(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2017-506846
(P2017-506846A)
(43)公表日　平成29年3月9日(2017.3.9)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	12/721	(2013.01)	H04L	12/721	A	5J104
H04L	9/32	(2006.01)	H04L	9/00	675B	5K030
G09C	1/00	(2006.01)	G09C	1/00	640D	
H04L	9/08	(2006.01)	H04L	9/00	601C	
H04L	12/717	(2013.01)	H04L	9/00	601F	

審査請求 有　予備審査請求 未請求　（全 16 頁）　最終頁に続く

(21)出願番号　特願2016-551194 (P2016-551194)
(86)(22)出願日　平成27年2月9日 (2015.2.9)
(85)翻訳文提出日　平成28年8月10日 (2016.8.10)
(86)国際出願番号　PCT/CN2015/072482
(87)国際公開番号　WO2015/120783
(87)国際公開日　平成27年8月20日 (2015.8.20)
(31)優先権主張番号　14/177,913
(32)優先日　平成26年2月11日 (2014.2.11)
(33)優先権主張国　米国 (US)

(71)出願人　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】公開鍵を基礎とするデジタル署名を使用してソースルーティングを保全するためのシステムおよび方法

(57)【要約】
公開鍵を基礎とするデジタル署名を使用してソースルーティングを保全するために実施形態が提供される。保護されるソースルートが改ざんされる場合、公開鍵に基づく方法は、下流のノードが改ざんを検出することを可能にする。本方法は、ソースルートの完全性を保護するためにデジタル署名を使用することに基づく。トラフィックフローのためのソースルートを作成するとき、指定されたネットワーク要素がデジタル署名を計算し、パケットにデジタル署名を加える。パケットがルート上のノードで受信されるとき、ノードはデジタル署名および公開鍵を使用してソースルートを検証し、それに基づいてソースルートが改ざんされたか否かを決定する。改ざんが検出される場合、受信ノードはパケットの転送を停止する。

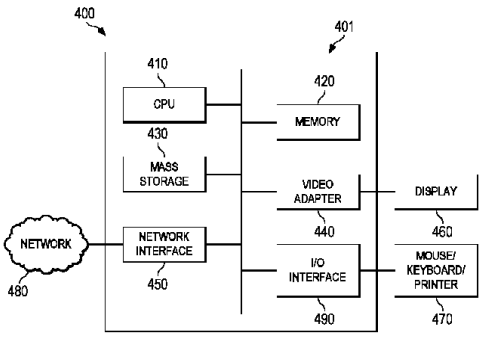

FIG. 4

【特許請求の範囲】
【請求項１】
公開鍵を基礎とするデジタル署名を使用してソースルーティングを保全するためのネットワーク要素による方法であって、
ネットワーク内のトラフィックをルーティングするために決定されるソースルートのためのデジタル署名を前記ネットワーク要素の秘密鍵を使用して生成するステップであって、前記ソースルートが前記ネットワーク内のノードの順序を示す、ステップと、
前記デジタル署名および前記ソースルートの組み合わせとして、安全なソースルートを提供するステップと、
前記安全なソースルートを前記トラフィックのパケットに加えるステップと、
前記ソースルート上で前記パケットを送信するステップと
を含む方法。
【請求項２】
前記ソースルートを検証するための公開鍵を前記ノードに配布するステップをさらに含む、請求項1に記載の方法。
【請求項３】
前記公開鍵を配布するステップが、前記ノードにおいて前記公開鍵の証明書を事前設定するステップを含む、請求項1に記載の方法。
【請求項４】
前記安全なソースルートを提供するステップが、前記パケット内で前記デジタル署名および前記ソースルートと共にフロールールを加えるステップをさらに含む、請求項1に記載の方法。
【請求項５】
前記デジタル署名が、前記ソースルート、および前記フロールールにより識別されるフロー情報の関数であり、前記フロー情報が、ソースアドレスおよび宛先アドレスのうちの少なくとも1つを含む、請求項4に記載の方法。
【請求項６】
前記ネットワーク要素の秘密鍵が前記ノードと共有されない、請求項1に記載の方法。
【請求項７】
公開鍵を使用してソースルーティングを保全するためのネットワーク要素であって、
少なくとも1つのプロセッサと、
前記プロセッサによる実行のためのプログラミングを記録する非一時的コンピュータ可読記録媒体とを含み、前記プログラミングは、
ネットワーク内のトラフィックをルーティングするために決定されるソースルートのためのデジタル署名を、公開鍵を使用して生成することであって、前記ソースルートが前記ネットワーク内のノードの順序を示す、ことと、
前記デジタル署名および前記ソースルートの組み合わせとして、安全なソースルートを提供することと、
前記安全なソースルートを前記トラフィックのパケットに加えることと、
前記ソースルートで前記パケットを送信することと
を行うための命令を含む、ネットワーク要素。
【請求項８】
前記プログラミングが、前記ソースルートを検証するための公開鍵を前記ノードに配布するための命令をさらに含む、請求項7に記載のネットワーク要素。
【請求項９】
前記安全なソースルートを提供するための命令が、前記パケット内に、前記デジタル署名および前記ソースルートと共にフロールールを含めるための命令をさらに含み、前記デジタル署名が、前記ソースルートおよび前記フロールールにより識別されるフロー情報の関数である、請求項7に記載のネットワーク要素。
【請求項１０】

