

膨大な数の極小データの効率的な配送基盤技術の研究開発

Enhancement of High-Speed Backbone Network Corresponding to Huge Number of Small-data Produced by Extremely Large Number of M2M Devices

研究代表者

中島 康之 株式会社 KDDI 研究所
Yasuyuki Nakajima, KDDI R&D Laboratories, Inc.

研究分担者

中村 勝一[†] 池永 全志^{††} 堀 良彰^{†††}
Katsuichi Nakamura[†] Takeshi Ikenaga^{††} Yoshiaki Hori^{†††}
[†]九州工業大学 ^{††}ネットワーク応用技術研究所 ^{†††}佐賀大学
[†]Kyushu Institute of Technology ^{††}Network Application Engineering Laboratories, LTD.
^{†††}Saga University

研究期間 平成 25 年度

概要

スマートフォンやセンサー等から集まるビッグデータの利活用による新市場の創出が期待されているが、そのビッグデータの収集に伴うネットワーク中の配送データ（トラフィック）は、広域に常時発生し、ときにはデバイスの異常挙動に伴う予測困難な変動が起きると予想される。本稿では、通信事業者の基幹ネットワークが、これらの特徴に柔軟に対応しながらビッグデータの流通を支えるために不可欠となる 2 つの課題：効率的なデータ配送とデバイス異常挙動検出を可能にする要素技術の研究開発について報告する。

1. まえがき

昨今、スマートフォンやセンサー等から集まる多種多量データ（ビッグデータ）の利活用による新市場の創出が期待されているが、ビッグデータのトラフィックは、そのトラフィックが大規模であるだけでなく、広域で常時発生する、局所的に予測困難な変動が発生するなどの、従来想定していなかった特徴を有している。このため、ネットワークがこれらの特徴に柔軟に対応しながらビッグデータの流通を支えることを可能とする技術が求められる。

具体的には、センサーやスマートフォン等の多様で膨大な数（数千万台か 1 億台）のデバイスが生成する極めて小さなサイズのデータ（以下、「極小データ」とする）が流入する通信事業者の基幹ネットワークにおいて、センサーデータ（位置、温度、加速度等）の生成頻度（1 分間に 1 回程度）に対応した効率的な伝送や、医療向けバイタルデータの低遅延伝送といった重要課題を解決していくことが求められる。これらの課題を解決し、膨大な数の極小データを、信頼性を担保しながら数種類から数十種類のアプリケーションサービス毎の要求配送遅延を考慮して効率よくネットワークに収容する基盤技術が求められる。このような環境において基幹ネットワークは、①中継伝送装置の処理負荷を軽減し、通信品質（通信帯域、遅延制約）及び信頼性の面で柔軟かつスケラビリティを保持して極小データを配送し、かつ②デバイスの異常挙動の検出及び①の通信品質制御に必要なスケラブルな監視ができる配送基盤である必要がある。

2. 研究開発内容及び成果

前章の 2 つの機能（①、②）を解決する配送基盤を実現するために、本研究開発では（1）極小データ配送効率化方式と、（2）デバイス異常挙動検出方式を開発した。以下では、各方式の概要とその成果を述べる。

2.1. 極小データ配送効率化

基幹ネットワークにおいて伝送路（回線）の広帯域化が飛躍的に進展しているが、中継伝送装置（イーサネットスイッチや IP ルータ）におけるデータ転送処理の性能向上はそれに追いついていない。そのため、今後の極小データが急増すると伝送装置のプロセッサに高い負荷が生じて円滑なデータ配送が困難になり、その結果、通信品質に対する多様な要求を満たすことが困難になる恐れがある。

そこで、基幹ネットワークの各拠点にエッジ装置を配備し、このエッジ装置によって基幹ネットワークの入り口に流入する複数の極小データ（以下、単に「パケット」とする）を、まとめてより大きい一つのチャンクパケットに集約する処理（chunking [チャンキング]）と、出口では逆に元のパケットに戻す処理（de-chunk [デチャンキング]）を行う（図 1）。

