インターネットの障害の「なぜ」を突き止める

ネットワーク事前知識を活用したSINETログデータの因果解析

NII

どんな研究？

大規模ネットワークの障害復旧や再発防止には、障害の原因を調べることが必要です。そのためには運用ログを始め大量のデータから必要な情報を見つけることが必要であり、多くの人手と時間を要する作業となります。この研究では、ネットワーク障害の原因究明を自動解析によってサポート・効率化する技術の開発に取り組んでいます。

何がわかる？

因果推論の考え方を応用することで、擬似相関が除かれた「より直接的な関係」についての情報のみを抽出することができます。これにより運用者は、従来の相関解析と比較して1/100程度の関係情報を読み取るだけでシステムの振る舞いを把握することができます。また過去の因果との比較を行うことで、障害の予兆分析などへの応用も計画されています。

状況設定

1日に15万行のログデータ (SINET5の場合)
人手では調べきれない -> 自動解析が必要

相関関係 (現在の主流) — 曖昧

因果関係 (この研究)

説明的関係 (将来的目標) — より具体的な自動解析へ

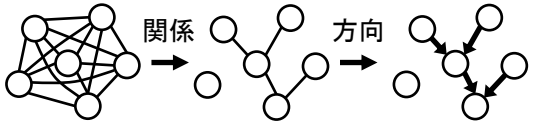
因果解析の特徴

- 利点
  関係を絞り込める
  関係の方向がわかる
- 問題点
  処理時間が大きい ⇨ 事前知識を使って効率的な因果解析

故障 → エラー / 切断

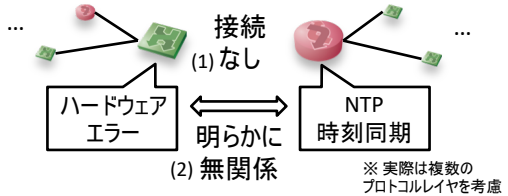
研究内容

PCアルゴリズム



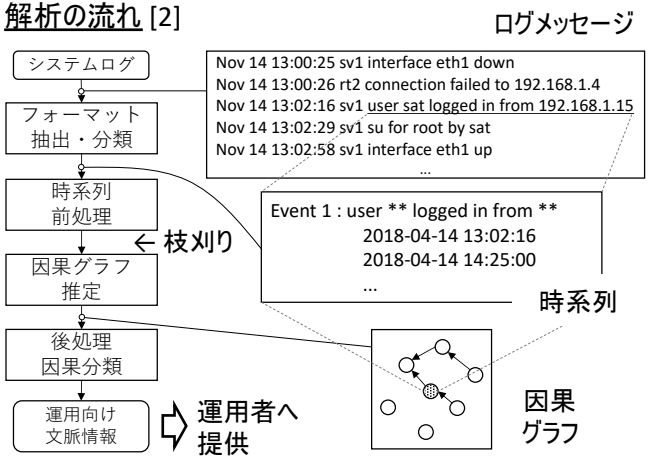
初期状態が完全グラフ -> 組み合わせ爆発、遅い

初期グラフのネットワーク知識による枝刈り [1]



(1) ネットワークトポロジ, (2) プロトコル分類の2つの知識を用いて無関係な候補を枝刈り

解析の流れ [2]



成果

枝刈りにより 74% の処理時間削減
エリア分割(既存手法)より 16% 高速、かつ高精度

[1] S. Kobayashi, et al. “Causal analysis of network logs with layered protocols and topology knowledge”, In Proceedings of IFIP/IEEE CNSM, p.8, 2019
[2] S. Kobayashi, et al. “Mining Causality of Network Events in Log Data”, IEEE Trans. on Network & Service Management, pp.53-67, vol.15, no.1, 2018

(本研究は総務省SCOPE #191603009の委託を受けたものです)