

モバイルコア網における ユーザ挙動に着目した障害検知方式

新保 宏之 小森田 賢史 小頭 秀行 長谷川 輝之 横田 英俊

株式会社 KDDI 研究所

近年、モバイルデータ通信の普及に伴い、各種サービスのより安定した提供が求められている。そのため、網運用においては、網の不具合がサービスに及ぼす影響を迅速かつ正確に把握することが重要である。しかし、パケット転送量をベースとした一般的なトラフィック監視では、サービスレベルの障害検知を行うことは困難である。そこで、本稿ではユーザ挙動に着目した障害検知方式を提案する。提案方式では、サービス利用時におけるモバイルコア網特有のシグナリングに基づき、ユーザの再接続挙動を抽出することで、サービスレベルの障害検知を実現する。さらに、提案方式の実装及び商用モバイルデータ網を利用した評価を行い、その有効性について示す。

A Detection Scheme for Service Abnormality based on User Actions in Mobile Core Network

Hiroyuki SHINBO Satoshi KOMORITA Hideyuki KOTO

Teruyuki HASEGAWA Hidetoshi YOKOTA

KDDI R&D Laboratories Inc.

As the spread of mobile data communications, operators are required to offer service stability. In network operations, it is important to precisely and quickly know the effects on services when network problems occur. However, traffic monitoring, such as measuring the amount of transferred packets, is not sufficient to detect service abnormalities. In this paper, we propose a detection scheme for service abnormalities based on users attempting to reconnect. They are measured by the specific signaling in mobile core networks. We implement and evaluate the proposed scheme in a commercial mobile network. With the results of the evaluation, we prove the usefulness of the proposed scheme.

1 はじめに

近年、性能向上が顕著なモバイルデータ通信を用いて、Webアクセス、電子メール、音楽配信、企業網アクセスによる業務管理 [1] などの様々なサービスが提供されている。これらのサービスの普及に伴い、モバイルデータ通信網での障害発生による企業や社会活動への影響が見られるようになった。

各種サービスのより安定した提供のためには、モバイルデータ通信網における障害検知が重要である。これには、網の不具合発生の検知だけでなく、不具合がサービスに及ぼす影響を迅速かつ正確に把握することも含まれる。具体的には、ある通信ノードでの不具合発生が、Webアクセスには影響し、企業網アクセスには影響しないというような状況の把握である。様々なサービスが提供されるモバイルデータ通信網では、サービスレベルの影響把握を幅広く行う必要がある。

一方、パケット転送量をベースとした一般的なトラフィック監視 (例: [2]) は網や通信ノードの不具合検知を目的としており、サービスの提供状況を把握するものではない。そのため、障害発生時にサービスレベルでその影響を把握することは困難である。

これに対し、筆者らは、cdma2000 HRPD (High Rate Packet Data) システム [3] を対象としたモバイルコア網でのユーザ挙動に着目した障害検知方式を提案する。提案方式は、ユーザが所望のサービスに接続できない場合に再接続しようとする挙動に基づき、サービスレベルでの障害検知を実現する。再接続挙動は、サービス利用時に発生するモバイルコア網特有のシグナリングを常時計測することで抽出する。

本稿の構成は次のとおりである。2 節でモバイルデータ網の概要、モバイルコア網特有のシグナリングを述べ、3 節で従来の監視方式と問題点を示す。4 節で提案方式の詳細について述

べ、5 節で提案方式の実装及び商用モバイルデータ網を利用した評価を示す。6 節でまとめを述べる。

2 cdma2000 HRPD システムにおけるモバイルコア網

2.1 モバイルデータ網概要

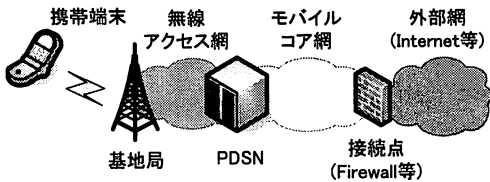
cdma2000 HRPDシステムでのモバイルデータ網は携帯端末に対する課金と認証機能を提供するPDSN (Packet Data Serving Node) を境界として、「モバイルコア網」と「無線アクセス網」とから構成される (図 1) [4]。