基幹ネットワークにおけるチャンキング処理の実現では入口装置（インGRESSエッジ装置）において滞留するパケットの配送遅延劣化を防ぐことが重要になる。パケットは、配送遅延に制限を求めるものと求めないものに大別することができる。本研究開発では、配送遅延に制限が伴うパケットの識別・複数の論理回線へのパケット振り分けと、配送遅延制約を満たしつつチャンク効率（チャンクパケットに格納するパケット数）を最大化するチャンクの構成の 2 つの課題に取り組んだ。以下の節ではそれぞれの方式について述べる。

なお本研究開発では、基幹ネットワークおよびトラフィックに以下の前提を置いた。

- エッジ装置の任意の組には一つ以上（多くの場合は

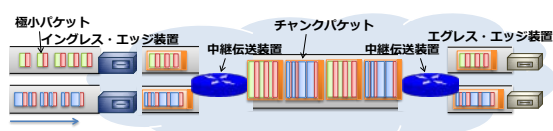


図 1 チャンクを用いる基幹ネットワークの構成

複数)の論理回線が構成される。

- 基幹ネットワークを通り抜けるパケットには配送遅延の制約があり、パケット内のバイト列から配送遅延の制約を導出できる。
- エッジ装置は論理回線ごとにチャンクパケット配送時間の統計量を取得できる
- 上記から、エッジ装置はパケットチャンク・デチャンクにかけられる時間を割り出すことができ、イングレスエッジ装置はこの時間を基にパケットごとの許容待機時間を設定できる。

パケットが基幹ネットワークを通過する際の配送遅延制約を O 、パケットが論理回線の通過にかかる時間を D 、イングレスエッジ装置にてパケットの識別にかかる処理時間を X とすると、パケットのチャンク処理にかけられる時間 W は、

$$W = O - (D + X) \quad (1)$$

と算出できる。なおここでは、デチャンク処理にかかる時間はパケットが基幹ネットワークの通過にかかる時間を含める。以下の各節では、このパケットのチャンク処理にかけられる時間を許容待機時間と呼ぶ。

また、論理回線ごとにチャンクパケット配送時間の統計量用を取得することについては、イングレス・エグレスエッジ装置間で回線利用率を共有するトラヒックエンジニアリングの機構を応用し、配送遅延も共有するものとする。

2.1.1. 配送パケットの識別

パケット識別では、スマートフォンのアプリケーションならびに M2M デバイス制御に普及が拡大している WebSocket など、パケットのペイロード部 (非ヘッダー部) のバイト・文字列 (キー) を抽出するテキスト解析がカギになる。そのためには、パケットのペイロード (アプリケーションデータ) 精査 (DPI: Deep Packet Inspection) を用いながらもパケット転送速度を劣化させないことが重要になる。本研究開発では、テキスト解析処理を行いつつ、高速にパケット転送を可能にするパケット識別方式に取り組んだ。

具体的なテキスト解析の手順は次の通りとした。

1. イングレスエッジ装置は入力するパケットの転送先エグレスエッジ装置を IP フローテーブルにより決定する。ここでは IP フローをネットワーク・トランスポート層のアドレス・プロトコル ID・ポート番号で識別されるパケット列とする。もし IP フローテーブルに当該パケットの IP フローエントリがない場合には、2 へ処理を進める。IP フローエントリがある場合には 5 へ処理を進める。
2. パケットの転送先エグレスエッジ装置を IP ルーティングテーブルにより解決し、3 へ処理を進める。IP ルーティングテーブルは通常の経路制御プロトコルによって管理する。
3. パケットに DPI 処理を施して許容待機遅延を求め、4 へ処理を進める。エッジ装置は、DPI 検索キー (バイト列) と配送遅延制約の組で構成される許容待機遅延テーブルを予め持ち、パケット種別からその配送遅延制約を取得できるものとする。
4. パケットの、チャンク後に配送する論理回線を選択し、当該パケットの IP フロー ID・配送遅延制約・決定した論理回線を IP フローエントリとして IP フローテーブルへ登録し、5 へ処理を進める。論理回線の決定方法は 2.1.2 節に述べる。
5. 配送遅延制約ならびに本ステップまでにかかった時