前記ネットワーク要素が、ソフトウェア・デファインド・ネットワーキング(SDN)コントローラである、請求項7に記載のネットワーク要素。
【請求項１１】
公開鍵を使用してソースルーティングを保全するためのネットワークノードによる方法であって、
ソースルートおよびデジタル署名を含むパケットを受信するステップであって、前記デジタル署名が、前記ソースルートと前記ネットワークノードに知られていない秘密鍵とに従って生成され、前記ソースルートがネットワーク内のノードの順序を示す、ステップと、
前記デジタル署名と前記ネットワークノードに知られる公開鍵とを使用して前記ソースルートを検証するステップと、
前記ソースルートの不一致を決定する際に、前記ソースルートの改ざんを示す通知メッセージを前記ネットワークに送信するステップと
を含む方法。
【請求項１２】
前記パケットが、フロー情報を含むフロールールをさらに含み、前記フロー情報は、ソースアドレスおよび宛先アドレスのうちの少なくとも1つを識別し、前記デジタル署名が、前記ソースルートおよび前記フロー情報の関数である、請求項11に記載の方法。
【請求項１３】
前記デジタル署名および前記公開鍵を使用して前記ソースルートを検証するステップが、
前記デジタル署名および前記公開鍵の関数としてローカルなソースルートを取得するステップと、
前記ローカルなソースルートを前記パケット内の前記ソースルートと比較するステップと
を含む、請求項11に記載の方法。
【請求項１４】
前記ネットワークから前記公開鍵の証明書を受信するステップをさらに含む、請求項11に記載の方法。
【請求項１５】
前記ネットワークノードにおいて前記ソースルートまたは前記デジタル署名をキャッシュするステップと、
前記キャッシュされたソースルートを使用するか、または前記キャッシュされたデジタル署名および前記公開鍵を使用して前記パケットの後で、第2の受信されるパケット内の第2のソースルートを検証するステップと
をさらに含む、請求項11に記載の方法。
【請求項１６】
前記第2のパケットがデジタル署名を含まない、請求項15に記載の方法。
【請求項１７】
反復的特異値分解における早期終了のためのネットワークノードであって、
少なくとも1つのプロセッサと、
前記プロセッサの実行のためのプログラミングを記録する非一時的コンピュータ可読記録媒体とを含み、前記プログラミングは、
ソースルートおよびデジタル署名を含むパケットを受信することであって、前記デジタル署名が、前記ソースルートと前記ネットワークノードに知られていない秘密鍵とに従って生成され、前記ソースルートがネットワーク内のノードの順序を示す、ことと、
前記デジタル署名と前記ネットワークノードに知られる公開鍵とを使用して前記ソースルートを検証することと、
前記ソースルートの不一致を決定する際に、前記ソースルートの改ざんを示す通知メッセージを前記ネットワークに送信すること

を行うための命令を含む、ネットワークノード。
【請求項１８】
前記パケットが、フロー情報を含むフロールールをさらに含み、前記フロー情報は、ソースアドレスおよび宛先アドレスのうちの少なくとも1つを識別し、前記デジタル署名が、前記ソースルートおよび前記フロー情報の関数である、請求項17に記載のネットワークノード。
【請求項１９】
前記パケットが、フロー情報を含むフロールールをさらに含み、前記フロー情報は、ソースアドレスおよび宛先アドレスのうちの少なくとも1つを識別し、前記デジタル署名が、前記ソースルートおよび前記フロー情報の関数である、請求項17に記載のネットワークノード。
【請求項２０】
前記プログラミングは、
前記ネットワークノードにおいて前記ソースルートまたは前記デジタル署名をキャッシュすることと、
前記キャッシュされたソースルートを使用するか、または前記キャッシュされたデジタル署名および前記公開鍵を使用して前記パケットの後で第2の受信されるパケット内の第2のソースルートを検証することと
を行うための命令をさらに含む、請求項17に記載のネットワークノード。
【発明の詳細な説明】
【技術分野】
【０００１】
本出願は、2014年2月11日付で提出された「公開鍵を基礎とするデジタル署名を使用してソースルーティングを保全するためのシステムおよび方法」という名称の米国非仮出願14/177,913号の利益を主張するものであり、当該出願は参照により本明細書に組み込まれる。
【０００２】
本発明は、ネットワーク通信およびルーティングの分野に関し、特定の実施形態では、公開鍵を基礎とするデジタル署名を使用してソースルーティングを保全するためのシステムおよび方法に関する。
【背景技術】
【０００３】
ネットワークにおいてソースルーティングを使用すると、パケットは、パケット内で示されるソースルートに従って、受信ノードから次のノードにルーティングされる。典型的には、MPLSセグメントルーティング等のルーティングプロトコルは、パケット内のソースルートの完全性の維持に関してセキュリティ保護を伴わないソースルーティングメカニズムを採用する。例えば、ソースルートは、通常、いかなる保護も伴わず平文でパケット内に示される。従って、パケット内のソースルートは、例えばルーティング経路上のノードによる変更、削除、および挿入等の改ざんに晒され得る。改ざんは、そのようなパケットを意図しない送り先に再ルーティングすることを引き起こし得る。この改ざんは、ソースルートを指示するネットワークオペレータのセキュリティポリシーに違反するものであり、ネットワークおよびユーザセキュリティに危害を及ぼす。ソースルートの完全性を保護するための効果的なセキュリティメカニズムの必要性が存在する。
【発明の概要】
【課題を解決するための手段】
【０００４】
本開示の実施形態に従えば、公開鍵を基礎とするデジタル署名を使用してソースルーティングを保全するためのネットワーク要素による方法は、ネットワーク内のトラフィックをルーティングするために決定されるソースルートのためのデジタル署名を、ネットワーク要素の秘密鍵を使用して生成するステップを含む。ソースルートは、ネットワーク内の

