(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7698714号
(P7698714)

(45)発行日　令和7年6月25日(2025.6.25)

(24)登録日　令和7年6月17日(2025.6.17)

(51)国際特許分類

		FI	
H04W	*12/108 (2021.01)*	H04W	12/108
H04W	*12/069 (2021.01)*	H04W	12/069

請求項の数　17　（全20頁）

(21)出願番号　特願2023-519026(P2023-519026)
(86)(22)出願日　令和3年4月29日(2021.4.29)
(65)公表番号　特表2023-544000(P2023-544000A)
(43)公表日　令和5年10月19日(2023.10.19)
(86)国際出願番号　PCT/US2021/029973
(87)国際公開番号　WO2022/066227
(87)国際公開日　令和4年3月31日(2022.3.31)
審査請求日　令和6年4月24日(2024.4.24)
(31)優先権主張番号　17/129,441
(32)優先日　令和2年12月21日(2020.12.21)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　17/095,420
(32)優先日　令和2年11月11日(2020.11.11)
最終頁に続く

(73)特許権者　502303739
オラクル・インターナショナル・コーポレイション
アメリカ合衆国 ９４０６５ カリフォルニア州 レッドウッド ショアーズ，メール ストップ ５オーピー７ オラクル パークウェイ ５００
(74)代理人　110001195
弁理士法人深見特許事務所
(72)発明者　ラジプット，ジャイ
インド、５６０１０３ カルナータカ、バンガロール、ボガナハリ、ビィ・ブイ・エス・ピナクル、３０９
(72)発明者　マハランク，シャシキラン・バラチャンドラ
最終頁に続く

(54)【発明の名称】　５Ｇローミングなりすまし攻撃を緩和するための方法、システム、およびコンピュータ読み取り可能な媒体

(57)【特許請求の範囲】

【請求項１】

５Ｇローミングなりすまし攻撃を緩和するための方法であって、

ＳＥＰＰ（セキュリティエッジ保護プロキシ）が、第１ノードからのＴＬＳ（トランスポートレイヤーセキュリティ）メッセージから、前記第１ノードの第１識別子を取得することと、

前記ＳＥＰＰが、前記第１ノードからのＮ３２－ｃセキュリティ機能ネゴシエーションメッセージから、前記第１ノードの第２識別子を取得することと、

前記第１ノードの前記第１識別子と前記第２識別子を比較することと、

第１識別子と第２識別子とは一致しないと判断し、これに応答して、前記第１ノードの第２識別子が無効であると判断することと、

前記第１ノードの前記第２識別子が無効であると判断したことに応答して、前記第１ノードとのＰＬＭＮ（公衆陸上移動体通信網）間通信をブロックすることとを含む、方法。

【請求項２】

ＴＬＳメッセージから前記第１ノードの前記第１識別子を取得することは、前記第１識別子をＴＬＳ証明書メッセージに含まれる証明書から取得することを含む、請求項１に記載の方法。

【請求項３】

前記証明書は、Ｘ．５０９証明書を含む、請求項２に記載の方法。

【請求項４】

前記第１ノードの前記第１識別子を取得することは、前記Ｘ．５０９証明書のサブジェクトの別名拡張から前記第１ノードのＦＱＤＮ（完全修飾ドメイン名）を抽出することを含む、請求項３に記載の方法。
【請求項５】
前記ＳＥＰＰは、Ｎ３２－ｃセキュリティ機能ネゴシエーション手順における応答側ＳＥＰＰであり、前記第１ノードの前記第２識別子を取得することは、前記Ｎ３２－ｃセキュリティ機能ネゴシエーションメッセージのＳｅｃＮｅｇｏｔｉａｔｅＲｅｑＤａｔａ情報要素の送信者属性から、前記第１ノードの前記第２識別子を抽出することを含む、請求項１～４のいずれか１項に記載の方法。
【請求項６】
前記ＳＥＰＰは、Ｎ３２－ｃセキュリティ機能ネゴシエーション手順における開始側ＳＥＰＰであり、前記第１ノードの前記第２識別子を取得することは、前記Ｎ３２－ｃセキュリティ機能ネゴシエーションメッセージのＳｅｃＮｅｇｏｔｉａｔｉｏｎＲｓｐＤａｔａ情報要素の送信者属性から前記第１ノードの前記第２識別子を抽出することを含む、請求項１～４のいずれか１項に記載の方法。
【請求項７】
前記ＳＥＰＰが、第２ノードからのＴＬＳハンドシェイクメッセージから、前記第２ノードの第１識別子を取得することと、
前記第２ノードからのＮ３２－ｃセキュリティ機能ネゴシエーションメッセージから、前記第２ノードの第２識別子を取得することと、
前記第２ノードの前記第１識別子と前記第２識別子を比較することと、
第１識別子と第２識別子が一致すると判断することと、
前記第２ノードの前記第１識別子および前記第２識別子のうち一方を用いてピアＳＥＰＰデータベースでルックアップを実行し、前記ピアＳＥＰＰデータベースにおいて一致する識別子を探し出すことと、
前記第２ノードの前記第１識別子と前記第２識別子が一致し、前記ピアＳＥＰＰデータベースに一致する識別子が存在すると判断したことに応答して、前記第２ノードとのＰＬＭＮ間通信を許可することとを含む、請求項１～６のいずれか１項に記載の方法。
【請求項８】
前記ＳＥＰＰが、第２ノードからのＴＬＳハンドシェイクメッセージから、前記第２ノードの第１識別子を取得することと、
前記ＳＥＰＰが、前記第２ノードからのＮ３２－ｃセキュリティ機能ネゴシエーションメッセージから、前記第２ノードの第２識別子を取得することと、
前記第２ノードの前記第１識別子と前記第２識別子を比較することと、
第１識別子と第２識別子が一致すると判断することと、
前記第２ノードの前記第１識別子および前記第２識別子のうち一方を用いてピアＳＥＰＰデータベースでルックアップを実行し、前記ピアＳＥＰＰデータベースにおいて一致する識別子を探し出せないことと、
前記第２ノードの前記第１識別子と前記第２識別子が一致し、前記ピアＳＥＰＰデータベースに一致する識別子が存在しないと判断したことに応答して、前記第２ノードからのＰＬＭＮ間通信をブロックすることとを含む、請求項１～７のいずれか１項に記載の方法。
【請求項９】
５Ｇローミングなりすまし攻撃を緩和するためのシステムであって、
少なくとも１つのプロセッサと、メモリとを含むＳＥＰＰ（セキュリティエッジ保護プロキシ）と、
前記少なくとも１つのプロセッサによって実装された５Ｇローミングなりすまし攻撃緩和モジュールとを備え、前記５Ｇローミングなりすまし攻撃緩和モジュールは、
第１ノードからのＴＬＳ（トランスポートレイヤーセキュリティ）メッセージから、前記第１ノードの第１識別子を取得し、
前記第１ノードからのＮ３２－ｃセキュリティ機能ネゴシエーションメッセージから

、前記第１ノードの第２識別子を取得し、
　前記第１ノードの前記第１識別子と前記第２識別子を比較し、
　第１識別子と第２識別子とは一致しないと判断し、これに応答して、前記第１ノードの第２識別子が無効であると判断し、
　前記第１ノードの前記第２識別子が無効であると判断したことに応答して、前記第１ノードとのＰＬＭＮ（公衆陸上移動体通信網）間通信をブロックするように構成される、システム。
【請求項１０】
　前記５Ｇローミングなりすまし攻撃緩和モジュールは、前記第１ノードの前記第１識別子を、ＴＬＳ証明書メッセージに含まれる証明書から取得するように構成される、請求項９に記載のシステム。
【請求項１１】
　前記証明書は、Ｘ．５０９証明書を含む、請求項１０に記載のシステム。
【請求項１２】
　前記５Ｇローミングなりすまし攻撃緩和モジュールは、前記証明書のサブジェクトの別名拡張から抽出される前記第１ノードのＦＱＤＮ（完全修飾ドメイン名）を抽出することによって、前記第１ノードの前記第１識別子を取得するように構成される、請求項１１に記載のシステム。
【請求項１３】
　前記ＳＥＰＰは、Ｎ３２－ｃセキュリティ機能ネゴシエーション手順における応答側ＳＥＰＰであり、５Ｇローミングなりすまし攻撃緩和モジュールは、前記Ｎ３２－ｃセキュリティ機能ネゴシエーションメッセージのＳｅｃＮｅｇｏｔｉａｔｅＲｅｑＤａｔａ情報要素の送信者属性から前記第１ノードの前記第２識別子を抽出することによって、前記第１ノードの前記第２識別子を取得するように構成される、請求項９～１２のいずれか１項に記載のシステム。
【請求項１４】
　前記ＳＥＰＰは、Ｎ３２－ｃセキュリティ機能ネゴシエーション手順における開始側ＳＥＰＰであり、前記５Ｇローミングなりすまし攻撃緩和モジュールは、前記Ｎ３２－ｃセキュリティ機能ネゴシエーションメッセージのＳｅｃＮｅｇｏｔｉａｔｅＲｓｐＤａｔａ情報要素の送信者情報要素属性から前記第１ノードの前記第２識別子を抽出することによって、前記第１ノードの前記第２識別子を取得するように構成される、請求項９～１２のいずれか１項に記載のシステム。
【請求項１５】
　前記５Ｇローミングなりすまし攻撃緩和モジュールは、
　第２ノードからのＴＬＳハンドシェイクメッセージから、前記第２ノードの第１識別子を取得し、
　前記第２ノードからのＮ３２－ｃセキュリティ機能ネゴシエーションメッセージから、前記第２ノードの第２識別子を取得し、
　前記第２ノードの前記第１識別子と前記第２識別子を比較し、
　第１識別子と第２識別子が一致すると判断し、
　前記第２ノードの前記第１識別子および前記第２識別子のうち一方を用いてピアＳＥＰＰデータベースでルックアップを実行し、前記ピアＳＥＰＰデータベースにおいて一致する識別子を探し出し、
　前記第２ノードの前記第１識別子と前記第２識別子が一致し、前記ピアＳＥＰＰデータベースに一致する識別子が存在すると判断したことに応答して、前記第２ノードとのＰＬＭＮ間通信を許可するように構成される、請求項９～１４のいずれか１項に記載のシステム。
【請求項１６】
　前記５Ｇローミングなりすまし攻撃緩和モジュールは、
　第２ノードからのＴＬＳハンドシェイクメッセージから、前記第２ノードの第１識別

