(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6144783号
(P6144783)
(45)発行日　平成29年6月7日(2017.6.7)　(24)登録日　平成29年5月19日(2017.5.19)

(51)Int.Cl.　　F I
H04L 12/66 (2006.01)　　H04L 12/66 B
H04L 12/70 (2013.01)　　H04L 12/70 B

請求項の数 18　(全 15 頁)

(21)出願番号　特願2015-561925(P2015-561925)
(86)(22)出願日　平成26年3月13日(2014.3.13)
(65)公表番号　特表2016-509457(P2016-509457A)
(43)公表日　平成28年3月24日(2016.3.24)
(86)国際出願番号　PCT/CN2014/073339
(87)国際公開番号　WO2014/139444
(87)国際公開日　平成26年9月18日(2014.9.18)
審査請求日　平成27年10月23日(2015.10.23)
(31)優先権主張番号　61/780,805
(32)優先日　平成25年3月13日(2013.3.13)
(33)優先権主張国　米国(US)
(31)優先権主張番号　13/970,713
(32)優先日　平成25年8月20日(2013.8.20)
(33)優先権主張国　米国(US)

(73)特許権者　504161984
ホアウェイ・テクノロジーズ・カンパニー・リミテッド
中華人民共和国・５１８１２９・グァンドン・シェンツェン・ロンガン・ディストリクト・バンティアン・（番地なし）・ホアウェイ・アドミニストレーション・ビルディング
(74)代理人　100146835
弁理士　佐伯　義文
(74)代理人　100140534
弁理士　木内　敬二

最終頁に続く

(54)【発明の名称】情報中心のネットワークにおけるトラストアンカーを用いたプロトコルのルーティングに基づく名前／プレフィックスの増加

(57)【特許請求の範囲】
【請求項１】
装置であって、前記装置は、
メモリと、
メモリに接続されたプロセッサと、を含み、前記メモリは、前記プロセッサによって実行されるとき、前記装置に、
情報指向ネットワーク（ＩＣＮ）に接続されるかまたは含まれるコンテンツ提供者ノード固有のメッセージプレフィックスと、
前記コンテンツ提供者固有の公開鍵と、
名前登録サービス（ＮＲＳ）の秘密鍵によってサインされた、前記コンテンツ提供者固有のデジタル署名と、
を含む、ＩＣＮ名前プレフィックス報知メッセージを受信させ、
前記ＮＲＳの公開鍵を用いて、前記署名を検証させ、
前記コンテンツ提供者が信頼できる提供者であることを示す内部データをアップデートさせる命令を含み、前記内部データは、前記プレフィックス、前記コンテンツ提供者固有の公開鍵、および前記署名を含む、装置。
【請求項２】
前記内部データが、インタフェースを示すための転送テーブルを含み、パケットが前記インタフェースを通して転送される、請求項１に記載の装置。
【請求項３】

名前登録サービスの公開鍵を用いた前記署名の検証が、前記名前登録サービスが前記コンテンツ提供者から前記コンテンツ提供者固有の公開鍵および付加情報を受信したことを検証することを含む、請求項１に記載の装置。

【請求項４】

前記ＩＣＮ名前プレフィックス報知メッセージが、ルータとデータを交換するための、第１の鍵付きハッシュメッセージ認証符号（ＨＭＡＣ）をさらに含む、請求項１に記載の装置。

【請求項５】

前記命令が、第２のＨＭＡＣを前記装置にさらに生成させ、前記命令は、前記第２のＨＭＡＣを対象として前記第１のＨＭＡＣを前記装置にさらに検証させ、ここで、前記検証をパスしたとき、前記ＩＣＮ名前プレフィックス報知メッセージは容認され、前記検証が失敗したとき、前記ＩＣＮ名前プレフィックス報知メッセージがドロップされる、請求項４に記載の装置。

【請求項６】

前記命令が、前記装置にルータとのセキュア・セッション・キー（ＳＳＫ）をさらに確立させる、請求項１に記載の装置。

【請求項７】

前記命令が、

前記コンテンツ提供者固有の前記メッセージプレフィックスと、

前記コンテンツ提供者固有の前記公開鍵と、

前記コンテンツ提供者固有の前記署名と、

を含む、ＩＣＮ名前プレフィックス取り消しメッセージの受信と、

前記ＮＲＳを用いた、前記署名の検証と、

前記プレフィックスを取り消すための内部データのアップデートと、を前記装置にさらにさせる、請求項１に記載の装置。

【請求項８】

プロセッサによって実行されるとき、前記プロセッサに、

第１のインタフェース経由での、プレフィックスとデジタル署名とを具備する情報指向ネットワーク（ＩＣＮ）名前プレフィックス報知メッセージの受信と、

前記第１のインタフェース、前記プレフィックス、および前記署名に対応するテーブルエントリのためのテーブルの問い合わせと、

前記テーブルエントリが前記テーブルに存在するとき、第２のインタフェース経由での、前記ＩＣＮ名前プレフィックス報知メッセージの転送と、

をさせる、持続性メディア上に格納されたコンピュータ実行可能な命令を含む、コンピュータプログラム。

【請求項９】

前記テーブルエントリが前記テーブルに存在しないとき、前記命令は、前記プロセッサに、

第３のインタフェース、前記プレフィックス、および前記署名に対応する第２のテーブルエントリのための前記テーブルの問い合わせと、

前記第２のテーブルエントリが存在するとき、前記第３のインタフェース経由での、前記ＩＣＮ名前プレフィックス報知メッセージの転送と、をさらにさせる、

請求項８に記載のコンピュータプログラム。

【請求項１０】

前記ＩＣＮ名前プレフィックス報知メッセージが、第１の鍵付きハッシュメッセージ認証符号（ＨＭＡＣ）をさらに含む、請求項８に記載のコンピュータプログラム。

【請求項１１】

前記命令が、前記プロセッサに、

第２のＨＭＡＣの生成と、

前記第１のＨＭＡＣと前記第２のＨＭＡＣとの比較と、

前記比較が、前記ＩＣＮ名前プレフィックス報知メッセージが認証されないことを示すとき、前記ＩＣＮ名前プレフィックス報知メッセージのドロップと、をさらにさせる、請求項１０に記載のコンピュータプログラム。

【請求項１２】

ルーティングプロトコルに基づいた名前プレフィックスを実行する方法であって、

プレフィックス、署名、および公開鍵を含む、第１の情報指向ネットワーク（ＩＣＮ）名前プレフィックス報知メッセージを受信するステップと、

前記ＩＣＮ名前プレフィックス報知メッセージに対応するエントリのための、ルーティングテーブルを照会するステップであって、ここで前記ルーティングテーブルは、それぞれのエントリフィールドのための、プレフィックス、署名、および公開鍵フィールドを含む、ステップと、

