

マルチレイヤのネットワークトポロジ抽出手法 A Method for Topology Discovery in Multi-Layer Network

日暮 一太[†]
Ichita Higurashi

金岡 晃[†]
Akira Kanaoka

加藤 雅彦[‡]
Masahiko Kato

岡本 栄司[†]
Eiji Okamoto

1. はじめに

インターネットを介して利用される電子商取引などの様々なサービスは、実際にサービスを行う Web サーバ、アプリケーションサーバ、データベースサーバ等のほか、これらの通信を中継するスイッチやルータ、ファイアウォールなどのネットワーク機器から構成されるネットワークシステム (NS) によって提供されている。現状の NS の管理・評価は、システムの構成情報とネットワークの構成情報を管理者独自のドキュメントや表を用いて管理・評価する、人に大きく依存する手法が用いられており、機械的な管理・評価はほとんど行われていない。

近年、これらの問題点を解決する手法としてマルチレイヤネットワークモデルが金岡ら [1, 2] によって提案され、このモデルを利用した NS の脆弱性評価 [3] や可用性評価の手法の研究が行われている。しかしこれらの手法を利用するためには、NS の情報を手作業でデータに変換する必要があり、自動化されることが望ましい。

本論文では、自動化において最も重要となるマルチレイヤでネットワークトポロジを抽出する手法の提案を行う。

2. マルチレイヤネットワークモデル

マルチレイヤネットワークモデルは、NS を構成する機器が持つ種々の機能をそれぞれ異なる通信層 (レイヤ) に分類し、さらにこの「レイヤ」の概念を利用することで機能が異なる様々なネットワーク機器を同一モデル内に表現可能にしたモデルである。このモデルはグラフ理論のグラフ $G = (V, E)$ を拡張したものであり、ノードとリンクの集合で表現される。また 1 つの機器は 1 つのノードで表現されるわけではなく、機能の要素としてノードが各レイヤに存在し、それらのノードとリンクの集合により 1 つの機器 (モジュール) が表現される。

レイヤは図 1 に示す通り、5 つに分類されている。各レイヤには通信の要素となる「ノード」が存在し、各ノードはノード間を結ぶ要素である「リンク」によって結ばれる。ノードは当該レイヤにおいて通信の端点や中継点となるものであり、終端ノードと中継ノードの 2 種類が存在する。ノードは MAC アドレスや IP アドレス、ポート番号、サービスの内容などの情報を持つ。リンクは通信路リンクと依存関係リンクと中継リンクが存在し、それぞれ通信の方向、ノードの依存関係、中継の方向を示す。

異なるレイヤ間でノードがリンクにより接続されたものを「モジュール」と定義する。モジュールはサービス

を提供する「サービスモジュール」、インターネットを表現する「インターネットモジュール」、そしてそれらの中継を行う「中継モジュール」の 3 種に大別される。

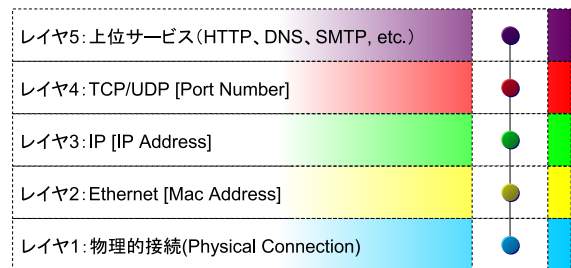


図 1: レイヤの定義

3. 提案手法

本研究では、マルチレイヤネットワークモデルを利用したネットワークトポロジの抽出のため Simple Network Management Protocol (SNMP)[6] と Management Information Base (MIB)[5] を利用する。

まず、ネットワークトポロジを抽出する手法の検討に際し、SNMP を利用した先行研究の調査を行った。Breitbart らの研究 [4] では、ネットワークトポロジを SNMP を利用して抽出する手法を提案しており、この手法は本研究のレイヤ 2・3 のネットワークトポロジの抽出に該当する。

次に、レイヤ 1・4・5 のネットワークトポロジ抽出に必要なノードやリンクの情報が MIB から抽出できるか調査を行った。ノードについては、「サービスモジュールとレイヤ 4 以上の中継モジュールにおけるレイヤ 4 ノードの送信ポートの情報」と「レイヤ 5 ノードのサービスの内容の情報」を MIB から抽出できないことが明らかになった。リンクについては、「ルーティング情報のないモジュール間の通信路リンクの情報」と「サービスモジュールとレイヤ 4 以上の中継モジュール内における一部の依存関係リンクの情報」を MIB から抽出できないことが明らかになった。

本研究では MIB から抽出できない情報を補うため、以下に示すネットワークトポロジ抽出手法を提案する。

1. Breitbart らの手法を利用しレイヤ 2・3 のネットワークトポロジを抽出。
2. サブネットスキャンと MIB の情報から、抽出可能なレイヤ 1・4・5 のノードとリンクの情報を抽出。
3. MIB から抽出できないノードとリンクの情報を推定。

提案手法では、MIB から抽出できないノードとリンクの情報を推定する手法を用いる。ノードに関しては、抽

[†]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

[‡]株式会社インターネットイニシアティブ、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, Internet Initiative Japan Inc., 1-105 Kanda jinbo-cho, Chiyoda-ku, Tokyo, Japan

出対象のモジュールの種類からノードのレイヤを決定し、ノード数を抽出対象のモジュールと隣り合うモジュールのノード数から推定することで抽出対象のモジュールのノードを推定する。リンクに関しては、推定されたノードからノードの組み合わせの数だけリンクを推定する。