子を取得し、
　前記第２ノードからのＮ３２－ｃセキュリティ機能ネゴシエーションメッセージから、前記第２ノードの第２識別子を取得し、
　前記第２ノードの前記第１識別子と前記第２識別子を比較し、
　第１識別子と第２識別子が一致すると判断し、
　前記第２ノードの前記第１識別子および前記第２識別子のうち一方を用いてピアＳＥＰＰデータベースでルックアップを実行し、前記ピアＳＥＰＰデータベースにおいて一致する識別子を探し出せず、
　前記第２ノードの前記第１識別子と前記第２識別子が一致し、前記ピアＳＥＰＰデータベースに一致する識別子が存在しないと判断したことに応答して、前記第２ノードからのＰＬＭＮ間通信をブロックするように構成される、請求項９～１５のいずれか１項に記載のシステム。
【請求項１７】
　実行可能な命令を備えるコンピュータプログラムであって、前記実行可能な命令は、コンピュータのプロセッサによって実行されると、請求項１～８のいずれか１項に記載の方法を実行するように前記コンピュータを制御する、コンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
　優先権の主張
　本願は、２０２０年１２月２１日に出願された米国特許出願第１７／１２９，４４１号、２０２０年１１月１１日に出願された米国特許出願第１７／０９５，４２０号、２０２０年１１月２日に出願されたインド仮出願第２０２０４１０４７７７９号、および２０２０年９月２５日に出願されたインド仮出願第２０２０４１０４１７５４号の優先権の利益を主張するものであり、これらのすべての開示内容を引用により本明細書に援用する。
【０００２】
　技術分野
　本明細書に記載の主題は、５Ｇ通信ネットワークにおけるセキュリティを向上させることに関する。特に、本明細書に記載の主題は、５Ｇローミングなりすまし攻撃を緩和するための方法、システム、およびコンピュータ読み取り可能な媒体に関する。
【背景技術】
【０００３】
　背景
　５Ｇ電気通信ネットワークでは、サービスを提供するネットワークノードは、プロデューサーＮＦ（ネットワーク機能）と称される。サービスを利用するネットワークノードは、コンシューマーＮＦと称される。ネットワーク機能は、サービスを利用しているかサービスを提供しているかに応じて、プロデューサーＮＦにもコンシューマーＮＦにもなり得る。
【０００４】
　所与のプロデューサーＮＦは、多くのサービスエンドポイントを有し得る。ここで、サービスエンドポイントとは、プロデューサーＮＦがホストする１つ以上のＮＦインスタンスの接続ポイントである。サービスエンドポイントは、ＩＰ（インターネットプロトコル）アドレスとポート番号との組合せ、またはプロデューサーＮＦをホストするネットワークノード上のＩＰアドレスおよびポート番号に変換される完全修飾ドメイン名によって識別される。ＮＦインスタンスは、サービスを提供するプロデューサーＮＦのインスタンスである。所与のプロデューサーＮＦは、２つ以上のＮＦインスタンスを含み得る。なお、複数のＮＦインスタンスが同じサービスエンドポイントを共有できる。
【０００５】
　プロデューサーＮＦは、ＮＲＦ（Ｎｅｔｗｏｒｋ　Ｆｕｎｃｔｉｏｎ　Ｒｅｐｏｓｉｔｏｒｙ　Ｆｕｎｃｔｉｏｎ）に登録される。ＮＲＦは、各ＮＦインスタンスがサポートする

サービスを識別する利用可能なＮＦインスタンスのサービスプロファイルを保持する。コンシューマーＮＦは、ＮＲＦに登録されているプロデューサーＮＦインスタンスについての情報を受信するようにサブスクライブできる。

【０００６】

コンシューマーＮＦに加えて、ＮＦサービスインスタンスについての情報を受信するようにサブスクライブできる別の種類のネットワークノードは、ＳＣＰ（Ｓｅｒｖｉｃｅ Ｃｏｍｍｕｎｉｃａｔｉｏｎ Ｐｒｏｘｙ）である。ＳＣＰは、ＮＲＦを介してサブスクライブし、プロデューサーＮＦサービスインスタンスに関するリーチャビリティとサービスプロファイル情報とを取得する。コンシューマーＮＦは、ＳＣＰに接続し、ＳＣＰは、要求されたサービスを提供するプロデューサーＮＦサービスインスタンス間でトラフィックの負荷を分散する、または、宛先であるプロデューサーＮＦインスタンスにトラフィックを直接ルーティングする。

【０００７】

ＳＣＰに加えて、プロデューサーＮＦとコンシューマーＮＦとの間でトラフィックをルーティング中間プロキシノードまたはネットワークノード群のその他の例として、ＳＥＰＰ（セキュリティエッジ保護プロキシ）、サービスゲートウェイ、および５Ｇサービスメッシュにあるノードなどが挙げられる。ＳＥＰＰは、異なる５Ｇ ＰＬＭＮ（公衆陸上移動体通信網）間で交換されるコントロールプレーントラフィックを保護するために用いられるネットワークノードである。このように、ＳＥＰＰは、すべてのＡＰＩ（Ａｐｐｌｉｃａｔｉｏｎ Ｐｒｏｇｒａｍｍｉｎｇ Ｉｎｔｅｒｆａｃｅメッセージについてメッセージフィルタリング、ポリシング、およびトポロジ隠蔽を実行する。

【０００８】

現在の５Ｇネットワークアーキテクチャでは、ＳＥＰＰ間のインタフェースであるＮ３２インタフェース上で１つの脆弱性が存在する。上記の通り、ＳＥＰＰは、ＰＬＭＮ（公衆陸上移動体通信網）のセキュリティスクリーニングノードとして機能する。Ｎ３２コントロールまたはＮ３２－ｃインタフェースは、リモートＳＥＰＰと制御メッセージを交換するために用いられる。Ｎ３２－ｃインタフェース上での通信の開始は、ＴＬＳ（トランスポートレイヤーセキュリティ）ハンドシェイク手順を含み、ＴＬＳ接続を確立する。また、通信の開始は、Ｎ３２－ｃセキュリティ機能ネゴシエーション手順も含む。Ｎ３２－ｃセキュリティ機能ネゴシエーション手順は、Ｎ３２－ｃメッセージの交換を含む。Ｎ３２－ｃセキュリティ機能ネゴシエーション手順の間、リモートエンドポイントのアイデンティティの検証は行われない。また、リモートエンドポイントも、開始側ＳＥＰＰのアイデンティティを検証しない。Ｎ３２－ｃインタフェース上で検証が行われないので、開始側ＳＥＰＰおよび応答側ＳＥＰＰは、サードパーティがＮ３２－ｃ通信の一方のエンドになりすましてＰＬＭＮに不正アクセスする、なりすまし攻撃に対して脆弱である。

【０００９】

これらのおよびその他の問題点に鑑みて、５Ｇローミングなりすまし攻撃を緩和するための方法、システム、およびコンピュータ読み取り可能な媒体が必要とされている。

【発明の概要】

【課題を解決するための手段】

【００１０】

概要

５Ｇローミングなりすまし攻撃を緩和するための方法は、ＳＥＰＰ（セキュリティエッジ保護プロキシ）が、第１ノードからのＴＬＳ（トランスポートレイヤーセキュリティ）メッセージから、第１ノードの第１識別子を取得することを含む。この方法は、ＳＥＰＰが、第１ノードからのＮ３２－ｃセキュリティ機能ネゴシエーションメッセージから、第１ノードの第２識別子を取得することをさらに含む。方法は、第１ノードの第１識別子と第２識別子を比較することをさらに含む。方法は、第１識別子と第２識別子とは一致しないと判断し、これに応答して、第１ノードの第２識別子が無効であると判断することをさらに含む。方法は、第１ノードの第２識別子が無効であると判断したことに応答して、第

