

(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2018-503323

(P2018-503323A)

(43) 公表日 平成30年2月1日(2018. 2. 1)

(51) Int.Cl.			F I			テーマコード (参考)
H04L	9/08	(2006.01)	H04L	9/00	601C	5J104
H04L	9/16	(2006.01)	H04L	9/00	601E	
			H04L	9/00	643	

審査請求 未請求 予備審査請求 未請求 (全 66 頁)

(21) 出願番号	特願2017-539291 (P2017-539291)	(71) 出願人	595020643
(86) (22) 出願日	平成28年1月27日 (2016. 1. 27)		クアルコム・インコーポレイテッド
(85) 翻訳文提出日	平成29年9月25日 (2017. 9. 25)		QUALCOMM INCORPORATED
(86) 国際出願番号	PCT/US2016/015196		
(87) 国際公開番号	W02016/123254		アメリカ合衆国、カリフォルニア州 92
(87) 国際公開日	平成28年8月4日 (2016. 8. 4)		121-1714、サン・ディエゴ、モア
(31) 優先権主張番号	62/108,374		ハウス・ドライブ 5775
(32) 優先日	平成27年1月27日 (2015. 1. 27)	(74) 代理人	100108855
(33) 優先権主張国	米国 (US)		弁理士 蔵田 昌俊
(31) 優先権主張番号	62/209,326	(74) 代理人	100109830
(32) 優先日	平成27年8月24日 (2015. 8. 24)		弁理士 福原 淑弘
(33) 優先権主張国	米国 (US)	(74) 代理人	100158805
(31) 優先権主張番号	15/006,881		弁理士 井関 守三
(32) 優先日	平成28年1月26日 (2016. 1. 26)	(74) 代理人	100112807
(33) 優先権主張国	米国 (US)		弁理士 岡田 貴志

最終頁に続く

(54) 【発明の名称】 データリンクグループのためのグループ鍵告知および配布

(57) 【要約】

ワイヤレス通信のためのデバイスは、データリンクグループに対応する候補グループ鍵を取得するように構成された鍵論理を含む。デバイスはまた、データリンクグループ用に指定されたページングウィンドウ中にデータリンクグループの1つまたは複数のデバイスに告知メッセージを送信するように構成されたワイヤレスインターフェースを含む。告知メッセージは、マルチキャストメッセージを含み、候補グループ鍵の利用可能性と告知メッセージとを示す。

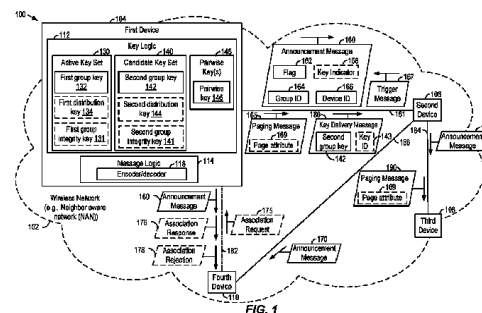


FIG. 1

【特許請求の範囲】**【請求項 1】**

ワイヤレス通信のためのデバイスであって、
データリンクグループに対応する候補グループ鍵を取得するように構成された鍵論理と

、
前記データリンクグループ用に指定されたページングウィンドウ中に前記データリンクグループの 1 つまたは複数のデバイスに告知メッセージを送信するように構成されたワイヤレスインターフェースと、ここにおいて、前記告知メッセージが、前記候補グループ鍵の利用可能性を示す、およびここにおいて、前記告知メッセージが、マルチキャストメッセージを備える、

10

を備えるデバイス。

【請求項 2】

前記ページングウィンドウが、送信ウィンドウの一部である、および、前記データリンクグループが、ネイバーアウェアネットワーク (NAN) またはワイヤレスメッシュネットワークの複数のデバイスを含む、請求項 1 に記載のデバイス。

【請求項 3】

アクティブ鍵セット、ペアワイズ鍵、候補鍵セット、またはそれらの組合せを記憶するように構成されたメモリと、ここにおいて、前記アクティブ鍵セットが、アクティブグループ鍵、アクティブ分布鍵、アクティブグループ完全性鍵、またはそれらの組合せを含む、

20

符号化された候補グループ鍵を生成するために前記候補グループ鍵を符号化するように構成されたエンコーダと、ここにおいて、前記エンコーダが、前記アクティブグループ鍵、前記アクティブ配布鍵、または前記ペアワイズ鍵に基づいて前記候補グループ鍵を符号化するように構成された、

をさらに備える、請求項 1 に記載のデバイス。

【請求項 4】

前記ワイヤレスインターフェースが、ユニキャストメッセージとして前記データリンクグループの第 2 のデバイスに前記候補グループ鍵を送信するように構成された、請求項 1 に記載のデバイス。

【請求項 5】

前記候補グループ鍵を含む第 2 のマルチキャストメッセージを生成するように構成されたメッセージ論理、前記第 2 のマルチキャストメッセージが、パブリックアクションフレームまたはデータリンクグループメッセージを備える、をさらに備え、ここにおいて、前記ワイヤレスインターフェースが、前記 1 つまたは複数のデバイスに前記第 2 のマルチキャストメッセージを送信するように構成された、請求項 1 に記載のデバイス。

30

【請求項 6】

前記ワイヤレスインターフェースが、前記告知メッセージの送信の後に前記データリンクグループの特定のデバイスから第 2 の告知メッセージを受信するようにさらに構成された、前記第 2 の告知メッセージが、第 2 の候補グループ鍵を示す、および、前記鍵論理が

40

、
前記第 2 の候補グループ鍵が前記候補グループ鍵よりも高い優先度を有するという決定に応答して前記第 2 の候補グループ鍵を選択することと、

第 1 のグループ鍵のアクティブグループ鍵としての満了の後に、前記第 2 の候補グループ鍵を前記アクティブグループ鍵として設定することと

を行うように構成された、請求項 1 に記載のデバイス。

【請求項 7】

前記鍵論理が、

前記候補グループ鍵に関係する第 1 の鍵インジケータに基づいて前記候補グループ鍵の第 1 の優先度を決定することと、ここにおいて、前記第 1 の鍵インジケータが、媒体アクセス制御 (MAC) アドレス、ハッシュ値、タイムスタンプ、またはそれらの組合せを含

50

む、ここにおいて、前記ハッシュ値が、前記MACアドレス、前記候補グループ鍵、またはその両方に基づいて生成される、

前記第2の告知メッセージ中に含まれる鍵インジケータに基づいて前記第2の候補グループ鍵の第2の優先度を決定することと、

第1の優先度と前記第2の優先度との比較に基づいて前記第2の候補グループ鍵が前記候補グループ鍵よりも高い優先度を有することを決定することと

を行うように構成された、請求項6に記載のデバイス。

【請求項8】

前記ワイヤレスインターフェースが、前記候補グループ鍵を含む鍵配信メッセージを送信するようにさらに構成された、ここにおいて、前記鍵配信メッセージが、前記候補グループ鍵の有効期限を示す鍵識別子を含む、および、前記鍵論理が、前記有効期限より前に第2の候補グループ鍵を生成するように構成された、請求項1に記載のデバイス。

【請求項9】

前記候補グループ鍵が、鍵配信メッセージ中に含まれる、および、前記鍵配信メッセージが、鍵識別番号、鍵インデックス、またはその両方を含む、ここにおいて、前記鍵インデックスが、非アクティブグループ鍵とアクティブグループ鍵とを示す、およびここにおいて、前記鍵インデックスにより、前記データリンクグループのデバイスが前記アクティブグループ鍵を決定することが可能になる、請求項1に記載のデバイス。

【請求項10】

ワイヤレス通信のための方法であって、

データリンクグループの第1のデバイスにおいて候補グループ鍵を取得することと、

前記データリンクグループの前記第1のデバイスから第2のデバイスに、前記候補グループ鍵の利用可能性を示す告知メッセージを送信することと、ここにおいて、前記告知メッセージが、前記データリンクグループ用に指定されたページングウィンドウ中に送信される、およびここにおいて、前記告知メッセージが、マルチキャストメッセージを備える、

を備える方法。

【請求項11】

前記第1のデバイスが、前記第1のデバイスにおいて前記候補グループ鍵を生成することによって、または前記データリンクグループの別のデバイスから前記第1のデバイスにおいて前記候補グループ鍵を受信することによって前記候補グループ鍵を取得する、および、前記候補グループ鍵により、前記データリンクグループに対応するグループアドレス指定されたデータメッセージの暗号化または解読のうちの少なくとも1つが可能になる、請求項10に記載の方法。

【請求項12】

前記候補グループ鍵を取得するより前に、

前記データリンクグループの第3のデバイスから第2の告知メッセージを受信することと、ここにおいて、前記第2の告知メッセージは、前記候補グループ鍵が利用可能であることを示す、

前記候補グループ鍵を要求するために前記データリンクグループに対応する要求を送ることと

を行うことをさらに備える、請求項10に記載の方法。

【請求項13】

前記告知メッセージが、鍵インジケータ、前記データリンクグループのデータリンクグループ識別子、前記候補グループ鍵を生成した特定のデバイスのデバイス識別子、またはそれらの組合せを含む、請求項10に記載の方法。

【請求項14】

前記鍵インジケータが、前記第1のデバイスの媒体アクセス制御(MAC)アドレス、ハッシュ値、前記候補グループ鍵の生成に対応するタイムスタンプ、またはそれらの組合せを備える、ここにおいて、前記ハッシュ値が、前記MACアドレス、前記候補グループ

鍵、またはその両方に基づいて生成される、および、前記デバイス識別子が、前記特定のデバイスの第2のMACアドレスを含む、請求項13に記載の方法。

【請求項15】

前記第1のデバイスが前記告知メッセージを送信するとき、前記第1のデバイスが、前記第2のデバイスに関連する、

前記第2のデバイスから前記第1のデバイスにおいて、前記第1のデバイスから前記第2のデバイスに前記候補グループ鍵を送ることを求める要求を受信することと、

ペアワイズ鍵を使用して前記候補グループ鍵を暗号化した後に前記第1のデバイスから前記第2のデバイスに前記候補グループ鍵を送ることと、ここにおいて、前記ペアワイズ鍵により、前記第1のデバイスと前記第2のデバイスとの間のセキュアな通信が可能になる、

10

をさらに備える、請求項10に記載の方法。

【請求項16】

前記告知メッセージを送信した後に、前記第2のデバイスに関連付けることを前記第1のデバイスに求める要求を受信することと、

前記第2のデバイスとのセキュリティ関連付けを行うことと、ここにおいて、前記第1のデバイスと前記第2のデバイスとに対応するペアワイズ鍵が、前記セキュリティ関連付け中に生成される、

前記セキュリティ関連付けの完了の後に、前記第2のデバイスに前記候補グループ鍵を送ることを前記第1のデバイスに求める第2の要求を受信することと

20

をさらに備える、請求項10に記載の方法。

【請求項17】

前記第1のデバイスが、前記データリンクグループの鍵生成器デバイスとして動作する、および、前記データリンクグループの他のデバイスは、前記第1のデバイスが前記鍵生成器デバイスとしての動作を中止するより前に鍵生成器デバイスとして動作しない、

前記データリンクグループの前記第1のデバイスから前記第2のデバイスにメッセージを送信することと、前記メッセージは、前記第2のデバイスが、前記データリンクグループの前記鍵生成器デバイスとして動作すべきであることを示す、

前記第1のデバイスにおいて鍵生成動作を終了することと、

前記第1のデバイスによって前記データリンクグループとの関連付けを解除すること、前記第1のデバイスにおいて低電力動作モードに遷移すること、またはその両方を行うことと

30

を行うことをさらに備える、請求項16に記載の方法。

【請求項18】

ワイヤレス通信のためのデバイスであって、

データリンクグループ用に指定されたページングウィンドウ中に第1の通信チャネルを監視するように構成された鍵論理と、

前記ページングウィンドウ中に前記データリンクグループの第1のデバイスから告知メッセージを受信するように構成されたワイヤレスインターフェースと、前記告知メッセージが、候補グループ鍵の利用可能性を示す、ここにおいて、前記告知メッセージが、マルチキャストメッセージを備える、

40

を備えるデバイス。

【請求項19】

前記ワイヤレスインターフェースが、符号化された候補グループ鍵を含む鍵配信メッセージを受信するようにさらに構成された、

アクティブ鍵セット、ペアワイズ鍵、候補鍵セット、またはそれらの組合せを記憶するように構成されたメモリと、ここにおいて、前記候補鍵セットが、前記候補グループ鍵、候補配布鍵、候補グループ完全性鍵、またはそれらの組合せを含む、

アクティブグループ鍵、アクティブ配布鍵、またはペアワイズ鍵に基づいて前記候補グループ鍵を生成するために前記符号化された候補グループ鍵を復号するように構成され

50

たデコーダと

をさらに備える、請求項 18 に記載のデバイス。

【請求項 20】

前記符号化された候補グループ鍵を生成するために前記候補グループ鍵を符号化するように構成されたエンコーダをさらに備える、ここにおいて、前記エンコーダが、前記アクティブグループ鍵、前記アクティブ配布鍵、または前記ペアワイズ鍵に基づいて前記候補グループ鍵を符号化するように構成された、およびここにおいて、前記鍵論理が、前記アクティブ鍵セット中に含まれるアクティブ完全性グループ鍵に基づいてグループアドレス指定されたトラフィックを検証するようにさらに構成された、請求項 19 に記載のデバイス。

10

【請求項 21】

ワイヤレス通信のための方法であって、

データリンクグループの第 2 のデバイスにおいて、前記データリンクグループ用に指定されたページングウィンドウ中に第 1 の通信チャネルを監視することと、

前記ページングウィンドウ中に前記データリンクグループの第 1 のデバイスから前記第 2 のデバイスにおいて告知メッセージを受信することと、前記告知メッセージが、候補グループ鍵の利用可能性を示す、ここにおいて、前記告知メッセージが、マルチキャストメッセージを備える、

を備える方法。

【請求項 22】

前記候補グループ鍵を取得することをさらに備える、ここにおいて、前記候補グループ鍵を取得することが、

前記ページングウィンドウ中に前記告知メッセージを受信したことに応答して前記第 1 のデバイスにトリガメッセージを送信することと、

データウィンドウ中に前記第 1 のデバイスから前記候補グループ鍵を受信することとを備える、請求項 21 に記載の方法。

20

【請求項 23】

カウンタを更新することと、前記カウンタが、前のグループ鍵の満了に関係する、

前記カウンタが特定の値に達するより前に前記告知メッセージを受信したことに応答して前記カウンタを更新することを停止することと、前記特定の値が、前記第 2 のデバイスによる新しいグループ鍵の生成に関係する、

をさらに備える、請求項 21 に記載の方法。

30

【請求項 24】

前記告知メッセージ中に含まれる第 1 の鍵インジケータを識別することと、

前記ページングウィンドウ中に前記データリンクグループの第 3 のデバイスから第 2 の告知メッセージを受信することと、前記第 2 の告知メッセージが、第 2 の鍵インジケータを含み、第 2 の候補グループ鍵の生成を示す、

前記第 2 の鍵インジケータよりも高い優先度を有する前記告知メッセージの前記第 1 の鍵インジケータに基づいて前記第 1 のデバイスにトリガメッセージを送信することと、

前記第 1 のデバイスから前記候補グループ鍵を受信することと

をさらに備える、請求項 21 に記載の方法。

40

【請求項 25】

前記告知メッセージを受信する前に、第 2 の候補グループ鍵の生成を開始することと、

前記告知メッセージを受信したことに応答して、前記第 2 の候補グループ鍵の生成を停止することと

をさらに備える、請求項 21 に記載の方法。

【請求項 26】

前記告知メッセージを受信したことに応答して、前記データリンクグループのデバイスに前記告知メッセージを再送信することをさらに備える、請求項 21 に記載の方法。

【請求項 27】

50

前記告知メッセージを受信したことに応答して、前記第 2 のデバイスが前記第 1 のデバイスに関連するのかどうかを決定することと、

前記第 1 のデバイスが前記第 2 のデバイスに関連するという決定に応答して、前記第 1 のデバイスに前記候補グループ鍵を要求することと

をさらに備える、請求項 2 1 に記載の方法。

【請求項 2 8】

前記告知メッセージを受信したことに応答して、前記第 2 のデバイスが前記第 1 のデバイスに関連するのかどうかを決定することと、

前記第 2 のデバイスが前記第 1 のデバイスに関連しないという決定に応答して、

前記候補グループ鍵を受信した、前記第 2 のデバイスに関連する前記データリンクグループの第 3 のデバイスを識別することと、ここにおいて、前記第 3 のデバイスが、前記データリンクグループのアクティブグループ鍵の満了より前に終了する時間期間中に識別される、ここにおいて、前記時間期間が、前記告知メッセージを受信された後に開始し、前記アクティブグループ鍵の前記満了の前の所定の時間に終了する、