間 (X) から許容待機時間 (W) を求め、パケットを前処理で決定した論理回線の配送用バッファ (キュー) へ格納する。パケットのチャンクの方法は 2.1.3 節に述べる。

2.1.2. 配送論理回線の選択

前節処理 4 の論理回線の選択では、イングレス・エグレスエッジ装置の間の論理回線の帯域の違いを考慮する。低帯域の論理回線から送り出されるチャンクパケットは、その間隔が大きくなる。そのため、許容待機遅延が小さいパケットは広帯域論理回線へ割り当てる方針とする。

基幹ネットワークへ入力するパケットは多数の IP フローを構成し、その許容待機遅延の分布はさまざまであり、パケット転送の各瞬間における前後に許容待機遅延の分布も変化する。そのため、許容待機遅延に基づく論理回線に割り当てを静的に (単純に) 行っている論理回線が持つ割り当て帯域を十分に消費できず、基幹ネットワークのパケット収容を低下させてしまう。本研究開発では、許容待機遅延の分布に応じて論理回線の割り当てる方法を考案したので、その具体的な手法は次に述べる。

まず準備として、論理回線に平均許容待機時間の指標を設ける。この値はこの論理回線に格納されるパケットの許容待機時間の平均値で、チャンクパケットの送出時に直近の複数のチャンクパケットを構成するパケットから求める。なお、簡易的な平均時間の算出に移動平均を用いてもよい。

イングレスエッジ装置の起動時はパケットの格納がないため、暫定的に平均許容待機時間を設定する。この時、広帯域な論理回線ほど小さい値を設定する。また、イングレスエッジ装置の動作中に論理回線を追加する場合には、既存論理回線の帯域と比較して間に入る既存論理回線の平均許容待機時間の間の値 (中間値など) を設定する。

論理回線の選択にはこの平均許容待機時間とパケットが持つ許容待機遅延を比較する。帯域がより広い論理回線はより小さい許容待機遅延を持つパケットを格納するように制御を行う。具体的には、パケットの許容待機時間が論理回線の平均許容待機時間よりも小さくなる論理回線の内、バッファの空きが最も大きい論理回線を選択する。

このようにパケットの振り分けを行うと時間の経過とともに許容論理回線の平均許容待機時間が小さくなる。そこで、すべての論理回線は定期的に平均許容待機時間を微増させる (たとえば、10 ミリ秒ごとに 10% 増加させるなど)。また、二つの論理回線の平均許容待機時間が接近し過ぎる場合には、広帯域 (小さい平均許容待機時間) の論理回線の平均許容待機時間を微減させる。

2.1.3. 通信品質を考慮したパケットチャンク

チャンクパケットを構成するタイミング (パケットのチャンクおよび送出のタイミング) は、次のいずれかの条件が成立した時とする。

- A) 待機可能タイマーが 0 になった場合。この時、バッファの先頭から、チャンクパケットのパケットサイズに達するまでのパケットを一つのチャンクパケットに構成する。待機可能タイマーは、パケットをバッファに格納するたびにその許容待機時間と比較し、パケットの許容待機時間の方が小さければ、その値を新たな待機可能タイマーとする。
- B) 格納中のパケット長の合計が最大チャンクパケット長に達した場合。

なお、バッファからチャンクパケットを構成した後の待機

可能タイマーには、残りのパケットの許容待機時間の最小値を設定し、次のチャンク処理に用いる。

論理回線において一定数のパケットを蓄積してチャンクする際に、アプリケーション（IP フロー）が要求する配送遅延制約が侵される要因として、基幹ネットワーク内の回線容量が不足する場合と、回線容量が十分に確保されていても中継伝送装置のパケット転送処理性能が不足する場合があります。前者は、配送トラヒックを基幹ネットワーク（空き回線）に分散させることで解決でき、トラヒックエンジニアリングで採られるトラヒック分散方式によって論理回線への割り当てトラヒック量を調整する。