- モバイルコア網

PDSN から外部網 (Internet 等) への接続点 (Firewall 等) に至る網である。

- 無線アクセス網

基地局と PDSN を接続する網である。



PDSN: Packet Data Serving Node

図 1 モバイルデータ網

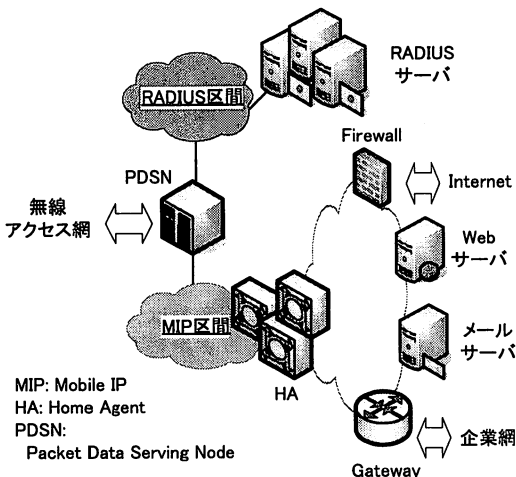
モバイルコア網をさらに詳細化した構成を図 2 に示す。

- RADIUS [5] 区間

モバイルデータ通信に関する課金や認証情報を管理するRADIUSサーバが存在する。

- MIP (Mobile IP [6]) 区間

MIP区間には、HA (Home Agent) が設置され



MIP: Mobile IP
HA: Home Agent
PDSN:
Packet Data Serving Node

図 2 モバイルコア網

る。PDSNはユーザの通信開始時にHAへ通信路を確立し、ユーザトラフィックはHAを経由して転送される。

- HA～サービスノード区間

サービスノードとして、Internetへの接続点である Firewall、サービスを提供するためのサーバ (Web や電子メールなど)、企業網アクセスのための Gateway 等が存在する。

2.2 モバイルコア網におけるシグナリング

ユーザがサービスを利用する際のモバイルコア網特有のシグナリングは、RADIUS 区間と MIP 区間で行われる。

- RADIUS 区間では、課金や認証情報のための RADIUS パケットが送受信される。

- MIP 区間では、HA への通信路確立に必要な MIP パケットの送受信、及びユーザトラフィック転送が行われる。

ユーザがサービスを利用する際のシグナリング手順例を図 3 に示す [7]。

- (1) 利用サービス情報、端末識別子、ユーザ認証情報を含む接続要求を端末が PDSN に送信する。

- (2) PDSN は RADIUS サーバでユーザ認証を実施する (RADIUS Access Request/Accept)。

- (3) HA に登録を実施する (MIP Registration Request/Reply)。

- (4) 認証及び登録が完了すると、PDSN は端末に接続許可を送信する。

- (5) 接続が完了し、HA を経由して、端末とサービス提供ノード間でユーザトラフィックを転送する。

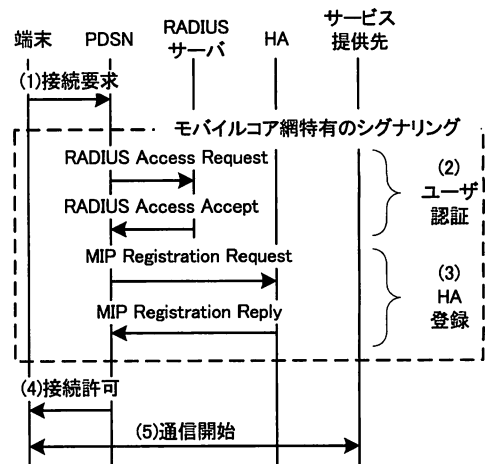


図 3 サービス利用時のシグナリング例

3 従来の監視方式と問題点

モバイルコア網を含むIP網の監視にはSNMP (Simple Network Management Protocol) [8] が一般的に用いられている。SNMPでは、パケット転送量等のトラフィック監視、及び通信ノードでの障害発生やCPU負荷等のハードウェア監視が可能である。