前記第 3 のデバイスに前記候補グループ鍵を要求することと、

前記アクティブグループ鍵の前記満了より前に前記第 3 のデバイスから前記候補グループ鍵を受信することと

をさらに備える、請求項 2 1 に記載の方法。

【請求項 2 9】

前記第 2 のデバイスが前記第 1 のデバイスに関連しないという決定に応答して前記第 3 のデバイスとのセキュリティ関連付けを実行することと、ここにおいて、前記セキュリティ関連付けがペアワイズ鍵を確立する、

前記第 3 のデバイスから符号化された候補グループ鍵を受信することと、

第 2 のデバイスにおいて前記候補グループ鍵を生成するために前記ペアワイズ鍵に基づいて前記符号化された候補グループ鍵を復号することと、

メモリにおいて前記候補グループ鍵を記憶することと

をさらに備える、請求項 2 8 に記載の方法。

【請求項 3 0】

前記第 2 のデバイスが前記第 1 のデバイスに関連しないという決定に応答して、

前記データリンクグループのアクティブグループ鍵の満了の前の所定の時間を識別することと、

前記所定の時間の前に、前記データリンクグループの少なくとも 1 つのデバイスに前記候補グループ鍵についてのマルチキャスト要求を送ることと、

前記マルチキャスト要求に応答して前記データリンクグループの第 3 のデバイスから前記候補グループ鍵を受信することと

を行うことをさらに備える、請求項 2 1 に記載の方法。

【発明の詳細な説明】

【技術分野】

【0001】

優先権の主張

[0001]本出願は、下記の出願の各々の内容全体が参照により本明細書に明確に組み込まれる、同一出願人が所有する、2015年1月27日に出願された「GROUP KEY ANNOUNCEMENT AND / OR DISTRIBUTION FOR A GROUP」と題する米国仮特許出願番-号第62 / 108,374号、2015年8月24日に出願された「GROUP KEY ANNOUNCEMENT AND DISTRIBUTION FOR A GROUP」と題する米国仮特許出願番号第62 / 209,326号、および2016年1月26日に出願された「GROUP KEY ANNOUNCEMENT AND DISTRIBUTION FOR A DATA LINK GROUP」と題する米国非仮特許出願番号第15 / 006,881号の優先権を主張する。

10

20

30

40

50

【 0 0 0 2 】

[0002]本開示は、概して、グループ鍵の告知および配布に関する。

【 背景技術 】

【 0 0 0 3 】

[0003]ネイバーアウェアネットワーク（NAN：neighbor aware network）またはワイヤレスメッシュネットワークのデータリンクグループ中に含まれるデバイスは、グループアドレス指定されたトラフィックを暗号化するためにグループ鍵（たとえば、共通グループ鍵）などのセキュリティ証明を使用する。セキュリティの理由のために、データリンクグループのデバイスによって使用される特定のグループ鍵（たとえば、アクティブグループ鍵）は、対応する時間期間の後に満了する。周期的に、新しいグループ鍵が、生成され、データリンクグループの各デバイスにセキュアに配布される。例示のために、新しいグループ鍵を生成する特定のデバイスは、データリンクグループの他のデバイスに鍵告知メッセージを送り得、ピア交換メッセージング（たとえば、ポイントツーポイント（P2P）通信）を使用してデータリンクグループの1つまたは複数のデバイス（たとえば、1つまたは複数の隣接デバイス）に新しいグループ鍵を送り得る。新しいグループ鍵は、追加の関連付け動作とデータリンクグループ中のデバイス間のユニキャストメッセージ交換とを使用してデータリンクグループの各デバイスに配布され得る。グループ鍵を配布するために関連付け動作またはユニキャストメッセージ交換を実行することは、NANまたはワイヤレスメッシュネットワークに有意なトラフィックおよびオーバーヘッドを追加し得る。

10

20

【 発明の概要 】

【 0 0 0 4 】

[0004]特定の態様では、デバイスは、データリンクグループに対応する候補グループ鍵を取得するように構成された鍵論理を含む。本デバイスはまた、データリンクグループ用に指定されたページングウィンドウ中にデータリンクグループの1つまたは複数のデバイスに告知メッセージを送信するように構成されたワイヤレスインターフェースを含む。告知メッセージは、マルチキャストメッセージを含み、候補グループ鍵の利用可能性を示す。

【 0 0 0 5 】

[0005]別の特定の態様では、方法は、データリンクグループの第1のデバイスにおいて候補グループ鍵を取得することを含む。本方法は、データリンクグループの第1のデバイスから第2のデバイスに、候補グループ鍵の利用可能性を示す告知メッセージを送信することをさらに含む。告知メッセージは、マルチキャストメッセージを含み、データリンクグループ用に指定されたページングウィンドウ中に送信される。

30

【 0 0 0 6 】

[0006]特定の態様では、デバイスは、データリンクグループ用に指定されたページングウィンドウ中に第1の通信チャネルを監視するように構成された鍵論理を含む。本デバイスはまた、ページングウィンドウ中にデータリンクグループの第1のデバイスから告知メッセージを受信するように構成されたワイヤレスインターフェースを含む。告知メッセージは、マルチキャストメッセージを含み、候補グループ鍵の利用可能性を示す。

40

【 0 0 0 7 】

[0007]別の特定の態様では、方法は、データリンクグループの第2のデバイスにおいて、データリンクグループ用に指定されたページングウィンドウ中に第1の通信チャネルを監視することを含む。本方法は、ページングウィンドウ中にデータリンクグループの第1のデバイスから第2のデバイスにおいて告知メッセージを受信することをさらに含む。告知メッセージは、マルチキャストメッセージを含み、候補グループ鍵の利用可能性を示す。

【 0 0 0 8 】

[0008]別の特定の態様では、デバイスは、データリンクグループに対応する候補グループ鍵を取得するように構成された鍵論理を含む。本デバイスはまた、第1の通信チャネル

50

の発見ウィンドウ中にデータリンクグループの１つまたは複数のデバイスに告知メッセージを送信するように構成されたワイヤレスインターフェースを含む。告知メッセージは、マルチキャストメッセージを含み、候補グループ鍵の利用可能性を示す。

【０００９】

【0009】別の特定の態様では、方法は、データリンクグループの第１のデバイスにおいて候補グループ鍵を取得することを含む。本方法は、データリンクグループの第１のデバイスからデバイスに、利用可能性候補グループ鍵を示す告知メッセージを送信することをさらに含む。告知メッセージは、マルチキャストメッセージを含み、発見ウィンドウ中に第１の通信チャネルを介して送信される。

【００１０】

10

【0010】別の特定の態様では、デバイスは、データリンクグループに対応する発見ウィンドウ中に第１の通信チャネルを監視するように構成された鍵論理を含む。本デバイスはまた、発見ウィンドウ中にデータリンクグループの第１のデバイスから告知メッセージを受信するように構成されたワイヤレスインターフェースを含む。告知メッセージは、マルチキャストメッセージを含み、候補グループ鍵の利用可能性を示す。

【００１１】

【0011】別の特定の態様では、方法は、データリンクグループの第２のデバイスにおいて、データリンクグループに対応する発見ウィンドウ中に第１の通信チャネルを監視することを含む。本方法は、発見ウィンドウ中にデータリンクグループの第１のデバイスから第２のデバイスにおいて告知メッセージを受信することをさらに含む。告知メッセージは、マルチキャストメッセージを含み、候補グループ鍵の利用可能性を示す。

20

【図面の簡単な説明】

【００１２】

【図１】【0012】告知メッセージの送信とデータリンクグループのグループ鍵の配布とをサポートするシステムの特定の実装形態の図。

【図２】【0013】候補グループ鍵を生成するように構成されたデバイスのブロック図。

【図３】【0014】データリンクグループに対応する通信の例示的な例のタイミング図。

【図４】【0015】配布鍵を使用する例示的な方法のラダー図。

【図５】【0016】データリンクグループに対応する通信の例示的な例のタイミング図。

【図６】【0017】ページ属性フィールドの態様の例示的な例の図。

30

【図７】【0018】データリンクグループのデバイスにおける動作の第１の例示的な方法のフロー図。

【図８】【0019】データリンクグループのデバイスにおける動作の第２の例示的な方法のフロー図。

【図９】【0020】データリンクグループのデバイスにおける動作の第３の例示的な方法のフロー図。

【図１０】【0021】データリンクグループのデバイスにおける動作の第４の例示的な方法のフロー図。

【図１１】【0022】データリンクグループのデバイスにおける動作の第５の例示的な方法のフロー図。

40

【図１２】【0023】データリンクグループのデバイスにおける動作の第６の例示的な方法のフロー図。

【図１３】【0024】本明細書で開示する１つまたは複数の方法、システム、装置、およびコンピュータ可読媒体の様々な実装形態をサポートするように動作可能であるワイヤレスデバイスの図。

【発明を実施するための形態】

【００１３】

【0025】本開示の特定の实装形態について、図面を参照しながら以下で説明する。説明では、共通の特徴は、図面全体にわたって共通の参照番号によって指定される。本明細書では、構造、構成要素、動作などの要素を修正するのに使用される順序を示す用語（たとえ

50

ば、「第1の」、「第2の」、「第3の」など)は、それ自体、別の要素に関する要素の優先順位または順序を示しておらず、要素を、(順序を示す用語の使用を別にすれば)同じ名前を有する別の要素から区別しているだけである。

【0014】

[0026]本明細書では、様々な用語は、特定の実装形態を記述するためのものにすぎず、実装形態を制限するものではない。たとえば、単数形「a」、「an」および「the」は、文脈が別段に明確に示すのでなければ、複数形をも含むものとする。さらに、「備える」および「備えている」という用語が、「含む」または「含んでいる」と互換的に使用され得ることが理解され得る。さらに、「ここにおいて」という用語が「ここで」という用語と互換的に使用され得ることを理解されよう。

10

【0015】

[0027]本開示では、ネイバーアウェアネットワーク(NAN)またはワイヤレスメッシュネットワークのデータリンクグループ中のデバイスは、新しいグループ鍵(または候補グループ鍵)などのグループ鍵を告知し、配布し得る。データリンクグループの第1のデバイスは、データリンクグループの1つまたは複数のデバイスに告知メッセージを送信し得る。たとえば、第1のデバイスは、データリンクグループに対応するグループ送信ウィンドウのページングウィンドウ中にマルチキャストメッセージとして告知メッセージを送り得る。別の例として、告知メッセージは、NANに対応する発見ウィンドウ中に送られ得る。告知メッセージは、候補グループ鍵(たとえば、潜在的に「次の」アクティブグループ鍵)の利用可能性を示すフラグを含み得る。データリンクグループの各デバイスは、ページングウィンドウ中に起動している(たとえば、アクティブモードにある)ことがあり、これは、第1のデバイスの隣接デバイスが告知メッセージを受信する可能性を増加させ得る。

20

【0016】

[0028]データリンクグループの第2のデバイスは、第1のデバイスから告知メッセージを受信し得、告知メッセージに応答して、第2のデバイスは、第2のデバイスが第1のデバイスに関連するのかどうかを決定し得る。第2のデバイスが第1のデバイスに関連する(たとえば、第1のデバイスと第2のデバイスとが、認証プロシージャなどのセキュリティ関連付けをうまく完了し、セキュアなピアツーピア(P2P)通信のためのペアワイズ鍵を確立した)場合、第2のデバイスは、P2P通信を介して第1のデバイスから候補グループ鍵を受信し得る。

30

【0017】

[0029]第1のデバイスと第2のデバイスとが関連しない場合、第2のデバイスは、第2のデバイスに関連する第3のデバイスから(候補グループ鍵に対応する)第2の告知メッセージを受信するのを待ち得る。たとえば、第2のデバイスに関連しない第1のデバイスから告知メッセージを受信した後に、第2のデバイスは、第2のデバイスに関連する第3のデバイスから第2の告知メッセージを受信するのを待ち得る。第2の告知メッセージを受信したことに応答して、第2のデバイスは、第3のデバイスに候補グループ鍵を要求し得る。第2のデバイスは、データリンクグループのアクティブグループ鍵が満了するよう設定される前の所定の時間まで、関連するデバイスから第2の告知メッセージを受信するのを待ち得る。例示のために、所定の時間が検出されると、アクティブグループ鍵の満了が間近であると見なされ、第2のデバイスは、第1のデバイスなどの関連しないデバイスとセキュリティ関連付けを開始し得、新たに関連したデバイス(たとえば、第1のデバイス)に候補グループ鍵を要求し得る。所定の時間が検出されるまで、関連するデバイスから告知メッセージを受信するのを待つことによって、第2のデバイスは、告知メッセージに応答して第1のデバイスとのセキュリティ関連付けを自動的に開始しない。したがって、候補グループ鍵を取得するためにセキュリティ関連付けを行う(たとえば、認証プロシージャを実行する)1つまたは複数のデバイスに対応するトラフィックの量は、告知メッセージを送ったデバイスに自動的に関連付けられ、それにグループ鍵を要求するデータリンクグループのデバイスと比較して低減され得る。

40

50

【 0 0 1 8 】

[0030] 図 1 を参照すると、データリンクグループの 1 つまたは複数のデバイスを含むシステム 1 0 0 の特定の実装形態が示されている。システム 1 0 0 は、データリンクグループのグループ鍵の配布とグループ鍵に対応する告知メッセージの送信とをサポートする N A N またはワイヤレスメッシュネットワークなどのワイヤレスネットワーク 1 0 2 を含む。ワイヤレスネットワーク 1 0 2 はまた、1 つまたは複数のデータリンクグループを含むかまたはそれに対応し得る。

【 0 0 1 9 】

[0031] ワイヤレスネットワーク 1 0 2 は、第 1 のデバイス 1 0 4、第 2 のデバイス 1 0 6、第 3 のデバイス 1 0 8、および第 4 のデバイス 1 1 0 などの 1 つまたは複数のデバイスを含み得る。デバイス 1 0 4 ~ 1 1 0 の各々は、ワイヤレスネットワーク 1 0 2 中に含まれる 1 つまたは複数の他のワイヤレス通信デバイスにデータを送信し、それからデータを受信するように構成されたワイヤレス通信デバイスであり得る。各ワイヤレスデバイスは、ワイヤレスネットワーク 1 0 2 の無線局またはワイヤレス通信デバイスなどの局を含むか、またはそれに対応し得る。ワイヤレスネットワーク 1 0 2 は、インフラストラクチャネットワークまたはピアツーピアネットワーク（たとえば、アドホックネットワーク）などのインフラストラクチャを伴わないネットワークであり得る。たとえば、ワイヤレスネットワーク 1 0 2（たとえば、N A N）のデバイス 1 0 4 ~ 1 1 0 の各々は、N A N に対応する 1 つまたは複数のワイヤレスチャネルを介して、関連付け動作（たとえば、セキュリティ関連付け動作）、セキュリティ情報交換動作、同期動作、および他の動作を実行するように構成され得る。いくつかの実装形態では、デバイス 1 0 4 ~ 1 1 0 は、例示的な非限定的な例として、電気電子技術者協会（I E E E）8 0 2 . 1 1 規格（たとえば、I E E E 8 0 2 . 1 1 s の規格）、W i - F i A l l i a n c e（登録商標）規格、N A N 規格、またはそれらの組合せなどの 1 つまたは複数の規格に従ってそのような動作を実行し得る。ワイヤレスネットワーク 1 0 2 が 4 つのデバイスを含むものとして示されているが、他の実装形態では、ワイヤレスネットワーク 1 0 2 は 5 つ以上のデバイスを含むことも、3 つ以下のデバイスを含むこともある。

【 0 0 2 0 】

[0032] ワイヤレスネットワーク 1 0 2 は、1 つまたは複数のデータリンクグループ（たとえば、1 つまたは複数のメッシュ）を含むか、またはそれに対応し得る。本明細書で使用するデータリンクグループは、アドホックネットワークなど、インフラストラクチャを伴わないピアツーピアネットワークを含み得る。データリンクグループは、分散型ワイヤレスネットワークなどのネットワークを形成することができる複数のデバイスを含み得る。さらに、データリンクグループの各デバイスは、データリンクグループによって使用される 1 つまたは複数の通信チャネルとともにインバンドまたはアウトオブバンドで交換され得る共通のセキュリティ証明を使用し得る。いくつかの実装形態では、データリンクグループのデバイスは、トラフィックおよび他のメッセージを広告および受信するためにデバイスの各々が起動する時間期間などの周期的な起動時間を有するように同期され得る。

