モバイルコンピューティングとワイヤレス通信　21－14
(2002. 5. 24)

モバイルIPベース移動体ネットワーク用プロトコルアナライザの設計

小林　修　　石川　彰夫　　井戸上　彰　　長谷川　亨

株式会社KDDI研究所
〒356-8502 埼玉県上福岡市大原2-1-15

E-mail: osamu@kddilabs.jp akio@kddilabs.jp idoue@kddilabs.jp hasegawa@kddilabs.jp

あらまし
携帯電話網や無線LANの普及に伴い，これらのIPベースのネットワークではIP上のモビリティを提供するため，モバイルIPが適用され始めている．また，モバイルIPベースの移動体ネットワークでは，Mobile IPv4を含め，複数のプロトコルが関連して動作し，その手順は複雑なものとなっている．このようなモバイルIPベースの移動体ネットワークにおいて，障害を検出しその原因を解析するにはネットワーク上のIPパケットを収集し，これらのプロトコル手順を解析するプロトコル解析ツールが必要である．そこで，筆者らはこれらのモバイルIPベースの移動体ネットワークを解析対象とした，プロトコルアナライザを設計開発した． 本稿ではこのプロトコルアナライザについてその概要を述べる．

キーワード　Mobile IPv4，プロトコルアナライザ，通信解析手順

Design of Network Protocol Analyzer for Mobile IP based Network

Osamu Kobayashi Akio Ishikawa Akira Idoue and Toru Hasegawa

KDDI R&D Laboratories Inc.
2-1-15 Ohara Kamifukuoka-shi, saitama 356-8502, Japan

E-mail: osamu@kddilabs.jp akio@kddilabs.jp idoue@kddilabs.jp hasegawa@kddilabs.jp

Abstract
Mobile IP begins to be applicable to provide mobility for the IP based network caused by diffusion of cellular phone and the wireless LAN. However, because many protocols work, the analysis of the difficulty is complex over the Mobile IP based network. In these networks, the analyzing tool which analyzing a protocol process is necessary to detect the network failure and to analyze a cause. We are developing protocol analyzing tool to analyze Mobile IP based network protocol. This paper presents the design of thus network protocol analyzer.

Keyword　Mobile IPv4, Protocol Analyzer, Communication Procedure Analysis

1. はじめに

近年，携帯電話網における IP サービスや無線 LAN の普及に伴い，ネットワーク上でのモビリティを提供するため，Mobile IPv4[1]が適用されている．また，3GPP2(3G Partnership Project 2)において検討されている ANSI 規格をベースとした IMT2000 仕様では携帯端末の IP サービスにおける移動管理に Mobile IPv4 を拡張した手順が使用されている．このように Mobile IP が適用されたネットワークにおける IP 通信において，発生する障害を検出するためには Mobile IP の位置登録手順の解析が不可欠である．また，Mobile IP では位置登録手順の後，ユーザパケットの送受に GRE[3]などのトンネリング手順を使用するため，これらの手順も同時に解析する必要がある．また一方，3GPP2 によって規定されている移動体ネットワークでは Mobile IPv4 による移動管理に加え，RADIUS[4][5]による認証及び課金管理や PPP[6]による移動ノード(Mobile Node 以下 MN)のコネクション管理が同時に行われている．

このように，複数のプロトコルが適用される移動体ネットワークおいて各種サーバやネットワークの障害を検出し，その原因を解析するにはネットワーク上の IP パケットを収集し，これらのパケットのプロトコル手順を解析する必要がある．通常，このような問題を調査するためには Sniffer[7]や Ethereal[8]など一般的なプロトコルアナライザを用いるが，これらのアナライザは，パケットフォーマットの解析を行うのみであり，各プロトコル手順においてコネクションを意識した詳細な解析機能を持っていない．このためこれらのプロトコルアナライザを用いて詳細な解析を行うには解析者がコネクションを意識して解析を行う必要がある．

本研究では Mobile IP を中心に移動体ネットワークにおいて使用される各種プロトコル手順を解析するアナライザソフトウェアを開発した．本稿ではこのプロトコルアナライザの設計についてその概要を紹介する．