前記エントリが前記ルーティングテーブルに存在するという確認を受信すると、前記ＩＣＮ名前プレフィックス報知メッセージを転送するステップと、

を含む、方法。

【請求項１３】

前記第１のＩＣＮ名前プレフィックス報知メッセージが、第１のインタフェース経由で受信され、ここで、前記ルーティングテーブルは、第３のインタフェースに対応する前記プレフィックス、前記署名、および前記公開鍵のための第２のエントリを含み、ここで、前記ルーティングテーブルは、前記第1のインタフェースに対応する前記プレフィックス、前記署名、および前記公開鍵のためのエントリを含まず、前記第３のインタフェースに従って、第３のＩＣＮ名前プレフィックス報知メッセージを転送するステップを、さらに含む、請求項１２に記載の方法。

【請求項１４】

第２のインタフェースが、リンクベースのセキュア・セッション・キー（ＳＳＫ）を利用する、請求項１２に記載の方法。

【請求項１５】

名前登録サービス（ＮＲＳ）からの前記確認が、追加された提供者提供の許可情報と対をなす許可のための、提供者の要求に応答して、前記ＮＲＳが前記署名を作成したことを示す、請求項１４に記載の方法。

【請求項１６】

前記プレフィックス、前記署名、および前記公開鍵を含む、ＩＣＮプレフィックス取り消しメッセージを受信するステップと、

名前登録サービス（ＮＲＳ）を用いて、前記署名の検証をするステップと、

前記プレフィックスを取り消すための、前記ルーティングテーブルをアップデートするステップと、をさらに含む、請求項１２に記載の方法。

【請求項１７】

前記ＩＣＮ名前プレフィックス報知メッセージが、ルータとデータを交換するための、第１の鍵付きハッシュメッセージ認証符号（ＨＭＡＣ）をさらに含む、請求項１２に記載の方法。

【請求項１８】

第２のＨＭＡＣを生成するステップと、

前記第２のＨＭＡＣを対象として前記第１のＨＭＡＣを検証するステップと、

前記検証をパスしたとき、前記ＩＣＮ名前プレフィックス報知メッセージを転送するステップと、

前記検証が失敗したとき、前記ＩＣＮ名前プレフィックス報知メッセージを中断するステップと、をさらに含む、請求項１７に記載の方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本出願は、「Method For Augmenting Name/Prefix Based Routing Protocols With Tru

st Anchor In Information-Centric Networks」という名称のXinwen Zhangらによって2013年3月13日に出願された米国特許出願第61/780,805号の優先権を主張する、「Augmenting Name/Prefix based Routing Protocols With Trust Anchor In Information-Centric Networks」という名称のXinwen Zhangらによって2013年8月20日に出願された米国特許仮出願第13/970,713号に対する優先権を主張するものであり、両者は、参照によりその全体が本明細書に組み込まれている。

【０００２】

連邦政府による資金提供を受けた研究開発の記載

適用不可。

【０００３】

マイクロフィッシュの補遺の参照

適用不可。

【背景技術】

【０００４】

現代の通信およびデータネットワークは、ネットワークを介してデータを搬送するルータ、スイッチ、ブリッジ、および他のデバイスのようなネットワークノードを含む。年とともに、通信業界は、ネットワークノードに対して、インターネット・エンジニアリング・タスクフォース（ＩＥＴＦ）によって標準化されたプロトコルと仕様との増加をサポートするための重要な改良を行った。様々なＩＥＴＦ標準規格（例えば、仮想プライベートネットワーク要求）をサポートおよび実装するネットワークを形成するための複雑なネットワークノードの生成および結合は、現代のネットワークが複雑になり、管理が難しくなる原因となる。結果として、ベンダおよびサードパーティオペレータは、ネットワークノードの織り交ざったウェブの性能のカスタマイズ、最適化、および向上を模索している。

【０００５】

情報指向ネットワーク（ＩＣＮ）は、データを交換するエンドホストに接続するよりもむしろ、位置を決定し、ユーザに情報を提供することに焦点をおいた、ネットワークアーキテクチャのタイプである。ＩＣＮの一つのタイプは、コンテンツ指向ネットワーク（ＣＯＮ）である。コンテンツ・セントリック・ネットワーク（ＣＣＮ）とも呼ばれるＣＯＮにおいて、コンテンツルータは、適切な受信者にユーザの要求やコンテンツをルーティングする責任がある。エンティティは、ビデオクリップまたはウェブページのようなデータコンテンツ、および／またはルータ、スイッチ、またはサーバのようなインフラ要素を含んでもよい。

【０００６】

ＩＣＮは、現在のホスト間モデル（例えば、インターネットモデル）から情報オブジェクト間モデル（例えば、ＩＣＮモデル）に、通信モデルをシフトすることによって、既存のインターネットプロトコル（ＩＰ）ネットワークを越える。ＩＣＮにおいて、情報オブジェクトは、通信モデル内に存在するエンティティのための第１クラスアブすトラクションとなる。情報オブジェクトは、名前を割り当てられ、そのように命名されたオブジェクトとやりとりするルーティングは、それらの名前に基づく。ＩＣＮにおいて、ＩＰアドレスは、名前の特別なタイプとして処理されてもよい。情報オブジェクトを取り出したいユーザは、そのような要求を送信するとき、ユーザが目的のホストのＩＰアドレスを特定する必要がある現在のＩＰネットワークと異なり、それらがどこに位置されているのかを知る必要がない。

【０００７】

したがって、ＩＣＮおよび他のコンテンツベースのインターネットアーキテクチャは、要求パケットに組み込まれたコンテンツ名、プレフィックス、または識別子（ＩＤ）に基づいてルータがデータ要求を次のホップノードに送るように、ルーティングラベルとしてコンテンツ名またはプレフィックスを使用する。組み込み信用検証構造なしで、悪質なクライアント（例えば、ボットネッツ（botnets））は、ネットワークに捏造プレフィックスを投入できる。これらの悪質な行為は、高額のネットワークリソースを消費し、低下さ

