべき点が多く、小規模なシステムでさえ設計が複雑となる。インターネットを介したさまざまなサービスが社会の基盤として構築されつつある現在、耐障害性や脆弱性による影響といったセキュリティ面での最適化は重要な問題である。しかし現状ではそれらセキュリティ面の設計は設計者の経験に依存しており、方法論の構築や上記最適性への学術的アプローチはされていない。本研究では、現在盛んに研究されている複雑ネットワークのアプローチを用いてネットワークシステムのセキュリティ面の設計を行う。従来の複雑ネットワークのアプローチでは、インターネットにあるルータ間の接続であらわしたトポロジや、AS間の接続で表したトポロジなどにおいて、1つのノードより他のノードに伸びる接続リンク数の分布がべき乗則にしたがっている性質（スケールフリー性）が見つかっている。しかし、ルータやASは単一機能同士の集まりのネットワーク特性を調べたものであり、これらの従来研究は複数の機能を持つ機器が複雑に関連しているようなネットワークシステムに直接適用することはできない。そこで本研究では、複数機能を表現可能なあらたなネットワーク表現モデルを構築し、ネットワークシステムを構成するさまざまな機能に対し機能ごとの特性判定や論理的整合性を1つのネットワークの中に表現可能とした。さらに、モデルにより表現されたさまざまなネットワークシステムが持つ特性を解析した。その結果アクセス制御に関してネットワークシステムの特性への変化を捕らえることに成功し、さらなる発展としてネットワークシステムが持つ共通特性に関する検討を行った。第2節では、本論文のアプローチに基礎となる複雑ネットワークとコンピュータ

* 筑波大学大学院 システム情報工学研究科, 茨城県つくば市天王台1-1-1, Graduate School of Systems and Information Engineering, University of Tsukuba, 1-1-1 ,Tennodai, Tsukuba, Ibaraki, Japan
† 株式会社アイアイジェイ テクノロジー, 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, IIJ Technology, Inc. , 1-105 Kanda Jinbo-cho, Chiyoda-ku, Tokyo, Japan

ネットワークについて述べる。続く第3節のおいて、新たなネットワークの表現モデルを提案する。第4節では提案モデルを利用し、いくつかの典型的ネットワークシステムの例を表現し、それらがもつ特性を解析する。最後に第5節でまとめる。

2 複雑ネットワークとコンピュータネットワーク

近年の研究により、インターネット構造の特性が明らかになってきた。インターネット上のルータのつながりにより構成されるネットワークは、それぞれのルータから出る出線数の分布がべき乗則に従う性質（スケールフリー性）を持つことが明らかになった。同じくAS（Autonomous System）同士のつながりにより構成されるネットワークについても同じく出線数の分布がスケールフリーの性質を持つことがあきらかになった [1],[2]。そういったスケールフリーネットワークなど新たなネットワーク理論のパラダイムを用いた複雑ネットワークの研究が盛んになっており、本研究も複雑ネットワークのアプローチをとることでネットワークシステムの安全性定量化を目指すものである。しかし、ネットワークシステムは複数の機能を持つ機器群から構成されるが、これまでの研究によるコンピュータネットワークの解析は、ルータやASなど同一機能を持つもの同士のつながりを示したネットワークの解析であった。そのためこれまでの研究を直接適用することは困難であるため、次章において複数機能を同時に表現可能なネットワーク表現モデルを提案する。

