(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2016-538770
(P2016-538770A)
(43)公表日　平成28年12月8日(2016.12.8)

| (51)Int.Cl. | | F I | | | テーマコード（参考） |
|---|---|---|---|---|---|
| ***H04L 9/08*** | ***(2006.01)*** | H04L | 9/00 | 601B | 5J104 |
| ***H04L 9/32*** | ***(2006.01)*** | H04L | 9/00 | 675A | 5K067 |
| ***H04W 12/06*** | ***(2009.01)*** | H04W | 12/06 | | 5K201 |
| ***H04M 11/00*** | ***(2006.01)*** | H04M | 11/00 | 302 | |

審査請求 未請求　予備審査請求 未請求　（全 56 頁）

(21)出願番号　特願2016-526324 (P2016-526324)
(86)(22)出願日　平成26年10月27日 (2014.10.27)
(85)翻訳文提出日　平成28年6月24日 (2016.6.24)
(86)国際出願番号　PCT/US2014/062421
(87)国際公開番号　WO2015/065907
(87)国際公開日　平成27年5月7日 (2015.5.7)
(31)優先権主張番号　61/899,064
(32)優先日　平成25年11月1日 (2013.11.1)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　62/002,009
(32)優先日　平成26年5月22日 (2014.5.22)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　14/523,487
(32)優先日　平成26年10月24日 (2014.10.24)
(33)優先権主張国　米国 (US)

(71)出願人　595020643
クゥアルコム・インコーポレイテッド
ＱＵＡＬＣＯＭＭ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国、カリフォルニア州　９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ　５７７５
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100109830
弁理士　福原　淑弘
(74)代理人　100158805
弁理士　井関　守三
(74)代理人　100112807
弁理士　岡田　貴志

最終頁に続く

(54)【発明の名称】統合されたメッシュ認証および関連付けのためのシステムおよび方法

(57)【要約】
より効率のよいメッシュ関連付けのためのシステムおよび方法が開示される。いくつかの態様では、非メンバーデバイスは、メッシュネットワークの任意のメンバーデバイスとの４ウェイメッセージ交換を介して、メッシュネットワークに加入し得る。メッシュメンバーデバイスと非メンバーデバイスとの間の４ウェイメッセージ交換は、２つのデバイス間の認証および関連付けをもたらす。４ウェイメッセージ交換の結果として、共通グループキーが非メンバーデバイスに提供される。共通グループキーは、メッシュメンバーデバイスのいずれかの間で交換される、グループアドレス指定されたメッシュメッセージを暗号化および暗号解読するために、すべてのメッシュメンバーデバイスによって利用される。２つのデバイスの各々に関する関連付け識別子も、交換の間に提供される。ＰＨＹ／ＭＡＣ機能も交換され得る。いくつかの態様では、２つのデバイスのためのＩＰアドレス割当ても、４ウェイメッセージハンドシェイクの間に完遂され得る。

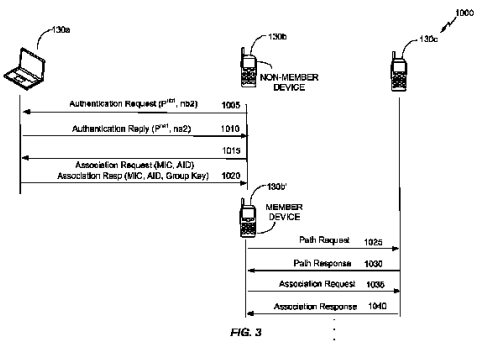


FIG. 3

【特許請求の範囲】
【請求項１】
メッシュネットワークの非メンバーデバイスの、前記メッシュネットワークのメンバーデバイスとのピア関連付けの方法であって、
前記非メンバーデバイスから前記メッシュネットワークの前記メンバーデバイスへ認証リクエストを送信することと、ここにおいて、前記認証リクエストはパスワードに基づく、
前記メンバーデバイスからの認証レスポンスを前記非メンバーデバイスによって受信することと、
前記非メンバーデバイスから前記メンバーデバイスへ、前記認証レスポンスに基づいて関連付けリクエストを送信することと、ここにおいて、前記関連付けリクエストは前記パスワードにさらに基づく、
前記メンバーデバイスからの関連付けレスポンスを前記非メンバーデバイスによって受信することと、
を備える、方法。
【請求項２】
前記認証レスポンスに基づいてペアワイズマスターキー（ＰＭＫ）を生成することと、
前記認証レスポンスからナンスを復号することと、
前記ペアワイズマスターキー（ＰＭＫ）および前記ナンスに基づいてペアワイズ一時キー（ＰＴＫ）を生成することと、
前記ペアワイズ一時キーに基づいて前記関連付けリクエストを生成することと、
をさらに備える、請求項１に記載の方法。
【請求項３】
メッシュピアリングインスタンス識別子に基づいて前記ペアワイズ一時キーを生成することをさらに備える、請求項２に記載の方法。
【請求項４】
前記ペアワイズ一時キーに基づいてメッセージ完全性コード（ＭＩＣ）を生成することと、
前記メッセージ完全性コードを示すための前記関連付けリクエストを生成することと、
をさらに備える、請求項２に記載の方法。
【請求項５】
関連付け識別子を前記メンバーデバイスに割り当てることと、
前記メンバーデバイスの前記関連付け識別子を示すための前記関連付けリクエストをさらに生成することと、
をさらに備える、請求項４に記載の方法。
【請求項６】
前記関連付けレスポンスから関連付け識別子を復号することと、
前記関連付け識別子を備えるためのメッシュメッセージを生成することと、
前記メッシュメッセージを前記メンバーデバイスへ送信することと、
をさらに備える、請求項４に記載の方法。
【請求項７】
前記パスワードに基づいて第１のメッセージ完全性コード（ＭＩＣ）を生成することと、
第２のメッセージ完全性コード（ＭＩＣ）を決定するために前記関連付けレスポンスを復号することと、
前記第１のメッセージ完全性コード（ＭＩＣ）を前記第２のメッセージ完全性コード（ＭＩＣ）と比較することと、
前記非メンバーデバイスが前記メンバーデバイスに関連付けられているかどうかを、前記比較に基づいて決定することと、
をさらに備える、請求項１に記載の方法。

【請求項８】
前記関連付けレスポンスからグループキーを復号することと、
第２の非メンバーデバイスからのメッシュメッセージを受信することと、
前記グループキーに基づいて前記メッシュメッセージを復号することと、
をさらに備える、請求項１に記載の方法。
【請求項９】
前記関連付けレスポンスからグループキーを復号することと、
シーケンス番号を備えるためのパスリクエストメッセージを生成することと、
前記グループキーに基づいて前記パスリクエストメッセージを暗号化することと、
前記暗号化されたパスリクエストメッセージを前記メッシュネットワーク上で送信することと、
をさらに備える、請求項１に記載の方法。
【請求項１０】
前記メッシュの第２のメンバーデバイスからのパスレスポンスメッセージを受信することと、
前記グループキーに基づいて前記パスレスポンスメッセージを暗号解読することと、
前記暗号解読されたパスレスポンスメッセージから前記シーケンス番号を復号することと、
前記暗号解読されたパスレスポンスに基づいて前記第２のメンバーデバイスに関連付けることと、
をさらに備える、請求項９に記載の方法。
【請求項１１】
前記メッシュ上の通信で使用するためのインターネットプロトコルアドレスを前記関連付けレスポンスから復号することをさらに備える、請求項１に記載の方法。
【請求項１２】
前記メッシュネットワーク上の通信で前記非メンバーデバイスによって使用するために提案されるインターネットプロトコルアドレスの少なくとも一部分を示すための前記認証リクエストを生成することをさらに備える、請求項１に記載の方法。
【請求項１３】
メッシュネットワークのメンバーデバイスに関連付けるための前記メッシュネットワークの非メンバー装置であって、
パスワードに基づいて認証リクエストを生成するように構成されたプロセッサと、
前記非メンバー装置から前記メッシュネットワークのメンバーデバイスへ前記認証リクエストを送信するように構成された送信機と、
前記メンバーデバイスからの認証レスポンスを受信するように構成された受信機と、
を備え、
前記プロセッサは、前記認証レスポンスおよび前記パスワードに基づいて関連付けリクエストを生成するようにさらに構成され、
前記送信機は、前記非メンバー装置から前記メンバーデバイスへ、前記関連付けリクエストを送信するようにさらに構成され、
前記受信機は、前記メンバーデバイスからの関連付けレスポンスを受信するようにさらに構成される、非メンバー装置。
【請求項１４】
前記プロセッサは、
前記認証レスポンスに基づいてペアワイズマスターキー（ＰＭＫ）を生成することと、
前記認証レスポンスからナンスを復号することと、
前記ペアワイズマスターキー（ＰＭＫ）および前記ナンスに基づいてペアワイズ一時キー（ＰＴＫ）を生成することと、
前記ペアワイズ一時キーに基づいて前記関連付けリクエストを生成することと、

を行うようにさらに構成される、請求項１３に記載の装置。
【請求項１５】
前記プロセッサは、メッシュピアリングインスタンス識別子に基づいて前記ペアワイズ一時キーを生成するようにさらに構成される、請求項１４に記載の装置。
【請求項１６】
前記プロセッサは、
前記ペアワイズ一時キーに基づいてメッセージ完全性コード（ＭＩＣ）を生成することと、
前記メッセージ完全性コードを示すための前記関連付けリクエストを生成することと、
を行うようにさらに構成される、請求項１４に記載の装置。
【請求項１７】
前記プロセッサは、
関連付け識別子を前記メンバーデバイスに割り当てることと、
前記メンバーデバイスの前記関連付け識別子を示すための前記関連付けリクエストをさらに生成することと、
を行うようにさらに構成される、請求項１５に記載の装置。
【請求項１８】
前記プロセッサは、
関連付け識別子を決定するために前記関連付けレスポンスを復号することと、
前記関連付け識別子を備えるためのメッシュメッセージを生成することと、
を行うようにさらに構成され、
前記送信機は、前記メッシュメッセージを前記メンバーデバイスへ送信するようにさらに構成される、請求項１５に記載の装置。
【請求項１９】
前記プロセッサは、
前記パスワードに基づいて第１のメッセージ完全性コード（ＭＩＣ）を生成することと、
第２のメッセージ識別コード（ＭＩＣ）を決定するために前記関連付けレスポンスを復号することと、
前記第１のメッセージ完全性コードを前記第２のメッセージ完全性コードと比較することと、
前記非メンバーデバイスが前記メンバーデバイスに関連付けられているかどうかを、前記比較に基づいて決定することと、
を行うようにさらに構成される、請求項１３に記載の装置。
【請求項２０】
前記プロセッサは、前記関連付けレスポンスからグループキーを復号するようにさらに構成され、
前記受信機は、第２の非メンバーデバイスからのメッシュメッセージを受信するようにさらに構成され、
前記プロセッサは、前記グループキーに基づいて前記メッシュメッセージを復号するようにさらに構成される、請求項１３に記載の装置。
【請求項２１】
前記プロセッサは、
前記関連付けレスポンスからグループキーを復号することと、
シーケンス番号を備えるためのパスリクエストメッセージを生成することと、
前記グループキーに基づいて前記パスリクエストメッセージを暗号化することと、
を行うようにさらに構成され、
前記送信機は、前記暗号化されたパスリクエストメッセージを前記メッシュネットワーク上で送信するようにさらに構成される、請求項１３に記載の装置。

【請求項２２】
前記送信機は、前記メッシュの第２のメンバーデバイスからのパスレスポンスメッセージを受信するようにさらに構成され、
前記プロセッサは、
前記グループキーに基づいて前記パスレスポンスメッセージを復号することと、
前記復号されたパスレスポンスメッセージから前記シーケンス番号を復号することと、
前記復号されたパスレスポンスメッセージに基づいて前記第２のメンバーデバイスに関連付けることと、
を行うようにさらに構成される、請求項２１に記載の装置。
【請求項２３】
前記プロセッサは、前記メッシュ上の通信で使用するためのインターネットプロトコルアドレスを前記関連付けレスポンスから復号するようにさらに構成される、請求項１３に記載の装置。
【請求項２４】
前記プロセッサは、前記メッシュネットワーク上の通信で前記非メンバーデバイスによって使用するために提案されるインターネットプロトコルアドレスの少なくとも一部分を示すための前記認証リクエストを生成するようにさらに構成される、請求項１３に記載の装置。
【請求項２５】
実行されたとき、メッシュネットワークの中の非メンバーデバイスの、前記メッシュネットワークのメンバーデバイスとのピア関連付けの方法をプロセッサに実行させる命令を備えるコンピュータ可読記憶媒体であって、前記方法は、
前記非メンバーデバイスから前記メッシュネットワークのメンバーデバイスへ認証リクエストを送信することと、ここにおいて、前記認証リクエストはパスワードに基づく、
前記メンバーデバイスからの認証レスポンスを前記非メンバーデバイスによって受信することと、
前記非メンバーデバイスから前記メンバーデバイスへ、前記認証レスポンスに基づいて関連付けリクエストを送信することと、ここにおいて、前記関連付けリクエストは前記パスワードにさらに基づく、
前記メンバーデバイスからの関連付けレスポンスを前記非メンバーデバイスによって受信することと、
を備える、コンピュータ可読記憶媒体。
【請求項２６】
前記方法は、
前記認証レスポンスに基づいてペアワイズマスターキー（ＰＭＫ）を生成することと、
前記認証レスポンスからナンスを復号することと、
前記ペアワイズマスターキー（ＰＭＫ）および前記ナンスに基づいてペアワイズ一時キー（ＰＴＫ）を生成することと、
前記ペアワイズ一時キーに基づいて前記関連付けリクエストを生成することと、
をさらに備える、請求項２５に記載のコンピュータ可読記憶媒体。
【請求項２７】
前記方法は、メッシュピアリングインスタンス識別子に基づいて前記ペアワイズ一時キー（ＰＴＫ）を生成することをさらに備える、請求項２６に記載のコンピュータ可読記憶媒体。
【請求項２８】
前記方法は、
前記ペアワイズ一時キーに基づいてメッセージ完全性コード（ＭＩＣ）を生成することと、
前記メッセージ完全性コードを示すための前記関連付けリクエストを生成することと、

をさらに備える、請求項２６に記載のコンピュータ可読記憶媒体。
【請求項２９】
前記方法は、
関連付け識別子を前記メンバーデバイスに割り当てることと、
前記メンバーデバイスの前記関連付け識別子を示すための前記関連付けリクエストをさらに生成することと、
をさらに備える、請求項２８に記載のコンピュータ可読記憶媒体。
【請求項３０】
前記方法は、
前記関連付けレスポンスから関連付け識別子を復号することと、
前記関連付け識別子を備えるためのメッシュメッセージを生成することと、
前記メッシュメッセージを前記メンバーデバイスへ送信することと、
をさらに備える、請求項２８に記載のコンピュータ可読記憶媒体。
【請求項３１】
前記方法は、
前記パスワードに基づいて第１のメッセージ完全性コード（ＭＩＣ）を生成することと、
第２のメッセージ完全性コード（ＭＩＣ）を決定するために前記関連付けレスポンスを復号することと、
前記第１のメッセージ完全性コード（ＭＩＣ）を前記第２のメッセージ完全性コード（ＭＩＣ）と比較することと、
前記非メンバーデバイスが前記メンバーデバイスに関連付けられているかどうかを、前記比較に基づいて決定することと、
をさらに備える、請求項２５に記載のコンピュータ可読記憶媒体。
【請求項３２】
前記方法は、
前記関連付けレスポンスからグループキーを復号することと、
第２の非メンバーデバイスからのメッシュメッセージを受信することと、
前記グループキーに基づいて前記メッシュメッセージを復号することと、
をさらに備える、請求項２５に記載のコンピュータ可読記憶媒体。
【請求項３３】
前記方法は、
前記関連付けレスポンスからグループキーを復号することと、
シーケンス番号を備えるためのパスリクエストメッセージを生成することと、
前記グループキーに基づいて前記パスリクエストメッセージを暗号化することと、
前記暗号化されたパスリクエストメッセージを前記メッシュネットワーク上で送信することと、
をさらに備える、請求項２５に記載のコンピュータ可読記憶媒体。
【請求項３４】
前記方法は、
前記メッシュの第２のメンバーデバイスからのパスレスポンスメッセージを受信することと、
前記グループキーに基づいて前記パスレスポンスメッセージを暗号解読することと、
前記暗号解読されたパスレスポンスメッセージから前記シーケンス番号を復号することと、
前記暗号解読されたパスレスポンスに基づいて前記第２のメンバーデバイスに関連付けることと、
をさらに備える、請求項３３に記載のコンピュータ可読記憶媒体。
【請求項３５】
前記方法は、前記メッシュ上の通信で使用するためのインターネットプロトコルアドレ

スを前記関連付けレスポンスから復号することをさらに備える、請求項２５に記載のコンピュータ可読記憶媒体。
【請求項３６】
前記方法は、前記メッシュネットワーク上の通信で前記非メンバーデバイスによって使用するために提案されるインターネットプロトコルアドレスの少なくとも一部分を示すための前記認証リクエストを生成することをさらに備える、請求項２５に記載のコンピュータ可読記憶媒体。
【請求項３７】
メッシュネットワーク上のピアに関連付けるための装置であって、
パスワードに基づいて認証リクエストを生成するための手段と、
前記メッシュネットワークのメンバーデバイスへ前記認証リクエストを送信するための手段と、
前記メンバーデバイスからの認証レスポンスを受信するための手段と、
前記認証レスポンスおよび前記パスワードに基づいて関連付けリクエストを生成するための手段と、
前記関連付けリクエストを前記メンバーデバイスへ送信するための手段と、
前記メンバーデバイスからの関連付けレスポンスを受信するための手段と、
を備える、装置。
【請求項３８】
前記認証レスポンスに基づいてペアワイズマスターキー（ＰＭＫ）を生成するための手段と、
前記認証レスポンスからナンスを復号するための手段と、
前記ペアワイズマスターキー（ＰＭＫ）および前記ナンスに基づいてペアワイズ一時キー（ＰＴＫ）を生成するための手段と、
前記ペアワイズ一時キーに基づいて前記関連付けリクエストを生成するための手段と、
をさらに備える、請求項３７に記載の装置。
【請求項３９】
メッシュピアリングインスタンス識別子に基づいて前記ペアワイズ一時キー（ＰＴＫ）を生成するための手段をさらに備える、請求項３８に記載の装置。
【請求項４０】
前記ペアワイズ一時キーに基づいてメッセージ完全性コード（ＭＩＣ）を生成するための手段と、
前記メッセージ完全性コードを示すための前記関連付けリクエストを生成するための手段と、
をさらに備える、請求項３８に記載の装置。
【請求項４１】
関連付け識別子を前記メンバーデバイスに割り当てるための手段と、
前記メンバーデバイスの前記関連付け識別子を示すための前記関連付けリクエストをさらに生成するための手段と
をさらに備える、請求項４０に記載の装置。
【請求項４２】
関連付け識別子を決定するために前記関連付けレスポンスを復号するための手段と、
前記関連付け識別子を備えるためのメッシュメッセージを生成するための手段と、
前記メッシュメッセージを前記メンバーデバイスへ送信するための手段と、
をさらに備える、請求項４０に記載の装置。
【請求項４３】
前記パスワードに基づいて第１のメッセージ完全性コード（ＭＩＣ）を生成するための手段と、
第２のメッセージ識別コード（ＭＩＣ）を決定するために前記関連付けレスポンスを復

号するための手段と、
前記第１のメッセージ完全性コードを前記第２のメッセージ完全性コードと比較するための手段と、
前記非メンバーデバイスが前記メンバーデバイスに関連付けられているかどうかを、前記比較に基づいて決定するための手段と、
をさらに備える、請求項３７に記載の装置。
【請求項４４】
前記関連付けレスポンスからグループキーを復号するための手段と、
第２の非メンバーデバイスからのメッシュメッセージを受信するための手段と、
前記グループキーに基づいて前記メッシュメッセージを復号するための手段と
をさらに備える、請求項３７に記載の装置。
【請求項４５】
前記関連付けレスポンスからグループキーを復号するための手段と、
シーケンス番号を備えるためのパスリクエストメッセージを生成するための手段と、
前記グループキーに基づいて前記パスリクエストメッセージを暗号化するための手段と、
前記暗号化されたパスリクエストメッセージを前記メッシュネットワーク上で送信するための手段と、
をさらに備える、請求項３７に記載の装置。
【請求項４６】
前記メッシュの第２のメンバーデバイスからのパスレスポンスメッセージを受信するための手段と、
前記グループキーに基づいて前記パスレスポンスメッセージを復号するための手段と、
前記復号されたパスレスポンスメッセージから前記シーケンス番号を復号するための手段と、
前記復号されたパスレスポンスメッセージに基づいて前記第２のメンバーデバイスに関連付けるための手段と、
をさらに備える、請求項４５に記載の装置。
【請求項４７】
前記メッシュ上の通信で使用するためのインターネットプロトコルアドレスを前記関連付けレスポンスから復号するための手段をさらに備える、請求項３７に記載の装置。
【請求項４８】
前記メッシュネットワーク上の通信で前記非メンバーデバイスによって使用するために提案されるインターネットプロトコルアドレスの少なくとも一部分を示すための前記認証リクエストを生成するための手段をさらに備える、請求項３７に記載の装置。
【請求項４９】
メッシュネットワークの非メンバーデバイスを、前記メッシュネットワークのメンバーデバイスに関連付ける方法であって、
前記メッシュネットワークの前記メンバーデバイスによって認証リクエストを受信することと、
前記メンバーデバイスから前記非メンバーデバイスへ認証レスポンスを送信することと、ここにおいて、前記認証レスポンスはパスワードに基づく、
前記非メンバーデバイスからの関連付けリクエストを前記メンバーデバイスによって受信することと、
前記メンバーデバイスから前記非メンバーデバイスへ関連付けレスポンスを送信することと、ここにおいて、前記関連付けレスポンスは前記パスワードに基づく、
を備える、方法。
【請求項５０】
前記認証リクエストからナンスを復号することと、
前記認証リクエストに基づいてペアワイズマスターキー（ＰＭＫ）を生成することと、

前記ペアワイズマスターキー（ＰＭＫ）および前記ナンスに基づいてペアワイズ一時キー（ＰＴＫ）を生成することと、
前記ペアワイズ一時キーに基づいて前記関連付けレスポンスを生成することと、
をさらに備える、請求項４９に記載の方法。
【請求項５１】
メッシュピアリングインスタンス識別子に基づいて前記ペアワイズ一時キー（ＰＴＫ）を生成することをさらに備える、請求項５０に記載の方法。
【請求項５２】
前記ペアワイズ一時キーに基づいてメッセージ完全性コード（ＭＩＣ）を生成することと、
前記メッセージ完全性コードを示すための前記関連付けレスポンスを生成することと、
をさらに備える、請求項５０に記載の方法。
【請求項５３】
関連付け識別子を前記非メンバーデバイスに割り当てることと、
前記非メンバーデバイスの前記関連付け識別子を示すための前記関連付けレスポンスをさらに生成することと、
をさらに備える、請求項５２に記載の方法。
【請求項５４】
関連付け識別子を決定するために前記関連付けリクエストを復号することと、
前記関連付け識別子を備えるためのメッシュメッセージを生成することと、
前記メッシュメッセージを前記非メンバーデバイスへ送信することと、
をさらに備える、請求項５２に記載の方法。
【請求項５５】
前記パスワードに基づいて第１のメッセージ完全性コード（ＭＩＣ）を生成することと、
第２のメッセージ完全性コード（ＭＩＣ）を決定するために前記関連付けリクエストを復号することと、
前記第１のメッセージ完全性コード（ＭＩＣ）を前記第２のメッセージ完全性コード（ＭＩＣ）と比較することと、
前記非メンバーデバイスが前記メンバーデバイスに関連付けられているかどうかを、前記比較に基づいて決定することと、
をさらに備える、請求項４９に記載の方法。
【請求項５６】
前記メッシュネットワークに関するグループキーを含めるための前記関連付けレスポンスを生成することと、
前記メッシュネットワークからのメッセージを受信することと、
前記グループキーに基づいて前記メッセージを復号することと、
をさらに備える、請求項４９に記載の方法。
【請求項５７】
前記非メンバーデバイスとの通信で使用するためのインターネットプロトコルアドレスを前記関連付けリクエストから復号することをさらに備える、請求項４９に記載の方法。
【請求項５８】
前記メッシュネットワーク上の前記非メンバーデバイスとの通信で前記メンバーデバイスによって使用するために提案されるインターネットプロトコルアドレスの少なくとも一部分を示すための前記認証レスポンスを生成することをさらに備える、請求項４９に記載の方法。
【請求項５９】
メッシュネットワークの非メンバーデバイスに関連付けるための前記メッシュネットワークのメンバー装置であって、
前記非メンバーデバイスからの認証リクエストを受信するように構成された受信機と、