【 0 0 2 1 】

[0033] ワイヤレスネットワーク 1 0 2 は、デバイス 1 0 4 ~ 1 1 0 などの 1 つまたは複数のデバイスを含むデータリンクグループを含むか、またはそれに対応し得る。データリンクグループは、データリンク、データリンクネットワーク、グループネットワーク、N A N データリンク（N D L）、N D L ネットワーク、データバスグループ、データバスグループネットワーク、N A N データバス、N A N データバスグループ、または N A N データバスグループネットワークと呼ばれることもある。いくつかの実装形態では、データリンクグループは、例示的な非限定的な例として、「ソーシャル W i - F i（登録商標）メッシュネットワーク」または米国電気電子学会（I E E E）8 0 2 . 1 1 s メッシュネットワークなどのメッシュネットワーク中に含まれるメッシュグループであり得る。別の例として、データリンクグループは、インフラストラクチャ不要のピアツーピア（p 2 p）

10

20

30

40

50

ネットワークを含み得る。

【0022】

[0034] データリンクグループの一部として、データリンクグループのデバイス104～110は、（たとえば、1つまたは複数のワイヤレスキャリア、1つまたは複数のWi-Fiアクセスポイント、インターネット、またはそれらの組合せを伴うことなしに）ワイヤレス通信を介してデータ交換を実行し得る。たとえば、データリンクグループのデバイス104～110は、通信を可能にするためにグループ鍵（たとえば、共通のグループ鍵）などのセキュリティ証明を共有し得る。例示のために、データリンクグループの各デバイスは、グループメッセージを符号化および復号するためにグループ鍵を使用し得る。いくつかの実装形態では、音楽サービス、ソーシャルメディア共有サービス、ファイル共有サービス、ゲームサービス、または他のサービスなどの1つまたは複数のサービスが、データリンクグループのデバイス104～110のうちの1つまたは複数によって与えられ得る。いくつかの実装形態では、データリンクグループのデバイス104～110は、デバイス104～110の各々がサービスを広告するために、トラフィックまたは他のメッセージを受信するために、あるいはそれらの組合せのために（たとえば、アクティブ動作モードで）「起動」している時間期間などの周期的な起動時間を有するように同期され得る。いくつかの実装形態では、ワイヤレスネットワーク102は、複数のデータリンクグループを含み得、ワイヤレスネットワーク102の各データリンクグループは、一意の値（たとえば、バイト値、グループアドレス、またはそれらの組合せ）などの対応するグループ識別子を有し得る。ワイヤレスネットワーク102が複数のデータリンクグループを含むとき、特定のデバイスは、2つ以上のデータリンクグループ中に含まれ得る。ワイヤレスネットワーク102がデータリンクグループ中に含まれる4つのデバイスを有するものとして記述されているが、他の実装形態では、ワイヤレスネットワーク102は5つ以上のデバイスを含むことも、3つ以下のデバイスを含むこともある。

【0023】

[0035] 第1のデバイス104は、鍵論理112とメッセージ論理114とを含み得る。鍵論理112は、アクティブ鍵セット130と、候補鍵セット140と、1つまたは複数のペアワイズ鍵145とを含むこと（または記憶すること）を行い得る。アクティブ鍵セット130は、データリンクグループに対応する、データリンクグループのデバイスによって使用されるように設定される1つまたは複数の鍵を含み得る。例示のために、アクティブ鍵セット130は、第1のグループ鍵132、第1の配布鍵134、第1のグループ完全性鍵131、またはそれらの組合せを含み得る。特定の实装形態では、アクティブ鍵セット130は、鍵131、132、および134のうちの2つを含み得、2つの鍵は、鍵ペアと呼ばれることがある。別の特定の实装形態では、アクティブ鍵セット130は、鍵131、132、および134のすべてを含み得、3つの鍵は、鍵トリオと呼ばれることがある。同様に、候補鍵セット140は、第2のグループ鍵142、第2の配布鍵144、第2のグループ完全性鍵141、またはそれらの組合せを含み得る。単一のアクティブ鍵セット130および単一の候補鍵セット140として説明されるが、いくつかの実装形態では、鍵論理112は、複数のアクティブ鍵セット、複数の候補鍵セット、またはその両方を記憶するように構成され得る。たとえば、鍵論理112は、第1のデータリンクグループに対応する第1のアクティブ鍵セットと第2のデータリンクグループに対応する第2のアクティブ鍵セットとを記憶するように構成され得る。

【0024】

[0036] アクティブ鍵セット130は、データリンクグループのアクティブグループ鍵として設定される第1のグループ鍵132を含み得る。第1のグループ鍵132により、データリンクグループのデバイス間で通信されるデータリンクグループメッセージの暗号化（または符号化）と解読（または復号）とが可能になり得る。

【0025】

[0037] 随意に、アクティブ鍵セット130は、データリンクグループのアクティブ配布鍵として設定される第1の配布鍵134を含み得る。第1の配布鍵134は、第1のグル

ープ鍵 1 3 2 と第 1 の配布鍵 1 3 4 とが第 1 の鍵ペアを構成するように第 1 のグループ鍵 1 3 2 に対応し得る。第 1 の配布鍵 1 3 4 がアクティブ配布鍵として設定されると、第 1 の配布鍵 1 3 4 は、本明細書でさらに説明するように、データリンクグループの他のデバイスに通信されるべき候補グループ鍵、候補配布鍵、候補グループ完全性鍵、またはそれらの組合せを暗号化するために使用され得る。

【0026】

[0038]さらに、アクティブ鍵セット 1 3 0 は、データリンクグループのアクティブ完全性グループ鍵として設定される第 1 の完全性グループ鍵 1 3 1 を含み得る。第 1 の完全性グループ鍵 1 3 1 は、第 1 のグループ鍵 1 3 2、第 1 の配布鍵 1 3 4、またはその両方に対応し得る。アクティブ鍵セット 1 3 0 が、第 1 のグループ鍵 1 3 2 と、第 1 の配布鍵 1 3 4 と、第 1 の完全性グループ鍵 1 3 1 とを含む実装形態では、第 1 のグループ鍵 1 3 2 と、第 1 の配布鍵 1 3 4 と、第 1 の完全性グループ鍵 1 3 1 とは第 1 の鍵トリオを構成する。第 1 の完全性グループ鍵 1 3 1 がアクティブ完全性グループ鍵として設定されると、第 1 の完全性グループ鍵 1 3 1 は、暗号化されていない（または符号化されていない）グループアドレス指定されたトラフィックの完全性保護のために使用され得る。たとえば、暗号化されていないグループアドレス指定されたメッセージとして送るべきメッセージをもつデバイスは、メッセージと第 1 の完全性グループ鍵 1 3 1 とに基づいて値を生成し得る。値は、メッセージの特定のフィールド中に含まれ得る。特定の实装形態では、値は、IEEE 802.11 規格によるメッセージ完全性コード（MIC）フィールド中に含まれる。暗号化されていないグループアドレス指定されたメッセージを受信するデバイスは、暗号化されていない（または符号化されていない）グループアドレス指定されたメッセージを検証するために第 1 のグループ完全性鍵 1 3 1 を使用し得、これは、デバイスが、グループアドレス指定されたトラフィックを改変し、改変されたグループアドレス指定されたトラフィックを中継することに対するセキュリティを与え得る。例示のために、第 1 のデバイス 104 の鍵論理 112 は、第 1 のグループ完全性鍵 1 3 1 と受信された第 1 の暗号化されていない（または符号化されていない）マルチキャストメッセージとに基づいて第 1 の値を生成し得、鍵論理 112 は、受信された暗号化されていない（または符号化されていない）マルチキャストメッセージの MIC フィールド中の特定の値などのメッセージ中の特定の値と第 1 の値を比較し得る。第 1 の値が特定の値に一致する場合、鍵論理 112 は、第 1 の暗号化されていないマルチキャストメッセージを検証し得る。第 1 の値が特定の値に一致しない場合、鍵論理 112 は、第 1 の暗号化されていないマルチキャストメッセージを検証することができないことがある。特定の实装形態では、検証されないメッセージは、転送されず、破棄されるかあるいは消去される。

【0027】

[0039]1 つまたは複数のペアワイズ鍵 1 4 5 は、第 1 のデバイス 104 と第 1 のデバイス 104 に関連するデバイスとの間のピアツーピア（P2P）通信のために使用され得る。たとえば、1 つまたは複数のペアワイズ鍵 1 4 5 は、本明細書でさらに説明するように、第 1 のデバイス 104 と第 2 のデバイス 106（第 1 のデバイス 104 に関連するデバイス）との間の P2P 通信のために使用され得るペアワイズ鍵 1 4 6 を含み得る。デバイスと第 1 のデバイス 104 とは、関連付けられるために関連付けプロセスを実行し得る。第 1 のデバイス 104 に関連するデバイスは、第 1 のデバイス 104 と関連する状態にあると呼ばれることもある。

【0028】

[0040]アクティブ鍵セット 1 3 0 中に含まれる各鍵は、対応する時間期間の間アクティブ鍵として設定され得る。たとえば、第 1 のグループ鍵 1 3 2 は、アクティブグループ鍵として設定され得、第 1 の時間期間の間アクティブ鍵セット 1 3 0 中に含まれ得る。別の例として、第 1 の配布鍵 1 3 4 は、アクティブ配布鍵として設定され得、第 2 の時間期間の間アクティブ鍵セット 1 3 0 中に含まれ得る。別の例として、第 1 のグループ完全性鍵 1 3 1 は、第 3 の時間期間の間アクティブ鍵セット 1 3 0 中に含まれ得る。他の実装形態では、第 1 の時間期間と、第 2 の時間期間と、第 3 の時間期間とは、同じ時間期間であり

得る。第1の時間期間、第2の時間期間、第3の時間期間、またはそれらの組合せは、データリンクグループ中に含まれる各デバイスによって知られている（または決定可能である）所定の時間期間であり得る。いくつかの実装形態では、第1の時間期間、第2の時間期間、または第3の時間期間は、鍵有効時間期間の別のものと部分的に重複し得る。特定の実装形態では、第1の時間期間は、IEEE 802.11規格、Wi-Fi Alliance規格、NAN規格、またはそれらの組合せなどのワイヤレス通信規格において定義されている。他の実装形態では、第1の時間期間と第2のものは、データリンクグループのデバイスによってネゴシエートされ得る。いくつかの実装形態では、第1の時間期間は、他のグループ鍵の時間期間と重複し得る。特定の実装形態では、第1のグループ鍵132と第1の時間期間とは満了しない。たとえば、第1の時間期間は、無制限の寿命を示し得るか、または終了時間を示さないことがあり、したがって、第1のグループ鍵132は、無制限の寿命を有し得、満了しないことがある。第1のグループ鍵132が満了しないと、デバイス104～110は、第1のグループ鍵132を置き換えるために候補鍵を生成しないことがある。

【0029】

[0041] 候補鍵セット140は、アクティブ鍵セット130のアクティブ鍵として設定されるために利用可能である1つまたは複数の鍵を含み得る。候補鍵セット140は、第2のグループ鍵142（たとえば、候補グループ鍵）、第2の配布鍵144（たとえば、候補配布鍵）、第2のグループ完全性鍵141（たとえば、候補グループ完全性）、またはそれらの組合せを含み得る。第2の配布鍵144は、第2のグループ鍵142と第2の配布鍵144とが第2の鍵ペアを構成するように第2のグループ鍵142に対応し得る。第2のグループ鍵142は、アクティブグループ鍵として使用され得（たとえば、設定され得）、第1の時間期間の満了時にアクティブ鍵セット130中に含まれ得る。したがって、第2のグループ鍵142は、アクティブグループ鍵として第1のグループ鍵132に続き得る（たとえば、それを置き換え得る）。第2の配布鍵144は、アクティブ配布鍵として使用され得（たとえば、設定され得）、第2の時間期間の満了時にアクティブ鍵セット130中に含まれ得る。したがって、第2の配布鍵144は、アクティブ配布鍵として第1の配布鍵134に続き得る（たとえば、それを置き換え得る）。第2のグループ完全性鍵141は、第3の時間期間の満了時に第1のグループ完全性鍵131に続き得る（たとえば、それを置き換え得る）。

【0030】

[0042] 第2のグループ完全性鍵141（たとえば、候補グループ完全性鍵）は、第2のグループ鍵142と、第2の配布鍵144と、第2のグループ完全性鍵141とが第2の鍵トリオを構成するように第2のグループ鍵142、第2の配布鍵144、またはその両方に対応し得る。第2のグループ完全性鍵141は、第1のグループ完全性鍵131に続き得（たとえば、それを置き換え得）、暗号化されていない（または符号化されていない）グループアドレス指定されたトラフィックのための完全性保護のために使用され得る。

【0031】

[0043] 候補鍵セット140は、アクティブ鍵セット130の満了より前に第1のデバイス104によって取得され得る。たとえば、第2のグループ鍵142は、第1の時間期間の満了の前に（たとえば、アクティブグループ鍵として第1のグループ鍵132の満了より前に）第1のデバイス104によって取得され得る。候補鍵セット140を取得するために、第1のデバイス104は、図2を参照しながら説明するように、候補鍵セット140を生成するように構成され得る。追加または代替として、候補鍵セット140は、本明細書でさらに説明するように、データリンクグループの別のデバイスによって生成され、鍵配信メッセージ180を使用して第1のデバイス104に通信され得る（たとえば、配布され得る）。

【0032】

[0044] メッセージ論理114は、ワイヤレスネットワーク102のデバイス間で通信されるメッセージを生成し、処理するように構成され得る。メッセージ論理114は、ワイ

10

20

30

40

50

ヤレスネットワーク 102 のデバイス 104 ~ 110 の間で通信されるメッセージを符号化および復号するように構成されるエンコーダ / デコーダ 118 を含み得る。たとえば、エンコーダ / デコーダ 118 は、データリンクグループの別のデバイスに通信されるべきメッセージを符号化（たとえば、暗号化）するために、132 または 134 などのアクティブ鍵セット 130 のうちの 1 つを使用し得る。他の実装形態では、メッセージ論理 114 は、エンコーダと、エンコーダとは別個であるデコーダとを含み得る。

【0033】

[0045]いくつかの実装形態では、メッセージ論理 114 は、第 1 のデバイス 104 と、（実線 181 によって示されるように）第 1 のデバイス 104 に関連する第 2 のデバイス 106 などのデバイスとの間で通信されるセキュアなメッセージを符号化および復号するように構成され得る。例示のために、第 1 のデバイス 104 と第 2 のデバイス 106 とは、第 1 のデバイス 104 と第 2 のデバイス 106 との間のピアツーピア（P2P）通信を可能にするためにセキュリティ関連付けを行うか、またはそれを実行し得る（たとえば、認証プロセスを実行し得る）。認証プロセスの一部として、ペアワイズ鍵 146 は、第 1 のデバイス 104 と第 2 のデバイス 106 との間のセキュアな通信を可能にするために生成され得る。ペアワイズ鍵 146 は、第 1 のデバイス 104 と第 2 のデバイス 106 との各々に記憶され得る。たとえば、第 1 のデバイス 104 は、1 つまたはペアワイズの鍵 145 中にペアワイズ鍵 146 を含み得る。第 1 のデバイス 104 が第 2 のデバイス 106 に関連する限り、1 つまたは複数のペアワイズ鍵 145 は、ペアワイズ鍵 146 を含み得る。メッセージ論理 114 は、第 1 のデバイス 104 と第 2 のデバイス 106 との間で通信される 1 つまたは複数の P2P メッセージを符号化および復号するためにペアワイズ鍵 146 を使用し得る。

【0034】

[0046]追加または代替として、ワイヤレスネットワーク 102 のデバイス 104 ~ 110 の間で通信されるメッセージのうちの 1 つまたは複数は、符号化されないことがある（たとえば、暗号化されないことがある）。たとえば、メッセージ論理 114 は、メッセージを生成し得、第 1 のデバイス 104 は、エンコーダ / デコーダ 118 を使用してメッセージを符号化することなしにワイヤレスネットワーク 102 の別のデバイスにメッセージを送り得る。例示のために、第 1 のデバイス 104 は、（破線 182 によって示されるように）第 4 のデバイス 110 に関連しないことがあり、第 1 のデバイス 104 は、第 4 のデバイス 110 に非セキュアなメッセージ（たとえば、符号化されていないメッセージまたは暗号化されていないメッセージ）を送り得る。さらに、第 1 のデバイス 104 は、1 つまたは複数の関連するデバイスに非セキュアなメッセージを送り得る。

