

災害 ID 付与方式による災害時のネットワーク優先配送 ～OpenFlow による実装と評価～

小川康一^{†1} 吉浦紀晃^{†2}

災害時には、人々のネットワーク利用の殺到によって、災害地への重要な通信が優先的にネットワークに転送されにくくなる問題点がある。本論文では、災害地の通信を優先するといった、災害時のネットワークの対応策について提案する。対応策の具体的な方法は、ネットワークを流れるパケット内の IP アドレス情報から災害地の通信であると判断できた場合には、その通信に「災害 ID」を付与することである。ネットワーク機器はこの災害 ID を確認し、災害 ID が付いている場合には優先的に配送を行う。また、災害地からの通信、または災害地への通信を優先制御するために、通信が災害地からのものであるかを把握する必要がある。そのためには、IP アドレスと位置情報の対応関係の把握が必要となる。この対応関係の把握のためにデータベースを利用する。この対応策を具体的に実現する方法の 1 つとして OpenFlow を用いる。

Network Priority Control during Disasters and effectiveness Evaluation

Kohichi Ogawa^{†1} Noriaki Yoshiura^{†2}

In disasters, important communication for disaster area should be given priority, but it is not given priority because many people use network to obtain information on disasters. This paper proposes a countermeasure against the network trouble during disasters. The countermeasure attaches IDs to communications from or to the disaster areas. The IDs are used to give priority communications from or to the disaster areas; network equipment identifies communications for disaster areas by IDs. This paper calls the IDs "Disaster IDs". Network equipment preferentially processes the communications with the IDs. Network equipment needs to identify communications that are related with disaster areas in order to control the priority of communication from or to the disaster areas. Identification of communications for disaster areas needs to obtain location information by IP Addresses of disaster areas. This paper uses OpenFlow to implement the proposed countermeasure.

1. はじめに

2011 年 3 月に発生した東日本大震災では、首都圏において交通機関が麻痺し、多くの人々が帰宅困難となった。帰宅困難となった人々は、地震の被害状況や安否確認の情報を求めた。昨今ではスマートフォンの普及によりインターネットの利用が一般化し、災害時の安否確認の手段としてインターネットの利用が増加すると予想される。結果、ネットワークにおいて急激なトラフィック増の状態が発生し、災害地への通信帯域が確保不可能な状況が想定される。東日本大震災のような広域災害においては、的確な情報収集や収集した情報の有効活用によって、被害の状態に応じた迅速な救助や支援活動への貢献が求められている[1]。災害時には、通常の通信よりも災害地の通信について一定の品質を確保する必要がある。総務省の「大規模災害等緊急事態における通信確保の在り方に関する検討会」で議論された内容がガイドライン[2]として反映されている。災害時に緊急性の高い通話の疎通確保のための帯域制御の正当性や必要性が定義されている。

このような背景を元に、災害時の通信品質を改善するため、2つの対応策を提案する。1つ目は、災害時においてはネットワークを持つ組織は協調し、「災害地への通信を優先する」という取り決めを行うことである。2つ目は、組織間での取り決めに従いネットワーク機器の設定を、災害地の通信を識別しその通信を優先するように変更することである。

しかし、ネットワーク上のどの通信が災害地に関連するものかを判断する方法は確立されていない。そこで、ネットワークを流れるパケット内の IP アドレスから災害地と判断できた場合には、その通信に目印となる「災害 ID」を付与する。パケットに災害 ID を付与することにより、ネットワーク機器は災害 ID に基づき配送の優先度を制御する。

災害地からの通信または災害地への通信を優先制御するためには、通信が災害地に関連するかを把握する必要がある。そのためには、IP アドレスと位置情報の対応関係を収集し、データベース化して利用する。

対応策を具体的に実現する方法の 1 つとして、本論文では OpenFlow[3]を用いる。OpenFlow とは、Software-Defined Networking (以下、SDN) の実現技術である。SDN はソフトウェアでネットワークの動作や振る舞いをプログラミング可能にし、ネットワーク管理の柔軟性を向上させる考え

^{†1} 産業技術大学院大学産業技術研究科
Industrial Technology Graduate Course Master Program, Advanced Institute of Industrial Technology

^{†2} 埼玉大学大学院理工学研究科
Graduate School of Science and Engineering, Saitama University