前記メンバー装置から前記非メンバーデバイスへ認証レスポンスを送信するように構成された送信機と、ここにおいて、前記認証レスポンスはパスワードに基づく、
を備え、
前記受信機は、前記非メンバーデバイスからの関連付けリクエストを受信するようにさらに構成され、
前記送信機は、前記非メンバー装置から前記非メンバーデバイスへ関連付けレスポンスを送信するようにさらに構成され、前記関連付けレスポンスは前記パスワードに基づく、メンバー装置。

【請求項６０】
プロセッサをさらに備え、前記プロセッサは、
前記認証リクエストからナンスを復号することと、
前記認証リクエストに基づいてペアワイズマスターキー（ＰＭＫ）を生成することと、
前記ペアワイズマスターキー（ＰＭＫ）および前記ナンスに基づいてペアワイズ一時キー（ＰＴＫ）を生成することと、
前記ペアワイズ一時キーに基づいて前記関連付けレスポンスを生成することと、
を行うように構成される、請求項５９に記載の装置。

【請求項６１】
前記プロセッサは、メッシュピアリングインスタンス識別子に基づいて前記ペアワイズ一時キー（ＰＴＫ）を生成するようにさらに構成される、請求項６０に記載の装置。

【請求項６２】
前記プロセッサは、
前記ペアワイズ一時キーに基づいてメッセージ完全性コード（ＭＩＣ）を生成することと、
前記メッセージ完全性コードを示すための前記関連付けレスポンスを生成することと、
を行うようにさらに構成される、請求項６０に記載の装置。

【請求項６３】
前記プロセッサは、
関連付け識別子を前記非メンバーデバイスに割り当てることと、
前記非メンバーデバイスの前記関連付け識別子を示すための前記関連付けレスポンスをさらに生成することと、
を行うようにさらに構成される、請求項６２に記載の装置。

【請求項６４】
プロセッサをさらに備え、前記プロセッサは、
前記パスワードに基づいて第１のメッセージ完全性コード（ＭＩＣ）を生成することと、
第２のメッセージ完全性コード（ＭＩＣ）を決定するために前記関連付けリクエストを復号することと、
前記第１のメッセージ完全性コード（ＭＩＣ）を前記第２のメッセージ完全性コード（ＭＩＣ）と比較することと、
前記非メンバーデバイスが前記メンバーデバイスに関連付けられているかどうかを、前記比較に基づいて決定することと、
を行うようにさらに構成される、請求項５９に記載の装置。

【請求項６５】
プロセッサをさらに備え、
前記プロセッサは、前記メッシュネットワークに関するグループキーを含めるための前記関連付けレスポンスを生成するように構成され、
前記受信機は、前記メッシュネットワークからのメッセージを受信するようにさらに構成され、

前記プロセッサは、前記グループキーに基づいて前記メッセージを復号するようにさらに構成される、請求項５９に記載の装置。

【請求項６６】

プロセッサをさらに備え、前記プロセッサは、

関連付け識別子を決定するために前記関連付けリクエストを復号することと、

前記関連付け識別子を備えるためのメッシュメッセージを生成することと、

を行うように構成され、

前記送信機は、前記メッシュメッセージを前記非メンバーデバイスへ送信するようにさらに構成される、請求項５９に記載の装置。

【請求項６７】

プロセッサをさらに備え、前記プロセッサは、前記非メンバーデバイスとの通信で使用するためのインターネットプロトコルアドレスを前記関連付けリクエストから復号するように構成される、請求項５９に記載の装置。

【請求項６８】

プロセッサをさらに備え、前記プロセッサは、前記メッシュネットワーク上の前記非メンバーデバイスとの通信で前記メンバーデバイスによって使用するために提案されるインターネットプロトコルアドレスの少なくとも一部分を示すための前記認証レスポンスを生成するように構成される、請求項５９に記載の装置。

【請求項６９】

メッシュネットワークの非メンバーデバイスに関連付けるための前記メッシュネットワークのメンバー装置であって、

前記非メンバーデバイスからの認証リクエストを受信するための手段と、

前記メンバー装置から前記非メンバーデバイスへ認証レスポンスを送信するための手段と、ここにおいて、前記認証レスポンスはパスワードに基づく、

前記非メンバーデバイスからの関連付けリクエストを受信するための手段と、

前記メンバー装置から前記非メンバーデバイスへ関連付けレスポンスを送信するための手段と、ここにおいて、前記関連付けレスポンスは前記パスワードに基づく、

を備える、メンバー装置。

【請求項７０】

前記認証リクエストからナンスを復号するための手段と、

前記認証リクエストに基づいてペアワイズマスターキー（ＰＭＫ）を生成するための手段と、

前記ペアワイズマスターキー（ＰＭＫ）および前記ナンスに基づいてペアワイズ一時キー（ＰＴＫ）を生成するための手段と、

前記ペアワイズ一時キーに基づいて前記関連付けレスポンスを生成するための手段と、

をさらに備える、請求項６９に記載の装置。

【請求項７１】

メッシュピアリングインスタンス識別子に基づいて前記ペアワイズ一時キー（ＰＴＫ）を生成するための手段をさらに備える、請求項７０に記載の装置。

【請求項７２】

前記ペアワイズ一時キーに基づいてメッセージ完全性コード（ＭＩＣ）を生成するための手段と、

前記メッセージ完全性コードを示すための前記関連付けレスポンスを生成するための手段と、

をさらに備える、請求項７０に記載の装置。

【請求項７３】

関連付け識別子を前記非メンバーデバイスに割り当てるための手段と、

前記非メンバーデバイスの前記関連付け識別子を示すための前記関連付けレスポンスをさらに生成するための手段と、

をさらに備える、請求項７２に記載の装置。

【請求項７４】
関連付け識別子を決定するために前記関連付けリクエストを復号するための手段と、
前記関連付け識別子を備えるためのメッシュメッセージを生成するための手段と、
前記メッシュメッセージを前記非メンバーデバイスへ送信するための手段と、
をさらに備える、請求項７２に記載の装置。
【請求項７５】
前記パスワードに基づいて第１のメッセージ完全性コード（ＭＩＣ）を生成するための手段と、
第２のメッセージ完全性コード（ＭＩＣ）を決定するために前記関連付けリクエストを復号するための手段と、
前記第１のメッセージ完全性コード（ＭＩＣ）を前記第２のメッセージ完全性コード（ＭＩＣ）と比較するための手段と、
前記非メンバーデバイスが前記メンバーデバイスに関連付けられているかどうかを、前記比較に基づいて決定するための手段と、
をさらに備える、請求項６９に記載の装置。
【請求項７６】
前記メッシュネットワークに関するグループキーを含めるための前記関連付けレスポンスを生成するための手段と、
前記メッシュネットワークからのメッセージを受信するための手段と、
前記グループキーに基づいて前記メッセージを復号するための手段と、
をさらに備える、請求項６９に記載の装置。
【請求項７７】
前記非メンバーデバイスとの通信で使用するためのインターネットプロトコルアドレスを前記関連付けリクエストから復号するための手段をさらに備える、請求項６９に記載の装置。
【請求項７８】
前記メッシュネットワーク上の前記非メンバーデバイスとの通信で前記メンバーデバイスによって使用するために提案されるインターネットプロトコルアドレスの少なくとも一部分を示すための前記認証レスポンスを生成するための手段、をさらに備える、請求項６９に記載の装置。
【請求項７９】
実行されたとき、メッシュネットワークの非メンバーデバイスを、前記メッシュネットワークのメンバーデバイスに関連付ける方法をプロセッサに実行させる命令を備えるコンピュータ可読記憶媒体であって、前記方法は、
前記非メンバーデバイスからの認証リクエストを前記メンバーデバイスによって受信することと、
前記メンバーデバイスから前記非メンバーデバイスへ認証レスポンスを送信することと、前記認証レスポンスはパスワードに基づく、
前記非メンバーデバイスからの関連付けリクエストを前記メンバーデバイスによって受信することと、
前記メンバーデバイスから前記非メンバーデバイスへ関連付けレスポンスを送信することと、前記関連付けレスポンスは前記パスワードに基づく、
を備える、コンピュータ可読記憶媒体。
【請求項８０】
前記方法は、
前記認証リクエストからナンスを復号することと、
前記認証リクエストに基づいてペアワイズマスターキー（ＰＭＫ）を生成することと、
前記ペアワイズマスターキー（ＰＭＫ）および前記ナンスに基づいてペアワイズ一時キー（ＰＴＫ）を生成することと、
前記ペアワイズ一時キーに基づいて前記関連付けレスポンスを生成することと、

をさらに備える、請求項７９に記載のコンピュータ可読記憶媒体。
【請求項８１】
前記方法は、メッシュピアリングインスタンス識別子に基づいて前記ペアワイズ一時キー（ＰＴＫ）を生成することをさらに備える、請求項８０に記載のコンピュータ可読記憶媒体。
【請求項８２】
前記方法は、
前記ペアワイズ一時キーに基づいてメッセージ完全性コード（ＭＩＣ）を生成することと、
前記メッセージ完全性コードを示すための前記関連付けレスポンスを生成することと、
をさらに備える、請求項８０に記載のコンピュータ可読記憶媒体。
【請求項８３】
前記方法は、
関連付け識別子を前記非メンバーデバイスに割り当てることと、
前記非メンバーデバイスの前記関連付け識別子を示すための前記関連付けレスポンスをさらに生成することと、
をさらに備える、請求項８２に記載のコンピュータ可読記憶媒体。
【請求項８４】
前記方法は、
関連付け識別子を決定するために前記関連付けリクエストを復号することと、
前記関連付け識別子を備えるためのメッシュメッセージを生成することと、
前記メッシュメッセージを前記非メンバーデバイスへ送信することと、
をさらに備える、請求項８２に記載のコンピュータ可読記憶媒体。
【請求項８５】
前記方法は、
前記パスワードに基づいて第１のメッセージ完全性コード（ＭＩＣ）を生成することと、
第２のメッセージ完全性コード（ＭＩＣ）を決定するために前記関連付けリクエストを復号することと、
前記第１のメッセージ完全性コード（ＭＩＣ）を前記第２のメッセージ完全性コード（ＭＩＣ）と比較することと、
前記非メンバーデバイスが前記メンバーデバイスに関連付けられているかどうかを、前記比較に基づいて決定することと、
をさらに備える、請求項７９に記載のコンピュータ可読記憶媒体。
【請求項８６】
前記方法は、
前記メッシュネットワークに関するグループキーを含めるための前記関連付けレスポンスを生成することと、
前記メッシュネットワークからのメッセージを受信することと、
前記グループキーに基づいて前記メッセージを復号することと、
をさらに備える、請求項７９に記載のコンピュータ可読記憶媒体。
【請求項８７】
前記方法は、前記非メンバーデバイスとの通信で使用するためのインターネットプロトコルアドレスを前記関連付けリクエストから復号することをさらに備える、請求項７９に記載のコンピュータ可読記憶媒体。
【請求項８８】
前記方法は、前記メッシュネットワーク上の前記非メンバーデバイスとの通信で前記メンバーデバイスによって使用するために提案されるインターネットプロトコルアドレスの少なくとも一部分を示すための前記認証レスポンスを生成することをさらに備える、請求項７９に記載のコンピュータ可読記憶媒体。

【発明の詳細な説明】
【技術分野】
【０００１】
[0001]本開示は、一般に、近隣認識ネットワーク（ＮＡＮ：neighborhood-aware network）に関し、より詳細には、２つのメッシュピアデバイス間でメッシュ通信を確立するためのシステム、方法、およびデバイスに関する。
【背景技術】
【０００２】
[0002]同等性同時認証（ＳＡＥ：Simultaneous Authentication of Equals）は、ポイントツーポイントの適用例およびインフラストラクチャなしのネットワーク（infrastructure-less networks）で主に使用されるパスワードベースの認証である。ＳＡＥメッセージは、交換に参加している各デバイスによって生成される「ナンス（nonce）」を搬送し得る。交換された「ナンス」を使用して、ペアワイズマスターキー（ＰＭＫ：pairwise master key）が確立される。認証メッシュピアリング交換プロトコル（ＡＭＰＥ：Authenticated Mesh Peering Exchange protocol）は、ペアワイズ一時キー（ＰＴＫ：pairwise transient key）の生成を容易にするために「ナンス」を交換する。
【０００３】
[0003]８０２．１１ｓは、上述されたようなペアワイズマスターキー（ＰＭＫ）を確立するためのＳＡＥ認証と、ＰＴＫを生成するＡＭＰＥプロトコルとの組合せを利用する。生成されたＰＴＫは、セキュリティの理由のため、ＡＭＰＥを実行する２つのデバイスによって交換されない。代わりに、両方のデバイスによって同じＰＴＫが所有されていることが、メッセージ完全性コード（ＭＩＣ：message integrity code）を含むメッセージを交換することによって確認される。ＭＩＣは、ＰＴＫに基づいて生成される。グループキーも、ＡＭＰＥプロトコルを使用して確立される。
【０００４】
[0004]８０２．１１ｓにおけるメッシュピアリングにおいてＳＡＥおよびＡＭＰＥプロトコルを使用することは、メッシュピア関係が確立される前に少なくとも８つのメッセージがデバイスの各ペア間で交換されなければならないという点で非効率である。したがって、より効率のよいメッシュピアリングに対する必要性がある。
【発明の概要】
【０００５】
[0005]既存のグループキー管理プロセスは、比較的大きいオーバーヘッドを有し、８０２．１１ｓにおける状態情報の相当な保守を必要とする。たとえば、各メッシュステーションは、それ自体の送信メッシュグループキーを決定する。送信メッシュグループキーは、次いで、メッシュまたはグループへの、グループアドレス指定された任意の送信（any group addressed transmissions）を暗号化するために使用される。各メッシュステーションは、各メッシュピアに関する別個の受信メッシュグループキーを記憶することが必要とされ、これにより、メッシュステーションが各メッシュピアから受信される任意のメッシュメッセージを首尾よく（successfully）暗号解読することが可能になる。その上、たとえば、特定のメッシュピアデバイスがネットワークから離れるようにメッシュの構成が変化するとき、残りの各メッシュデバイスは、それの前のグループキーを廃棄し得、新しいグループキーを生成し得る。新しいグループキーは、次いで、残りのグループピアの各々に再配布され得る。
【０００６】
[0006]開示される方法およびシステムは、上述された複雑で厄介な認証プロセスをなくす軽量の（light-weight）メッシュ認証メカニズムを提供する。最初に、提案される方法とシステムとを使用すると、ソーシャルＷｉ－Ｆｉ（登録商標）（social Wi-Fi）ネットワークに加入することを求める非メンバーステーションは、ただ１つのメッシュメンバーステーションと認証する／関連付けることが必要とされる。認証／関連付けが成功した場合、新しいメッシュステーションは、メッシュネットワークに完全に関連付けられる。こ

の簡易化した手法は、上述された既存のシステムによって使用されるようなメッシュ通信向けのステーション固有のグループキーをなくすことによって、少なくとも部分的に可能にされる。代わりに、共通グループキーが、メッシュネットワークに関連付けられたすべてデバイスに対して使用される。この単一の共通グループキーは、グループアドレス指定されたメッシュネットワークトラフィックを暗号化および暗号解読するために、関連付けられた各デバイスによって使用され得る。いくつかの態様はまた、共通グループキーを使用してユニキャストパケットを暗号化し得、－そのような実装形態では、メッシュトラフィックはまた、グループキーを使用して暗号化され得る。

【０００７】

[0007]開示される方法およびシステムは、８０２．１１ａｉにおいてソーシャルＷｉ－Ｆｉ環境に対して使用される高速初期リンクセットアップ（ＦＩＬＳ：Fast Initial Link Setup）メッセージと類似のメッセージを適用する。新しいメッセージはまた、４ウェイハンドシェイク（four way handshake）のみを使用してメッシュピア認証と関連付けとを完遂する（accomplish）ために、同等性同時認証（ＳＡＥ）メッセージからいくつかの機能を包含する。提案される４ウェイハンドシェイクを介した関連付けが成功すると、上記で説明した共通グループキーは新しいメンバーデバイスと共有される。ＰＨＹ／ＭＡＣ機能も、認証／関連付けプロセスの間に２つのデバイスによって交換され得る。提案される４ウェイハンドシェイクはまた、交換に参加している各デバイスに関する関連付け識別子を確立する。提案される４ウェイハンドシェイクはまた、他のデバイスとの通信の間、交換に参加している各デバイスによって使用されるべきＩＰアドレスを確立するために使用され得る。たとえば、提案されるメッセージのうちのいくつかは、交換に参加している第１のデバイスが、交換の第２のデバイスとの通信のために使用することを選好する（prefers）ＩＰアドレスを提案するための方法を提供する。他のメッセージは、関連付けプロセスが完了すると、他のデバイスがどのＩＰアドレスを使用するべきであるかを、第１のデバイスまたは第２のデバイスのいずれかが示すためのメカニズムを提供する。

【０００８】

[0008]開示される一態様は、メッシュネットワークにおけるピア関連付けの方法である。方法は、メッシュネットワークの非メンバーデバイスを介してパスワードを受信することと、認証リクエストをメッシュネットワークのメンバーデバイスへ非メンバーデバイスを介して送信することと、認証リクエストはパスワードに基づき、メンバーデバイスからの認証レスポンスを非メンバーデバイスを介して受信することと、認証レスポンスに基づいて関連付けリクエストをメンバーデバイスへ非メンバーデバイスを介して送信することと、関連付けリクエストはパスワードにさらに基づき、メンバーデバイスからの関連付けレスポンスを非メンバーデバイスを介して受信することと、を含む。

【０００９】

[0009]方法のいくつかの態様はまた、認証レスポンスに基づいてペアワイズマスターキー（ＰＭＫ）を生成することと、認証レスポンスからナンスを復号することと、ペアワイズマスターキー（ＰＭＫ）およびナンスに基づいてペアワイズ一時キー（ＰＴＫ）を生成することと、ペアワイズ一時キーに基づいて関連付けリクエストを生成することと、を含む。方法のいくつかの態様はまた、ペアワイズ一時キーに基づいてメッセージ完全性コード（ＭＩＣ）を生成することと、メッセージ完全性コードを示すための関連付けリクエストを生成することと、を含む。方法のいくつかの態様はまた、関連付け識別子をメンバーデバイスに割り当てることと、メンバーデバイスの関連付け識別子を示すための関連付けリクエストをさらに生成することと、を含む。方法のいくつかの態様はまた、関連付けレスポンスから関連付け識別子を復号することと、関連付け識別子を備えるためのメッシュメッセージを生成することと、メッシュメッセージをメンバーデバイスへ送信することと、を含む。

【００１０】

[0010]方法のいくつかの態様はまた、パスワードに基づいて第１のメッセージ完全性コード（ＭＩＣ）を生成することと、第２のメッセージ完全性コード（ＭＩＣ）を決定する

ために関連付けレスポンスを復号することと、第１のメッセージ完全性コード（ＭＩＣ）を第２のメッセージ完全性コード（ＭＩＣ）と比較することと、非メンバーデバイスがメンバーデバイスに関連付けられているかどうかを、比較に基づいて決定することと、を含む。方法のいくつかの態様はまた、関連付けレスポンスからグループキーを復号することと、第２の非メンバーデバイスからのメッシュメッセージを受信することと、グループキーに基づいてメッシュメッセージを復号することと、を含む。方法のいくつかの態様はまた、関連付けレスポンスからグループキーを復号することと、シーケンス番号を備えるためのパスリクエストメッセージ（a path request message）を生成することと、グループキーに基づいてパスリクエストメッセージを暗号化することと、暗号化されたパスリクエストメッセージをメッシュネットワーク上で送信することと、を含む。

【００１１】

[0011]方法のいくつかの態様はまた、メッシュの第２のメンバーデバイスからのパスレスポンスメッセージを受信することと、グループキーに基づいてパスレスポンスメッセージを復号することと、復号されたパスレスポンスメッセージからシーケンス番号を復号することと、復号されたパスレスポンスに基づいて第２のメンバーデバイスに関連付けることと、を含む。方法のいくつかの態様はまた、メッシュ上の通信で使用するためのインターネットプロトコルアドレスを関連付けレスポンスから復号することを含む。方法のいくつかの態様はまた、メッシュネットワーク上の通信で非メンバーデバイスによって使用するために提案されるインターネットプロトコルアドレスの少なくとも一部分を示すための認証リクエストを生成することを含む。

【００１２】

[0012]開示される別の態様は、メッシュネットワーク上のピアに関連付けるための装置である。装置は、パスワードを受信するように構成された入力デバイスと、パスワードに基づいて認証リクエストを生成するように構成されたプロセッサと、メッシュネットワークのメンバーデバイスへ認証リクエストを送信するように構成された送信機と、メンバーデバイスからの認証レスポンスを受信するように構成された受信機と、を含む。プロセッサは、認証レスポンスおよびパスワードに基づいて関連付けリクエストを生成するようにさらに構成され、送信機は、関連付けリクエストをメンバーデバイスへ送信するようにさらに構成され、受信機は、メンバーデバイスからの関連付けレスポンスを受信するようにさらに構成される。

【００１３】

[0013]装置のいくつかの態様では、プロセッサは、認証レスポンスに基づいてペアワイズマスターキー（ＰＭＫ）を生成することと、認証レスポンスからナンスを復号することと、ペアワイズマスターキー（ＰＭＫ）およびナンスに基づいてペアワイズ一時キー（ＰＴＫ）を生成することと、ペアワイズ一時キーに基づいて関連付けリクエストを生成することと、を行うようにさらに構成される。いくつかの態様では、プロセッサは、ペアワイズ一時キーに基づいてメッセージ完全性コード（ＭＩＣ）を生成することと、メッセージ完全性コードを示すための関連付けリクエストを生成することと、を行うようにさらに構成される。いくつかの態様では、プロセッサは、関連付け識別子をメンバーデバイスに割り当てることと、メンバーデバイスの関連付け識別子を示すための関連付けリクエストをさらに生成することと、を行うようにさらに構成される。いくつかの態様では、プロセッサは、関連付け識別子を決定するために関連付けレスポンスを復号することと、関連付け識別子を備えるためのメッシュメッセージを生成することと、を行うようにさらに構成され、送信機は、メッシュメッセージをメンバーデバイスへ送信するようにさらに構成される。

【００１４】

[0014]いくつかの態様では、プロセッサは、パスワードに基づいて第１のメッセージ完全性コード（ＭＩＣ）を生成することと、第２のメッセージ識別コード（ＭＩＣ）を決定するために関連付けレスポンスを復号することと、第１のメッセージ完全性コードを第２のメッセージ完全性コードと比較することと、非メンバーデバイスがメンバーデバイスに