3 提案ネットワーク表現モデル

ネットワークシステムは、ルータやスイッチングハブ、ファイアウオール、ロードバランサ、Webサーバなど複数の機能を持つ機器の集まりによって構成される。それぞれの機器が持つ機能を、OSI基本参照モデルに照らし合わせてみると、たとえばルータが行うルーティングは、レイヤ3での経路制御を行うものであり、スイッチングハブはレイヤ2での経路制御を行うものであることがわかる。同時に、Webサーバへのアクセスを行うクライアントから見たレイヤ7でのサーバ-クライアント通信では、途中にあるルータやスイッチングハブを意識することはない。ここでレイヤごとに論理的なネットワークが存在することがわかる。[2] では、レイヤ3のルータノード間の論理ネットワークについて解析したものであると言うことができよう。このように、ネットワークシステム内の各機器が提供する機能により、各レイヤごとに論理ネットワークを組むことができる。さらに、各機器は複数のレイヤにノードとして存在しうるため、1つの機器により提供される機能ノード群（この集まりをモジュールと呼ぶことにする）をレイヤ間で接続することで、複数のレイヤの論理ネットワークを繋ぎ、全体として1つの論理ネットワークを構築するモデルを提案する。次小節では、本提案モデルの定義を示し、モデルにより表現されるネットワークシステムの例示を行う。

3.1 用語定義

通信　情報の送受信

通信路　送信者（情報源）から受信者への情報伝達媒体であり、1つ以上のリンクにより構成される。

ノード　通信が行われる際の、送信者・受信者・中継者

レイヤ　同種情報が同種通信路で通信を行う際のノードとリンクの集まり

リンク　2つのノード間をつなぐもの

レイヤ内リンク　同一レイヤにある2つのノードをつなぐリンク

レイヤ間リンク　異なるレイヤにある2つのノードをつなぐリンク

モジュール　1つ以上のレイヤにまたがって機能を提供するもの

中継　当該レイヤの通信路を形成するにあたり、1つ下位のレイヤの通信路形成を決定する処理を行うこと

3.2 レイヤ定義

ここでは本研究で用いるレイヤの定義を行う。

レイヤ1　物理的に接続され、電気的な信号を基にした通信が行われる層

レイヤ2　MACアドレスを基にした通信が行われる層

レイヤ3　IPアドレスを基にした通信が行われる層

レイヤ4　TCP/UDPポート番号を基にした通信が行われる層

レイヤ5　HTTP、SMTP、DNSなどサービスの通信が行われる層

3.3 モジュール定義

ここでは各モジュールの表現を定義する。各モジュールが持つノードは表 1 に示す通りである。ここで、単一モジュールが同一レイヤに複数のノードを持つ場合は、該当レイヤにおいて通信路の始点・終点・中継点となる場合が複数あることを示す。たとえばルータの場合、IP アドレスを 2 つ以上持つことから、レイヤ 3 では 2 つ以上のノードを持つ。また単一モジュールの同一レイヤ内で複数のノードを持つ場合に、該当するレイヤにおいてそのモジュールが経路制御を行う場合、モジュール内での同一レイヤ内リンクが発生する。ルータの場合のレイヤ 3 や、サーキットゲートウェイ型のファイアウオールではレイヤ 4 がそれに当たる。

これら定義により、現存する多くのネットワーク機器が本モデルで表現可能である。詳細なモジュール表現は代表的なネットワーク機能に対し可能であるが、ここでは割愛し、いくつか代表的なモジュールを解説する。

図 1 はいくつかのモジュール表現を示したものであり、左に示したものは Web サータなど単体のサーバを示すモジュールである。物理的な筐体を 1 つもち、1 枚の NIC (MAC アドレス)、1 つの IP アドレス、1 つのポートとサービス、とそれぞれが 1 つのノードで示され、それらをレイヤ間リンクで接続している。中央のものはスイッチングハブである。スイッチングハブ自体は MAC アドレスを持たないためにレイヤ 2 において通信の始点や終点にはならないが、MAC アドレスを元に通信を制御しているため、中継点となる。そのためレイヤ 1 だけでなくレイヤ 2 でもノードを持つモジュールとなっている。右に示したものは IP アドレスを 2 つ持つケースのルータを示したものである。ルータでは、2 つの IP アドレスを用い、レイヤ 3 において経路制御を用いるため、同一モジュール内でレイヤ内リンクが張られている。

