(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2012-134976
(P2012-134976A)
(43)公開日　平成24年7月12日(2012.7.12)

(51)Int.Cl.		F I			テーマコード（参考）
H04W 8/06	(2009.01)	H04Q	7/00	143	5K067

審査請求 未請求　請求項の数 4　OL　外国語出願　（全 44 頁）

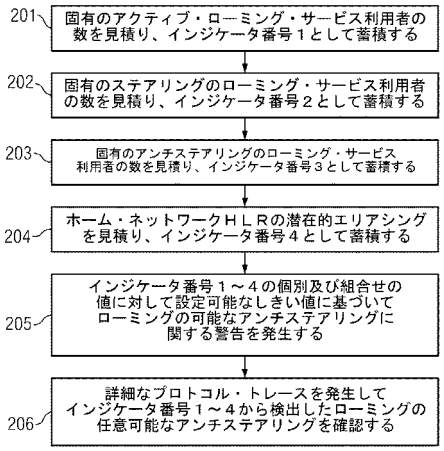
(21)出願番号　特願2011-278462 (P2011-278462)
(22)出願日　平成23年12月20日 (2011.12.20)
(31)優先権主張番号　12/975,137
(32)優先日　平成22年12月21日 (2010.12.21)
(33)優先権主張国　米国 (US)

(71)出願人　391002340
テクトロニクス・インコーポレイテッド
ＴＥＫＴＲＯＮＩＸ，ＩＮＣ．
アメリカ合衆国　オレゴン州　９７０７７－０００１　ビーバートン　サウスウエスト　カール・ブラウン・ドライブ　１４１５０
(74)代理人　110001209
特許業務法人山口国際特許事務所
(72)発明者　パオロ・ノルベルト・アグレッティ
イタリア共和国　３５１３３　パドヴァ　ヴィア　レオナルド・ダ・ヴィンチ　１２／Ａ

最終頁に続く

(54)【発明の名称】訪問先ネットワークでローミングのアンチステアリングを検出する方法、ネットワーク・モニタリング・システム、及びコンピュータの読出し可能な蓄積媒体

(57)【要約】
【課題】訪問先ネットワークがホーム・ネットワークによるローミングのステアリングを拒否するかを判断する。
【解決手段】ローミングのアンチステアリング活動を自動的に検出するシステム及び方法を開示している。訪問先ネットワークによる全てのインターナショナルＭＡＰシグナリングを連続的にモニタするホーム・ネットワークでのモニタリング・システムによりこの方法を用いることができる。固有のアクティブなローミング・サービス利用者の数、固有のステアリングされたローミング・サービス利用者の数、固有のアンチステアリングされたローミング・サービス利用者の数を含む異なる形式のローミング加入者の数を見積もって、ローミングのアンチステアリングを検出する。異なる形式の加入者の数は、単独又は組合せで、しきい値と比較される。数がしきい値を超えれば、モニタリング・システムは、訪問先ネットワークがローミングのアンチステアリングの技術を用いているとホーム・ネットワークに警告する。
【選択図】図２



【特許請求の範囲】
【請求項１】
訪問先ネットワークでのローミングのアンチステアリングを検出する方法であって；
ホーム・ネットワークで受信した上記訪問先ネットワークでのローミング加入者からのシグナリング・メッセージを捕捉し；
加入者毎に上記捕捉したメッセージを相関させ；
上記訪問先ネットワークでのアクティブなローミング加入者の数を見積り；
上記訪問先でのステアリングされたローミング加入者の数を見積り；
上記訪問先ネットワークでのアンチステアリングされたローミング加入者の数を見積り；
上記アクティブなローミング加入者、ステアリングされたローミング加入者及びアンチステアリングされたローミング加入者の見積り数を単独又は組合せて１つ以上の所定しきい値と比較し；
上記１つ以上の見積り値が単独又は組合せでしきい値を超えたときにローミング活動の潜在的なアンチステアリングを識別する方法。
【請求項２】
ホーム・ネットワーク及び１つ以上の訪問先ネットワークの間で交換されるメッセージを含むデータ・トラフィックをＳＳ７リンクから捕捉するのに適する少なくとも１つのＳＳ７インタフェースと；
上記捕捉したデータ・トラフィックを蓄積するメモリと；
上記訪問先ネットワークでのアクティブなローミング加入者の数を計算し、
上記訪問先ネットワークでのステアリングされたローミング加入者の数を計算し、
上記訪問先ネットワークでのアンチステアリングされたローミング加入者の数を計算し、
上記アクティブなローミング加入者、ステアリングされたローミング加入者及びアンチステアリングされたローミング加入者の数を所定しきい値と比較し、
上記比較に応じて上記訪問先ネットワークがローミング技術のアンチステアリングを用いているかを判断するのに適したプロセッサと
を備えるネットワーク・モニタリング・システム。
【請求項３】
ネットワーク・モニタリング・システムを制御するインストラクションを備えており、
上記インストラクションは、実行の際にプロセッサにより；
ホーム・ネットワークで受信した訪問先ネットワークからのシグナリング・メッセージを捕捉し、ここで、ローミング・ホーム・ネットワーク加入者が上記訪問先ネットワークにアタッチしようとする試みに上記シグナリング・メッセージが対応し；
上記訪問先ネットワークでのアクティブなローミング加入者の数を見積り；
上記訪問先でのステアリングされたローミング加入者の数を見積り；
上記訪問先ネットワークでのアンチステアリングされたローミング加入者の数を見積り；
上記アクティブなローミング加入者、ステアリングされたローミング加入者及びアンチステアリングされたローミング加入者の見積り数を単独又は組合せて１つ以上の所定しきい値と比較し；
上記１つ以上の見積り値が単独又は組合せでしきい値を超えたときにローミング活動の潜在的なアンチステアリングを識別する
ことを行うことを特徴とするコンピュータが読出し可能な蓄積媒体
【請求項４】
ホーム・ネットワーク及び１つ以上の訪問先ネットワークの間で交換されるメッセージを含むデータ・トラフィックをＳＳ７リンクから捕捉するのに適する少なくとも１つのＳＳ７インタフェースと；
上記捕捉したデータ・トラフィックを蓄積するメモリと；
訪問先ネットワーク用の成功したローミングの数に対応するローミング変数を上記所定期間の初めにてゼロにリセットし、
上記所定期間中に上記訪問先ネットワークにて個別の出て行くローミング加入者を追跡

し、
上記所定期間中に少なくとも１つの成功したサービスの試みを特定ローミング加入者が実行すると上記ローミング加入者をアクティブなローミング・サービス利用者として識別し、
各アクティブなローミング・サービス利用者に対してローミング・サービス利用者変数の値を増分するのに適するプロセッサと
を備えるネットワーク・モニタリング・システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般に、ホーム及び訪れた一般モバイル・ネットワークの間のシグナリングのモニタリングに関し、特に、訪問先ネットワークがホーム・ネットワークによるローミングのステアリングを拒否するかの判断に関する。
【背景技術】
【０００２】
モバイル・サービス・プロバイダは、典型的には、特定の国又は１つ以上の大都市サービス・エリア（Metropolitan Service Area：ＭＳＡ）の如く特定された地理的エリア内での無線カバレージを提供する。サービス・プロバイダの加入者がそれらエリア内でのモバイル・サービスを要求するとき、加入者の携帯電話又はユーザ装置は、サービス・プロバイダのネットワークをサーチし、そのネットワークにアタッチする。加入者がそのサービス・プロバイダの指定カバレージ・エリアの外を訪問するとき、加入者の携帯電話は、サービスを得るためには、ローミングすべきかを検討し、他のサービス・プロバイダによるモバイル・ネットワークである訪問先ネットワークにアタッチしなければならない。加入者がアタッチして加入者の携帯電話が有効な装置であるかを確認するときに、訪問先ネットワークは、ホーム・ネットワークと情報を交換する。認証メッセージの交換が成功すると、ローミング加入者は、訪問先ネットワークからサービスを得る。
【０００３】
例えば、米国を本拠とするモバイル・ネットワークの加入者がヨーロッパに旅行する。ヨーロッパにいる間にモバイル・サービスを受けるには、米国を本拠にする加入者の携帯電話は、ヨーロッパのサービス・プロバイダのモバイル・ネットワークを探し、そこにアタッチしなければならない。ローミング・モバイル装置は、多数の可能性のある訪問先ネットワークを検出できる。典型的には、モバイル装置は、最強の信号を有する訪問先ネットワークにアタッチする。
【０００４】
しばしば、ホーム・モバイル・サービス・プロバイダは、ホーム・サービス・エリアの外側のエリア内でのカバレージを提供する好ましい外国サービス・プロバイダと契約上の合意を行う。かかる契約は、例えば、ホーム・ネットワークからのローミング加入者に低い課金レート及び／又は保証されたクラスのサービスを提供する。よって、ホーム・ネットワーク・サービス・プロバイダは、通常、その加入者のローミング装置が、推奨外国サービス・プロバイダにアタッチすることを望む。これを達成するためには、ホーム・ネットワークは、ローミングのステアリング（Steering of Roaming：ＳｏＲ）を用いて、その加入者のモバイル装置を推奨訪問先ネットワークに案内しようとする。非推奨訪問先ネットワークのいくつかは、ローミング加入者をそのネットワークに維持するため、又はそのローミング加入者が他の訪問先ネットワークを利用するのを防ぐために、ローミングのアンチステアリング（Anti-Steering of Roaming：アンチＳｏＲ）技術を用いる。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２００７－２８２２３号公報
【特許文献２】国際公開第２００２／０１３５６７号パンフレット（特表２００４－５０

６３５９号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
モニタリング・システムは、訪問先の一般モバイル・ネットワーク及びホームの一般モバイル・ネットワークの間のシグナリング・トラフィックを分析して、訪問先ネットワークがホーム・ネットワーク加入者に対するローミング技術のアンチステアリングを用いているかを判断する。モニタリング・システムは、例えば、訪問先ネットワークが加入者の手動切り離しをエミュレーションしているか、又はホーム・ネットワークからのメッセージの切り離しに応答していないかを検出する。
【課題を解決するための手段】
【０００７】
一実施例において、モニタリング・システムは、訪問先ネットワークでのローミングのアンチステアリングを検出する。モニタリング・システムは、訪問先ネットワークからホーム・ネットワークで受信したシグナリング・メッセージを捕捉する。シグナリング・メッセージは、ホーム・ネットワーク加入者をローミングすることによって訪問先ネットワークにアタッチする試みに対応する。モニタリング・システムは、アクティブなローミング加入者の数、ステアリングされたローミング加入者の数、訪問先ネットワークでアンチステアリングされたローミング加入者の数を見積る。モニタリング・システムは、次に、アクティブなローミング加入者、ステアリングされたローミング加入者及びアンチステアリングされたローミング加入者の見積り数を単独又は組合せで、予め選択された１つ以上のしきい値と比較する。単独又は他の見積り数と組合さった１つ以上の見積り数が、予め選択されたしきい値を超えると、モニタリング・システムは、ローミング活動の潜在的なアンチステアリングを識別する。
【０００８】
本発明の第１態様によれば、訪問先ネットワークでのローミングのアンチステアリングを検出する方法は；ホーム・ネットワークで受信した上記訪問先ネットワークでのローミング加入者からのシグナリング・メッセージを捕捉し；加入者毎に上記捕捉したメッセージを相関させ；上記訪問先ネットワークでのアクティブなローミング加入者の数を見積り；上記訪問先でのステアリングされたローミング加入者の数を見積り；上記訪問先ネットワークでのアンチステアリングされたローミング加入者の数を見積り；上記アクティブなローミング加入者、ステアリングされたローミング加入者及びアンチステアリングされたローミング加入者の見積り数を単独又は組合せて１つ以上の所定しきい値と比較し；上記１つ以上の見積り値が単独又は組合せでしきい値を超えたときにローミング活動の潜在的なアンチステアリングを識別する。
【０００９】
本発明の第２態様によれば、上記第１態様の方法は、更に、特定加入者が上記訪問先ネットワークで通信を成功裏に開始又は受信すると、アクティブなローミング加入者として特定ネットワーク加入者をカウントすることを特徴とする。
【００１０】
本発明の第３態様によれば、上記第２態様の方法は、上記訪問先ネットワークでの上記通信が音声コール、データ接続又はショート・メッセージ・サービス通信から選択された通信を含むことを特徴とする。
【００１１】
本発明の第４態様によれば、上記第１態様の方法は、更に、上記特定加入者に対して上記訪問先ネットワークから成功裏にアップデートしたロケーション・トランザクションを上記ホーム・ネットワークが実行しないと、ステアリングされたローミング加入者として特定加入者をカウントすることを特徴とする。
【００１２】
本発明の第５態様によれば、上記第４態様の方法は、システム障害、許可されないロー