トラフィック監視は、通信ノードやインターフェイスを単位として行われるため、得られるデータにはサービス別の情報は含まれていない。このため、障害発生時のサービスへの影響把握には別の調査が必要となり、把握に時間を要するという問題がある。また、トラフィックは障害発生だけでなく、日時やイベント等により変動する。この変動についても、サービスへの影響を把握する必要があるが、トラフィック監視情報からの判断は容易でない。従って、従来のトラフィック監視と別の基準による客観的なサービスレベルの障害検知方式が必要である。

また、監視にSNMPを用いる場合、通信ノードでの処理負荷やSNMPトラフィック発生に伴う網負荷の問題を考慮する必要がある。さらに、大規模網では監視対象の通信ノードが多数存在し、高性能な監視ノードが必要となる。この現状から、SNMPベースで広く用いられているMRTG [9] では、監視間隔がデフォルトでは5分である。一方、サービスの利用状況によっては、瞬間的に通信ノードへの負荷が高くなることもある。この状況を「スパイク負荷」と呼称する。通信ノードによっては、スパイク負荷が処理遅延や異常処理の原因となる可能性があるため、発生状況を把握する必要がある。しかし、スパイク負荷は秒単位で発生するため、5分間隔の監視ではその把握が困難である。

4. 提案方式

4.1 基本方針

サービスレベルでの障害検知を実現するための方式として、実際にサービスへアクセスして正常性の確認を行う「アクティブ計測」方式が考えられる。しかし、サービス単位に計測が必要になること、計測パケット送信による網負荷発生の問題から、多数のサービスが提供されるモバイルデータ網への適用は困難である。

そこで、本検討では通信リンクでのパケット収集と解析に基づく「パッシブ計測」方式を基本方針とした。しかし、モバイルコア網では1

日に数十 Gbyte オーダのトラフィックが発生する。そのため、パッシブ計測に基づいてサービスレベルの障害検知を実現するためには、高性能かつ高額な機材が必要となる。

パケット収集及び解析の処理量を削減するため、2.2節で述べた、ユーザのサービス利用時におけるモバイルコア網特有のシグナリングに着目した。MIPやRADIUSのシグナリングパケットには、端末やサービスの識別子が含まれている。そのため、シグナリングパケットの詳細な解析を行うことで、端末別かつサービス別に接続回数や接続間隔を計測することが可能となる。

安定した品質のサービスが提供されている場合、端末単位で計測したあるサービスへの接続回数や接続間隔を単位時間あたりで集計すると、その分布は大きく変動しないと想定される。この分布が変動する場合、ユーザがサービスへの接続を繰り返し行っていると考えられる [10]。このことから、ユーザのサービスへの再接続挙動をシグナリングパケットから計測し、その変動を監視することで、サービスレベルの障害検知が実現可能である。

また、MIPやRADIUSのシグナリングパケットはPDSNとHAもしくはRADIUSサーバ間で送受信される。そのため、パッシブ計測を行う場合、PDSN側のみのパケットキャプチャで障害検知に必要なデータ収集が可能である。加えて、シグナリングパケットは非常に少量であるため、パッシブ計測でも十分に処理可能である。

4.2 詳細手順

4.1節の基本方針に基づく、モバイルコア網におけるサービスレベルの障害検知に関する詳細手順を述べる。

【手順1】

シグナリングパケットのキャプチャ及び解析を行い、端末識別子と利用サービス情報を得る。具体的な解析対象は、ユーザのサービス利用に関連するMIP Registration Requestパケット、RADIUS Access Requestパケットである。