方である。OpenFlow コントローラの機能拡張によって災害地に関連する通信を判別する。

2. 災害時におけるネットワークの問題点

本章では、災害時におけるネットワークの問題点を述べる。

2.1 重要な通信の品質確保の方法

災害時には、情報発信を担う通信基盤が重要である。インターネットは、安否確認や人命救助などに重要な役割を果たす。しかし、ネットワークの利用が増え、大量のトラフィックが流れるとネットワークが飽和状態となり輻輳が発生する。その結果、災害地に関連する通信の優先転送が不可能となりうる。これはインターネットの性質上、どの通信も等しく扱われることに起因している。よって、重要な通信であっても、何の手当もなければ優先されることはなく、災害時には問題となる。

2.2 管理者の被災の可能性とネットワーク制御の困難さ

2011年の東日本大震災では、電気やガソリンなどのエネルギー確保の問題が人々の生活や活動に大きな影響を与えた。交通機関の麻痺も震災の影響のひとつであり、震災時には、管理者が情報システムを操作する場所にたどり着けない状況が想定される。システム管理者も被災する可能性があるため、情報システムの操作が不可能な状況が想定される。よって、災害時には平時と同じ情報システムの管理運用が可能とは限らない。対策として、遠隔操作や状況に応じて自動的に設定が切り替わる仕組みが必要となる。

3. 災害時のネットワークの対応策

本章では、前章で述べた災害時におけるネットワークの問題点を踏まえた対応策を検討する。

3.1 災害地の通信品質確保のための合意形成

前章で述べた問題点の解決には、災害地向けの情報を優先的にインターネット上で配送する対策が有効である。そのためには、インターネットを構成する各ネットワークが協調し優先配送をする必要がある。

ただし、協調動作のためには、組織間において災害時に有効化するネットワーク設定について予め合意しなければならない。合意があって初めて、各ネットワーク機器が、災害時には取り決めた設定情報に基づいて運用される。しかし、取り決めた設定を実装するには次の問題がある。

- (1) 災害の発生場所を事前に特定することは不可能
- (2) 各災害地に応じた動的なネットワークの設定変更が困難
- (3) 災害地の特定のために IP アドレスと位置情報の対応関係が必要

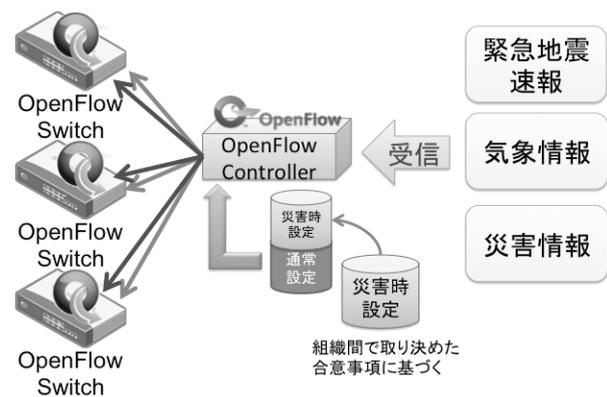


図1 OpenFlow Controller の機能拡張による
気象・災害情報等の収集

Fig.1 By extension of OpenFlow Controller Collection of meteorological and disaster information.

3.2 災害情報によるネットワーク機器の自動設定

3.1の問題点を解決するために、管理者が対応不可能であっても、災害発生の情報に応じて、ネットワーク機器の設定を自動的に変更する仕組みが必要である。しかし、現状ではネットワーク機器の機能での実現は困難で、ネットワーク機器に合わせたツール類の開発が必要となる。このようなツールは特定の情報基盤に特化されるため、汎用性がない。そこで、本論文では OpenFlow によって提案手法を実装することにした。OpenFlow は、従来のネットワーク機器の筐体内で一体となっていた2つの機能、パケット転送機能と制御機能を分離する考え方である。OpenFlow では、制御機能は OpenFlow コントローラが担当し、OpenFlow スイッチは OpenFlow コントローラの指示を受けてパケット転送を行う。OpenFlow コントローラと OpenFlow スイッチ間の通信は、OpenFlow プロトコル[4]で行われる。