2. 要求条件と設計方針

2.1. 要求条件

本アナライザを設計するにあたり，要求される条件を以下に整理する．

(1)適用ネットワークモデルとプロトコル

本アナライザを適用するネットワークモデルとして図 1 に Mobile IPv4 を適用した一般的なネットワーク構成の例を，図 2 に 3GPP2 において検討されている IMT2000 仕様の公衆移動体ネットワーク構成の例を示す．Mobile IPv4 では Care of Address(以下 COA とする)の設定に Foreign Agent(以下 FA とする)を使用する FA-COA モデルと FA を使用しない Co-Located-COA モデルの 2 つのネットワークモデルが存在する．また，3GPP2-IMT2000 仕様の IP ネットワークモデルは，RAN(Radio Access Network)と呼ばれるアクセス網とパケット交換網から構成され，RAN は基地局(BS： Base Station)，基地局制御装置(BSC: BS Controller)，PCF(Packet Control Function)から構成される．MN の移動は，PDSN(Packet Data Serving Node)と呼ばれるノードで管理され，RAN 内の MN の位置管理には Mobile IPv4 を拡張した A11[2]と呼ばれるプロトコルが使用されている．さらに，PDSN を跨って端末が移動する場合には，HA (Home Agent)と PDSN 間で Mobile IPv4 を用いて位置管理を行う．ここで，PDSN は FA としての役割を果たす．さらに，MN が RAN に新たに収容される場合には，AAA と PPP を用いて，認証が行われる．

本アナライザはこれらの解析対象のネットワークにおいて MN と通信相手先ノード(CN: Correspondent Node)間のプロトコル手順及び Mobile IP の位置登録手順及びこれらのネットワーク使用されている各種プロトコル手順の解析を行う．

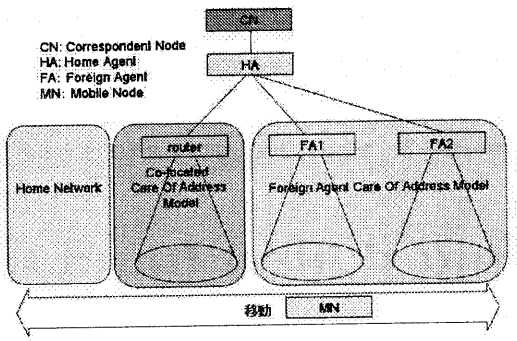

図 1 Mobile IPv4 を適用したネットワーク構成

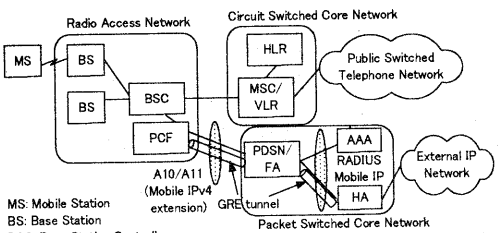

図 2 3GPP2 の IMT2000 仕様のネットワーク構成

適用するネットワーク構成から本アナライザの解析対象となるプロトコル手順は以下のものとなる．

・Mobile IPv4 手順
・A10/A11（3GPP2 仕様における Mobile IPv4 ベースの移動管理プロトコル）手順[6]
・RADIUS 手順
・PPP 手順
・GRE カプセル化手順
・カプセル化された内部パケットの手順

(2)解析対象のフィルタリング

図 2 に示すような公衆サービスを提供する移動体ネットワークモデルにおいては，収集されたキャプチャデータ中に多数のコネクションが存在する．また，問題の解析についてコネクションを指定したい場合，このようなデータの中から解析対象を検出するためには，複数のコネクションの中から所望の条件で対象を絞り込む必要である．

(3)プロトコル解析

本アナライザは前述のような各ネットワークモデルにおいて発生する問題を検出するため，単にプロトコルを構造解析するだけでなく，プロトコル手順を解析し誤りがあればこれを検出する．また，移動体ネットワークにおいては MN の移動が起因する障害が想定されるため，MN のハンドオフについて解析を行う．

(4)位置登録状況の把握

Mobile IP では FA や HA などの位置管理ノードに位置登録手順に従って MN が登録される．これらのノードにおける MN の位置登録状況を把握することは，Mobile IP での障害と他の障害を切り分けるために有益な情報となる．したがってこの MN 登録状況を明示する仕組みを必要とする．