【0035】

[0047]動作中、第 1 のデバイス 104 は、第 1 のグループ鍵 132 の満了より前に第 2 のグループ鍵 142 を生成するように構成され得る。たとえば、第 1 のデバイス 104 は、図 2 を参照しながらさらに説明するように、ランダム値または擬似ランダム値からのカウントダウンを完了したことに応答して、第 2 のグループ鍵 142 を生成し得る。第 2 のグループ鍵 142 は、データリンクグループ中の各デバイスがグループメッセージ（たとえば、グループ送信）を暗号化および解読することを可能にするために第 1 のグループ鍵 132 をデータリンクグループのアクティブグループ鍵として置き換え得る。

【0036】

[0048]いくつかの実装形態では、データリンクグループのデバイス 104 ~ 110 は、乱数発生によってグループ鍵を生成し得る。たとえば、第 1 のデバイス 104 は、乱数発生器、擬似乱数生成器、または他の乱数発生方法を使用することによって第 2 のグループ鍵 142 を生成するように構成され得る。第 2 のグループ鍵 142 は、ランダムに生成されたまたは擬似ランダムに生成された 256 ビットを含み得る。ワイヤレスネットワーク 102 の各データリンクグループは、一意のグループ鍵を含み得る。データリンクグループのデバイスは、前に使用されたグループ鍵を使用しないことがある。たとえば、データリンクグループのデバイスは、グループ鍵の再利用を防げるために、満了した鍵（たとえ

ば、満了したアクティブ鍵セット)と候補鍵(たとえば、候補鍵セット)とを記憶し得る。例示のために、第1のデバイス104は、第1のグループ鍵132を生成し、第2のグループ鍵142が一意であるのかどうかを決定するために第1のグループ鍵132を第2のグループ鍵142と比較し得る。第2のグループ鍵142が一意でないと決定したことに応答して、第1のデバイス104は、第2の候補グループ鍵などの別の候補鍵をランダムに生成し得る。第2のグループ鍵142が一意であると決定したことに応答して、第1のデバイス104は、第2のグループ鍵142の生成に対応するかまたはそれを示す告知メッセージを送信し得る。特定の実装形態では、第2のグループ鍵142は、ランダム値からのカウントダウンに応答して生成され得る。

【0037】

[0049]いくつかの実装形態では、データリンクグループの専用デバイスは、候補グループ鍵を生成するように構成され得る。デバイスは、データリンクグループの鍵生成器デバイスと呼ばれることがある。例示のために、特定のデバイスが、鍵生成器デバイスとして動作する間に、データリンクグループの他のデバイスは、グループ鍵(または候補グループ鍵)を生成しないことがある。鍵生成器デバイスはまた、データリンクグループの「リーダー」デバイスと呼ばれることもある。いくつかの実装形態では、鍵生成器デバイスは、1対1のサービス、1対多のサービス、またはその両方など、データリンクグループのサービスのプロバイダであり得る。いくつかの実装形態では、データリンクグループの特定のデバイスは、1つまたは複数の基準を満たすことに基づいて鍵生成器デバイスとして動作することを決定し得る。たとえば、第1のデバイス104は、第1のデバイス104がデータリンクグループの発信者であることに基づいて、第1のデバイス104が、データリンクグループの任意の他のデバイスと比べてデータリンクグループのより多くのデバイスと関連する状態にあることに基づいて、第1のデバイス104が、データリンクグループの他のデバイスと比べてNAN中でより多くの時間を費やしたことに基づいて、第1のデバイス104と関連する状態にあるデバイスの数に基づいて、NANのトポロジに基づいて、第1のデバイス104がNAN中に含まれていた持続時間に基づいて、NAN内の第1のデバイス104のランクに基づいて、第1のデバイス104のバッテリーレベルに基づいて、またはそれらの組合せで、鍵生成器デバイスとして動作することを決定し得る。特定の実装形態では、鍵生成器デバイスは、データリンクグループの発信者によるデータリンクグループの作成後に示され得る。たとえば、発信者は、特定のデバイスが鍵生成器デバイスとして動作すべきであることを示すメッセージをデータリンクグループのデバイスに送信し得る。

【0038】

[0050]別の特定の実装形態では、データリンクグループの特定のデバイスは、データリンクグループのデバイスによって鍵生成器デバイスとして動作するように選択され得る。選択は、上に列挙した基準のうちの1つまたは複数に基づき得る。たとえば、特定のデバイスは、データリンクグループの他のデバイスと比べて特定のデバイスがデータリンクトポロジ中でより「有利な」位置を有することに基づいて鍵生成器デバイスとして動作するように選択され得る。データリンクグループのトポロジ中の有利な位置は、データリンクグループの互いのデバイスからのホップのしきい値数と比べて特定のデバイスがより少ないことに対応し得る。別の例として、特定のデバイスは、特定のデバイスがデータリンクグループの任意の他のデバイスよりも多くのデバイスと関連する状態にあることに基づいて鍵生成器デバイスとして動作するように選択され得る。

【0039】

[0051]特定の実装形態では、現在の鍵生成器デバイスが、利用不可能になるか、または鍵生成動作の実行を終了する場合、候補鍵を生成するように構成されたデバイスが鍵生成器デバイスになり得る。たとえば、鍵生成器デバイスとして現在動作している特定のデバイスが、データリンクグループまたはNANとの関連付けを解除する場合、または特定のデバイスが、鍵生成動作を実行する能力がないことを示す場合、データリンクグループの異なるデバイスが鍵生成器デバイスとして動作するように選択され得る。特定の実装形態

では、利用不可能になるより前に、特定のデバイスは、鍵生成器デバイスとして動作すべき異なるデバイスを選択し得、特定のデバイスは、選択されたデバイスにメッセージを送信し得る。別の実装形態では、デバイスは、特定のデバイスが鍵生成動作をもはや実行していないと決定し得、デバイスは、鍵生成動作を実行し始め得る。代替的に、データリンクグループの異なるデバイスは、鍵生成器デバイスとして動作するようにデータリンクグループのデバイスによって選択され得る。

【0040】

[0052]データリンクグループのデバイスはまた、グループ鍵に対応するメッセージを送信または受信するように構成され得る。例示のために、メッセージ論理114は、データリンクグループのデバイス間で通信されるメッセージを生成し、処理するように構成され得る。いくつかの実装形態では、メッセージ論理114は、第1のデバイス104と、（実線181によって示されるように）第1のデバイス104に関連する第2のデバイス106などのデバイスとの間で通信されるセキュアなメッセージを符号化および復号するかまたは暗号化および解読するように構成され得る。いくつかの実装形態では、第1のグループ鍵132は、マルチキャストデータまたはブロードキャストデータなどのグループアドレス指定されたデータを暗号化または解読するために使用され得る。

【0041】

[0053]第1のデバイス104は、第2のグループ鍵142の生成に対応する告知メッセージ160を生成するように構成され得る。たとえば、メッセージ論理114は、告知メッセージ160を生成するように構成され得る。告知メッセージ160は、候補鍵セット140の少なくとも1つの鍵が利用可能であることを示し得る。たとえば、候補グループ鍵（たとえば、第2のグループ鍵142）が、利用可能であり、アクティブグループ鍵として第1のグループ鍵132を置き換えるべきである告知メッセージ160。告知メッセージ160は、第2のグループ鍵142を生成したことに応答して、データリンクグループの他のデバイス106～110に第2のグループ鍵142を配布する前に第1のデバイス104によって生成され得る。代替的に、第2のグループ鍵142は、カウントダウンの完了後に生成され得、告知メッセージ160は、カウントダウンの完了に応答して、第2のグループ鍵142の生成または配布より前に生成され得る。いくつかの実装形態では、告知メッセージ160は、第1のグループ鍵132またはペアワイズ鍵146などの鍵を使用してメッセージ論理114によって符号化（または暗号化）され得る。他の実装形態では、メッセージ論理114は、告知メッセージ160を符号化（または暗号化）しないことがある。

【0042】

[0054]告知メッセージ160は、フラグ162と、グループ識別子（ID）164と、デバイスID166とを含み得る。フラグ162は、告知メッセージがグループ鍵告知メッセージであることを示す1つまたは複数のビット、フィールド、またはそれらの組合せを含み得る。グループID164は、データリンクグループを一意に識別するデータリンクグループの識別子であり得る。たとえば、グループID164は、データリンクグループに対応するバイト値またはグループアドレスなどの1つまたは複数のビットを含み得る。デバイスID166は、候補グループ鍵を生成したデバイスに対応する媒体アクセス制御（MAC）アドレスであり得る。たとえば、告知メッセージ160のデバイスID166は、第1のデバイス104のMACアドレスであり得る。いくつかの実装形態では、告知メッセージ160は、第2のグループ鍵142（または候補鍵セット140）が生成されたとき、または第2のグループ鍵142（または候補鍵セット140）の生成が開始されたときに対応するタイムスタンプを含み得る。追加または代替として、告知メッセージ160は、告知メッセージ160を送信する特定のデバイスに対応する第2のデバイスIDを含み得る。たとえば、第2のデバイスIDは、第1のデバイス104など、告知メッセージ160を送信するデバイスのMACアドレスであり得る。

【0043】

[0055]いくつかの実装形態では、告知メッセージ160はまた、鍵インジケータ168

10

20

30

40

50

を含む。鍵インジケータ 1 6 8 は、第 2 のグループ鍵 1 4 2 に関係する情報を与え得る。たとえば、鍵インジケータ 1 6 8 は、第 2 のグループ鍵 1 4 2、第 2 のグループ鍵 1 4 2 の生成に対応するタイムスタンプ、第 1 のデバイス 1 0 4 の M A C アドレス、またはそれらの組合せに基づいて生成されるハッシュ値を含み得る。鍵インジケータ 1 6 8 は、本明細書でさらに説明するように、告知メッセージ 1 6 0 を受信するデバイスが、第 2 のグループ鍵 1 4 2 がデータリンクグループのための次のアクティブ鍵になるべきであるのかどうかを決定することを可能にし得る。

【 0 0 4 4 】

[0056]告知メッセージ 1 6 0 の生成の後に、第 1 のデバイス 1 0 4 は、告知メッセージ 1 6 0 をデータリンクグループの他のデバイスに送信し得る。告知メッセージ 1 6 0 は、セキュアなメッセージとして、または非セキュアなメッセージとして送られ得る。告知メッセージ 1 6 0 がセキュアなメッセージとして送られる場合、告知メッセージ 1 6 0 は、暗号化されたメッセージであり得、告知メッセージ 1 6 0 が非セキュアなメッセージとして送られる場合、告知メッセージ 1 6 0 は、暗号化されていないメッセージであり得る。たとえば、告知メッセージ 1 6 0 を送るより前に、エンコーダ/デコーダ 1 1 8 は、第 1 のグループ鍵 1 3 2 などのアクティブ鍵セット 1 3 0 の特定の鍵を使用して告知メッセージ 1 6 0 を暗号化し得る。代替的に、エンコーダ/デコーダ 1 1 8 は、告知メッセージ 1 6 0 を暗号化しないことがある。告知メッセージ 1 6 0 が暗号化されない場合、エンコーダ/デコーダ 1 1 8 は、第 1 のグループ完全性鍵 1 3 1 を使用して告知メッセージ 1 6 0 を保護し得る。

【 0 0 4 5 】

[0057]第 1 のデバイス 1 0 4 は、データリンクグループのデバイス 1 0 6 ~ 1 1 0 のうちの少なくとも 1 つにマルチキャストメッセージとして告知メッセージ 1 6 0 を送信するように構成され得る。告知メッセージ 1 6 0 は、第 1 のワイヤレスチャネルを介して送信され得る。告知メッセージ 1 6 0 は、第 1 のデバイス 1 0 4 に関連するデバイスと第 1 のデバイス 1 0 4 に関連しないデバイスとに送信され得る。たとえば、告知メッセージ 1 6 0 は、（実線 1 8 1 によって示されるように）第 1 のデバイス 1 0 4 に関連する第 2 のデバイス 1 0 6 に送信され得る。さらに、告知メッセージ 1 6 0 は、（破線 1 8 2 によって示されるように）第 1 のデバイス 1 0 4 に関連しない第 4 のデバイス 1 1 0 に送信され得る。第 1 のワイヤレスチャネルは、N A N 通信チャネル、データリンクグループチャネル、またはその両方に対応し得る。

【 0 0 4 6 】

[0058]特定の実装形態では、第 1 のデバイス 1 0 4 は、第 1 の通信チャネルのページングウィンドウ中に告知メッセージ 1 6 0 を送信し得る。ページングウィンドウは、データリンクグループ用に指定され得、ページングウィンドウは、N A N 通信チャネルまたはデータリンクグループチャネルに対応し得る。例示のために、ページングウィンドウは、N A N 通信チャネルまたはデータリンクグループチャネルを介した特定の通信用に指定された特定の時間期間を含み得る。別の特定の実装形態では、第 1 のデバイス 1 0 4 は、第 1 の通信チャネルの発見ウィンドウ中に告知メッセージ 1 6 0 を送信し得る。発見ウィンドウは、N A N 通信チャネルに対応し得る。追加または代替として、第 1 のデバイス 1 0 4 は、第 1 のデバイス 1 0 4 に関連する第 2 のデバイス 1 0 6 などの特定のデバイスにピアツーピア（P 2 P）通信として告知メッセージ 1 6 0 を送り得る。

【 0 0 4 7 】

[0059]データリンクグループのデバイス 1 0 4 ~ 1 1 0 の各々は、ページングウィンドウ、発見ウィンドウ、またはその両方中にアクティブモードにあり得、これは、第 1 のデバイス 1 0 4 の隣接デバイスが告知メッセージ 1 6 0 を受信する可能性を増加させ得る。第 1 のデバイス 1 0 4 から 1 ホップだけ離れているデバイスなど、第 1 のデバイス 1 0 4 の通信範囲内にあるデバイスが告知メッセージ 1 6 0 を受信し得る。たとえば、第 2 のデバイス 1 0 6 と第 4 のデバイス 1 1 0 とは、告知メッセージ 1 6 0 を受信し得、デバイス 1 0 6 および 1 1 0 が、I E E E 8 0 2 . 1 1 s 規格、W i - F i A l l i a n c e 規

10

20

30

40

50

格、またはそれらの組合せによって記述されているように、第1のデバイス104の特定の通信範囲（たとえば、1ホップの範囲）内にあるので、第1のデバイス104の「隣接」デバイスと呼ばれることがある。第3のデバイスは、第1のデバイス104から複数ホップだけ離れているので、第3のデバイス108は、特定の通信範囲内になく、第1のデバイス104の隣接デバイスであるとは考えられない。

【0048】

[0060]告知メッセージ160がデータリンクグループ中の各デバイスに達するように、1つまたは複数のデバイスは、告知メッセージ160を受信し、転送し得る。たとえば、第2のデバイス106が第1のデバイス104から告知メッセージ160を受信したことに応答して、第2のデバイス106は、データリンクグループの他のデバイスに告知メッセージ170（たとえば、転送された告知メッセージ）として告知メッセージ160を転送し得る。例示のために、第2のデバイス106は、第3のデバイス108と第4のデバイス110とに告知メッセージ170を送り得る。いくつかの実装形態では、他のデバイスが、告知メッセージ160に対応する第2のグループ鍵142（または候補鍵セット140）を受信する後まで、第1のデバイス104から告知メッセージ160を受信する別のデバイスは、告知メッセージ160を転送しないことがある。

【0049】

[0061]いくつかの実装形態では、メッセージ論理114は、告知メッセージ160が送信された後にページングメッセージ165を生成するようにさらに構成され得る。ページングメッセージ165は、第1のデバイス104などの特定のデバイスからデータリンクグループの他のデバイスに送信するようにデータをスケジュールしたことを示し得る。送信するようにスケジュールしたデータは、第2のグループ鍵142など、候補鍵セット140の少なくとも1つの鍵を含み得る。いくつかの実装形態では、ページングメッセージ165はマルチキャストメッセージであり得る。たとえば、ページングメッセージ165は、データリンクグループの複数のデバイスに送信され得、ページングメッセージ165は、データリンクグループの複数のデバイスに送信するようにデータをスケジュールしたことを示し得る。いくつかの実装形態では、ページングメッセージ165は、第1のグループ鍵132を使用して暗号化され得る。ページングメッセージ165は、ページ属性169を随意に含み得る。ページ属性169の詳細について、図6を参照しながらさらに説明する。