ミング、データ損失、予期せぬデータ値コードから成るグループから選択された応答コードによって、失敗したアップデート・ロケーション・トランザクションが拒絶されると、ステアリングされたローミング加入者として特定加入者がカウントされることを特徴とする。

【００１３】

本発明の第６態様によれば、上記第１態様の方法は、更に、成功したアップデート・ロケーション・トランザクションが続く所定期間内に、特定加入者が失敗したアップデート・ロケーション・トランザクションのシーケンスを行うと、アンチステアリングされたローミング加入者として特定ネットワーク加入者をカウントすることを特徴とする。

【００１４】

本発明の第７態様によれば、上記第１態様の方法は、更に、特定加入者がアップデート・ロケーション・トランザクションのシーケンスを実行すると、アンチステアリングされたローミング加入者として特定ネットワーク加入者をカウントとし、各アップデート・ロケーション・トランザクションが所定のインターバルで離れており、上記シーケンスに上記所定インターバルで成功したアップデート・ロケーション・トランザクションが続くことを特徴とする。

【００１５】

本発明の第８態様によれば、上記第１態様の方法は、更に、所定期間内に上記訪問先ネットワークによる複数のトランザクション・シーケンスを上記特定加入者が実行すると、アンチステアリングされたローミング加入者として特定ネットワーク加入者をカウントすることを特徴とする。

【００１６】

本発明の第９態様によれば、上記第１態様の方法は、更に、少なくとも１つのアンチステアリング・ローミング加入者に関連したメッセージを含むプロトコル・トレースを発生することを特徴とする。

【００１７】

本発明の第１０態様によれば、ネットワーク・モニタリング・システムは；ホーム・ネットワーク及び１つ以上の訪問先ネットワークの間で交換されるメッセージを含むデータ・トラフィックをＳＳ７リンクから捕捉するのに適する少なくとも１つのＳＳ７インタフェースと；上記捕捉したデータ・トラフィックを蓄積するメモリと；上記訪問先ネットワークでのアクティブなローミング加入者の数を計算し、上記訪問先ネットワークでのステアリングされたローミング加入者の数を計算し、上記訪問先ネットワークでのアンチステアリングされたローミング加入者の数を計算し、上記アクティブなローミング加入者、ステアリングされたローミング加入者及びアンチステアリングされたローミング加入者の数を所定しきい値と比較し、上記比較に応じて上記訪問先ネットワークがローミング技術のアンチステアリングを用いているかを判断するのに適したプロセッサとを備えている。

【００１８】

本発明の第１１態様によれば、上記第１０態様のシステムは、上記データ・トラフィックが捕捉されると上記比較ステップをほぼ実時間で実行するのに上記プロセッサが適することを特徴とする。

【００１９】

本発明の第１２態様によれば、上記第１０態様のシステムは、上記メモリに蓄積された捕捉データ・トラフィックを用いて所定インターバルで上記比較ステップを実行するのに上記プロセッサが適することを特徴とする。

【００２０】

本発明の第１３態様によれば、上記第１２態様のシステムは、上記所定インターバルが操作者の選択した期間に対応することを特徴とする。

【００２１】

本発明の第１４態様によれば、上記第１２態様のシステムは、上記所定インターバルが捕捉データの所定量に対応することを特徴とする。

【００２２】
本発明の第１５態様によれば、上記第１０態様のシステムは、上記訪問先ネットワークのサービス・エリア内で動作するテスト・モバイル・ユニットを更に備え、上記テスト・モバイルは、上記モニタリング・システムに命令されるときに上記訪問先ネットワークにアタッチすると共に、上記訪問先ネットワークから受信したメッセージ・トラフィックを上記モニタリング・システムにレポートするのに適しているのを特徴とする。
【００２３】
本発明の第１６態様によれば、コンピュータが読出し可能な蓄積媒体がネットワーク・モニタリング・システムを制御するインストラクションを備えており；上記インストラクションは、実行の際にプロセッサにより；ホーム・ネットワークで受信した訪問先ネットワークからのシグナリング・メッセージを捕捉し；ローミング・ホーム・ネットワーク加入者が上記訪問先ネットワークにアタッチしようとする試みに上記シグナリング・メッセージが対応し；上記訪問先ネットワークでのアクティブなローミング加入者の数を見積り；上記訪問先でのステアリングされたローミング加入者の数を見積り；上記訪問先ネットワークでのアンチステアリングされたローミング加入者の数を見積り；上記アクティブなローミング加入者、ステアリングされたローミング加入者及びアンチステアリングされたローミング加入者の見積り数を単独又は組合せて１つ以上の所定しきい値と比較し；上記１つ以上の見積り値が単独又は組合せでしきい値を超えたときにローミング活動の潜在的なアンチステアリングを識別する。
【００２４】
本発明の第１７態様によれば、上記第１６態様のコンピュータが読出し可能な蓄積媒体は、更に、上記特定加入者が上記訪問先ネットワークでの通信を成功裏に開始するか受信すると、アクティブなローミング加入者として上記特定ネットワークの加入者をカウントし；上記訪問先ネットワークでの上記通信は、音声コール、データ接続又はショート・メッセージ・サービス通信から成るグループから選択された通信を含むことを特徴とする。
【００２５】
本発明の第１８態様によれば、上記第１６態様のコンピュータが読出し可能な蓄積媒体は、更に、特定加入者に対して上記訪問先ネットワークからの成功したアップデート・ロケーション・トランザクションを上記ホーム・ネットワークが実行しないと、ステアリングされたローミング加入者として上記特定加入者をカウントし；システム故障、許可されないローミング、データ損失及び予期せぬデータ値コードから成るグループから選択された応答コードにより、失敗したアップデート・ロケーション・トランザクションが拒絶されると、ステアリングされたローミング加入者として上記特定加入者がカウントされることを特徴とする。
【００２６】
本発明の第１９態様によれば、上記第１６態様のコンピュータが読出し可能な蓄積媒体は、更に；成功したアップデート・ロケーション・トランザクションが続く所定期間内に失敗したアップデート・ロケーション・トランザクションの試験を上記特定加入者が実行すると、アンチステアリングされたローミング加入者として特定ネットワーク加入者をカウントし；上記特定加入者がアップデート・ロケーション・トランザクションのシーケンスを実行すると、アンチステアリングされたローミング加入者として特定ネットワーク加入者をカウントし、各アップデート・ロケーション・トランザクションが所定のインターバルで離れており、上記シーケンスに上記所定インターバルで成功したアップデート・ロケーション・トランザクションが続き；所定期間内で上記訪問先ネットワークにより複数のトランザクション・シーケンスを上記特定加入者が実行すると、アンチステアリングされたローミング加入者として特定ネットワーク加入者をカウントし、上記トランザクション・シーケンスの各々が少なくとも１つのキャンセル・ロケーション・メッセージ及び少なくとも１つのアップデート・ロケーション・メッセージの交換を含むことを特徴とする。
【００２７】

本発明の第２０態様によれば、上記第１６態様のコンピュータが読出し可能な蓄積媒体は、更に、少なくとも１つのアンチステアリング・ローミング加入者に関連したメッセージを含むプロトコル・トレースを発生することを特徴とする。

【００２８】

本発明の第２１態様によれば、ネットワーク・モニタリング・システムは；ホーム・ネットワーク及び１つ以上の訪問先ネットワークの間で交換されるメッセージを含むデータ・トラフィックをＳＳ７リンクから捕捉するのに適する少なくとも１つのＳＳ７インタフェースと；上記捕捉したデータ・トラフィックを蓄積するメモリと；訪問先ネットワーク用の成功したローミングの数に対応するローミング変数を上記所定期間の初めにてゼロにリセットし、上記所定期間中に上記訪問先ネットワークにて個別の出て行くローミング加入者を追跡し、上記所定期間中に少なくとも１つの成功したサービスの試みを特定ローミング加入者が実行すると上記ローミング加入者をアクティブなローミング・サービス利用者として識別し、各アクティブなローミング・サービス利用者に対してローミング・サービス利用者変数の値を増分するのに適するプロセッサとを備える。

【００２９】

本発明の第２２態様によれば、上記第２１態様のネットワーク・モニタリング・システムは、更に、加入者のユーザ装置のＩＭＳＩ又はＭＩＳＩＤＮを用いてローミング加入者身元を決めることを特徴とする。

【００３０】

本発明の第２３態様によれば、上記第２１態様のネットワーク・モニタリング・システムは、上記所定期間が２４時間の期間であることを特徴とする。

【００３１】

本発明の第２４態様によれば、上記第２１態様のネットワーク・モニタリング・システムは、モバイル音声コールの発信、モバイル音声コールの終了、ＳＭＳメッセージの発信及びＳＭＳメッセージの終了から成るグループから、少なくとも１つの成功したサービスの試みを選択することを特徴とする。

【００３２】

よって、一般用語で本発明を説明することにより、添付図について説明を行う。

【図面の簡単な説明】

【００３３】

【図１】図１は、訪問先公衆モバイル・ネットワーク（Visited Public Mobile Network：ＶＰＭＮ）とユーザ装置（User Equipment：ＵＥ）との相互作用を説明する高レベルのブロック図である。

【図２】図２は、本発明の一実施例によるローミング活動のアンチステアリングを検出する処理を説明する流れ図である。

【発明を実施するための形態】

【００３４】

以下に添付図を参照して本発明を更に詳細に説明する。しかし、本発明は、多くの異なる形式で実施でき、ここでの説明の実施例に限定することを意図するものではない。むしろここでの開示が詳細且つ完全になるようにこれら実施例を提供し、当業者に本発明の範囲を充分に示すものである。当業者は、本発明の種々の実施例を用いることができよう。

【００３５】

図１は、訪問先公衆モバイル・ネットワーク（Visited Public Mobile Network：ＶＰＭＮ）１０２～１０４とユーザ装置（User Equipment：ＵＥ）１０１との相互作用を説明する高レベルのブロック図である。ＵＥ１０１は、ホーム公衆モバイル・ネットワーク（Home Public Mobile Network：ＨＰＭＮ）１０５であり、装置がそのホーム・エリア、領域又は国で動作するとき、無線サービスをＵＥ１０１に提供する。ＨＰＭＮ１０５が無線サービスを提供しないときは、ＵＥ１０１の如き加入者がローミングか、異なるエリア、領域又は国に出かけているときである。この状態にて、加入者は、他の公衆モバイル・ネットワークをサーチしなければならず、無線サービスを得るために他のネットワークにア

クセスしようとする。例えば、ＵＥ１０１は、ローミング・プロバイダをサーチする間に、３つのＶＰＭＮ１０２～１０４を検出する。ＵＥ１０１は、典型的には、ＶＰＭＮ１０２～１０４の信号強度を測定し、最強信号のＶＰＭＮに接続しようとする。ＵＥ１０１がＶＰＭＮの１つにアタッチすると、ＨＰＭＮ１０５は、ＵＥ１０１用の登録処理期間中にＶＰＭＮからの認証メッセージを受ける。ＵＥ１０１がローミングであり、特定ＶＰＭＮにアタッチしていることを、ＶＰＭＮからのアタッチ及び認証メッセージがＨＰＭＮ１０５に知らせる。

【００３６】

ＨＰＭＮ１０５は、ＨＰＭＮサービス・エリアの外側のエリア内の１つ以上の推奨ＶＰＭＮを有する。例えば、ＨＰＭＮ１０５は、ＶＰＭＮ１０２のパートナであり、ＨＰＭＮ１０５のローミング加入者をサポートする。ＶＰＭＮ１０２は、推奨課金レート又は進化したサービスをＨＰＭＮ１０５のローミング加入者に提供できる。その結果、ＨＰＭＮ１０５は、ＶＰＭＮサービス・エリア内でローミングしている間、ＵＥ１０１を含む加入者がＶＰＭＮ１０２を使用することを好む。ＵＥ１０１がＶＰＭＮ１０２にアタッチすると、ＨＰＭＮ１０５は、ＵＥ１０１用の登録処理期間中にＶＰＭＮからの認証メッセージを受ける。ＨＰＭＮ１０５は、ＵＥ１０１がパートナ又は優先のＶＰＭＮ１０２にアタッチしたと判断し、ＨＰＭＮ１０５は、認証データを提供して、ＵＥ１０１がＶＰＭＮ１０２により登録できるようにする。