ノードの順序を示す。当該方法は、デジタル署名およびソースルートの組み合わせとして安全なソースルートを提供するステップをさらに含む。安全なソースルートはトラフィックのパケットに加えられ、パケットはソースルート上で送信される。

【０００５】

本開示の他の実施形態に従えば、公開鍵を使用してソースルーティングを保全するためのネットワーク要素は、少なくとも1つのプロセッサと、プロセッサによる実行のためのプログラミングを記録する非一時的コンピュータ可読記録媒体とを含む。プログラミングは、ネットワーク内のトラフィックをルーティングするために決定されるソースルートのための電子署名を、公開鍵を使用して生成するための命令を含む。ソースルートは、ネットワーク内のノードの順序を示す。プログラミングは、デジタル署名およびソースルートの組み合わせとして、安全なソースルートを提供するための命令をさらに含む。プログラミングは、安全なソースルートをトラフィックのパケットに加え、ソースルート上でパケットを送信するようにネットワーク要素をさらに構成する。

【０００６】

本開示の他の実施形態に従えば、公開鍵を使用してソースルーティングを保全するためのネットワークノードによる方法は、ソースルートと、ソースルートおよびネットワークノードに知られていない秘密鍵に従って生成されるデジタル署名とを含むパケットを受信するステップを含む。ソースルートは、ネットワーク内のノードの順序を示す。前記方法は、デジタル署名、およびネットワークノードに知られる公開鍵を使用してソースルートを検証するステップをさらに含む。ソースルートの不一致を決定する際に、ソースルートの改ざんを示す通知メッセージが、ネットワークへ送信される。

【０００７】

本開示のさらなる他の実施形態に従えば、反復的特異値分解における早期終了のためのネットワークノードは、少なくとも1つのプロセッサと、プロセッサによる実行のためのプログラミングを記録する非一時的コンピュータ可読記録媒体とを含む。プログラミングは、ソースルートと、ソースルートおよびネットワークノードに知られていない秘密鍵に従って生成されるデジタル署名とを含むパケットを受信するための命令を含む。ソースルートは、ネットワーク内のノードの順序を示す。プログラミングは、デジタル署名およびネットワークノードに知られる公開鍵を使用しソースルートを検証するための命令をさらに含む。ネットワークノードは、ソースルートの不一致を決定する際に、ソースルートの改ざんを示す通知メッセージをネットワークに送信するようにさらに構成される。

【０００８】

上記の記載は、以下の本発明の詳細な説明をより良く理解することができるように、本発明の実施形態の特徴をやや大まかに概説してきた。本発明の特許請求の範囲の特定事項を形作る本発明の実施形態の追加の特徴および利点が、以下で説明される。開示される概念および特定の実施形態が、本発明の同一の目的を遂行するためのその他の構成または過程を変更または設計するために基礎として容易に利用可能であることは、当業者により理解されるべきである。また、このような等価な構成は、添付の特許請求の範囲で規定される本発明の主旨および範囲から逸脱しないことも、当業者により理解されるべきである。