2.2. 設計方針

前節に示した要求条件に基づき，今回設計したアナライザの設計方針を以下に示す．

(1)解析データ

本アナライザは図 1 及び図 2 に示したネットワークモデルにおける有線区間において，tcpdump を用いて取得されたキャプチャデータ（libpcap 形式データ）を解析対象とする．また，解析対象とする情報は，キャプチャデータ中でコネクションが開始され且つ終了したもののみとする．

(2)解析モード選択

解析対象のデータが取得されたネットワークモデル及びプロトコルをオペレータが選択し解析を行う．具体的にはネットワークモデルを以下の 4 つの解析モードに集約する

・Mobile IPv4 (FA-COA)解析モード
・Mobile IPv4 (Co-Located COA)解析モード
・A10/A11 解析モード
・RADIUS 解析モード

解析者はこれらの解析モードを選択することにより，所望のネットワークモデルにおける解析を行う．また，選択した解析モードにおいて直接関係しないデータは表示しない．

(3)解析フィルタ

取得したデータ中のコネクションをインデックスする主要パラメータ一覧を表示し，解析者がこれを選択することにより所望のコネクション決定する．

(4)プロトコル動作の推定

選択された解析モード毎に想定されるイベント順序を推定し，誤りがあればこれを検出する．FA-COA の Mobile IP を例にとって説明すると，MN が移動した場合，移動する度に経由する FA は変わるが，MN が登録されている HA は変わらない．したがって Mobile IP の位置登録メッセージから HA における MN の状態推定を行う．また，この状態推定を用いて，MN が移動した場合のハンドオフを検出する．

(5)解析結果表示

本アナライザは解析モード毎にイベントシーケンス図を GUI により表示する．イベントシーケンス図では Mobile IP の位置登録手順とユーザデータの要求メッセージと応答メッセージの対応，及び再送データとオリジナルデータとの対応を表示する．

(6)統計表示

本アナライザは解析モード毎に入力されたファイルから各プロトコル手順の統計情報を収集し，表示する．

3. 詳細設計

本節では本アナライザのプロトコル解析機能の幾つかを詳細に解説する．

3.1. プロトコルの状態解析

プロトコルの状態解析を解説するため，具体例として 3GPP2-IMT2000 のコールシーケンスを図 3 に示す．

このコールシーケンスでは MN が送出する Mobile IP メッセージや移動体ネットワーク(PCF)が送出する A11 メッセージ，RADIUS メッセージなど複数の解析対象メッセージが存在するが，ここでは A11 のプロトコル動作に着目する．本アナライザはネットワークモデル毎に解析対象とするノードの状態遷移をエミュレートしている．図 4 に A11 の解析に使用するエミュレート状態遷移図を，表 1 にエミュレート状態遷移表（一部）示す．ここでエミュレートとは本アナライザにおける状態推定を意味する．A11 のプロトコル手順では移動体通信特有のメッセージが複数存在する．以下に代表的な動作を取り上げ，それぞれの動作が起こった場合の状態遷移を解説する．