１ノードとのＰＬＭＮ（公衆陸上移動体通信網）間通信をブロックすることをさらに含む。
【００１１】
本明細書に記載の主題の別の態様によると、ＴＬＳメッセージから第１ノードの第１識別子を取得することは、第１識別子をＴＬＳ証明書メッセージに含まれる証明書から取得することを含む。
【００１２】
本明細書に記載の主題の別の態様によると、証明書は、Ｘ．５０９証明書を含む。
本明細書に記載の主題の別の態様によると、第１ノードの第１識別子を取得することは、Ｘ．５０９証明書のサブジェクトの別名拡張から第１ノードのＦＱＤＮ（完全修飾ドメイン名）を抽出することを含む。
【００１３】
本明細書に記載の主題の別の態様によると、ＳＥＰＰは、Ｎ３２－ｃセキュリティ機能ネゴシエーション手順における応答側ＳＥＰＰであり、第１ノードの第２識別子を取得することは、Ｎ３２－ｃセキュリティ機能ネゴシエーションメッセージのＳｅｃＮｅｇｏｔｉａｔｅＲｅｑＤａｔａ情報要素の送信者属性から、第１ノードの第２識別子を抽出することを含む。
【００１４】
本明細書に記載の主題の別の態様によると、ＳＥＰＰは、Ｎ３２－ｃセキュリティ機能ネゴシエーション手順における開始側ＳＥＰＰであり、第１ノードの第２識別子を取得することは、Ｎ３２－ｃセキュリティ機能ネゴシエーションメッセージのＳｅｃＮｅｇｏｔｉａｔｉｏｎＲｓｐＤａｔａ情報要素の送信者属性から第１ノードの第２識別子抽出することを含む。
【００１５】
本明細書に記載の主題の別の態様によると、５Ｇローミングセキュリティ攻撃を緩和するための方法は、ＳＥＰＰが、第２ノードからのＴＬＳハンドシェイクメッセージから、第２ノードの第１識別子を取得することと、第２ノードからのＮ３２－ｃセキュリティ機能ネゴシエーションメッセージから、第２ノードの第２識別子を取得することと、第２ノードの第１識別子と第２識別子を比較することと、第１識別子と第２識別子が一致すると判断することと、第２ノードの第１識別子および第２識別子のうち一方を用いてピアＳＥＰＰデータベースでルックアップを実行し、ピアＳＥＰＰデータベースにおいて一致する識別子を探し出すことと、第２ノードの第１識別子と第２識別子が一致し、ピアＳＥＰＰデータベースに一致する識別子が存在すると判断したことに応答して、第２ノードとのＰＬＭＮ間通信を許可することとを含む。
【００１６】
本明細書に記載の主題の別の態様によると、５Ｇローミングセキュリティ攻撃を緩和するための方法は、ＳＥＰＰが、第２ノードからのＴＬＳハンドシェイクメッセージから、第２ノードの第１識別子を取得することと、ＳＥＰＰが、第２ノードからのＮ３２－ｃセキュリティ機能ネゴシエーションメッセージから、第２ノードの第２識別子を取得することと、第２ノードの第１識別子と第２識別子を比較することと、第１識別子と第２識別子が一致すると判断することと、第２ノードの第１識別子および第２識別子のうち一方を用いてピアＳＥＰＰデータベースでルックアップを実行し、ピアＳＥＰＰデータベースにおいて一致する識別子を探し出せないことと、第２ノードの第１識別子と第２識別子が一致し、ピアＳＥＰＰデータベースに一致する識別子が存在しないと判断したことに応答して、第２ノードからのＰＬＭＮ間通信をブロックすることとを含む。
【００１７】
本明細書に記載の主題の別の態様によると、５Ｇローミングなりすまし攻撃を緩和するためのシステムは、少なくとも１つのプロセッサと、メモリとを含むＳＥＰＰ（セキュリティエッジ保護プロキシ）を備える。このシステムは、少なくとも１つのプロセッサによって実装された５Ｇローミングなりすまし攻撃緩和モジュールをさらに備える。５Ｇローミングなりすまし攻撃緩和モジュールは、第１ノードからのＴＬＳ（トランスポートレイ

ヤーセキュリティ）メッセージから、第１ノードの第１識別子を取得し、第１ノードからのＮ３２－ｃセキュリティ機能ネゴシエーションメッセージから、第１ノードの第２識別子を取得し、第１ノードの第１識別子と第２識別子を比較し、第１識別子と第２識別子とは一致しないと判断し、これに応答して、第１ノードの第２識別子が無効であると判断し、第１ノードの第２識別子が無効であると判断したことに応答して、第１ノードとのＰＬＭＮ（公衆陸上移動体通信網）間通信をブロックするように構成される。

【００１８】

本明細書に記載の主題の別の態様によると、５Ｇローミングなりすまし攻撃緩和モジュールは、第１ノードの第１識別子を、ＴＬＳ証明書メッセージに含まれる証明書から取得するように構成される。

【００１９】

本明細書に記載の主題の別の態様によると、５Ｇローミングなりすまし攻撃緩和モジュールは、証明書のサブジェクトの別名拡張から第１ノードのＦＱＤＮ（完全修飾ドメイン名）を抽出することによって、第１ノードの第１識別子を取得するように構成される。

【００２０】

本明細書に記載の主題の別の態様によると、ＳＥＰＰは、Ｎ３２－ｃセキュリティ機能ネゴシエーション手順における応答側ＳＥＰＰであり、５Ｇローミングなりすまし攻撃緩和モジュールは、Ｎ３２－ｃセキュリティ機能ネゴシエーションメッセージのＳｅｃＮｅｇｏｔｉａｔｅＲｅｑＤａｔａ情報要素の送信者属性から第１ノードの第２識別子を抽出することによって、第１ノードの第２識別子を取得するように構成される。

【００２１】

本明細書に記載の主題の別の態様によると、ＳＥＰＰは、Ｎ３２－ｃセキュリティ機能ネゴシエーション手順における開始側ＳＥＰＰであり、５Ｇローミングなりすまし攻撃緩和モジュールは、Ｎ３２－ｃセキュリティ機能ネゴシエーションメッセージのＳｅｃＮｅｇｏｔｉａｔｅＲｓｐＤａｔａ情報要素の送信者情報要素属性から第１ノードの第２識別子を抽出することによって、第１ノードの第２識別子を取得するように構成される。

【００２２】

本明細書に記載の主題の別の態様によると、５Ｇローミングなりすまし攻撃緩和モジュールは、第２ノードからのＴＬＳハンドシェイクメッセージから、第２ノードの第１識別子を取得し、第２ノードからのＮ３２－ｃセキュリティ機能ネゴシエーションメッセージから、第２ノードの第２識別子を取得し、第２ノードの第１識別子と第２識別子を比較し、第１識別子と第２識別子が一致すると判断し、第２ノードの第１識別子および第２識別子のうち一方を用いてピアＳＥＰＰデータベースでルックアップを実行し、ピアＳＥＰＰデータベースにおいて一致する識別子を探し出し、第２ノードの第１識別子と第２識別子が一致し、ピアＳＥＰＰデータベースに一致する識別子が存在すると判断したことに応答して、第２ノードとのＰＬＭＮ間通信を許可するように構成される。

【００２３】

本明細書に記載の主題の別の態様によると、５Ｇローミングなりすまし攻撃緩和モジュールは、第２ノードからのＴＬＳハンドシェイクメッセージから、第２ノードの第１識別子を取得し、第２ノードからのＮ３２－ｃセキュリティ機能ネゴシエーションメッセージから、第２ノードの第２識別子を取得し、第２ノードの第１識別子と第２識別子を比較し、第１識別子と第２識別子が一致すると判断し、第２ノードの第１識別子および第２識別子のうち一方を用いてピアＳＥＰＰデータベースでルックアップを実行し、ピアＳＥＰＰデータベースにおいて一致する識別子を探し出せず、第２ノードの第１識別子と第２識別子が一致し、ピアＳＥＰＰデータベースに一致する識別子が存在しないと判断したことに応答して、第２ノードからのＰＬＭＮ間通信をブロックするように構成される。

【００２４】

本明細書に記載の主題の別の態様によると、実行可能な命令を格納した、非一時的なコンピュータ読み取り可能な媒体を提供する。実行可能な命令は、コンピュータのプロセッサによって実行されると、ステップを実行するようにコンピュータを制御する。当該ステ

ップは、ＳＥＰＰ（セキュリティエッジ保護プロキシ）が、第１ノードからのＴＬＳ（トランスポートレイヤーセキュリティ）メッセージから、第１ノードの第１識別子を取得するステップを含む。ステップは、ＳＥＰＰが、第１ノードからのＮ３２－ｃセキュリティ機能ネゴシエーションメッセージから、第１ノードの第２識別子を取得するステップをさらに含む。ステップは、第１ノードの第１識別子と第２識別子を比較するステップと、第１識別子と第２識別子とは一致しないと判断し、これに応答して、第１ノードの第２識別子が無効であると判断するステップとをさらに含む。ステップは、第１ノードの第２識別子が無効であると判断したことに応答して、第１ノードとのＰＬＭＮ（公衆陸上移動体通信網）間通信をブロックするステップをさらに含む。