後者に関しては、チャンクパケットの集約効率が低下していることが原因で、パケットレートが高まっていることを意味する。また、広帯域な論理回線ほど、許容待機時間が小さいパケットが集まるため、このような問題が発生しやすい。そのため、広帯域な論理回線のチャンクパケットの集約効率を高める（一つのチャンクパケットを構成するパケット数を増大させる）ことで、中継伝送装置に求めるパケット転送処理の負荷を軽減する。

具体的な解決策としては、パケットが配送論理回線を通過する時間と流量（基幹ネットワークへの入力パケットレート）のフィードバック情報を、エグレスエッジ装置から得て、それに応じてパケットの許容待機時間を調整する方式とした。

パケットが、配送論理回線を通過する時間のフィードバック情報を定期的にて得て、パケットの許容待機時間を調整するには、前回までのフィードバック情報を用いる。具体的には前回（ $n-1$ ）と前々回（ $n-2$ ）の入力パケットレートを P_{n-1} 、 P_{n-2} とすると、チャンク可能時間 W_n^* を以下の計算式によって再設定する。

$$W_n^* = W_n + \min[(P_{n-1} - P_{n-2}) / P_{n-1}, 0] \quad (2)$$

この際設定は、十分に大きな許容待機時間をもつパケットが低速論理回線に割り当たり難くする、つまりは十分な許容待機時間をもつパケットであって高速論理回線へ割り当て、高速論理回線におけるチャンクパケットのサイズを大きくしやすくする効果をもたらす。

シミュレーションによって、チャンク可能時間の調整の効果を評価した結果が、エラー！参照元が見つかりません。である。基幹ネットワークに流入するパケットレートが増加するに従って、チャンクを行わない場合のパケットロスが増加するが、集約を行うことでパケットロスが抑えられることが確認できる。さらに、チャンク可能時間を調整するほうが、調整しない（固定の）場合よりもよりパケットロスを抑えられることが確認できる。これらの結果より、チャンク可能時間を調整することによってパケットロスの割合を抑えられることを確認した。

なお、本シミュレーション実験は、NS-3 (Network Simulator-3) を用いた。2 台のイングレスエッジ装置が 40 バイトの極小パケットをチャンクして、パケット転送性能に 5 Mpps の制約がある中継伝送装置へ送り出す状況をシミュレートした。与えたトラヒックは図 2 の各プロットの平均レートを持つ指数分布のトラヒック変動を与えた。

2.2. デバイス異常挙動検出方式

ビッグデータ利活用による新市場の創出を促進するためには、ビッグデータ用ネットワーク配送基盤は高信頼でなければならない。そのためには、異常な挙動をするデバイスを速やかに検出し、対処可能な管理機構が必要である。本研究開発では、定常的に数分もしくは数十分に 1 回程