【０００９】

本発明、およびその利点の理解をより完全なものにするために下記の添付の図面と併せて以下の説明を参照する。

【図面の簡単な説明】

【００１０】

【図１】ソースルートを改ざんしパケットを再ルーティングする例示的なシナリオを示す。

【図２】保護されるソースルートの実施形態を示す。

【図３】ソースルートを保護するための方法の実施形態を示す。

【図４】様々な実施形態を実施するために使用可能な処理システムの概略図を示す。

【発明を実施するための形態】

【００１１】
異なる図面内の対応する符号および記号は、別段の表示がない限り通常、対応する部分を示す。図面は、実施形態の関連する態様を明確に説明するために描かれ、必ずしも正確な出尺で描かれない。
【００１２】
現在の好ましい実施形態の作成および使用が、以下で詳細に説明される。一方で、本発明が、多種多様な特定の文脈で実現可能である様々な適用可能な発明概念を提供することが理解されるべきである。説明される特定の実施形態は、本発明を作成および使用するための特定の方法を単に説明するものであり、本発明の範囲を限定するものではない。
【００１３】
公開鍵を基礎とするデジタル署名を使用してソースルーティングを保全するために、ここで実施形態が提供される。保護されるソースルートが改ざんされる場合、公開鍵に基づく方法は、下流のノードが改ざんを検出すること可能にする。本方法は、ソースルートの完全性を保護するためにデジタル署名を使用することに基づく。トラフィックフローのためのソースルートを作成するときに、ソフトウェア・デファインド・ネットワーキング(SDN)コントローラなどの指定されたネットワークノードは、デジタル署名を計算し、パケットにデジタル署名を加える。パケットがルート上のノードで受信されるとき、ノードは、ソースルートを検証するためにデジタル署名および公開鍵を使用し、それに基づいてソースルートが改ざんされているか否かを決定する。改ざんが検出される場合、ノードは、パケットの転送を停止する。
【００１４】
図1は、ソースルートを改ざんしパケットを再ルーティングする例示的なシナリオ100を示す。このシナリオ100では、SDNコントローラ(図示せず)が、ネットワークのセキュリティポリシーに合うように、与えられたトラフィックのフローのためにノード[A，B，E，F]に沿いその順でソースルートを決定する。ネットワークは、A、B、C、D、E、およびFを含む複数のノードを含む。ノードは、ルータ、スイッチ、ゲートウェイ、ブリッジ、またはネットワーク内でパケットを転送するその他のネットワークノードであり得る。全てのノードが適切に挙動し、ソースルートに従ってトラフィックを転送する場合、セキュリティポリシーが施行され得る。一方で、不正な動作をするノードBは、トラフィックを受信すると、下流ノード(E、D、またはF)のいずれにも検出されることなく、パケット内のソースルートを不正な経路[A，B，D，F]に変更することが可能である。この場合、Bは、トラフィックのための特定のセキュリティサービス(例えば、仮想ファイアウォール)をホストし得るEにトラフィックを転送しないことで、セキュリティポリシーを避けることができる。
【００１５】
この状況を避けるために、SDNコントローラが、例えばソースノードを決定する際に、ソースルートのためのデジタル署名を生成するように構成される。図2は、保護されるソースルート200の実施形態を示す。保護されるまたは安全なソースルート200は、SDNコントローラにのみ知られ、ネットワークノードと共有されない秘密鍵に従いSDNコントローラによって生成されるデジタル署名を含む。安全なソースルート200は、実際のソースルートと、場合によりフロールールとをさらに含む。フロールールは、各ノードで事前設定されたフロールールを示すフロー識別子、フローを識別するために使用されるパケット内のフィールドの位置および対応する長さ、またはその他の形態を含むいくつかの形態を取り得るが、これらに限定されるものではない。フロールールは、デジタル署名を生成するために使用されるパケット内の追加の値(例えば、宛先アドレス)を識別するために使用される。例えば、ソースルートは、シナリオ100の正当なソースルート[A，B，E，F]であり、フロールールは、ソース・インターネットプロトコル(IP)・アドレス(sip)および/または宛先IPアドレス(dip)を識別する。デジタル署名は、ソースルートと、例えばsig([A，B，E，F]，[sip|dip])であるフロールールに従う識別されたアドレスとの関数であり得る。安全なソースルート200を形成するソースルート、フロールール、およびデジタル署名

は、パケットヘッダ内に含まれ得る。

【００１６】

安全なソースルート200を有するパケットを受信するとき、ノードは、ノードおよびSDNコントローラに共有される公開鍵を使用してデジタル署名に対してソースルートを検証する。例えば、公開鍵は、各ノードで通常事前設定されるSDNコントローラの公開鍵証明書内で見つけられ得る。代替的に、公開鍵は、SDNコントローラまたはネットワークによってノードにブロードキャストまたはマルチキャストされ得る。受信ノードは、パケット内の公開鍵およびデジタル署名の関数を使用してソースルートを検証することができる。関数が不一致の結果を生じる場合、エラーおよび/または通知メッセージが、さらなる動作を取るために、ノードによってSDNコントローラへ送信される。ノードは、ソースルートが例えばルート上の先行するノードにより改ざんされたことをSDNコントローラに伝える。例えば、シナリオ100においてノードFは、公開鍵に基づく関数を使用し、受信されたパケット内のソースルートの改ざんを検出する。

【００１７】

SDNコントローラのみが秘密鍵の情報を有しているので、その他のノードは、偽装されたソースルートについて有効なデジタル署名を作成することができない。このことが、ソースルートについての完全性保護を提供する。さらに、デジタル署名の送信からのオーバーヘッドを低減するために、デジタル署名自体の代わりにデジタル署名のハッシュまたはハッシュの一部がパケットに含まれてよい。検証に際して、まずノードは上記のデジタル署名を計算し、その後デジタル署名のハッシュを計算し、続いてパケットに含まれるデジタル署名に対する計算されたハッシュを検証する。デジタル署名の送信および検証の両方からのオーバーヘッドをさらに低減するために、一度ノードが検証されると安全なソースルートは、ノードにおいてキャッシュされてよく、将来のパケットは、例えば、保護されるソースルート200の一部に過ぎない実際のソースルート等の通常のソースルートを含みさえすればよい。受信ノードは、後続のパケット内のソースルートを、キャッシュされた安全なソースルートと比較する、またはキャッシュされたデジタル署名と公開鍵を使用して比較することができる。