【００２５】

本明細書において説明する主題は、ハードウェア、ソフトウェア、ファームウェア、または、それらの任意の組合せで実現されてもよい。このように、「機能」、「ノード」、または「モジュール」という用語は、本明細書において用いられる場合、記載の特徴を実現するためのハードウェア（ソフトウェアおよび／またはファームウェアコンポーネントも含んでもよい）を指す。一例示的な実施態様では、本明細書において説明する主題は、コンピュータにより実行可能な命令を格納したコンピュータ読み取り可能な媒体を用いて実現されてもよい。当該命令は、コンピュータのプロセッサによって実行されると、ステップを実行させるようにコンピュータを制御する。本明細書において説明する主題を実現するのに適した例示的なコンピュータ読み取り可能な媒体として、ディスク記憶装置、チップ記憶装置、プログラム可能な論理回路、および特定用途向け集積回路など、非一時的なコンピュータ読み取り可能な媒体などが挙げられる。これに加えて、本明細書において説明する主題を実現するコンピュータ読み取り可能な媒体は、１つのデバイスまたは１つのコンピューティングプラットフォーム上に位置してもよいし、複数のデバイスまたは複数のコンピューティングプラットフォーム間で分散されてもよい。

【００２６】

ここで、添付の図面を参照して本明細書に記載の主題を説明する。

【図面の簡単な説明】

【００２７】

【図１】例示的な５Ｇネットワークアーキテクチャを示すネットワーク図である。

【図２】ＳＥＰＰ間のＴＬＳ（トランスポートレイヤーセキュリティ）メッセージおよびＮ３２－ｃメッセージの交換を示すメッセージフロー図である。

【図３】ＳＥＰＰになりすましているハッカーを示すネットワーク図である。

【図４】ＳＥＰＰ間で交換されたＮ３２－ｃメッセージにおいて提示されたアイデンティティの検証を示すメッセージフロー図である。

【図５】Ｎ３２－ｃインタフェース上での検証が失敗すると、応答側ＳＥＰＰによってメッセージがブロックされる様子を示す図である。

【図６】Ｎ３２－ｃインタフェース上での検証が失敗すると、開始側ＳＥＰＰによってメッセージがブロックされる様子を示す図である。

【図７】５Ｇローミングなりすまし攻撃を緩和するためのＳＥＰＰの例示的なアーキテクチャを示すブロック図である。

【図８】例示的な５Ｇローミングなりすまし攻撃を緩和するための方法を示すフローチャートである。

【発明を実施するための形態】

【００２８】

詳細な説明

本明細書に記載の主題は、５Ｇローミングなりすまし攻撃を緩和するための方法、システム、およびコンピュータ読み取り可能な媒体に関する。図１は、例示的な５Ｇシステムネットワークアーキテクチャを示すブロック図である。図１のアーキテクチャは、同じＨＰＬＭＮ（ホーム側公衆陸上移動体通信網）に位置し得るＮＲＦ１００とＳＣＰ１０１とを備える。上述したように、ＮＲＦ１００は、利用可能なプロデューサーＮＦサービスイ

ンスタンスのプロファイルおよびこれらがサポートするサービスを保持し、コンシューマーＮＦまたはＳＣＰが新しい／更新されたプロデューサーＮＦサービスインスタンスをサブスクライブすることまたは新しい／更新されたプロデューサーＮＦサービスインスタンスの登録について通知されることを可能にする。また、ＳＣＰ１０１は、サービス検出およびプロデューサーＮＦインスタンスの選択をサポートし得る。ＳＣＰ１０１は、コンシューマーＮＦとプロデューサーＮＦとの接続の負荷分散を行い得る。これに加えて、本明細書に記載の技法を用いて、ＳＣＰ１０１は、ＮＦの位置に基づいた、好ましい選択およびルーティングを行い得る。

【００２９】

ＮＲＦ１００は、ＮＦまたはプロデューサーＮＦインスタンスのサービスプロファイルのリポジトリである。プロデューサーＮＦインスタンスと通信を行うために、コンシューマーＮＦまたはＳＣＰは、ＮＦもしくはサービスプロファイル、またはプロデューサーＮＦインスタンスをＮＲＦ１００から取得しなければならない。ＮＦまたはサービスプロファイルは、３ＧＰＰ（登録商標）（Ｔｈｉｒｄ Ｇｅｎｅｒａｔｉｏｎ Ｐａｒｔｎｅｒｓｈｉｐ Ｐｒｏｊｅｃｔ）ＴＳ（技術仕様書）２９．５１０で規定されたＪＳＯＮ（ＪａｖａＳｃｒｉｐｔ（登録商標） Ｏｂｊｅｃｔ Ｎｏｔａｔｉｏｎ）データ構造である。ＮＦまたはサービスプロファイルの規定は、ＦＱＤＮ（完全修飾ドメイン名）、ＩＰｖ４（ＩＰ（インターネットプロトコル）バージョン４）アドレスまたはＩＰｖ６（ＩＰバージョン６）アドレスのうち、少なくとも１つを含む。図１では、すべてのノード（ＮＲＦ１００以外）は、要求側サービスであるか提供側サービスであるかに応じて、コンシューマーＮＦまたはプロデューサーＮＦのいずれかであり得る。図示した例では、これらのノードは、ネットワークにおけるポリシー関連の操作を実行するＰＣＦ（Ｐｏｌｉｃｙ Ｃｏｎｔｒｏｌ Ｆｕｎｃｔｉｏｎ）１０２と、ユーザデータを管理するＵＤＭ（Ｕｎｉｆｉｅｄ Ｄａｔａ Ｍａｎａｇｅｍｅｎｔ）機能１０４、アプリケーションサービスを提供するＡＦ（Ａｐｐｌｉｃａｔｉｏｎ Ｆｕｎｃｔｉｏｎ）１０６とを含む。図１に示すノードは、ＡＭＦ（Ａｃｃｅｓｓ Ａｎｄ Ｍｏｂｉｌｉｔｙ Ｍａｎａｇｅｍｅｎｔ Ｆｕｎｃｔｉｏｎ）１１０とＰＣＦ１０２との間のセッションを管理するＳＭＦ（Ｓｅｓｓｉｏｎ Ｍａｎａｇｅｍｅｎｔ Ｆｕｎｃｔｉｏｎ）１０８をさらに含む。ＡＭＦ１１０は、４ＧネットワークにおいてＭＭＥ（Ｍｏｂｉｌｉｔｙ Ｍａｎａｇｅｍｅｎｔ Ｅｎｔｉｔｙ）が実行するモビリティ管理操作と同様のモビリティ管理操作を実行する。ＡＵＳＦ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｓｅｒｖｅｒ Ｆｕｎｃｔｉｏｎ）１１２は、ネットワークにアクセスしたいＵＥ（ユーザ機器）１１４など、ＵＥ（ユーザ機器）の認証サービスを実行する。

【００３０】

ＮＳＳＦ（Ｎｅｔｗｏｒｋ Ｓｌｉｃｅ Ｓｅｌｅｃｔｉｏｎ Ｆｕｎｃｔｉｏｎ）１１６は、ネットワークスライスに関連する特定のネットワーク機能および特性にアクセスしたいデバイスのためのネットワークスライシングサービスを提供する。ＮＥＦ（Ｎｅｔｗｏｒｋ Ｅｘｐｏｓｕｒｅ Ｆｕｎｃｔｉｏｎ）１１８は、ネットワークにアタッチされているＩｏＴ（Ｉｎｔｅｒｎｅｔ ｏｆ ｔｈｉｎｇｓ）デバイスおよびその他のＵＥについての情報を取得したいアプリケーション機能のためのＡＰＩ（Ａｐｐｌｉｃａｔｉｏｎ Ｐｒｏｇｒａｍｍｉｎｇ Ｉｎｔｅｒｆａｃｅ）を提供する。ＮＥＦ１１８は、４ＧネットワークにおけるＳＣＥＦ（Ｓｅｒｖｉｃｅ Ｃａｐａｂｉｌｉｔｙ Ｅｘｐｏｓｕｒｅ Ｆｕｎｃｔｉｏｎ）と同様の機能を実行する。

【００３１】

ＲＡＮ（無線アクセスネットワーク）１２０は、ワイヤレスリンクを経由してＵＥ（ユーザ機器）１１４をネットワークに接続する。無線アクセスネットワーク１２０には、ｇＮＢ（ｇ－ＮｏｄｅＢ）（図１に図示せず）またはその他のワイヤレスアクセスポイントを用いてアクセスされ得る。ＵＰＦ（Ｕｓｅｒ Ｐｌａｎｅ Ｆｕｎｃｔｉｏｎ）１２２は、ユーザプレーンサービスに関する様々なプロキシ機能をサポートできる。このようなプロキシ機能の一例は、ＭＰＴＣＰ（Ｍｕｌｔｉｐａｔｈ Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏ

ｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ）プロキシ機能である。ＵＰＦ１２２は、パフォーマンス測定機能もサポートし得る。パフォーマンス測定機能は、ネットワーク性能の測定値を取得するためにＵＥ１１４によって用いられ得る。図１には、ＵＥがインターネットサービスなどのデータネットワークサービスにアクセスするＤＮ（データネットワーク）１２４も示されている。

【００３２】

ＳＥＰＰ１２６は、別のＰＬＭＮからの受信トラフィックをフィルタリングし、ホーム側ＰＬＭＮから出るトラフィックのトポロジ隠蔽を実行する。ＳＥＰＰ１２６は、外部ＰＬＭＮのセキュリティを管理する、外部ＰＬＭＮにあるＳＥＰＰと通信し得る。よって、それぞれ異なるＰＬＭＮにおけるＮＦ間のトラフィックは、ホーム側ＰＬＭＮのためのＳＥＰＰ機能および外部ＰＬＭＮのためのＳＥＰＰ機能という２つのＳＥＰＰ機能を横断し得る。