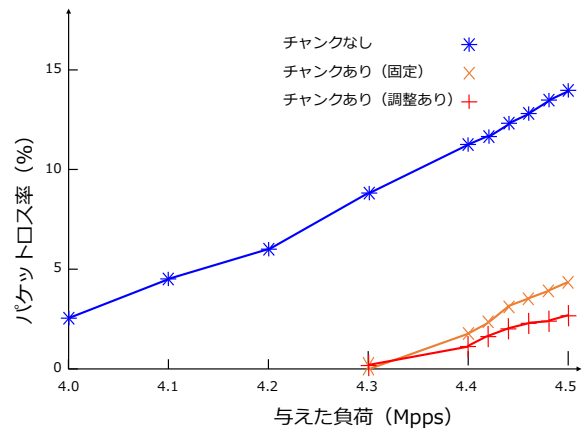


図 2 パケットチャンク時の集約の効果調整

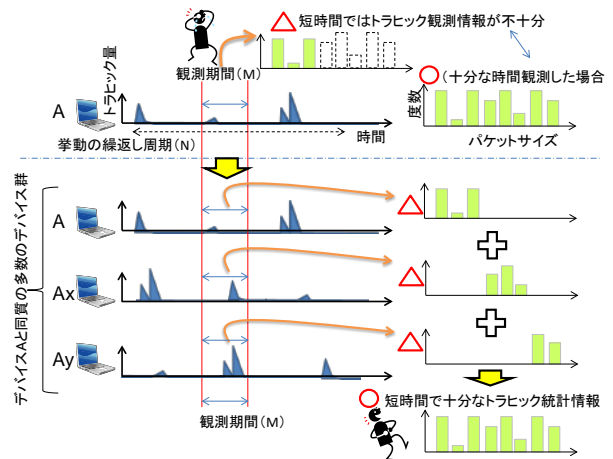


図 3 複数デバイスによる通信異常検出の概要

度の頻度でサーバにセンシングデータを送信するデバイスが、マルウェアに感染し、他デバイスへの攻撃もしくは感染活動に関与し始める事象を考え、このような事象を速やかに検知するためのデータ蓄積方式を開発した。本研究開発で定義するデバイスの異常挙動とは、デバイスが送受信する通信において、それ以前（定常状態）に比べて通信レート・パターンが変化することとした。数分から数十分の間隔で通信するデバイスの定常状態の変化を一つひとつのデバイスの監視によって捉えるには長時間を要する。そこで、同様の通信パターンを持つデバイスを多数収容することが予想される基幹ネットワークにおいて通信パターンの変化を速やか（数分程度）に検出する。

このような手法によるデバイスの通信異常検出の手順は、通信の定常状態モデルの生成と、そのモデルを用いる異常検出の 2 つのステップに大別される。以下の節でこれらを説明する。

2.2.1. デバイス通信の定常状態モデルの生成

一般に異常検出を行う場合、異常を定義しておきそれに合致する観測情報をもって異常を検知する手法と、正常を定義しておきそれと合致しない観測情報をもって異常と検知する方法の 2 種に大別される。

ネットワーク侵入検知システムやマルウェア対策ソフトウェアにおける攻撃やマルウェアのシグニチャは前者に相当し、あらかじめ異常を直接表すシグニチャを定義しておく必要がある。本研究では、後者のアプローチで臨こととし、トラヒックの定常モデル作成において特性情報を保存できるヒストグラム方式に着目しながら、多数

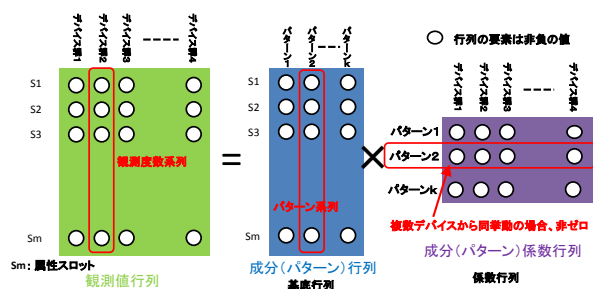


図 4 非負値行列因子分解 (NMF) を利用した
トラフィックパターン

の始点から送出されるトラフィックからヒストグラムを使用した定常モデルを作成する手法とした。

本研究開発では、多数のセンサーから発せられるネットワークトラフィックに非負値行列因子分解 (NMF: Non-Negative Matrix Factorization) を適用し、定常パターンを導出する手法を提案する。本手法は、同じ挙動を含有する始点のクラスタリングと挙動パターンと導出を一度の解析で行う。今手法は、単一のアプリケーショントラフィックパターンに従うトラフィックを送出する M2M デバイス、スマートフォンの自動通信を抽出しや特徴がある。

図 4 に NMF を利用したトラフィックパターンの抽出について示す。ある期間における観測によって得られたトラフィックから、観測値行列を作成する。始点 IP アドレス等によって識別されるデバイス群の各々からのパケットについて、それぞれを各列として、パケットが有するある属性に関してそれが出現する度数を抽出し観測値行列 (左の行列) を作成する。