【００１８】

図3は、ソースルートを保護するための方法300の実施形態である。ステップ310において、公開鍵証明書が、例えばSDNコントローラまたは任意の信頼できるネットワークエンティティによって、ネットワーク内の複数のノードに配布される。ステップ320において、ソースルートが、ネットワーク内でトラフィックを転送するために決定される。ステップ330において、SDNコントローラまたは信頼できるエンティティがソースルートのためのデジタル署名を、コントローラまたはエンティティにのみ知られる秘密鍵と、検討中のソースルートと、任意でソース/宛先アドレスなどのフロールールを使用して識別され得る追加の情報との関数として生成する。ステップ340において、ソースルートと、デジタル署名(またはデジタル署名のハッシュもしくはデジタル署名のハッシュの一部)と、任意でデジタル署名を生成するための追加の情報を識別するためのフロールールとの組み合わせであり得る安全なソースルートが、ソースルート上で転送されるパケット内で送信される。ステップ350において、ソースルート上の各受信ノードは、公開鍵およびデジタル署名を使用し、パケット内に含まれるソースルートを検証する。ステップ360において、受信ノードは、ソースルートが改ざんされたか否か、例えばパケット内のソースルートと公開鍵によってデジタル署名を処理した結果との間に不一致があるか否かを決定する。ソースルートが改ざんされている場合、ステップ370において、その後そのような改ざんをネットワーク(またはコントローラ)に通知する。パケットは廃棄されてよく、転送は停止される。そうでなければ、ステップ380において、ノードは、通常通りパケットの転送または処理を継続する。方法200において、ステップ310から340は、コントローラまたはネットワークエンティティによって実施される。ステップ350から380は、各受信ノードまたは宛先ノードによって実施される。

【００１９】

図4は、様々な実施形態を実施するために使用され得る例示的な処理システムのブロック図である。処理システムは、コントローラ(もしくはネットワークエンティティ)または、ソースルーティングに従ってパケットを受信および/または送信するノードの一部であってよい。一実施形態において、処理システム400は、異なる構成要素が、各々から分離した、または遠隔の構成要素に位置するとともに、1つまたは複数のネットワークを介して接続され得るクラウドまたは分散されたコンピューティング環境の一部であってよい。処理システム400は、スピーカ、マイクロフォン、マウス、タッチスクリーン、キーパッド、キーボード、プリンタ、ディスプレイ等の1つまたは複数の入出力デバイスを備えた処理ユニット401を含み得る。処理ユニット401は、バスに結合される中央処理ユニット(CPU)410、メモリ420、大容量記録装置430、ビデオアダプタ、および入出力(I/O)インターフェイスを含み得る。バスは、メモリバスまたはメモリコントローラ、周辺バス、およびビデオバス等を含むいくつかのバスアーキテクチャの任意の種類のうちの1つまたは複数であり得る。

【００２０】

CUP410は、電子データプロセッサの任意の種類を含んでよい。メモリ420は、例えば、静的ランダムアクセスメモリ(SRAM)、動的ランダムアクセスメモリ(DRAM)、シンクロナスDRAM(SDRAM)、リードオンリメモリ(ROM)、またはそれらの組み合わせ等のシステムメモリの任意の種類を含む。一実施形態において、メモリ420は、起動時において使用するためのROM、ならびにプログラムのためのDRAMおよびプログラム実行時に使用するためのデータ記録装置を含み得る。大容量記録装置430は、データ、プログラム、およびその他の情報を記録し、バスを介してアクセス可能なデータ、プログラム、およびその他の情報を作成するように構成される記録装置の任意の種類を含んでよい。大容量記録装置430は、例えば、ソリッドステートドライブ、ハードディスクドライブ、磁気ディスクドライブ、または光学ディスクドライブ等のうちの1つまたは複数を含み得る。

【００２１】

ビデオアダプタ440およびI/Oインターフェイス490は、外部入力および出力装置を処理ユニットに結合するためにインターフェイスを提供する。図示されるように、入出力装置の例示は、ビデオアダプタ440に結合されるディスプレイ460、およびI/Oインターフェイス490に結合されるマウス/キーボード/プリンタ470の任意の組み合わせを含み得る。その他の装置は、処理ユニット401に結合されてよく、追加のまたは数少ないインターフェイスカードが用いられ得る。例えば、シリアルインターフェイスカード(図示せず)が、プリンタのためのシリアルインターフェイスを提供するために使用されてよい。

【００２２】

処理ユニット401は、ノードまたは1つもしくは複数のネットワーク480にアクセスするための、例えばイーサネット(登録商標)ケーブル等の有線リンクおよび/または無線リンクを含み得る1つまたは複数のネットワークインターフェイス450をも含む。ネットワークインターフェイス450は、処理ユニット401がネットワーク480を介して遠隔のユニットと通信を行うことを可能にする。例えば、ネットワークインターフェイス450は、1つまたは複数の送信機/送信アンテナ、および1つまたは複数の受信機/受信アンテナを介する無線通信を提供し得る。一実施形態では、処理ユニット401は、データ処理のためのローカルエリアネットワークまたはワイドエリアネットワークに結合され、例えば他の処理ユニット、インターネット、または遠隔記録施設等の遠隔装置と通信する。

【００２３】

いくつかの実施形態が本開示において提供されてきたが、開示されたシステムおよび方法が、本開示の主旨および範囲から逸脱しない多数の他の特定の形態で実施され得ることは理解されるべきである。本例示は、説明のためであり限定するものではないと考えられるべきであり、ここで与えられた詳細に限定する意図はない。例えば、様々な要素または構成要素が、その他のシステムにおいて組み合わされ、または統合されてよく、いくつかの特徴が省略され、または実施されなくてよい。

【００２４】

さらに、個別のまたは分離したものとして様々な実施形態で説明または図示された技術、システム、サブシステム、および方法は、その他のシステム、モジュール、技術、または方法と、本開示の範囲を逸脱せずに組み合わされ、または統合されてよい。各々と結合もしくは直接的に結合または通信するとして示され、または説明されたその他のアイテムは、電気的、機械的、またはその他の形態であろうといくつかのインターフェイス、装置、または中間構成要素を介して間接的に結合または通信してよい。変更、代用、および改変が、当業者によって確認され、ここで開示された主旨および範囲に逸脱することなく行われ得る。