関連付けられているかどうかを、比較に基づいて決定することと、を行うようにさらに構成される。いくつかの態様では、プロセッサは、関連付けレスポンスからグループキーを復号するようにさらに構成され、受信機は、第２の非メンバーデバイスからのメッシュメッセージを受信するようにさらに構成され、プロセッサは、グループキーに基づいてメッシュメッセージを復号するようにさらに構成される。

【００１５】

[0015]いくつかの態様では、プロセッサは、関連付けレスポンスからグループキーを復号することと、シーケンス番号を備えるためのパスリクエストメッセージを生成することと、グループキーに基づいてパスリクエストメッセージを暗号化することと、を行うようにさらに構成され、送信機は、暗号化されたパスリクエストメッセージをメッシュネットワーク上で送信するようにさらに構成される。いくつかの態様では、送信機は、メッシュの第２のメンバーデバイスからのパスレスポンスメッセージを受信するようにさらに構成され、プロセッサは、グループキーに基づいてパスレスポンスメッセージを復号することと、復号されたパスレスポンスメッセージからシーケンス番号を復号することと、復号されたパスレスポンスメッセージに基づいて第２のメンバーデバイスに関連付けることと、を行うようにさらに構成される。いくつかの態様では、プロセッサは、メッシュ上の通信で使用するためのインターネットプロトコルアドレスを関連付けレスポンスから復号するようにさらに構成される。いくつかの態様では、プロセッサは、メッシュネットワーク上の通信で非メンバーデバイスによって使用するために提案されるインターネットプロトコルアドレスの少なくとも一部分を示すための認証リクエストを生成するようにさらに構成される。

【００１６】

[0016]開示される別の態様は、実行されたとき、メッシュネットワークの中のピア関連付けの方法をプロセッサに実行させる命令を備えるコンピュータ可読記憶媒体であって、方法は、メッシュネットワークの非メンバーデバイスを介してパスワードを受信することと、認証リクエストをメッシュネットワークのメンバーデバイスへ非メンバーデバイスを介して送信することと、認証リクエストはパスワードに基づき、メンバーデバイスからの認証レスポンスを非メンバーデバイスを介して受信することと、認証レスポンスに基づいて関連付けリクエストをメンバーデバイスへ非メンバーデバイスを介して送信することと、関連付けリクエストはパスワードにさらに基づき、メンバーデバイスからの関連付けレスポンスを非メンバーデバイスを介して受信することと、を備える。

【００１７】

[0017]方法のいくつかの態様はまた、認証レスポンスに基づいてペアワイズマスターキー（ＰＭＫ）を生成することと、認証レスポンスからナンスを復号することと、ペアワイズマスターキー（ＰＭＫ）およびナンスに基づいてペアワイズ一時キー（ＰＴＫ）を生成することと、ペアワイズ一時キーに基づいて関連付けリクエストを生成することと、を含む。方法のいくつかの態様はまた、ペアワイズ一時キーに基づいてメッセージ完全性コード（ＭＩＣ）を生成することと、メッセージ完全性コードを示すための関連付けリクエストを生成することと、を含む。方法のいくつかの態様はまた、関連付け識別子をメンバーデバイスに割り当てることと、メンバーデバイスの関連付け識別子を示すための関連付けリクエストをさらに生成することと、を含む。方法のいくつかの態様はまた、関連付けレスポンスから関連付け識別子を復号することと、関連付け識別子を備えるためのメッシュメッセージを生成することと、メッシュメッセージをメンバーデバイスへ送信することと、を含む。

【００１８】

[0018]方法のいくつかの態様はまた、パスワードに基づいて第１のメッセージ完全性コード（ＭＩＣ）を生成することと、第２のメッセージ完全性コード（ＭＩＣ）を決定するために関連付けレスポンスを復号することと、第１のメッセージ完全性コード（ＭＩＣ）を第２のメッセージ完全性コード（ＭＩＣ）と比較することと、非メンバーデバイスがメンバーデバイスに関連付けられているかどうかを、比較に基づいて決定することと、を含

む。方法のいくつかの態様はまた、関連付けレスポンスからグループキーを復号することと、第２の非メンバーデバイスからのメッシュメッセージを受信することと、グループキーに基づいてメッシュメッセージを復号することと、を含む。方法のいくつかの態様はまた、関連付けレスポンスからグループキーを復号することと、シーケンス番号を備えるためのパスリクエストメッセージを生成することと、グループキーに基づいてパスリクエストメッセージを暗号化することと、暗号化されたパスリクエストメッセージをメッシュネットワーク上で送信することと、を含む。

【００１９】

[0019]方法のいくつかの態様はまた、メッシュの第２のメンバーデバイスからのパスレスポンスメッセージを受信することと、グループキーに基づいてパスレスポンスメッセージを復号することと、復号されたパスレスポンスメッセージからシーケンス番号を復号することと、復号されたパスレスポンスに基づいて第２のメンバーデバイスに関連付けることと、を含む。方法のいくつかの態様はまた、メッシュ上の通信で使用するためのインターネットプロトコルアドレスを関連付けレスポンスから復号することを含む。方法のいくつかの態様はまた、メッシュネットワーク上の通信で非メンバーデバイスによって使用するために提案されるインターネットプロトコルアドレスの少なくとも一部分を示すための認証リクエストを生成することを含む。

【００２０】

[0020]開示される別の態様は、メッシュネットワークの中のピア関連付けの方法を実行するための装置であって、装置は、パスワードを受信するための手段と、メッシュネットワークのメンバーデバイスへ認証リクエストを送信するための手段と、認証リクエストはパスワードに基づき、メンバーデバイスからの認証レスポンスを受信するための手段と、認証レスポンスに基づいて関連付けリクエストをメンバーデバイスへ送信するための手段と、関連付けリクエストはパスワードにさらに基づき、メンバーデバイスからの関連付けレスポンスを受信するための手段と、を備える。

【００２１】

[0021]装置のいくつかの態様はまた、認証レスポンスに基づいてペアワイズマスターキー（ＰＭＫ）を生成するための手段と、認証レスポンスからナンスを復号するための手段と、ペアワイズマスターキー（ＰＭＫ）およびナンスに基づいてペアワイズ一時キー（ＰＴＫ）を生成するための手段と、ペアワイズ一時キーに基づいて関連付けリクエストを生成するための手段と、を含む。装置のいくつかの態様はまた、ペアワイズ一時キーに基づいてメッセージ完全性コード（ＭＩＣ）を生成するための手段と、メッセージ完全性コードを示すための関連付けリクエストを生成するための手段と、を含む。装置のいくつかの態様はまた、関連付け識別子をメンバーデバイスに割り当てるための手段と、メンバーデバイスの関連付け識別子を示すための関連付けリクエストをさらに生成するための手段と、を含む。装置のいくつかの態様はまた、関連付けレスポンスから関連付け識別子を復号するための手段と、関連付け識別子を備えるためのメッシュメッセージを生成するための手段と、メッシュメッセージをメンバーデバイスへ送信するための手段と、を含む。

【００２２】

[0022]装置のいくつかの態様はまた、パスワードに基づいて第１のメッセージ完全性コード（ＭＩＣ）を生成するための手段と、第２のメッセージ完全性コード（ＭＩＣ）を決定するために関連付けレスポンスを復号するための手段と、第１のメッセージ完全性コード（ＭＩＣ）を第２のメッセージ完全性コード（ＭＩＣ）と比較するための手段と、非メンバーデバイスがメンバーデバイスに関連付けられているかどうかを、比較に基づいて決定するための手段と、を含む。装置のいくつかの態様はまた、関連付けレスポンスからグループキーを復号するための手段と、第２の非メンバーデバイスからのメッシュメッセージを受信するための手段と、グループキーに基づいてメッシュメッセージを復号することと、を含む。装置のいくつかの態様はまた、関連付けレスポンスからグループキーを復号するための手段と、シーケンス番号を備えるためのパスリクエストメッセージを生成するための手段と、グループキーに基づいてパスリクエストメッセージを暗号化するための手

段と、暗号化されたパスリクエストメッセージをメッシュネットワーク上で送信するための手段と、を含む。

【００２３】

[0023]装置のいくつかの態様はまた、メッシュの第２のメンバーデバイスからのパスレスポンスメッセージを受信するための手段と、グループキーに基づいてパスレスポンスメッセージを復号するための手段と、復号されたパスレスポンスメッセージからシーケンス番号を復号するための手段と、復号されたパスレスポンスに基づいて第２のメンバーデバイスに関連付けるための手段と、を含む。装置のいくつかの態様はまた、メッシュ上の通信で使用するためのインターネットプロトコルアドレスを関連付けレスポンスから復号するための手段を含む。装置のいくつかの態様はまた、メッシュネットワーク上の通信で非メンバーデバイスによって使用するために提案されるインターネットプロトコルアドレスの少なくとも一部分を示すための認証リクエストを生成するための手段を含む。

【００２４】

[0024]開示される別の態様は、メッシュネットワークの非メンバーデバイスに関連付ける方法である。方法は、メンバーデバイスを介してパスワードを受信することと、認証リクエストをメッシュネットワークのメンバーデバイスを介して受信することと、認証レスポンスを非メンバーデバイスへメンバーデバイスを介して送信することと、認証レスポンスはパスワードに基づき、非メンバーデバイスからの関連付けリクエストをメンバーデバイスを介して受信することと、関連付けレスポンスを非メンバーデバイスへメンバーデバイスを介して送信することと、関連付けレスポンスはパスワードに基づき、を含む。いくつかの態様では、方法は、認証リクエストからナンスを復号することと、認証リクエストに基づいてペアワイズマスターキー（ＰＭＫ）を生成することと、ペアワイズマスターキー（ＰＭＫ）およびナンスに基づいてペアワイズ一時キー（ＰＴＫ）を生成することと、ペアワイズ一時キーに基づいて関連付けレスポンスを生成することと、を含む。いくつかの態様では、方法は、ペアワイズ一時キーに基づいてメッセージ完全性コード（ＭＩＣ）を生成することと、メッセージ完全性コードを示すための関連付けレスポンスを生成することと、を含む。いくつかの態様では、方法は、関連付け識別子を非メンバーデバイスに割り当てることと、非メンバーデバイスの関連付け識別子を示すための関連付けレスポンスをさらに生成することと、を含む。いくつかの態様では、方法は、関連付け識別子を決定するために関連付けリクエストを復号することと、関連付け識別子を備えるためのメッシュメッセージを生成することと、メッシュメッセージを非メンバーデバイスへ送信することと、を含む。

【００２５】

[0025]いくつかの態様では、方法は、パスワードに基づいて第１のメッセージ完全性コード（ＭＩＣ）を生成することと、第２のメッセージ完全性コード（ＭＩＣ）を決定するために関連付けリクエストを復号することと、第１のメッセージ完全性コード（ＭＩＣ）を第２のメッセージ完全性コード（ＭＩＣ）と比較することと、非メンバーデバイスがメンバーデバイスに関連付けられているかどうかを、比較に基づいて決定することと、を含む。いくつかの態様では、方法は、メッシュネットワークに関するグループキーを含めるための関連付けレスポンスを生成することと、メッシュネットワークからのメッセージを受信することと、グループキーに基づいてメッセージを復号することと、を含む。いくつかの態様では、方法は、非メンバーデバイスとの通信で使用するためのインターネットプロトコルアドレスを関連付けリクエストから復号することを含む。いくつかの態様では、方法は、メッシュネットワーク上の非メンバーデバイスとの通信でメンバーデバイスによって使用するために提案されるインターネットプロトコルアドレスの少なくとも一部分を示すための認証レスポンスを生成することを含む。

【００２６】

[0026]開示される別の態様は、メッシュネットワークの非メンバーデバイスに関連付けるための装置である。装置は、パスワードを受信するように構成されたプロセッサと、非メンバーデバイスからの認証リクエストを受信するように構成された受信機と、認証レス

ポンスを非メンバーデバイスへ送信するように構成された送信機と、を含み、認証レスポンスはパスワードに基づく。受信機は、非メンバーデバイスからの関連付けリクエストを受信するようにさらに構成され、送信機は、関連付けレスポンスを非メンバーデバイスへ送信するようにさらに構成され、関連付けレスポンスはパスワードに基づく。いくつかの態様では、プロセッサは、認証リクエストからナンスを復号することと、認証リクエストに基づいてペアワイズマスターキー（ＰＭＫ）を生成することと、ペアワイズマスターキー（ＰＭＫ）およびナンスに基づいてペアワイズ一時キー（ＰＴＫ）を生成することと、ペアワイズ一時キーに基づいて関連付けレスポンスを生成することと、を行うようにさらに構成される。いくつかの態様では、プロセッサは、ペアワイズ一時キーに基づいてメッセージ完全性コード（ＭＩＣ）を生成することと、メッセージ完全性コードを示すための関連付けレスポンスを生成することと、を行うようにさらに構成される。いくつかの態様では、プロセッサは、関連付け識別子を非メンバーデバイスに割り当てることと、非メンバーデバイスの関連付け識別子を示すための関連付けレスポンスをさらに生成することと、を行うようにさらに構成される。いくつかの態様では、プロセッサは、パスワードに基づいて第１のメッセージ完全性コード（ＭＩＣ）を生成することと、第２のメッセージ完全性コード（ＭＩＣ）を決定するために関連付けリクエストを復号することと、第１のメッセージ完全性コード（ＭＩＣ）を第２のメッセージ完全性コード（ＭＩＣ）と比較することと、非メンバーデバイスがメンバーデバイスに関連付けられているかどうかを、比較に基づいて決定することと、を行うようにさらに構成される。

【００２７】

[0027]装置のいくつかの態様では、プロセッサは、メッシュネットワークに関するグループキーを含めるための関連付けレスポンスを生成するようにさらに構成され、受信機は、メッシュネットワークからのメッセージを受信するようにさらに構成され、プロセッサは、グループキーに基づいてメッセージを復号するようにさらに構成される。

【００２８】

[0028]いくつかの態様では、プロセッサは、関連付け識別子を決定するために関連付けリクエストを復号することと、関連付け識別子を備えるためのメッシュメッセージを生成することと、を行うようにさらに構成され、送信機は、メッシュメッセージを非メンバーデバイスへ送信するようにさらに構成される。いくつかの態様では、プロセッサは、非メンバーデバイスとの通信で使用するためのインターネットプロトコルアドレスを関連付けリクエストから復号するようにさらに構成される。いくつかの態様では、プロセッサは、メッシュネットワーク上の非メンバーデバイスとの通信でメンバーデバイスによって使用するために提案されるインターネットプロトコルアドレスの少なくとも一部分を示すための認証レスポンスを生成するようにさらに構成される。

【００２９】

[0029]開示される別の態様は、メッシュネットワークの非メンバーデバイスに関連付けるための装置である。装置は、パスワードを受信するための手段と、認証リクエストを受信するための手段と、認証レスポンスを非メンバーデバイスへ送信するための手段と、認証レスポンスはパスワードに基づき、非メンバーデバイスからの関連付けリクエストを受信するための手段と、関連付けレスポンスを非メンバーデバイスへ送信するための手段と、関連付けレスポンスはパスワードに基づき、を含む。いくつかの態様では、装置は、認証リクエストからナンスを復号するための手段と、認証リクエストに基づいてペアワイズマスターキー（ＰＭＫ）を生成するための手段と、ペアワイズマスターキー（ＰＭＫ）およびナンスに基づいてペアワイズ一時キー（ＰＴＫ）を生成するための手段と、ペアワイズ一時キーに基づいて関連付けレスポンスを生成するための手段と、を含む。いくつかの態様では、装置は、ペアワイズ一時キーに基づいてメッセージ完全性コード（ＭＩＣ）を生成するための手段と、メッセージ完全性コードを示すための関連付けレスポンスを生成するための手段と、を含む。いくつかの態様では、装置は、関連付け識別子を非メンバーデバイスに割り当てるための手段と、非メンバーデバイスの関連付け識別子を示すための関連付けレスポンスを生成するためのさらなる手段と、を含む。いくつかの態様では、装

置は、関連付け識別子を決定するために関連付けリクエストを復号するための手段と、関連付け識別子を備えるためのメッシュメッセージを生成するための手段と、メッシュメッセージを非メンバーデバイスへ送信するための手段と、を含む。

【００３０】

[0030]いくつかの態様では、装置は、パスワードに基づいて第１のメッセージ完全性コード（ＭＩＣ）を生成するための手段と、第２のメッセージ完全性コード（ＭＩＣ）を決定するために関連付けリクエストを復号するための手段と、第１のメッセージ完全性コード（ＭＩＣ）を第２のメッセージ完全性コード（ＭＩＣ）と比較するための手段と、非メンバーデバイスがメンバーデバイスに関連付けられているかどうかを、比較に基づいて決定するための手段と、を含む。いくつかの態様では、装置は、メッシュネットワークに関するグループキーを含めるための関連付けレスポンスを生成するための手段と、メッシュネットワークからのグループアドレス指定されたメッセージ（a group-addressed message）を受信するための手段と、グループキーに基づいてグループアドレス指定されたメッセージを復号するための手段と、を含む。いくつかの態様では、装置は、非メンバーデバイスとの通信で使用するためのインターネットプロトコルアドレスを関連付けリクエストから復号するための手段を含む。いくつかの態様では、方法は、メッシュネットワーク上の非メンバーデバイスとの通信でメンバーデバイスによって使用するために提案されるインターネットプロトコルアドレスの少なくとも一部分を示すための認証レスポンスを生成するための手段を含む。

【００３１】

[0031]開示される別の態様は、実行されたとき、メッシュネットワークの非メンバーデバイスに関連付ける方法をプロセッサに実行させる命令を備えるコンピュータ可読記憶媒体である。方法は、メンバーデバイスを介してパスワードを受信することと、認証リクエストをメッシュネットワークのメンバーデバイスを介して受信することと、認証レスポンスを非メンバーデバイスへメンバーデバイスを介して送信することと、認証レスポンスはパスワードに基づき、非メンバーデバイスからの関連付けリクエストをメンバーデバイスを介して受信することと、関連付けレスポンスを非メンバーデバイスへメンバーデバイスを介して送信することと、関連付けレスポンスはパスワードに基づき、を含む。いくつかの態様では、方法は、認証リクエストからナンスを復号することと、認証リクエストに基づいてペアワイズマスターキー（ＰＭＫ）を生成することと、ペアワイズマスターキー（ＰＭＫ）およびナンスに基づいてペアワイズ一時キー（ＰＴＫ）を生成することと、ペアワイズ一時キーに基づいて関連付けレスポンスを生成することと、を含む。いくつかの態様では、方法は、ペアワイズ一時キーに基づいてメッセージ完全性コード（ＭＩＣ）を生成することと、メッセージ完全性コードを示すための関連付けレスポンスを生成することと、を含む。いくつかの態様では、方法は、関連付け識別子を非メンバーデバイスに割り当てることと、非メンバーデバイスの関連付け識別子を示すための関連付けレスポンスをさらに生成することと、を含む。いくつかの態様では、方法は、関連付け識別子を決定するために関連付けリクエストを復号することと、関連付け識別子を備えるためのメッシュメッセージを生成することと、メッシュメッセージを非メンバーデバイスへ送信することと、を含む。

【００３２】

[0032]いくつかの態様では、方法は、パスワードに基づいて第１のメッセージ完全性コード（ＭＩＣ）を生成することと、第２のメッセージ完全性コード（ＭＩＣ）を決定するために関連付けリクエストを復号することと、第１のメッセージ完全性コード（ＭＩＣ）を第２のメッセージ完全性コード（ＭＩＣ）と比較することと、非メンバーデバイスがメンバーデバイスに関連付けられているかどうかを、比較に基づいて決定することと、を含む。いくつかの態様では、方法は、メッシュネットワークに関するグループキーを含めるための関連付けレスポンスを生成することと、メッシュネットワークからのメッセージを受信することと、グループキーに基づいてメッセージを復号することと、を含む。いくつかの態様では、方法は、非メンバーデバイスとの通信で使用するためのインターネットプ

ロトコルアドレスを関連付けリクエストから復号することを含む。いくつかの態様では、方法は、メッシュネットワーク上の非メンバーデバイスとの通信でメンバーデバイスによって使用するために提案されるインターネットプロトコルアドレスの少なくとも一部分を示すための認証レスポンスを生成することを含む。

【００３３】

[0033]開示される一態様は、メッシュピアデバイスとの安全な接続を確立する方法である。方法は、メッシュピアデバイスからのピアリンクオープンメッセージを受信することと、メッシュピアデバイスに関するピアコミットスカラー（a peer commit scalar）を決定するためにピアリンクオープンメッセージを復号することと、メッシュピアデバイスに関するピアコミット要素を決定するためにピアリンクオープンメッセージを復号することと、ピアコミットスカラーおよびピアコミット要素に基づいてセキュリティキー識別子を決定することと、セキュリティキー識別子に基づいてメッシュピアデバイスと通信することと、を含む。

【００３４】

[0034]いくつかの態様では、方法は、コミットスカラーを生成することと、コミット要素を生成することと、ピアリンクオープンメッセージを送信することと、をさらに含み、ピアリンクオープンメッセージはコミットスカラーとコミット要素とを示す。いくつかの態様では、セキュリティキー識別子を決定することは、コミットスカラーおよびコミット要素にさらに基づく。

【００３５】

[0035]いくつかの態様では、方法は、ピアリンク確認メッセージを受信することと、ピアリンク確認メッセージはピア確認識別子を示し、ピア確認識別子に基づいてセキュリティキー識別子を検証することと、メッシュピアデバイスと通信するべきかどうかを検証に基づいて決定することと、を含む。

【００３６】

[0036]いくつかの態様では、方法は、コミットスカラーおよびコミット要素に基づいて確認識別子を生成することと、確認識別子を示すピアリンク確認メッセージを生成することと、ピアリンク確認メッセージをメッシュピアデバイスへ送信することと、を含む。

【００３７】

[0037]いくつかの態様では、方法は、メッシュピアデバイスのために提案されるインターネットプロトコル（ＩＰ）アドレスの少なくとも一部分を決定するためにピアリンクオープンメッセージを復号することと、メッシュピアデバイスのために提案されるインターネットプロトコルアドレスの部分に少なくとも部分的に基づいて、メッシュピアデバイスに割り当てるためのインターネットプロトコルアドレスを決定することと、メッシュピアデバイスに割り当てられるインターネットプロトコルアドレスを示すピアリンク確認メッセージを生成することと、ピアリンク確認メッセージをメッシュピアデバイスへ送信することと、を含む。

【００３８】

[0038]いくつかの態様では、方法は、提案されるインターネットプロトコルアドレスが別のデバイスによって使用中であるかどうかを決定することをさらに含み、メッシュピアデバイスに割り当てられるインターネットプロトコルアドレスは、決定に少なくとも部分的に基づく。いくつかの態様では、方法は、メッシュピアデバイスからのサービスディスカバリメッセージを受信することをさらに含み、ピアリンクオープンメッセージがサービスディスカバリメッセージに基づいてメッシュピアデバイスへ送信される。いくつかの態様では、方法は、サービスディスカバリメッセージを受信することがサービス通知メッセージ（a service advertisement message）を受信することを備えることをさらに含む。いくつかの態様では、方法はまた、メッシュピアデバイスがピアリングされる１つまたは複数のデバイスを決定するためにピアリンクオープンメッセージを復号することを含む。

