7S-03

ネットワーク情報の監視支援のための自動編纂手法の提案

松村 洋志† 笹井 一人‡ 北形 元‡ 木下 哲男‡

†東北大学大学院情報科学研究科 ‡東北大学電気通信研究所

1 はじめに

ネットワーク管理において，ネットワーク管理者が管理対象のネットワークの状態を把握することは，ネットワークを運用するうえで重要である．ネットワークに関するデータの可視化はネットワーク管理者がネットワークの挙動の理解を補助する方法の一つである．しかしながら，管理対象のネットワークが大規模になるに従い，監視するデータやその可視化方法を適切に選択することは難しくなる．本稿では，ルータやスイッチ，サーバなどの計算機から取得される計測データの状況に応じて，有用なデータやその可視化方法を絞り込み，自動的にグラフ等を提示する，ネットワーク情報の自動編纂手法を提案する．また，試作システムを用いた実験により，提案手法の有効性を示す．

2 関連研究

ネットワークやシステム管理において，様々な可視化技術や方法が提案されている．P3D と呼ばれる 3 次元並列可視化手法では，送信元 IP とポート，宛先 IP とポートの範囲を表す 2 つの平面を線で結んだ，3 次元座標系を用いることで，ネットワーク管理者が DDoS 攻撃やポートスキャンといった攻撃の識別の手助けをする[1]．大規模なダークネットの監視において，アラート状況を視覚的な理解を可能とするために，DAEDAKYS-VIS と呼ばれるリアルタイム 3 次元可視化エンジンが提案されている[2]．また，しばしば発生する誤検出によるアラートに対して，管理者による誤検知の認識を助けることを目的として，侵入検知システム(IDS)の可視化フレームワークが提案されている[3]．

可視化手法はアラートの発生や DDoS 攻撃など，特定の状況やシステムにおいて特に有効である．しかしながら，状況に合わせて適切なデータや手法を選択することはネットワーク管理者の負担となる．

3 ネットワーク情報の自動編纂手法

管理者の負担を軽減し，様々な可視化手法を有効に用いるため，ネットワーク情報の自動編纂手法を提案する．本手法では，ネットワークに流れるトラフィックやサーバにかかる計算機負荷などの計測データから，特定の判断基準を基にデータを選択し，データをグラフ化したものをダッシュボードにまとめて管理者に提示するものである．図 1 に本手法の概要を示す．本稿では本手法の主要な要素である(1) 加工プロセスの適用機能，及び (2) グラフの自動編纂機能について詳述する．

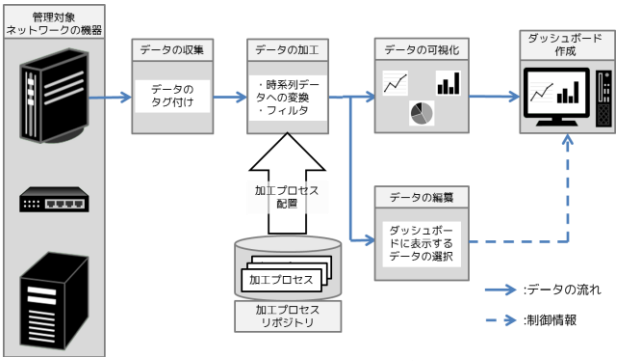

図 1 ネットワーク情報の自動編纂手法の概要

3.1 加工プロセスの適用機能

ネットワーク機器から取得されるデータは，加工プロセスで加工された後可視化プロセスに送られる．ここで各加工プロセスの入出力データの個数やタイプは固定されている．本機能では，新たなデータが利用可能となったとき，それを検出し，加工プロセスリポジトリに登録済みの加工プロセスが必要とする入力データのタイプと照合する．加工プロセスが必要とする入力データの条件を満たす場合には，新たな加工プロセスを配置し，処理を実行する．また，リポジトリに加工プロセスを追加することで，システムを停止させることなく機能を拡張することが可能となる．

3.2 グラフの自動編纂機能

本機能は，加工プロセスから出力される複数数のデータを受け取り，表示するデータの組み合わせとその並び方を決定する．そのため，複数の入力されたデータに対し，数値の変動具合や過去の特徴的なデータとの相関などを算出し，入力データの順位付けを行う．これを編纂プロセスと呼ぶ．順位が高い入力データのグラフをダッシュボードにまとめてユーザに提示する．編纂プロセスは一定時間毎，あるいは入力データからアラートが発生した場合に行われる．本機能により，状況に合わせて適したグラフを管理者に提示することが可能となる．

3.3 設計・実装

図 2 に試作システムの構成を示す．データの加工プロセスや編纂プロセスなどをエージェントによって制御し，エージェントの自律性を活用して動的なプロセス配置を実現する．エージェントの実装には

Automatic information curation technique for network monitoring
Hiroshi Matsumura†, Kazuto Sasai‡, Gen Kitagata‡, Tetsuo Kinoshita‡
†Graduate School of Information Sciences, Tohoku University
‡Research Institute of Electrical Communication, Tohoku University