観測値行列の各行は、パケットが有する属性についての値を、値に応じて m 個のカテゴリに分類したものを配置する。カテゴリ S_1, \dots, S_m がそれである。そうした場合、各列はデバイス群から送出される度数系列を表す。観測値行列 V に対して、非負値因子行列分解を行うと、成分 (パターン) 行列 W (基底行列ともいう成分 (パターン) 係数行列 H (係数行列ともいう) に分解できる。成分 (パターン) 行列 W の列は解析によって抽出される複数のパターンであり、行は観測値行列と同じカテゴリ S_1, \dots, S_m に相当する。つまり、例えばパターン 2 に相当する第 2 列はそれぞれ属性値が m 個のカテゴリに分けられた後の各々の度数に相当する。成分 (パターン) 係数行列は、各々のデバイス群が送出するトラフィックがどのパターンがどの程度重なりあったものかを示す係数行列となる。各行はいずれかのパターンを表し、各列はデバイス群を表す。あるデバイス群から送出されるトラフィックが抽出されたいずれかのパターン成分を含む場合、該当する要素は正の数となる。この NMF を用いた解析により、観測された度数情報から、内在するパターンの抽出と、各始点であるデバイス群との関係を一度に導出することができる。

観測されるネットワークの適用へあたっては、観測値行列をどのように構成するか問題となる。つまり、成分 (パターン) 行列が実際のアプリケーションに相当するパターンを生成できるような属性値を選択する必要がある。本研究開発では以下の 4 つのメトリックを通信の特徴量として用いた。なお、これらはどれかを選ぶものではなく併用することができる。

- パケット長

- TCP/UDP の終点ポート番号
- パケット・バイトレート
- パケット間隔

NMF 行列分解の演算時間が通信の異常挙動の検出への応用において妥当かどうか検証するための評価実験を行った。python ライブラリ (動作 PC : Intel Core i7-3960X) による NMF 実装を用いて、 $1,000 \times 1,000$ 列の場合を、表 2 に $1,000 \times 10,000$ 行列の場合の計算時間を示す。NMF は成分 (パターン) の数を指定する必要があるため、100, 200, 300, 400 パターンの場合について計測した。本実験では要素を乱数により生成していることから、その値は最悪値に近いものと考えられる。real, user, sys はそれぞれ Linux の time コマンドの出力である。観測行列の列数つまりデバイス群の数は 10,000 のでも数十秒で計算できることから、実装技術の工夫により、数十分の 1 から数百分の一の計算時間での計算が見込める。

表 1 $1,000 \times 1,000$ 列の行列分解時間

パターン数	read [s]	user [s]	sys [s]
100	4.3	4.0	0.2
200	6.6	6.1	0.2
300	8.7	8.3	0.2
400	11.2	10.7	0.3

表 2 $1,000 \times 10,000$ 行列

パターン数	read [s]	user [s]	sys [s]
100	40.9	39.1	1.5
200	64.3	58.2	1.8
300	85.7	77.4	2.0
400	106.5	98.4	2.2

さらに、GPU ライブラリを使用した NMF を用いたトラフィック解析と異常検知システムを開発した。提案する NMF を用いたトラフィック解析手法を異常検知システムにおける定常パターン導出として用いる場合、NMF の処理速度が問題となる。NMF における計算コストは行列計算を繰返し実施する必要があるため、この部分の高速化のために GPU を用いた実装により処理速度の短縮を実現する。GPU の利用により、先に述べた PyMF を利用した実装と比較し、2 桁程度の速度向上が得られた。それにより、始点グループ数 1000 (行数) およびカテゴリ数 48 (列) の場合において、5 秒程度の計算時間で定常パターン導出を実現した。3 万集約グループ数の場合において、5 分以内でのモデル作成を実現した。

2.2.2. デバイスの異常検出のためのトラフィック監視

前節の定常状態モデルの生成を踏まえて、異常検出のためのトラフィック監視機能を有する配送管理サーバの方式検討、設計、検証用プロトタイプシステムとしての実装を行った。本システムの概要を図 5 に示す。トラフィック収集は、監視対象ネットワークの出入り口に位置するエッジ装置を通過する全ての IP パケットを対象に IP フロー単位に収集する。トラフィック統計情報は前節の観測値行列を構成するトラフィック属性別のヒストグラムである。