【００３７】

ＵＥ１０１は、ＶＰＭＮ１０３が最強の信号であると判断し、ＶＰＭＮ１０３にアタッチしようとする。ＨＰＭＮ１０５は、ＵＥ１０１用の登録処理期間中にＶＰＭＮ１０３からの認証メッセージを受ける。ＨＰＭＮ１０５は、ＵＥ１０１が非推奨又は未知のＶＭＰＮにアタッチしたと判断する。ＨＰＭＮ１０５は、ＶＰＭＮ１０３と同じエリアでパートナＶＰＭＮ１０２がＵＥ１０１にサービスしているとも判断する。次に、ＶＰＭＮ１０３から切り離れ、他のＶＭＰＮを探し、特にパートナＶＭＰＮ１０２に再アタッチするように、ＨＰＭＮ１０５がＵＥ１０１に命令する。

【００３８】

特定のＶＰＭＮにアタッチするようにＨＰＭＮ１０５がＵＥ１０１に指示するか指示しようとする処理は、ローミングのステアリング（Steering of Roaming：ＳｏＲ）と呼ばれる。ローミングのステアリングは、ＨＰＭＮ１０５の如きホーム・ネットワークが用いる技術であり、推奨又はパートナ・ネットワーク（好ましくはＶＰＭＮ）と交換されるローミング・トラフィックのパーセントを制御するために、ＵＥ１０１の如き加入者用の外に向かうローミング・トラフィックを管理する。典型的には、ローミングのステアリングは、ホーム・ネットワークがサービスをしない異国に出かける加入者に適用する。例えば、無線（over-the-air：ＯＴＡ）ステアリング及びＳＳ７ノード・ベース・レダイレクションを含むいくつかの異なる方法で、ローミングのステアリングを達成できる。

【００３９】

ＯＴＡ動作において、ＵＥ１０１は、ＨＰＭＮ１０５が割り当てた推奨ネットワークのリストを維持する。ＵＥ１０１は、ローミングがＨＰＭＮ１０５から離れるとき、ＶＰＭＮ１０２の如き推奨ネットワークの１つに接続しようとする。推奨ネットワーク・リストは、ＧＳＭ（登録商標）ＭＡＰメッセージ、即ち、ＭＴＦＳＭ６３－（Ｕ）ＳＭデータ・ダウンロードをＵＥ１０１へ送るようにして、ＨＰＭＮ１０５によりアップデートできる。

【００４０】

ＳＳ７ノード・ベースのリダイレクションにおいて、ＵＥ１０１が訪問国でのＶＰＭＮ１０３の如き他のネットワークにアタッチするとき、モバイル・アプリケーション・パート（Mobile Application Part：ＭＡＰ）アップデート・ロケーション・メッセージは、ＶＰＭＮ１０３からＳＳ７ネットワーク１０６を介してＵＥ１０１用のホーム・ネットワーク１０５でのホーム・ロケーション・レジスタ（Home Location Resister：ＨＬＲ）１０７に送られる。ホーム・ネットワーク１０５内に配置されたステアリング・プラットホ

ーム１０８は、アップデート・ロケーション・メッセージを遮断し、発信されたメッセージからＶＰＭＮ１０３を識別する。ＶＰＭＮ１０３がＨＰＭＮ１０５用の推奨又はパートナ・ネットワークでなければ、ホーム・ネットワークは、そのネットワークから離れるようにローミング加入者をステアリングすることを望む。ステアリング・プラットホーム１０８は、アップデート・ロケーション・メッセージを拒否する。失敗したロケーション・アップデート手順は、ＵＥ１０１がＶＰＭＮ１０３から切り離されるようにし、次の利用可能なネットワークへのアタッチを試みる。ＵＥ１０１は、利用可能なネットワークを再びサーチし、ＶＰＭＮ１０３の後の次に最強の信号のネットワークにアタッチしようとする。推奨ＶＰＭＮ１０２からメッセージが来るまで、ＨＰＭＮ１０５及びステップ・プラットホーム１０８は、ＵＥ１０１用にアップデート・ロケーション・メッセージを拒否し続ける。

【００４１】

ＭＡＰアップデート・ロケーション・メッセージへの返信にて異なる応答コードを送ることができる。ステアリング・プラットホーム１０８によりこれらメッセージも用いて、異なるＶＰＭＮへＵＥ１０１をリダイレクションする。ステアリング・プラットホーム１０８は、ある応答コードを用いて、アップデート・ロケーション・メッセージを拒否し、他のＶＰＭＮへローミング加入者をステアリングする。３ＧＰＰ_ＧＳＭ（登録商標）_ＭＡＰ規格において、例えば、アップデート・ロケーション・メッセージに応答するために許された値は、システム障害、許可されないローミング、データ損失及び予期せぬデータ値である。

【００４２】

ＵＥ１０１がＶＰＭＮ１０４の如きあるローミング・プローブにアタッチするとき、訪問先ネットワークは、ホーム・ネットワーク１０５が実行しようとしているいかなるローミングのステアリングに対抗しようとする。ローミングのステアリングを対抗又は拒否する処理は、ローミングのアンチステアリング（アンチＳｏＲ）と呼ばれる。

【００４３】

非推奨ＶＰＭＮがローミングのアンチステアリングを用いて、ＨＰＭＮからのローミングのステアリングを無視する。非推奨ＶＰＭＮ１０４は、例えば、ローミング・トラフィックを捕捉するためのローミング加入者の身元と対応収益とを維持しようとするかもしれない。その代わりに、非推奨ＶＰＭＮ１０４は、推奨ＶＰＭＮ１０２の如き競合ネットワークで生じる収益を防ぐか最小にしようとするかもしれない。

【００４４】

訪問先ネットワークは、異なる形式のローミングのアンチステアリングを用いて、ローミングのステアリングの異なる形式に対抗する。ＳＳ７ノード・ベースのリダイレクション・メカニズムを無視するため、例えば、アンチＳｏＲ方法は、ＳＳ７シグナリングをあてにし、２つのメイン・カテゴリである強制手動モード又は周期的回復に入る。強制手動モードにおいて、ＶＰＭＮアンチＳｏＲプラットホームは、ＳｏＲプラットホームがアップデート・ロケーション・メッセージの拒否を止めるまで、ＨＰＭＮへの連続的アップデート・ロケーションを発生する。ある数のアップデート・ロケーションを受信した後、ＨＰＭＮＳｏＲプラットホームは、加入者が手動で特定ネットワークを選択しようとしていると仮定する。周期的回復において、非推奨ＶＰＭＮがＭＡＰキャンセル・ロケーションをＨＰＭＮから受信するとき、ＶＰＭＮのアンチＳｏＲプラットホームは、ＭＡＰアップデート・ロケーションを出す。キャンセル・ロケーションであるアップデート・ロケーション・パターンが半連続シーケンスにて繰り返し、（非常に短時間のウィンドウを除いて）ＵＥがモバイル終了又はモバイル発信サービスを実行できない。いくつかの場合において、ＶＰＭＮにより他のシグナリングもサポートされて、ローミング加入者に対するサービス途絶のリスクを低減する。非推奨ＶＰＭＮがこれらの方法を単独又は組合せで用いて、ホーム・ネットワークでのローミングのステアリングの活動に対抗する。一実施例において、非推奨ＶＰＭＮ１０４は、ＶＰＭＮ１０４及びＨＰＭＮ１０５の間のＳＳ７トラフィックをモニタするローミングのアンチステアリング・プラットホーム１１０を有する。

【００４５】
加入者が用いるＵＥ１０１は、ローミング期間中に特定のＶＰＭＮを用いることを望む。このオプションを加入者に提供するために、ＨＰＭＮ１０５は、ＵＥ１０１が手動モードで動作することを認め、加入者は、どの訪問先ネットワークを用いるかを手動で選択する。ローミング・プラットホーム１１０のアンチステアリングは、ＵＥ１０１のこの能力を活用する。アンチＳｏＲプラットホーム１１０は、連続アップデート・ロケーション・メッセージを発生し、これらがＵＥ１０１で開始されるようにこれらをＨＰＭＮ１０５に送ることにより、強制手動ノードにて動作する。ローミングのステアリング・プラットホーム１０８は、アップデート・ロケーション・メッセージを最初に拒否するが、その理由は、これらが非推奨訪問先ネットワークから発信されるためである。しかし、ローミングのステアリング１０８は、加入者が特定ネットワークを手動で選択しようとしているという仮定でアップデート・ロケーション・メッセージの拒否を結局は停止する。例えば、１５秒間隔で４つのアップデート・ロケーション・メッセージが受信された後、ＨＰＭＮがアップデート・ロケーションの拒否を停止するということを３ＧＰＰＴＳ２４．００８が規定している。この方法において、加入者の知識がなくても、ＶＰＭＮ１０４は、ＵＥ１０１からのメッセージを成功裏に模倣して、パートナＶＰＭＮ１０２の如き推奨ＶＰＭＮにＵＥ１０１をＨＰＭＮがリダイレクションすることを防ぐ。その結果、加入者は、推奨訪問先ネットワークで利用できるよりも高速レート又は準標準サービスを非推奨ＶＰＭＮ１０４で受けることができる。

【００４６】
ローミング加入者が競合ネットワークにアタッチするのを防ぐだけで、非推奨ＶＰＭＮは、加入者がそのネットワークにうまくアタッチするかを配慮しない。ローミングのアンチステアリング・プラットホーム１１０は、周期的な回復を用いて、ＵＥ１０１が他の訪問先ネットワークにアタッチするのを妨げる。ＵＥ１０１がＶＰＭＮ１０４にアタッチしようとするとき、上述のようにアップデート・ロケーション・メッセージをＨＰＭＮ１０５に送る。ＶＰＭＮ１０４が推奨ＶＰＭＮでないため、ＵＥ１０１が他の訪問先ネットワークにアタッチするように強制しようとして、ＳｏＲプラットホーム１０８は、キャンセル・ロケーション又は他のＭＡＰメッセージをＶＰＭＮ１０４に送る。非推奨ＶＰＭＮ１０４がＨＰＭＮ１０５からキャンセル・ロケーション・メッセージを受信するとき、アンチＳｏＲプラットホーム１１０は、他のＭＡＰアップデート・ロケーションをＨＰＭＮ１０５に再度出す。ＳｏＲプラットホーム１０８は、キャンセル・ロケーション・メッセージを再度出す。アップデート・ロケーション／キャンセル・ロケーション・パターンは、連続又は準連続シーケンスにてアンチＳｏＲプラットホーム１１０により繰り返される。その結果、ＵＥ１０１は、いかなるモバイル終了又はモバイル発信サービスも達成できない。よくても、ＵＥ１０１は、アンチＳｏＲ及びＳｏＲプラットホームからのアップデート・ロケーション／キャンセル・ロケーションの交換の間で、非常に短時間のウィンドウの間だけサービスを受ける。

【００４７】
ＳＳ７モニタリング・システムを用いて、上述の如きローミングのアンチステアリングのアタックを検出できる。一実施例において、受動モニタリング・システムにより備えられたＨＰＭＮは、全ての国際的なＭＡＰシグナリングを連続的にモニタする。ＭＡＰシグナリングを分析することにより、モニタリング・システムは、訪問先ネットワークでのアンチＳｏＲ動作を自動的に検出できる。

【００４８】
受動モニタリング・システムは、１つ以上のネットワーク・モニタリング・プローブ１１１を備える。図１に示すように、プローブ１１１は、ホーム・ネットワーク１０５で１つ以上のインタフェース又は相互接続リンクに結合される。プローブ１１１は、ステアリング・プラットホーム１０８からＨＬＲ１０７及びＶＰＭＮ１０２～１０４へのリンクに加えて、ホーム・ネットワーク１０５内の任意のインタフェース又は相互接続リンクにも結合できることが理解できよう。簡単にするため、図１は、ネットワーク１０５内の全て