せ、または例えばルータのようなネットワークインフラ内の一つもしくは複数の構成要素に対して、例えばサービス拒否（ＤｏＳ）あるいは分散型ＤｏＳ（ＤＤｏＳ）攻撃で、良いユーザのアクセスを妨げる。他の悪質なクライアントは、例えばコンテンツプロバイダ／所有者に対するＤｏＳ攻撃で、ユーザが有効なデータを受信することを妨げ、電子コンテンツの良い提供者のコンテンツ名および／またはプレフィックスを公開し得る。例えばフェイスおよび／またはプレフィックスを用いたレート制御のような提案された解決法は、悪質なクライアントの適応行動、例えば、架空の名前、および／またはフェイスなどのために、大抵は効果がなく、要求処理の増加によるユーザの体感品質（ＱｏＥ）の潜在的な減少が証明されている。

【発明の概要】

【課題を解決するための手段】

【０００８】

一実施形態では、本開示は、メモリと、メモリに接続されたプロセッサと、を含み、前記メモリは、前記プロセッサによって実行されるとき、前記装置に、ＩＣＮに接続されるかまたは含まれるコンテンツ提供者ノードに対して固有の、メッセージプレフィックスと、前記コンテンツ提供者に対して固有の、公開鍵暗号化証明書と、前記コンテンツ提供者に対して固有の、デジタル署名と、を含む、ＩＣＮ名前プレフィックス報知メッセージの受信と、名前登録サービス（ＮＲＳ）を用いた、前記署名の検証と、前記コンテンツ提供者が信頼できる提供者であることを示す内部データのアップデートであって、前記内部データは、前記プレフィックス、前記公開鍵、および前記署名を含む、アップデートと、を実行させる命令を含む、装置を包含する。

【０００９】

別の実施形態では、本開示は、プロセッサによって実行されるとき、前記プロセッサに、第１フェイス経由での、ＩＣＮ名前プレフィックス報知メッセージの受信と、前記第１のフェイス、前記プレフィックス、および前記署名に対応するテーブルエントリのためのデータテーブルの問い合わせと、前記テーブルエントリが前記テーブルに存在するとき、第２のフェイス経由での、前記プレフィックス報知の転送と、前記テーブルエントリが前記テーブルに存在しないとき、信号検証要求のＮＲＳに対する送信と、ここで、前記要求は、前記署名を含み、前記要求に応答して検証失敗通知を前記ＮＲＳから受信したとき、前記データを中断し、前記要求に応答して検証確認通知を前記ＮＲＳから受信したとき、前記第１のフェイス、前記プレフィックス、および前記署名に対応した、前記テーブルエントリの作成と、前記第２のフェイス経由での、前記プレフィックス報知メッセージの転送と、をさせる、持続性メディア上に格納されたコンピュータ実行可能な命令を含む、コンピュータプログラムを包含する。

【００１０】

また別の実施形態では、本開示は、ルーティングプロトコルに基づいた名前プレフィックスを実行する方法であって、プレフィックス、署名、および公開鍵証明書を含む、第１の情報指向ネットワーク（ＩＣＮ）名前プレフィックス報知メッセージを受信するステップと、前記プレフィックス報知メッセージに対応するエントリのための、ルーティングテーブルを問い合わせるステップであって、ここで前記ルーティングテーブルは、それぞれのエントリフィールドのための、プレフィックス、署名、および公開鍵暗号化証明書フィールドを含む、ステップと、前記エントリが、前記ルーティングテーブルに存在するという確認を受信すると、前記データリクエストを転送するステップと、前記エントリが、前記ルーティングテーブルに存在しないという確認を受信すると、署名検証リクエストをＮＲＳに送信するステップと、前記ＮＲＳから検証失敗指示の受信をすると、前記第１のプレフィックス報知メッセージを中断するステップと、前記ＮＲＳから検証確認を受信すると、前記プレフィックス、前記署名、および前記公開鍵に対応する、前記ルーティング・テーブル・エントリを作成し、第２のフェイス経由で第２のプレフィックス報知メッセージを送信する、ステップと、を含む、方法を包含する。

【００１１】

これらおよび他の特徴は、添付の図面および特許請求の範囲とともに行われる以下の発明を実施するための形態からより明確に理解されよう。

【００１２】

本開示のより完全な理解のために、ここで、添付の図面および発明を実施するための形態と併せて行われる以下の簡単な説明を参照されたい。同様の参照番号は同様の部分を表す。

【図面の簡単な説明】

【００１３】

【図１】ＩＣＮネットワークインフラの構成要素に対するＤｏＳ攻撃を表すシステムの概略図である。

【図２】コンテンツ提要者に対するＤＤｏＳ攻撃を表すシステムの概略図である。

【図３】ネットワーク要素の実施形態の概略図である。

【図４】コンテンツ提供者のためのブートストラップ名前登録手続きを示す図である。

【図５】第１ルータと第２ルータとの間のリンクベースのセキュア・セッション・キー（ＳＳＫ）確立手続きを示す図である。

【図６】名前プレフィックス報知のためのプロトコル図である。

【図７】名前プレフィックス取り消しのためのプロトコル図である。

【図８】ＩＣＮネットワークインフラ内の信用増加ルーティングシステムを示す図である。

【発明を実施するための形態】

【００１４】

以下に1つまたは複数の実施形態の例示的な実装形態を与えるが、開示するシステムおよび/または方法は、現在知られているか、存在するかにかかわらず、任意の数の技法を使用して実装され得ることを最初に理解されたい。本開示は、本明細書で示し説明する例示的な設計および実装形態を含む、以下に示す例示的な実装形態、図、および技法にいかなる場合も限定されるべきではなく、全範囲の均等物とともに添付の特許請求の範囲内で修正され得る。

【００１５】

図１は、ＩＣＮネットワークインフラ１０２の構成要素に対するＤｏＳ攻撃を表すシステム１００の概略図である。ＩＣＮネットワークインフラ１０２は、ルータ１０４、１０６、および１０８を含む。システム１００は、自律的なシステムのネットワーク１１０および／またはボットネッツ１１２を含む。ボットネッツは、例えば、単体の外部ルーティングポリシーの下で操作するようなタスクを実行するための、他の類似のプログラムと通信するインターネット接続されたプログラムの集まりとして定義されてもよい。システム１００は、ボットネッツ１１６のネットワーク１１４をさらに含む。ネットワーク１１０および１１４は、ＩＣＮネットワークインフラ１０２と通信してもよい。ボットネッツ１１２および１１６は、コマンドおよび制御チャネル１１８によって制御されてもよい。コマンドおよび制御チャネル１１８は、ＩＣＮネットワークインフラ１０２に対する、例えば、ＤＤｏＳ攻撃のようなボットネット攻撃をコーディネートし得る。