OpenFlow は、ネットワークの振る舞いをソフトウェアにより設定可能にしている。この性質により、災害情報等の情報を OpenFlow コントローラで受信し、ネットワーク機器の制御が可能となる。

現在では、緊急地震速報など災害情報がインターネット等で提供されている。提案手法では、災害情報を OpenFlow コントローラが受信した場合、ネットワーク機器設定を災害時の設定に自動的に切り替える。その結果、図1にあるように災害情報に応じたネットワークの制御が可能となる。例えば、緊急地震速報で震度6以上の震災情報を得た場合、被害地域への通信を優先させる、ことが可能となる。

4. 提案手法

本章では災害時の具体的な対応策として、OpenFlow コントローラに拡張実装する機能について述べる。

4.1 災害地の通信品質確保のための合意形成

災害時の設定情報は、取り決めに合意した組織の OpenFlow コントローラに予め保持する。災害時の設定情報は、災害地の通信を優先的に配送する処理を OpenFlow スイッチに行わせる。組織間の取り決めに基づく設定情報により、災害時に重要な情報を優先して配送することが可能となる。OpenFlow コントローラは、通常の設定とは別に災害時の設定情報を持つこととなる。

4.2 災害情報の収集方法

OpenFlow コントローラを拡張し、災害情報を収集する機能を実装する。災害情報とは緊急地震速報や気象情報である。このように、OpenFlow コントローラによる災害情報や気象情報の収集機能によって、管理を受け持つネットワークの災害時における被災の可能性などの状況を把握できる。本手法によりネットワーク機器を 4.1 に述べた災害時の設定へ切り替えるタイミングも把握できる。

4.3 IP アドレスと位置情報の対応関係の把握

現在のネットワークの品質制御 (Quality of Service, 以下 QoS) 技術では、送信先・送信元の IP アドレスに基づき優先制御が行われる。本論文では、通信の送信元や送信先の IP アドレスから通信の優先度を決定する方法を用いる。

このとき、OpenFlow コントローラや OpenFlow 対応ネットワーク機器では、収集可能な情報は IP アドレスのみであり、送信先や送信元の IP アドレスがどのような場所であるかの判断が困難である。つまり、災害地の通信であるかを判別できない。そこで、IP アドレスと位置情報 (緯度/経度) の対応が必要となる。この対応関係を収集し、データベース化して OpenFlow コントローラと連携させる。本論文ではこのデータベースを「IP アドレスマッピングデータベース」と呼ぶ。あわせて、データベース内のテーブルを「マッピングテーブル」と呼ぶ。

5. 災害時の通信品質確保の具体的手法

本章では前章の提案手法に基づき、具体的な通信の品質確保の方法について述べる。

5.1 災害地への重要通信の判別手法

論文[5]で、専用の ID として「災害 ID」の付与によって災害地からの通信を区別する方法を提案した。「災害地からの通信には災害 ID を付与する」というルールを定義したフローエントリをフローテーブルに追加する。本設定により、OpenFlow スイッチは災害 ID の読み取りが可能となる。結果、災害地向けの通信を区別し、優先制御や帯域確保を実現する。

5.2 災害 ID の割り当て方法

図 2 に災害時における通信制御の方法を示す。

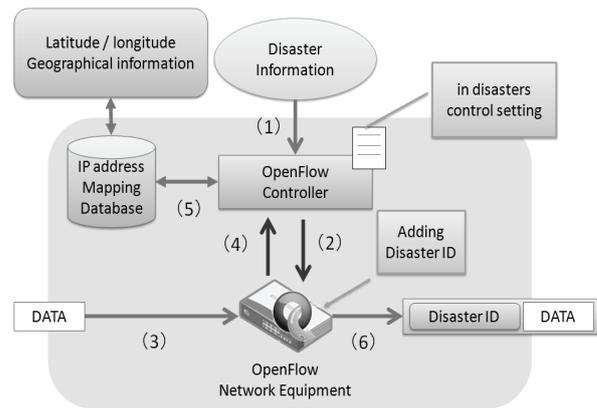


図 2 災害 ID の割り当て方法

Fig.2 Method for allocating disaster ID.