【0050】

[0062]第1のデバイス104は、第1のデバイス104に関連するデータリンクグループの隣接デバイスにページングメッセージ165を送信するように構成され得る。たとえば、第1のデバイス104は、第2のデバイス106にページングメッセージ165を送信し得る。いくつかの実装形態では、ページングメッセージ165は、第1のワイヤレスチャネル（NAN通信チャネル）を介して送信され得る。他の実装形態では、ページングメッセージ165は、第2のワイヤレスチャネル（データリンクグループチャネル）を介して送信され得る。ページングメッセージ165は、データリンクグループ用に指定された（またはそれに対応する）送信ウィンドウのページングウィンドウ中に送信され得る。データリンクグループの各デバイスは、ページングメッセージが受信および送信され得るように、ページングウィンドウ中にアクティブ動作モードで動作するように構成され得る。

【0051】

[0063]いくつかの実装形態では、第2のデバイス106は、ページングメッセージ165を受信したことに応答して第1のデバイス104にトリガメッセージ167を送信するように構成され得る。トリガメッセージ167は、現在の送信ウィンドウまたは後続の送信ウィンドウのデータウィンドウ中にアクティブ動作モードで動作するように第2のデバイス106がスケジュールされることを示す。たとえば、データウィンドウ中に第2のデバイス106に送信するようにスケジュールされたデータを第1のデバイス104が有することを示すページングメッセージ165を受信したことに応答して、第2のデバイス1

10

20

30

40

50

06はトリガメッセージ167を送信し得る。さらに、第2のデバイス106は、第1のデバイス104からデータを受信するために、データウィンドウ中にアクティブ動作モードで動作したままであり得る。トリガメッセージ167は、ページングウィンドウまたはデータウィンドウ中に第2のワイヤレスチャネル(データリンクグループチャネル)を介して送信され得る。代替的に、トリガメッセージ167は、第1のワイヤレスチャネル(NAN通信チャネル)を介して送信され得る。

【0052】

[0064]トリガメッセージ167を受信した後に、第1のデバイス104は、鍵配信メッセージ180を生成し得る。鍵配信メッセージ180は、データリンクグループのデバイス106~110に配布されるべき第2のグループ鍵142を含み得る。いくつかの実装形態では、鍵配信メッセージ180は、候補鍵セット140の1つまたは複数の鍵を含み得る。第1のデバイス104は、第1のグループ鍵132(たとえば、アクティブグループ鍵)の満了より前に第2のデバイス106に鍵配信メッセージ180を送信し得る。いくつかの実装形態では、鍵配信メッセージ180は、図1中で鍵IDとして示された鍵識別子143をさらに含み得る。鍵識別子143は、第2のグループ鍵142の寿命または有効期限を示し得る。いくつかの実装形態では、鍵配信メッセージ180は、セキュアなメッセージであり得、第1のデバイス104から第2のデバイス106にユニキャストメッセージとして送信され得る。たとえば、鍵配信メッセージ180は、ペアワイズ鍵146に基づいて暗号化され得、ユニキャスト送信を介して第1のデバイス104から第2のデバイス106に送信され得る。鍵配信メッセージ180は、データウィンドウ中に第2のワイヤレスチャネル(データリンクグループチャネル)を介して送信され得る。代替的に、鍵配信メッセージ180は、第1のワイヤレスチャネル(NAN通信チャネル)を介して送信され得る。

【0053】

[0065]第1のデバイス104がトリガメッセージ167を受信しない場合、たとえば、ページングメッセージ165またはトリガメッセージ167が宛先に達しない場合、または第2のデバイス106がページングメッセージ165に应答することができない場合、第1のデバイス104は鍵配信メッセージ180を送信しない。この例では、第1のデバイス104は、第2のページングウィンドウ中に第2のデバイス106に第2のページングメッセージを送信し得る。このようにして、第1のデバイス104は、第2のデバイス106からトリガメッセージ167などのトリガメッセージを受信するまで鍵配信メッセージ180を送信しないことがある。他の実装形態では、ページングメッセージ、トリガメッセージまたはその両方が使用されないことがある。たとえば、第1のデバイス104は、ページングメッセージ165を送信することまたはトリガメッセージ167を受信することなしに鍵配信メッセージ180を生成し得る。特定の実装形態では、第1のデバイス104は、告知メッセージ160が発見ウィンドウ中に送信された後に鍵配信メッセージ180を生成し、送信し得る。別の特定の実装形態では、第1のデバイス104は、カウントダウンの完了に应答して鍵配信メッセージ180を生成し、送信し得る。カウントダウンは、アクティブグループ鍵の満了に関係し得、アクティブグループ鍵の満了の前に行なわれ得る。

【0054】

[0066]第2のデバイス106は、データリンクグループの他のデバイスに第2のグループ鍵142を伝搬するように構成され得る。たとえば、鍵配信メッセージ180(または候補鍵セット140の少なくとも1つの鍵)を受信したことに应答して、第2のデバイス106は、データリンクグループの隣接デバイスにページングメッセージ190を送信し得る。例示のために、第2のデバイス106が、(実線184によって示されるように)第3のデバイス108に関連し、第2のデバイス106は、第3のデバイス108にページングメッセージ190を送信し得る。ページングメッセージ190は、第2のデバイス106が、第3のデバイス108に送信するようにスケジュールされた(第2のグループ鍵142などの候補鍵セット140の少なくとも1つの鍵に対応する)データを有するこ

とを示し得る。第3のデバイス108からトリガメッセージ(図示せず)を受信したことに応答して、第2のデバイス106は、第3のデバイス108に鍵配信メッセージ180を転送し得る。このようにして、第2のグループ鍵142は、データリンクグループのデバイスに伝搬し得る。

【0055】

[0067]単一の候補グループ鍵(たとえば、第2のグループ鍵142)の生成について説明されるが、いくつかの実装形態では、第2のグループ鍵142に関係する告知メッセージが特定の時間までに受信されていない場合、データリンクグループの複数のデバイスは、候補グループ鍵(または候補鍵セット)を生成するように構成され得る。たとえば、デバイス104~110の各々は、ランダム値からタイマーを開始し、タイマーが特定の値に達すると、新しい候補グループ鍵(または新しい候補鍵セット)を生成するように構成され得る。デバイス104~110の各々は、(第1のグループ鍵132などの)前のグループ鍵が満了したことまたは(第2のグループ鍵142などの)候補グループ鍵がアクティブグループ鍵になったことに応答してタイマーを開始するように構成され得る。タイマーが特定の値に達する前に告知メッセージが特定のデバイスによって受信される場合、特定のデバイスのタイマーが停止され得、候補グループ鍵が特定のデバイスによって生成される。タイマーが特定の値に達した場合、特定のデバイスは、候補グループ鍵の生成を開始する。

【0056】

[0068]複数の告知メッセージまたは複数のグループ鍵(たとえば、複数の候補鍵セット)がデータリンクグループのデバイスによって受信される場合、データリンクグループのデバイスは、鍵インジケータに基づいて次のアクティブグループ鍵(または次のアクティブ鍵セット)として特定の候補グループ鍵(または特定の候補鍵セット)を設定し得る。例示のために、特定の候補グループ鍵は、他の候補グループ鍵に対応する他の鍵インジケータよりも高い優先度を有する特定の候補グループ鍵に対応する鍵インジケータに基づいて次のアクティブグループ鍵として選択され得る。例示的な例として、最古のタイムスタンプを有する候補グループ鍵が次のアクティブグループ鍵として設定され得る。例示のために、第2のデバイス106は、第1のタイムスタンプ(たとえば、第1の優先度)と第2のタイムスタンプ(たとえば、第2の優先度)との間の比較を実行し得る。第2のデバイス106は、第1のタイムスタンプが第2のタイムスタンプよりも前のものであることに基づいて、第1のタイムスタンプに対応する候補グループ鍵を選択し得る。別の例として、最大の(または最低の)ハッシュ値を有する候補グループ鍵が次のアクティブグループ鍵として設定され得る。別の例として、最も優先度の高いMACアドレスを有するデバイスによって生成された候補グループ鍵が次のアクティブグループ鍵として設定され得る。

【0057】

[0069]選択されない候補グループ鍵に対応する告知メッセージは、データリンクグループのデバイスによって転送されない。たとえば、第2のデバイス106が、告知メッセージ160を受信した後に第2の告知メッセージを受信し、第2の告知メッセージが、別の候補グループ鍵に対応する後のタイムスタンプを含む場合、第2のデバイス106は、第2の告知メッセージを転送しない。いくつかの実装形態では、第2のデバイス106は、第2の告知メッセージを受信したことに応答して、または第2の告知メッセージに対応するページングメッセージを受信したことに応答して拒絶メッセージを送り得る。

【0058】

[0070]いくつかの実装形態では、第1のデバイス104は、データリンクグループの1つまたは複数のデバイスに鍵配信メッセージ180をマルチキャストメッセージとして通信し得る。マルチキャストメッセージは、パブリックアクションフレームまたはデータリンクグループメッセージを含むか、またはそれに対応し得る。鍵配信メッセージ180がマルチキャストメッセージとして通信されると、第1のデバイス104は、データリンクグループの特定のアクティブ鍵を使用して鍵配信メッセージ180を符号化(または暗号

化)し得る。たとえば、アクティブ鍵セット130が、データリンクグループのアクティブ配布鍵として設定された第1の配布鍵134を含むとき、エンコーダ/デコーダ118は、第1の配布鍵134を使用して鍵配信メッセージ180を符号化(または暗号化)し得る。鍵配信メッセージ180を暗号化するために第1の配布鍵134を使用することは、鍵配信メッセージ180を送信するときに追加のセキュリティを与え得る。例示のために、第1の配布鍵134は、鍵配信メッセージ180などの鍵配信メッセージを符号化および復号(または暗号化および解読)するためにのみ使用され得、第1のグループ鍵132は、他のセキュアなグループ通信のために使用され得る。第1のグループ鍵132が第1の配布鍵134よりも頻繁に使用されるので、第1のグループ鍵132は、より漏洩しやすい(たとえば、データリンクグループの一部でないデバイスによってより識別されやすい)。したがって、データリンクグループのデバイスにマルチキャストメッセージとして第2のグループ鍵142、第2の配布鍵144、またはその両方を配布するために第1の配布鍵134を使用することは、データリンクグループのデバイスに第2のグループ鍵142、第2の配布鍵144、またはその両方を配布するために第1のグループ鍵132を使用することよりもセキュアであり得る。

【0059】

[0071]第1のデバイス104は、第2のグループ鍵142を生成することによって、またはデータリンクグループの別のデバイスから第2のグループ鍵142を受信することによって、第1のデバイス104が第2のグループ鍵142を取得したかどうかにかかわらず、マルチキャストメッセージとして鍵配信メッセージ180を配布し得る。第1の配布鍵134を使用して第2のグループ鍵142を符号化(または暗号化)し、符号化された第2のグループ鍵を含むマルチキャストメッセージを送ることによって、符号化された第2のグループ鍵(たとえば、第2のグループ鍵142)は、第1のデバイス104とデータリンクグループの別のデバイスとの間でセキュリティ関連付け手順、P2P通信、またはそれらの組合せを実行することなしにデータリンクグループの1つまたは複数のデバイスに配布され得るたとえば、第1のデバイス104は、複数のデバイスが第1のデバイス104に関連するか関連しないかにかかわらず、複数のデバイスに符号化(または暗号化)された第2のグループ鍵142を同時に配布するためにマルチキャストメッセージを送信し得る。例示のために、第1のデバイス104は、第1のデバイス104に関連する第2のデバイス106に、および第1のデバイス104に関連しない第4のデバイス110に符号化(または暗号化)された第2のグループ鍵142をマルチキャストし得る。したがって、符号化された第2のグループ鍵(第2のグループ鍵142)をマルチキャストするために第1の配布鍵134を使用することは、ワイヤレスネットワーク102内での候補グループ鍵配布に関する鍵関連のトラフィックとオーバーヘッドとを低減し得る。

【0060】

[0072]追加または代替として、第1のデバイス104は、P2P通信として鍵配信メッセージ180を通信し得る。例示のために、告知メッセージ160の送信の後に、第1のデバイス104は、関連するデバイスから第2のグループ鍵142についての要求を受信し得る。いくつかの実装形態では、第2のグループ鍵142についての要求は、候補鍵セット140についての要求を含み得る。第2のデバイス106が告知メッセージ160を受信すると、第2のデバイス106は、第1のデバイス104に関連し得、第2のデバイス106は、告知メッセージ160に回答して第2のグループ鍵142についての要求を送り得る。第2のデバイス106は、P2Pメッセージとして要求を送り得る。要求に回答して、第1のデバイス104は、P2Pメッセージとして第2のデバイス106に鍵配信メッセージ180を送り得る。いくつかの実装形態では、第1のデバイス104は、第1のデバイス104に関連する1つまたは複数のデバイスにP2Pメッセージとして鍵配信メッセージ180を自動的に送り得る。たとえば、第1のデバイス104は、関連するデバイスから第2のグループ鍵142についての要求を受信することなしにP2Pメッセージとして鍵配信メッセージ180を自動的に送り得る。

【0061】

10

20

30

40

50

[0073]いくつかの実装形態では、第1のデバイス104に関連しない特定のデバイスに告知メッセージ160を送った後に、第1のデバイス104は、特定のデバイスに関連付けられるためにセキュリティ関連付け手順を実行し得る。たとえば、第4のデバイス110が告知メッセージ160を受信するとき、第4のデバイス110は、第1のデバイス104に関連しないことがある。告知メッセージ160を受信した後に、第4のデバイス110は、第1のデバイス104に関連付けられるために第1のデバイス104とのセキュリティ関連付け手順を開始し得る。第4のデバイス110が第1のデバイス104に関連した後、第1のデバイス104は、第4のデバイス110に第2のグループ鍵142を含むP2P通信を送り得る。たとえば、第1のデバイス104は、第4のデバイス110に第2のグループ鍵142を自動的に送り得、または第1のデバイス104は、第2のグループ鍵142についての、第4のデバイス110から受信された要求に回答して第2のグループ鍵142を送り得る。

10

【0062】

[0074]特定の実装形態では、第1のデバイス104から告知メッセージ160を受信する特定のデバイスが、第1のデバイス104に関連しないとき、特定のデバイスは、データリンクグループの第1のグループ鍵132などのアクティブグループ鍵が満了するように設定される前の所定の時間まで関連するデバイスから別の告知メッセージ（たとえば、告知メッセージ170）を受信するのを待ち得る。所定の時間が検出されると、アクティブグループ鍵の満了が間近であると見なされる。特定のデバイスが無関連のデバイスから告知メッセージ160を受信するのと所定の時間の検出との間の時間期間は待ち期間と呼ばれることがある。待ち期間中に、特定のデバイスは、特定のデバイスに関連するデバイスから第2の告知メッセージを受信するのを待ち得、したがって、特定のデバイスは、第2のグループ鍵142を受信することができる。特定のデバイスが、待ち期間中に第2の告知メッセージを受信しない場合、特定のデバイスは、所定の時間が検出された後に無関連のデバイスとのセキュリティ関連付け手順を開始し得、したがって、特定のデバイスは、第2のグループ鍵142を収集することができる。

20

【0063】

[0075]例示のために、第4のデバイス110が告知メッセージ160を受信するとき、第4のデバイス110は、第1のデバイス104に関連しないことがある。告知メッセージ160を受信したことに回答して第1のデバイス104に関連するためにセキュリティ関連付けプロセスを開始するのではなく、第4のデバイス110は、第4のデバイス110が関連するデータリンクグループの別のデバイスから告知メッセージ170などの告知メッセージ160の転送バージョンを受信するのを待ち得る。例示のために、第4のデバイス110は、（実線186によって示されるように）第2のデバイス106に関連し得、第1のデバイス104から告知メッセージ160を受信した後に第2のデバイス106から告知メッセージ170を受信し得る。第2のデバイス106から告知メッセージ170を受信した後に、第4のデバイス110は、P2P通信として第2のデバイス106から第2のグループ鍵142（または候補鍵セット140）を受信し得る。たとえば、第2のデバイス106は、自動的に、または第2のグループ鍵142についての、第4のデバイス110から受信された要求に回答して、第4のデバイス110に第2のグループ鍵142を送り得る。関連するデバイス106から別の告知メッセージ170を受信するのを待つことによって、第4のデバイス110は、第1のデバイス104から告知メッセージ160を受信したことに回答して第1のデバイス104とのセキュリティ関連付けを自動的に開始しない。