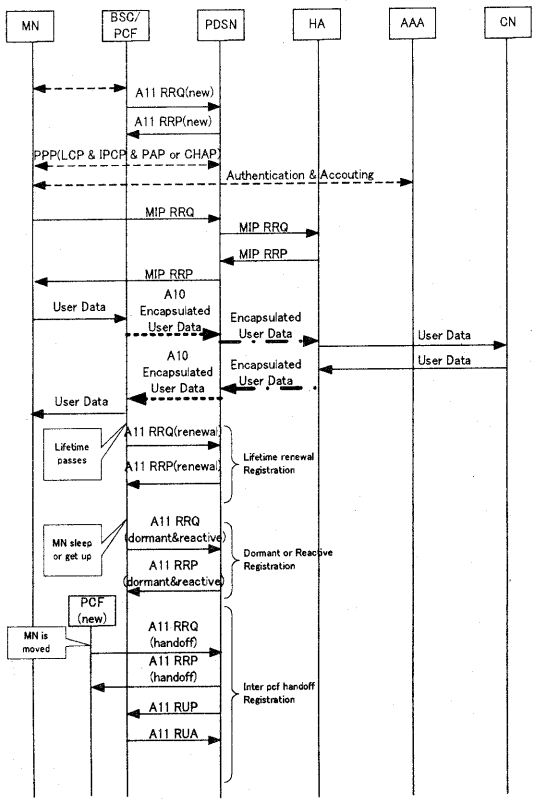

図 3 3GPP2-IMT2000 コールシーケンス

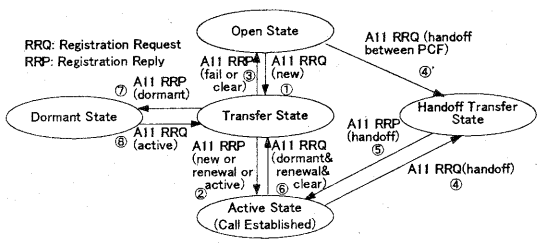

図 4 エミュレート状態遷移図

・位置登録

Open State で A11-RRQ メッセージを検出した場合，状態を Transfer State に遷移させる.(図表中①)．ここでは A11-RRP メッセージが次に検出されるべきであるため，本アナライザは A11-RRP メッセージの検出を推定する．次に A11-RRP メッセージを検出した場合，そのコードフィールドを参照して正常受付であれば状態を Active State (Call Established)とする．(図表中②)．ここで，期待しないメッセージやコードフィールドが正常受付で無いメッセージを受信した場合は，原因を推定してアラームメッセージを出力し，その後状態を Open State へ遷移させる．(図表中③)．

・ハンドオフ要求(PCF 間ハンドオフ)

Active State 状態で，登録した PCF と異なる PCF からの A11-RRQ メッセージを受信すると本アナライザは状態を Handoff Transfer に遷移させる．(図表中④)．次に Handoff Transfer 状態で A11-RRP メッセージを検出するとコードフィールドを参照し，正常受付であれば”ハンドオフが発生した”というメッセージを解析結果として出力し，Active State へ遷移する．正常受付でない場合はそのメッセージを解析し，原因を推定してアラームメッセージを出力する．その後状態を Active State に遷移させる．(図表中⑤)．

・ハンドオフ要求 2(PDSN 間ハンドオフ)

Open State で A11-RRQ メッセージを検出し，そのメッセージ中の Air Link Record Type フィールドに Mobility Event Indicator が設定されていた場合，この MN は他 PDSN で起呼されたセッションが PDSN を跨ってハンドオフしたものであると判断する．このメッセージを受信した場合，エミュレータは状態を Open State から Handoff transfer へ遷移させる．(図表中④')．また，前述と同様に A11-RRP メッセージを検出し，正常受付であれば”ハンドオフが発生した”というメッセージを解析結果として出力し，Active State へ遷移する．(図表中⑤)

表 1 エミュレート状態遷移表(一部)

Event No / State_No	A11-RRQ-recv_1	A11-RRP-recv_2	Lifetime expire_3	message-wait timeout_4
Open state	nw=① Next_State=2 ho=④' Next_State=4	Error	–	–
Transfer State_2	retransmitte	nw=② Next_State=3 fl=③ Next_State=1 do=⑦ Next_State=5 rw=② Next_State=3 cr=③ Next_State=1	Next_State=1	if (Before State == Open) Next_State=1 else Next_State=3
Active State_3	rw=⑥ Next_State=2 ho=④ Next_State=4 dm=⑥ Next_State=2 cr=⑥ Next_State=2	–	Next_State=1	–
Handoff transfer State_4	–	④ Next_State=3	Next_State=1	Next_State=3
Dormant State_5	⑧ Next_State=2	–	Next_State=1	–

nw:new rw:renewal ho:handoff dm:dormant cr:clear fl:fail

・Lifetime 更新

Mobile IP では MN の登録有効時間を Lifetime として位置登録手順において規定するが， A11 においてもこれは同様である．MN は A11-RRP 上設定された Lifetime 値を計算し，Lifetime が満了する前に再登録を行う．再登録の手順は通常の位置登録と同様である.(図表中①→②と同様)

・ドーマント移行

MN-CN 間の IP 通信で，MN の要求による通信が無く，且つ CN からの通信要求が無い状態がある時間経過した場合に，MN はドーマント（睡眠）と呼ばれる状態となる．これを A11 ではメッセージで表している．Active State で A11-RRQ メッセージを検出し，そのメ

ッセージ中の Air Link Record Type フィールドに Stop が設定されていた場合，この MN はドーマントへ移行したものであると判断する．(図表中⑥→⑦)