【符号の説明】

【００２５】

２００　ソースルート
４００　処理システム
４０１　処理ユニット
４１０　中央処理ユニット(ＣＰＵ)
４２０　メモリ
４３０　大容量記録装置
４４０　ビデオアダプタ
４５０　ネットワークインターフェイス
４６０　ディスプレイ
４７０　マウス/キーボード/プリンタ
４８０　ネットワーク
４９０　インターフェイス

【図１】

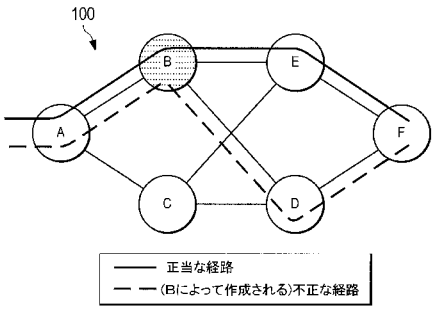

FIG. 1

【図２】

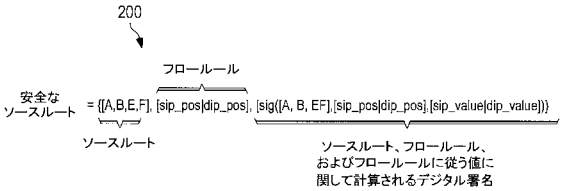

FIG. 2

【図３】

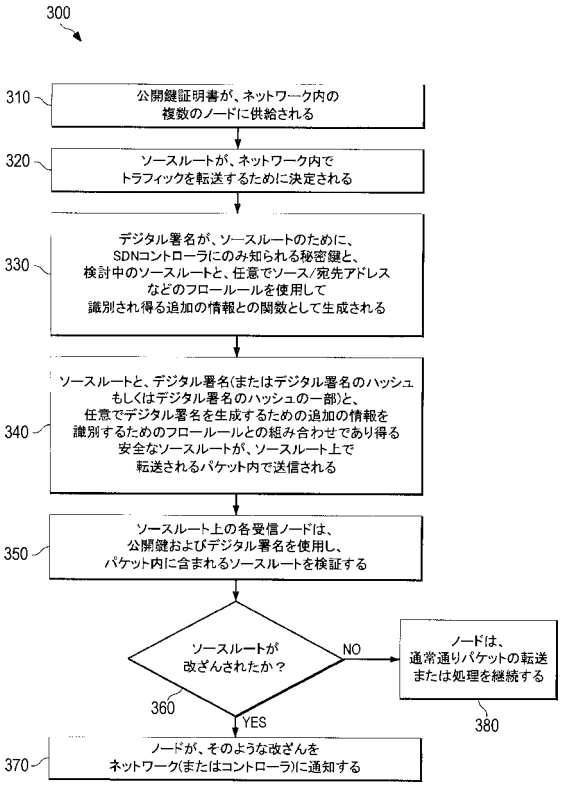

FIG. 3

【図４】

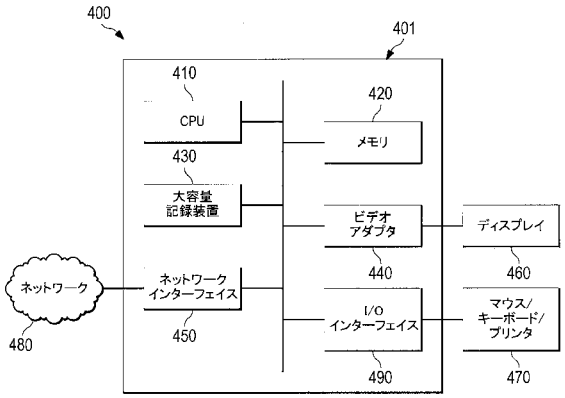

FIG. 4

【手続補正書】
【提出日】平成28年8月17日(2016.8.17)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】０００５
【補正方法】変更
【補正の内容】
【０００５】
本開示の他の実施形態に従えば、公開鍵を使用してソースルーティングを保全するためのネットワーク要素は、少なくとも1つのプロセッサと、プロセッサによる実行のためのプログラミングを記録する非一時的コンピュータ可読記録媒体とを含む。プログラミングは、ネットワーク内のトラフィックをルーティングするために決定されるソースルートのための電子署名を、秘密鍵を使用して生成するための命令を含む。ソースルートは、ネットワーク内のノードの順序を示す。プログラミングは、デジタル署名およびソースルートの組み合わせとして、安全なソースルートを提供するための命令をさらに含む。プログラミングは、安全なソースルートをトラフィックのパケットに加え、ソースルート上でパケットを送信するようにネットワーク要素をさらに構成する。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００１８
【補正方法】変更
【補正の内容】
【００１８】
図3は、ソースルートを保護するための方法300の実施形態である。ステップ310において、公開鍵証明書が、例えばSDNコントローラまたは任意の信頼できるネットワークエン