【００３３】

上記の通り、既存の５Ｇアーキテクチャの１つの問題は、Ｎ３２－ｃハンドシェイクがリモートエンドポイントのＩＤを検証しないことである。エンドポイントのＩＤを検証しない場合、悪意があるＳＥＰＰが別のＳＥＰＰのアイデンティティになりすましてセキュリティ攻撃を仕掛ける可能性がある。応答側ＳＥＰＰは、Ｎ３２－ｃハンドシェイクメッセージを正規開始側ＳＥＰＰから受信しているかどうかを検証しない。同様に、開始側ＳＥＰＰは、Ｎ３２－ｃハンドシェイクメッセージが正規応答側ＳＥＰＰに送られるかどうかを検証しない。本明細書に記載の主題は、ＳＥＰＰのＮ３２－ｃアイデンティティを、ＴＬＳレイヤーのアイデンティティ、ならびに開始側ＳＥＰＰおよび応答側ＳＥＰＰが保持するピアＳＥＰＰデータベースに格納されているピアＳＥＰＰアイデンティティと交差検証することによって、これらのおよびその他の問題点に対処する。

【００３４】

図２は、Ｎ３２インタフェース上のＳＥＰＰ間でハンドシェイクが生じている様子を示す図である。図２では、開始側ＳＥＰＰ１２６Ａと、応答側ＳＥＰＰ１２６Ｂは、ＴＬＳハンドシェイクメッセージングおよびＮ３２－ｃセキュリティ機能ネゴシエーションメッセージングを、Ｎ３２インタフェース上で交換する。ＴＬＳハンドシェイクには、証明書の交換が含まれる。証明書は、ＴＬＳレイヤーにおいて送信者のアイデンティティを検証するために使用され得、なりすますことが困難である。しかしながら、ＴＬＳハンドシェイクの間に交換されるアイデンティティと、Ｎ３２－ｃセキュリティ機能ネゴシエーションメッセージングの間に交換されるアイデンティティとの間には交差検証が存在しない。その結果、開始側ＳＥＰＰ１２６Ａおよび応答側ＳＥＰＰ１２６Ｂの両方が、ローミングなりすまし攻撃に対して脆弱である。ローミングなりすまし攻撃とは、携帯電話加入者がローミング中のネットワークにおいて攻撃者がノードとして装う攻撃である。Ｎ３２－ｃセキュリティ機能ネゴシエーション手順の間にノードのアイデンティティになりすます場合、攻撃者は、サブスクライバがローミング中のネットワークにサービスを提供しているＳＥＰＰのアイデンティティになりすます。

【００３５】

図３は、正規ＳＥＰＰを装うハッカーＳＥＰＰ３００の例を示す図である。図３では、ＰＬＭＮ１に位置するＳＥＰＰ１２６Ａは、ＰＬＭＮ２に位置するピアＳＥＰＰ１２６Ｂと通信していると信じている。しかしながら、ハッカーＳＥＰＰ３００が正規ＳＥＰＰ１２６ＢのフリをしてＳＥＰＰ１２６ＡとのＮ３２－ｃ通信を確立している可能性がある。このような通信が確立されると、ハッカーＳＥＰＰ３００は、ＰＬＭＮ１から機密であるサブスクライバ情報を取得することができるおよび／またはＤｏＳ（Ｄｅｎｉａｌ　ｏｆ　Ｓｅｒｖｉｃｅ）攻撃などその他の種類の攻撃をＰＬＭＮ１上で引き起こすことができるようになるであろう。

【００３６】

Ｎ３２－ｃインタフェース上でなりすまし攻撃が成功してしまうのを回避するまたはその可能性を低くするために、ＳＥＰＰ１２６Ａおよび１２６Ｂは、Ｎ３２－ｃアイデンテ

ィティをＴＬＳアイデンティティと交差検証し得、さらに、構成済みのピアＳＥＰＰデータベースを用いてＮ３２－ｃアイデンティティをピアＳＥＰＰアイデンティティと検証し得る。図４は、開始側ＳＥＰＰ１２６Ａおよび応答側ＳＥＰＰ１２６Ｂが実行し得る例示的な交差検証を示す図である。図４を参照すると、開始側ＳＥＰＰ１２６Ａと応答側ＳＥＰＰ１２６Ｂは、Ｎ３２－ｃインタフェース上でＴＬＳハンドシェイクメッセージを交換してＴＬＳ接続を確立する。ＴＬＳハンドシェイクは、クライアントのｈｅｌｌｏメッセージとサーバのｈｅｌｌｏメッセージとの交換、続いて、証明書メッセージの交換を含む。証明書メッセージには、送信者のＸ．５０９証明書が含まれる。送信者のアイデンティティは、Ｘ．５０９証明書に含まれており、なりすますことは困難である。なぜならば、認証局によってＸ．５０９証明書に署名されているためである。

【００３７】

したがって、一例では、送信者のＮ３２－ｃアイデンティティを交差検証するためにＸ．５０９証明書から抽出した送信者のアイデンティティが用いられ得る。ＴＬＳハンドシェイクプロトコルは、ＩＥＴＦ（Ｉｎｔｅｒｎｅｔ Ｅｎｇｉｎｅｅｒｉｎｇ Ｔａｓｋ Ｆｏｒｃｅ）のＲＦＣ（Ｒｅｑｕｅｓｔ ｆｏｒ Ｃｏｍｍｅｎｔｓ）５２４６において規定されており、ＴＬＳ接続の両エンドによる証明書メッセージの交換を含む。ＩＥＴＦＲＦＣ５２４６において規定されているＴＬＳハンドシェイクメッセージの構造（証明書メッセージを含む）は、以下のように表示される。

【００３８】

【表１】

```
enum {
        hello_request(0), client_hello(1), server_hello(2),
        certificate(11), server_key_exchange (12),
        certificate_request(13), server_hello_done(14),
        certificate_verify(15), client_key_exchange(16),
        finished(20), (255)
    } HandshakeType;


    struct {
        HandshakeType msg_type;    /* ハンドシェイクの種類 */
        uint24 length;          /* メッセージに含まれるバイト*/
        select (HandshakeType) {
            case hello_request:       HelloRequest;
            case client_hello:        ClientHello;
            case server_hello:        ServerHello;
            case certificate:         Certificate;
            case server_key_exchange: ServerKeyExchange;
            case certificate_request: CertificateRequest;
            case server_hello_done:   ServerHelloDone;
            case certificate_verify:  CertificateVerify;
            case client_key_exchange: ClientKeyExchange;
            case finished:            Finished;
        } body;
    } Handshake;
```

【００３９】

ＴＬＳハンドシェイクメッセージの構造によって示されているように、規定されたハンドシェイクメッセージの種類の１つは、証明書メッセージである。証明書メッセージは、送信者がクライアントとして機能しているかサーバとして機能しているかに応じて、クライアントの証明書またはサーバの証明書を含む。Ｎ３２－ｃインタフェースでセキュアなＴＬＳ通信を確立する際、ＴＬＳ接続の両エンドが他方のエンドのＸ．５０９証明書を受信および検証する共通のＴＬＳまたはｍ－ＴＬＳが使用される。ＩＥＴＦ　ＲＦＣ５２４６は、明らかにネゴシエーションされない限り、証明書の種類がＸ．５０９ｖ３でなければならないことを示す。本明細書に記載の実施例では、例としてＸ．５０９ｖ３証明書を用いるが、本明細書に記載の主題は、Ｘ．５０９ｖ３から抽出した送信者のアイデンティティを用いて送信者のＮ３２－ｃアイデンティティを検証することだけに限られない。Ｘ．５０９ｖ３証明書のフォーマットは、ＩＥＴＦ　ＲＦＣ３２８０で規定されている。ＩＥＴＦ　ＲＦＣ３２８０によると、Ｘ．５０９ｖ３証明書が含み得る拡張子またはパラメ

ータは、サブジェクトの別名拡張である。サブジェクトの別名拡張は、次のように定義される。

【００４０】

サブジェクトの別名拡張により、証明書のサブジェクトに追加のアイデンティティをバインドできるようになる。定義済みオプションは、インターネット電子メールアドレスと、ＤＮＳ名と、ＩＰアドレスと、ＵＲＩ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｉｄｅｎｔｉｆｉｅｒ）とを含む。完全にローカルな定義を含む、その他のオプションも存在する。複数の名前形式、および各名前形式の複数のインスタンスが含まれてもよい。このようなアイデンティティが証明書にバインドされる時はいつも、サブジェクトの別名（発行者の別名）拡張を使わなければならない。しかしながら、ＤＮＳ名は、４．１．２．４節に記載されているように、ｄｏｍａｉｎＣｏｍｐｏｎｅｎｔ属性を用いてサブジェクトフィールドで表されてもよい。