(1) OpenFlow コントローラは災害発生の情報を受け取り、予め保持している災害時用の設定情報を読み込む。

(2) OpenFlow コントローラは OpenFlow スイッチに対して、災害 ID に基づく優先制御を実施する設定をスイッチに行う。

(3) パケットが新しく入ってきたとき、災害 ID が付与されているかのチェックを行う。付与されていない場合には次の手順 (4) に進む。災害 ID が付与されている場合には、OpenFlow スイッチで優先的に転送され、以降の手順は行われない。

(4) OpenFlow スイッチは、送信元もしくは送信先の IP アドレスを確認し、OpenFlow コントローラに問い合わせる。

(5) OpenFlow コントローラは IP アドレスマッピングデータベースで IP アドレスを照合し、当該通信の位置情報を確認する。

(6) 災害地に対応する IP アドレスであれば、災害 ID を付与しデータを送信する。災害地の IP アドレスでない場合には、災害 ID と別の ID を付与して、他のスイッチが同じ処理を行うことを防ぐ。

6. 位置情報を用いた災害地向け通信の判断

本章では、位置情報を用いた災害地向け通信の判断方法について述べる。

6.1 IP アドレスと位置情報の対応

送信先と送信元として優先すべき場所の位置情報の正確な把握は、現在の TCP/IP プロトコルの機能では難しい。そのため、IP アドレスと位置情報を対応させる IP アドレスマッピングデータベースが必要となる。

東日本大震災のような広範囲に渡る災害では、地域によって状況が異なる可能性があり、柔軟な対応のためには細かな地域の情報が重要となる。

6.2 データベースを用いた地域の特定

IP アドレスと位置情報を結びつける方法に「GeoIP」が

ある[6]. GeoIPはMaxmind社が無償・有償で提供しており、IPアドレスによって位置情報を国レベル、場合によっては都市レベルまでの特定が可能である。しかし、本研究では災害地の特定には詳細の地域情報を把握する必要がある。

当初、本研究でもIPアドレスと位置情報を対応づける方法としてGeoIPを想定していた。しかし、GeoIPでは誤った情報も多く、場所の特定も国や都市のレベルでの把握にとどまることもあり、IPアドレスから正確な位置情報を把握できない。そこで、OpenFlowコントローラを拡張し、IPアドレスと位置情報の対応関係を把握する機能を持つ、IPアドレスマッピングデータベースの作成を検討した。本データベースの利用によって、IPアドレスと位置情報とを対応づけることを実現する。データベースの情報は、取り決めを行った組織間で共有する。



Disaster ID	IP Address	Latitude	Longitude	country	State	City	Street
5	133.38.0.0/16	35.865439	139.608474	Japan	Saitama	Saitama	Simookubo

図3 IPアドレスマッピングデータベースのデータ構造
 Fig.3 Data structure of IP address mapping database.

図3はIPアドレスマッピングデータベースのデータ構造の概略である。IPアドレスに対応する緯度、経度を予め登録しておくことで位置状況を把握する。これらの位置情報は、OpenFlowコントローラとともに予め設定しておくものである。しかし、OpenFlowコントローラで利用するIPアドレスブロックの位置情報をOpenFlowコントローラの設定箇所として、同一の位置として登録すると、実際のIPアドレスを利用している正確な位置情報の把握は困難である。例えば、地域のIX(Internet eXchange)やISP(Internet Service Provider)などでは、利用者はその地域から離れた場所からネットワークに接続する可能性がある。一例としては、VPNで離れた地点と接続している場合である。そこで、OpenFlowコントローラには、IPアドレスマッピングデータベースを通じて管理するIPアドレスブロックの細部の割当状況を把握する機能が必要である。例えば、IPアドレスと郵便番号で把握可能な範囲の位置情報を把握する方法である。本手法では、市区町村までの把握が可能である。この情報は各OpenFlowコントローラが保持し、災害時以外にも組織間で共有する。