ティティによって、ネットワーク内の複数のノードに配布される。ステップ320において、ソースルートが、ネットワーク内でトラフィックを転送するために決定される。ステップ330において、SDNコントローラまたは信頼できるエンティティがソースルートのためのデジタル署名を、コントローラまたはエンティティにのみ知られる秘密鍵と、検討中のソースルートと、任意でソース/宛先アドレスなどのフロールールを使用して識別され得る追加の情報との関数として生成する。ステップ340において、ソースルートと、デジタル署名(またはデジタル署名のハッシュもしくはデジタル署名のハッシュの一部)と、任意でデジタル署名を生成するための追加の情報を識別するためのフロールールとの組み合わせであり得る安全なソースルートが、ソースルート上で転送されるパケット内で送信される。ステップ350において、ソースルート上の各受信ノードは、公開鍵およびデジタル署名を使用し、パケット内に含まれるソースルートを検証する。ステップ360において、受信ノードは、ソースルートが改ざんされたか否か、例えばパケット内のソースルートと公開鍵によってデジタル署名を処理した結果との間に不一致があるか否かを決定する。ソースルートが改ざんされている場合、ステップ370において、その後そのような改ざんをネットワーク(またはコントローラ)に通知する。パケットは廃棄されてよく、転送は停止される。そうでなければ、ステップ380において、ノードは、通常通りパケットの転送または処理を継続する。方法300において、ステップ310から340は、コントローラまたはネットワークエンティティによって実施される。ステップ350から380は、各受信ノードまたは宛先ノードによって実施される。

【手続補正３】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
公開鍵を基礎とするデジタル署名を使用してソースルーティングを保全するためのネットワーク要素による方法であって、
ネットワーク内のトラフィックをルーティングするために決定されるソースルートのためのデジタル署名を前記ネットワーク要素の秘密鍵を使用して生成するステップであって、前記ソースルートが前記ネットワーク内のノードの順序を示す、ステップと、
前記デジタル署名および前記ソースルートの組み合わせとして、安全なソースルートを提供するステップと、
前記安全なソースルートを前記トラフィックのパケットに加えるステップと、
前記ソースルート上で前記パケットを送信するステップと
を含む方法。
【請求項２】
前記ソースルートを検証するための公開鍵を前記ノードに配布するステップをさらに含む、請求項1に記載の方法。
【請求項３】
前記公開鍵を配布するステップが、前記ノードにおいて前記公開鍵の証明書を事前設定するステップを含む、請求項1に記載の方法。
【請求項４】
前記安全なソースルートを提供するステップが、前記パケット内で前記デジタル署名および前記ソースルートと共にフロールールを加えるステップをさらに含む、請求項1に記載の方法。
【請求項５】
前記デジタル署名が、前記ソースルート、および前記フロールールにより識別されるフロー情報の関数であり、前記フロー情報が、ソースアドレスおよび宛先アドレスのうちの少なくとも1つを含む、請求項4に記載の方法。

【請求項６】
前記ネットワーク要素の秘密鍵が前記ノードと共有されない、請求項1に記載の方法。
【請求項７】
公開鍵を使用してソースルーティングを保全するためのネットワーク要素であって、
少なくとも1つのプロセッサと、
前記プロセッサによる実行のためのプログラミングを記録する非一時的コンピュータ可読記録媒体とを含み、前記プログラミングは、
ネットワーク内のトラフィックをルーティングするために決定されるソースルートのためのデジタル署名を、秘密鍵を使用して生成することであって、前記ソースルートが前記ネットワーク内のノードの順序を示す、ことと、
前記デジタル署名および前記ソースルートの組み合わせとして、安全なソースルートを提供することと、
前記安全なソースルートを前記トラフィックのパケットに加えることと、
前記ソースルートで前記パケットを送信することと
を行うための命令を含む、ネットワーク要素。
【請求項８】
前記プログラミングが、前記ソースルートを検証するための公開鍵を前記ノードに配布するための命令をさらに含む、請求項7に記載のネットワーク要素。
【請求項９】
前記安全なソースルートを提供するための命令が、前記パケット内に、前記デジタル署名および前記ソースルートと共にフロールールを含めるための命令をさらに含み、前記デジタル署名が、前記ソースルートおよび前記フロールールにより識別されるフロー情報の関数である、請求項7に記載のネットワーク要素。
【請求項１０】
前記ネットワーク要素が、ソフトウェア・デファインド・ネットワーキング(SDN)コントローラである、請求項7に記載のネットワーク要素。
【請求項１１】
公開鍵を使用してソースルーティングを保全するためのネットワークノードによる方法であって、
ソースルートおよびデジタル署名を含むパケットを受信するステップであって、前記デジタル署名が、前記ソースルートと前記ネットワークノードに知られていない秘密鍵とに従って生成され、前記ソースルートがネットワーク内のノードの順序を示す、ステップと、
前記デジタル署名と前記ネットワークノードに知られる公開鍵とを使用して前記ソースルートを検証するステップと、
前記ソースルートの不一致を決定する際に、前記ソースルートの改ざんを示す通知メッセージを前記ネットワークに送信するステップと
を含む方法。
【請求項１２】
前記パケットが、フロー情報を含むフロールールをさらに含み、前記フロー情報は、ソースアドレスおよび宛先アドレスのうちの少なくとも1つを識別し、前記デジタル署名が、前記ソースルートおよび前記フロー情報の関数である、請求項11に記載の方法。
【請求項１３】
前記デジタル署名および前記公開鍵を使用して前記ソースルートを検証するステップが、
前記デジタル署名および前記公開鍵の関数としてローカルなソースルートを取得するステップと、
前記ローカルなソースルートを前記パケット内の前記ソースルートと比較するステップと
を含む、請求項11に記載の方法。