30

40

【0064】

[0076]第4のデバイス110は、データリンクグループの第1のグループ鍵132などのアクティブグループ鍵が満了するように設定される前の所定の時間まで、関連するデバイスから第2の告知メッセージ（たとえば、告知メッセージ170）を受信するのを待ち得る。例示のために、所定の時間が検出されると、アクティブグループ鍵の満了が間近であると見なされる。第4のデバイス110が、関連するデバイスから第2の告知メッセー

50

ジを受信しなかった場合、第4のデバイス110は、第2のグループ鍵142（または候補鍵セット140）を受信するために、第1のデバイス104などの無関連のデバイスとのセキュリティ関連付け手順を開始し得る。例示のために、第4のデバイス110は、第1のデバイス104とのセキュリティ関連付け手順を開始し得、セキュリティ関連付け手順の完了の後に、第4のデバイス110は、第1のデバイス104から第2のグループ鍵142（または候補鍵セット140）を受信し得る。たとえば、第1のデバイス104は、自動的に、または第2のグループ鍵142についての、第4のデバイス110から受信された要求に応答して、第4のデバイス110に第2のグループ鍵142を送り得る。

【0065】

[0077]別の特定の実装形態では、データリンクグループの各デバイスは、アクティブグループ鍵の満了を予想して候補グループ鍵の生成を開始するように構成され得る。例示のために、各デバイスは、図2を参照しながら説明するように、ランダム値を生成し、アクティブグループ鍵の時間期間が満了に近づく、生成されたランダム値からカウントダウンを開始するように構成され得る。特定のデバイスにおけるカウントダウンが完了すると、特定のデバイスは、候補グループ鍵を生成し、他のデバイスに告知メッセージを送信し得る。たとえば、第1のデバイス104は、対応するカウントダウンを完了し、第2のグループ鍵142を生成し、告知メッセージ160を送信し得る。第2のデバイス106および第4のデバイス110などの他のデバイスは、告知メッセージ（たとえば、告知メッセージ160）を受信したことに応答してそれらのそれぞれのカウントダウンを停止し（追加の候補グループ鍵を生成するのを控え）得る。告知メッセージ160または告知メッセージ170を受信すると、特定のデバイスはまた、1つまたは複数の追加の告知メッセージ、候補グループ鍵、またはそれらの組合せの伝搬を（抑制基準に基づいて）条件付きで抑制し得る。たとえば、抑制基準は、例示的な非限定的な例として、より古いタイムスタンプ、またはより高い値のMACアドレスを有するデバイスによって生成されたタイムスタンプに対応する特定の候補グループ鍵を選択するために適用され得る。告知メッセージ、候補グループ鍵、またはそれらの組合せを抑制することによって、データリンクグループは、複数の（競合する）候補グループ鍵がアクティブグループ鍵として設定されることを回避し得る。

【0066】

[0078]いくつかの実装形態では、データリンクグループの2つのデバイスは、隣接デバイスであり得、無関連であり得る。たとえば、図1に示したように、第1のデバイス104は、第4のデバイス110の通信範囲（たとえば、1ホップ範囲）内にあり得、（破線182によって示されるように）第4のデバイス110に関連しないことがある。第4のデバイス110は、（実線186によって示されるように）第2のデバイス106など、データリンクグループの異なるデバイスに関連し得る。デバイスは関連しないが、マルチキャストメッセージなどのいくつかのメッセージは、デバイス間で共有され得る。たとえば、告知メッセージ160がマルチキャストされると、第1のデバイス104は、第4のデバイス110に告知メッセージ160を送信し得る。

【0067】

[0079]いくつかの実装形態では、データリンクグループのデバイスは、データリンクグループの他のデバイスから候補グループ鍵を受信するために特定の時間まで待つように構成され得る。候補グループ鍵が、現在のグループ鍵の満了より前の特定の量の時間などの特定の時間までに受信されない場合、デバイスは、候補グループ鍵を受信するためにデータリンクグループの別のデバイスに関連するように構成され得る。現在のグループ鍵の満了より前の特定の量の時間は、グループ鍵更新ウィンドウの終了、関連付けウィンドウの開始、またはその両方を示し得るかまたはそれに対応し得る。グループ鍵更新ウィンドウは、鍵更新動作（たとえば、特定の候補グループ鍵を選択し、データリンクグループのデバイスに特定の候補グループ鍵を配布すること）の実行に対応する特定の時間間隔を含み得る。第1のグループ鍵132がアクティブグループ鍵として設定されると、データリンクグループのデバイスは、カウントダウンを開始し得る。カウントダウンは、第1のグル

ープ鍵 1 3 2 の有効期間よりも短い継続時間を有し得る。カウントダウンの継続時間（または最初のカウントダウン値）は、カウントダウンの満了と第 1 のグループ鍵 1 3 2 の満了との間の時間期間が、デバイスがデータリンクグループの他のデバイスとの 1 つまたは複数の関連付け動作を実行するのに十分であるように選択され得る。カウントダウンについて説明されるが、カウントダウンに対応する時間期間を追跡するために任意の形態のタイマーまたはタイミング回路が使用され得る。

【0068】

[0080] 図 1 に示す例では、第 1 のグループ鍵 1 3 2 がアクティブ鍵として設定されると、第 4 のデバイス 1 1 0 は、（第 1 の継続時間を有する）カウントダウンを開始し得る。他の実装形態では、カウントダウンは、告知メッセージ 1 6 0 が第 1 のデバイス 1 0 4 から受信されたときに開始され得、カウントダウンは、第 1 の継続時間とは異なる継続時間を有し得る。カウントダウンが満了し、第 4 のデバイス 1 1 0 が、たとえば、鍵配信メッセージを受信することによって、第 2 のグループ鍵 1 4 2 を受信しなかった場合、第 4 のデバイス 1 1 0 は、「パニックモード」に入り得、第 4 のデバイス 1 1 0 が告知メッセージを受信したデバイスに関連しようと試み得る。たとえば、第 4 のデバイス 1 1 0 が、第 1 のデバイス 1 0 4 から告知メッセージ 1 6 0 を受信したので、第 4 のデバイス 1 1 0 は、第 1 のデバイス 1 0 4 に関連しようと試み得る。

10

【0069】

[0081] 第 1 のデバイス 1 0 4 に関連するために、第 4 のデバイス 1 1 0 は、第 1 のデバイス 1 0 4 に関連付け要求 1 7 5 を送信し得る。関連付け要求 1 7 5 は、第 4 のデバイス 1 1 0 を識別し得、第 4 のデバイス 1 1 0 が第 1 のデバイス 1 0 4 との関連付けを実行することを望むことを示し得る。関連付け要求 1 7 5 を受信したことに応答して、第 1 のデバイス 1 0 4 は、少なくとも 1 つの基準に基づいて第 4 のデバイス 1 1 0 に関連すべきかどうかを決定し得る。一例として、基準は、第 1 のデバイス 1 0 4 が現在関連するいくつかの他のデバイスを含み得る。例示のために、第 1 のデバイス 1 0 4 は、データリンクグループのしきい値数以下の他のデバイスに関連するように構成され得る。この例では、第 1 のデバイス 1 0 4 は、第 1 のデバイス 1 0 4 がしきい値数の他のデバイスに現在関連するかどうかを決定し得る。第 1 のデバイス 1 0 4 が、少なくともしきい値数のデバイスに関連する場合、第 1 のデバイス 1 0 4 は、第 4 のデバイス 1 1 0 に関連しないことを決定し得る。第 1 のデバイス 1 0 4 が、しきい値数未満のデバイスに関連する場合、第 1 のデバイス 1 0 4 は、第 4 のデバイス 1 1 0 に関連することを決定し得る。

20

30

【0070】

[0082] 追加または代替として、少なくとも 1 つの基準は、「必要ベースの」関連付けに關係し得る。たとえば、第 1 のデバイス 1 0 4 は、「必要」に応じて他のデバイスに関連するように構成され得る。一例として、必要ベースの関連付けは、データリンクグループの任意の他のデバイスに現在関連しないデバイスとの関連付けを含み得る。別の例として、必要ベースの関連付けは、アクティブトラフィックセッションに基づいて決定され得る。例示のために、第 1 のデバイス 1 0 4 は、第 1 のデバイス 1 0 4 が次のページングウィンドウ中に第 2 のデバイス 1 0 6 のためのアクティブトラフィックセッションを有しないと決定したことに応答して、第 2 のデバイス 1 0 6 との関連付けを解除し得る。別の例として、第 1 のデバイス 1 0 4 は、第 2 のデバイス 1 0 6 が第 2 のグループ鍵 1 4 2 をすでに受信したと決定したことに応答して第 2 のデバイス 1 0 6 との関連付けを解除し得る。このようにして、第 1 のデバイス 1 0 4 は、「必要性」がより大きいであろう他のデバイスに関連するためにデータリンクグループのいくつかのデバイスとの関連付けを解除するように構成され得る。

40

【0071】

[0083] 第 1 のデバイス 1 0 4 が、第 4 のデバイス 1 1 0 に関連することを決定する場合、第 1 のデバイス 1 0 4 は第 4 のデバイス 1 1 0 に関連付け応答 1 7 6 を送信し得る。関連付け応答 1 7 6 は、第 4 のデバイス 1 1 0 が第 1 のデバイス 1 0 4 に関連することを可能にする情報を含み得る。関連付け応答 1 7 6 を受信したことに応答して、第 4 のデバイ

50

ス 1 1 0 は、第 1 のデバイス 1 0 4 に関連し得る。たとえば、第 4 のデバイス 1 1 0 は、第 1 のデバイス 1 0 4 との 1 つまたは複数の関連付け動作を実行し得る。特定の実装形態では、1 つまたは複数の関連付け動作は、2 ウェイハンドシェイク、4 ウェイのハンドシェイク、セキュリティ情報の交換、またはそれらの組合せを含み得る。他の実装形態では、他の関連付け動作が実行され得る。関連付け動作の実行中に、第 1 のデバイス 1 0 4 と第 4 のデバイス 1 1 0 との間でペアワイズ鍵が発生され得る。

【0072】

[0084] 第 1 のデバイス 1 0 4 が、第 4 のデバイス 1 1 0 に関連しないことを決定する場合、第 1 のデバイス 1 0 4 は第 4 のデバイス 1 1 0 に関連付け拒絶 1 7 8 を送信し得る。関連付け拒絶 1 7 8 は、第 1 のデバイス 1 0 4 が、この時点で第 4 のデバイス 1 1 0 との
10 関連付け動作を実行することができないことを示し得る。関連付け拒絶 1 7 8 は、第 1 のデバイスに関連するデバイスのセット（たとえば、第 2 のグループ鍵 1 4 2 を持っているデバイスのセット）を示し得る。たとえば、関連付け拒絶 1 7 8 は、第 1 のデバイス 1 0 4 が第 2 のデバイス 1 0 6 に関連することを示し得る。追加または代替として、関連付け拒絶 1 7 8 は、第 2 のグループ鍵 1 4 2 をすでに受信しているか、またはそれをすでに持っているデバイスのセットを示し得る。たとえば、関連付け拒絶 1 7 8 は、第 2 のデバイス 1 0 6 が第 2 のグループ鍵 1 4 2 をすでに受信しているか、またはそれをすでに持っていることを示し得る。第 4 のデバイス 1 1 0 は、関連付け拒絶 1 7 8 中に第 2 のデバイス 1 0 6 が示されたことに応答して第 2 のデバイス 1 0 6 に第 2 の関連付け要求を送信し得る。関連付け要求 1 7 5 と、関連付け応答 1 7 6 と、関連付け拒絶 1 7 8 とは、第 1 のワイヤレスチャネルまたは第 2 のワイヤレスチャネルを介して送信され得る。
20

【0073】

[0085] いくつかの実装形態では、第 4 のデバイス 1 1 0 は、関連付けが実行されるまで、または第 1 のグループ鍵 1 3 2 が満了するまで、第 1 のデバイス 1 0 4 に関連しようと試み続けるように構成され得る。たとえば、第 4 のデバイス 1 1 0 が、第 2 のグループ鍵 1 4 2 を受信している別のデバイスに関連しない場合、第 4 のデバイス 1 1 0 は、第 1 のデバイス 1 0 4 に第 2 の関連付け要求（図示せず）を送信し得る。別の例として、第 4 のデバイス 1 1 0 が第 2 のデバイス 1 0 6 から告知メッセージ 1 7 0 を受信する場合、第 4 のデバイス 1 1 0 は、第 2 のデバイス 1 0 6 に関連しようと試み得る。

【0074】

[0086] いくつかの実装形態では、第 4 のデバイス 1 1 0 は、第 1 のデバイス 1 0 4 に関連しようと試みるより前に、カウントダウンの満了を待たない。代わりに、第 4 のデバイス 1 1 0 は、告知メッセージ 1 6 0 を受信したことに応答して第 1 のデバイス 1 0 4 に関連するように構成され得る。たとえば、第 4 のデバイス 1 1 0 は、第 1 のデバイス 1 0 4 から告知メッセージ 1 6 0 を受信したことに応答して第 1 のデバイス 1 0 4 に関連付け要求 1 7 5 を送信し得る。追加または代替として、第 4 のデバイス 1 1 0 が、第 2 のデバイス 1 0 6 に関連しないとき、第 4 のデバイス 1 1 0 は、第 2 のデバイス 1 0 6 から告知メッセージ 1 7 0 を受信したことに応答して第 2 のデバイス 1 0 6 に関連付け要求を送信し得る。第 1 のデバイス 1 0 4（または第 2 のデバイス 1 0 6）は、上記で説明されるように、第 4 のデバイス 1 1 0 に関連すべきかどうかを決定し得る。第 4 のデバイス 1 1 0 は、データリンクグループの他のデバイスに関連しようと試みるより前にカウントダウンの満了を待たないので、関連付け試みが失敗した場合、第 4 のデバイス 1 1 0 は、異なるデバイスに関連するためにより多くの時間を有し、それによって、第 4 のデバイス 1 1 0 が、異なるデバイスに関連し、第 1 のグループ鍵 1 3 2 の満了より前に第 2 のグループ鍵 1 4 2 を受信することができる可能性が増加し得る。
40

【0075】

[0087] いくつかの実装形態では、データリンクグループのデバイス 1 0 4 ~ 1 1 0 は、ユニキャストメッセージとしてデータリンクグループの別のデバイスに鍵配信メッセージと候補グループ鍵（または候補鍵セット）とを通信し得る。特定の実装形態では、ユニキャストメッセージを使用してデータリンクグループの 2 つの無関連のデバイス間で候補グ
50

ループ鍵（または候補鍵セット）を交換するために4ウェイハンドシェイクが使用され得る。4ウェイハンドシェイクは、鍵暗号化鍵（KEK：key encryption key）を使用して暗号化され、鍵確認鍵（CKK：key confirmation key）を使用して完全性を保護されるローカルエリアネットワークを介した拡張認証プロトコル（EAPOL：extension authentication protocol over local area network）鍵フレームを含み得る。KEKとCKKとは、ペアワイズ鍵中に含まれ得る。EAPOL鍵フレームは、第2のグループ鍵142などの候補グループ鍵を含み得る。いくつかの実装形態では、EAPOL鍵フレームは、候補鍵セット140を含み得る。EAPOL鍵フレームは、2つの無関連のデバイス間の第3のメッセージ（または通信）に対応するか、またはそれの中に含まれ得る。

【0076】

10

[0088] 4ウェイハンドシェイクを実行することの例示的な例として、第1のデバイス104と第4のデバイス110とは無関連であり得、第1のデバイス104は、第4のデバイス110に第1のメッセージを送信し得る。第1のメッセージにより、第4のデバイス110は、ペアワイズ鍵を生成することが可能になり得る。第1のデバイス104は、第4のデバイス110から第2のメッセージを受信し、第2のメッセージに基づいてペアワイズ鍵を生成し得る。第1のデバイス104は、第4のデバイス110にEAPOL鍵フレームを含む第3のメッセージを送信し、EAPOL鍵フレームは、第2のグループ鍵142を含み得る。EAPOL鍵フレームは、KEKに基づいて暗号化され、CKKに基づいて完全性を保護され得る。第1のデバイス104は、第4のデバイス110から第4のメッセージを受信し得る。第4のメッセージは、第4のデバイス110が第2のグループ鍵142を受信したことと、第4のデバイス110が第1のデバイス104に現在関連することとを示す肯定応答メッセージを含み得る。