また図 2 はサーバ 2 台の間にそれぞれハブとスイッチングハブが接続されている構成を示したモデル図である。

図 3 に示す従来型のネットワークシステムの表現を、本モデルを使う場合、図 4 の用なモデルとして示される。なお、提案モデルの表現にあたり、Java により提案モデル描画ツールを開発した。

レイヤ	1	2	3	4	5
ハブ	1	0	0	0	0
スイッチングハブ	1	1	0	0	0
スイッチ (VLAN 機能)	1	複数	0	0	0
ルータ	1	複数	複数	0	0
サーバ	1	1	1	1	1

表 1: 各モジュールのノード数

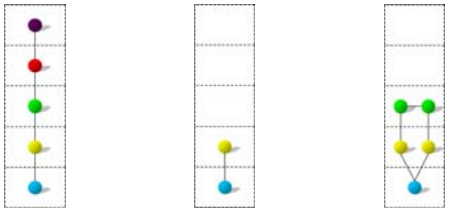

図 1: 各機能のモデル表現 : サーバ、スイッチングハブ、ルータ

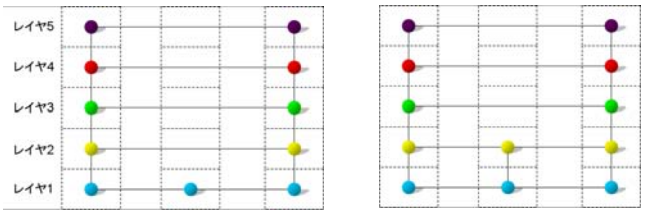

図 2: サーバ 2 台と中継機器の表現

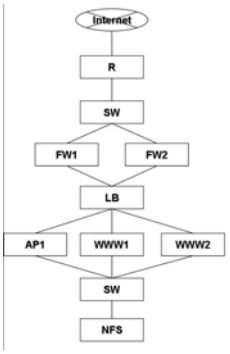

図 3: 従来のシステム設計モデル

次章では、提案モデルにより表現されたネットワークがどういった特性を持つかを典型的なネットワークシステムを利用し解析を行う。

4 ネットワークシステムの解析

本章ではネットワークシステムの例をいくつか用い、そのネットワークの特性を見る。特性を測るにあたり、それぞれのノードが持つリンク数（次数）の分布を見ることとした。解析対象のネットワークシステムは、ファイアウォールなどのセキュリティ境界によりフロントとなる Web サーバ、そしてアプリケーションサーバとデータベースから構成されるような階層構造を持つネットワークシステムとした。この構成はネットワークシステムを構築する場合の典型的な構造であり、この構成は多くのケースで適用されているものである。各レイヤにおけるリンクの意味は、ノード間の通信が実現可能であることを示すものであり、アクセス制御と密接な関係がある。従来のネットワークシステムでは上位レイヤのアクセス

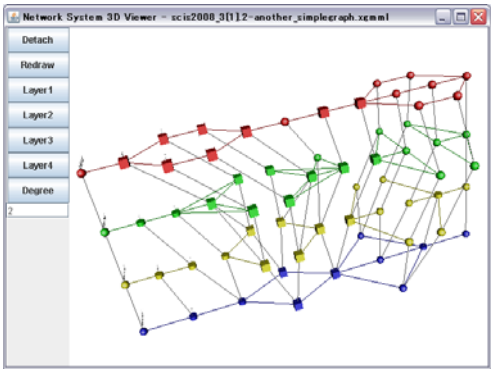

図 4: 提案モデルによる表現

制御については表現されない。そのために看過されてしまう上位レイヤのアクセス制御も解析するために、2 つのケースを用意した。1 つはネットワークシステムが提供するサービスの性質に従い適切に各レイヤでアクセス制御されているケースであり、もう 1 つは上位レイヤでのアクセス制御が不適切なケースである。これら 2 つの比較も行う。