【００３９】

[0039]方法のいくつかの態様は、メッシュピアデバイスのメッシュプロファイルを決定

するためにピアリンクオープンメッセージを復号することと、拡張サポートレート要素（an extended supported rates element）、電力機能要素（a power capability element）、サポートチャネル要素（a supported channels element）、サポート規制クラス要素（a supported regulatory classes element）、高スループット機能要素（a high throughput capabilities element）、高スループット動作要素（a high throughput operations element）、２０／４０基本サービスセット共存要素（a 20/40 basic service set coexistence element）、拡張機能要素（an extended capabilities element）またはインターネットワーク要素（an internetwork element）のうちの１つまたは複数に関する値がメッシュプロファイルの中で規定されているかどうかを決定するためにメッシュプロファイルを復号することと、対応するデフォルト値をメッシュプロファイルの１つまたは複数の規定されていない要素に、決定に基づいて関連付けることと、をさらに含む。

【００４０】

[0040]開示される別の態様は、メッシュピアデバイスとの安全な接続を確立するための装置である。装置は、メッシュピアデバイスからのピアリンクオープンメッセージを受信することと、メッシュピアデバイスに関するピアコミットスカラーを決定するためにピアリンクオープンメッセージを復号することと、メッシュピアデバイスに関するピアコミット要素を決定するためにピアリンクオープンメッセージを復号することと、ピアコミットスカラーおよびピアコミット要素に基づいてセキュリティキー識別子を決定することと、セキュリティキー識別子に基づいてメッシュピアデバイスと通信することと、を行うように構成された処理システムを含む。

【００４１】

[0041]装置のいくつかの態様では、処理システムは、コミットスカラーを生成することと、コミット要素を生成することと、ピアリンクオープンメッセージを送信することと、を行うようにさらに構成され、ピアリンクオープンメッセージはコミットスカラーとコミット要素とを示す。

【００４２】

[0042]装置のいくつかの態様では、セキュリティキー識別子を決定することは、コミットスカラーおよびコミット要素にさらに基づく。いくつかの態様では、処理システムは、ピアリンク確認メッセージを受信することと、ピアリンク確認メッセージはピア確認識別子を示し、ピア確認識別子に基づいてセキュリティキー識別子を検証することと、メッシュピアデバイスと通信するべきかどうかを検証に基づいて決定することと、を行うようにさらに構成される。

【００４３】

[0043]装置のいくつかの態様では、処理システムは、コミットスカラーおよびコミット要素に基づいて確認識別子を生成することと、確認識別子を示すピアリンク確認メッセージを生成することと、ピアリンク確認メッセージをメッシュピアデバイスへ送信することと、を行うようにさらに構成される。いくつかの態様では、処理システムは、メッシュピアデバイスのために提案されるインターネットプロトコル（ＩＰ）アドレスの少なくとも一部分を決定するためにピアリンクオープンメッセージを復号することと、メッシュピアデバイスのために提案されるインターネットプロトコルアドレスの少なくとも一部分に少なくとも部分的に基づいて、メッシュピアデバイスに割り当てるためのインターネットプロトコルアドレスを決定することと、メッシュピアデバイスに割り当てられるインターネットプロトコルアドレスを示すピアリンク確認メッセージを生成することと、ピアリンク確認メッセージをメッシュピアデバイスへ送信することと、を行うようにさらに構成される。

【００４４】

[0044]装置のいくつかの態様では、処理システムは、提案されるインターネットプロトコルアドレスが別のデバイスによって使用中であるかどうかを決定するようにさらに構成され、メッシュピアデバイスに割り当てられるインターネットプロトコルアドレスは、決定に少なくとも部分的に基づく。装置のいくつかの態様では、処理システムは、メッシュ

ピアデバイスからのサービスディスカバリメッセージを受信するようにさらに構成され、ピアリンクオープンメッセージがサービスディスカバリメッセージに基づいてメッシュピアデバイスへ送信される。いくつかの態様では、サービスディスカバリメッセージを受信することは、サービス通知メッセージを受信することを備える。

【００４５】

[0045]装置のいくつかの態様では、処理システムは、メッシュピアデバイスがピアリングされる１つまたは複数のデバイスを決定するためにピアリンクオープンメッセージを復号するようにさらに構成される。装置のいくつかの態様では、処理システムは、メッシュピアデバイスのメッシュプロファイルを決定するためにピアリンクオープンメッセージを復号することと、拡張サポートレート要素、電力機能要素、サポートチャネル要素、サポート規制クラス要素、高スループット機能要素、高スループット動作要素、２０／４０基本サービスセット共存要素、拡張機能要素またはインターネットワーク要素のうちの１つまたは複数に関する値がメッシュプロファイルの中で規定されているかどうかを決定するためにメッシュプロファイルを復号することと、対応するデフォルト値をメッシュプロファイルの１つまたは複数の規定されていない要素に、決定に基づいて関連付けることと、を行うようにさらに構成される。

【００４６】

[0046]開示される別の態様は、メッシュピアデバイスとの安全な接続を確立するための装置である。装置は、メッシュピアデバイスからのピアリンクオープンメッセージを受信するための手段と、メッシュピアデバイスに関するピアコミットスカラーを決定するためにピアリンクオープンメッセージを復号するための手段と、メッシュピアデバイスに関するピアコミット要素を決定するためにピアリンクオープンメッセージを復号するための手段と、ピアコミットスカラーおよびピアコミット要素に基づいてセキュリティキー識別子を決定するための手段と、セキュリティキー識別子に基づいてメッシュピアデバイスと通信するための手段と、を含む。

【００４７】

[0047]いくつかの態様では、装置は、コミットスカラーを生成するための手段と、コミット要素を生成するための手段と、ピアリンクオープンメッセージを送信するための手段と、をさらに含み、ピアリンクオープンメッセージはコミットスカラーとコミット要素とを示す。

【００４８】

[0048]いくつかの態様では、セキュリティキー識別子を決定することは、コミットスカラーおよびコミット要素にさらに基づく。いくつかの態様では、装置は、ピアリンク確認メッセージを受信するための手段と、ピアリンク確認メッセージはピア確認識別子を示し、ピア確認識別子に基づいてセキュリティキー識別子を検証するための手段と、メッシュピアデバイスと通信するべきかどうかを検証に基づいて決定するための手段と、をさらに含む。

【００４９】

[0049]いくつかの態様では、装置は、コミットスカラーおよびコミット要素に基づいて確認識別子を生成するための手段と、確認識別子を示すピアリンク確認メッセージを生成するための手段と、ピアリンク確認メッセージをメッシュピアデバイスへ送信するための手段と、をさらに含む。いくつかの態様では、装置は、メッシュピアデバイスのために提案されるインターネットプロトコル（ＩＰ）アドレスの少なくとも一部分を決定するためにピアリンクオープンメッセージを復号するための手段と、メッシュピアデバイスのために提案されるインターネットプロトコルアドレスの少なくとも一部分に少なくとも部分的に基づいて、メッシュピアデバイスに割り当てるためのインターネットプロトコルアドレスを決定するための手段と、メッシュピアデバイスに割り当てられるインターネットプロトコルアドレスを示すピアリンク確認メッセージを生成するための手段と、ピアリンク確認メッセージをメッシュピアデバイスへ送信するための手段と、をさらに含む。

【００５０】

[0050]いくつかの態様では、装置は、提案されるインターネットプロトコルアドレスが別のデバイスによって使用中であるかどうかを決定するための手段をさらに含み、メッシュピアデバイスに割り当てられるインターネットプロトコルアドレスは、決定に少なくとも部分的に基づく。

【００５１】

[0051]いくつかの態様では、装置は、メッシュピアデバイスからのサービスディスカバリメッセージを受信するための手段をさらに含み、ピアリンクオープンメッセージがサービスディスカバリメッセージに基づいてメッシュピアデバイスへ送信される。いくつかの態様では、サービスディスカバリメッセージを受信することは、サービス通知メッセージを受信することを備える。いくつかの態様では、装置は、メッシュピアデバイスがピアリングされる１つまたは複数のデバイスを決定するためにピアリンクオープンメッセージを復号するための手段をさらに含む。

【００５２】

[0052]いくつかの態様では、装置は、メッシュピアデバイスのメッシュプロファイルを決定するためにピアリンクオープンメッセージを復号するための手段と、拡張サポートレート要素、電力機能要素、サポートチャネル要素、サポート規制クラス要素、高スループット機能要素、高スループット動作要素、２０／４０基本サービスセット共存要素、拡張機能要素またはインターネットワーク要素のうちの１つまたは複数に関する値がメッシュプロファイルの中で規定されているかどうかを決定するためにメッシュプロファイルを復号するための手段と、対応するデフォルト値をメッシュプロファイルの１つまたは複数の規定されていない要素に、決定に基づいて関連付けるための手段と、をさらに含む。

【００５３】

[0053]開示される別の態様は、実行されたとき、メッシュピアデバイスとの安全な接続を確立する方法を処理システムに実行させる命令を備えるコンピュータ可読記憶媒体である。方法は、含み、方法は、メッシュピアデバイスからのピアリンクオープンメッセージを受信することと、メッシュピアデバイスに関するピアコミットスカラーを決定するためにピアリンクオープンメッセージを復号することと、メッシュピアデバイスに関するピアコミット要素を決定するためにピアリンクオープンメッセージを復号することと、ピアコミットスカラーおよびピアコミット要素に基づいてセキュリティキー識別子を決定することと、セキュリティキー識別子に基づいてメッシュピアデバイスと通信することと、を含む。

【００５４】

[0054]いくつかの態様では、方法は、コミットスカラーを生成することと、コミット要素を生成することと、ピアリンクオープンメッセージを送信することと、をさらに含み、ピアリンクオープンメッセージはコミットスカラーとコミット要素とを示す。いくつかの態様では、セキュリティキー識別子を決定することは、コミットスカラーおよびコミット要素にさらに基づく。

【００５５】

[0055]いくつかの態様では、方法は、ピアリンク確認メッセージを受信することと、ピアリンク確認メッセージはピア確認識別子を示し、ピア確認識別子に基づいてセキュリティキー識別子を検証することと、メッシュピアデバイスと通信するべきかどうかを検証に基づいて決定することと、を含む。

【００５６】

[0056]いくつかの態様では、方法は、コミットスカラーおよびコミット要素に基づいて確認識別子を生成することと、確認識別子を示すピアリンク確認メッセージを生成することと、ピアリンク確認メッセージをメッシュピアデバイスへ送信することと、を含む。

【００５７】

[0057]いくつかの態様では、方法は、メッシュピアデバイスのために提案されるインターネットプロトコル（ＩＰ）アドレスの少なくとも一部分を決定するためにピアリンクオープンメッセージを復号することと、メッシュピアデバイスのために提案されるインター

ネットプロトコルアドレスの部分に少なくとも部分的に基づいて、メッシュピアデバイスに割り当てるためのインターネットプロトコルアドレスを決定することと、メッシュピアデバイスに割り当てられるインターネットプロトコルアドレスを示すピアリンク確認メッセージを生成することと、ピアリンク確認メッセージをメッシュピアデバイスへ送信することと、を含む。

【００５８】

[0058]いくつかの態様では、方法は、提案されるインターネットプロトコルアドレスが別のデバイスによって使用中であるかどうかを決定することをさらに含み、メッシュピアデバイスに割り当てられるインターネットプロトコルアドレスは、決定に少なくとも部分的に基づく。いくつかの態様では、方法は、メッシュピアデバイスからのサービスディスカバリメッセージを受信することをさらに含み、ピアリンクオープンメッセージがサービスディスカバリメッセージに基づいてメッシュピアデバイスへ送信される。いくつかの態様では、方法は、サービスディスカバリメッセージを受信することがサービス通知メッセージを受信することを備えることをさらに含む。いくつかの態様では、方法はまた、メッシュピアデバイスがピアリングされる１つまたは複数のデバイスを決定するためにピアリンクオープンメッセージを復号することを含む。

【００５９】

[0059]方法のいくつかの態様は、メッシュピアデバイスのメッシュプロファイルを決定するためにピアリンクオープンメッセージを復号することと、拡張サポートレート要素、電力機能要素、サポートチャネル要素、サポート規制クラス要素、高スループット機能要素、高スループット動作要素、２０／４０基本サービスセット共存要素、拡張機能要素またはインターネットワーク要素のうちの１つまたは複数に関する値がメッシュプロファイルの中で規定されているかどうかを決定するためにメッシュプロファイルを復号することと、対応するデフォルト値をメッシュプロファイルの１つまたは複数の規定されていない要素に、決定に基づいて関連付けることと、をさらに含む。

【図面の簡単な説明】

【００６０】

【図１】[0060]近隣認識ネットワーク（ＮＡＮ）の一例を示す図。

【図２】[0061]図１のモバイルデバイスのうちの１つまたは複数のワイヤレスデバイスの例示的な実施形態を示す図。

【図３】[0062]ＮＡＮネットワークを介するメッシュピアリングプロセスのメッセージフロー図。

【図４】[0063]管理フレームに関する例示的なメッセージフォーマットを示す図。

【図５】[0064]図４のタイプフィールドおよびサブタイプフィールドに関する値の様々な例示的な組合せを示す表。

【図６Ａ】[0065]認証メッセージに関する例示的なメッセージ本文を示す図。

【図６Ｂ】[0066]ＩＰアドレスリクエスト情報要素の例示的なフォーマットを示す図。

【図６Ｃ】[0067]ＩＰアドレスデータフィールドの例示的なフォーマットを示す図。

【図６Ｄ】[0068]ＩＰアドレスリクエスト制御フィールドの一例を示す図。

【図６Ｅ】[0069]高レベルプロトコル（ＨＬＰ：High Level Protocol）コンテナ要素の例示的なフォーマットを示す図。

【図７Ａ】[0070]関連付けリクエストメッセージの例示的なメッセージ本文を示す図。

【図７Ｂ】[0071]ＦＩＬＳキー確認要素の１つの例示的なフォーマットを示す図。

【図８】[0072]例示的なＩＰアドレス割当て情報要素を示す図。

【図９】[0073]関連付けレスポンスメッセージの例示的なメッセージ本文を示す図。

【図１０】[0074]図１の近隣認識ネットワーク上でのメッシュピアデバイスとの効率のよいメッシュピアリングのための方法の一例を示す図。

【図１１】[0075]図１の近隣認識ネットワーク上でのメッシュピアデバイスとの効率のよいメッシュピアリングのための方法の一例を示す図。

【図１２】[0076]図１の近隣認識ネットワーク上でのメッシュピアデバイスとの効率のよ

いメッシュピアリングのための方法の一例を示す図。
【発明を実施するための形態】
【００６１】
[0077]添付の図面を参照しながら、新規のシステム、装置、および方法の様々な態様が以下でより十分に説明される。ただし、本開示は、多くの異なる形態で実施され得、本開示全体にわたって提示される特定の構造または機能に限定されるものと解釈されるべきではない。そうではなく、これらの態様は、本開示が十分なものであり、完全であるように、また本開示の範囲を当業者に十分伝えるように提供される。本明細書の教示に基づいて、本開示の範囲は、本発明の任意の他の態様とは無関係に実装されるか、本発明の任意の他の態様と組み合わされるかにかかわらず、本明細書で開示される新規のシステム、装置、および方法の任意の態様を包含することが意図されることを、当業者は理解されたい。たとえば、本明細書で示される任意の数の態様を使用して、装置が実装されてよく、または、方法が実践されてよい。加えて、本発明の範囲は、本明細書に記載される本発明の様々な態様に加えて、またはそれ以外の、他の構造、機能、または構造および機能を使用して実践されるような装置または方法を包含することが意図される。本明細書で開示されるいずれの態様も、請求項の１つまたは複数の要素によって具現化され得ることを理解されたい。
【００６２】
[0078]特定の態様が本明細書で説明されるが、これらの態様の多数の変形および置換が、本開示の範囲に入る。好ましい態様のいくつかの利益および利点が述べられるが、本開示の範囲は特定の利益、使用、または目的に限定されるものではない。むしろ、本開示の態様は、異なるワイヤレス技術、システム構成、ネットワーク、および伝送プロトコルに広く適用可能なものであることが意図され、そのうちのいくつかが図面および好ましい態様の以下の説明において例として示される。詳細な説明および図面は、限定的ではなく、本開示の例示にすぎず、本開示の範囲は、添付の特許請求の範囲およびその均等物によって定義される。
【００６３】
[0079]普及している（popular）ワイヤレスネットワーク技術は、様々なタイプのワイヤレスローカルエリアネットワーク（ＷＬＡＮ）を含み得る。ＷＬＡＮは、広く使用されているネットワーキングプロトコルを採用して、近くのデバイスを一緒に相互接続するために使用され得る。本明細書で説明される様々な態様は、ワイヤレスプロトコルなどの任意の通信規格に適用され得る。
【００６４】
[0080]いくつかの態様では、サブギガヘルツ帯域内のワイヤレス信号は、直交周波数分割多重（ＯＦＤＭ）、直接シーケンス拡散スペクトル（ＤＳＳＳ）通信、ＯＦＤＭ通信とＤＳＳＳ通信との組合せ、または他の方式を使用して、８０２．１１ａｈプロトコルまたは８０２．１１ａｃプロトコルに従って送信され得る。８０２．１１ａｈプロトコルまたは８０２．１１ａｃプロトコルの実装は、センサー、計測（metering）、およびスマートグリッドネットワークに使用され得る。有利なことに、８０２．１１ａｈプロトコルまたは８０２．１１ａｃプロトコルを実装するいくつかのデバイスの態様は、他のワイヤレスプロトコルを実装するデバイスよりも少ない電力を消費する場合があり、および／または、比較的長い距離、たとえば、約１キロメートル以上にわたってワイヤレス信号を送信するために使用され得る。
【００６５】
[0081]いくつかの実装形態では、ＷＬＡＮは、ワイヤレスネットワークにアクセスする構成要素である様々なデバイスを含む。たとえば、２つのタイプのデバイス、すなわちアクセスポイント（「ＡＰ」）およびクライアント（ステーションまたは「ＳＴＡ」とも呼ばれる）があり得る。一般に、ＡＰはＷＬＡＮのためのハブまたは基地局として働き得、ＳＴＡはＷＬＡＮのユーザとして働く。たとえば、ＳＴＡはラップトップコンピュータ、携帯情報端末（ＰＤＡ）、携帯電話などであり得る。一例では、ＳＴＡは、インターネッ

トまたは他のワイドエリアネットワークへの一般的接続性を取得するために、ＷｉＦｉ（登録商標）（たとえば、８０２．１１ａｈまたは８０２．１１ａｃなどのＩＥＥＥ８０２．１１プロトコル）準拠ワイヤレスリンクを介してＡＰに接続する。いくつかの実装形態では、ＳＴＡはまた、ＡＰとして使用され得る。

【００６６】

[0082]アクセスポイント（「ＡＰ」）はまた、ノードＢ、無線ネットワークコントローラ（「ＲＮＣ」）、ｅノードＢ、基地局コントローラ（「ＢＳＣ」）、トランシーバ基地局（「ＢＴＳ」）、基地局（「ＢＳ」）、トランシーバ機能（「ＴＦ」）、無線ルータ、無線トランシーバ、またはいくつかの他の用語を備えるか、それらのいずれかとして実装されるか、またはそれらのいずれかとして知られる場合がある。

【００６７】

[0083]ステーション「ＳＴＡ」はまた、アクセス端末（「ＡＴ」）、加入者局、加入者ユニット、移動局、リモート局、リモート端末、ユーザ端末、ユーザエージェント、ユーザデバイス、ユーザ機器、またはいくつかの他の用語を備えるか、それらのいずれかとして実装されるか、またはそれらのいずれかとして知られる場合がある。いくつかの実装形態では、アクセス端末は、セルラー電話、コードレス電話、セッション開始プロトコル（「ＳＩＰ」）電話、ワイヤレスローカルループ（「ＷＬＬ」）局、携帯情報端末（「ＰＤＡ」）、ワイヤレス接続機能を有するハンドヘルドデバイス、またはワイヤレスモデムに接続されたいくつかの他の適切な処理デバイスを備える場合がある。したがって、本明細書で教示される１つまたは複数の態様は、電話（たとえば、セルラーフォンまたはスマートフォン）、コンピュータ（たとえば、ラップトップ）、ポータブル通信デバイス、ヘッドセット、ポータブルコンピューティングデバイス（たとえば、携帯データ端末）、エンターテインメントデバイス（たとえば、音楽デバイスもしくはビデオデバイス、または衛星ラジオ）、ゲームデバイスもしくはゲームシステム、全地球測位システムデバイス、または、ワイヤレス媒体を介して通信するように構成された任意の他の適切なデバイスに組み込まれ得る。

【００６８】

[0084]図１を参照すると、ワイヤレスネットワークの特定の例示的な実施形態が示され、概して１００と指定される。いくつかの態様では、ワイヤレスネットワーク１００は、近隣認識ネットワークすなわちＮＡＮである。ＮＡＮは、本開示ではアドホックネットワークと呼ばれることもある。図１は、デバイス１３０ｂを除くすべてのワイヤレスデバイス１３０ａ～ｌが、ワイヤレスネットワーク１００に参加していることを示す。たとえば、デバイス１３０ａおよび１３０ｃ～ｌの各々は、ビーコンまたは他の時間同期情報をワイヤレスネットワーク１００から受信する。一態様では、ワイヤレスデバイス１３０ａおよび１３０ｃ～ｌのうちの１つは、ワイヤレスネットワーク１００のための「ルート」ノードとして指定されてよく、したがって、他のデバイス１３０ａおよび１３０ｃ～ｌの各々によって受信される同期メッセージを周期的に送信する。いくつかの態様では、ワイヤレスネットワーク１００上で行われる通信の一部分は、標準的な通信チャネル、たとえば、いくつかの態様ではチャネル６の上で実行され得る。いくつかの態様では、ワイヤレスデバイス１３０ａおよび１３０ｃ～ｌのうちの１つまたは複数は、ステーションとみなされてよい。

【００６９】

[0085]ワイヤレスネットワーク１００はまた、４つのサービスメッシュネットワーク１１０ａ～１１０ｄを含む。サービスメッシュネットワーク１１０ａ～１１０ｄの各々は、ワイヤレスデバイス１３０ａおよび１３０ｃ～ｋの一部分を含むように示される。サービスメッシュネットワーク１１０ａは、ワイヤレスデバイス１３０ａおよび１３０ｃを含む。サービスメッシュネットワーク１１０ｂは、ワイヤレスデバイス１３０ｃ～ｇを含む。サービスメッシュネットワーク１１０ｃは、ワイヤレスデバイス１３０ｆ～ｉを含む。サービスメッシュネットワーク１１０ｄは、ワイヤレスデバイス１３０ｉ～ｋを含む。ワイヤレスデバイス１３０ｂは、サービスメッシュネットワーク１１０ａ～ｄのいずれにも含

まれない。本明細書で開示される方法、システムおよびコンピュータ可読媒体を使用すると、非メンバーデバイス１３０ｂは、図１に示すネットワークのうちの１つまたは複数のメンバーになり得る。たとえば、デバイス１３０ｂは、サービスメッシュネットワーク１１０ａのメンバーになり得る。

【００７０】

[0086]各サービスメッシュネットワーク１１０ａ～ｄは、サービスメッシュネットワークの他のメンバーにサービスを提供するためのサービス提供デバイスによって利用され得る。たとえば、ワイヤレスデバイス１３０ａは、一例では、音楽サービスをワイヤレスデバイス１３０ｂ～ｃに提供する、メッシュ１１０ａのためのサービス提供デバイスであり得る。モバイルデバイス１３０ａは、サービスメッシュネットワーク１１０ａ上に提供されているサービスを、ワイヤレスネットワーク１００上のデバイスに通知し（advertise）得る。たとえば、モバイルデバイス１３０ａ（すなわち、ワイヤレスネットワーク１００上の他のサービス提供デバイス）は、提供され得るサービスとそのサービスの取得に関連した１つまたは複数のパラメータとを示すメッセージを、ワイヤレスネットワーク１００を介してブロードキャストまたはマルチキャストし得る。加えて、ワイヤレスネットワーク１００上のサービス提供デバイスは、上述されたようなワイヤレスネットワーク１００から受信されるサービスディスカバリリクエストに応答し得る。たとえば、サービス提供デバイス１３０ａは、サービスメッシュネットワーク１１０ａ上に提供されているサービスを示す情報を含むディスカバリレスポンスを送信し得る。