トラフィック統計情報の生成は、定期的に観測されるパケットサイズのリストを IP フロー毎に収集する。エッジ装

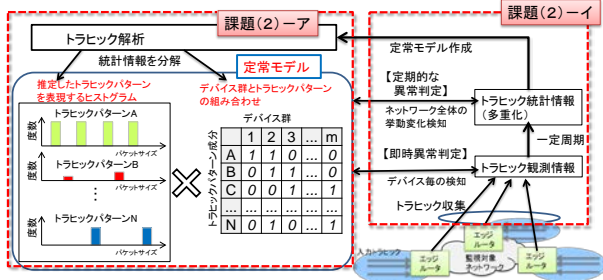


図 5 配送管理サーバの概要

置～サーバ間の収集データ量を抑制する観点で、パケット毎の到着タイムスタンプは取得せず、求める時間精度で収集周期を設定してトラヒック情報を収集することとした。この周期は NMF を実施できる時間精度とし、収集周期を 5 秒程度とした。

通信異常の検出は、定常モデル生成後、収集するトラヒック統計情報と既に生成済みの定常モデルを比較し、該当フローの生成元センサデバイスが属するデバイス群に対応するトラヒックパターン成分に存在しない挙動(外れ値)を検知する。定常モデルと一致しない収集トラヒックのパターン成分 (IP フロー) が場合には、IP アドレス毎に管理するペナルティスコアについてフローの送信元 IP アドレスについてそのペナルティスコアを 1 点ずつ加算する。同時に、パケットレート、バイトレートについても、対応するグループの観測閾値を読み出し、この閾値を超えていた場合はペナルティスコアを 1 点ずつ加算する。このペナルティスコアには 2 つの検出閾値 (Warning と Error) を設けておき、それぞれの閾値を超えた場合に異常挙動検知デバイスとして異常を発報する。

3. 今後の研究開発成果の展開及び波及効果創出への取り組み

本研究開発の成果の実用化は、キャリア事業の研究開発を担う KDD I 研究所、先駆的なネットワーキング技術の研究を進める九州工業大学・佐賀大学、先端ネットワーク技術を駆使した新しいネットワークサービスを標ぼうするネットワーク応用技術研究所の共同連携により、迅速な実現を目指し、事業化に向けた実用化戦略の立案を行った。戦略立案の取り組みとして、研究会およびプレスリリース、さらには、有識者を交えた会議にて事業化の可能性や方向性を協議した。次に、新サービスの創出を目的として、市場調査を実施し、サービスイメージの検討を行った。

基幹ネットワークのチャンク技術については、モバイル通信サービスが、第一種通信事業者に留まることなく、多数の Mobile Virtual Network Operator (MVNO) によって提供されると考え、第一種通信事業者が仮想ネットワークを構築し、MVNO の要望に応じてネットワークリソースならびにネットワーク機能を提供する形態への適用が有力と考えられる。パケットチャンク機能が、ハードウェアとして実装する場合と、ソフトウェア機能として実装する場合の 2 つの方向性で実用化イメージを作成した。ハードウェアとして実装する場合には、流通する通信データが所属する仮想ネットワークを区別して、コア網へ入力する通信データを集約してコア網のパケット転送負荷を抑制することができる。またソフトウェア機能として実装する場合には、エッジルータ機能 (ソフトウェア) が配備される仮想ネットワークごとに、その仮想ネットワークを流通する通信データを区別して、パケット集約を行う。

また、サービスイメージの作成と並行して、標準化活動

にも注力し、ITU-T SG13 に、将来網のネットワーク仮想化要件に関する Y. 3012 の勧告化に貢献して、その成果をもとに、アーキテクチャの標準化作業に着手する見通しとなった。また、ETSI NFV ISG においても、ネットワーク機能の仮想化における信頼性要件を入力 (8 件) した。ITU-T SG13、ETSI NFV ISG に加え、3GPP へのネットワーク要件の入力を行うことで、本研究開発が想定するサービスや仮想化技術を用いた実現のイメージを通信サービス事業者・ベンダに認知させることが予想され、それにより、ビッグデータ配送基盤の高速基幹網の構築だけでなく、通信サービス事業者による仮想化技術を活用した、多様かつ迅速なサービス提供の形態や環境の整備について加速化されることが期待される。