・アクティブ移行

ドーマント状態において MN からの通信要求か，あるいは CN からの通信要求があった場合，MN はドーマント状態からアクティブ状態へ移行する．(図表中⑧→②)

・位置登録解除

Active State で A11-RRQ メッセージを検出し，Lifetime が 0 且つ Air Link Record Type フィールドに Stop が設定されていた場合，この MN は位置登録削除したと判断する．(図表中⑥→③)．

上記のようなイベントをコネクション単位で解析し，状態遷移を推定することによりメッセージの再送やイベント順序違いなどプロトコル手順における障害を検出することが可能となる．また，本アナライザは前述の 4 つの解析モードにおいてそれぞれのネットワークモデルに沿ったエミュレート状態を持ち，同様な解析を可能とする．

3.2. アドレスフィルタリング

解析者が特定のコネクションについて解析を行いたい場合，コネクションを特定するキー情報を入力することにこれを実現する．具体的には解析に先んじて，各ネットワークモデルにおける構成ノードの IP アドレス情報や解析対象パケットに設定されているユーザ ID を抽出し，アドレスリストと呼ぶコネクション特定する情報リストを生成することにより，解析者がこれを参照し解析対象を絞り込む．アドレスリストの構成要素（パラメータ）は解析モード毎に表 2 に示すように設定する．

表 2 解析モードとアドレスリストパラメータ

解析モード	アドレスリストパラメータ
Mobile IPv4 FA COA 解析モード	Mobile Node address Foreign Agent address Home Agent address Correspondent Node address Network Access Identifier
Mobile IPv4 Co-Located COA 解析モード	Mobile Node address Home Agent address Correspondent Node address Network Access Identifier
A10/A11 解析 モード	Mobile Node address PCF address PDSN address Home Agent address RADIUS Server address Correspondent Node address Network Access Identifier
RADIUS 解析モード	NAS address RADIUS Server address username

アドレスリストパラメータの選択は複数回可能とし，1 つのパラメータが選択されるたびに他パラメータのアドレスリストを更新し，コネクションを絞り込むことを可能とする．

3.3. MN 登録情報表示

解析対象キャプチャデータ中の任意の時間における HA や FA への MN の登録状況を表示可能とする．キャプチャデータ中に複数の FA や HA が存在する場合は IP アドレスのテーブル表示を所望のアドレスを入力することにより，HA であれば Binding Cache 情報を FA であれば Visitor List 情報を明示する．以下に Visitor List 及び Binding Cache の表示パラメータを以下に示す．

・MN Address (Home Address)
・Care of Address
・Foreign Agent Address
・Lifetime
・NAI
・reg-info

ここで reg-info とは MN の登録状態を明示するパラメータであり，以下のように定義する

reg-info	0	登録なし
	1	登録中
	2	登録済
	3	登録失敗、異常信号受信

登録なしとは過去に在圏していたがハンドオーバにて移動し，在圏していない状態．登録中とは Registration Request メッセージを送信し，その Reply が帰っていない状態．登録済とは Registration Request が accept (codefield＝0) された状態．登録失敗とは Registration Request が denied (codefield ≠0)された状態あるいは期待しないメッセージを受信した状態を意味する．

4. 機能実装と解析例

4.1. 機能実装

本アナライザのソフトウェア構成を図 5 に示す．本アナライザはプロトコル解析を行うパケット解析部と統計情報を生成する統計解析部及び結果を表示する GUI 部から構成される．以下に各構成におけるモジュールの機能を説明する．

(1) プロトコル解析モジュール

統計モジュールにより生成されたアドレスフィルタファイルと入力ファイルから所望のコネクション情報を抽出し，Mobile IPv4，A10/A11，PPP 等のパケット構造を解析し，プロトコル毎のパラメータを抽出して中間ファイルを生成する．

(2) エミュレートモジュール

中間ファイルをプロトコル毎に解析して プロトコ

ルの状態解析を行う．解析モード毎に Mobile IP の解析においては HA 及び PDSN の状態遷移を，RADIUS の解析においては RADIUS サーバの状態遷移を推定し，その情報を出力ファイルに付加する．