【手順2】

手順1で得られた端末識別子、利用サービス情報から、端末単位かつサービス別の「接続回数」と「接続間隔」を得る。図4はこれらを模式的に表したものである。

● 接続回数

ある端末が、単位時間 (例: 180秒) 内におい

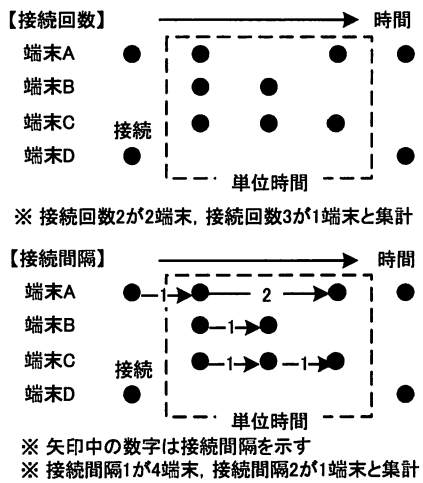


図 4 接続回数と接続間隔

て当該サービスに接続を試みた回数。

- 接続間隔
ある端末が単位時間 (例: 60 秒) 内で接続操作を試みた場合の前回接続した時刻 (単位時間内に入っていないなくてもよい) との差分。

【手順 3】

手順 2 で得られた端末単位の接続回数、接続間隔の分布をサービス別に作成する。具体的には、接続回数の場合は回数別 (例: 1、2、3、…回) の端末数、接続間隔の場合は間隔別 (例: 0~20 秒、20~40 秒、…) の端末数に関する度数分布を作成する。

【手順 4】

手順 3 で得られたサービス別の接続回数や接続間隔の度数分布の変動を調査し、障害発生を判断する。想定される分布は次のとおりである。

- 正常時
接続回数の大部分は 1~2 回に分布し、接続間隔は各値域で一定の割合となる。
- 障害発生時
3 節で述べたようなユーザの再接続動作により、単位時間あたりの接続回数は多くなり、短い接続間隔に分布する。

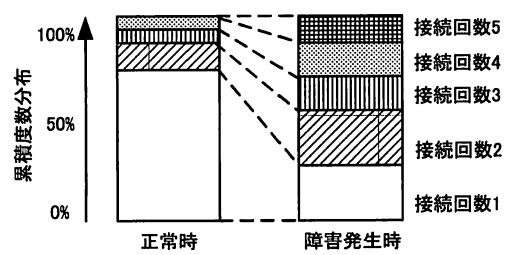


図 5 接続回数分布の変化

図 5 は接続回数の分布変動を模式的に表している。提案方式ではこのような分布の変動を監視し、サービスレベルの障害検知を実現する。

5 商用網での評価

提案方式を実装し、商用モバイルデータ網を利用した評価を行った。実装したシステムを NANDS (Network AbNormality Detection System based on call-signaling) と呼称する。

5.1 システム構成

- 測定装置
MIP 区間、RADIUS 区間に設置し、シグナリングパケットの収集及び解析を行う。その後、シグナリングパケット数や端末単位かつサービス別の接続回数と接続間隔を集計した後に、収集装置に通知する。
- 収集装置
測定装置からの集計データをデータベース化し、サービス別の接続回数や接続間隔に関する

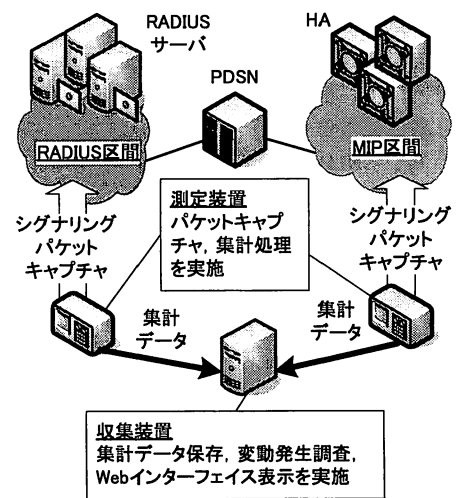


図 6 NANDS 構成



図 7 NANDS 起動画面

変動発生を調査する。また、変動状況をグラフ表示するための Web インターフェイスを有する (図 7)。

5.2 障害検知例

提案方式で検知した障害例を示す。

5.2.1 検知例 1

最初に、単一サービスの障害発生時における接続間隔分布が時系列で変動する例を示す。

図 8 は、値域を 20 秒単位とした接続間隔に属する端末数の累積度数分布の時系列推移である。例えば、0:00 の場合、接続間隔 20 秒以上 40 秒未満と、40 秒以上 60 秒未満の端末が、それぞれ 25% 程度存在する。

この例では、0:02 に障害が発生し、0:08 に障害が解決した。障害発生期間に注目すると、正常時にはほとんど存在しない接続間隔 20 秒未満の分布が 80% 以上の割合を占めている。