20

【0077】

[0089] 別の特定の实装形態では、ユニキャストメッセージを使用してデータリンクグループの2つの関連するデバイス間で候補グループ鍵を交換するためにグループ鍵ハンドシェイク（たとえば、2ウェイハンドシェイク）が使用され得る。グループ鍵ハンドシェイクは、暗号化され、完全性を保護され得るEAPOL鍵フレームを含み得る。EAPOL鍵フレームは、2つの関連するデバイス間で第1のメッセージ（または通信）として送信され得る。グループ鍵ハンドシェイクを実行することの例示的な例として、第1のデバイス104と第2のデバイス106とは、関連し得、第1のデバイス104と第2のデバイス106とは、ペアワイズ鍵146をすでに所有していることがある。たとえば、ペアワイズ鍵146は、グループハンドシェイクより前に行なわれた関連付け動作中に生成されていることがある。ペアワイズ鍵146は、KEKとCKKとを含み得る。第1のデバイス104は、第2のデバイス106に、第2のグループ鍵142を有するEAPOL鍵フレームを含む第1のメッセージを送信し得る。（または候補鍵セット140）EAPOL鍵フレームは、ペアワイズ鍵146のKEKに基づいて暗号化され、ペアワイズ鍵146のCKKに基づいて完全性を保護され得る。第1のデバイス104は、第2のデバイス106から第2のメッセージを受信し得る。第2のメッセージは、肯定応答メッセージを含み得、第2のデバイス106が第2のグループ鍵142を受信していることを示し得る。

30

【0078】

40

[0090] 別の特定の实装形態では、鍵配信メッセージ180は、NAN管理フレームを含むか、またはそれに対応し得、これは、ユニキャストメッセージを使用してデータリンクグループの2つのデバイス間で候補グループ鍵を交換するために使用され得る。NAN管理フレームは、EAPOL鍵フレームをカプセル化し得る（または含み得る）。NAN管理フレーム、EAPOL鍵フレーム、またはその両方は、KEKに基づいて暗号化され、CKKに基づいて完全性を保護され得る。たとえば、第1のデバイス104は、第2のグループ鍵142など、候補鍵セット140の少なくとも1つの鍵を有するEAPOL鍵フレームを含むNAN管理フレームとして鍵配信メッセージ180を送信し得る。第1のデバイス104は、第2のデバイス106など、第1のデバイス104に関連する別のデバイスにNAN管理フレームを送信し得る。

50

【 0 0 7 9 】

[0091]別の特定の実装形態では、鍵配信メッセージ 1 8 0 は、パブリックアクションフレームを含むか、またはそれに対応し得、これは、ユニキャストメッセージを使用してデータリンクグループの 2 つのデバイス間で候補グループ鍵を交換するために使用され得る。パブリックアクションフレームは、時間鍵 (T K) を使用して保護され得る。 T K は、ペアワイズ鍵中に含まれ得る。グループ鍵を搬送するために、パブリックアクションフレームの特定の属性 (たとえば、特定のフィールド) が規定され得る。たとえば、1 つまたは複数のワイヤレス通信規格においてなど、グループ鍵を搬送するために、パブリックアクションフレームの第 1 の属性が規定され得る。第 1 のデバイス 1 0 4 は、パブリックアクションフレームの第 1 の属性中に、第 2 のグループ鍵 1 4 2 など、候補鍵セット 1 4 0 の少なくとも 1 つの鍵を含むパブリックアクションフレームとして鍵配信メッセージ 1 8 0 を送信し得る。鍵配信メッセージ 1 8 0 は、第 2 のデバイス 1 0 6 など、第 1 のデバイス 1 0 4 に関連する別のデバイスに送信され得る。

10

【 0 0 8 0 】

[0092]いくつかの実装形態では、第 1 のデバイス 1 0 4 は、告知メッセージ 1 6 0 などの告知メッセージを送信しない。これらの実装形態では、第 2 のグループ鍵 1 4 2 を生成したことに応答して、第 1 のデバイス 1 0 4 は、データリンクグループの隣接デバイスにページングメッセージ 1 6 5 を送信し得る。上記で説明されるように、ページングメッセージ 1 6 5 は、第 1 のワイヤレスチャネル (N A N 通信チャネル) または第 2 のワイヤレスチャネル (データリンクグループチャネル) のページングウィンドウ中に送信され得る。これらの実装形態では、ページングメッセージ 1 6 5 は、第 2 のグループ鍵 1 4 2 の生成を示すページ属性 1 6 9 を含む。ページ属性 1 6 9 の詳細について、図 6 を参照しながら本明細書でさらに説明する。いくつかの実装形態ではまた、ページングメッセージ 1 6 5 は、グループ I D 1 6 4 、デバイス I D 1 6 6 、鍵インジケータ 1 6 8 、またはそれらの組合せを含み得る。告知メッセージ 1 6 0 などの告知メッセージを使用する代わりにページングメッセージを使用してグループ鍵を告知することは、第 1 のワイヤレスチャネル、第 2 のワイヤレスチャネル、またはその両方上でトラフィックを低減し得る。

20

【 0 0 8 1 】

[0093]ページングメッセージ 1 6 5 を受信したことに応答して、第 2 のデバイス 1 0 6 は、上記で説明されるように、第 1 のデバイス 1 0 4 にトリガメッセージ 1 6 7 を送信し得る。第 1 のデバイス 1 0 4 は、トリガメッセージ 1 6 7 を受信したことに応答して第 2 のデバイス 1 0 6 に第 2 のグループ鍵 1 4 2 を含む鍵配信メッセージ 1 8 0 を送信し得る。第 2 のグループ鍵 1 4 2 を受信した後に、第 2 のデバイス 1 0 6 は、第 3 のデバイス 1 0 8 にページングメッセージを送信し得、第 2 のデバイス 1 0 6 と第 3 のデバイス 1 0 8 とは、第 1 のデバイス 1 0 4 と第 2 のデバイス 1 0 6 とに関して説明されるように、トリガメッセージと鍵配信メッセージとを交換し得る。さらに、第 2 のデバイス 1 0 6 は、(第 2 のグループ鍵 1 4 2 を含む) 鍵配信メッセージ 1 8 0 を受信したことに応答して第 1 のデバイス 1 0 4 に M A C A C K などの肯定応答 (A C K) を送り得る。さらに、ページングメッセージは、マルチキャストであり得、暗号化されていないことがあるので、第 4 のデバイス 1 1 0 などの第 1 のデバイス 1 0 4 に関連しない隣接デバイスは、ページングメッセージ 1 6 5 を受信し得、候補鍵セット 1 4 0 の少なくとも 1 つの鍵 (たとえば、第 2 のグループ鍵 1 4 2) など、ページングメッセージ 1 6 5 に関連するデータを受信するために第 1 のデバイス 1 0 4 に関連しようと試み得る。

30

40

【 0 0 8 2 】

[0094]ページングメッセージ 1 6 5 は、複数のページングウィンドウ中に再送信されるか、または繰り返され得る。たとえば、第 1 のデバイス 1 0 4 は、第 1 のグループ鍵 1 3 2 が満了するまで、複数のページングウィンドウ中にページングメッセージ 1 6 5 を送信し得る。いくつかの実装形態では、第 1 のデバイス 1 0 4 と関連する状態にある各隣接デバイスが第 2 のグループ鍵 1 4 2 を受信した場合、第 1 のデバイス 1 0 4 は、第 1 のグループ鍵 1 3 2 の満了より前にページングメッセージ 1 6 5 を送信することを停止し得る。

50

例示のために、第1のデバイス104は、第2のデバイス106が第2のグループ鍵142を受信するまで、複数のページングウィンドウ中にページングメッセージ165を送信し得る。第1のデバイス104は、鍵配信メッセージ180を送信したことに応答して第2のデバイス106からACKを受信することに基づいて第2のデバイス106が第2のグループ鍵142を受信したと決定し得る。したがって、第1のデバイス104が、データリンクグループの各隣接デバイスからACKを受信する場合、第1のデバイス104は、ページングメッセージ165を送信することを停止し得る。

【0083】

[0095]追加または代替として、グループ鍵（アクティブ鍵セット130および候補鍵セット140）は、鍵インデックス、鍵識別番号、またはその両方に関連し得る。鍵インデックス、鍵識別番号、またはその両方は、サービス情報フィールド、鍵配信メッセージ180、またはその両方の中などのNANサービス発見フレーム中に含まれ得る。鍵インデックス、鍵識別番号、またはその両方は、アクティブグループ鍵がデータリンクグループのためのトラフィックを暗号化するために使用されることを示し得る。鍵識別番号は、グループ鍵を識別するために使用され得る数値または英数字文字列を含み得る。鍵インデックスは、非アクティブグループ鍵とアクティブグループ鍵との表を含み得る。いくつかの実装形態では、鍵インデックスの表は、各非アクティブグループ鍵とアクティブグループ鍵とのための鍵識別番号を含み得る。

【0084】

[0096]鍵インデックス、鍵識別番号、またはそれらの組合せにより、データリンクグループのデバイスは、アクティブグループ鍵を決定することが可能になり得る。たとえば、特定のデータリンクグループを離れ、後で、特定のデータリンクグループに再加入するデバイスは、前のアクティブグループ鍵が、鍵インデックス、鍵識別番号、またはそれらの組合せに基づいて依然として有効であるのかどうかを決定し得る。前のアクティブグループ鍵が依然として有効である場合、デバイスは、データリンクグループのアクティブグループ鍵を受信するためにデータリンクグループの別のデバイスと認証する必要がない。別の例として、アクティブグループ鍵としての第1のグループ鍵132からの第2のグループ鍵142への遷移中に、デバイスは、データを暗号化するためにデバイスがどのグループ鍵（たとえば、第1のグループ鍵132または第2のグループ鍵142）を使用しているのかを示し得る。たとえば、第1のデバイス104は、メッセージ中に、データを暗号化するために第1のデバイス104が使用している第1のグループ鍵132に関連する鍵識別番号を含み得る。

【0085】

[0097]システム100のいくつかの動作および機能について、対応するデバイスに関して説明されたが、デバイス104～110の各々は、デバイス104～110の別のものを参照しながら説明される1つまたは複数の動作、機能、またはそれらの組合せを実行するように構成され得る。たとえば、デバイス104～110の各々は、第1のデバイス104の、それぞれ、鍵論理112およびメッセージ論理114を参照しながら説明されるように対応する鍵論理と対応するメッセージ論理とを含み得る。追加または代替として、1つまたは複数の例について第2のグループ鍵142の配布に関して説明されたが、そのような例は、候補鍵セット140の1つまたは複数の鍵の配布に適用され得る。

【0086】

[0098]開示する態様のうちの少なくとも1つによって与えられる1つの利点は、ワイヤレスネットワーク内の鍵関係のトラフィックおよびオーバーヘッドの低減である。たとえば、NANのデバイスがアクティブ動作モードにある（たとえば、起動している）とき、鍵関連のトラフィックは、ページングウィンドウまたは発見ウィンドウ中に告知メッセージ160を送ることによって低減され得る。ページングウィンドウまたは発見ウィンドウ中に告知メッセージ160を送ることは、第1のデバイス104の隣接デバイスが告知メッセージ160を受信する可能性を増加させ得、これは、再送信を低減し得る。別の例として、データリンクグループ中のデバイスがアクティブ動作モードにあるとき、鍵関連の

トラフィックは、ページングウィンドウ中にページ属性 1 6 9 を有するページングメッセージ 1 6 5 を送ることによって低減され得る。ページ属性 1 6 9 は、次のデータウィンドウ中に特定のデバイスからトラフィックを受信するようにスケジュールされた複数のデバイスを示し得、グループ鍵伝搬のために必要とされるページングメッセージの数を低減し得る。

【 0 0 8 7 】

[0099]別の例示的な利点は、告知メッセージ 1 6 0 (またはその転送バージョン)を受信するデバイスが、アクティブグループ鍵の満了より前の所定の時間までの待ち期間を実装し得ることである。待ち期間中に、告知メッセージ 1 6 0 (またはその転送バージョン)を受信した特定のデバイスは、告知メッセージ 1 6 0 (またはその転送バージョン)に対応する第 2 のグループ鍵 1 4 2 を取得するためにセキュリティ関連付け手順を開始するのを控え得る(自制し得る)。第 2 のグループ鍵 1 4 2 を収集するために別のデバイスに関連するのを控えることによって、第 2 のグループ鍵 1 4 2 を取得するためにセキュリティ関連付け手順を実行する 1 つまたは複数のデバイスに対応するトラフィックの量が低減され得る。別の例として、第 2 のグループ鍵 1 4 2 を符号化(または暗号化)するために第 1 の配布鍵 1 3 4 などのアクティブ配布鍵が使用され得、符号化された第 2 のグループ鍵が、データリンクグループの 1 つまたは複数のデバイスに送られ得る(たとえば、マルチキャストされ得る)。符号化された第 2 のグループ鍵を送ることによって、第 2 のグループ鍵 1 4 2 は、第 2 のグループ鍵 1 4 2 を有する別のデバイスと第 2 のグループ鍵 1 4 2 を有しないデータリンクグループのデバイスとの間でセキュリティ関連付け手順、P 2 P 通信、またはそれらの組合せを実行することなしにデータリンクグループの 1 つまたは複数のデバイスに配布され得る。

【 0 0 8 8 】

[0100]図 2 は、候補グループ鍵を生成するシステム 2 0 0 の特定の例示的な実装形態である。システム 2 0 0 は、ワイヤレスネットワーク中に含まれるデバイスなどのデバイス 2 0 2 を含む。デバイス 2 0 2 は、図 1 のワイヤレスネットワーク 1 0 2 のデバイス 1 0 4 ~ 1 1 0 のうちの 1 つを含むか、またはそれに対応し得る。

【 0 0 8 9 】

[0101]デバイス 2 0 2 は、カウンタ 2 0 4 と、鍵生成器 2 0 6 と、鍵記憶装置 2 0 8 と、受信機 2 1 0 と、送信機 2 1 2 とを含み得る。受信機 2 1 0 と送信機 2 1 2 とは、それぞれ、ワイヤレスネットワークの他のデバイスから 1 つまたは複数の信号を受信し、それに 1 つまたは複数の信号を送信するように構成され得る。いくつかの実装形態では、受信機 2 1 0 と送信機 2 1 2 とは、トランシーバなどの単一の構成要素を含み得る。鍵記憶装置 2 0 8 は、メモリなどのストレージデバイスを含むか、またはそれに対応し得る。カウンタ 2 0 4 は、鍵生成器 2 0 6 と受信機 2 1 0 とに結合され得、鍵生成器 2 0 6 は、鍵記憶装置 2 0 8 と送信機 2 1 2 とに結合され得、鍵記憶装置 2 0 8 は、受信機 2 1 0 と送信機 2 1 2 とに結合され得る。いくつかの実装形態では、カウンタ 2 0 4 は、タイマーを含むか、またはそれに対応し得る。

【 0 0 9 0 】

[0102]カウンタ 2 0 4 は、本明細書でさらに説明するように、グループ鍵 2 1 4 の生成より前にランダム値 2 2 0 からカウントダウンを実行するように構成され得る。鍵生成器 2 0 6 は、グループ鍵 2 1 4、配布鍵(図示せず)、グループ完全性鍵、またはそれらの組合せなどの 1 つまたは複数の鍵を生成することと、鍵記憶装置 2 0 8 と送信機 2 1 2 とに 1 つまたは複数の鍵を与えることとを行うように構成され得る。たとえば、鍵生成器は、グループ鍵 2 1 4 を生成し、鍵記憶装置 2 0 8 と送信機 2 1 2 とにグループ鍵 2 1 4 を与え得る。グループ鍵 2 1 4 は、図 1 の第 1 のグループ鍵 1 3 2 または第 2 のグループ鍵 1 4 2 を含むか、またはそれに対応し得る。配布鍵は、図 1 の第 1 の配布鍵 1 3 4 または第 2 の配布鍵 1 4 4 を含むか、またはそれに対応し得る。鍵生成器 2 0 6 は、ハードウェア、ソフトウェア、またはそれらの組合せを含み得る。いくつかの実装形態では、鍵生成器 2 0 6 は、グループ鍵 2 1 4 を生成するためにメモリ中に含まれる 1 つまたは複数の命