4.1 ケース 1 : Web サーバ 4 台、AP サーバ 2 台、DB1 台

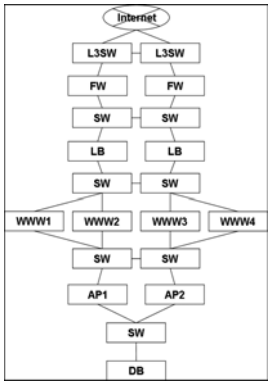

図 5: ケース 1 の従来表現

このケースでは、Web サーバが 4 台、アプリケーションサーバ（AP サーバ）が 2 台、データベース（DB）が 1 台より構成され、それらをネットワークシステムとして構成させるためのロードバランサやファイアウオール、スイッチングハブ、ルータが設置されている（図 5）。提案モデルによるネットワークシステムは図 6 においてアクセス制御が適切に施されているケース、図 7 においてアクセス制御が不適切なケースが示される。ここでの不適切とは、レイヤ 2-4 において同一セグメント内の他ノードへのアクセスが可能である状態を指している。またリンクが持つ次数の分布の適切なアクセス制御ケースと不適切なアクセス制御ケースの比較を図 8 に示す。

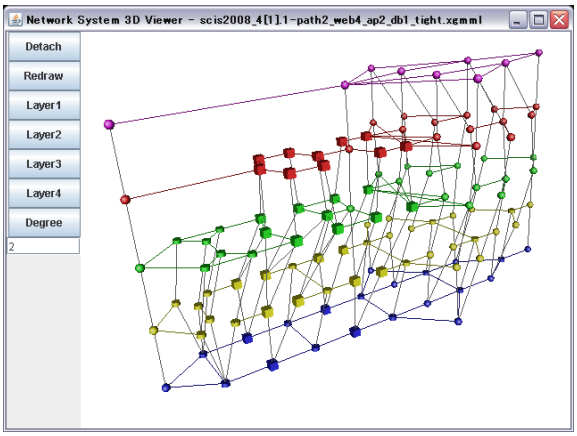

図 6: 提案モデルによるケース 1 表現（アクセス制御あり）

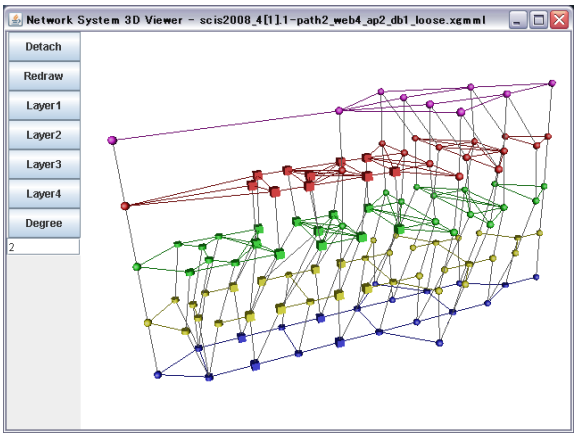

図 7: 提案モデルによるケース 1 表現（アクセス制御なし）

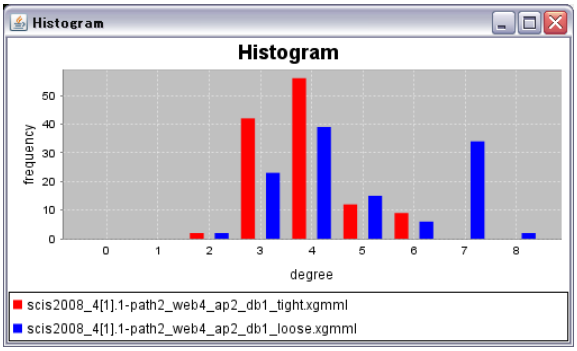

図 8: アクセス制御による次数分布の差:ケース 1

図 8 に示された次数分布を見ると、アクセス制御が適切に行われている場合、その分布はリンク数 4 をピークとしている。提案モデルの特徴上、1 つのノードは同一レイヤ内に少なくとも 1 つのリンクを持ち、レイヤ間リンクを少なくとも 1 つもつことから、最低次数は 2 となっている。リンク数 4 を持つノードの数は 56 であり、これは全体のノード数 114 の 46.3%を占めている。