このような分布の変動は接続回数でも同様に発生する。このことから、提案方式では値域分布の変動をサービス別に監視することで、障害発生を検知可能である。

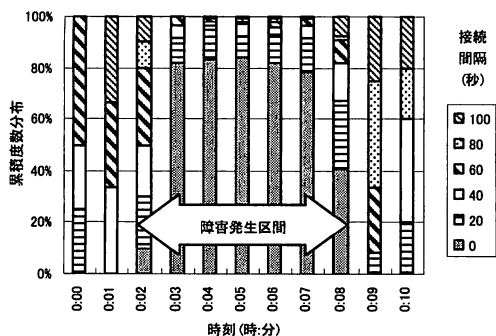


図 8 障害発生時の接続間隔分布

5.2.2 検知例 2

次に、パケット数ベースのトラフィック監視では検知できないが、本方式により特定の通信ノードで障害を検知している例を示す。

図 9 は MIP シグナリングパケットである MIP Registration Request と Reply の 1 秒単位でのパケット数変化である。MIP Registration Request と Reply パケットの割合は 80% 前後で一定に推移しており、問題はないように見える。

しかし、この期間において、特定の HA で障害が発生している。図 9 と同一時刻における HA 別の接続回数 2 から 5 の累積度数分布を図 10 に示す。障害の発生していない HA1 では接続回数 2 の割合が 80% 以上を占めており、全体的な割合にそれほど変化はない。これに対して、障

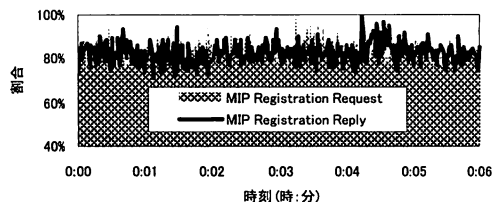


図 9 MIP シグナリングパケット数推移

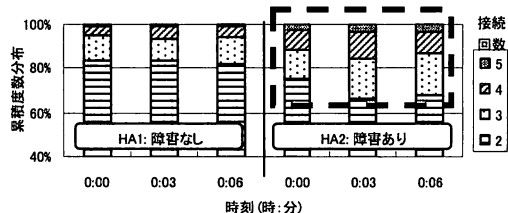


図 10 障害発生有無での接続回数分布の相違

害の発生している HA2 では、図 10 の囲み部分のように、接続回数 2 の割合は減少し、接続回数 3 回以上の割合が増加する。このように、提案方式では通信ノード単位で接続回数や接続間隔を集計することで、障害検知が可能である。

5.2.3 検知例 3

最後に、スパイク負荷が発生しているものの、接続回数からサービスに対する影響はないと判断した例を示す。

図 11 は MIP 区間のシグナリングパケットの 1 秒単位のパケット数変化である。ほとんどの場合において、20% 程度のパケット数であるが、図 11 の 0:07 付近においては 5 倍程度になっており、スパイク負荷が発生している。

図 12 は図 11 と同一時刻における接続回数 1 から 3 回の累積度数分布である。図 12 の 0:06 から 0:09 における分布は、他の時刻と比較してほとんど変化はない。このことは、スパイク負荷は発生しているが、提供しているサービスへの影響はないことを示している。

5.3 考察

提案方式の障害検知における最大の特徴は、所望サービスに接続できない場合の再接続動作という、ユーザ挙動に着目していることである。その利点として、サービス提供状況に関する正常性の判断が容易である。加えて、障害とは言えないまでも、さらなるサービス品質向上という観点における問題点の把握もしやすい。

さらに、提案方式では、シグナリングパケットに着目したパッシブ計測を行っている。これにより、MIP 区間においてはユーザトラフィック全てを解析する場合に比べ、処理パケット数を