【００４１】

サブジェクトの別名は、最終的に公開鍵にバインドされると考えられるので、サブジェクトの別名のすべての部分をＣＡによって確認しなければならない。

【００４２】

上記の通り、Ｘ．５０９ｖ３証明書のサブジェクトの別名拡張は、証明書のサブジェクトを識別する、認証局によって確認されるＤＮＳ名、ＩＰアドレス、またはＵＲＩを含み得る。サブジェクトの別名は認証局によって確認されるので、サブジェクトの別名をなりすますことは困難である。しかしながら、送信者が有効なＸ．５０９証明書を有していることを確実にするだけでは、Ｎ３２－ｃアプリケーションレベルで送信者のアイデンティティを検証することにならない。このような交差検証を実行するために、開始側ＳＥＰＰ１２６Ａおよび応答側ＳＥＰＰ１２６Ｂは、Ｎ３２－ｃメッセージからアイデンティティを抽出し、これらのアイデンティティを、ＴＬＳハンドシェイクの間に共有したＸ－５０９証明書から抽出したアイデンティティと比較し得る。これらのアイデンティティが一致した場合、ＳＥＰＰ１２６Ａおよび１２６Ｂは、Ｎ３２－ｃメッセージまたはＴＬＳメッセージのいずれかから抽出したアイデンティティを構成済みピアＳＥＰＰアイデンティティのデータベースと比較するさらなる検証ステップを実行し得る。いずれの検証も失敗した場合、ＳＥＰＰは、リモートノードとのＰＬＭＮ間通信をブロックし得、リモートノードを攻撃者として識別する。

【００４３】

図４に戻ると、開始側ＳＥＰＰ１２６Ａと応答側ＳＥＰＰ１２６Ｂとの間でＴＬＳハンドシェイクメッセージが交換され、ＴＬＳ接続が確立された後、開始側ＳＥＰＰ１２６Ａは、ＨＴＴＰ　ＰＯＳＴメッセージを応答側ＳＥＰＰ１２６Ｂに送る。ＨＴＴＰ　ＰＯＳＴメッセージは、ＳｅｃＮｅｇｏｔｉａｔｅＲｅｑＤａｔａ情報要素を含む。ＳｅｃＮｅｇｏｔｉａｔｅＲｅｑＤａｔａ情報要素は、送信者のＦＱＤＮを含んだ送信者情報要素を含む。応答側ＳＥＰＰ１２６Ｂは、ＨＴＴＰ　ＰＯＳＴメッセージを受信し、ＳｅｃＮｅｇｏｔｉａｔｅＲｅｑＤａｔａ情報要素から送信者のＦＱＤＮを抽出し、送信者のＸ．５０９証明書から取得した送信者のアイデンティティに照らしてＦＱＤＮを検証する。この場合、これらのアイデンティティが一致すると仮定する。したがって、次のステップでは、応答側ＳＥＰＰ１２６Ｂは、応答側ＳＥＰＰ１２６Ｂが保持するピアＳＥＰＰデータベースでルックアップを実行し、送信者のアイデンティティを検索する。開始側ＳＥＰＰ１２６Ａのアイデンティティが応答側ＳＥＰＰ１２６ＢのピアＳＥＰＰデータベース上に存在すると仮定するので、応答側ＳＥＰＰ１２６Ｂの観点からは両方の検証が合格となり、その結果、応答側ＳＥＰＰ１２６Ｂは、開始側ＳＥＰＰ１２６ＡからのＰＬＭＮ間通信を許可する。

【００４４】

図４のメッセージフローを引き続き参照すると、応答側ＳＥＰＰ１２６Ｂは、開始側ＳＥＰＰ１２６ＡにＨＴＴＰ　２００　ＯＫ　メッセージを送る。ＨＴＴＰ　２００　ＯＫ　メッセージは、送信者属性を含んだＮ３２－ｃＳｅｃＮｅｇｏｔｉａｔｅＲｓｐＤａｔａ情

報要素を含む。図５では、送信者属性は、応答側ＳＥＰＰ１２６ＢのＦＱＤＮを保持している。開始側ＳＥＰＰ１２６Ｂは、ＨＴＴＰ　２００　ＯＫ　メッセージを受信し、ＳｅｃＮｅｇｏｔｉａｔｅＲｓｐＤａｔａ情報要素の送信者属性から送信者のＦＱＤＮを抽出し、このＦＱＤＮをＴＬＳ証明書メッセージから抽出した送信者のＦＱＤＮと比較する。この場合、これらのＦＱＤＮが一致すると仮定する。したがって、開始側ＳＥＰＰ１２６Ａは、開始側ＳＥＰＰ１２６Ａが保持するピアＳＥＰＰデータベースに送信者のアイデンティティが存在するかどうかを判断するさらなる検証ステップを実行する。この例では、送信者のアイデンティティが存在すると仮定するので、開始側ＳＥＰＰ１２６Ａは、応答側ＳＥＰＰ１２６ＢとのＰＬＭＮ間通信を許可する。

【００４５】

図５は、Ｎ３２－ｃセキュリティ機能ネゴシエーション手順に関してハッカーＳＥＰＰ３００が開始側ＳＥＰＰである場合を説明する図である。図５では、ハッカーＳＥＰＰ３００は、応答側ＳＥＰＰ１２６ＢとのＴＬＳハンドシェイクを開始する。応答側ＳＥＰＰ１２６Ｂは、ＴＬＳハンドシェイクメッセージからＸ．５０９証明書を抽出し、証明書においてハッカーＳＥＰＰ３００が提示するアイデンティティを抽出する。ハッカーＳＥＰＰ３００は、アイデンティティをＮ３２－ｃセキュリティ機能ネゴシエーションメッセージ（図示した例では、ＨＴＴＰ　ＰＯＳＴメッセージ）のＮ３２－ｃＳｅｃＮｅｇｏｔｉａｔｅＲｅｑＤａｔａ情報要素に含めて応答側ＳＥＰＰ１２６Ｂに伝達する。応答側ＳＥＰＰ１２６Ｂは、Ｎ３２－ｃセキュリティ機能ネゴシエーションメッセージのＮ３２－ｃＳｅｃＮｅｇｏｔｉａｔｅＲｅｑＤａｔａ情報要素にあるハッカーＳＥＰＰ３００が提示するアイデンティティを抽出し、Ｎ３２－ｃセキュリティ機能ネゴシエーションメッセージのＳｅｃＮｅｇｏｔｉａｔｅＲｅｑＤａｔａ情報要素から抽出したアイデンティティをＴＬＳメッセージから取得した証明書から抽出したアイデンティティと比較する。この場合、これらのアイデンティティは一致しない。その結果、応答側ＳＥＰＰ１２６Ｂは、検証が失敗したと判断する。したがって、応答側ＳＥＰＰ１２６Ｂは、ハッカーＳＥＰＰ３００からのその後の通信をブロックする。

【００４６】

図６は、Ｎ３２－ｃセキュリティ機能ネゴシエーショントランザクションにおいてＴＬＳのアイデンティティとＮ３２－ｃのアイデンティティの交差検証を実行するＳＥＰＰが、開始側ＳＥＰＰである場合を示す図である。図６では、開始側ＳＥＰＰは、ハッカーＳＥＰＰ３００からＴＬＳメッセージおよびＮ３２－ｃメッセージを受信する。開始側ＳＥＰＰ１２６Ａは、ＴＬＳハンドシェイクメッセージのうち１つからＸ．５０９証明書を取得する。開始側ＳＥＰＰ１２６Ａは、Ｘ．５０９証明書からアイデンティティを抽出し、このアイデンティティをＮ３２－ｃセキュリティ機能ネゴシエーションメッセージ（図示した例では、ＨＴＴＰ　２００　ＯＫ　メッセージ）のＳｅｃＮｅｇｏｔｉａｔｅＲｓｐＤａｔａ情報要素にあるハッカーＳＥＰＰ３００から受信したアイデンティティと比較する。この場合、これらのアイデンティティは、一致しない。したがって、開始側ＳＥＰＰ１２６Ａは、ハッカーＳＥＰＰ３００とのその後の通信をブロックする。

【００４７】

図７は、ＳＥＰＰ１２６Ａまたは１２６Ｂの例示的なアーキテクチャを示すブロック図である。ＳＥＰＰ１２６Ａまたは１２６Ｂは、少なくとも１つのプロセッサ７００と、メモリ７０２とを備える。ＳＥＰＰ１２６Ａまたは１２６Ｂは、Ｎ３２－ｃメッセージにあるアイデンティティとＴＬＳメッセージから抽出したアイデンティティと交差検証するための本明細書に記載のこれらのステップを実行する５Ｇローミングなりすまし緩和モジュール７０４をさらに備える。ＳＥＰＰ１２６Ａまたは１２６Ｂは、ＰＬＭＮ間通信が許可されているピアＳＥＰＰのアイデンティティで構成されたピアＳＥＰデータベース７０６をさらに備える。５Ｇローミングなりすまし緩和モジュール７０４は、プロセッサ７００によって実装され得、また、データベース７０６に格納されているピアＳＥＰＰアイデンティティに照らして、リモートノードが提示するＮ３２－ｃアイデンティティのクロスチェックを実行し得る。Ｎ３２－ｃセキュリティ機能ネゴシエーションメッセージにおいて

提示されたリモートノードのアイデンティティがデータベース７０６に存在しない場合、または、ＴＬＳアイデンティティとのクロスチェックが失敗した場合、５Ｇローミングなりすまし緩和モジュール７０４は、リモートノードとのＰＬＭＮ間通信をブロックし得る。両方のアイデンティティクロスチェックが合格であった、５Ｇローミングなりすまし緩和モジュール７０４は、リモートノードとのＰＬＭＮ間通信を許可し得る。