アクセス制御が不適切なケースにおいても、その次数分布のピークにリンク数 4 が含まれるが、そのノード数は 39 であり、全体ノード数の 32.2%と適切なケースと比較して割合が減少していることがわかる。同時に、適切なケースでは存在しなかったリンク数 7 や 8 のノード数が存在している。特にリンク数 7 はそのノード数が 34 であり、最大のノード数であるリンク数 4 に匹敵する数字となっていることがわかる。これら分布の相違は、アクセス制御が不適切であることによる不必要なリンクが上位レイヤで存在していることを示している。

4.2 ケース 2 : Web サーバ 12 台、AP サーバ 6 台、DB2 台

ケース 1 と同様の階層構造だが、Web サーバ、AP サーバ、DB の台数がそれぞれ多いケースである。その場合のネットワークシステムの従来表現は図 9、そして図 10、図 11 にそれぞれ適切なアクセス制御ケースと不適切なアクセス制御ケースが示される。同様に図 12 においてそれぞれのリンク次数分布を示す。分布では、アクセス制御が適切／不適切なケースの双方においてピークがリンク数 3 となっている。適切なケースでのリンク数 3 ノードの全体に対する割合は 40.5%、不適切ケースでの割合は 22.0%となっている。また、適切なケースではピーク後になだらかであるが多くのリンクを持つノードがごく少数分布している様子がわかる。

不適切なケースでは、適切なケースでは存在しなかったリンク数に分布が存在することはケース 1 と同様であるが、増加が顕著であるリンク数の大きさ（15，19）にはケース 1 との大きな違いがある。これは図 11 を見るとわかるように、同一セグメント内のノードが増加し、それらノード群の間でアクセスが可能となるため、部分的なネットワークでは完全グラフを形成していることが原因である。

4.3 リンク数分布における考察

4.1 節、4.2 節の各ケースにおける適切なアクセス制御と不適切なアクセス制御のリンク分布にはそれぞれ同様の特徴が見られた。アクセス制御が不適切である場合、その分布グラフは特徴的なピークを 1 つとしたものではなくなり、複数の小さなピークを持つグラフとなる。これは先述したように、同一セグメント内のアクセス制御