7. データベースを用いた実際の通信

本章では、IPアドレスマッピングデータベースを用いた実際の動作について述べる。

7.1 データベースへの情報登録手順

本提案手法におけるIPアドレスマッピングデータベー

スへの情報登録手順は以下の通りである。

- (1) OpenFlowコントローラのIPアドレスと位置情報をIPアドレスマッピングデータベースに登録する。
- (2) OpenFlowスイッチとOpenFlowコントローラを環境に合わせ初期設定を行う
- (3) OpenFlowコントローラに災害時用の設定を行う
- (4) IPアドレスマッピングデータベースにDHCPによるIP割当時の認証に用いる郵便番号を紐づけるコードと対応させたテーブルの設定を行う。
- (5) IPアドレスマッピングデータベースとOpenFlowコントローラの協調動作により、個別のIPアドレスの収集を可能にする。そして、IP割当時に紐づくIDの情報と合わせて郵便番号コードを参照し、マッピングテーブルにデータ挿入する。

7.2 データベースを用いた実際の通信

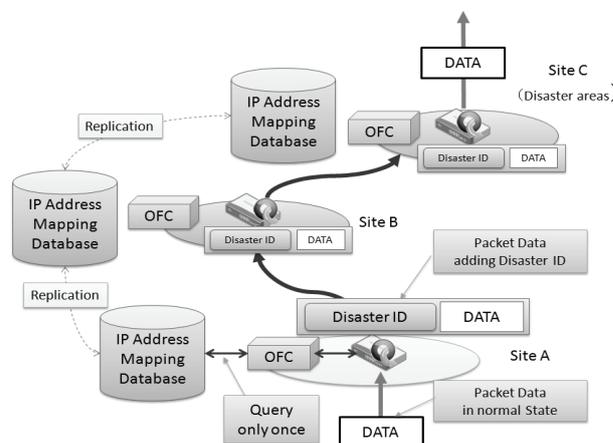


図4 災害地への通信イメージ
 Fig.4 Communications to disaster areas.

災害地への通信イメージは図4の通りである。通常、各ネットワークのOpenFlowコントローラから各ネットワークにあるIPアドレスマッピングデータベースへの災害地のIPアドレスであるかどうかの問い合わせは、一度限りである。以降、災害IDの付与された通信はOpenFlow対応のネットワーク機器ではコントローラに問い合わせを行うことなく、優先して転送されるため、高速な転送が可能となる。データベースの内容については、組織間で相互にデータを交換し、各組織が持つ情報を統合する。

8. システムの実装

本章では前章までに述べた手法に基づく具体的なシステムの実装について述べる。

8.1 システム基本設計

本論文で述べる手法を実際に稼働するシステムとして実現するには、OpenFlowコントローラ、OpenFlowスイッチ

が必要となる。合わせて、IP アドレスマッピングデータベースを実現するデータベースや災害情報を自律的に取得する機能などが必要である。システムの機能概要を図5に示す。OpenFlow コントローラでは、災害 ID の確認と付与を行う。この災害 ID の埋め込み箇所には ToS フィールドを用いる。災害 ID がないパケットの場合には、災害地か非災害地かを IP アドレスマッピングデータベースにより判断し、災害地であった場合には ToS フィールドに高い数値を、非災害地であった場合には ToS フィールドに低い数値を割り当てる。そして、以後災害 ID が付与済みのパケットは、フローテーブルに従い転送される。

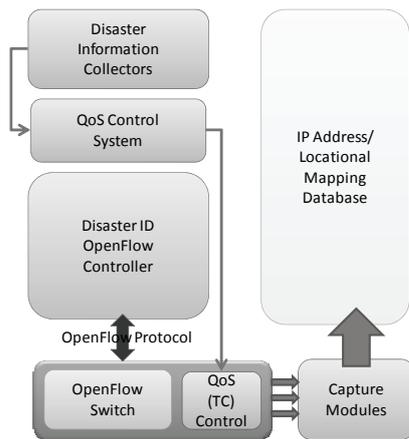


図5 システム構成の概略図
 Fig.8 Schematic diagram of the system structure.