【００４８】

図８は、５Ｇスピーキング攻撃を緩和するための例示的な方法を示すフローチャートである。図８を参照すると、ステップ８００では、ＳＥＰＰが、第１ノードからのＴＬＳメッセージから第１識別子を取得する。たとえば、開始側または応答側ＳＥＰＰ１２６Ａまたは１２６Ｂは、送信側ノードから受信したＴＬＳメッセージにあるＸ．５０９証明書の別ＩＤフィールドから、送信側ノードのアイデンティティを抽出し得る。ＴＬＳメッセージは、リモートノードとのＴＬＳ接続を確立するための用いられるＴＬＳハンドシェイク手順の一部としてリモートノードと交換する証明書メッセージであり得る。

【００４９】

ステップ８０２では、ＳＥＰＰは、第１ノードからのＮ３２－ｃセキュリティ機能ネゴシエーションメッセージから、第１ノードの第２識別子を取得する。たとえば、ＳＥＰＰがＮ３２－ｃセキュリティ機能ネゴシエーショントランザクションを目的とする開始側ＳＥＰＰである場合、開始側ＳＥＰＰは、リモートノードからのＨＴＴＰ　２００　ＯＫ　メッセージのＮ３２－ｃＳｅｃＮｅｇｏｔｉａｔｅＲｓｐＤａｔａ情報要素の送信者ＩＤ属性から、Ｎ３２ｃアイデンティティを抽出し得る。ＳＥＰＰがＮ３２－ｃセキュリティ機能ネゴシエーショントランザクションを目的とする応答側ＳＥＰＰである場合、応答側ＳＥＰＰは、リモートノードからのＨＴＴＰ　ＰＯＳＴメッセージのＮ３２－ｃＳｅｃＮｅｇｏｔｉａｔｅＲｅｑＤａｔａ情報要素の送信者ＩＤ属性から、Ｎ３２ｃアイデンティティを抽出し得る。以下に示す表１および表２は、Ｎ３２－ｃセキュリティ機能ネゴシエーションの一部であるＳｅｃＮｅｇｏｔｉａｔｅＲｅｑＤａｔａおよびＳｅｃＮｅｇｏｔｉａｔｅＲｓｐＤａｔａ情報要素に含まれ得る属性を示す、３ＧＰＰ　ＴＳ２９．５７３の表６．１．５．２．２．１および表６．５．１．２．２に対応する。

【００５０】

【表２】

表１：ＳｅｃＮｅｇｏｔｉａｔｅＲｅｑＤａｔａタイプの定義

属性名	データタイプ	P	濃度	説明
sender	Fqdn	M	1	このＩＥは、リクエストを送信しているＳＥＰＰを一意に識別する。このＩＥは、ネゴシエーションされたセキュリティ機能を正しいＳＥＰＰに照らして格納するために使われる。
supportedSecCapabilityList	array(SecurityCapability)	M	1..N	このＩＥは、要求側ＳＥＰＰがサポートするセキュリティ機能の一覧を含む。

【００５１】

【表３】

表２：ＳｅｃＮｅｇｏｔｉａｔｅＲｓｐＤａｔａタイプの定義

属性名	データタイプ	Ｐ	濃度	説明
sender	Fqdn	M	1	このＩＥは、レスポンスを送信しているＳＥＰＰを一意に識別する。このＩＥは、ネゴシエーションされたセキュリティ機能を正しいＳＥＰＰに照らして格納するために使われる。
selectedSecCapability	SecurityCapability	M	1	このＩＥは、応答側ＳＥＰＰが選択したセキュリティ機能を含む。

【００５２】

表１および表２からわかるように、送信者属性は、ＳｅｃＮｅｇｏｔｉａｔｅＲｅｑＤａｔａ情報要素およびＳｅｃＮｅｇｏｔｉａｔｅＲｓｐＤａｔａ情報要素の必須パラメータであり、リクエストまたはレスポンスを送るＳＥＰＰのＦＱＤＮを含む。ＴＬＳレイヤーのアイデンティティと交差検証され得るのはこのＦＱＤＮである。

【００５３】

ステップ８０４では、ＳＥＰＰは、第１ノードの第１識別子と第２識別子を比較する。たとえば、ＳＥＰＰは、Ｘ．５０９証明書から抽出したＴＬＳ識別子をＮ３２－ｃセキュリティ機能ネゴシエーションメッセージのＳｅｃＮｅｇｏｔｉａｔｅＲｓｐＤａｔａ情報要素またはＳｅｃＮｅｇｏｔｉａｔｅＲｅｑＤａｔａ情報要素から抽出したＮ３２－ｃ識別子と比較し得る。

【００５４】

ステップ８０６では、これらの識別子が一致しなかった場合、制御は、ステップ８０８に進む。ステップ８０８では、ＳＥＰＰが、第１ノードの第２の（Ｎ３２－ｃ）アイデンティティを無効であると分類する。その後、制御は、ステップ８１０に進む。ステップ８１０では、ＳＥＰＰは、第１ノードからのＰＬＭＮ間通信をブロックする。

【００５５】

ステップ８０６に戻ると、ＴＬＳのアイデンティティとＮ３２－ｃアプリケーションレイヤーのアイデンティティが一致した場合、制御は、ステップ８１２に進む。ステップ８１２では、ＳＥＰＰは、ピアＳＥＰＰデータベースでルックアップを実行し、第１ノードのアイデンティティを検索する。ステップ８０６においてＴＬＳレイヤーのアイデンティティとＮ３２ｃ（アプリケーション）レイヤーのアイデンティティが一致したので、ＴＬＳレイヤーのアイデンティティまたはＮ３２－ｃレイヤーのアイデンティティのいずれかを用いてルックアップが実行され得る。ネットワーク事業者のネットワークにある所与のＳＥＰＰが通信を許可されるＳＥＰＰのアイデンティティを有するピアＳＥＰＰデータベースが事業者によってプロビジョニングされ得る。このようなＳＥＰＰは、本明細書において、ピアＳＥＰＰと称する。なぜならば、ピアネットワーク事業者のＰＬＭＮと対応付けられ得るためである。

【００５６】

ステップ８１４では、ピアＳＥＰＰデータベースにアイデンティティが存在する場合、制御は、ステップ８１６に進む。ステップ８１６では、ＳＥＰＰは、第１ノードとのＰＬＭＮ間通信を許可する。データベースにアイデンティティが存在しない場合、制御は、ステップ８１０に進む。ステップ８１０では、ＳＥＰＰは、第１ノードとのＰＬＭＮ間通信

をブロックする。

【００５７】

本明細書に記載の主題は、異なるネットワークプロトコルレイヤーにあるＳＥＰＰ間で交換されるアイデンティティの交差検証を実行することによって、ＳＥＰＰとＰＬＭＮとの間のネットワークセキュリティを改善する。Ｎ３２－ｃアイデンティティを、なりすますことが困難なＴＬＳレイヤーアイデンティティと比較することによって、本明細書に記載のＳＥＰＰは、Ｎ３２－ｃセキュリティ機能交換手順の間になりすまし攻撃が成功する可能性を低くする。これに加えて、本明細書に記載の交差検証ステップを、Ｎ３２セキュリティ機能ネゴシエーションにおける開始側ＳＥＰＰおよび応答側ＳＥＰＰの両方で実行できるので、攻撃者がＮ３２－ｃ接続のいずれのエンドになりすましてしまうことが成功する可能性を低くする。

【００５８】

下記文献の各々の開示内容のすべてを引用により本明細書に援用する。

文献

1. IETF RFC5246; The Transport Layer Security (TLS) Protocol, Version 1.2; August 2008

2. IETF RFC3280; Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002.

3. 3GPP TS 29.573; 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 5G System; Public Land Mobile Network (PLMN) Interconnection; Stage 3 (Release 16) V16.3.0 (2020-07)

4. 3GPP TS 33.501; 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Architecture and Procedures for the 5G System; (Release 16), V16.3.0 (2020-07).

5. 3GPP TS 29.510; 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 5G System; Network Function Repository Services; Stage 3 (Release 16), V16.4.0 (2020-07).

今回開示した主題の様々な詳細は、今回開示した主題の範囲を逸脱することなく変更してもよいことが理解されるであろう。さらには、上記の説明は、あくまで例示にすぎず、限定ではない。