のモニタ可能なリンクを示すわけではない。プローブ１１１は、ネットワーク動作を中断することなく、インタフェースからのメッセージ・トラフィックを受動的に捕捉する。

【００４９】

図１に示すモニタリング・プローブ１１１は、ホーム・ネットワーク１０５での１つ以上のモニタリング・プローブを代表する。各モニタリング・プローブは、ネットワークでの１つ以上のリンクからのトラフィックを捕捉する。さらに、１つ以上のプローブ１１１が、あるリンクのトラフィックを捕捉できる。多数のプローブ１１１を用いれば、これらプローブを相互接続して、捕捉したトラフィックを共有及び交換できる。モニタリング・システムは、大量のシグナリング・トラフィックを扱うのに最適化された分布アーキテクチャを利用できる。モニタリング・システム及びプローブ１１１は、実時間、ネットワークにわたる全てのトランザクションのマルチプロトコル追跡、ベアラ／サービス加入者の付勢、リンク／インタフェース、及びノード状態モニタリングを提供できる。一実施例において、プローブ１１１は、テクトロニクス社製アイリス・アナライザ・ツールセット・アプリケーション並びにＳｐＩプローブ及びＧ１０プローブを含むＧｅｏＰｒｏｂｅプラットホームの一部でもよい。モニタリング・プローブは、ＳＳ７リンクから捕捉したデータ・トラフィックを分析するためのソフトウェア・アプリケーションを実行するプロセッサと、ソフトウェア・アプリケーション・インストラクション及び捕捉データ・トラフィックを蓄積するメモリとを備えている。ここで開示し記載した技術を用いて、ローミングのアンチステアリングを検出するために他のネットワーク・モニタリング装置又はプローブを用いることができることが理解できよう。

【００５０】

図２は、本発明の一実施例によるローミングのアンチステアリング動作を検出する処理を示す流れ図である。ホーム・ネットワーク内のリンクからのデータを捕捉するモニタリング・システムは、図２に示す処理を実行して、ホーム・ネットワークの加入者に対してローミングのアンチステアリング技術を訪問先ネットワークが適用するときに、検出を行う。ステップ２０１において、モニタリング・システムは、一実施例において、「インジケータ番号１」と指定された第１パラメータを見積る。これは、固有のアクティブ・ローミング・サービス利用者の数に対応する。所定期間にわたって訪問先ネットワークでローミングするホーム・ネットワーク加入者の数がどれくらいかの見積りが、インジケータ番号１である。

【００５１】

ステップ２０２において、モニタリング・システムは、一実施例において、「インジケータ番号２」と指定された第２パラメータを見積る。これは、固有のステアリング・ローミングの数に対応する。所定期間にわたってホーム・ネットワークが開始したローミング活動のステアリングを示すシグナリング・トラフィックに関連するホーム・ネットワーク加入者の数がどれくらいであるかの見積りが、インジケータ番号２である。ステップ２０３において、モニタリング・システムは、一実施例において、「インジケータ番号３」と指定された第３パラメータを見積る。これは、固有のアンチステアリング・ローミングの数に対応する。所定期間にわたって訪問先ネットワークが開始したローミング活動のアンチステアリングを示すシグナリングに関連したホーム・ネットワーク加入者の数がどれくらいかであるかの見積りが、インジケータ番号３である。

【００５２】

ステップ２０４にて、モニタリング・システムは、一実施例において、「インジケータ番号４」と指定された第４パラメータを見積る。これは、ホーム・ネットワークＨＬＲの潜在的エリアシングに対応する。訪問先ネットワークからのトラフィックに応答するときに、訪問先ネットワークでのアンチステアリング・プラットホームがホーム・ネットワークＨＬＲのアドレスを用いることを示すシグナリング・トラフィックの量の見積りが、インジケータ番号４である。

【００５３】

インジケータ番号１～４パラメータは、特定の訪問先ネットワーク又は訪問先ネットワ

ークのグループに関連する。インジケータ番号１～４パラメータは、分、時、日又は他の時間での選択された期間の如き特定期間にわたり検出された活動に対応する。

【００５４】

ステップ２０５において、モニタリング・システムは、ローミング活動の可能なアンチステアリングに関する警告を発生する。設定可能なしきい値と、インジケータ番号１～４パラメータ値との比較に基づいて、アンチＳｏＲ警告を決める。ホーム・ネットワーク・サービス・プロバイダの如きユーザは、インジケータ番号１～４パラメータの各々に対するしきい値を確立又は選択できる。これらしきい値は、一般的であり、全ての訪問先ネットワークに適用されるか、１つ以上の特定訪問先ネットワーク用に特に選択される。個別のインジケータ及び／又は２つ以上のインジケータの種々の組合せの値を用いて、潜在的なアンチＳｏＲ活動を識別する。

【００５５】

ステップ２０６において、モニタリング・システムは、詳細なプロトコル・トレースを発生して、特定訪問先ネットワークでの任意の検出可能なローミングのアンチステアリング活動を確認する。

【００５６】

処理のステップ２０１～２０４は、同時に及び／又はシーケンスで実行できることが理解できよう。これらステップは、任意の順序で実行でき、１回又は繰り返し実行できることが更に理解できよう。図２の処理は、モニタリング・システムで利用可能な処理能力及びリソースに応じて連続的に実行できる。インジケータの連続及び同時のモニタリングにより、モニタリング・システムは、アンチＳｏＲ活動のほぼ実時間の警告を発生できる。

【００５７】

代わりに、ホーム・ネットワーク及び訪問先ネットワークの間のトラフィック・トレースを時間と伴に捕捉する。選択したインターバルで、又は所望量のデータを捕捉したときに、モニタリング・システムは、捕捉したトラフィックをバッチ・モードで分析して、アンチＳｏＲ活動が前の期間に生じたかを判断する。アンチＳｏＲ活動の実時間及び経過的な両方の検出は、ホーム・ネットワーク・サービス・プロバイダに対する潜在的なビジネス価値がある。ホーム・ネットワーク・サービス・プロバイダは、技術的、商業的又は法務的な方法を用いて、訪問先ネットワークのアンチＳｏＲに対抗しようとする。しかし、アンチＳｏＲ活動に対するホーム・ネットワーク・サービス・プロバイダが採る対策には、対策が有効になるまでに、長くなくても、日又は週の如きある程度の期間がかかる。

【００５８】

［インジケータ番号１の見積り：固有のアクティブなローミング・サービス利用者の数］

ホーム・ネットワークでのＳＳ７リンクから受動的に捕捉したデータを用いて、ネットワーク・モニタリング・システムが、所定訪問先ネットワーク用の固有の成功したローミング・サービス利用者の数を見積もることができる。一実施例において、モニタリング・システムは、以下の処理を実行する。

１．各日の開始にて、選択した訪問先ネットワーク用のインジケータ番号１の値をゼロにリットする。

２．訪問先ネットワークにて、外に向かうローミング加入者（subscriber：ＳＵＢ）の各々を追跡する。例えば、ユーザ装置のＩＭＳＩ又はＭＳＩＳＤＮを用いて、加入者の身元を判断できる。

３．その日の終わりにて、各ＳＵＢ用のトラフィックを精査する。次の動作、即ち、モバイル発信音声コール、モバイル終了音声コール、モバイル発信ＳＭＳ及びモバイル終了ＳＭＳの中で少なくとも１つの成功したサービスの試みをＳＵＢが実行したならば、特定のＳＵＢをアクティブ・ローミング・サービス利用者としてカウントし、その日に訪問先ネットワーク用のインジケータ番号１の値を増分する。

【００５９】

［インジケータ番号２の見積り：固有のステアリングされたローミング・サービス利用者の数］

以下の処理を用いて、所定訪問先ネットワーク用の固有のステアリングされたローミング・サービス利用者の数をモニタリング・システムにより見積もることができる。
１．各日の開始にて、選択された訪問先ネットワーク用のインジケータ番号２の値をゼロにリセットする。
２．訪問先ネットワークにて、外に向かうローミング加入者（ＳＵＢ）の各々を追跡する。例えば、ユーザ装置のＩＭＳＩ／ＭＳＩＳＤＮを用いて、加入者の身元を判断できる。
３．その日の終わりにて、各ＳＵＢのトラフィックを精査する。次の条件の両方が満足すれば、特定のＳＵＢをステアリングされたローミング・サービス利用者としてカウントし、その日の訪問先ネットワーク用のインジケータ番号２の値を増分する。
ａ）訪問先ネットワークからの成功しないＭＡＰアップデート・ロケーション・トランザクションをそのＳＵＢが実行する。
ｂ）ＳＵＢからの全ての失敗したＭＡＰロケーション・トランザクションが、所定リスト内で識別された応答コードにより拒否される。応答コード・リストは、設定可能であり、例示又はディフォルトの実施例において、システム障害、許されないローミング、データ損失及び予期せぬデータ値であるコードを含む。応答コード・リストは、各訪問先ネットワークに対して異なった構成となる。

【００６０】

インジケータ番号２は、ステアリングされたローミング・サービス利用者の正確なカウントを提供できない。これは、異なる訪問先ネットワークにローミング加入者をステアリングするのにステアリング・プラットホームが用いた応答コードを、実際のネットワーク又は加入の問題をレポートするのにホーム・ネットワーク自体が用いるためである。しかし、インジケータ番号２の値は、アンチＳｏＲ活動の発見的検出の役割を果たす関連情報を提供する。

【００６１】

［インジケータ番号３の見積り：固有のアンチステアリングされたローミング・サービス利用者の数］

所定訪問先ネットワーク用の固有のアンチステアリングされたローミング・サービス利用者の数は、以下の条件を用いてモニタリング・システムにより見積もることができる。
１．各日の開始にて、選択された訪問先ネットワーク用のインジケータ番号３の値をゼロにリセットする。
２．訪問先ネットワークにて外に向かうローミング加入者（ＳＵＢ）の各々を追跡する。加入者の身元は、例えば、ユーザ装置のＩＭＳＩ／ＭＳＩＳＤＮを用いて判断できる。
３．その日の終わりにて、各ＳＵＢ用のトラフィックを精査する。以下の条件の少なくとも１つを満足したならば、特定のＳＵＢをアンチステアリングされたローミング・サービス利用者としてカウントし、その日の訪問先ネットワーク用のインジケータ番号３の値を増分する。
ａ）その特定ＳＵＢが、t_1秒の期間中に、訪問先ネットワークからのｎ個のＭＡＰアップデート・ロケーション・トランザクションの少なくとも１個のシーケンスを実行する。ここでは、最初のｎ－１回のトランザクションが応答コードで失敗し、最後のトランザクションが成功する。t_1及び／又はｎは、設定可能である。応答コードは、所定又は設定可能なリストにて任意のＭＡＰ応答コードである。例示的な実施例において、t_1のディフォルト値が２０秒であり、ｎの値が５であり、応答コードの設定可能なリストが次のコードを含んでいる。すなわち、システム障害、許可されないローミング、データ損失、及び予期せぬデータ値である。ＭＡＰ応答コードは、各訪問先ネットワークで異なって構成される。
ｂ）この特定ＳＵＢは、訪問先ネットワークからのｎ個のＭＡＰアップデート・ロケーション・トランザクションの少なくとも１個を実行する。ここで、ＭＡＰアップデート・ロケーションの試みは、最短がt_2秒で最長がt_3秒だけ離れた間隔である。また、最初のｎ－１回のトランザクションが応答コードＲＣで失敗し、最後のトランザクションが成功する。t_2、t_3の値が設定可能である。例示的な実施例において、t_2のディフォルト

値が３５秒であり、t_3のディフォルト値が４０秒であり、ｎのディフォルト値が５である。応答コードは、所定又は設定可能なリストにて任意のＭＡＰ応答コードである。例示的な実施例において、応答コードの構成可能なリストは、システム障害、許可されないローミング、データ損失、及び予期せぬデータ値を含んでいる。
ｃ）その特定ＳＵＢは、１時間の期間にてＭＡＰ手順の少なくともｍ回のシーケンスを実行する。ここで、各シーケンスは、訪問先ネットワークへのＭＡＰキャンセル・ロケーションにより開始し、訪問先ネットワークからのＭＡＰアップデート・ロケーションにより終了する。各シーケンスに含まれるＭＡＰ手順と、そのシーケンス内の引き続く手順の間の時間インターバルは、設定可能である。一実施例において、ディフォルトの構成は、２０秒間隔未満で離れたＭＡＰアップデート・ロケーション・トランザクション及びＭＡＰキャンセル・ロケーションを備えたシーケンスである。ｍの値は、設定可能である。一実施例において、ｍ＝２のディフォルト値を用いる。

【００６２】

インジケータ番号３は、アンチステアリング・ローミングの正確なカウントを提供しない。これは、アンチＳｏＲプラットホームでなく加入者又はユーザ装置が、ネットワークの選択を手動強制するためである。これは、インジケータ番号３の下でカウントされるＭＡＰ手順のシーケンスを含むことができる。さらに、アンチＳｏＲの動きは、タイミング及びシグナリングの流れの観点からの変動を含み、上述の処理を用いて、検出を潜在的に避けることができる。しかし、インジケータ番号２の値は、アンチＳｏＲ活動の発見的な検出での役割を果たす関連情報を提供する。