【請求項１４】
前記ネットワークから前記公開鍵の証明書を受信するステップをさらに含む、請求項11に記載の方法。
【請求項１５】
前記ネットワークノードにおいて前記ソースルートまたは前記デジタル署名をキャッシュするステップと、
前記キャッシュされたソースルートを使用するか、または前記キャッシュされたデジタル署名および前記公開鍵を使用して前記パケットの後で、第2の受信されるパケット内の第2のソースルートを検証するステップと
をさらに含む、請求項11に記載の方法。
【請求項１６】
前記第2の受信されるパケットがデジタル署名を含まない、請求項15に記載の方法。
【請求項１７】
反復的特異値分解における早期終了のためのネットワークノードであって、
少なくとも1つのプロセッサと、
前記プロセッサの実行のためのプログラミングを記録する非一時的コンピュータ可読記録媒体とを含み、前記プログラミングは、
ソースルートおよびデジタル署名を含むパケットを受信することであって、前記デジタル署名が、前記ソースルートと前記ネットワークノードに知られていない秘密鍵とに従って生成され、前記ソースルートがネットワーク内のノードの順序を示す、ことと、
前記デジタル署名と前記ネットワークノードに知られる公開鍵とを使用して前記ソースルートを検証することと、
前記ソースルートの不一致を決定する際に、前記ソースルートの改ざんを示す通知メッセージを前記ネットワークに送信すること
を行うための命令を含む、ネットワークノード。
【請求項１８】
前記パケットが、フロー情報を含むフロールールをさらに含み、前記フロー情報は、ソースアドレスおよび宛先アドレスのうちの少なくとも1つを識別し、前記デジタル署名が、前記ソースルートおよび前記フロー情報の関数である、請求項17に記載のネットワークノード。
【請求項１９】
前記プログラミングは、
前記ネットワークノードにおいて前記ソースルートまたは前記デジタル署名をキャッシュすることと、
前記キャッシュされたソースルートを使用するか、または前記キャッシュされたデジタル署名および前記公開鍵を使用して前記パケットの後で第2の受信されるパケット内の第2のソースルートを検証することと
を行うための命令をさらに含む、請求項17に記載のネットワークノード。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/072482

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/721(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, CNKI, CNPAT, IEEE, GOOGLE: source, route, traffic, path, secure, signature, encrypt, packet, header, add, SDN, MPLS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2014029445 A1 (CISCO TECHNOLOGY, INC.) 30 January 2014 (2014-01-30) description, paragraphs [0046] and [0049]; figures 3-5	1-20
A	US 2007101144 A1 (THE GO DADDY GROUP, INC.) 03 May 2007 (2007-05-03) the whole document	1-20
A	US 2005195814 A1 (NTT DOCOMO, INC.) 08 September 2005 (2005-09-08) the whole document	1-20
A	CN 1610334 A (MAO, DECAO) 27 April 2005 (2005-04-27) the whole document	1-20

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 April 2015	**15 May 2015**
Name and mailing address of the ISA/CN **STATE INTELLECTUAL PROPERTY OFFICE OF THE P.R.CHINA** **6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing 100088, China**	Authorized officer **LIU,Yi**
Facsimile No. **(86-10)62019451**	Telephone No. **(86-10)62413400**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/072482

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2014029445	A1	30 January 2014	WO	2014022296	A1	06 February 2014
US	2007101144	A1	03 May 2007	None			
US	2005195814	A1	08 September 2005	JP	2005286989	A	13 October 2005
				CN	100350774	C	21 November 2007
				US	7486651	B2	03 February 2009
				EP	1571790	A2	07 September 2005
				CN	1665211	A	07 September 2005
				EP	1571790	A3	30 November 2005
CN	1610334	A	27 April 2005	CN	100337456	C	12 September 2007

Form PCT/ISA/210 (patent family annex) (July 2009)

フロントページの続き

(51)Int.Cl.	F I		テーマコード（参考）
	Ｈ０４Ｌ 9/00	６７５Ｄ	
	Ｈ０４Ｌ 12/717		

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JP,KE,KG,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US

(72)発明者 タオ・ワン
カナダ・オンタリオ・Ｋ１Ｚ・１Ｇ１・オタワ・メトロポール・プライヴェート・７２
(72)発明者 ピーター・アッシュウッドースミス
カナダ・ケベック・Ｊ９Ａ－２Ｖ８・ガティノー・デ・ジェネヴリエ・２０
(72)発明者 メハディ・アラシュミド・アクハヴァイン・モハマディ
カナダ・オンタリオ・Ｋ２Ｈ・８Ｂ３・オタワ・グランドヴュー・ロード・４２
(72)発明者 グオリ・イン
カナダ・オンタリオ・Ｋ２Ｇ６Ｔ６・オタワ・ブルックストーン・ストリート・２３
(72)発明者 ヤペン・ウー
カナダ・オンタリオ・Ｋ２Ｇ・５Ｙ１・ネピアン・ストーンブライアー・ドライヴ・９３

Ｆターム(参考) 5J104 AA09 LA03
5K030 GA15 HA08 HC01 HD03 JA10 JA11 LB07 MC09