【図面】

【図１】

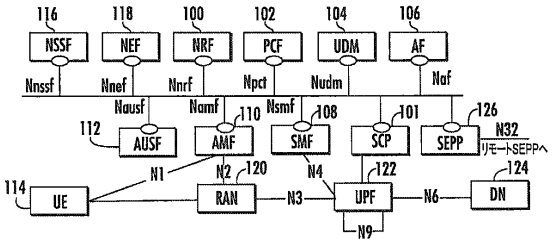

FIG. 1

【図２】

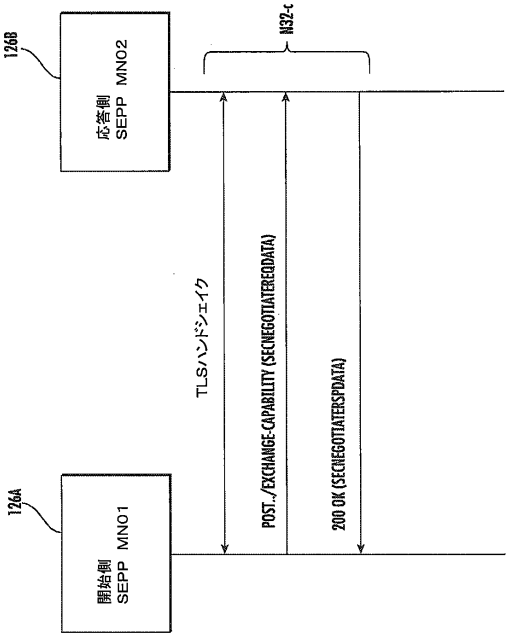

FIG. 2

【図３】

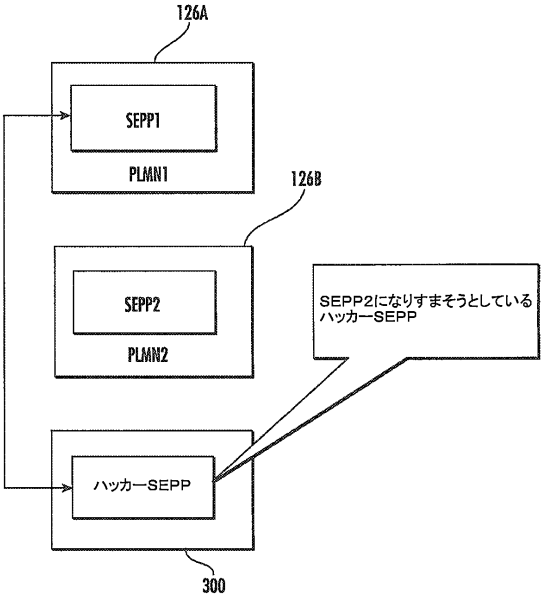

FIG. 3

【図４】

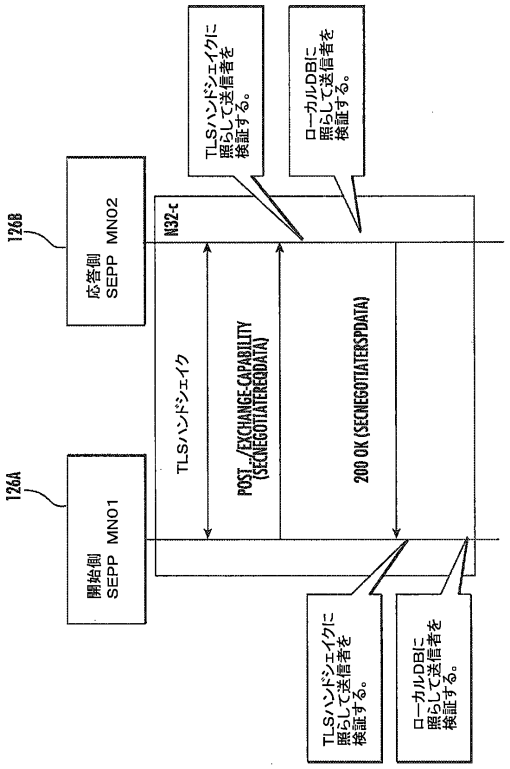

FIG. 4

【図５】

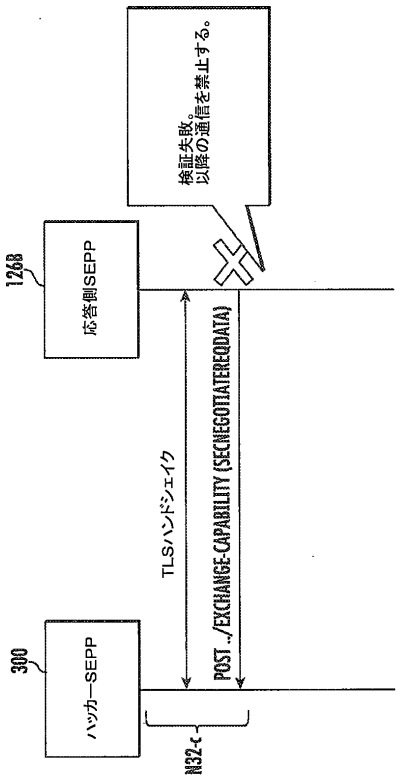

FIG. 5

【図６】

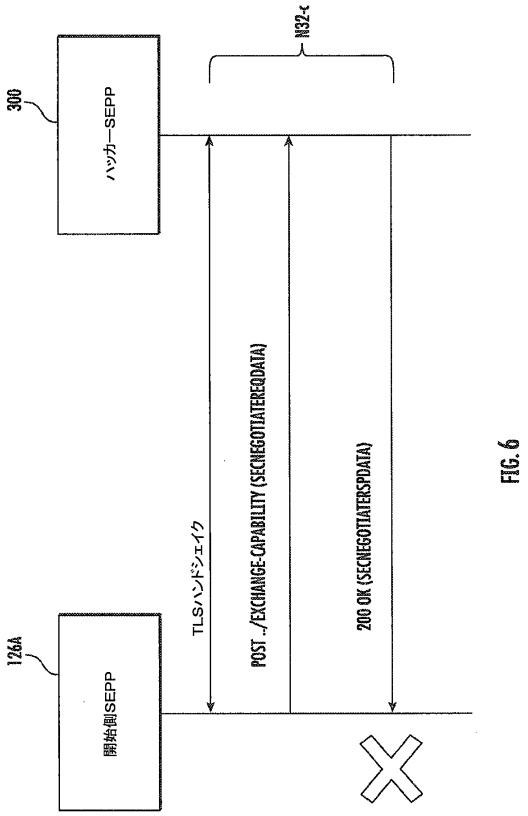

FIG. 6

【図７】

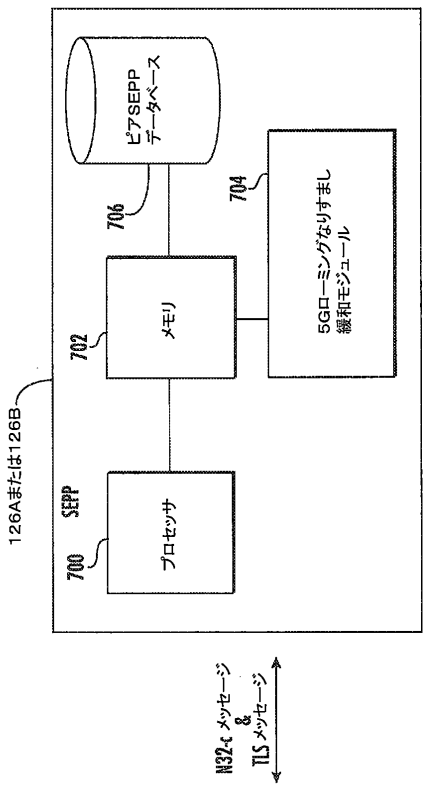

FIG. 7

【図８】

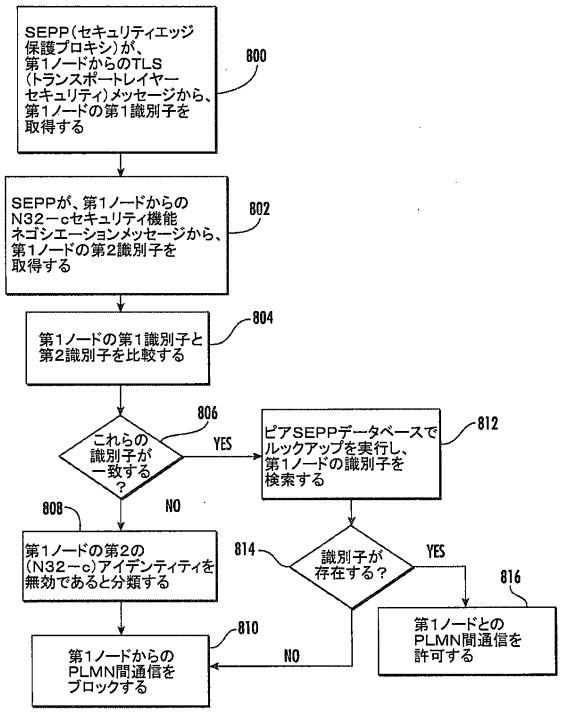

FIG. 8

フロントページの続き

(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号 202041041754
(32)優先日 令和2年9月25日(2020.9.25)
(33)優先権主張国・地域又は機関
インド(IN)
(31)優先権主張番号 202041047779
(32)優先日 令和2年11月2日(2020.11.2)
(33)優先権主張国・地域又は機関
インド(IN)
インド、５６００７６ バンガロール、フリマビュー、トゥウェンティーフォース・クロス、ケンパマ・レイアウト、ブイ・２・バイブハブ・アパートメント、ユニット・ナンバー・００３
審査官 望月 章俊
(56)参考文献 Deutsche Telekom AG，N32 message anti-spoofing within the SEPP[online]，3GPP TSG SA WG3 #91 S3-181480，Internet〈URL:https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_91_Belgrade/Docs/S3-181480.zip〉，2018年04月20日，[検索日 2025.01.21]
Huawei, Hisilicon，New Annex for the SEPP in TR 33.926[online]，3GPP TSG SA WG3 #95 Bis S3-192180，Internet〈URL:https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_95Bis_Sapporo/Docs/S3-192180.zip〉，2019年06月17日，[検索日 2025.01.21]
(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｗ４／００－Ｈ０４Ｗ９９／００
Ｈ０４Ｂ７／２４－Ｈ０４Ｂ７／２６
３ＧＰＰ ＴＳＧ ＲＡＮ ＷＧ１－４
ＳＡ ＷＧ１－４
ＣＴ ＷＧ１、４