【００７１】

[0087]同様に、サービスメッシュネットワーク１１０ｂ～ｄの各々はまた、上記で提供されたデバイス１３０ａの例と同様に動作し得るサービス提供デバイスを含む。たとえば，モバイルデバイス１３０ｄは、ビデオゲームサービスをモバイルデバイス１３０ｃ、１３０ｅ、１３０ｆ、および１３０ｇに提供する、サービスメッシュネットワーク１１０ｂのためのサービス提供デバイスであり得る。モバイルデバイス１３０ｈは、ピクチャ共有サービスをモバイルデバイス１３０ｆ、１３０ｇ、および１３０ｉに提供することによって、サービスメッシュネットワーク１１０ｃのためのサービス提供デバイスであり得る。同様に、モバイルデバイス１１０ｊは、サービスメッシュネットワーク１１０ｄを介するビデオサービスを、モバイルデバイス１３０ｉおよび１３０ｋに提供し得る。

【００７２】

[0088]モバイルデバイスは、同時に２つ以上のサービスメッシュネットワークのメンバーであり得、したがって、それぞれのサービスメッシュネットワークのサービス提供デバイスの各々によって提供されるサービスを受けることがある。たとえば、モバイルデバイス１３０ｃは、サービスメッシュネットワーク１１０ａと１１０ｂの両方のメンバーとして示される。したがって、モバイルデバイス１３０ｃは、モバイルデバイス１３０ａによって提供される音楽サービスと、モバイルデバイス１３０ｄによって提供される画像サービスとを、同時に受けていることがある。同様に、モバイルデバイス１３０ｆ～ｇはサービスメッシュネットワーク１１０ｂおよび１１０ｃに参加し、モバイルデバイス１３０ｉはサービスメッシュネットワーク１１０ｃと１１０ｄの両方に参加する。

【００７３】

[0089]図２は、図１のワイヤレスネットワーク１００内で採用され得るワイヤレスデバイス２０２の例示的な機能ブロック図を示す。ワイヤレスデバイス２０２は、本明細書で説明される様々な方法を実施するように構成され得るデバイスの一例である。たとえば、ワイヤレスデバイス２０２は、ステーション１３０ａ～ｌのうちの１つを備え得る。

【００７４】

[0090]ワイヤレスデバイス２０２は、ワイヤレスデバイス２０２の動作を制御するプロセッサ２０４を含み得る。プロセッサ２０４は、中央処理装置（ＣＰＵ）と呼ばれることもある。読取り専用メモリ（ＲＯＭ）とランダムアクセスメモリ（ＲＡＭ）の両方を含み得るメモリ２０６は、命令とデータとをプロセッサ２０４に提供し得る。メモリ２０６の一部分はまた、不揮発性ランダムアクセスメモリ（ＮＶＲＡＭ）を含み得る。プロセッサ

２０４は、通常、メモリ２０６内に記憶されたプログラム命令に基づいて論理演算と算術演算とを実行する。メモリ２０６の中の命令は、本明細書で説明される方法を実施するように実行可能であり得る。

【００７５】

[0091]プロセッサ２０４は、１つまたは複数のプロセッサとともに実装された処理システムを備え得るか、またはその構成要素であり得る。１つまたは複数のプロセッサは、汎用マイクロプロセッサ、マイクロコントローラ、デジタル信号プロセッサ（ＤＳＰ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）、プログラマブル論理デバイス（ＰＬＤ）、コントローラ、状態機械、ゲート論理、個別ハードウェア構成要素、専用ハードウェア有限状態機械、または情報の計算もしくは他の操作を実行することができる任意の他の適切なエンティティの任意の組合せにより実装され得る。

【００７６】

[0092]処理システムはまた、ソフトウェアを記憶するための機械可読媒体を含み得る。ソフトウェアは、ソフトウェア、ファームウェア、ミドルウェア、マイクロコード、ハードウェア記述言語と呼ばれるか、またはそれ以外の名称で呼ばれるかにかかわらず、任意のタイプの命令を意味すると広く解釈されるものとする。命令は、（たとえば、ソースコードフォーマット、バイナリコードフォーマット、実行可能コードフォーマット、または任意の他の適切なコードのフォーマットの）コードを含み得る。命令は、１つまたは複数のプロセッサによって実行されたとき、処理システムに、本明細書で説明される様々な機能を実行させる。

【００７７】

[0093]ワイヤレスデバイス２０２はまた、ワイヤレスデバイス２０２と遠隔ロケーションとの間のデータの送信と受信とを可能にするために、送信機２１０および／または受信機２１２を含み得るハウジング２０８を含んでよい。送信機２１０および受信機２１２は、トランシーバ２１４へ組み合わされてよい。アンテナ２１６は、ハウジング２０８に取り付けられてよく、トランシーバ２１４に電気的に結合され得る。ワイヤレスデバイス２０２はまた、複数の送信機、複数の受信機、複数のトランシーバ、および／または複数のアンテナを含み得る（図示せず）。

【００７８】

[0094]ワイヤレスデバイス２０２はまた、トランシーバ２１４によって受信される信号のレベルを検出し定量化するために使用され得る、信号検出器２１８を含み得る。信号検出器２１８は、総エネルギー、シンボルごとのサブキャリア当たりのエネルギー、電力スペクトル密度、および他の信号などの信号を検出し得る。ワイヤレスデバイス２０２はまた、信号を処理する際に使用するためのデジタル信号プロセッサ（ＤＳＰ）２２０を含み得る。ＤＳＰ２２０は、送信のためのパケットを生成するように構成され得る。いくつかの態様では、パケットは、物理層データユニット（ＰＰＤＵ）を備え得る。

【００７９】

[0095]いくつかの態様では、ワイヤレスデバイス２０２は、ユーザインターフェース２２２をさらに備え得る。ユーザインターフェース２２２は、キーパッド、マイクロフォン、スピーカー、および／またはディスプレイを備え得る。ユーザインターフェース２２２は、ワイヤレスデバイス２０２のユーザに情報を伝え、および／またはユーザからの入力を受け取る、任意の要素または構成要素を含み得る。

【００８０】

[0096]ワイヤレスデバイス２０２の様々な構成要素は、バスシステム２２６によって一緒に結合され得る。バスシステム２２６は、たとえば、データバス、ならびに、データバスに加えて電力バス、制御信号バス、およびステータス信号バスを含み得る。ワイヤレスデバイス２０２の構成要素が、いくつかの他の機構を使用して、互いに結合されるか、または互いに入力を受け付けもしくは与え得ることを当業者は諒解されよう。

【００８１】

[0097]いくつかの別個の構成要素が図２に示されるが、構成要素のうちの１つまたは複

数が組み合わされてよく、または共通に実装されてよいことを当業者は認識されよう。たとえば、プロセッサ２０４は、プロセッサ２０４に関して上述された機能を実装するためだけでなく、信号検出器２１８および／またはＤＳＰ２２０に関して上述された機能を実装するためにも使用され得る。さらに、図２に示される構成要素の各々は、複数の別個の要素を使用して実装され得る。

【００８２】

[0098]ワイヤレスデバイス２０２は、ワイヤレスデバイス１３０ａ～ｌのいずれかを備えてよく、通信を送信および／または受信するために使用されてよい。すなわち、ワイヤレスデバイス１３０ａ～ｌのいずれかは、送信機デバイスまたは受信機デバイスとして働き得る。いくつかの態様は、送信機または受信機の存在を検出するために、メモリ２０６およびプロセッサ２０４上で動作しているソフトウェアによって信号検出器２１８が使用されることを企図する。

【００８３】

[0099]上述されたように、ワイヤレスデバイス２０２などのワイヤレスデバイスは、ワイヤレス通信システム１００などのワイヤレス通信システム内でサービスを提供するように構成され得る。たとえば、ワイヤレスデバイス２０２は、データ（たとえば、センサー測定値、ロケーション座標など）を取り込み、または計算するために使用されるハードウェア（たとえば、センサー、全地球測位システム（ＧＰＳ）など）を含み得る。

【００８４】

[00100]開示される方法およびシステムは、知られている方法およびシステムと比較されるとき、メッシュ通信の改善された効率をもたらす。たとえば、開示された方法およびシステムは、４つのメッセージの交換を用いて２つのメッシュデバイス間で確立されるべき安全なメッシュ通信を提供し得る。いくつかの態様では、メッシュ通信で使用するためのＩＰアドレスの交渉も、２つのメッシュピアデバイス間でのメッシュ通信の確立とともに、合計４つのメッセージの交換を用いて確立され得る。いくつかの態様では、これらの２つの機能は、ＩＰアドレスの交渉／割当ておよび安全なメッシュ通信が４つのメッセージの交換を用いて２つのメッシュピアデバイス間で確立されるように組み合わされる。このことは、メッシュに参加しているデバイスでの低減された計算オーバーヘッドとともに、メッシュ通信の確立でのより小さいレイテンシ（latency）をもたらし得る。

【００８５】

[00101]本開示は、統合された認証および関連付けプロセスを提供する方法およびシステムを対象とする。この統合されたプロセスは、メッシュメンバーデバイスと非メンバーデバイスとの間の４ウェイメッセージ交換を使用するメッシュ関連付けを提供する。これらの方法およびシステムにおいて共通グループキーを使用することは、任意のメッシュメンバーデバイスへ送信され、および／または任意のメッシュメンバーデバイスから受信される、グループアドレス指定されたメッシュメッセージの暗号化および暗号解読を容易にする。いくつかの態様はまた、共通グループキーを使用してユニキャストパケットを暗号化および／または暗号解読し得る。

【００８６】

[00102]これらの開示される方法およびシステムは、各メッシュメンバーデバイスの送信のために別個のグループキーを利用する知られている方法およびシステムと比較されるとき、メッシュ通信を大幅に簡易化する。

【００８７】

[00103]図３を参照すると、ＮＡＮネットワークを介するメッシュピアリングプロセスのメッセージフロー図が示され、概して、１０００と指定される。図３は、１つの例示的な実施形態においてメッシュピアリングプロセスを実行する３つのデバイス１３０ａ～ｃを示す。示されているメッセージフローが開始する前、デバイス１３０ａおよび１３０ｃは、すでにメッシュネットワークのメンバーである。上記で説明したように、メッシュネットワークは、メッシュのメンバーデバイス間で交換される、グループアドレス指定されたメッセージを暗号化および／または暗号解読するために、共通グループキーを利用する

。

【００８８】

[00104]デバイス１３０ａ～ｃは、それらの間での安全な通信を容易にする共通パスワードを共有し得る。いくつかの態様では、共通パスワードは、デバイス１３０ａ～ｃの各々の入力インターフェースを介して独立に入力されてよい。いくつかの態様では、デバイス１３０ａ～ｃのうちの１つまたは複数は、共通パスワードを使用してパスワード要素（Ｐ）を作成してよい。いくつかの態様では、ＳＴＡ１０６ａ～ｃの間での通信のために使用されるパスワード要素（Ｐ）は、ＳＡＥ認証で使用されるものと同じ方式で決定されてよい。

【００８９】

[00105]デバイス１３０ａ～ｃの各々のうちの１つまたは複数はまた、２つのナンスを（いくつかの態様では、ランダムに）決定してよい。たとえば、デバイス１３０ｂは、$N_{b1}$と$N_{b2}$とを作成してよい。デバイス１３０ａ～ｃのうちの１つまたは複数は、いくつかの態様では、それらのそれぞれ生成されたナンス値のうちの少なくとも１つに基づいて、ディフィーヘルマン（ＤＨ：Diffie-Hellman）公開値（public value）を生成してよい。たとえば、デバイス１３０ｂは、パスワード要素と$N_{b1}$とを使用して公開値$P^{nb1}$を生成し得る。

【００９０】

[00106]示されている態様では、デバイス１３０ｂは、認証リクエストメッセージ１００５をデバイス１３０ａへ送信する。認証リクエストメッセージ１００５は、$P^{nb1}$値と$N_{b2}$とを含む。認証リクエストメッセージ１００５はまた、デバイス１３０ｂがデバイス１３０ａとのメッシュ通信で使用するために提案されるＩＰアドレス（または、それの一部分）を含み得る。認証リクエスト１００５は、近隣認識ネットワーク（ＮＡＮ）上で通知されるようなページングウィンドウ（ＰＷ：paging window）の間に送信され得る。いくつかの態様では、認証リクエストメッセージは、いくつかの特性を８０２．１１ａｉの高速初期リンクセットアップ認証リクエストフレームと共有し得る。

【００９１】

[00107]デバイス１３０ａは、デバイス１３０ｂと類似のプロセスを実行し得る。デバイス１３０ａは、２つのナンス、$N_{a1}$と$N_{a2}$とを作成してよい。デバイス１３０ａがデバイス１３０ｂと同じパスワードを知っているので、
デバイス１３０ｂも共有のパスワードに基づいてパスワード要素を作成する。パスワード要素およびナンス$N_{a1}$は、いくつかの態様では、ディフィーヘルマン（ＤＨ）公開値、$P^{na1}$を作成するために使用される。認証リクエスト１００５をデバイス１３０ｂから受信すると、デバイス１３０ａは、$P^{na1}$と$N_{a2}$とをデバイス１３０ｂへ認証返答メッセージ１０１０の中で送信する。認証返答メッセージ１０１０はまた、デバイス１３０ｂとの通信の間にデバイス１３０ａによって使用するために提案されるＩＰアドレスを含み得る。いくつかの態様では、認証返答メッセージ１０１０は、特定の特性を８０２．１１ａｉの高速初期リンクセットアップ（ＦＩＬＳ）認証レスポンスフレームと共有し得る。

【００９２】

[00109]メッセージ１００５および１０１０がそれぞれデバイス１３０ａおよび１３０ｂの各々によって受信された後、２つのデバイス１３０ａ～ｂの各々は、ペアワイズマスターキー（ＰＭＫ）を生成し得る。ペアワイズマスターキーは、いくつかの態様では、ＳＡＥ認証によって規定されるものと同様の方式で生成され得る。

【００９３】

[00110]ＰＭＫがデバイス１３０ｂによって生成された後、ペアワイズ一時キー（ＰＴＫ）がＰＭＫに基づいて生成される。いくつかの態様では、ＰＴＫは、ＰＭＫ、$N_{a2}$および$N_{b2}$に基づく。いくつかの態様では、ＰＴＫは、８０２．１１ａｉ認証で使用される方法に実質的に従って生成される。

【００９４】

[00111]ＳＴＡ１０６ｂは、ＰＴＫに基づいてメッセージ完全性コード（ＭＩＣ）を作

成し得る。ＳＴＡ１０６ｂは、次いで、関連付けリクエストメッセージ１０１５をＳＴＡ１０６ａへ送信する。関連付けリクエストは、ＭＩＣを含む。ＳＴＡ１０６ｂはまた、関連付け識別子（ＡＩＤ：association identifier）をＳＴＡ１０６ａに割り当て得、ＡＩＤを関連付けリクエストメッセージ１０１５の中に含め得る。いくつかの態様では、関連付けリクエストメッセージ１０１５は、デバイス１０６ｂとのメッシュ通信のためにデバイス１０６ｂによってデバイス１０６ａに割り当てられたＩＰアドレスを含み得る。いくつかの態様では、関連付けリクエストメッセージ１０１５は、８０２．１１ａｉプロトコルの高速初期リンクセットアップ（ＦＩＬＳ）関連付けリクエストフレームの１つまたは複数の特性を共有する。たとえば、リクエストメッセージ１０１５は、上記で説明したメッセージ完全性コードとＩＰアドレスとを含むように修正されたＦＩＬＳ関連付けリクエストフレームであり得る。いくつかの態様では、デバイス１３０ｂは、それのＰＨＹおよび／またはＭＡＣ機能を関連付けリクエストメッセージ１０１５の中に含める。

【００９５】

[00112]関連付けリクエストメッセージ１０１５を受信すると、デバイス１３０ａはまた、第２のメッセージ完全性コード（ＭＩＣ）を作成し得、それ自体の第２の関連付け識別子（ＡＩＤ）をデバイス１３０ｂに割り当て得る。デバイス１３０ａは、それのＰＨＹおよび／またはＭＡＣ機能を関連付けレスポンスメッセージ１０２０の中に含め得る。

【００９６】

[00113]デバイス１３０ａがすでにメッシュネットワークのメンバーであるので、デバイス１３０ａはまた、メッシュに関する共通グループキーを関連付けレスポンスメッセージ１０２０の中に含める。この共通グループキーは、メッシュネットワークを介して交換される、グループアドレス指定されたメッセージを暗号化および／または暗号解読するために、デバイス１３０ｂによって使用され得る。デバイス１３０ａは、次いで、第２のＡＩＤと第２のＭＩＣとを含む関連付けレスポンスメッセージ１０２０をデバイス１３０ｂへ送信する。関連付けレスポンスメッセージ１０２０は、高速初期リンクセットアップ（ＦＩＬＳ）関連付けレスポンスメッセージの１つまたは複数の特性を共有し得る。たとえば、関連付けレスポンスメッセージ１０２０は、上記で説明したようなＭＩＣ、ＡＩＤ、およびグループキーを含めるために必要な修正を伴うＦＩＬＳ関連付けレスポンスメッセージであり得る。

【００９７】

[00114]メッセージ１０２０の中の共通グループキーを受信すると、デバイス１３０ｂは、今やメッシュネットワーク上のデバイス間で交換される、グループアドレス指定されたメッセージを暗号化および／または暗号解読することが可能であり得る。したがって、デバイス１３０ｂは、メッシュネットワークのメンバーデバイスになる。このことは、それがメンバーデバイスになったときにデバイス１３０ｂを１３０ｂ’として示すことによって、図３に示される。たとえば、デバイス１３０ｂは、パスリクエストメッセージ１０２５を暗号化するためにメッセージ１０２０からの共通グループキーを利用するメッシュネットワークを介して、パスリクエストメッセージ１０２５を送信（ユニキャストまたはブロードキャスト）し得る。いくつかの態様では、パスリクエストメッセージは、ハイブリッドワイヤレスメッシュプロトコル（ＨＷＭＰ：Hybrid Wireless Mesh Protocol）の一部であるパスリクエスト（ＰＲＥＱ：path request）メッセージであり得る。パスリクエストメッセージ１０２５は、シーケンス番号フィールドを含み得、シーケンス番号フィールドの中の値は、受信された任意のパスレスポンスメッセージをデバイス１３０ｂがパスリクエストメッセージに関連付けることを可能にし得る。パスリクエストメッセージは、デバイス１３０ｂによって関連付けレスポンスメッセージ１０２０の中で受信された共通グループキーを使用して、デバイス１３０ｂによって暗号化され得る。

【００９８】

[00115]パスリクエストメッセージ１０２５は、デバイス１３０ｃによって受信され得、デバイス１３０ｃもメッシュネットワークのメンバーであり、したがって、メッセージ１０２５を（同様に共通グループキーを使用して）首尾よく暗号解読することができる。

いくつかの態様では、デバイス１３０ｃは、図示のようにパスレスポンスメッセージ１０３０を送信し得る。パスレスポンスメッセージ１０３０は、いくつかの態様では、ＨＷＭＰパスレスポンスメッセージ（ＰＲＥＰ：path response）であり得る。パスレスポンスメッセージ１０３０は、デバイス１３０ｃを介してメッシュネットワークを通過するパスを示す情報を含み得る。パスレスポンスメッセージ１０３０はまた、シーケンス番号フィールドを含み得る。パスレスポンスメッセージ１０３０のシーケンス番号フィールドがデバイス１３０ｂによってパスリクエストメッセージ１０２５の中で提供されるものと同じ値を有する場合、デバイス１３０ｂは、パスレスポンスメッセージ１０３０がパスリクエストメッセージ１０２５に応答していることを理解し得る。

【００９９】

[00116]メッセージ１０３０を受信しそれを共通グループキーにより首尾よく復号すると、デバイス１３０ｂは、デバイス１３０ｂが１つまたは複数の有用なサービスを提供することを決定し得る。デバイス１３０ｂは、次いで、関連付けリクエスト１０３５によるデバイス１３０ｃとの関連付けを開始し得る。いくつかの態様では、関連付けリクエストメッセージ１０３５は、関連付けリクエスト１０１５の特性の一部または全部を共有し得る。デバイス１３０ｃは、次いで、関連付けレスポンスメッセージ１４０をデバイス１３０ｂへ送信し得る。デバイス１３０ｂと１３０ｃとの間の関連付けが完了すると、デバイス１３０ｂは、１つまたは複数のサービスメッセージをメッシュネットワークを介してデバイス１３０ｃを使用して送信し得る（図示せず）。

【０１００】

[00117]上記のメッセージフローは、開示される方法およびシステムのいくつかの利点を示す。最初に、非メンバーデバイスは、ただ１つの参加しているデバイス／メンバーデバイスと認証することによって、メッシュネットワーク（および／またはソーシャルＷｉＦｉネットワーク）に加入し得る。このことは、メッシュネットワークメッセージの暗号化および暗号解読のために共通グループキーをメッシュネットワークが使用することにより、少なくとも部分的に容易にされる。この共通グループキーは、それがメッシュに加入するとき、関連付けプロセスを介して新しいデバイスと共有される。いくつかの態様では、ＰＨＹ／ＭＡＣ機能も、関連付けの間に交換される。

【０１０１】

[00118]上記で説明した４ウェイハンドシェイクはまた、ハンドシェイクに参加しているメンバーデバイスおよび非メンバーデバイスの各々に関する関連付け識別子を確立する。これらの関連付け識別子は、２つのデバイス間でのメッセージ交換のために使用される。たとえば、関連付け識別子は、メッシュネットワークのページングウィンドウの間のトラフィック通知（ＴＩＭメッセージ）の間に使用され得る。いくつかの態様では、ＩＰアドレス割当ても、４ウェイハンドシェイクの一部として実行される。たとえば、認証メッセージの各々は、デバイスが認証メッセージを送信するために提案されるＩＰアドレスを含み得る。関連付けメッセージは、関連付けメッセージを受信しているデバイスに割り当てられたＩＰアドレスを含み得る。

【０１０２】

[00119]図４は、管理フレームに関する例示的なメッセージフォーマットである。管理フレーム４００は、フレーム制御フィールド４０２と、持続時間フィールド４０４と、第１のアドレスフィールド４０６と、第２のアドレスフィールド４０８と、第３のアドレスフィールド４１０と、シーケンス制御フィールド４１２と、高スループット制御フィールド４１４と、フレーム本体４１６と、フレームチェックシーケンス４１８とを含む。

【０１０３】

[00120]フレーム制御フィールドは、プロトコルバージョンフィールド４２０と、タイプフィールド４２２と、サブタイプフィールド４２４と、ツーＤＳフィールド（a toDS field）４２６と、フロムＤＳフィールド４２８と、モアフラグメントフィールド（a more fragments field）４３０と、リトライフィールド４３２と、電力管理フィールド４３４と、モアデータフィールド４３６と、保護フレームフィールド４３８と、順序フィールド

４４０とを含み得る。

【０１０４】

[00121]図５は、図４のタイプフィールド４２２およびサブタイプフィールド４２４に関する値の様々な例示的な組合せを示す表である。図５によって示されるように、いくつかの態様では、図３の認証リクエストメッセージ１００５および認証レスポンスメッセージ１０１０のような認証メッセージは、管理フレームを示す００ｂのタイプ値と、認証メッセージを示す１０１１ｂのサブタイプ値とを有し得る。いくつかの態様では、図３の関連付けリクエストメッセージ１０１５のような関連付けリクエストは、管理フレームを示す００ｂのタイプ値と、ゼロ（０ｂ）のサブタイプ値とを有し得る。いくつかの態様では、図３の関連付けレスポンスメッセージ１０２０のような関連付けレスポンスは、管理フレームを示す００ｂのタイプ値と、関連付けレスポンスを示す０００１ｂのサブタイプ値とを有し得る。