【００１６】

例えば、コマンドおよび制御チャネル１１８は、ネットワーク１１４のボットネッツ１１６にルータ１０８を攻撃するように命令し得る。コマンドおよび制御チャネル１１８は、例えば、利用可能なルーティング構造およびルータ１０４、１０６、および／または１０８によって承認された報知を使用して、ＩＣＮネットワークインフラ１０２によって使用される1つもしくは複数のプレフィックスを取得してもよい。コマンドおよび制御チャネル１１８は、これらのプレフィックスをボットネッツ１１６および１１２に送信し得る。ボットネッツ１１２は、例えば、/aname/nounceのような、同一のプレフィックスを有し、しかし異なる名前を有する名前を公開し得、次いで、ボットネッツ１１６は、ボットネッツ１１２によって公開された名前にインタレスト（interest）を送信し得る。ＩＣＮネットワークインフラ１０２のルータは、インタレストを転送し、ネットワーク内の状態

情報を保ち、データバックを転送し、および、コンテンツキャッシュを保存し得るので、ペンディング・インタレスト・テーブル（ＰＩＴ）および／またはアクセスルータのコンテンツストア（ＣＳ）は、多数のインタレストで溢れる恐れがある。したがって、良いユーザ１２０がルータ１０８に正規のインタレストを送信するとき、正規のインタレストは、アクセスルータ１０８の多数の未処理ＤｏＳインタレストによって遅延し、またはルータ１０８インタフェースのレート制御保護構造によってドロップされることがある。アクセスルータのＣＳは、ボットネッツ１１６および／または１１２からのＤｏＳデータによって消耗されることがあるため、どちらの結果も、送付効率の低下を生じさせ得る。

【００１７】

図２は、例えば、サーバ、エンドユーザ等のコンテンツ提供者２０２に対するＤＤｏＳ攻撃を表すシステム２００の概略図である。図２の構成要素は、実質的に図１の構成要素に対応するものと同一である。図２において、ボットネッツ１１６は、ターゲットにされた良いユーザ１２０と同一のドメイン内に位置し、ボットネッツ１１２は、コンテンツ提供者２０２と同じドメイン内に位置する。コンテンツ提供者２０２に対するＤＤｏＳ攻撃を開始するために、ボットネッツ１１２は、有効なオリジン（origin）サーバのものと同一の名前プレフィックスを公開し得る。標準の規則に従って、ＩＣＮネットワークインフラ１０２は、プレフィックスを報知および承認し得る。標準の規約に従って、ＩＣＮネットワークインフラ１０２は、プレフィックスを報知および承認する。ボットネッツ１１６は、ボットネッツ１１２によって公開された名前に対して、例えばPublisherPublicKeyDigestのようなボットネットのマスタ公開鍵のハッシュとともにインタレスト名を送信する。ＩＣＮルータ１０４、１０６および／または１０８が、同一名プレフィックスのためにそれらのルーティングテーブル内に記録された二つのポート、またはフェイスを有するとき、複数のパスにインタレストが送信され得る。これは、ネットワークの混雑を増加させ、遅延時間をもたらし、およびネットワーク効率を低下させることがある。ＩＣＮルータ１０４、１０６、および／または１０８がプロトコル・データ・ユニット（ＰＤＵ）を受信したとき、「有効な」PublisherPublicKeyDigestを有しているために、ボットネッツ１１２および／または１１６からのＰＤＵが承認される可能性がある。ＩＣＮルータ１０４、１０６、および／または１０８は、通常どおり、それらのデータＰＤＵを転送およびキャッシュし得る。したがって、同一のプレフィックスに対する良いユーザ１２０のインタレストは、ＩＣＮネットワークインフラ１０２のルータ１０４、１０６、および／または１０８内のキャッシュにより、満たされ得る。これは、コンテンツ提供者２０２によって公開された本物のコンテンツとは異なることがある。

【００１８】

開示されたシステムおよび方法は、上述されたＤｏＳおよびＤＤｏＳ攻撃を避けるために十分であろう。具体的には、開示されたシステムおよび方法は、トラストアンカーデータ（例えば、設定されたトラストアンカーからそのデータに対する信頼チェーン経由で検証状態を確認するデータ）を、ＩＣＮのプロトコルのルーティング、および／または、コンテンツ名またはＩＤがルーティングおよび転送に使用されてもよい他のインターネットアーキテクチャに基づいた名前／プレフィックスに挿入することによって、ＤｏＳおよびＤＤｏＳに対して安全性を高め得る。例えば、送信者は、報知をルーティングする名前／プレフィックスの検証が成功したあと、対応する証明書とともに、ルータのルーティングテーブル（例えば、転送テーブルまたは転送情報ベース（ＦＩＢ））が増加することによって、「信頼された」ものとして示されてもよい。開示されたシステムおよび方法は、信用されたデータおよび／または構成要素を確立および検証するための鍵交換プロトコルを含む。開示されたシステムおよび方法は、コンテンツ名/プレフィックスの権限および確実性、および／または関連する証明書を検証することによって、信用されたデータおよび／または構成要素を確立および検証するための鍵交換プロトコルを含む。一例として、以下の図４で議論されるNRSおよびブートストラップ手順と、図５で議論されるリンクベースのSSKとを組み合わせて使用することによって、既知および／または信用されたパスに従って、信用されたデータをパスすることができる。図６および７は、開示された実施形

態を使用した、プレフィックスの報知およびプロトコルの取り消しがどのように生じるかを説明する。

【００１９】

本開示で記載された少なくともいくつかの機能／方法は、ネットワーク要素によって実装される、および／または実行されてもよい。例えば、開示された機能／方法はハードウェア、ファームウェア、および／またはハードウェア上で実行するためにインストールされたソフトウェアを使用して実装されてもよい。ネットワーク要素は、例えば、スイッチ、ルータ、ブリッジ、サーバ、クライアント等の、ネットワークを介してデータを搬送するいずれのデバイスであってもよい。図３は、ネットワーク要素３００の、実施形態の概略図である。ネットワーク要素３００は、例えばＩＣＮネットワークインフラ１０２のようなネットワークを介してデータを搬送および処理する、いずれのデバイスであってもよい。例えば、ネットワーク要素３００は、例えばルータ１０４、１０６、および１０８のような上述されたＩＣＮスキームのコンテンツルータまたはいずれの装置、またはルータであってもよい。ネットワーク要素３００は、上述された適用転送方法を実装またはサポートするように構成されてもよい。