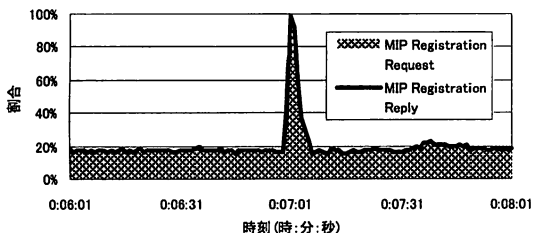


図 11 スパイク負荷発生例

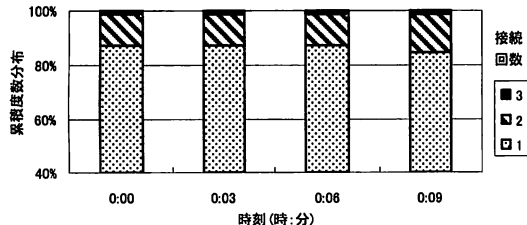


図 12 スパイク負荷時の接続回数分布

数パーセントに抑制した。また、秒単位でのシグナリングパケット数の集計により、スパイク負荷の状況も把握可能である。

加えて、図 2 に示すように、PDSN 側でのパケットキャプチャにより、全てのシグナリングパケットを得ることが可能である。このため、比較的少数のパッシブ計測で、幅広いサービスに対する障害検知に必要な情報を得られる。

なお、商用モバイルデータ網を利用した評価を通して、次の課題を得た。

● 課題 1

障害判定の単位がシグナリングパケットに含まれる利用サービス別になっている。そのため、サーバ単位等のより細かい単位の障害検知には適用できない。この点については、計測対象の追加等を含めた対応が必要と考えられる。

● 課題 2

単位時間あたりに一定量の端末が利用するようなサービスについては提案方式での障害判定が可能である。しかし、利用端末数が少数のサービスでは、相対的に分布の変化が大きく、障害判定が困難である。これに対しては、まず提案方式が有効に機能する単位時間あたりの利用端末数を詳細に評価する必要がある。さらに、接続回数や接続間隔の集計や変動検知方法の改善により、利用端末数が少数のサービスでの障害検知を実現することが課題である。

6 まとめ

本稿では、広く普及したモバイルデータ網に

おいて、さらに安定したサービス提供のために、サービスレベルの障害検知が可能な方式を提案した。提案方式は、モバイルコア網特有のシグナリングに着目し、障害発生時におけるユーザの再接続挙動に基づき障害検知を行っている。具体的には、シグナリングパケットを端末単位かつサービス別に集計し、単位時間あたりの接続回数や接続間隔の分布の変動により障害を検知する。さらに、提案方式を実装し、商用モバイルデータ網を利用した評価を行い、提案方式の有効性を示した。

今後は、5.3節で示した課題の解決に向けた検討を実施していく予定である。

謝辞

NANDS の商用モバイルデータ網での評価にご協力いただいた KDDI 株式会社 古田 GL、河合 GL、佐藤課長、長尾課長補佐、村岡課長補佐、加藤課長補佐、藤川課長補佐、加藤主任に深く感謝致します。また、日頃ご指導いただく株式会社 KDDI 研究所 鈴木執行役員、中村 GL に深く感謝致します。

参考文献

- [1] 山崎洋一、”配送員に新型 au 携帯 7000 台、POS の役割を BREW アプリで - ヤマト運輸”、日経コミュニケーション、<http://itpro.nikkeibp.co.jp/article/COLUMN/20061226/257790/?ST=keitai>、Jan 2007.
- [2] APAN Tokyo XP Traffic Monitor、<http://tools.jp.apan.net/mrtg/>
- [3] 3GPP2、”cdma2000 High Rate Packet Data Air Interface Specification”、C.S.0024-A v3.0、Sep 2006.
- [4] 3GPP2、”cdma2000 Wireless IP Network Standard: Introduction”、X.S.0011-001-C v3.0、Nov 2006.
- [5] C. Rigney et al.、”Remote Authentication Dial In User Service (RADIUS)”、RFC2865、Jun 2000.
- [6] C. Perkins et al.、”IP Mobility Support for IPv4”、RFC3344、Aug 2002.
- [7] 3GPP2、”cdma2000 Wireless IP Network Standard: Simple IP and Mobile IP Access Services”、X.S.0011-002-D v1.0、Feb 2006.
- [8] J.D.Case et al.、”Simple Network Management Protocol (SNMP)”、RFC1157、May 1990.
- [9] MRTG (Multi Router Traffic Grapher)、<http://oss.oetiker.ch/mrtg/>
- [10] 新井田他、”携帯電話キー操作から見た WEB アクセス行動の分析”、電子情報通信学会 第 5 回ブレインコミュニケーション研究会予稿、May 2008.