【０１０５】

[00122]図６Ａは、認証メッセージに関する例示的なメッセージ本文を示す。いくつかの態様では、認証メッセージ１００５および／または１０１０は、図６Ａのメッセージ本文６００を含み得る。いくつかの態様では、それぞれ、図３の認証メッセージ１００５および１０１０の$P^{nbl}$および／または$P^{nal}$などのディフィーヘルマン公開値は、スカラーフィールド６０５、要素フィールド６１０、またはスカラーフィールド６０５と要素フィールド６１０の組合せの中に記憶され得る。いくつかの態様では、ＦＩＬＳナンスフィールド６１５は、図３のナンス値ｎｂ２またはｎａ２などのナンス値を記憶し得る。

【０１０６】

[00123]いくつかの態様では、認証メッセージ本文６００は、ＩＰアドレスリクエスト情報要素（図示せず）を含み得る。ＩＰアドレスリクエスト情報要素６２０の例示的なフォーマットが、図６Ｂに示される。ＩＰアドレスリクエスト情報要素６２０は、ＩＰアドレスデータフィールド６２５を含む。関連付けリクエストに関するＩＰアドレスデータフィールド６２５の例示的なフォーマットが、図６Ｃで６２５ａとして示される。ＩＰアドレスデータフィールド６２５ａは、ＩＰアドレスリクエスト制御フィールド６３０を含み、その一例が図６Ｄに示される。ＩＰアドレスデータフィールド６２５はまた、被要求ＩＰアドレス（a requested IP address）を含む。被要求インターネットプロトコル（ＩＰ）ｖ４アドレスは、フィールド６３５の中で搬送され、被要求インターネットプロトコル（ＩＰ）ｖ６アドレスは、フィールド６４０の中で搬送される。いくつかの態様では、認証メッセージを送信しているデバイスは、認証メッセージを受信しているデバイスとの通信のための特定のＩＰアドレスの使用を、ＩＰアドレスリクエスト情報要素６２０を使用して要求し得る。たとえば、いくつかの態様では、デバイス１３０ａは、デバイス１３０ｂと通信するときの特定のＩＰアドレスの使用を、ＩＰアドレスリクエスト情報要素６２０を認証リクエスト１００５の中に含めることによって要求し得る。同様に、デバイス１３０ｂは、デバイス１３０ａとの通信のための特定のＩＰアドレスの使用を、ＩＰアドレスリクエスト情報要素６２０を認証返答１０１０の中に含めることによって要求し得る。

【０１０７】

[00124]いくつかの他の態様では、ＩＰアドレスを要求し、および／または認証メッセージを送信または受信しているデバイスにそれを割り当てるために、他の方法が使用され得る。たとえば、いくつかの態様では、ＩＰアドレスを要求し、および／またはデバイスにそれを割り当てるために、動的ホスト構成プロトコル（ＤＨＣＰ：dynamic host configuration protocol）が利用され得る。これらの態様では、認証メッセージ本文６００は、ＦＩＬＳ　ＨＬＰコンテナ要素を含み得る。

【０１０８】

[00125]図６Ｅは、高速初期リンクセットアップ（ＦＩＬＳ）高レベルプロトコル（ＨＬＰ）コンテナ要素を示す。いくつかの態様では、ＨＬＰ要素６５０は、関連付けの間に移送される（transported）フレームをカプセル化する。１つまたは複数のＦＩＬＳ　ＨＬＰコンテナ要素は、以下で説明するように、ｄｏｔ１１ＦＩＬＳＡｃｔｉｖａｔｅｄが

真である場合、関連付けリクエストまたは関連付けレスポンスの中に含まれ得る。

【０１０９】

[00126]ＨＬＰ要素６５０は、長さフィールド６５２と、宛先メディアアクセス制御（ＭＡＣ）アドレスフィールド６５８と、ソースメディアアクセス制御（ＭＡＣ）アドレスフィールド６５６と、ＭＳＤＵフィールド６５４とを含む。長さフィールド６５２が２４３オクテットよりも小さい場合、長さフィールドの値は、１２＋ＨＬＰ　ＭＳＤＵフィールド６５８の長さである。ＨＬＰ　ＭＳＤＵフィールド６５８の長さが２４３オクテットよりも長い場合、長さフィールドの値は２５５である。

【０１１０】

[00127]宛先ＭＡＣアドレスフィールド６５４の値は、ＨＬＰ　ＭＳＤＵフィールド６５８の中に記憶されているＨＬＰフレームの宛先ＭＡＣアドレスである。ソースＭＡＣアドレスフィールド６５６の値は、ＨＬＰフレームのソースＭＡＣアドレスであり、それはＨＬＰフレームを生成するＳＴＡと同じソースアドレスであり得る。ＨＬＰ　ＭＳＤＵフィールド６５８は、ＨＬＰフレームのＭＳＤＵを含む。

【０１１１】

[00128]図７Ａは、関連付けリクエストメッセージの例示的なメッセージ本文を示す。いくつかの態様では、図３の関連付けリクエストメッセージ１０１５のメッセージ本文は、図７Ａに示すフォーマットに適合し得る。様々な態様では、メッセージ本文９００に示すフィールドの一部または全部は、関連付けリクエストメッセージの中に存在し得る。

【０１１２】

[00129]いくつかの態様では、メッセージ本文７００のＦＩＬＳキー確認フィールド７０５は、図３の関連付けリクエスト１０１５のメッセージ完全性コードのようなメッセージ完全性コードを記憶し得る。いくつかの他の態様では、関連付けリクエスト１０１５は、暗号ブロック連鎖メッセージ認証コード（ＣＢＣ－ＭＡＣ：cipher block chaining message authentication code）を用いるカウンター（ＣＣＭ：counter with CBC-MAC）を使用して保護され得る。これらの態様では、メッセージ完全性コードは、保護された関連付けリクエストの暗号化されたペイロードの中で搬送され得る。いくつかの態様では、メッセージ完全性コードは、ＣＢＣ－ＭＡＣ保護でのメッセージ認証コードとして使用され得る。いくつかの態様では、ガロアメッセージ認証コード（ＧＭＡＣ：Galois Message Authentication Codes）が利用され得る。これらの態様では、ガロア／カウンターモード（ＧＣＭ：Galois/Counter Mode）が、上記で説明したようなＣＣＭの代わりに使用されてよい。

【０１１３】

[00130]いくつかの態様では、関連付けリクエストメッセージ本文は、情報要素でないさらなるフィールドを含んでよい。いくつかの態様では、関連付けリクエストメッセージ本文は、確認フィールド（図示せず）を含み得る。いくつかの態様では、メッセージ完全性コードは、確認フィールドの中で搬送され得る。

【０１１４】

[00131]いくつかの態様では、関連付けリクエストメッセージ本文は、情報要素を含み得る。たとえば、ＦＩＬＳキー確認要素７０５は、いくつかの態様では、関連付けリクエストの中に含まれ得る。いくつかの態様では、ＦＩＬＳキー確認要素７０５は、図３に示すメッセージ完全性コード、メッセージ１０１５を搬送し得る。

【０１１５】

[00132]図７Ｂは、ＦＩＬＳキー確認要素７０５の１つの例示的なフォーマットを示す。いくつかの態様では、メッセージ完全性コードは、ＦＩＬＳキー確認要素７０５のＦＩＬＳ認証フィールド７１０の中で搬送され得る。

【０１１６】

[00133]いくつかの態様では、関連付けリクエストメッセージ本文は、ＩＰアドレス割当て情報要素７１５を含み得る。いくつかの態様では、ＩＰアドレス割当て要素７１５は、図６Ｂに示すＩＰアドレスリクエスト情報要素６２０と同じフォーマットのものであり

得る。ただし、ＩＰアドレス割当て情報要素７１５の中で、ＩＰアドレスデータフィールド６２５は、図８に示すフォーマット６２５ｂのものであり得る。

【０１１７】

[00134]図８は、例示的なＩＰアドレス割当て情報要素６２５ｂを示す。レスポンスに関するＩＰアドレスデータフィールド６２５ｂは、割当て済みＩＰｖ４アドレスフィールド（an assigned IP v4 address field）８０５と、割当て済みＩＰｖ６アドレスフィールド８１０とを含む。いくつかの態様では、ＩＰアドレス割当て情報要素を受信しているデバイスに割り当てられるＩＰアドレスは、フィールド８０５またはフィールド８１０のいずれかによって搬送され得る。

【０１１８】

[00135]図９は、関連付けレスポンスメッセージの例示的なメッセージ本文を示す。いくつかの態様では、図３の関連付けレスポンスメッセージ１０２０のメッセージ本文は、図９に示すメッセージ本文９００のフォーマットに適合し得る。様々な態様では、メッセージ本文９００に示すフィールドの一部分のみまたは全部は、関連付けレスポンスメッセージの中に存在し得る。

【０１１９】

[00136]いくつかの態様では、ＦＩＬＳキー確認要素９０５は、図３におけるメッセージ１０２０に関して説明したメッセージ完全性コードのようなメッセージ完全性コードを搬送し得る。いくつかの態様では、ＦＩＬＳキー確認要素９０５は、図７Ｂに示すキー確認要素フォーマット７０５に適合し得る。いくつかの他の態様では、メッセージ１０２０に関して説明したメッセージ完全性コードは、確認フィールドなどの関連付けレスポンスの別のフィールドによって搬送され得る。

【０１２０】

[00137]いくつかの態様では、関連付けレスポンスメッセージ本文９００は、ＩＰアドレス割当て情報要素９１５を含む。関連付けリクエストメッセージ本文７００のＩＰアドレス割当て情報要素７１５に関して上記で説明したように、ＩＰアドレス割当て情報要素は、関連付けレスポンスメッセージ本文９００を含む関連付けレスポンスを受信しているデバイスによる使用のために割り当てられたＩＰアドレスを搬送し得る。いくつかの態様では、ＩＰアドレス割当て情報要素９１５は、図８に関して説明したＩＰアドレス割当て情報要素７１５とともに実質的に確認する。

【０１２１】

[00138]図１０は、効率のよいメッシュピアリングのための方法の一例を示す。方法１１００は、いくつかの態様では、デバイス２０２によって実行され得る。方法１１００はまた、図３に示すデバイス１３０ａ～ｃのうちの１つまたは複数によって実行され得る。上記の図３の特有の説明に対して、方法１１００は、非メンバーデバイスであるデバイス１３０ｂによって実行され得る（ただし、他のデバイス１３０ａおよび／または１３０ｃによって実行されてもよい）。

【０１２２】

[00139]いくつかの知られているメッシュピアリングプロセスでは、２つのメッシュピア間で安全なメッシュ通信チャネルを確立するために、８つまでの異なるメッセージが交換され得る。開示されるメッシュピアリングプロセスは、メッシュネットワークに関する共通グループキーを新しいメンバーデバイスに提供する。共通グループキーは、メッシュの任意のメンバーデバイス間で交換される、グループアドレス指定されたメッセージを暗号化および暗号解読するために、メッシュの各メンバーデバイスによって使用され得る。

【０１２３】

[00140]提案される方法１１００はまた、メッシュ認証プロセスを関連付けプロセスと統合し、メッシュ関連付けの複雑さをさらに低減する効率をもたらす。開示される安全なメッシュピアリングプロセスは、メンバーデバイスと非メンバーデバイスとの間の単に４つのメッセージの交換を用いて実行され得る。このことは、メッシュ関連付けにおける低減されたレイテンシと計算オーバーヘッドをもたらし得る。

【０１２４】
[00141]ブロック１１０５では、認証リクエストが、非メッシュメンバーデバイスによってメッシュネットワークのメンバーデバイスへ送信される。いくつかの態様では、認証リクエストを送信している非メンバーデバイスは、メッシュネットワークへ加入することを認証リクエストを用いて要求していることがある。いくつかの態様では、認証リクエストは、図３に関して上記で説明した認証リクエスト１００５の１つまたは複数の特性を共有し得る。
【０１２５】
[00142]メンバーデバイスと非メンバーデバイスの両方は、共通パスワードを共有し得る。たとえば、共通パスワードは、各デバイス上の入力インターフェースを介して独立に受け取られてよい。メンバーデバイスおよび非メンバーデバイスの各々は、パスワードを使用してパスワード要素（Ｐ）を作成し得る。非メンバーデバイスは、第１のナンス値に基づいてディフィーヘルマン（ＤＨ）公開値を生成するために、パスワード要素を利用し得る。いくつかの態様では、ブロック１１０５において送信される認証リクエストは、公開値を含む。このようにして、認証リクエストはパスワード要素に基づいて生成されたナンスに基づいて生成されたディフィーヘルマン公開値を含み、パスワード要素はパスワードに基づくので、認証リクエストはパスワードに基づく。いくつかの態様では、認証リクエストはまた、非メンバーデバイスによって生成される第２のナンス値を含む。
【０１２６】
[00143]いくつかの態様では、第１のナンス値に基づいて生成される公開値は、認証リクエストの要素フィールドまたはスカラーフィールドの中で符号化される。いくつかの態様では、公開値は、要素フィールドとスカラーフィールドの両方の中で符号化されてよい。いくつかの態様では、第２のナンス値は、図６Ａに示すＦＩＬＳナンスフィールド６１５のようなＦＩＬＳナンスフィールドの中で符号化されてよい。
【０１２７】
[00144]いくつかの態様では、非メンバーデバイスは、メンバーデバイスとのメッシュ通信の間にそれが使用するために提案されるＩＰアドレスを決定する。認証リクエストは、提案されるＩＰアドレスを含むように非メンバーデバイスによって生成され得る。たとえば、いくつかの態様では、提案されるＩＰアドレスは、図６Ｂ～図６Ｄに関して説明したＩＰアドレスリクエスト情報要素６２０の中で搬送され得る。いくつかの他の態様では、提案されるＩＰアドレスは、認証リクエストの中に含まれないことがある。これらの態様のうちのいくつかでは、アドレス割当てのためにＤＨＣＰが使用され得る。
【０１２８】
[00145]ブロック１１１０では、非メンバーデバイスが、メンバーデバイスからの認証レスポンスを受信する。いくつかの態様では、非メンバーデバイスは、公開値を認証レスポンスから復号する。公開値は、メンバーデバイスによって独立に生成されていてよい。たとえば、いくつかの態様では、復号される公開値は、第３のナンスに基づいてメンバーデバイスによって生成されていてよい。非メンバーデバイスはまた、第４のナンス値を認証レスポンスから復号し得る。第４のナンスはまた、メンバーデバイスによって独立に生成されていてよい。いくつかの態様では、復号される公開値は、認証レスポンスの要素フィールド６１０および／またはスカラーフィールド６０５のうちの１つまたは複数から復号され得る。いくつかの態様では、第４のナンス値は、ＦＩＬＳナンスフィールド６１５から復号され得る。本開示での「復号する」または「復号すること」という用語の使用は、必ずしも特定の値の暗号解読または変換を暗示しないことに留意されたい。たとえば、いくつかの態様では、値をメッセージから復号することは、値をメッセージデータから抽出することと、それを何らかの方式で処理することと、を備え得る。たとえば、いくつかの態様では、復号された値は、別のプロセスへの入力パラメータとして使用され得る。
【０１２９】
[00146]いくつかの態様では、メンバーデバイスに対して提案されるＩＰアドレスの少なくとも一部分は、認証レスポンスから復号され得る。たとえば、認証レスポンスは、図

３のメッセージ１０１０に関して上記で説明した機能のうちの１つまたは複数を含み得る。いくつかの態様では、メンバーデバイスに対して提案されるＩＰアドレスは、図６Ｂに示す情報要素６２０のようなＩＰアドレスリクエスト情報要素から復号され得る。いくつかの他の態様では、提案されるＩＰアドレスは、認証レスポンスの中に含まれないことがある。上記で説明したように、いくつかの態様は、ＩＰアドレスを交渉し、および／またはメッシュネットワークのメンバーにそれを割り当てるための他の手段を使用し得る。たとえば、いくつかの態様では、ＤＨＣＰがアドレス割当てのために使用され得る。

【０１３０】

[00147]プロセス１１００のいくつかの態様では、ペアワイズマスターキー（ＰＭＫ）が、認証レスポンスに基づいて生成される。いくつかの態様では、ＰＭＫは、ＳＡＥ認証におけるＰＭＫに実質的に従って生成され得る。たとえば、ＰＭＫは、第１のナンス、第２のナンス、第３のナンスに基づく公開値、および／または第４のナンスのうちの１つまたは複数に基づいて生成され得る。

【０１３１】

[00148]いくつかの態様では、ペアワイズ一時キー（ＰＴＫ）が、少なくともペアワイズマスターキー、第２のナンス値および第４のナンス値に基づいて、非メンバーデバイスによって生成される。いくつかの態様では、ＰＴＫは、メッシュピアリングインスタンス識別子に基づいて生成され得る。いくつかの態様では、メッシュピアリングインスタンス識別子は、ローカルリンク識別子、非メンバーデバイスのメディアアクセス制御（ＭＡＣ）アドレス、およびメンバーデバイスのメディアアクセス制御（ＭＡＣ）アドレスに基づく。ローカルリンク識別子は、メンバーデバイスによって生成され得、メンバーデバイスによって使用されるすべての既存のリンク識別子の間で一意であり得る。いくつかの態様では、「ｄｏｔ１１ＭｅｓｈＳｅｃｕｒｉｔｙＡｃｔｉｖａｔｅｄ」が真である場合、メッシュピアリングインスタンスはまた、共有ＰＭＫセキュリティ関連付け（ＰＭＫＳＡ：PMK Security Association）を識別するＰＭＫＩＤと、メンバーデバイスによって選ばれたローカルなナンスと、非メンバーデバイスによって選ばれたピアなナンスとを含む。

【０１３２】

[00149]メッセージ完全性コード（ＭＩＣ））が、次いで、ＰＴＫに基づいて非メンバーデバイスによって生成される。

【０１３３】

[00150]ブロック１１２０では、関連付けリクエストが、メンバーデバイスへ送信される。いくつかの態様では、関連付けリクエストメッセージは、生成されたＭＩＣを含む。上記で説明したように、メッセージ完全性コードは、いくつかの態様では、図７Ｂに関して説明した情報要素７０５のようなＦＩＬＳキー確認情報要素によって搬送され得る。いくつかの他の態様、たとえば、関連付けリクエストを保護するためにＣＣＭ、またはＧＣＭなどの、関連付けられたデータを用いて認証される暗号化（ＡＥＡＤ：authenticated encryption with associated data）のアルゴリズムまたは方法を利用する態様では、メッセージ完全性コードは、関連付けリクエストメッセージの暗号化されたペイロードの中で搬送され得る。いくつかの他の態様では、関連付けリクエストの確認フィールドが、メッセージ完全性コードを搬送するために使用され得る。いくつかの態様では、関連付けリクエストは、図３に関して上記で説明した関連付けリクエスト１０１５の１つまたは複数の特性を共有し得る。

【０１３４】

[00151]いくつかの態様では、非メンバーデバイスはまた、関連付け識別子をメンバーデバイスに割り当てる。これらの態様のうちのいくつかでは、関連付け識別子はまた、関連付けリクエストの中に含まれる。関連付け識別子は、非メンバーデバイスがメッシュメッセージを送信するとき、メンバーデバイスを意図された宛先として識別するために非メンバーデバイスによって使用され得る。関連付けリクエストはまた、非メンバーデバイスのＰＨＹ／ＭＡＣ機能の１つまたは複数の指示を含み得る。

【０１３５】

[00152]いくつかの態様では、関連付けリクエストはまた、メンバーデバイスに非メンバーデバイスによって割り当てられるＩＰアドレスを含む。ＩＰアドレスは、メンバーデバイスと非メンバーデバイスとの間のメッシュ通信のためのソースアドレスとして、メンバーデバイスによって使用されるべきである。いくつかの態様では、割り当てられるＩＰアドレスは、図７Ａおよび図８に関して上述されたＩＰアドレス割当て情報要素の中で搬送される。いくつかの他の態様では、割り当てられるＩＰアドレスは、関連付けリクエストのＩＰアドレス割当て情報要素の中に含まれない。代わりに、いくつかの態様では、ＩＰアドレスを割り当てるためにＤＨＣＰが使用され得る。これらの態様のうちのいくつかでは、関連付けリクエストは、図６Ｅに示すようなＦＩＬＳ　ＨＬＰコンテナ要素６５０のような情報要素を介してＤＨＣＰプロトコルメッセージを搬送し得る。

【０１３６】

[00153]ブロック１１２５では、関連付けレスポンスが、メンバーデバイスから受信される。いくつかの態様では、第２のメッセージ完全性コード（ＭＩＣ）が、関連付けレスポンスから復号され得る。復号されたＭＩＣは、非メンバーデバイスおよびメンバーデバイスが同じパスワードを共有しているかどうかを決定するために使用され得る。いくつかの態様では、メッセージ完全性コードは、ＦＩＬＳキー確認情報要素から復号され得る。いくつかの態様では、ＭＩＣは、関連付けレスポンスの別のフィールド、たとえば８０２．１１　２０１２規格のセクション８．４．１．４．４１において定義されるような確認フィールドから復号され得る。いくつかの他の態様、たとえば、ＣＣＭ、またはＧＣＭなどの、関連付けられたデータを用いて認証される暗号化によって関連付けレスポンスを保護する態様では、ＭＩＣは、関連付けレスポンスの暗号化されたペイロードから復号され得る。

【０１３７】

[00154]メンバーデバイスから関連付けレスポンスの中で受信されたＭＩＣは、生成されたＭＩＣと比較され得る。復号されたＭＩＣおよび生成されたＭＩＣが同等である場合、非メンバーデバイスは、メンバーデバイスおよび非メンバーデバイスが関連付けられてよいと決定し得る。

【０１３８】

[00155]いくつかの態様では、非メンバーデバイスに関する関連付け識別子は、関連付けレスポンスから復号され得る。復号された関連付け識別子は、メンバーデバイスとメッシュネットワーク上で通信するときに使用され得る。たとえば、非メンバーデバイスとメンバーデバイスとの間の通信は、メッシュメッセージが非メンバーデバイスによって送信され、または非メンバーデバイスを宛先とすることを示すために、復号された関連付け識別子を使用し得る。

【０１３９】

[00156]いくつかの態様では、メンバーデバイスのＭＡＣおよび／またはＰＨＹ機能は、関連付けレスポンスから非メンバーデバイスによって復号され得る。機能は、メンバーデバイスとどのように通信するのかを決定するために、非メンバーデバイスによって使用され得る。

【０１４０】

[00157]メッシュネットワークに関する共通グループキーは、関連付けレスポンスから非メンバーデバイスによって復号され得る。グループキーは、メッシュネットワーク内のデバイスにとって共通であり得る。グループキーは、メッシュネットワーク上のデバイスへの送信向けの、グループアドレス指定されたメッセージを暗号化するために、非メンバーデバイスによって使用され得る。グループキーはまた、メッシュネットワークのメンバーである任意の他のデバイスから受信される、グループアドレス指定されたメッセージを復号するために、非メンバーデバイスによって使用され得る。

【０１４１】

[00158]いくつかの態様では、関連付けレスポンスは、図３の関連付けレスポンスメッセージ１０２０と同等であり得る。たとえば、メンバーデバイスと非メンバーデバイスと