【００２０】

ネットワーク要素３００は、トランスミッタ、レシーバ、またはそれらの組合せであってもよいトランシーバ（Ｔｘ/Rx）３１２と結合された１つまたは複数のダウンストリームポート３１０を含んでもよい。Tx/Rx３１２は、他のノードからフレームを転送され、および／または受信するために、複数のダウンストリームポート３１０に結合されてもよい。Ｔｘ/Rx３１２は、他のノードからフレームを転送され、および／または受信するために、複数のアップストリームポート３３０に結合されてもよい。プロセッサ３２５は、フレームを処理する、および／またはフレームを送信するノードを特定するために、Ｔｘ/Rx３１２に結合されてもよい。プロセッサ３２５は、１つまたは複数のマルチコアプロセッサ、および／またはデータ格納として機能してもよいメモリモジュール３２２、バッファなどを含んでもよい。プロセッサ３２５は、一般的なプロセッサとして実装されてもよく、または、１つまたは複数の特定用途向け集積回路（ＡＳＩＣ）および／またはデジタル信号プロセッサ（ＤＳＰ）の一部であってもよい。ダウンストリームポート３１０および／またはアップストリームポート３３０は、電気的なおよび／または光学の、送信および／または受信する構成要素を含んでもよい。ネットワーク要素３００は、ルーティング方向を作るルーティング構成要素であってもよいし、そうでなくともよい。メモリモジュール３２２は、例えばキーを格納する、処理および／またはプロトコルの認識などの、ここで開示されたシステムおよび方法を実行するための、命令を収容するために使用してもよい。メモリモジュール３２２は、プロセッサ３２５によって実行されてもよい命令を含む、プログラム可能なコンテンツブロック３２８を含んでもよい。プログラム可能なコンテンツブロック３２８は、開放型システム間相互接続（ＯＳＩ）モデルのアプリケーションレイヤまたはレイヤ３（L3）において、コンテンツ転送および処理機能を実装するように構成されてもよく、ここでコンテンツは、コンテンツの名前またはプレフィックス、および、場合により、ネットワークトラフィックにコンテンツをマッピングする他のコンテンツ関連情報に基づいて転送されてもよい。こうしたマッピング情報は、メモリモジュール３２２内に含まれるコンテンツテーブル３２９内で保持されてもよい。プログラム可能なコンテンツブロック３２８は、例えば、メタデータおよび／またはコンテンツ名といった、コンテンツおよび適宜フェッチコンテンツのために、ネットワークまたは他のコンテンツルータからのユーザリクエストを解釈してもよく、例えば、メモリモジュール３２２に、例えば、一時的にコンテンツを格納してもよい。プログラム可能なコンテンツブロック３２８は、キャッシュされたコンテンツを次いでユーザに転送してもよい。プログラム可能なコンテンツブロック３２８は、ソフトウェア、ハードウェア、または両方を使用して実装されてもよく、レイヤ２（Ｌ２）またはＬ３をリンクするような、ＯＳＩモデルの上記ＩＰレイヤを操作してもよい。また、メモリモジュール３２２は、コンテンツを一時保存するために、例えば、ランダム・アクセス・メモリ（ＲＡＭ）のようなキャッシュ

を含んでもよい。例えば、キャッシュおよびロングタームストレージは、ダイナミック・ランダム・アクセス・メモリ（ＤＲＡＭ）、ソリッドステート・ドライブ（ＳＳＤ）、ハードディスク、またはそれらの組合せを含んでもよい。

【００２１】

プロセッサ３２５、キャッシュ、およびロングタームストレージが変更されたうち少なくとも一つであるネットワーク要素３００は、実行可能な命令をプログラムまたはロードされることによって、本明細書によって解説される新しい機能を有する、例えばマルチコア転送アーキテクチャといった、特定の機械または装置の一部として、ネットワーク要素３００は変形されることが理解される。コンピュータが実行可能なソフトウェアをロードすることによって実現可能な機能は、周知の技術によってハードウェアの実装に変換することができることは、電気工学およびソフトウェア工学の分野の基本である。ハードウェア対ソフトウェアにおける概念の実装する間の決定は、ソフトウェア領域からハードウェア領域への変換に係る問題よりも、通常、設計の安定性の考慮と生産されるユニットの数で定まる。一般的に、ハードウェアの実装は、ソフトウェアの設計の再設計よりも高価であるため、まだ頻繁に変更される設計は、ソフトウェアで実装されることが好ましい場合がある。大規模な生産を実行するハードウェア実装は、ソフトウェア実装よりも安価となり得るため、一般的に、大量に生産され安定している設計は、ハードウェア、例えばASICにおいて実装されることが好ましい場合がある。多くの場合、設計は、ソフトウェアの命令をハードウェアに組み込まれているアプリケーション特定用途向け集積回路において、同等のハードウェア実装のために周知の設計ルールによって、ソフトウェア上で開発されおよびテストされ、後に変換されてもよい。実行可能な命令とともにプログラムされおよび／またはロードされたコンピュータが、特定の機械または装置として見なされ得るのと同様に、新ASICにより制御される機械と同様に、特定の機会および／または装置である。

【００２２】

図４は、ＮＲＳ４０２と通信するコンテンツ提供者４０４のためのブートストラップ名登録手続きを示す。コンテンツ提供者４０４は、例えば、ＩＣＮネットワークインフラ１０２といったネットワークにコンテンツを公開する能力がある、例えば、図２のコンテンツ提供者２０２といった、いずれのデバイスであってもよい。ＮＲＳ４０２は、例えば、図１のルータ１０４、１０６、および１０８のうちの一つといったデバイス、または、ネットワークのためのローカルあるいはグローバル権限としての機能が有効なサービスであってもよい。ブートストラップ名前登録手続きを実装するための手続きおよび／またはプロトコルの知識は（より具体的には、鍵自体）、コンテンツ提供者４０４またはＮＲＳ４０２のいずれかのために、例えば、図３のメモリモジュール３２２内に保存されている可能性がある。

【００２３】

コンテンツ提供者４０４は、例えば、pbk_p/prk_pといった公開/秘密鍵のペアを含んでもよい。pbk_pの信用は、例えば、リソース公開鍵インフラ（ＰＲＫＩ）/簡易公開鍵インフラ（ＳＰＫＩ）/ＲＰＫＩといった、他の信用管理構造、行政または社会的信用の管理構造の上に構築されてもよい。図４は、コンテンツ提供者４０４がNRSを用いて名前プレフィックスを登録することを示す。示されるように、コンテンツ提供者４０４の登録要求は、公開鍵証明書pbk_pを含んでもよい。NRS402は、例えば、(name，pbk_p)といったプレフィックス名およびコンテンツ提供者名を結合してもよく、およびプレフィックス名および提供者名をネットワーク内の他のノードに報知してもよい。NRS４０２が、コンテンツ提供者４０４からの付加情報を取得することを含み得る証明書の検証に一度成功すると、NRS４０２は、例えばprk_nrsといったNRS４０２のプライベート鍵によってサインされた、例えば(pre_nおよびpbk_p)といった署名を返送してもよい。