8.2 システム構成

OpenFlow コントローラは、フレームワークの一つである Trema[7]を用いて開発した。今回は開発の容易さやソースコードの可読性を重視し、Ruby で記述している。

OpenFlow スイッチは、オープンソースで提供されている Open vSwitch[8]を用いる。現状、Open vSwitch はソフトウェアそのものに QoS を実現する機能はなく、Linux の OS の機能である Traffic Control (TC) を設定することで対応する。この設定は、Open vSwitch を制御するためのコマンドで設定可能であるが、実際の管理運用には不便であるため、Web インターフェイスを開発した。

8.3 今後の実装予定

本システムで、現在実装を進めている機能は地震検知の部分である。本提案手法では災害が発生した非常時と通常時の運用時の設定を、災害情報を収集することによって OpenFlow コントローラの設定を切り替える。現在、切替部分については現在開発中である。

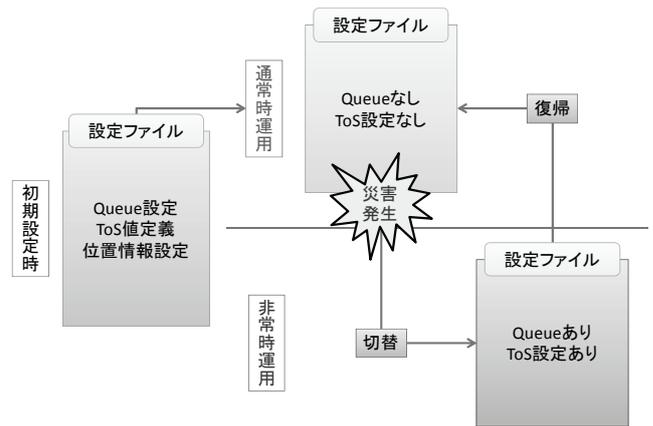


図6 状況に応じた OpenFlow コントローラの設定切替
 Fig.6. Configuration of OpenFlow controller depending on the situation

9. 提案手法の有効性評価

本章では、前章で述べたシステムを用い、災害 ID 付与方式についての有効性の評価と実験結果について述べる。

9.1 評価実験の目的

8 章で実装したシステムを用い、性能について実験を通して評価する。以下2点の項目を実施した。

(1)災害 ID 付与方式と災害 ID 付与方式を用いない場合の比較

Ping を用い、2つの設定で処理にかかる時間に違いがあるかを確認する。

(2)災害 ID 付与方式における有効性評価とパフォーマンス測定

OpenFlow スイッチを用いた場合に、災害 ID が付与された側のクライアントで優先的な帯域を選択が可能で、制御が自動で正しく行われるかを確認する。今回は、250M/bps, 250M/bps, 100M/bps の3つの帯域を用意し設定した。

9.2 評価実験構成

図7は今回実施した実験環境の概略を示したものである。

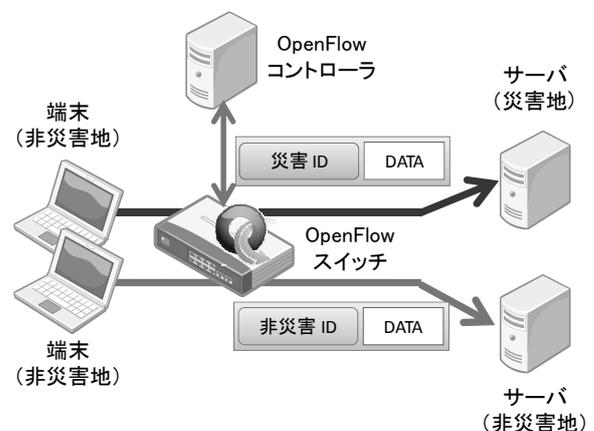


図7 評価実験の概略図

Fig.7. Schematic diagram of the evaluation experiment.

2 台のサーバと 2 台の端末を用意し、OpenFlow スイッチを通して接続し、OpenFlow コントローラが正しく災害 ID に従い優先制御が機能するかを確認する。サーバと端末はそれぞれ災害地と非災害地に見立てて 1 台ずつ用意する。

OpenFlow スイッチは、Linux サーバに Open vSwitch をインストールし、ネットワークカードを 2 枚用意し、実験用のスイッチとした。また、IP アドレスから災害地かの判断を行うための IP アドレスマッピングデータベースとして MySQL を用いた。実験に用いたスイッチは iperf[9]による評価の結果、約 945M/sec のスループットを得た。

9.3 評価実験結果

(1) 実験結果

Open vSwitch を単純な Layer2 スイッチとして実装した場合、端末間の転送が 1.8ms であるのに対し、災害 ID 付与方式では 1.9~2.45ms 程度であった。遅延の原因は、SQL への問い合わせが負荷になっているものと考えられる。

(2) 実験結果

iperf を用い、様々な条件下にある送信元 IP アドレスから、送信元が災害地である場合と、非災害地である場合について 3 回ずつパケットの転送を実施した (表 1)。「DB 有」とは IP アドレスマッピングデータベースにレコードがある場合、「DB 無」はテーブルにレコードがない場合でもシステムが問題なく動作するかを確認するために実施した。

表 1 災害 ID 付与方式のパフォーマンス測定結果

Table 1 Performance measurement results of Disaster ID assignment method.