【００６３】

［インジケータ番号４の見積り：訪問先ネットワークＨＬＲの潜在的エリアシング］

アンチステアリング・プラットホームは、訪問先ネットワークＨＬＲのアドレスを用いて、訪問先ネットワークに応答する。これが生じると、モニタリング・システムは、応答のみのＭＡＰトランザクションをレポートする。インジケータ番号４の値は、応答のみのトランザクションの数をカウントする。インジケータ番号４を計算するのに用いる応答のみのトランザクションのリストは、設定可能であり、一実施例においては、アップデート・ロケーション／挿入加入者データ（Insert Subscriber Data）がディフォルトである。

【００６４】

［ローミングのアンチステアリングの可能な存在での警告の発生］

ローミングの可能なアンチステアリングの指示が検出されると、モニタリング・システムは、インジケータ番号１～４に基づいて警告を発生する。

【００６５】

上述のインジケータ番号３の規則３に基づいてモニタリング・システムにより、ほぼ実時間の警告が発生される。モニタリング・システムでの処理パワーが充分ならば、システムは、この規則を連続的に評価でき、１つのＳＵＢが規則３の第１又は第２条件のいずれかに一致したときに、警告を発生できる。

【００６６】

インジケータ番号４を用いて、モニタリング・システムは、ほぼ実時間の警告も発生する。インジケータ番号４の値が設定可能又は現在の時間インターバル内の設定可能又はプリセットのしきい値に達すると、モニタリング・システムは、訪問先ネットワークがアンチＳｏＲを用いていると判断する。

【００６７】

一実施例において、モニタリング・システムは、以下のアプローチによる如くインジケータの組合せを用いて、アンチＳｏＲレポートを発生できる。
もし、（インジケータ番号２／（インジケータ番号１＋インジケータ番号２））＜Ｘで
且つ（インジケータ番号３／インジケータ番号２）＞Ｙならば、
アンチＳｏＲ活動をレポートする。

【００６８】

最初の式（インジケータ番号２／（インジケータ番号１＋インジケータ番号２））は、

ステアリングされたローミング加入者の総数の分数として、訪問先ネットワークによるステアリングの効率を計っている。

【００６９】

２番目の式（インジケータ１／インジケータ２）は、ステアリングの効果に対するアンチＳｏＲの効果を計っている。

【００７０】

Ｘ及びＹの値は、設定可能であり、各訪問先ネットワーク用に個別に選択される。Ｘ及びＹは、訪問先ネットワーク用のステアリング・プラットホームの構成と、ステアリングされた加入者の要求パーセントに基づく。校正期間を用いて、Ｘ及びＹの値を選択する。

【００７１】

インジケータ番号１及びインジケータ番号２は、発見的アプリケーションで単に見積もることができ、これは、可能なアンチＳｏＲの必要性を確認する。かかる更なる確認は、訪問先ネットワークが法務的又は商業的活動を行う前に、必要である。

【００７２】

アンチＳｏＲの確認をテスト・モビリティで得る。例えば、テスト・モバイル１１２を１つ以上のＶＰＭＮ１０２～１０４用のカバレージ・エリアシング内に配置する。訪問先ネットワーク１０５又はモニタリング・システム１１１は、リンク１１３を介してテスト・モバイル１１２と通信を行うが、これは、ＳＳ７シグナリング、インターネット接続、又は他の任意の通信方法である。訪問先ネットワーク１０５又はモニタリング・システム１１１は、ＶＰＭＮ１０４の如き選択された訪問先ネットワークにアタッチすることをテスト・モバイル１１２に指示する。アタッチ・メッセージがＶＰＭＮ１０４からホーム・ネットワーク１０５に送られるとき、ステアリング・プラットホーム１０８は、テスト・モバイル１１２を他のＶＰＭＮにステアリングしようとして、アップデート・ロケーション・メッセージを拒否する。ＶＰＭＮ１０４がアンチＳｏＲを用いていれば、アップデート・ロケーション・メッセージが拒否されたことをテスト・モバイル１１２に通知しない。ホーム・ネットワーク１０５及び／又はモニタリング・システム１１１がテスト・モバイル１１２へのバック・チャネル１１３接続を有するので、これらは、何のメッセージが実際に送られテスト・モバイル１１２で受信されたかをモニタできる。ホーム・ネットワーク１０５のインストラクションに基づいて送信又は受信された期待メッセージと実際のメッセージとを比較できる。アップデート・ロケーション又はキャンセル・ロケーション・メッセージが期待されたように伝送されないなどのように、実際のメッセージが期待メッセージと一致しなければ、アンチＳｏＲ活動を確認できる。

【００７３】

［何が検出されたかを確認するための詳細プロトコル・トレースの発生］

モニタリング・システムは、データ記録として、コール捕捉したＭＡＰシグナリング・トラフィックのログをとり、完全なプロトコル・トレースを発生する能力がある。モニタリング・システムのアンチＳｏＲ検出処理が警告を発生するとき、それは、加入者の検出されたＩＭＳＩ／ＭＳＩＳＤＮのリストも提供する。このリストを、プロトコル・トレース質問及び履歴的コール・トレース・アプリケーションに用いることができる。検出されたＩＭＳＩ／ＭＳＩＳＤＮに対応するユーザ装置用に詳細なプロトコル・トレースを発生して、インジケータが示唆したようにアンチＳｏＲが生じたかを確認できる。

【００７４】

本発明の多くの変更及び他の実施例が当業者には想定され、本発明は、上述及び添付図に示す利点を有する。よって、本発明は、開示した特定実施例に限定されないことを理解すべきである。特定の用語をここでは用いたが、これらは、汎用且つ説明のためのみであり、限定の目的ではない。

【符号の説明】

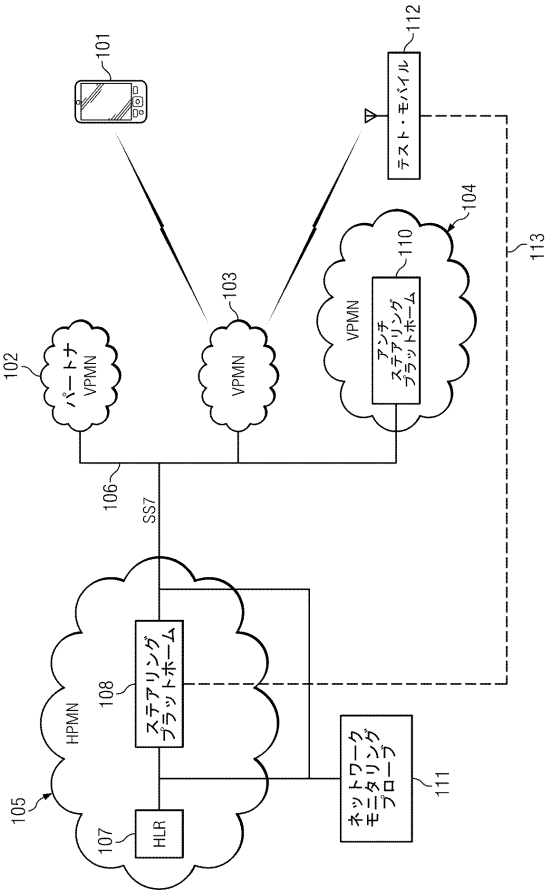
【００７５】

１０１：ユーザ装置（ＵＥ）

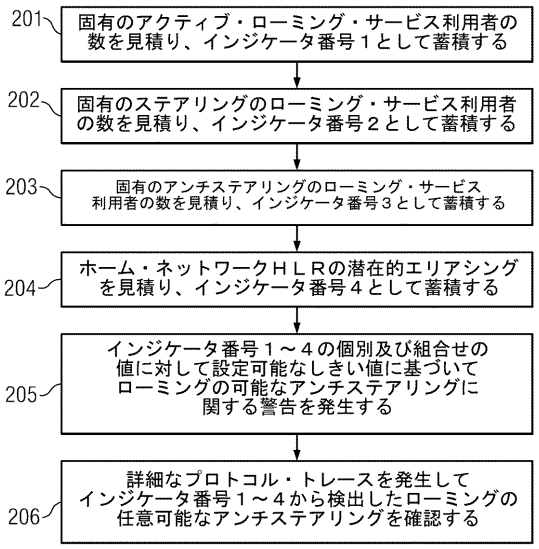
１０２；訪問先公衆モバイル・ネットワーク（ＶＰＭＮ）

１０３：ＶＰＭＮ
１０４：ＶＰＭＮ
１０５：ＨＰＭＮ
１０６：ＳＳ７ネットワーク
１０７：ＨＬＲ
１０８：ステアリング・プラットホーム
１１０：ローミング・プラットホーム
１１１：モニタリング・プローブ（アンチＳｏＲプラットホーム）
１１２：テスト・モバイル

【図１】



【図２】



フロントページの続き

(72)発明者　ダニエル・ポール・ルッソ
アメリカ合衆国　テキサス州　７５２１４　ダラス　シラキュース・ドライブ　７３２０
(72)発明者　サメー・エム・ヤマニー
アメリカ合衆国　テキサス州　７５０９３　プラノ　エヴァ　ピーエル．４７０１

Ｆターム(参考) 5K067 AA21 EE02 EE10 EE16 FF02 HH22 JJ64

【外国語明細書】

【TITLE OF INVENTION】 A method for detecting anti-steering of roaming on a visited network, a network monitoring system and a computer-readable storage medium

【TECHNICAL FIELD】

【０００１】

This invention relates, in general, to monitoring signaling between home and visited public mobile networks and, more specifically, to determining if a visited network is rejecting steering of roaming by the home network.

【BACKGROUND ART】

【０００２】

A mobile service provider typically provides wireless coverage in a designated geographical area, such as a particular country or one or more Metropolitan Service Area (MSA). When the service provider's subscribers require mobile service within these areas, the subscribers' mobile phone or user equipment searches for and attaches to the service provider's network. When a subscriber travels outside the service provider's designated coverage area, the subscriber's mobile phone is considered to be roaming and must attach to another service provider's mobile network - a visited network - to obtain service. The visited network exchanges information with the home network when the subscriber attaches to verify that the subscriber's mobile phone is a valid device. If an authentication message exchange is successful, the roaming subscriber obtains service from the visited network.

【０００３】

For example, a subscriber of a U.S.-based mobile network may travel to Europe. To obtain mobile service while in Europe, the U.S.-based subscriber's mobile phone must look for and attempt to attach to a European service provider's mobile network. The roaming mobile device may detect multiple potential visited networks. Typically, the mobile device will attach to the visited network having the strongest signal.

【０００４】

Often, a home mobile service provider will enter into contractual agreements with preferred foreign service providers that provide coverage in areas outside the home service area. Such

contracts may provide, for example, lower billing rates and/or a guaranteed class of service for roaming subscribers from the home network. Accordingly, the home network service provider usually wants its subscribers' roaming mobile devices attach to a preferred foreign service provider. To accomplish this, the home network uses Steering of Roaming (SoR) in an attempt to guide its subscribers' mobile devices to the preferred visited networks. In order to maintain the roaming subscriber on its network, or to prevent the roaming subscriber's from using another visited network, some non-preferred visited networks employ Anti-Steering of Roaming (Anti-SoR) techniques.

【PRIOR ART DOCUMENTS】

【０００５】

【PATENT DOCUMENTS】

【PATENT DOCUMENT 1】 Japanese Patent Application Publication No. 2007-28223

【PATENT DOCUMENT 2】 WO2002/013567(Japanese translation publication no.2004-506359)

【SUMMARY OF THE INVENTION】

【PROBLEMS TO BE SOLVED BY THE INVENTION】

【０００６】

A monitoring system analyzes signaling traffic between a visited public mobile network and a home public mobile network to determine if the visited network is using anti-steering of roaming techniques against the home network's subscribers. The monitoring system may detect, for example, whether the visited network is emulating a manual detach by the subscriber or is not responding to detach messages from the home network.

【MEANS FOR SOLVING THE PROBLEMS】

【０００７】

In one embodiment, a monitoring system detects anti-steering of roaming on a visited network. The monitoring system captures signaling messages received at a home network from a visited network. The signaling messages correspond to attempts by roaming home network subscribers

to attach to the visited network. The monitoring system estimates a number of active roaming subscribers, a number of steered roaming subscribers, and a number of anti-steered roaming subscribers on the visited network. The monitoring system then compare the estimated numbers of active roaming subscribers, steered roaming subscribers, and anti-steered roaming subscribers alone or in combination to one or more preselected thresholds. If one or more of the estimated numbers, either alone or in combination with other estimated numbers, exceed a preselected threshold, then the monitoring system identifies potential anti-steering of roaming activity.