【００２４】

図５は、例えば、図１のルータ１０４のような第１ルータ（Rx）５０２と、例えば、図１のルータ１０６のような第２ルータ（Ｒｙ）５０４との間のリンクベースのＳＳＫ確立を示し、これは、例えば、ＩＣＮネットワークインフラといったネットワーク内のデータ

転送のための知られた、および／または信頼されたパスを確立してもよい。Ｒｘ５０２およびＲｙ５０４は、物理リンクをシェアしている直接の隣接であってもよい。Ｒｘ５０２は、請求項やされた秘密鍵パッケージを含むシェアされた秘密鍵、kxyを生成してもよい。いくつかの属性は、例えば、満期日時、ルータ名および／または識別子、（リプレイ攻撃を避けるための）ランダムノンスなどの、シェアされた秘密鍵パッケージ内に含まれてもよい。受領すると、Ｒｙ５０４は、シェアされた秘密鍵パッケージを取得するためにkxyを復号してもよい。シェアされた秘密鍵を確立するための多くのオプションは、使用されることができ、および、開示された実施形態は、特定の一つを使用することを要求するものではない。一実施形態において、Diffie-Hellmanプロトコルは、シェアされた秘密鍵を確立するために使用される。

【００２５】

図６は、コンテンツ提供者２０２とルータ１０４、１０６、および１０８との間の名前プレフィックス報知のためのプロトコル図を示す。図６は、物理リンクを用いたルータの各ペアは、共有の秘密鍵、例えば、図５の共有の秘密鍵を有することを前提とする。６０２において、コンテンツ提供者２０２は、ルータ１０４に報知（例えば、PrePub (pre_n, pbk_p, sig(pre, pbk_p, prk_nrs))を送信し、ここでpre_nは、コンテンツ提供者２０２が所有するか、公開することを許可されたプレフィックスであり、pbk_pは、コンテンツ提供者２０２の公開鍵であり、sigは、例えば、図４のＮＲＳ４０２のようなＮＲＳからの署名である。６０４において、ルータ１０４は、pbk_nrsを用いて署名を検証してもよい。検証が失敗した場合、ルータ１０４は、報知をドロップしてもよい。検証をパスした場合、ルータ１０４は、検証を反映するために、例えば（pre_n, pbk_p, f1）を用いてその内部のＦＩＢを更新してもよい。いくつかの実施形態において、鍵付きハッシュメッセージ認証符号（ＨＭＡＣ）、Hash(pbk_p)は、スペースをセーブするために生成される、および／または使用されてもよい。６０６において、ルータ１０４は、例えばPreAnnounce(pre_n, sig, pbk_p, R1)（ここでR1はルータ１０４の属性である）といった報知を、例えばHMAC(PreAnnounce||K12)（ここで、K12はルータ１０４と１０６との間の公開された秘密鍵である）といったHMACとともにルータ１０６に送信する。６０８において、ルータ１０６は、受信した(PreAnnounce||K12)に対して検証するためのHMAC’(PreAnnounce||K12)を生成し、およびpbk_nrsを用いてsigを検証してもよい。検証が失敗した場合、報知はドロップされてもよい。検証がパスした場合、ルータ１０６は、例えば、(pre_n, pbk_p, f1)（ここで、f1はルータ１０６がルータ１０４と通信するポートまたはフェイスである）を用いて検証を反映するためにその内部FIBを更新してもよい。６１０において、ルータ１０６は、例えばPreAnnounce (pre_n, sig, pbk_p, R2)（ここで、R2はルータ１０６の属性である）といった報知を、例えばHMAC(PreAnnounce||K23)（ここで、K23はルータ１０６と１０８との間の公開された秘密鍵である）といったHMACに従ってルータ１０８に送信してもよい。６１２において、ルータ１０８は、受信した(PreAnnounce||K23)に対して検証するためのHMAC’(PreAnnounce||K23)を生成し、およびpbk_nrsを用いてsigを検証してもよい。検証が失敗した場合、報知はドロップされてもよい。検証がパスした場合、ルータ１０６は、例えば、(pre_n, pbk_p, f1)（ここで、f1はルータ１０８がルータ１０６と通信するポートまたはフェイスである）を用いて検証を反映するためにその内部FIBを更新してもよい。とりわけ、報知のいくつかの実施形態は、例えば、メッセージリプライ攻撃を避けるためのランダムノンスといった他のフィールドを含んでもよいことが当業者によって理解されよう。

【００２６】

図７は、コンテンツ提供者２０２とルータ１０４、１０６、および１０８との間の名前プレフィックス取り消しのためのプロトコル図を示す。図７の構成要素は、実質的に図６の構成要素と同一であってもよい。コンテンツ提供者２０２が、そのプレフィックスへのコンテンツ要求に応答しないように、プレフィックスを取り消したいとき、コンテンツ提供者２０２は、取り消し（例えば、PreRvk (pre_n, pbk_p, sig(pre, pbk_p, prk_nrs))）をルータ１０４に送信することによって、７０２で取り消し処理を開始することができ

る。取り消しを受信すると、７０４において、ルータ１０４は、pbk_nrsを用いて署名を検証してもよい。検証が失敗した場合、ルータ１０４は、取り消しをドロップしてもよい。検証をパスした場合、ルータ１０４はプレフィックス（例えば、(pre_n，pre_p，f1)）が、そのＦＩＢ内かどうかをチェックしてもよい。もし、そうであれば、ルータ１０４は、そのルーティングテーブルからプレフィックスを取り除いてもよい。７０６において、ルータ１０４は、ハッシュ（例えば、HMAC(PreRvk||K12)）とともに、ルータ１０６に対して取り消し（例えば、PreRvk(pre_n，pbk_p，R1)）を送信してもよい。受理すると、７０８において、ルータ１０６は、受信したHMAC(PreRvk||K12)を検証するためのHMAC’(PreRvk||K12)を生成してもよく、pbk_nrsを用いて署名を検証してもよい。検証が失敗した場合、ルータ１０６は、取り消しをドロップしてもよい。検証がパスした場合、ルータ１０６は、プレフィックス（例えば、(pre_n，pre_p，f1)）が、そのＦＩＢ内かどうかをチェックしてもよい。もし、そうであれば、ルータ１０６は、そのルーティングテーブルからプレフィックスを取り除いてもよい。７１０において、ルータ１０６は、ハッシュ（例えば、HMAC(PreRvk||K23)）とともに、ルータ１０８に対して取り消し（例えば、PreRvk(pre_n，pbk_p，R2)）を送信してもよい。取り消しを受信すると、７１２において、ルータ１０８は、受信したHMAC(PreRvk||K23)を検証するためのHMAC’(PreRvk||K23)を生成してもよく、pbk_nrsを用いて署名を検証してもよい。検証が失敗した場合、ルータ１０８は、取り消しをドロップしてもよい。検証がパスした場合、ルータ１０８は、プレフィックス（例えば、(pre_n，pre_p，f1)）が、そのＦＩＢ内かどうかをチェックしてもよい。もし、そうであれば、ルータ１０８は、そのルーティングテーブルからプレフィックスを取り除いてもよい。特に、報知のいくつかの実施形態は、他のフィールド（例えば、メッセージリプレイ攻撃を避けるためのランダムノンス）を含んでもよいことが、当業者には理解されよう。