送信元	受信先	
	災害地 (Mbits/sec)	非災害地 (Mbits/sec)
192.168.1.3 (非災害地, DB有)	247	97.4
	247	97.4
	247	97.4
192.168.1.4 (災害地, DB有)	247	247
	247	248
	248	249
192.168.1.33 (非災害地, DB無)	249	249
	247	98.3
	248	98.3

送信元 IP アドレスが非災害地である場合には、災害地向けの通信は低帯域が利用され、送信 IP アドレスまたは受信先 IP アドレスが災害地である場合には広帯域が利用されることが確認できた。非災害地からの問い合わせで 1 回の計測で期待値が得られなかった理由としては、フローテーブルの削除に時間がかかったものと推測している。

10. 課題

10.1 位置情報の精度と必要範囲の粒度の調整

本研究の提案手法では IP アドレスと位置情報の対応関係が重要である。データベースによる対応では、データベースの破損や、問い合わせの速度がデータベースソフトウェアに依存する問題がある。データの更新滞った場合、災害地の IP アドレス情報が古い状態であるため、災害地への通信が優先的に転送されない可能性がある。今後、今回実装した IP アドレスマッピングデータベースの評価を継続し、性能向上を検討したい。

10.2 優先転送する情報の信憑性

東日本大震災においては、Twitter をはじめとするソーシャルメディアの情報が注目された[10]。しかし、ソーシャルメディアは自由に情報を投稿可能なため、デマなどの誤った情報が確認されることなく、かつ広範囲にわたって流布する悪影響をもたらした[11]。やりとりされる情報が信頼できる情報かどうかを判断する指標が別途必要になる。誤ってデマの情報を優先転送しない仕組みが必要である。

11. 今後に向けて

本論文では、災害時におけるネットワークの問題点を指摘するとともに、対応策として組織間での合意形成とネットワークの優先制御による手法を述べた。また、OpenFlow によるシステム実装を行い、評価実験により本提案手法の有効性を確認した。

参考文献

- 1) “大震災からの教訓と ICT の役割”, 平成 24 年版情報通信白書”, pp.255-265, 総務省.
- 2) “大規模災害等緊急事態における通信確保の在り方について”, http://www.soumu.go.jp/main_content/000141084.pdf, 総務省大規模災害等緊急事態における通信確保の在り方に関する検討会, 2011 年 11 月 27 日.
- 3) Nick McKnown et al., “OpenFlow: enabling innovation in campus networks,” ACM SIGCOMM Computer Communication Review, vol.38, issue 2, pp.69-74, April 2008.
- 4) OpenFlow Switch Specification 1.0.0 (Dec. 31, 2009), Open Network Foundation, <https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.0.0.pdf>
- 5) 小川 康一, 吉浦 紀晃, “OpenFlow を用いた災害時の通信品質の向上 — 位置情報に基づく災害 ID 付与方式の提案 —,” 信学技報, vol.113, no.94, IA2013-5, pp.25-30, 2013 年 6 月.
- 6) GeoIP, <http://dev.maxmind.com/geoip/>
- 7) Trema, <http://trema.github.io/trema/>
- 8) Open vSwitch, <http://openvswitch.org/>
- 9) iperf, <http://sourceforge.net/projects/iperf/>
- 10) 三浦麻子, “東日本大震災とオンラインコミュニケーションの社会心理学: そのときツイッターでは何が起こったか”, 電子情報通信学会誌, 2012-03-01, No.95-3, pp219-223.
- 11) 梅島彩奈, 宮部真衣, 荒牧英治, 灘本明代, “災害時 Twitter におけるデマとデマ訂正 RT の傾向”, 情報処理学会研究報告, データベースシステム研究会, Vol.2011-DBS-152, No.4, pp.1-6, 2011.