デバイスの異常挙動検出機構については、低コストのデバイスアプリケーションの開発の検討を、医療分野の企業、エネルギー分野の企業と継続して実施する。具体的には、本研究課題で確立される極小データの配送品質および挙動の監視・管理技術を基に、医療関係センサネットワーク、医療関連センサネットワーク、さらには、通信キャリアネットワークと連携した新規サービス等を対象としてローカライズしたデータ配送品質の監視や異常検出を行う管理システムの開発を目指し、セキュアな M2M デバイス通信サービスを事業化する取組みを継続して実施する。さらに、デバイスの異常挙動検知に関して、迅速にマルウェアを検出する技術を地域クラウド事業者と協議しながら、M2M デバイス向けセキュリティサービスを検討し事業化を行うことを検討する。

4. むすび

新市場の創出が期待されている多種多量データ (ビッグデータ) の利活用には、スマートフォンやセンサー等からの円滑なデータ収集技術が鍵となる。ビッグデータのトラヒックは、そのトラヒックが大規模であるだけでなく、広域で常時発生する、局所的に予測困難な変動が発生するなどの、従来想定していなかった特徴を有している。このため、ネットワークがこれらの特徴に柔軟に対応しながらビッグデータの流通を支えることを可能とする技術として、ビッグデータの効率的な配送を可能にするチャンク方式と、セキュアなデータ収集を可能にするデバイス通信異常検出方式を開発した。

本研究開発の取り組みでは、方式検討、シミュレーション実験ならびにプロトタイプ実装による効果検証を行い、その有効性を明らかにした。さらに研究開発成果の成果展開ならびに波及効果送の取り組みとして、成果技術を活用するサービスイメージの検討、そのための市場調査、標準化活動、本研究開発終了後の実用化戦略の立案を行った。

【査読付発表論文リスト】

- [1] 塚本他, "QoS-aware Packet Chunking Schemes for M2M Cloud Services", Proceedings of the First International Workshop on Device Centric Cloud (DC2-2014) (2014 年 5 月)
- [2] 梅木他, "On Architecture for QoS-Aware Packet Aggregation", Proceedings of the 38th Annual International Computers, Software & Applications Conference (COMPSAC2014) (2014 年 6 月)
- [3] 永田他, "Behavioral Anomaly Detection System on Network Application Traffic from Many Sensors"

Proceedings of the 38th Annual International Computers, Software & Applications Conference (COMPSAC2014) (2014年6月)

【出願特許リスト】

- [1] 北辻佳憲、特願 2013-170875 「許容待機時間を考慮して集約パケットの収容効率を高める通信装置、プログラム及び方法」、日本、2013年8月
- [2] 梅木智光、特願 2013-169942 「通信遅延とパケット集約効率を考慮したマルチパスパケット収容方式」、2013年8月、日本、2013年8月
- [3] 中村勝一、小寺康平、永田晃、「低頻度な通信データを考慮した異常検知方式及びプログラム」、日本、2014年6月

【国際標準提案・獲得リスト】

- [1] ITU-T/SG1、ジュネーブ会合、“Proposed modification of Y.FNvirtreq on requirements”、2013年6月、2013年6月、2013年6月
- [2] ETSI/NFV ISG、ボン会合、“NFV RELA Architecture and Procedures for Supporting Resiliency”、2013年10月、2013年10月、2013年10月
- [3] ETSI/NFV ISG、ソフィアアンチポリス会合、“Proposal of Resiliency Flows (Section 13)”、2014年1月22日、2014年1月22日、2014年1月22日

【報道掲載リスト】

- [1] “極小データ配送基盤技術を確立”、電波新聞、2014年3月24日