提案手法を利用することで抽出対象の NS と異なるノードやリンクが推定されるが、抽出対象の NS に近いネットワークトポロジを抽出できるようになる。

4. 提案手法によるトポロジ抽出シミュレーション

提案手法によるトポロジ抽出手法のシミュレーションを行う。抽出対象の NS は、Web サービスを構成する際に用いられやすい三層構造の NS である (図 2)。

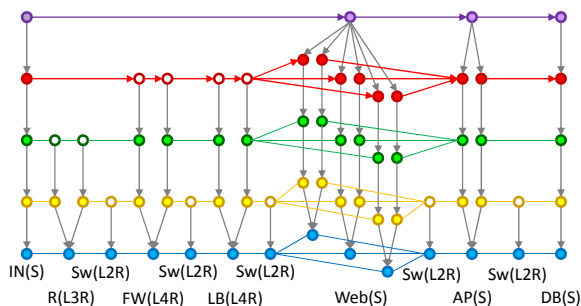


図 2: 抽出対象の NS

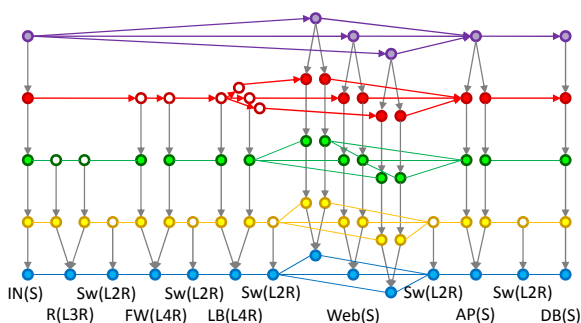


図 3: 提案手法による抽出結果

提案手法を抽出対象の NS (図 2) に適用し、図 3 の結果が得られた。提案手法は MIB から抽出できないノードやリンクを推定するため、抽出結果の NS の一部に冗長なノードやリンクが抽出されるが、抽出対象の NS に近い NS が抽出できることがわかる。

抽出の結果、冗長なノードとリンクが 3 箇所で抽出されているのがわかる。まず、Web サーバとアプリケーションサーバ間のレイヤ 3 通信路リンクが抽出されている。これはルーティング情報が得られないため、サブネット内をスキャンし通信の可能性のあるノードに対して全ての通信路リンクを推定したためである。次に、ロードバランサのモジュール内のレイヤ 4 ノードとレイヤ 4 中継リンクが抽出されている。これはロードバランサの送信ポートの情報を抽出できないため、隣り合う Web サーバのレイヤ 4 ノードからロードバランサのレイヤ 4 ノー

ドを推定したためである。それに伴い、レイヤ 4 中継リンクも推定している。さらに、同一サービスを行う冗長化された Web サーバ群のレイヤ 5 ノードとリンクが複数抽出されている。これは冗長化された Web サーバ群のサービスの内容が同一サービスかどうか判別できていないため、各 Web サーバごとに別々のレイヤ 5 ノードを推定したためである。それに伴い、レイヤ 5 通信路リンクも推定している。

5. まとめ

本論文ではマルチレイヤでネットワークトポロジを抽出する手法の提案を行った。また提案手法を三層構造の NS に適用し、抽出対象の NS に近い NS が抽出できることを示した。

本研究ではネットワークトポロジの抽出の際、MIB から抽出できないノードやリンクをどのように扱うかが問題であった。この問題を解決するため、提案手法では抽出できないノードやリンクを推定する手法を採用した。これにより冗長なノードやリンクも抽出されるが、抽出対象の NS に近い NS のネットワークトポロジを、マルチレイヤで抽出することが可能になった。

今後の課題として、三層構造以外の NS に対してもネットワークトポロジを抽出できるように提案手法の改善を目指す。また提案手法は NS の一部のノードやリンクを推定するため、冗長なノードやリンクが抽出されるが、正確なネットワークトポロジが抽出できるよう目指す。そして、最終的に提案手法の実装を行う。

参考文献

- [1] 金岡晃, 原田敏樹, 加藤雅彦, 勝野恭治, 岡本栄司. 安全なネットワークシステム設計のためのマルチレイヤネットワークモデルの提案と応用. 情報処理学会論文誌, Vol.51. No.9, pp.1726-1735, 2010.
- [2] 金岡晃, 加藤雅彦, 原田敏樹, 岡本栄司. 向きを持つマルチレイヤネットワークモデルの提案とセキュリティへの応用. 情報処理学会研究報告, Vol.2009-CSEC-47 No.3, 2009.
- [3] T. Harada, A. Kanaoka, E. Okamoto and M. Kato. Identifying Potentially-Impacted Area by Vulnerabilities in Networked Systems Using CVSS 2010 10th IEEE/IPSJ International Symposium on Applications and the Internet, pp. 367-370, July 2010.
- [4] Y. Breitbart, M. Garofalakis, B. Jai, C. Martin, R. Rastogi and A. Silberschatz. Topology discovery in heterogeneous IP networks: the NetInventory system *Trans. on Networking*, Vol. 12, No. 3, pp. 401-414, June 2004.
- [5] K. McCloghrie and M. Rose. Management Information Base for Network Management of TCP/IP-based internets:MIB-II RFC1213, March 1991.
- [6] Douglas R. Mauro, Kevin J. Schmidt, 土本康生訳, 福田剛士訳. 入門 SNMP オライリー・ジャパン, 2002.