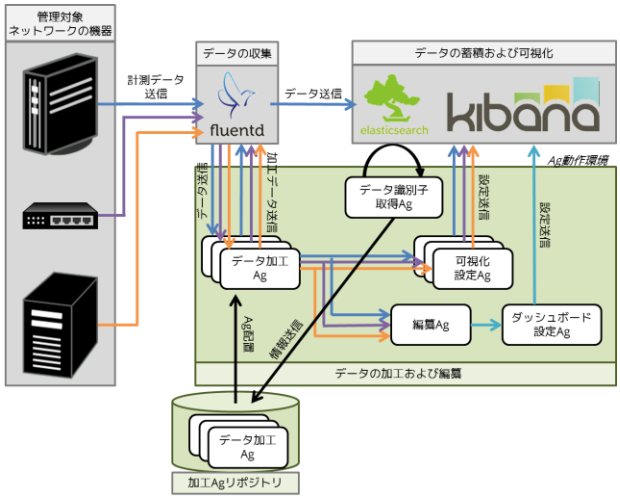

図 2 試作システムの構成

ADIPS/DASH を用いた．データ識別子取得エージェントは，現在蓄積されているデータの識別子の情報を取得し，データ加工エージェントが保管されているリポジトリに送信する．データ加工エージェントは必要な入力データのタイプを知識として持つ．データ識別子取得エージェントから，現在蓄積されているデータの識別子の名称とそのタイプが送られてきたとき，データ加工エージェントは自身が保持する知識と照合して，必要とする入力データのタイプと合致する場合は，エージェント動作環境にデータ加工エージェントを配置する．編纂エージェントは一定時間毎にデータ加工エージェントにデータ送信要求を発行し，編纂に用いるデータを受け取る．可視化設定エージェントは，ダッシュボード設定エージェントが用いるグラフの設定を行う．ダッシュボード設定エージェントは，編纂エージェントから送られる順位付けられたデータを基にグラフを選択し，ダッシュボードの設定を行う．なお，データの収集に fluentd を，データの可視化及びダッシュボードの作成に elasticsearch と kibana を用いた．

4 動作実験

本手法によって，状況に合わせたデータが提示されることを確認するために，以下の設定による動作実験を行った．すなわち，SNMP を用いてネットワークスイッチの各インターフェースで受信した総バイト数 ifInOctets を 30 秒毎に取得する．取得したインターフェースの数は 15 個である．本実験では，計測用のトラフィックとして，ビデオストリーミングや OS のイメージファイルのダウンロードを用いた．また，トラフィックの変動具合から，ダッシュボードに表示するインターフェースの情報を 6 個に絞り込んだ．

図 3 に動作結果を示す．計測用の大量のトラフィックを流したとき，その大量のトラフィックが流れたインターフェースのグラフが選択・提示された．すなわち，大量のトラフィックが発生するという状況に対し，その状況に関連する情報が選択・提示された．以上より，複数の情報から状況に合わせた情報の絞り込みが可能となり，ネットワーク管理者の負担が軽減される．

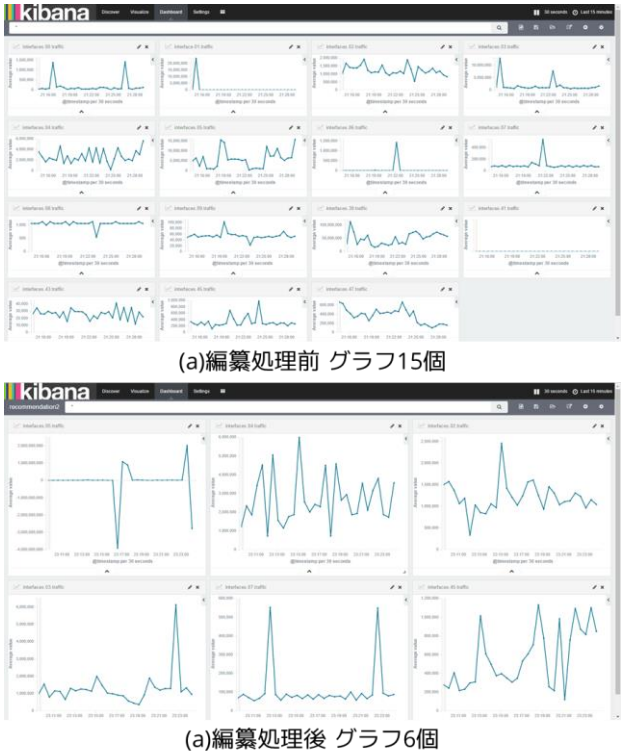

図 3 自動編纂システムの動作実験

5 おわりに

本稿では，管理対象のネットワークに接続された機器類から得られる情報について，有用な情報の候補を絞り込み，ネットワーク管理者に自動的に提示する，ネットワーク情報の自動編纂手法を提案した．また，試作システムの設計・実装及び，動作実験を行った．実験結果より，有用なグラフが選択・提示され，管理者の監視負担が軽減できることを確認した．

謝辞

本研究の一部は，総合科学技術・イノベーション会議の SIP（戦略的イノベーション創造プログラム）「レジリエントな防災・減災機能の強化」及び東北大学電気通信研究所における共同プロジェクト研究によって実施されました．

参考文献

[1] T. Nunnally et al., “P3D: A parallel 3D coordinate visualization for advanced network scans,” in Proc. IEEE ICC, Jun. 2013, pp. 2052–2057.

[2] D. Inoue, M. Eto, K. Suzuki, M. Suzuki, and K. Nakao, “DAEDALUS-VIZ: Novel real-time 3D visualization for darknet monitoring-based alert system,” in Proc. 9th Int. Symp. VizSec, 2012, pp. 72–79.

[3] Y. Zhao, F. Zhou, and X. Fan, “A real-time visualization framework for IDS alerts,” in Proc. 5th Int. Symp. VINCI, 2012, pp. 11–17.