の間でメッセージを交換するときに非メンバーデバイスがソースＩＰアドレスとして使用するためのＩＰアドレスは、関連付けレスポンスから復号され得る。いくつかの態様では、非メンバーデバイスに割り当てられるＩＰアドレスは、図７Ａおよびフィールド７１５に関して上記で説明したようなＩＰアドレス割当て情報要素から復号され得る。あるいは、いくつかの態様では、関連付けレスポンスは、いくつかの態様では、ＩＰアドレスを割り当てるように機能するＤＨＣＰプロトコル情報を搬送し得る、ＦＩＬＳ　ＨＬＰコンテナ要素を含み得る。ＨＬＰコンテナ要素の一例が、図６Ｅに示される。

【０１４２】

[00159]いくつかの態様では、方法１１００は、少なくとも認証回路と関連付け回路とを含むデバイスによって実施され得る。認証回路は、図１０に示すブロック１１０５～１１１０に関して上記で説明した機能のうちの１つまたは複数を実行するように構成され得る。いくつかの態様では、認証回路は、プロセッサ２０４および／または送信機２１０および／または受信機２１２に相当し得る。関連付け回路は、図１１に示すブロック１１２０～１１２５に関して上記で説明した機能のうちの１つまたは複数を実行するように構成され得る。いくつかの態様では、関連付け回路は、プロセッサ２０４に相当し得る。

【０１４３】

[00160]図１１は、メッシュピアリングのための方法の一例を示す。方法１２００は、いくつかの態様では、デバイス２０２によって実行され得る。方法１２００はまた、図３に示すデバイス１３０ａ～ｃのうちの１つまたは複数によって実行され得る。特に図３の説明に関して、プロセス１２００は、メンバーデバイス１３０ａによって実行され得る。

【０１４４】

[00161]方法１２００は、より効率のよいメッシュピアリングプロセスを提供するために利用され得る。たとえば、いくつかの知られているメッシュピアリングプロセスでは、２つのメッシュピア間で安全なメッシュ通信チャネルを確立するために、８つまでの異なるメッセージが交換され得る。認証プロセスを関連付けプロセスと統合することによって、安全なメッシュピア接続が、２つのメッシュピアデバイス間での単に４つのメッセージの交換を用いて実行され得る。このことは、メッシュピアデバイスにとって低減されたレイテンシと計算オーバーヘッドをもたらし得る。

【０１４５】

[00162]プロセス１２００は、メッシュネットワークのメンバーによって実行される方法である。メンバーデバイスは、メッシュネットワークの非メンバーデバイスと認証しそれに関連付ける。認証および関連付けが完了した後、非メンバーデバイスは、メンバーデバイスになり、メッシュネットワーク上のグループアドレス指定されたメッセージを共通グループキーを使用して暗号化および復号することができる。

【０１４６】

[00163]ブロック１２０５では、メッシュネットワークのメンバーデバイスは、非メンバーデバイスからの認証リクエストを受信する。メンバーデバイスは、メッシュネットワークに参加している。いくつかの態様では、認証リクエストを送信している非メンバーデバイスは、メッシュネットワークへ加入することを認証リクエストを用いて要求していることがある。いくつかの態様では、認証リクエストは、図３に関して上記で説明した認証リクエスト１００５と、１つまたは複数の特性を共有し得る。

【０１４７】

[00164]いくつかの態様では、ブロック１２０５において受信される認証リクエストは、第１のナンス値に基づいて生成された公開値を含み、公開値は、非メンバーデバイスによって生成される。いくつかの態様では、認証リクエストはまた、第２のナンス値を含み、第２のナンス値も非メンバーデバイスによって生成されていることがある。メンバーデバイスは、第１のナンス値および／または第２のナンス値に基づいて、公開値を認証リクエストから復号し得る。いくつかの態様では、公開値は、認証リクエストの要素フィールドまたはスカラーフィールドから復号され得る。いくつかの態様では、公開値は、認証リクエストの要素フィールドとスカラーフィールドの両方から復号され得る。いくつかの態

様では、第２のナンス値は、図６Ａに示すＦＩＬＳナンスフィールド６１５のようなＦＩＬＳナンスフィールドから復号され得る。

【０１４８】

[00165]いくつかの態様では、メンバーデバイスは、メンバーデバイスとのメッシュ通信で非メンバーデバイスによって使用するために提案されるＩＰアドレスを、認証リクエストから復号し得る。たとえば、提案されるＩＰアドレスは、図６Ｂ～図６Ｄおよびフィールド６２０に関して上記に示したようなＩＰアドレスリクエスト情報要素から復号され得る。認証リクエストの他の態様は、提案されるＩＰアドレスを含まないことがある。

【０１４９】

[00166]非メンバーデバイスとメンバーデバイスの両方は、共通パスワードを共有し得る。たとえば、共通パスワードは、各デバイス上の入力インターフェースを介して独立に受け取られてよい。非メンバーデバイスおよびメンバーデバイスの各々は、パスワードを使用してパスワード要素（Ｐ）を作成し得る。いくつかの態様では、パスワード要素は、ＳＡＥ認証において使用されるものと類似の方式で生成され得る。

【０１５０】

[00167]メンバーデバイスは、第３および第４のナンス値を生成し得る。パスワード要素を使用して、非メンバーデバイスは、第３のナンス値に基づいて公開値を生成し得る。たとえば、公開値は、第３のナンス値に基づくディフィーヘルマン（ＤＨ）公開値であってよい。

【０１５１】

[00168]ブロック１２１０では、メンバーデバイスが、認証レスポンスを非メンバーデバイスへ送信する。認証レスポンスは、第３のナンス値および／または第４のナンス値に基づく公開値を含み得る。いくつかの態様では、メンバーデバイスは、メッシュ通信の間に非メンバーデバイスと通信するときにメンバーデバイスがソースＩＰアドレスとして使用し得る提案されるＩＰアドレスを含むように、認証レスポンスを生成する。いくつかの態様では、認証レスポンスは、図１０に関して上記で説明した認証返答１０１０の１つまたは複数の特性を共有し得る。たとえば、提案されるＩＰアドレスは、図６Ｂ～図６Ｄおよびフィールド６２０に関して示すように、認証レスポンスの中でＩＰアドレスリクエスト情報要素を介して搬送され得る。認証レスポンスの他の態様は、提案されるＩＰアドレスを搬送しないことがある。

【０１５２】

[00169]プロセス１２００のいくつかの態様では、ペアワイズマスターキー（ＰＭＫ）は、ブロック１２０５において受信された認証リクエスト、ならびに第３および第４のナンス値に基づいて、メンバーデバイスによって生成される。ＰＭＫは、第１のナンス、第２のナンス、第３のナンス、および／または第４のナンスに基づいて生成された公開値に基づいて生成され得る。いくつかの態様では、ＰＭＫは、ＳＡＥ認証において使用される方法に実質的に従って生成される。

【０１５３】

[00170]いくつかの態様では、ペアワイズ一時キー（ＰＴＫ）は、少なくともペアワイズマスターキー、第２のナンス値および第４のナンス値に基づいて、メンバーデバイスによって生成される。いくつかの態様では、ＰＴＫは、８０２．１１ａｉ認証に記載される方法に実質的に従って生成される。いくつかの態様では、ＰＴＫは、メッシュピアリングインスタンス識別子に基づいて生成される。いくつかの態様では、メッシュピアリングインスタンス識別子は、ローカルリンク識別子、非メンバーデバイスのメディアアクセス制御（ＭＡＣ）アドレス、およびメンバーデバイスのメディアアクセス制御（ＭＡＣ）アドレスに基づく。ローカルリンク識別子は、メンバーデバイスによって生成され得、メンバーデバイスによって使用されるすべての既存のリンク識別子の間で一意であり得る。いくつかの態様では、「ｄｏｔ１１ＭｅｓｈＳｅｃｕｒｉｔｙＡｃｔｉｖａｔｅｄ」が真である場合、メッシュピアリングインスタンスはまた、共有ＰＭＫセキュリティ関連付け（ＰＭＫＳＡ）を識別するＰＭＫＩＤと、メンバーデバイスによって選ばれたローカルなナン

ス（a local Nonce）と、非メンバーデバイスによって選ばれたピアなナンス（a peer Nonce）とを含む。

【０１５４】

[00171]メッセージ完全性コード（ＭＩＣ）が、次いで、ＰＴＫに基づいてメンバーデバイスによって生成される。

【０１５５】

[00172]ブロック１２１５では、関連付けリクエストが、メンバーデバイスによって受信される。メッセージ完全性コード（ＭＩＣ）は、関連付けリクエストメッセージから復号される。いくつかの態様では、ＭＩＣは、図７Ｂに関して上記で説明した情報要素７０５のようなＦＩＬＳキー確認情報要素から復号され得る。いくつかの態様では、ＭＩＣは、関連付けリクエストメッセージのペイロードから復号される。たとえば、ＣＣＭ、またはＧＣＭなどの、関連付けられたデータを用いて認証される暗号化（ＡＥＡＤ）のアルゴリズムまたは方法を使用して関連付けリクエストのペイロードを保護する態様では、ＭＩＣは、暗号解読されたペイロードから復号され得る。

【０１５６】

[00173]復号されたＭＩＣは、非メンバーデバイスおよびメンバーデバイスが同じパスワードを共有しているかどうかを決定するために使用され得る。復号されたＭＩＣはまた、同じキー（たとえば、ＰＭＫおよび／またはＰＴＫ）が非メンバーデバイスとメンバーデバイスの両方によって導出されていることを検証するために使用され得る。たとえば、メンバーデバイスは、上記で説明したようにＰＴＫに基づいて第２のＭＩＣを生成し得る。第２のＭＩＣを復号されたＭＩＣと比較することによって、メンバーデバイスは、メンバーデバイスおよび非メンバーデバイスが同じパスワードを共有しているかどうかを決定することができる（２つのＭＩＣが同等である場合、２つのパスワードは同等である）。

【０１５７】

[00174]いくつかの態様では、関連付け識別子は、関連付けリクエストから復号される。関連付け識別子は、非メンバーデバイスとのメッシュメッセージ交換で使用するために、メンバーデバイスに非メンバーデバイスによって割り当てられる。たとえば、メンバーデバイスは、非メンバーデバイスによって（それがメッシュのメンバーになった後に）送信されたメッシュメッセージがメンバーデバイスのために意図されているかどうかを、関連付け識別子がメッシュメッセージの中に含まれているかどうかに基づいて決定し得る。

【０１５８】

[00175]いくつかの態様では、非メンバーデバイスと通信するためにメンバーデバイスに割り当てられたＩＰアドレスは、関連付けリクエストから復号される。いくつかの態様では、関連付けリクエストは、図７Ａの情報要素７１５に関して上述されたようなＩＰアドレス割当て情報要素を含む。これらの態様では、メンバーデバイスは、割り当てられたＩＰアドレスを決定するために、情報要素７１５を復号し得る。いくつかの他の態様では、ＩＰアドレスは、代替手段を使用して割り当てられ得る。たとえば、いくつかの態様では、ＩＰアドレスをメンバーデバイスおよび／または非メンバーデバイスに割り当てるために、ＤＨＣＰが使用され得る。ＤＨＣＰメッセージは、いくつかの態様では、ＦＩＬＳ　ＨＬＰコンテナ要素を介して、関連付けリクエストの中で搬送され得る。例示的なＦＩＬＳ　ＨＬＰコンテナ要素が、図６Ｅに示される。

【０１５９】

[00176]ブロック１２２５では、関連付けレスポンスが、非メンバーデバイスへ送信される。いくつかの態様では、メンバーデバイスはまた、第２の関連付け識別子を非メンバーデバイスに割り当てる。これらの態様のうちのいくつかでは、第２の関連付け識別子はまた、関連付けレスポンスの中に含まれる。第２の関連付け識別子は、メッセージが非メンバーデバイスを宛先とするときにメンバーデバイスによって送信されるメッシュメッセージの中に含まれ得る。

【０１６０】

[00177]上記で説明した生成されたＭＩＣは、関連付けレスポンスの中にメンバーデバ

イスによって含められ得る。たとえば、生成されたＭＩＣは、いくつかの態様では、ＦＩＬＳキー確認情報要素９０５の中で符号化され得る。いくつかの態様では、関連付けレスポンスは、ＣＣＭによって保護され得る。これらの態様では、ＭＩＣは、関連付けレスポンスの暗号化されたペイロードの中で通信され得る。

【０１６１】

[00178]メッシュネットワークに関する共通グループキーは、関連付けレスポンスの中にメンバーデバイスによって含められ得る。グループキーは、メッシュネットワーク内のデバイスにとって共通であり得る。共通グループキーは、メッシュネットワークへの送信向けの、グループアドレス指定されたメッセージを暗号化するために、非メンバーデバイスによって使用され得る。共通グループキーはまた、メッシュネットワークから受信される、グループアドレス指定されたメッセージを復号するために、非メンバーデバイスによって使用され得る。

【０１６２】

[00179]いくつかの態様では、メンバーデバイスと非メンバーデバイスとの間でメッセージを交換するときに非メンバーデバイスがソースＩＰアドレスとして使用するためのＩＰアドレスは、関連付けレスポンスの中にメンバーデバイスによって含められ得る。いくつかの態様では、関連付けレスポンスは、図９に関して上記で説明したようなＦＩＬＳ　ＩＰアドレス割当て情報要素９１５を含むように生成される。情報要素９１５は、非メンバーデバイスに割り当てられたＩＰアドレスを符号化し得る。いくつかの態様では、割り当てられたＩＰアドレスは、ＦＩＬＳ　ＩＰアドレス割当て情報要素９１５を介して通信されない。これらの態様のうちのいくつかでは、ＩＰアドレスは、ＤＨＣＰによって割り当てられ得る。いくつかの態様では、ＤＨＣＰプロトコルメッセージは、関連付けレスポンスの中でＦＩＬＳ　ＨＬＰコンテナ要素を介して搬送され得る。ＦＩＬＳ　ＨＬＰコンテナ要素の一例が、図６Ｅに示される。

【０１６３】

[00180]いくつかの態様では、メンバーデバイスは、メンバーデバイスの１つまたは複数のＰＨＹ／ＭＡＣ機能の指示を含むように、関連付けレスポンスメッセージを生成する。

【０１６４】

[00181]方法１２００は、いくつかの態様では、認証回路および関連付け回路によって実施され得る。認証回路は、図１１に示すブロック１２０５～１２１０に関して上記で説明した機能のうちの１つまたは複数を実行するように構成され得る。いくつかの態様では、認証回路は、プロセッサ２０４および／または送信機２１０および／または受信機２１２に相当し得る。関連付け回路は、図１１に示すブロック１２１５～１２２５に関して上記で説明した機能のうちの１つまたは複数を実行するように構成され得る。いくつかの態様では、関連付け回路は、プロセッサ２０４に相当し得る。

【０１６５】

[00182]図１２は、メッシュピアリングのための方法の一例を示す。方法１３００は、いくつかの態様では、デバイス２０２によって実行され得る。方法１３００はまた、図３に示すデバイス１３０ａ～ｃのうちの１つまたは複数によって実行され得る。特に図３の説明に関して、方法１３００は、デバイス１３０ｂ（非メンバーデバイス）によって実行され得る。ただし、他のデバイス１３０ａおよび／または１３０ｃも、プロセス１３００を実行し得る。

【０１６６】

[00183]方法１３００は、より効率のよいメッシュピアリングプロセスを提供するために利用され得る。たとえば、いくつかの知られているメッシュピアリングプロセスでは、新しいデバイスがメッシュに加入するために、新しいデバイスは、特定のメンバーデバイスによって送信されたメッセージが新しいメンバーデバイスによって復号され得る前にメッシュの各メンバーデバイスに関連付けなければならない。開示される方法およびシステムは、メッシュの任意のメンバーデバイスによって送信されるメッセージを復号するため

に使用され得る共通グループキーを提供する。このことは、他のメッシュデバイスからのメッセージが暗号解読または暗号化されメッシュへ送信され得る前に、メッセージを受信する新しいメンバーデバイスが、わずか１つの他のメンバーデバイスに関連付けることを可能にする。たとえば、共通グループキーをメッシュのメンバーデバイスから取得した後、新しいデバイスは、メッシュの他のメンバーデバイスとのルーティングメッセージまたはパスメッセージを送信および受信し得る。特定のメンバーデバイスによって維持されている特定のパスが有用であると決定すると、新しいデバイスは、次いで、その特定のデバイスに関連付けることを決定し得る。新しいデバイスは、メッシュの少なくともいくつかの他のメンバーデバイスに関連付けないことを決定し得る。たとえば、いかなる関心があるサービスまたは値も新しいデバイス（非メンバーデバイス）に提供し得ない他のメンバーデバイスは、したがって、新しいメンバーデバイスによって関連付けられないことがある。

【０１６７】

[00184]ブロック１３０５では、メッシュの第１のメンバーデバイスとの関連付けが、非メンバーデバイスによって実行される。第１のメンバーデバイスとの関連付けは、メッシュに関する共通グループキーを非メンバーデバイスに提供する。いくつかの態様では、共通グループキーは、メッシュ上で送信または受信される１つまたは複数のグループアドレス指定されたメッセージを暗号化および／または暗号解読するために使用され得る。いくつかの態様では、ブロック１３０５の関連付けは、プロセス１１００および図１０によって説明されたように実行され得る。関連付けが完了した後、非メンバーデバイスは、メッシュネットワークのメンバーであり得る。したがって、同じデバイスが、以下の説明では新しいメンバーデバイスと呼ばれることがある。

【０１６８】

[00185]ブロック１３１０では、第１のメッセージが、メッシュの第２のメンバーデバイスから受信される。いくつかの態様では、第１のメッセージは、メッシュネットワークによって提供されるサービスへのルートに関係する情報を含むパスレスポンスメッセージ（ＰＲＥＰ）であり得る。

【０１６９】

[00186]いくつかの態様では、第１のメッセージの受信は、非メンバーデバイスによるパスリクエストメッセージ（ＰＲＥＱ）の送信によって先行される。送信されるパスリクエストメッセージは、受信された任意のパスレスポンスメッセージをこのパスリクエストメッセージに、新しいメンバーデバイスが整合させる（match）ことを可能にするシーケンス番号を含み得る。

【０１７０】

[00187]送信されるパスリクエストメッセージは、ブロック１３０５の関連付けから受信された共通グループキーに基づいて、暗号化および／または暗号解読され得る。これらの態様では、関連付けの間に受信される共通グループキーは、メッシュのすべてのメンバーデバイスにとって共通であり得る。このことは、メッシュメンバーデバイス間で交換されるべきグループアドレス指定されたメッセージの、共通グループキーに基づく暗号化および暗号解読を可能にし得る。

【０１７１】

[00188]ブロック１３１５では、第１のメッセージが、ブロック１３０５の関連付けプロセスによって提供された共通グループキーに基づいて暗号解読される。メッシュの複数のメンバーデバイスによって送信される、グループアドレス指定されたメッセージを暗号化および／または暗号解読するために、メッシュが共通グループキーを利用し得ることに留意されたい。したがって、新しいメンバーデバイスは、新しいメンバーデバイスに関連付けられていないメッシュメンバーデバイスによって送信されたメッセージを暗号解読し得る。

【０１７２】

[00189]ブロック１３２０では、第２のメッセージが、メッシュの第３のメンバーデバ

イスから受信される。第２のメッセージはまた、いくつかの態様では、ルーティングメッセージまたはパスレスポンスメッセージであり得る。いくつかの態様では、第２のパスレスポンスメッセージは、上記で説明した新しいメンバーデバイスによって送信されたパスリクエストメッセージと同じシーケンス番号を含む。（すなわち、第１および第２のパスレスポンスメッセージは、同じパスリクエストメッセージに応答しているが、おそらくは異なるメンバーデバイスによって送信されている）。

【０１７３】

[00190]いくつかの態様では、第２のメッセージは、第１のメッセージに無関係である。たとえば、第２のメッセージは、いくつかの態様では、第１のメッセージと類似のパスレスポンスメッセージであり得るが、前に説明したパスリクエストメッセージと異なるパスリクエストメッセージに応答して送信されている。したがって、いくつかの態様では、第２のメッセージの受信は、第２のパスリクエストメッセージの送信によって先行される。送信される第２のパスリクエストメッセージは、ブロック１３０５の関連付けから受信された共通グループキーに基づいて暗号化され得る。

【０１７４】

[00191]ブロック１３２５では、第２のメッセージが、共通グループキーに基づいて暗号解読される。少なくともメッシュの第２のメンバーデバイスと第３のメンバーデバイスの両方によって送信される、グループアドレス指定されたメッセージを暗号化および／または暗号解読するためにメッシュが共通グループキーを利用するので、新しいメンバーデバイスが第２のメンバーデバイスまたは第３のメンバーデバイスのいずれかに関連付けられていないにもかかわらず、新しいメンバーデバイスは第２および第３のメンバーデバイスによって送信されるメッセージを首尾よく暗号解読することができる。

【０１７５】

[00192]いくつかの態様では、第２および／または第３のメンバーデバイスのうちの１つまたは複数からの少なくとも１つのメッセージを首尾よく暗号解読した後、新しいメンバーデバイスは、それが第２および／または第３のメンバーデバイスに関連付けるべきであると決定し得る。たとえば、これらのデバイスのうちの少なくとも１つとの関連付けは、１つまたは複数のデバイスによって提供される１つまたは複数のサービスにアクセスするために実行され得る。この関連付けは、いくつかの態様では、図１０のプロセス１１００に実質的に従って実行され得る。関連付けが首尾よく完了すると、新しいメンバーデバイスは、新たに関連付けられたデバイスと１つまたは複数のサービスメッセージを交換し得る。いくつかの他の態様では、ブロック１３２０および１３２５は、プロセス１３００によって実行されないことがある。

【０１７６】

[00193]プロセス１３００のいくつかの態様は、共通グループキーを使用してユニキャストパケットを暗号化し得、－そのような実装形態では、メッシュトラフィックはまた、グループキーを使用して暗号化され得る。

【０１７７】

[00194]方法１３００は、いくつかの態様では、関連付け回路および受信回路、ならびに暗号解読回路によって実行され得る。関連付け回路は、図１２に示すブロック１３０５に関して上記で説明した機能のうちの１つまたは複数を実行するように構成され得る。いくつかの態様では、関連付け回路は、プロセッサ２０４および／または送信機２１０および／または受信機２１２に相当し得る。受信回路は、図１２に示すブロック１３１０および／または１３２０に関して上記で説明した機能のうちの１つまたは複数を実行するように構成され得る。いくつかの態様では、受信回路は、受信機２１２に相当し得る。暗号解読回路は、図１２に示すブロック１３１５および／または１３２５に関して上記で説明した機能のうちの１つまたは複数を実行するように構成され得る。いくつかの態様では、暗号解読回路は、プロセッサ２０４に相当し得る。

【０１７８】

[00195]本明細書で開示された実施形態に関して説明された様々な例示的な論理ブロッ

ク、構成、モジュール、回路、およびアルゴリズムステップは、電子ハードウェア、コンピュータソフトウェア、または両方の組合せとして実装され得ることを、当業者はさらに諒解されよう。様々な例示的な構成要素、ブロック、構成、モジュール、回路、およびステップが、上記では概して、それらの機能に関して説明された。そのような機能がハードウェアとして実装されるか、ソフトウェアとして実装されるかは、特定の適用例および全体的なシステムに課された設計制約に依存する。当業者は、説明された機能を、特定の適用例ごとに様々な形で実装することができるが、そのような実装決定が、本開示の範囲からの逸脱を引き起こすと解釈されるべきではない。