【０００８】

According to a first aspect of this invention, a method for detecting anti-steering of roaming on a visited network, comprises:

capturing signaling messages received at a home network from roaming subscribers on the visited network;

correlating the captured messages on a per-subscriber basis;

estimating a number of active roaming subscribers on the visited network;

estimating a number of steered roaming subscribers on the visited network;

estimating a number of anti-steered roaming subscribers on the visited network;

comparing the estimated numbers of active roaming subscribers, steered roaming subscribers, and anti-steered roaming subscribers alone or in combination to one or more preselected thresholds; and

identify potential anti-steering of roaming activity if one or more of the estimated numbers alone or in combination exceed a preselected threshold.

【０００９】

According to a second aspect of this invention, the method of the first aspect is characterized in that the method further comprises:

counting a particular network subscriber as an active roaming subscriber if the particular subscriber successfully initiated or received a communication on the visited network.

【００１０】

According to a third aspect of this invention, the method of the second aspect is characterized in that the communication on the visited network comprises a communication selected from the group consisting of a voice call, a data connection, or a short message service communication.

【００１１】

According to a fourth aspect of this invention, the method of the first aspect is characterized in that the method further comprises:

counting a particular subscriber as a steered roaming subscriber if the home network did not perform any successful update location transactions from the visited network for the particular subscriber.

【００１２】

According to a fifth aspect of this invention, the method of the fourth aspect is characterized in that the particular subscriber is counted as a steered roaming subscriber if a group of failed update location transactions were rejected with a response code selected from the group consisting of System Failure, Roaming Not Allowed, Data Missing, and Unexpected Data Value codes.

【００１３】

According to a sixth aspect of this invention, the method of the first aspect is characterized in that the method further comprises:

counting a particular network subscriber as an anti-steered roaming subscriber if the particular subscriber performed a sequence of failed update location transactions within a predetermined period of time followed by a successful update location transaction.

【００１４】

According to a seventh aspect of this invention, the method of the first aspect is characterized in that the method further comprises:

counting a particular network subscriber as an anti-steered roaming subscriber if the particular subscriber performed a sequence of update location transactions wherein each update location transaction is spaced within a predetermined interval and wherein the sequence is followed by a successful update location transaction with the predetermined interval.

【００１５】

According to an eighth aspect of this invention, the method of the first aspect is characterized in that the method further comprises:

counting a particular network subscriber as an anti-steered roaming subscriber if the particular subscriber performed a plurality of transactions sequences with the visited network within a predetermined period of time, the transaction sequences each comprising an exchange of at least one cancel location message and at least one update location message.

【００１６】

According to a ninth aspect of this invention, the method of the first aspect is characterized in that the method further comprises:

generating a protocol trace comprising messages associated with at least one anti-steer roaming subscriber.

【００１７】

According to a tenth aspect of this invention, a network monitoring system, comprises:

at least one SS7 interface adapted to capture data traffic from SS7 links, the data traffic comprising messages exchanged between a home network and one or more visited networks;

a memory storing the captured data traffic;

a processor adapted to

calculate a number of active roaming subscribers on the visited network;

calculate a number of steered roaming subscribers on the visited network;

calculate a number of anti-steered roaming subscribers on the visited network;

compare the numbers active roaming subscribers, steered roaming subscribers, and anti-steered roaming subscribers to predetermined thresholds; and

determine whether the visited network is employing anti-steering of roaming techniques based upon the comparison.

【００１８】

According to an eleventh aspect of this invention, the system of tenth aspect is characterized in that the processor is adapted to perform the compare step in near real-time as the data traffic is captured.

【００１９】

According to a twelfth aspect of this invention, the system of tenth aspect is characterized in that the processor is adapted to perform the compare step at preselected intervals using captured data traffic stored in the memory.

【００２０】

According to a thirteenth aspect of this invention, the system of twelfth aspect is characterized in that the preselected intervals correspond to an operator selected period of time.

【００２１】

According to a fourteenth aspect of this invention, the system of twelfth aspect is characterized in that the preselected intervals correspond to a predetermined amount of captured data.

【００２２】

According to a fifteenth aspect of this invention, the system of tenth aspect is characterized in that the system further comprises:

a test mobile unit operating within a service area of the visited network, the test mobile adapted to attach to the visited network when commanded by the monitoring system, and to report message traffic received from the visiting network to the monitoring system.

【００２３】

According to a sixteenth aspect of this invention, a computer-readable storage medium comprises instructions for controlling a network monitoring system, wherein the instructions, when executed, cause a processor to perform actions comprising:

capture signaling messages received at a home network from a visited network, wherein the signaling messages correspond to attempts by roaming home network subscribers to attach to the visited network;

estimate a number of active roaming subscribers on the visited network;

estimate a number of steered roaming subscribers on the visited network;

estimate a number of anti-steered roaming subscribers on the visited network;

compare the estimated numbers of active roaming subscribers, steered roaming subscribers, and anti-steered roaming subscribers alone or in combination to one or more preselected thresholds; and

identify potential anti-steering of roaming activity if one or more of the estimated numbers alone or in combination exceed a preselected threshold.

【００２４】

According to a seventeenth aspect of this invention, the computer-readable storage medium of sixteenth aspect is characterized in that the computer-readable storage medium further comprises:

count a particular network subscriber as an active roaming subscriber if the particular subscriber successfully initiated or received a communication on the visited network, wherein the communication on the visited network comprises a communication selected from the group consisting of a voice call, a data connection, or a short message service communication.

【００２５】

According to an eighteenth aspect of this invention, the computer-readable storage medium of sixteenth aspect is characterized in that the computer-readable storage medium further comprises:

count a particular subscriber as a steered roaming subscriber if the home network did not perform any successful update location transactions from the visited network for the particular subscriber, wherein the particular subscriber is counted as a steered roaming subscriber if a group of failed update location transactions were rejected with a response code selected from the group consisting of System Failure, Roaming Not Allowed, Data Missing, and Unexpected Data Value codes.

【００２６】

According to a nineteenth aspect of this invention, the computer-readable storage medium of sixteenth aspect is characterized in that the computer-readable storage medium further comprises:

count a particular network subscriber as an anti-steered roaming subscriber if the particular subscriber performed a sequence of failed update location transactions within a predetermined period of time followed by a successful update location transaction;

count a particular network subscriber as an anti-steered roaming subscriber if the particular subscriber performed a sequence of update location transactions wherein each update location transaction is spaced within a predetermined interval and wherein the sequence is followed by a successful update location transaction with the predetermined interval; and

count a particular network subscriber as an anti-steered roaming subscriber if the particular subscriber performed a plurality of transactions sequences with the visited network within a predetermined period of time, the transaction sequences each comprising an exchange of at least one cancel location message and at least one update location message.

【００２７】

According to a twentieth aspect of this invention, the computer-readable storage medium of sixteenth aspect is characterized in that the computer-readable storage medium further comprises:

generate a protocol trace comprising messages associated with at least one anti-steer roaming subscriber.

【００２８】

According to twenty-first aspect of this invention, a network monitoring system, comprises:

at least one SS7 interface adapted to capture data traffic from SS7 links, the data traffic comprising messages exchanged between a home network and one or more visited networks;

a memory storing the captured data traffic;

a processor adapted to:

reset a roamer variable to zero at the begin of the predetermined periods, the roamer variable corresponding to a number of successful roamers for a Visited network;

track individual outbound roaming subscribers in the Visited network during the predetermined period;

identify a particular roaming subscriber as an active roamer if that roaming subscriber performed at least one successful service attempt during the predetermined period; and

increment the value of roamer variable for each active roamer.

【００２９】

According to a twenty-second aspect of this invention, the network monitoring system of twenty-first aspect is characterized in that the network monitoring system further comprises:

determine a roaming subscriber's identity using the IMSI or MSISDN of the subscriber's user equipment.

【００３０】

According to a twenty-third aspect of this invention, the network monitoring system of twenty-first aspect is characterized in that the predetermined period is a twenty-four hour period.

【００３１】

According to a twenty-fourth aspect of this invention, the network monitoring system of twenty-

first aspect is characterized in that at least one successful service attempt is selected from the group consisting of: originating a mobile voice call, terminating a mobile voice call, originating an SMS message, and terminating an SMS message.

【００３２】

Having thus described the invention in general terms, reference will now be made to the accompanying drawings.

【BRIEF DESCRIPTION OF THE DRAWINGS】

【００３３】

【FIGURE 1】 Fig.1 is a high level block diagram illustrating the interaction of User Equipment (UE) with Visited Public Mobile Networks (VPMN).

【FIGURE 2】 Fig.2 is a flowchart illustrating a process for detecting Anti-Steering of Roaming activity according to one embodiment of the invention.

【EMBODIMENTS FOR CARRYING OUT THE INVENTION】

【００３４】

The invention now will be described more fully hereinafter with reference to the accompanying drawings. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. Rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. One skilled in the art may be able to use the various embodiments of the invention.

【００３５】

FIGURE 1 is a high level block diagram illustrating the interaction of User Equipment (UE) 101 with Visited Public Mobile Networks (VPMN) 102-104. UE 101 is a subscriber of Home Public Mobile Network (HPMN) 105, which provides wireless services to UE 101 when the device is operating in its home area, region or country. When HPMN 105 does not provide wireless services when subscribers, such as UE 101, are roaming or have traveled to a different area,

region or country. In that situation, the subscriber must search for other public mobile networks and will attempt to access another network to obtain wireless service. For example, UE 101 may detect three VPMNs 102-104 while searching for a roaming provider. UE 101 will typically measure the signal strength of VPMNs 102-104 and will attempt to connect to the VPMN that has the strongest signal. If UE 101 attaches to one of the VPMNs, then HPMN 105 will receive authentication messages from that VPMN during the registration process for UE 101. The attachment and authentication messages from the VPMN will notify HPMN 105 that UE 101 is roaming and has attached to a particular VPMN.

【００３６】

HPMN 105 may have one or more preferred VPMNs in areas outside the HPMNs service area. For example, HPMN 105 may partner with VPMN 102 to support HPMN 105's roaming subscribers. VPMN 102 may provide preferred billing rates or enhanced services to the roaming subscribers of HPMN 105. As a result, HPMN 105 would prefer that subscribers, including UE 101, use VPMN 102 while roaming in the VPMNs service area. If UE 101 attaches to VPMN 102, then HPMN 105 will receive authentication messages from VPMN 102 during the registration process for UE 101. HPMN 105 will determine that UE 101 has attached to a partner or preferred VMPN 102, and HPMN 105 will provide authentication data to allow UE 101 to register with VPMN 102.

【００３７】

UE 101 may determine that VPMN 103 has the strongest signal and may attempt to attach to VPMN 103. HPMN 105 will receive authentication messages from VPMN 103 during the registration process for UE 101. HPMN 105 will determine that UE 101 has attached to a non-preferred or unknown VMPN. HPMN 105 will also determine that partner VPMN 102 could serve UE 101 in the same area as VPMN 103. HPMN 105 may then command UE 101 to detach from VMPN 103 and to look for another VMPN or to reattach to Partner VMPN 102 specifically.

【００３８】

The process wherein HPMN 105 directs or attempts to direct UE 101 to attach to a specific VPMN is referred to as Steering of Roaming (SoR). Steering of Roaming is a technology employed by the Home network, such as HPMN 105, to manage outbound roaming traffic for

subscribers, such as UE 101, in order to control the percentage of roaming traffic that is exchanged with preferred or partner networks (preferred VPMN). Typically, Steering of Roaming applies to subscribers that have traveled to a different country that the Home network does not service. Steering of Roaming may be accomplished in several different ways, including, for example, over-the-air (OTA) steering and SS7-node-based redirection.

【００３９】

In OTA steering, UE 101 maintains a list of preferred networks assigned by the HPMN 105. The UE 101 attempts to connect to one of the preferred networks, such as VPMN 102, when roaming away from the HPMN 105. The preferred network list can be updated by the HPMN 105, such as by sending a GSM MAP message: MT FSM 63 - (U)SIM Data download to the UE 101.

【００４０】

In SS7-node-based redirection, when the UE 101 attaches to another network, such as a VPMN 103 in a visited country, a Mobile Application Part (MAP) Update Location message is sent over an SS7 network 106 from VPMN 103 to the Home Location Register (HLR) 107 on the Home network 105 for UE 101. A steering platform 108 located in Home network 105 and intercepts the Update Location message and identifies the VPMN 103 from which the message originated. If VPMN 103 is not preferred or partner network for HPMN 105, then the Home network may desire to steer roaming subscribers away from that network. The steering platform 108 will reject the Update Location message. The failed Location Update procedure will force UE 101 to detach from VPMN 103 and to attempt to attach to the next available network. UE 101 will again search for available networks and will attempt to attach to the network with the next strongest signal after VPMN 103. HPMN 105 and steering platform 108 will continue to reject Update Location messages for UE 101 until the message comes from a preferred VPMN 102.