【００２７】

図８は、ＩＣＮネットワークインフラ１０２内の信用増大ルーティングシステム８００を示す。良いユーザ８０２および８０４は、例えば、図１の良いユーザ１２０のようないずれのユーザデバイスであってもよい。悪質な提供者８０８は、例えば、図２の悪質なコンテンツ提供者２０２のような、いずれのユーザデバイスであってもよい。ルータ１０４は、検証されたプレフィックス報知を有するポートまたはフェイスからインタレストを転送すること優先するように構成されてもよい。ルータ１０４は、例えば‘Ccnx/804’といった良いユーザ８０４を示すプレフィックスのための2つのエントリを有する内部ルーティングテーブル８０６を含んでもよい。内部ルーティングテーブル８０６における第1のエントリは、ポートまたは例えばF1といったフェイス、プレフィックスが図６の下で説明されたものとしてプレフィックスの報知に従って、信用された接続から受信されたポートまたはフェイスf1を介して受信されたことを示す、例えばpub_Bといった公開鍵を受信することを含んでもよい。内部ルーティングテーブル８０６における第二エントリは、ポートおよび例えばf2といったフェイスを関連する公開鍵なしの、第2の受信を含んでもよい。理解されるように、交互に起こる攻撃は、検証されていない公開鍵を含み得る。例えばプレフィックスの乗っ取りCcnx/804といった、悪質な提供者８０８に起因する名前/プレフィックスの乗っ取り攻撃のイベントにおいて、ルータ１０４は、ポートまたはフェイスf1を介して信用された接続に関連するエントリを選択してもよい。

【００２８】

少なくとも1つの実施形態が開示され、当業者によって行われる実施形態および/または実施形態の特徴への変形、組合せ、および/または変更が本開示の範囲内に入る。実施形態の特徴を組み合わせること、統合すること、および/または省略することから生じる代替実施形態も本開示の範囲内に入る。数値範囲または限定が明確に述べられている場合、そのような明示的な範囲または限定が、明確に述べられた範囲または限定内に入る同様の大きさの反復範囲または限定を含むことを理解されたい(例えば、約1～約10は2、3、4などを含み、0.10よりも大きいは0.11、0.12、0.13などを含む)。例えば、下限がRlおよび上限がRuの数値範囲が開示されるときはいつでも、その範囲内に入る任意の数が明確に開

示される。特に、範囲内の以下の数が明確に開示される。R=Rl+k*(Ru-Rl)、ここで、kは、1パーセントずつ増分する、1パーセントから100パーセントの範囲にある変数であり、すなわち、kは、1パーセント、2パーセント、3パーセント、4パーセント、5パーセント、...、50パーセント、51パーセント、52パーセント、...、95パーセント、96パーセント、97パーセント、98パーセント、99パーセント、または100パーセントである。さらに、上記で定義されている2つのR数によって定義される任意の数値範囲も明確に開示される。「約」という用語の使用は、別段に明記されていない限り、後続の数の+/-10%を意味する。請求項の任意の要素に関する「随意に」という用語の使用は、要素が必要であること、または代替的に、要素が必要でないことを意味し、両方の代替が請求項の範囲内に入る。備える、含む、および有するなどの上位語の使用は、からなる、本質的にからなる、実質的にからなるなどの下位語のサポートを行うことを理解されたい。本開示で説明されるすべての文書は、参照により本明細書に組み込まれる。

【００２９】

本開示でいくつかの実施形態を与えたが、開示するシステムおよび方法が、本開示の趣旨または範囲から逸脱することなく、多くの他の特定の形態で実施され得ることが理解され得る。提示する例は、限定的なものではなく例示的なものと見なすべきであり、その意図は、本明細書で与える詳細に限定されるものではない。例えば、様々な要素または構成要素が別のシステムと組み合わされるかまたは統合され得、あるいはいくつかの特徴が省略されるか、または実装されないことがあり得る。

【００３０】

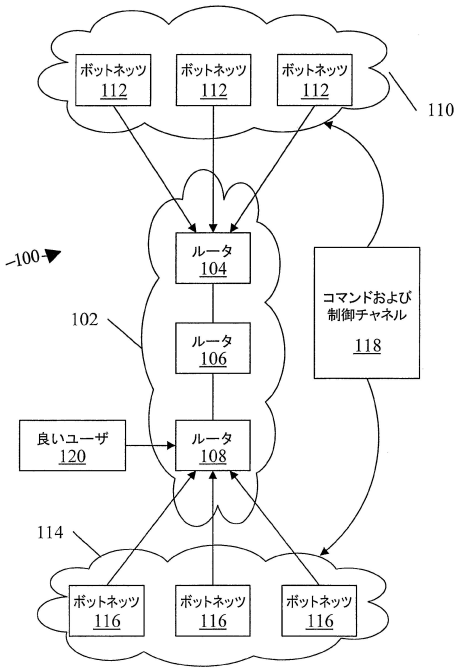
さらに、個別または別個のものとして様々な実施形態で説明されたか、またはそのように示された技法、システム、サブシステム、および方法は、本開示の範囲から逸脱することなく他のシステム、モジュール、技法、または方法と組み合わされるか、または一体化され得る。相互に結合されるものとしてか、または相互に直接結合されるものとしてか、または相互に通信するものとして示されているか、またはそのように説明された他の部材は、間接的に結合されるか、あるいは何らかのインターフェース、デバイス、または電気的でか、機械的でか、もしくは他の方法でかにかかわらず、中間構成要素を通して通信し得る。変更、代替、および改変の他の例が、当業者によって確認可能であり、本明細書で開示した趣旨および範囲から逸脱することなくなされ得る。