【０１７９】

[00196]本明細書で開示される実施形態に関して説明された方法またはアルゴリズムのステップは、ハードウェア内で、プロセッサによって実行されるソフトウェアモジュール内で、またはこれら２つの組合せで直接実施され得る。ソフトウェアモジュールは、ランダムアクセスメモリ（ＲＡＭ）、フラッシュメモリ、読取り専用メモリ（ＲＯＭ）、プログラマブル読取り専用メモリ（ＰＲＯＭ）、消去可能プログラマブル読取り専用メモリ（ＥＰＲＯＭ）、電気消去可能プログラマブル読取り専用メモリ（ＥＥＰＲＯＭ（登録商標））、レジスタ、ハードディスク、リムーバブルディスク、コンパクトディスク読取り専用メモリ（ＣＤ－ＲＯＭ）、または当技術分野で知られている任意の他の形態の記憶媒体中に常駐し得る。例示的な非一時的（たとえば、有形）記憶媒体は、プロセッサが記憶媒体から情報を読み取り、記憶媒体に情報を書き込むことができるように、プロセッサに結合される。代替として、記憶媒体はプロセッサと一体であってよい。プロセッサおよび記憶媒体は特定用途向け集積回路（ＡＳＩＣ）中に存在し得る。ＡＳＩＣはコンピューティングデバイスまたはユーザ端末中に存在し得る。代替として、プロセッサおよび記憶媒体は、コンピューティングデバイスまたはユーザ端末中に個別の構成要素として存在し得る。

【０１８０】

[00197]開示されている実施形態の上記の説明は、当業者が開示されている実施形態を製作または使用することを可能にするために提供されている。これらの実施形態に対する様々な修正は、当業者には容易に明らかであり、本明細書で定義されている原理は、本開示の範囲から逸脱することなく、他の実施形態に適用され得る。したがって、本開示は、本明細書に示されている実施形態に限定されることを意図されておらず、以下の特許請求の範囲によって定義される原理および新規な特徴と一致する可能な最も広い範囲を与えられるべきである。

【図１】

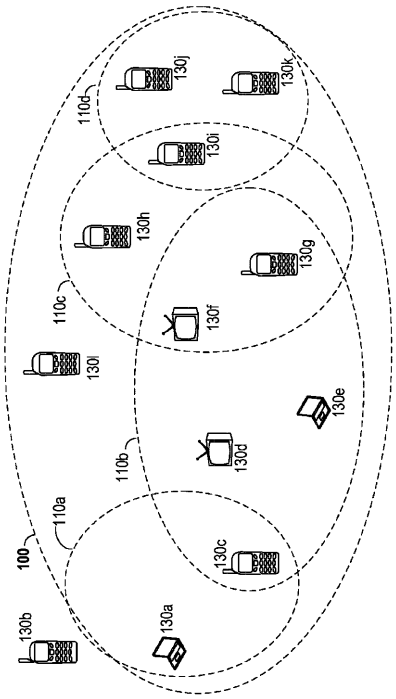



FIG. 1

【図２】

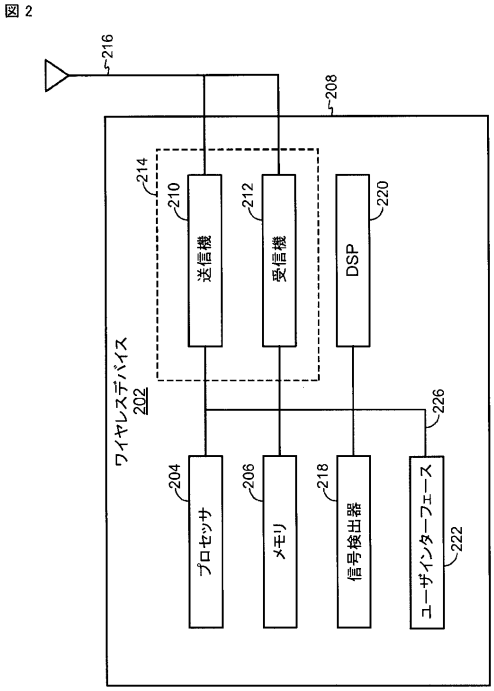



FIG. 2

【図３】

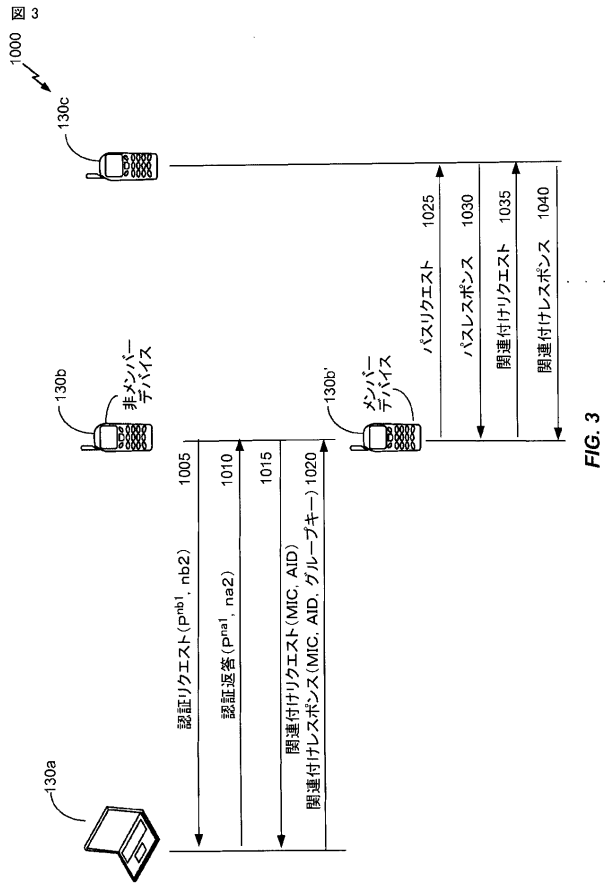



FIG. 3

【図４】

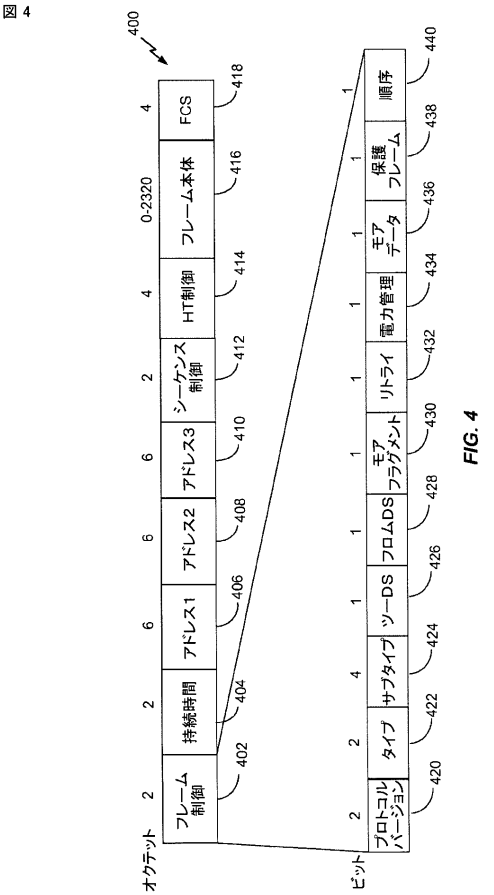
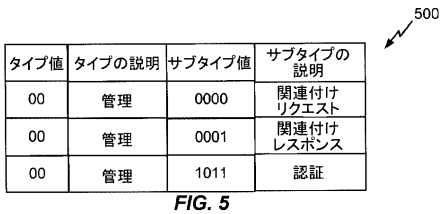



FIG. 4

【図５】

図 5



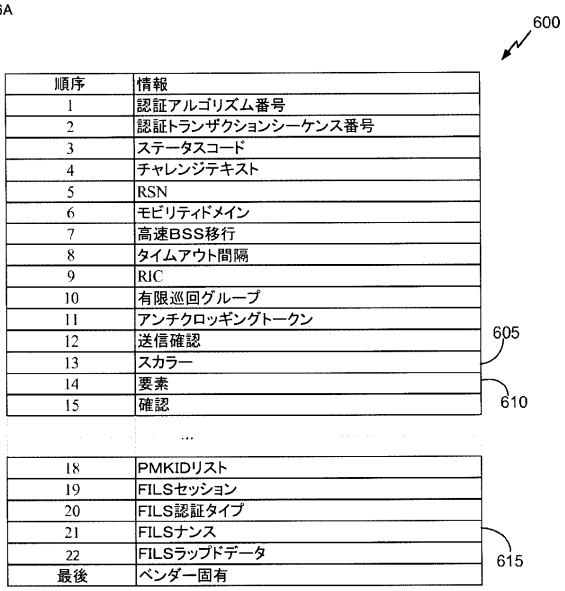
| タイプ値 | タイプの説明 | サブタイプ値 | サブタイプの説明 |
|---|---|---|---|
| 00 | 管理 | 0000 | 関連付けリクエスト |
| 00 | 管理 | 0001 | 関連付けレスポンス |
| 00 | 管理 | 1011 | 認証 |

500

FIG. 5

【図６Ａ】

図 6A



| 順序 | 情報 |
|---|---|
| 1 | 認証アルゴリズム番号 |
| 2 | 認証トランザクションシーケンス番号 |
| 3 | ステータスコード |
| 4 | チャレンジテキスト |
| 5 | RSN |
| 6 | モビリティドメイン |
| 7 | 高速BSS移行 |
| 8 | タイムアウト間隔 |
| 9 | RIC |
| 10 | 有限巡回グループ |
| 11 | アンチクロッギングトークン |
| 12 | 送信確認 |
| 13 | スカラー |
| 14 | 要素 |
| 15 | 確認 |
| ... | |
| 18 | PMKIDリスト |
| 19 | FILSセッション |
| 20 | FILS認証タイプ |
| 21 | FILSナンス |
| 22 | FILSラップドデータ |
| 最後 | ベンダー固有 |

600

605

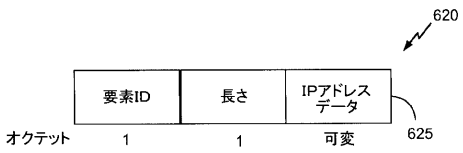
610

615

FIG. 6A

【図６Ｂ】

図 6B



| | 要素ID | 長さ | IPアドレスデータ |
|---|---|---|---|
| オクテット | 1 | 1 | 可変 |

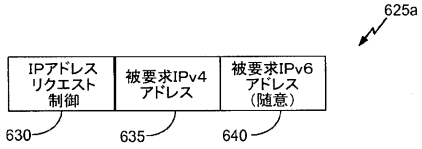
620

625

FIG. 6B

【図６Ｃ】

図 6C



| IPアドレスリクエスト制御 | 被要求IPv4アドレス | 被要求IPv6アドレス（随意） |
|---|---|---|

625a

630

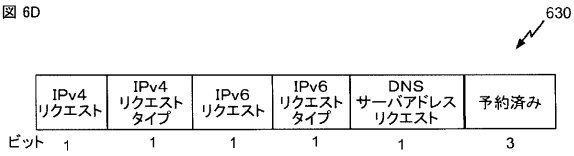
635

640

FIG. 6C

【図６Ｄ】

図 6D



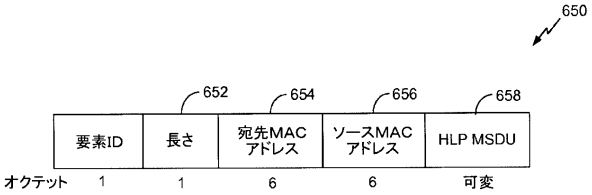
| | IPv4リクエスト | IPv4リクエストタイプ | IPv6リクエスト | IPv6リクエストタイプ | DNSサーバアドレスリクエスト | 予約済み |
|---|---|---|---|---|---|---|
| ビット | 1 | 1 | 1 | 1 | 1 | 3 |

630

FIG. 6D

【図６Ｅ】

図 6E



| | 要素ID | 長さ | 宛先MACアドレス | ソースMACアドレス | HLP MSDU |
|---|---|---|---|---|---|
| オクテット | 1 | 1 | 6 | 6 | 可変 |

650

652

654

656

658

FIG. 6E

【図７Ａ】

図 7A

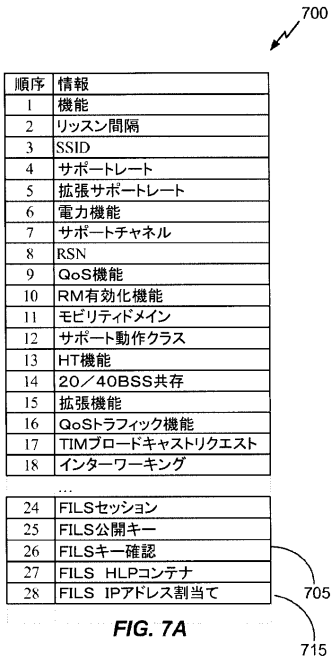



FIG. 7A

【図７Ｂ】

図 7B

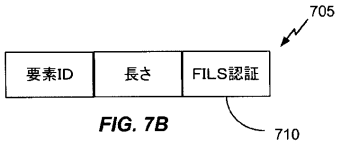



FIG. 7B

【図８】

図 8

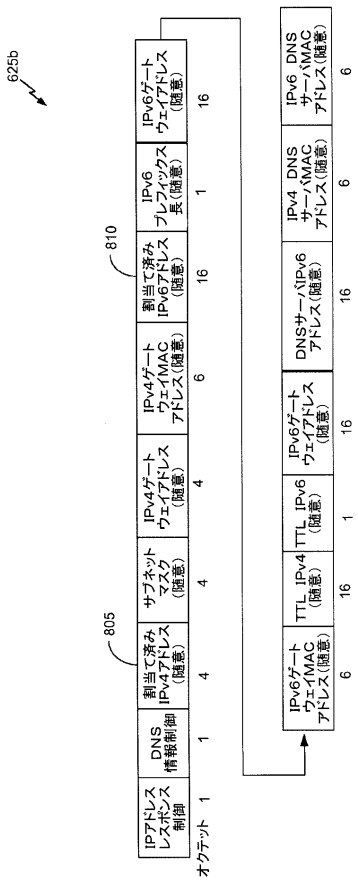



FIG. 8

【図９】

図 9

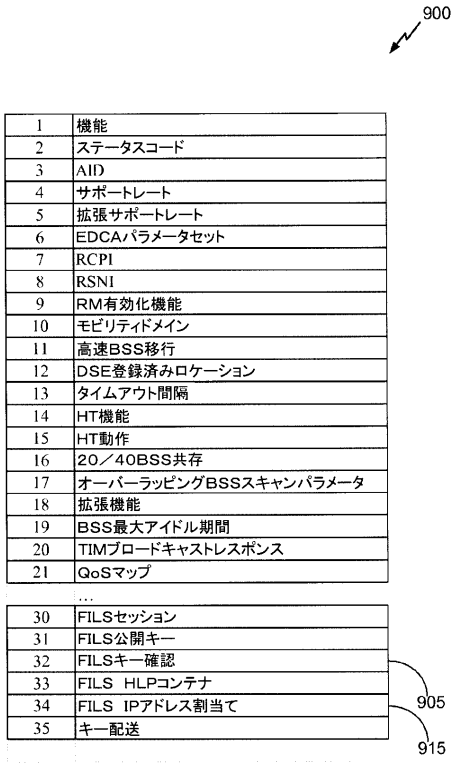



FIG. 9

【図１０】

図 10

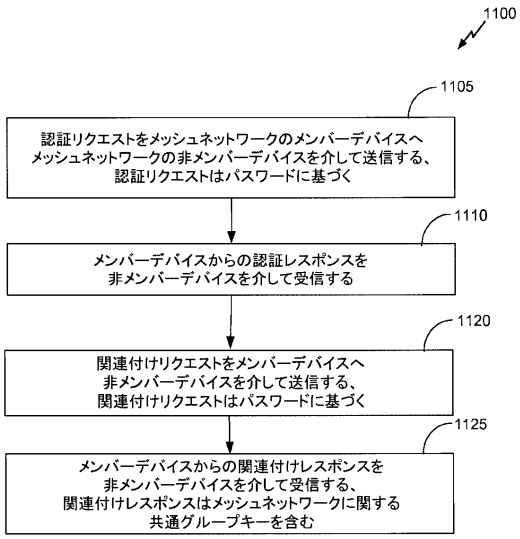



*FIG. 10*

【図１１】

図 11

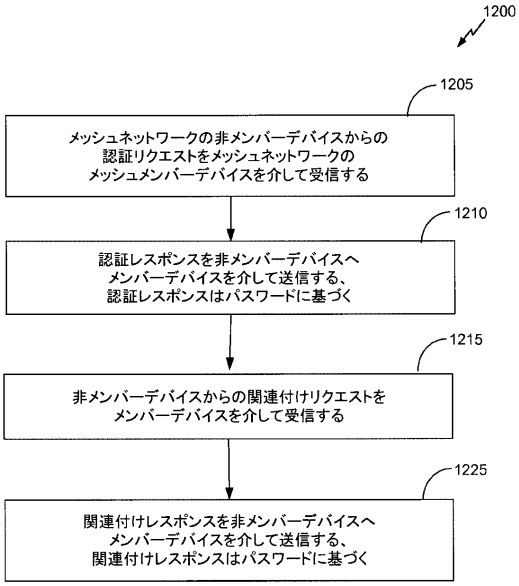



*FIG. 11*

【図１２】

図 12

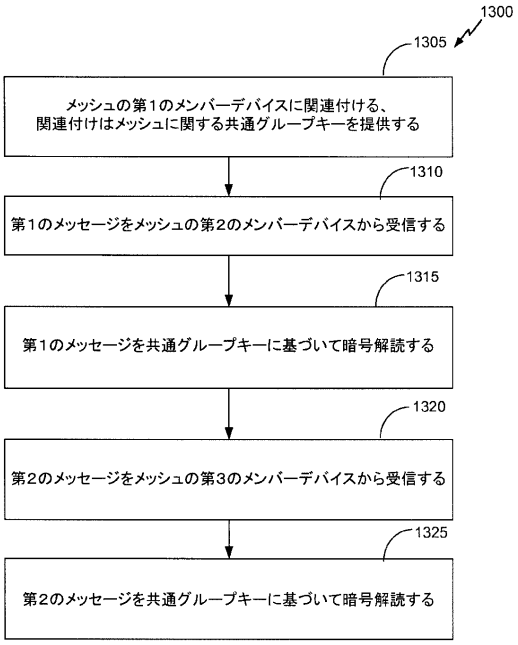



*FIG. 12*

【国際調査報告】

## INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/062421

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/08 H04W84/18
ADD.

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)
H04W

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)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | WO 2008/030705 A2 (MOTOROLA INC [US]; EMEOTT STEPHEN P [US]; BRASKICH ANTHONY J [US]) 13 March 2008 (2008-03-13)<br>paragraph [0001]<br>paragraph [0006]<br>paragraph [0033]<br>paragraph [0036]<br>paragraph [0048] - paragraph [0051]<br>paragraph [0106] - paragraph [0114]<br>----- | 1-88 |
| X | US 2005/032506 A1 (WALKER JESSE R [US]) 10 February 2005 (2005-02-10)<br>paragraph [0002]<br>paragraph [0021] - paragraph [0022]<br>paragraph [0026] - paragraph [0028]<br>paragraph [0030]<br>-----<br>-/-- | 1-88 |

[X] Further documents are listed in the continuation of Box C. [X] 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 |
|---|---|
| 10 February 2015 | 17/02/2015 |

| Name and mailing address of the ISA/ | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040,<br>Fax: (+31-70) 340-3016 | Oliveira, Joel |

Form PCT/ISA/210 (second sheet) (April 2005)

## INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/062421

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | WO 2007/111710 A2 (MOTOROLA INC [US]; BRASKICH ANTHONY J [US]; EMEOTT STEPHEN P [US]) 4 October 2007 (2007-10-04)<br>page 1, line 35 - page 2, line 24<br>page 3, line 6 - line 27<br>page 4, line 4 - page 5, line 20<br>5.3.3.1 WLAN Mesh Capability Element;<br>page 7<br>6.5.4 Fast Authentication Handshake;<br>page 8 | 1-88 |
| Y | ANDRE EGNERS ET AL: "Wireless Mesh Network security: State of affairs", LOCAL COMPUTER NETWORKS (LCN), 2010 IEEE 35TH CONFERENCE ON, IEEE, 10 October 2010 (2010-10-10), pages 997-1004, XP031986902,<br>DOI: 10.1109/LCN.2010.5735848<br>ISBN: 978-1-4244-8387-7<br>page 1001, column 1, line 15 - page 1002, column 1, line 4 | 1-88 |
| Y | HIERTZ G R ET AL: "IEEE 802.11s: The WLAN Mesh Standard", IEEE WIRELESS COMMUNICATIONS, IEEE SERVICE CENTER, PISCATAWAY, NJ, US, vol. 17, no. 1, 1 February 2010 (2010-02-01), pages 104-111, XP011303163,<br>ISSN: 1536-1284<br>Security in 802.11s;<br>page 108, column 2<br>Path Selection in 802.11s;<br>page 108, column 2 - page 109, column 1 | 1-88 |
| Y | DAN HARKINS ED - ANONYMOUS: "Simultaneous Authentication of Equals: A Secure, Password-Based Key Exchange for Mesh Networks", SENSOR TECHNOLOGIES AND APPLICATIONS, 2008. SENSORCOMM '08. SECOND INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 25 August 2008 (2008-08-25), pages 839-844, XP031319664,<br>ISBN: 978-0-7695-3330-8<br>the whole document | 1-88 |

-/--

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

## INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/062421

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | MD SHARIFUL ISLAM ET AL: "A Secure Hybrid Wireless Mesh Protocol for 802.11s Mesh Network", 30 June 2008 (2008-06-30), COMPUTATIONAL SCIENCE AND ITS APPLICATIONS - ICCSA 2008; [LECTURE NOTES IN COMPUTER SCIENCE], SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 972 - 985, XP019091476, ISBN: 978-3-540-69838-8 the whole document<br>----- | 9,10,21, 22,33, 34,45,46 |

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

## INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2014/062421

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| WO 2008030705 A2 | 13-03-2008 | AU 2007292554 A1 | 13-03-2008 |
| | | BR PI0716595 A2 | 03-12-2013 |
| | | CA 2662846 A1 | 13-03-2008 |
| | | CN 101529794 A | 09-09-2009 |
| | | EP 2067296 A2 | 10-06-2009 |
| | | JP 2010503330 A | 28-01-2010 |
| | | KR 20090051268 A | 21-05-2009 |
| | | RU 2009112635 A | 20-10-2010 |
| | | US 2008065884 A1 | 13-03-2008 |
| | | WO 2008030705 A2 | 13-03-2008 |
| US 2005032506 A1 | 10-02-2005 | CN 1846398 A | 11-10-2006 |
| | | CN 101917714 A | 15-12-2010 |
| | | CN 103973434 A | 06-08-2014 |
| | | EP 1671449 A1 | 21-06-2006 |
| | | MY 140228 A | 31-12-2009 |
| | | US 2005032506 A1 | 10-02-2005 |
| | | WO 2005022822 A1 | 10-03-2005 |
| WO 2007111710 A2 | 04-10-2007 | US 2008016350 A1 | 17-01-2008 |
| | | WO 2007111710 A2 | 04-10-2007 |

フロントページの続き

(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 パティル、アビシェク・プラモド
アメリカ合衆国、カリフォルニア州 ９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 リ、ソ・ボン
アメリカ合衆国、カリフォルニア州 ９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 チェリアン、ジョージ
アメリカ合衆国、カリフォルニア州 ９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 アブラハム、サントシュ・ポール
アメリカ合衆国、カリフォルニア州 ９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ ５７７５

Ｆターム(参考) 5J104 AA07 AA16 AA32 EA01 EA04 EA18 JA03 KA02 MA05 NA02
NA36 NA37 NA38 PA01
5K067 AA21 BB21 DD17 EE02 EE25 HH36
5K201 AA08 AA09 BB07 BD06 CB04 CB06 CB10 CB12 DA07 EB07
ED04