【００４１】

Different response codes may be sent in the Reply to the MAP Update Location message. Those messages may also be used by steering platform 108 to redirect UE 101 to a different VPMN. Steering platform 108 may use certain Response Codes to reject the Update Location messages and to steer the roaming subscribers to other VPMNs. In networks using the 3GPP GSM MAP

specification, for example, the values that are allowed for responding to the Update Location messages are System Failure, Roaming Not Allowed, Data Missing, and Unexpected Data Value.

【００４２】

When UE 101 attaches to certain roaming providers, such as VPMN 104, the Visited network may attempt to counter any Steering of Roaming that is being implemented by the Home network 105. The process by which Steering of Roaming is countered or rejected is referred to as Anti-Steering of Roaming (Anti-SoR).

【００４３】

Anti-Steering of Roaming is used by non-preferred VPMNs to override Steering of Roaming from the HPMN. The non-preferred VPMN 104 may desire, for example, to retain the roaming subscriber's identity in order to capture the roaming traffic and the corresponding revenues. Alternatively, the non-preferred VPMN 104 may attempt to prevent or minimize revenues from being generated on a competitor's network, such as preferred VPMN 102.

【００４４】

Visited networks use different types of Anti-Steering of Roaming to counter the different types of Steering of Roaming. In order to override the SS7-node-based redirection mechanism, for example, the Anti-SoR methods rely on SS7 signaling and fall into two main categories: forced manual mode or periodic recapture. In forced manual mode, the VPMN Anit-SoR platform generates consecutive Update Locations to the HPMN until the SoR platform stops rejecting the Update Location messages. After a certain number of Update Locations are received, the HPMN SoR platform assumes that the subscriber is trying to manually select a specific network. In periodic recapture, when a non-preferred VPMN receives a MAP Cancel Location from the HPMN, the Anti-SoR platform on the VPMN issues a MAP Update Location. The Cancel Location – Update Location pattern repeats in a semi-continuous sequence and the UE is never (with the exception of very short time windows) able to perform any mobile terminating or mobile originating service. In some situations, other signaling may also be supported by the VPMN to reduce the risk of service disruption for the roaming subscriber. These methods may be used alone or in combination by a non-preferred VPMN to counter steering of roaming activities

on the Home network. In one embodiment, the non-preferred VPMN 104 has an anti-steering of roaming platform 110 that monitors SS7 traffic between VMPN 104 and HPMN 105.

【００４５】

The subscriber using UE 101 may desire to use a particular VPMN while roaming. To provide this option to the subscriber, HPMN 105 may allow UE 101 to operate in a manual mode in which the subscriber manually chooses which Visited network to use. Anti-Steering of Roaming platform 110 may take advantage of this capability of UE 101. Anti-SoR platform 110 operates in the forced manual node by generating consecutive Update Location messages and sending them to HPMN 105 as if they were initiated by UE 101. Steering of Roaming platform 108 will initially reject the Update Location messages because they are originating from a non-preferred Visited network. However, Steering of Roaming 108 will eventually stop rejecting the Update Location messages on the assumption the subscriber is trying to manually select a specific network. For example, 3GPP TS 24.008 specifies that after four Update Location messages are received at fifteen seconds intervals, then the HPMN should stop rejecting the Update Locations. In this manner, without the subscriber's knowledge, VMPN 104 may successfully mimic messages from UE 101 and prevent HPMN from redirecting UE 101 to a preferred VPMN, such as partner VPMN 102. As a result, the subscriber may be subject to higher rates or substandard service on non-preferred VPMN 104 than what is available on a preferred Visited network.

【００４６】

The non-preferred VPMN may not care whether the subscriber successfully attaches to its network as long as the roaming subscriber is also prevented from attaching to a competitor's network. Anti-Steering of Roaming platform 110 uses periodic recapture to keep UE 101 from attaching to other Visited networks. When UE 101 attempts to attach to VPMN 104, an Update Location message is sent to HPMN 105 as discussed above. Because VPMN 104 is not a preferred VPMN, the SoR platform 108 will send a Cancel Location or other MAP message to VPMN 104 in an attempt to force UE 101 to attach to another Visited network. When non-preferred VPMN 104 receives the Cancel Location message from HPMN 105, Anti-SoR platform 110 again issues another MAP Update Location to HPMN 105. SoR platform 108 will again issue a Cancel Location message. The Update Location/Cancel Location pattern is repeated by Anti-SoR platform 110 in a continuous or semi-continuous sequence. As a result,

UE 101 is never able to achieve any mobile-terminating or mobile-originating service. At best, the UE 101 may have service for very short time windows in between the Update Location/Cancel Location exchanges from the Anti-SoR and SoR platforms.

【００４７】

Anti-Steering of Roaming attacks, such as those described above, may be detected using an SS7 monitoring system. In one embodiment, a HPMN that is equipped with a passive monitoring system continuously monitors all international MAP signaling. By analyzing the MAP signaling, the monitoring system can automatically detect Anti-SoR activity on a Visited network.

【００４８】

The passive monitoring system may comprise of one or more network monitoring probes 111. As illustrated in FIGURE 1, the probe 111 may be coupled to one or more interfaces or interconnect links on the Home network 105. It will be understood that probe 111 may also be coupled to any interfaces or interconnect links within Home network 105 in addition to the links from steering platform 108 to HLR 107 and VPMNs 102-104. For purposes of simplification, FIGURE 1 does not illustrate all possible monitored links in network 105. Probe 111 passively captures message traffic from the interfaces without interrupting the network's operation.

【００４９】

Monitoring probe 111 as illustrated in FIGURE 1 is representative of one or more monitoring probes on Home network 105. Each monitoring probe may capture traffic from one or more links on the network. In addition, traffic on certain links may be captured by more than one probe 111. If multiple probes 111 are used, the probes may be interconnected to share and exchange captured traffic. The monitoring system may use a distributed architecture optimized to handle high volume signaling traffic. The monitoring system and probe 111 may provide real-time, multi-protocol tracking of every transaction across a network, enabling bearer/service subscriber, link/interface, and node status monitoring. In one embodiment, probe 111 may be part of the GeoProbe platform, including the Iris Analyzer Toolset applications and SpIprobes and G10 probes, from Tektronix Incorporated. The monitoring probe may comprise a processor running software applications for analyzing data traffic captured from the SS7 links and a memory for storing software application instructions and captured data traffic. It will be

understood that other network monitoring devices or probes may also be used to detect Anti-Steering of Roaming using the techniques disclosed and described herein.

【００５０】

FIGURE 2 is a flowchart illustrating a process for detecting Anti-Steering of Roaming activity according to one embodiment of the invention. A monitoring system capturing data from links in a Home network may run the process shown in FIGURE 2 to detect when a Visited network is applying Anti-Steering of Roaming techniques against the Home network's subscribers. In step 201, the monitoring system estimates a first parameter, designated in one embodiment as "Indicator No. 1," which corresponds to the number of unique Active Roamers. Indicator No. 1 is an estimate of how many of the Home network's subscribers are roaming on a Visited network over a given period.

【００５１】

In step 202, the monitoring system estimates a second parameter, designated as "Indicator No. 2" in one embodiment, which corresponds to the number of unique Steered Roamers. Indicator No. 2 is an estimate of how many of the Home network's subscribers are associated with signaling traffic that indicates steering of roaming activity initiated by the Home network over a given period. In step 203, the monitoring system estimates a third parameter, designated as "Indicator No. 3" in one embodiment, which corresponds to the number of unique Anti-Steered Roamers. Indicator No. 3 is an estimate of how many of the Home network's subscribers are associated with signaling that indicates anti-steering of roaming activity initiated by a Visited network over a given period.

【００５２】

In step 204, the monitoring system estimates a fourth parameter, designated as "Indicator No. 4" in one embodiment, which corresponds to the potential aliasing of the Home network's HLR. Indicator No. 4 is an estimate the amount of signaling traffic that indicates that an anti-steering platform on a Visited network is using the address of the Home network's HLR when responding to traffic from the Visited network.

【００５３】

The Indicator No. 1-4 parameters may be associated with a specific Visited network or a group of Visited networks. The Indicator Nos. 1-4 parameters may correspond to activity detected over a specific period, such as a selected period of minutes, hours, days, or any other time.

【００５４】

In step 205, the monitoring system generates warnings regarding possible anti-steering of roaming activity. The Anti-SoR warnings are determined based on comparisons of the Indicator No. 1-4 parameter values to configurable thresholds. A user, such as the Home network service provider, may establish or select thresholds for each of the Indicator No. 1-4 parameters. The thresholds may be generic and applied to all Visited networks, or selected specifically for one or more particular Visited networks. The values of the individual Indicators and/or various combinations of two or more of the Indicators may be used to identify potential Anti-SoR activity.

【００５５】

In step 206, the monitoring system generates a detailed protocol trace to confirm any detected possible Anti-Steering of Roaming activity on a specific Visited network.

【００５６】

It will be understood that steps 201-204 of the process may be executed simultaneously and/or sequentially. It will be further understood that the steps may be performed in any order and may be performed once or repetitiously. The process in FIGURE 2 may be performed continuously depending upon the processing capabilities and resources available on monitoring system. Continuous and simultaneous monitoring of the Indicators would allow the monitoring system to generate near real-time warnings of Anti-SoR activity.

【００５７】

Alternatively, traffic traces between a Home network and Visited networks may be captured over time. At selected intervals, or when a desired amount of data has been captured, the monitoring system may than analyze the captured traffic in a batch mode to determine whether any Anti-SoR activity has occurred in a previous period. Both real-time and historical detection of Anti-SoR activity has potential business value to the Home network service provider. The Home network

service provider may attempt to counter a Visited network's Anti-SoR activity using technical, commercial, or legal methods. However, any counter-measures taken by the Home network service provider against the Anti-SoR activity would likely take some period of time, such as days or weeks - if not longer, before they were effective.

【００５８】

Estimating Indicator No. 1: Number of Unique Active Roamers

The number of unique successful roamers for a given Visited network can be estimated by the network monitoring system using data passively captured from SS7 links on the Home network. In one embodiment, the monitoring system performs the following process.

1. At the start of each day, reset the value of Indicator No. 1 for a selected Visited network to zero.

2. Track each individual outbound roaming subscriber (SUB) in the Visited network. The subscribers' identity can be determined, for example, using the IMSI or MSISDN of the user equipment.

3. At the end of the day, review the traffic for each SUB. Count a particular SUB as an Active Roamer, and increment the value of Indicator No. 1 for the Visited network on that day, if that SUB performed at least one successful service attempt among the following operations: Mobile Originating Voice Call, Mobile Terminating Voice Call, Mobile Originating SMS, and Mobile Terminating SMS.

【００５９】

Estimating Indicator No 2: Number of Unique Steered Roamers

The number of unique steered roamers for a given Visited network can be estimated by the monitoring system using the following process.

1. At the start of each day, reset the value of Indicator No. 2 for a selected Visited network to zero.

2. Track each individual outbound roaming subscriber (SUB) in the Visited network. The subscribers' identity can be determined, for example, using the IMSI/MSISDN of the user equipment.

3. At the end of that day, review the traffic for each SUB. Count a particular SUB as a Steered Roamer, and increment the value of Indicator No. 2 for the Visited network on that day, if both of the following conditions have been met:

a) that SUB performed no successful MAP Update Location transactions from the Visited network; and

b) all failed MAP Update Location transactions from that SUB were rejected with a Response Code identified in a predetermined list. The Response Code list may be configurable and, in an exemplary or default embodiment, includes the codes: System Failure, Roaming Not Allowed, Data Missing, and Unexpected Data Value. The Response Code list may be configured differently for each Visited network.

【００６０】

Indicator No. 2 may not provide a precise count of the Steered Roamers, because the Response Codes used by the Steering platform to steer roaming subscribers to different Visited networks may also be used by the Home network itself to report real network or subscription problems. However, the value of Indicator No. 2 does provide relevant information will play a role in the heuristic detection of Anti-SoR activity.

【００６１】

Estimating Indicator No. 3: Number of Unique Anti-Steered Roamers

The number of unique Anti-Steered Roamers for a given Visited network may be estimated by the monitoring system using the following process.

1. At the start of each day, reset the value of Indicator No. 3 for a selected Visited network to zero.

2. Track each individual outbound roaming subscriber (SUB) in the Visited network. The subscribers' identity can be determined, for example, using the IMSI/MSISDN of the user equipment.