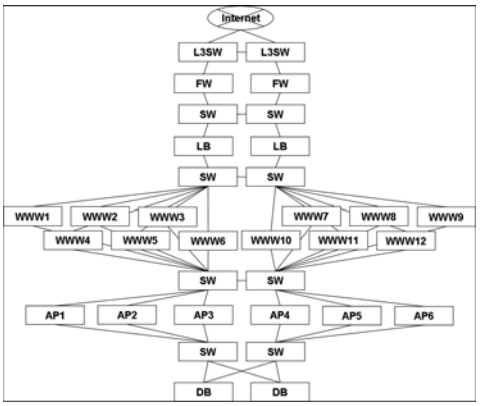

図 9: ケース 2 の従来表現

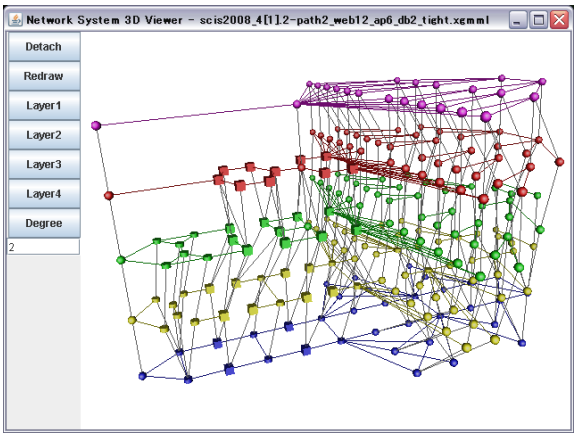

図 10: 提案モデルによるケース 2 表現（アクセス制御あり）

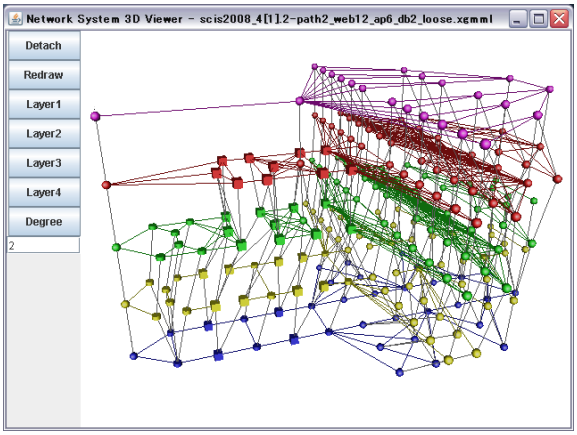

図 11: 提案モデルによるケース 2 表現（アクセス制御なし）

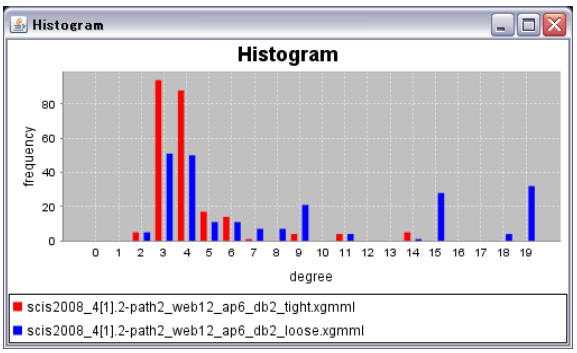

図 12: アクセス制御による次数分布の差:ケース 2

不備により発生する部分的な完全グラフによる影響であり、アクセス制御の不備が提案モデルを用いたリンク数分布により確認することが可能となった。

次に、適切なアクセス制御ケースでの 2 つを比較した場合、特徴的なピークをリンク数 3 または 4 で迎え、そのノード数は全体のノード数と比較して 46.3%、40.5%と高い割合を持っている。さらに、ピークに次いで多いリンク数（4 または 3）とあわせた場合の割合は 81.0%、78.4%と、これら 2 つに多くのノードが含まれていることがわかる。対照的に、多くのリンク数を持つノードは少数であるが、その分布は広範であり、いわゆる Long-Tail となっていることがわかる。これら 2 つの特徴は、その分布にべき乗則の成分が入っていることを感じさせるが、リンク数 2 の次数はべき乗則に沿うものではなく、単純なべきではなく他の要因が入っていることが考えられる。

5　まとめ

複数の機能をそれぞれの機器で担当し、全体で 1 つのサービスを提供するネットワークシステムでは、従来の複雑ネットワーク理論のアプローチでは解析が困難であった。本論文では、機能ごとの特性を失うことなく、各機器を同時に 1 つのネットワーク内に表現することが可能なネットワーク表現モデルを提案した。また提案モデルを用い、典型的なネットワークシステムのいくつかについてその特性を解析した。その結果、リンクの度数分布においてアクセス制御に関して適切なものと、これまでのネットワークシステム設計に用いられてきた表現でおろそかになっていたアクセス制御との間に、論理的ネットワークとしての特性の明確な差異を見つけ、モデル上からアクセス制御の適正さを知ることを可能とした。また、これら結果を用いリンクの度数分布に共通する特性についても検討を行った。今後は、これらネットワークシステムが持つ共通特性についてより詳細な検討を行い、適切なネットワークシステムにおいて共通する特性の抽出を目指す。さらに、抽出特性を用いた定量化により、ネットワークシステムの適切な設計を補助・あるいは自動構築するアルゴリズムを検討する。

参考文献

[1] M. Faloutsos, et. al, “On power-law relationships of the Internet topology,” SIGCOMM ’99, pp.251-262, 1999

[2] R. Govindan, et. al, “Heuristics for Internet map discovery,” INFOCOM 2000, pp.1371-1380, 2000