(3) 統計解析モジュール

入力ファイルからプロトコル毎に単位時間当たりのパケット数やメッセージ数などの統計ファイルを出力する．また同時に，解析対象を絞り込むためのアドレスリスト情報を生成する．さらに，FA に一時的に登録されている MN のリスト Visitor List や，HA と通信している MN のリスト Binding Cache を，中間ファイルから抽出する．

(4) GUI 処理

出力ファイル及び統計ファイルから解析結果を出力する．また，必要に応じイベントシーケンス図や Visitor List テーブルや Binding Cache テーブルを表示する．

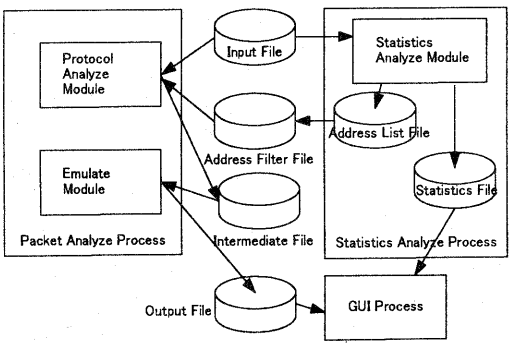

図 5 ソフトウェア構成

4.2. 解析例

今回開発した本アナライザを使用し Mobile IPv4 FA COA モデルのネットワークについて解析を行った例を図 6 及び図 7 に示す．

この解析では MN が異なる FA にハンドオフを行う様子が示されている．本アナライザはこのような正常な Mobile IP 位置登録手順や再送メッセージの明示やシーケンスエラーをネットワークモデル毎に解析することができる．

5. おわりに

本稿では， Mobile IPv4 をベースとする移動体ネットワークおいて使用される各種制御プロトコルを解析するアナライザの設計についてその詳細を述べた．また，これを開発し要求条件を満足するアナライザを開発した．今後は本アナライザを用い移動体ネットワークにおけるユーザデータの振る舞いに着目した詳細な検討を行う予定である．

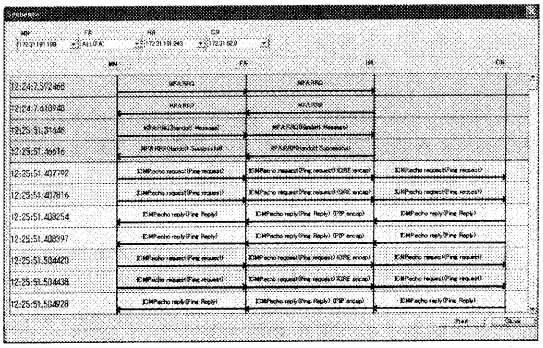

図 6 Mobile IPv4 FA COA モデルにおけるイベントシーケンス解析画面

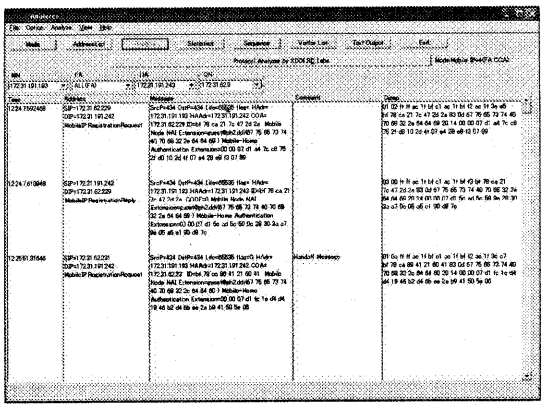

図 7 Mobile IPv4 FA COA モデルにおける解析画面

謝辞

日頃御指導頂く KDDI 研究所浅見所長に感謝します．

文 献

[1] RFC2002 "IP Mobility Support"

[2] RFC2784 "Generic Routing Encapsulation (GRE)" (2000.3)

[3] RFC2865 "Remote Authentication Dial In User Service (RADIUS) " (2000.6)

[4] RFC2866 "RADIUS Accounting" (2000.6)

[5] RFC1661 "The Point-to-Point Protocol (PPP)" (1994.7)

[6] 3GPP2 Access Network Interface Inter-operability Specification 3GPP2 A.S001-A IOSv4.1 (2000.11)

[7] Networks Associates Technology: Sniffer http://www.sniffer.com

[8] Gerald Combs: Ethereal http://www.ethereal.com