3. At the end of that day, review the traffic for each SUB. Count a particular SUB as an Anti-Steered Roamer and increment the value of Indicator No. 3 for the Visited network on that day if at least one of the following conditions has been met:

a) That particular SUB performed at least one sequence of n MAP Update Location transactions from the Visited network in a period of t_1 seconds, wherein the first $n-1$ transactions failed with a Response Code and the last transaction was successful. The values of t_1 and/or n may be configurable. The Response Code may be any MAP Response Code in a predetermined or configurable list. In an exemplary embodiment, the default value of t_1 is 20 seconds, the value of n is 5, and the Response Code configurable list includes the codes: System Failure, Roaming Not Allowed, Data Missing, and Unexpected Data Value. The MAP Response Code may be configured differently on each Visited network.

b) That particular SUB performed at least one sequence of n MAP Update Location transactions from the Visited network, wherein the MAP Update Location attempts are spaced a minimum t_2 seconds and a maximum t_3 seconds apart, and wherein the first $n-1$ transactions failed with a Response Code RC and the last transaction was successful. The values of t_2, t_3 and n may be configurable. In an exemplary embodiment, the default value of t_2 is 35 seconds, the default value of t_3 is 40 seconds, and the default value of n is 5. The Response Code may be any MAP Response Code in a predetermined or configurable list. In an exemplary embodiment, the Response Code configurable list includes the codes: System Failure, Roaming Not Allowed, Data Missing, and Unexpected Data Value.

c) That particular SUB performed at least m sequences of MAP procedures in a period of 1 hour, wherein each sequence starts with a MAP Cancel Location to the Visited network and terminates with a MAP Update Location from the Visited network. The MAP procedures included in each sequence and the time interval between subsequent procedures in the sequence may be configurable. In one embodiment, a default configuration will be a sequence comprising MAP Cancel Location and MAP Update Location transactions that are spaced less than 20

seconds apart. The value of *m* may be configurable. A default value of *m = 2* is used in one embodiment.

【００６２】

Indicator No. 3 may not provide a precise count of the Anti-Steered Roamers, because the subscriber or user equipment - and not a not an Anti-SoR platform - may have manually forced the selection of the network, which could include a sequence of MAP procedures that is counted under Indicator No. 3. Additionally, Anti-SoR behavior may include variations in terms of timing and signaling flow, which could potentially elude detection using the process described above. However, the value of Indicator No. 2 does provide relevant information will play a role in the heuristic detection of Anti-SoR activity.

【００６３】

Estimating Indicator No. 4: Potential Aliasing of the Home Network HLR

An Anti-Steering platform may respond to the Visited network using the address of the Home network's HLR. If this happens, the monitoring system will report a Response-only MAP Transaction. The value of Indicator No. 4 counts the number of Response-only Transactions. The list of Response-only Transactions used to calculate Indicator No. 4 may be configurable and, in one embodiment, may default to Update Location/Insert Subscriber Data.

【００６４】

Generating warnings on the possible presence of Anti-Steering of Roaming

Based on the values of Indicators Nos. 1-4, the monitoring system will generate warnings if an indication of possible Anti-Steering of Roaming is detected.

【００６５】

Near real-time warnings may be generated by the monitoring system based on the rule 3 of the Indicator No. 3 process described above. If processing power in the monitoring system is sufficient, the system can continuously evaluate this rule and generate warnings when one SUB matches either the first or the second condition of rule 3.

【００６６】

Near real-time warnings may also be generated by the monitoring system using Indicator No. 4. If the value of Indicator No. 4 reaches a configurable or preset threshold within a configurable or preset time interval, then the monitoring signal may determine that the Visited network is using Anti-SoR.

【００６７】

In one embodiment, the monitoring system may generate Anti-SoR reports using a combination of the Indicators, such as with the following approach.

IF	(Indicator No. 2 / (Indicator No. 1 + Indicator No. 2)) < X
AND	(Indicator No. 3 / Indicator No. 2) > Y
THEN	Report Anti-SoR activity

【００６８】

The first expression (Indicator No. 2 / (Indicator No. 1 + Indicator No. 2)) measures the efficiency of steering by the Home network as a fraction of the total number of roaming subscribers that have been steered.

【００６９】

The second expression (Indicator1 / Indicator2) measures the effect of Anti-SoR against the effect of Steering.

【００７０】

The values of X and Y are configurable and may be selected independently for each Visited network. X and Y may depend on the configuration of the Steering platform for the Home network and on the required percentage of steered subscribers. A calibration period may be used to select the values of X and Y.

【００７１】

Indicator No. 1 and Indicator No. 2 can only be estimated with a heuristic approach, which makes confirmation of possible Anti-SoR necessary. Such further confirmation may be necessary before the Home network operator takes legal or commercial actions.

【００７２】

Confirmation of Anti-SoR can be obtained with test mobiles. For example, test mobile 112 may be placed in the coverage area for one or more of VPMN 102-104. Home network 105 or monitoring system 111 are in communication with test mobile 112 via link 113, which may be SS7 signaling, an Internet connection, or any other communication method. Home network 105 or monitoring system 111 may direct the test mobile 112 to attach to a selected Visited network, such as VPMN 104. When attachment messages are sent from VPMN 104 to Home network 105, the steering platform 108 rejects the Update Location message in an attempt to steer test mobile 112 to another VPMN. If VPMN 104 is employing Anti-SoR, then it will not notify test mobile 112 that the Update Location message was rejected. Since Home network 105 and/or monitoring system 111 have a back channel 113 connection to test mobile 112, they can monitor what messages are actually sent and received by test mobile 112. The actual messages can be compared to expected messages that should have been sent or received based upon Home network 105's instructions. If the actual messages do not match the expected messages, such as when an Update Location or Cancel Location message is not transmitted as expected, then Anti-SoR activity can be confirmed.

【００７３】

Generating a detailed protocol trace to confirm what detected

The monitoring system has the capability to log call captured MAP signaling traffic as data records and to generated full protocol traces. When the monitoring system's Anti-SoR detection process generates warnings, it will also provide a list of detected IMSI/MSISDN identities of the subscribers. This list can be used in a protocol trace query tool and in a historical call trace application. Detailed protocol traces can be generated for the user equipment corresponding to the detected IMSI/MSISDN to confirm whether Anti-SoR occurred as suggested by the Indicators.

【００７４】

Many modifications and other embodiments of the invention will come to mind to one skilled in the art to which this invention pertains having the benefit of the teachings presented in the foregoing descriptions, and the associated drawings. Therefore, it is to be understood that the

invention is not to be limited to the specific embodiments disclosed. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

【DESCRIPTION OF CODES】

【００７５】

101...User Equipment (UE)

102...Visited Public Mobile Networks (VPMN)

103...VPMN

104...VPMN

105...HPMN

106...SS7 Network

107... HLR

108...Steering Platform

110...Roaming Platform

111...Monitoring Probe (Anti-SoR Platform)

112... Test Mobile

【Claim 1】

A method for detecting anti-steering of roaming on a visited network, comprising:

capturing signaling messages received at a home network from roaming subscribers on the visited network;

correlating the captured messages on a per-subscriber basis;

estimating a number of active roaming subscribers on the visited network;

estimating a number of steered roaming subscribers on the visited network;

estimating a number of anti-steered roaming subscribers on the visited network;

comparing the estimated numbers of active roaming subscribers, steered roaming subscribers, and anti-steered roaming subscribers alone or in combination to one or more preselected thresholds; and

identify potential anti-steering of roaming activity if one or more of the estimated numbers alone or in combination exceed a preselected threshold.

【Claim 2】

A network monitoring system, comprising:

at least one SS7 interface adapted to capture data traffic from SS7 links, the data traffic comprising messages exchanged between a home network and one or more visited networks;

a memory storing the captured data traffic;

a processor adapted to

calculate a number of active roaming subscribers on the visited network;

calculate a number of steered roaming subscribers on the visited network;

calculate a number of anti-steered roaming subscribers on the visited network;

compare the numbers active roaming subscribers, steered roaming subscribers, and anti-steered roaming subscribers to predetermined thresholds; and

determine whether the visited network is employing anti-steering of roaming techniques based upon the comparison.

【Claim 3】

A computer-readable storage medium comprising instructions for controlling a network monitoring system, wherein the instructions, when executed, cause a processor to perform actions comprising:

capture signaling messages received at a home network from a visited network, wherein the signaling messages correspond to attempts by roaming home network subscribers to attach to the visited network;

estimate a number of active roaming subscribers on the visited network;

estimate a number of steered roaming subscribers on the visited network;

estimate a number of anti-steered roaming subscribers on the visited network;

compare the estimated numbers of active roaming subscribers, steered roaming subscribers, and anti-steered roaming subscribers alone or in combination to one or more preselected thresholds; and

identify potential anti-steering of roaming activity if one or more of the estimated numbers alone or in combination exceed a preselected threshold.

【Claim 4】

A network monitoring system, comprising:

at least one SS7 interface adapted to capture data traffic from SS7 links, the data traffic comprising messages exchanged between a home network and one or more visited networks;

a memory storing the captured data traffic;

a processor adapted to:

reset a roamer variable to zero at the begin of the predetermined periods, the roamer variable corresponding to a number of successful roamers for a Visited network;

track individual outbound roaming subscribers in the Visited network during the predetermined period;

identify a particular roaming subscriber as an active roamer if that roaming subscriber performed at least one successful service attempt during the predetermined period; and

increment the value of roamer variable for each active roamer.

【ABSTRACT】

【PROBLEM】

To determine if a visited network is rejecting steering of roaming by the home network.

【SOLVING MEANS】

A system and method for automatically detecting Anti-Steering of Roaming activity is disclosed. This method can be used by a monitoring system on a home network that continuously monitors all international MAP signaling with a visited network. Anti-Steering of Roaming is detected by estimating a number of roaming subscribers of different types, including a number of unique active roamers, a number of unique steered roamers, and a number of unique anti-steered roamers. The numbers of subscribers of the different types, either alone or in combination, are compared to threshold values. If the numbers exceed the threshold value, then the monitoring system alerts the home network that a visited network may be using Anti-Steering of Roaming technology.

【REPRESENTATIVE DRAWING】 FIG. 2

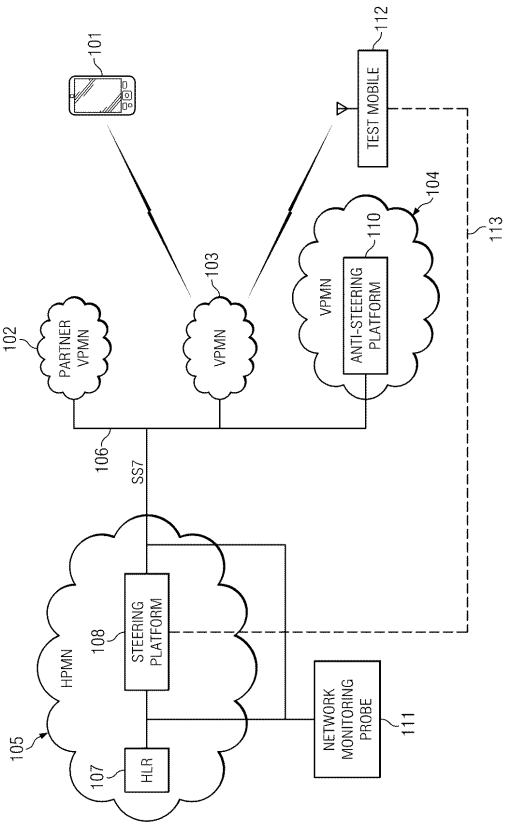


FIG. 1

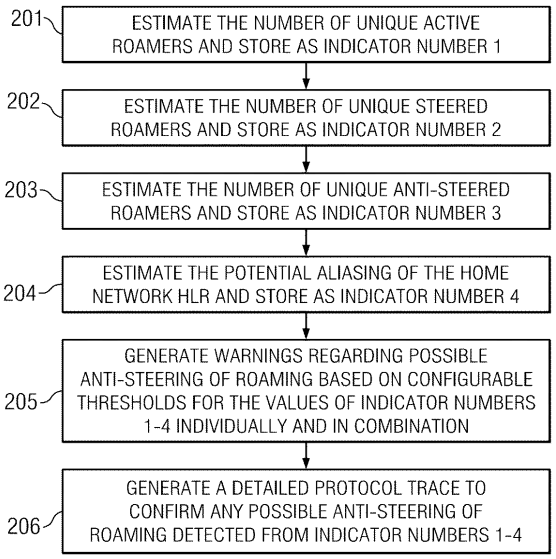


FIG. 2