【符号の説明】

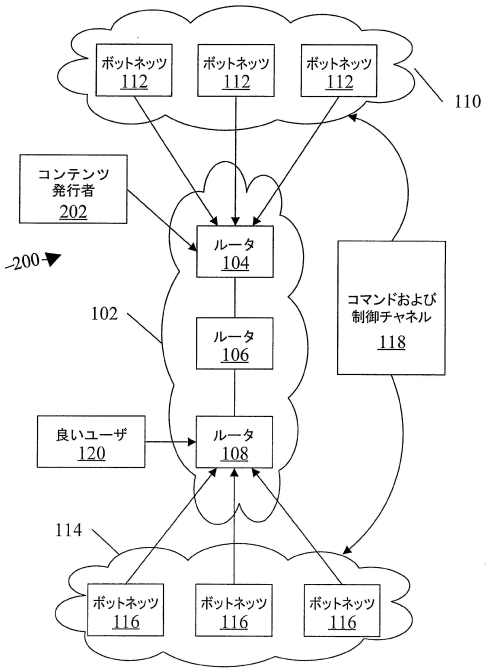
【００３１】

１００　システム
１０２　ＩＣＮネットワークインフラ
１０４、１０６、１０８　ルータ
１１０　ネットワーク
１１２　ボットネッツ
１１４　ネットワーク
１１６　ボットネッツ
１２０　ユーザ
２００　システム
２０２　コンテンツ提供者
３００　ネットワーク要素
３１０　ダウンストリームポート
３２２　メモリモジュール
３２５　プロセッサ
３３０　アップストリームポート
４０２　ＮＲＳ
４０４　コンテンツ提供者
８０２　ユーザ

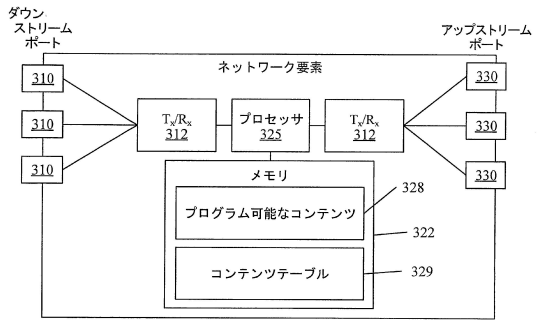
【図１】



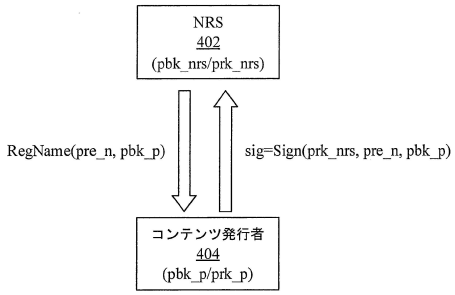
【図２】



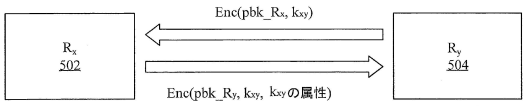
【図３】



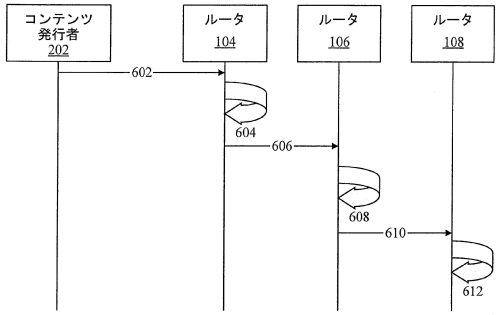
【図４】



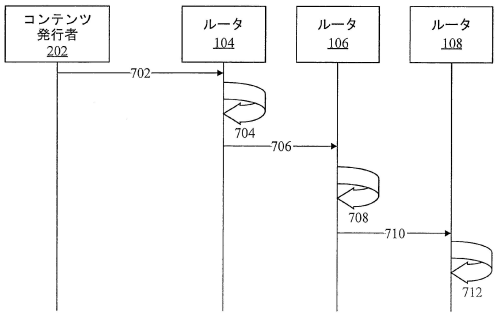
【図５】



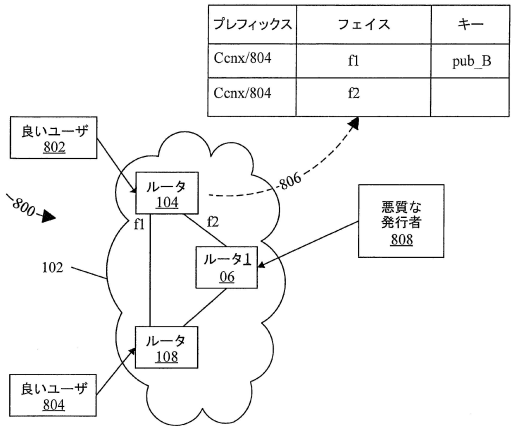
【図６】



【図７】



【図８】


プレフィックス
フェイス
キー
Ccnx/804
f1
pub_B
Ccnx/804
f2
良いユーザ
802
ルータ
104
806
800
f1
f2
悪質な
発行者
808
102
ルータ1
06
ルータ
108
良いユーザ
804

フロントページの続き

(72)発明者　シンウェン・ジャン
アメリカ合衆国・カリフォルニア・９４５８３・サン・ラモン・カードナ・サークル・３４８
(72)発明者　ハイヨン・シエ
アメリカ合衆国・カリフォルニア・９４５８７・ユニオン・シティ・リージェンツ・ブールヴァード・３２４１５
(72)発明者　ラヴィシャンカール・ラヴィンドラン
アメリカ合衆国・カリフォルニア・９４５８２・サン・ラモン・レメンウッド・コート・２０５８
(72)発明者　グオ－チアン・ワン
アメリカ合衆国・カリフォルニア・９５０５１・サンタ・クララ・フローラ・ヴィスタ・アヴェニュー・３６０４・アパートメント・２１６

審査官　速水　雄太

(56)参考文献　米国特許出願公開第２０１２／０１６６８０６（ＵＳ，Ａ１）
特開２０１２－１２８８４８（ＪＰ，Ａ）
特開２００４－０７２６３３（ＪＰ，Ａ）
特表２０１０－５３８５６３（ＪＰ，Ａ）
Zhang, X. et al., Towards mame-based trust and security for content-centric network, 2011 19th IEEE International Conference on Network Protocols, IEEE, ２０１１年, pp. 1-6

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ　１２／６６
Ｈ０４Ｌ　１２／７０