令を実行するように構成されたプロセッサを含むか、またはそれに対応し得る。

【0091】

[0103] 鍵記憶装置 208 は、グループ鍵 214、配布鍵、ペアワイズ鍵、グループ完全性鍵、またはそれらの組合せなどの 1 つまたは複数の鍵を記憶するように構成され得る。別の例として、鍵記憶装置 208 は、データリンクグループの 1 つまたは複数の満了したグループ鍵などの 1 つまたは複数の前のグループ鍵、あるいは別のデバイスによって生成され、受信機 210 を介してデバイス 202 において受信された 1 つまたは複数の候補グループ鍵を記憶し得る。

【0092】

[0104] 動作中、鍵生成器 206 は、グループ鍵 214 の形成を開始し得る。特定の実装形態では、アクティブグループ鍵の満了の前の特定の所定の量の時間（たとえば、アクティブグループ鍵として設定された前のグループ鍵が満了に近づいていること）を検出することに基づいて、鍵記憶装置 208 は、前のグループ鍵（たとえば、アクティブグループ鍵）を記憶し得、鍵生成器 206 は、グループ鍵 214 の形成を開始し得る。たとえば、特定の所定の量の時間は、アクティブグループ鍵に関連するタイミング情報に基づいて、カウンタ 204、鍵生成器 206、またはそれらの組合せによって検出され得る。特定の所定の量の時間は、アクティブグループ鍵の満了の前に残された時間量が、アクティブグループ鍵の満了より前に候補グループ鍵が生成され、データリンクグループの各デバイスに伝搬されるのに十分であるように選択され得る。

【0093】

[0105] 図 2 に、タイミング図 230 中のデータリンクグループのグループ鍵（たとえば、アクティブグループ鍵）の満了に対応するタイミングをも示す。図示のように、時間 t_1 に第 1 のグループ鍵（鍵 1）が生成され得る（または、生成が開始され得る）。第 1 のグループ鍵（鍵 1）は、時間 t_1 に、または時間 t_1 のすぐ後にアクティブグループ鍵として設定され得る。第 1 のグループ鍵（鍵 1）がデータリンクグループのデバイス間で送信されるとき、第 1 のグループ鍵（鍵 1）に対応するタイムスタンプが、生成され、第 1 のグループ鍵（鍵 1）とともに、図 1 の鍵配信メッセージ 180 などのメッセージ中に含まれ得る。

【0094】

[0106] 時間 t_2 に、第 2 のグループ鍵（鍵 2）の生成が開始される。いくつかの実装形態では、時間 t_2 は、第 1 のグループ鍵（鍵 1）の満了の前の特定の所定の量の時間（または第 1 のグループ鍵（鍵 1）の生成の後のある量の時間）に関連し得る。時間 t_3 に、第 1 のグループ鍵（鍵 1）が満了する。時間 t_2 に生成されるものとして示されているが、他の例では、第 2 のグループ鍵（鍵 2）の生成は、時間 t_2 に開始され得、第 2 のグループ鍵（鍵 2）の生成は、時間 t_2 と時間 t_3 との間にある時間に行なわれ得る。第 2 のグループ鍵（鍵 2）の生成の後に、第 2 のグループ鍵（鍵 2）は、第 1 のグループ鍵（鍵 1）の満了より前にデータリンクグループの 1 つまたは複数のデバイスに与えられ得る。第 2 のグループ鍵（鍵 2）は、第 1 の候補グループ鍵であり得、図 1 の候補鍵セット 140 に対応し得る。第 2 のグループ鍵（鍵 2）は、時間 t_2 と時間 t_3 との間の時間期間中にアクティブグループ鍵になり得る。特定の実装形態では、第 2 のグループ鍵（鍵 2）は、時間 t_3 にアクティブグループ鍵として設定される。

【0095】

[0107] 第 3 のグループ鍵（鍵 3）の生成は、時間 t_4 に開始され得、これは、第 2 のグループ鍵（鍵 2）の満了の前の特定の所定の量の時間に対応する。第 2 のグループ鍵（鍵 2）は、時間 t_5 に満了し得、第 3 のグループ鍵（鍵 3）は、アクティブグループ鍵として設定され得る。図示されていないが、第 4 のグループ鍵は、時間 t_6 に第 3 のグループ鍵（鍵 3）の満了より前に生成され得る。さらに、特定の所定の量の時間が、アクティブグループ鍵の各々の満了の前の同じ時間量であるものとして説明されたが、他の実装形態では、特定の所定の量の時間は、アクティブグループ鍵の各々ごとに異なる量の、満了の前の時間であり得る。第 3 のグループ鍵（鍵 3）は、第 2 の候補グループ鍵であり得、図

10

20

30

40

50

1の候補鍵セット140に対応し得る。

【0096】

[0108]デバイス202を参照すると、アクティブグループ鍵の満了より前に特定の所定の量の時間を検出したことに応答して、鍵生成器206は、グループ鍵214の生成を開始することを決定し得る。鍵生成器206は、カウンタ204に、ランダム値220からカウントダウンを開始すること（またはランダム値220までカウントアップするカウンタを開始すること）を行わせることによってグループ鍵214の生成を開始し得る。ランダム値220は、デバイス202に記憶された特定の範囲の値内から生成（または選択）され得る。たとえば、製造中に、デバイス202は、1つまたは複数の規格に対応する範囲の値などの特定の範囲の値を示すデータを用いてプログラムされ得る。別の例として、デバイス202は、デバイス202がデータリンクグループに加わる時に実行されるセキュリティ関連付け手順（たとえば、関連付け手順）中にデータリンクグループの別のデバイスから特定の範囲の値を示すデータを受信し得る。

10

【0097】

[0109]カウントダウンが0に達すると（またはカウントアップがランダム値220に達すると）、鍵生成器206は、グループ鍵214を生成し、鍵記憶装置208、送信機212、またはそれらの組合せにグループ鍵214を与え得る。さらに、鍵生成器206は、図1の告知メッセージ160などの告知メッセージを生成するか、またはその生成を開始し得、鍵生成器206は、グループ鍵214の送信より前に告知メッセージを送信機212によって送信することを行わせ得る。グループ鍵214は、データリンクグループのデバイス202から他のデバイスに送られるグループメッセージを暗号化すること、データリンクグループの他のデバイスからデバイス202において受信されたグループメッセージを解読すること、またはそれらの組合せを行う際に使用するアクティブグループ鍵として鍵記憶装置208中に記憶され得る。追加または代替として、グループ鍵214は、候補グループ鍵として鍵記憶装置208中に記憶され得、アクティブグループ鍵として後で設定され得る。グループ鍵214（および告知メッセージ）は、（たとえば、シングルホップまたはマルチホップルートを通じて）グループ中の1つまたは複数の他のデバイスに送信機212によって送信され得る。いくつかの実装形態では、告知メッセージは、カウントダウンが0に達した（またはカウントアップがランダム値220に達した）後に、グループ鍵214の生成より前に送られ得る。

20

30

【0098】

[0110]鍵生成器206は、グループ鍵214の生成より前に別の告知メッセージまたは別のグループ鍵が受信されるときにグループ鍵414の生成を防げる（たとえば、禁止する）ように構成され得る。たとえば、カウンタ204は、別の告知メッセージまたは別の候補グループ鍵（たとえば、異なるデバイスによって生成された告知メッセージ、異なるデバイスによって生成された候補グループ鍵、またはそれらの組合せ）が受信機210によって受信される場合にカウントダウンを停止し得る。さらに、グループ鍵214が生成され、デバイス202が、別のデバイスから別のグループ鍵が生成されたことを示す特定の告知メッセージを受信する場合、デバイス202は、グループ鍵214または他のグループ鍵を既存のアクティブグループ鍵の満了の後に潜在的な「次の」アクティブグループ鍵として使用すべきであるのかどうかを決定するために抑制基準を適用し得る。たとえば、抑制基準は、例示的な非限定的な例として、より古いタイムスタンプに対応する特定の候補グループ鍵、またはより高い値のMACアドレスを有するデバイスによって生成された候補グループ鍵を選択するために適用され得る。

40

【0099】

[0111]図2に、単一のデバイス202を示すが、データリンクグループ中の各デバイスがデバイス202として同様に構成され得る。したがって、データリンクグループ中の任意のデバイスは、データリンクグループの他のデバイスによって使用されるべき対応する候補グループ鍵を生成し得る。データリンクグループの各デバイスが対応する候補グループ鍵を生成することを可能にすることによって、データリンクグループは、データリンク

50

グループのデバイスによって使用されるべき候補グループ鍵を生成するように単一の中央デバイスを構成することなしにデータを交換することを可能にし得る。(中央デバイスを含む)各デバイスが任意の時間にワイヤレスネットワークを離れ得るので、単一の中央デバイスの使用はワイヤレスネットワークにおいて望ましくないことがある。

【0100】

[0112]図3は、データリンクグループ中で通信されるメッセージのタイミング図300の特定の例示的な実装形態である。データリンクグループは、デバイス104~110を含む図1のデータリンクグループを含むか、またはそれに対応し得る。データリンクグループは、第1のデバイス(STA1)、第2のデバイス(STA2)、および第3のデバイス(STA3)などの複数のデバイスを含み得る。たとえば、第1のデバイスと、第2のデバイスと、第3のデバイスとは、図1のデバイス104~110または図2のデバイス202を含むか、またはそれに対応し得る。

10

【0101】

[0113]タイミング図300に、NAN通信チャンネル302とデータリンクグループチャンネル304とを示す。NAN通信チャンネル302は、第1の発見ウィンドウ310と第2の発見ウィンドウ312などの複数の発見ウィンドウを含む。データリンクグループチャンネル304は、複数のグループ送信ウィンドウ320~326を含む。いくつかの実装形態では、グループ送信ウィンドウ320~326は、NAN通信チャンネル302に関して発生する。たとえば、データリンクグループチャンネル304がないとき、グループ送信ウィンドウ320~326は、NAN通信チャンネル302に関して発生し、第1の発見ウィンドウ310と第2の発見ウィンドウ312との間にあり得る。

20

【0102】

[0114]他の実装形態では、データリンクグループチャンネル304は、(発見ウィンドウ310、312と同様の)発見ウィンドウを含み得、グループ送信ウィンドウ320~326は、データリンクグループチャンネル304の2つの発見ウィンドウ間に発生する。いくつかの実装形態では、データリンクグループチャンネル304の発見ウィンドウは、NAN通信チャンネル302の第1の発見ウィンドウ310と第2の発見ウィンドウ312とに加えたものであり得る。他の実装形態では、NAN通信チャンネル302がないことがある。これらの実装形態では、データリンクグループチャンネル304は、対応する発見ウィンドウを有し得るか、または有し得る。

30

【0103】

[0115]いくつかの実装形態では、データリンクグループは、NAN中に含まれ得、データリンクグループのデバイスは、NAN通信チャンネル302を介して通信し得る。NANのデバイスは、NANのマスタデバイスによって、またはNANの特定のグループのマスタデバイスによって通信される1つまたは複数の同期ビーコンを介して同期され得る。たとえば、データリンクグループのデバイスのうちの1つは、マスタデバイスとして動作し得、NAN通信チャンネル302を介してNAN中に含まれる他のデバイスに1つまたは複数の同期ビーコンをブロードキャストし得る。

【0104】

[0116]追加または代替として、データリンクグループ中に含まれるデバイスは、データリンクグループチャンネル304を介して通信し得る。データリンクグループのデバイスは、データリンクグループのマスタデバイスまたはデータリンクグループを含むNANのマスタデバイスによって通信される1つまたは複数の同期ビーコンを介して同期され得る。たとえば、データリンクグループのデバイスのうちの1つは、マスタデバイスとして動作し得、NAN通信チャンネル302、データリンクグループチャンネル304、またはその両方を介してデータリンクグループの他のデバイス、NANの他のデバイス、またはそれらの組合せに1つまたは複数の同期ビーコンをブロードキャストし得る。

40

【0105】

[0117]デバイスは、データリンクグループチャンネル304に対応するグループ送信ウィンドウを検出するために同期され得る。たとえば、データリンクグループのデバイスの各

50

々は、本明細書でさらに説明するように、グループ送信ウィンドウ、ページングウィンドウ、データパスウィンドウ、またはそれらの組合せの開始と終了との正しい決定を可能にするために、IEEE 802.11s規格、Wi-Fi Alliance規格、またはそれらの組合せによって記述されているように同期クロックを有し得る。グループ送信ウィンドウは、第1のグループ送信ウィンドウ320と、第2のグループ送信ウィンドウ322と、第3のグループ送信ウィンドウ324と、第4のグループ送信ウィンドウ326とを含み得る。データパス送信ウィンドウの各々は、対応するページングウィンドウと対応するデータウィンドウとを含み得る。例示のために、第1のグループ送信ウィンドウ320は、第1のページングウィンドウ332と第1のデータウィンドウ334とを含み得、第2のグループ送信ウィンドウ322は、第2のページングウィンドウ342と第2のデータウィンドウ344とを含み得、第3のグループ送信ウィンドウ324は、第3のページングウィンドウ352と第3のデータウィンドウ354とを含み得、第4のグループ送信ウィンドウ326は、第4のページングウィンドウ362と第4のデータウィンドウ364とを含み得る。

10

20

30

40

50

【0106】

[0118]いくつかの実装形態では、各グループ送信ウィンドウは、第1の発見ウィンドウ310など、NAN通信チャネルの発見ウィンドウからのオフセットを含む。デバイスは、第1の発見ウィンドウ310からのオフセットに基づいてグループ送信ウィンドウ、ページングウィンドウ、またはデータパスウィンドウの開始または終了を決定し得る。第1の発見ウィンドウ310と第2の発見ウィンドウ312との間の継続時間は、グループ鍵更新ウィンドウを含むか、またはそれに対応し得る。

【0107】

[0119]発見ウィンドウ中に、データリンクグループのデバイスの各々は、起動している（たとえば、省電力モード、低電力モード、またはスリープモードにない）ことがあり、ビーコン、メッセージ、またはその両方を監視し得る。いくつかの実装形態では、ビーコン、メッセージ、またはその両方は、後続のデータウィンドウ中に送られるべきトラフィックを示し得る。発見ウィンドウ中に送られるビーコン、メッセージ、またはそれらの組合せは、セキュアである（たとえば、符号化または暗号化されている）ことも、セキュアでない（たとえば、符号化または暗号化されていない）こともある。セキュアなビーコン、セキュアなメッセージ、またはその両方が発見ウィンドウ中に送信されるとき、セキュアなビーコン、セキュアなメッセージ、またはその両方は、アクティブグループ鍵、アクティブ配布鍵、または完全性グループ鍵などの鍵を使用して符号化され得る。たとえば、アクティブグループ鍵およびアクティブ配布鍵は、それぞれ、図1の第1のグループ鍵132と図1の第1の配布鍵134とを含むか、またはそれに対応し得る。完全性グループ鍵は、図1の完全性グループ鍵を含むか、またはそれに対応し得る。特定のデバイスが、発見ウィンドウ中に受信されたビーコン、メッセージ、またはその両方に基づいて特定のデバイスがデータを受信し得ると決定する場合、特定のデバイスは、後続のデータウィンドウ中に起動したままであることがある。特定のデバイスが、発見ウィンドウ中にビーコン、メッセージ、またはその両方を受信しない場合、特定のデバイスは、後続のデータウィンドウ中に「スリープに移行する」（たとえば、スリープモードまたは省電力モードに入る）。

【0108】

[0120]ページングウィンドウ中に、データリンクグループのデバイスの各々は、起動している（たとえば、省電力モード、低電力モード、またはスリープモードにない）ことがあり、ビーコン、メッセージ、またはその両方を監視し得る。いくつかの実装形態では、ビーコン、メッセージ、またはその両方は、後続のデータウィンドウ中に送られるべきトラフィックを示し得る。ページングウィンドウ中に送られるビーコン、メッセージ、またはその両方は、セキュアである（たとえば、符号化または暗号化されている）ことも、セキュアでない（たとえば、符号化または暗号化されていない）こともある。セキュアなビーコン、セキュアなメッセージ、またはその両方がページングウィンドウ中に送信される

とき、セキュアなビーコン、セキュアなメッセージ、またはその両方は、アクティブグループ鍵、アクティブ配布鍵、またはペアワイズ鍵などの鍵を使用して符号化され得る。たとえば、アクティブグループ鍵およびアクティブ配布鍵は、それぞれ、図1の第1のグループ鍵132と図1の第1の配布鍵134とを含むか、またはそれに対応し得る。ペアワイズ鍵は、図1のペアワイズ鍵146を含むか、またはそれに対応し得る。特定のデバイスが、ページングウィンドウ中に受信されたビーコン、メッセージ、またはそれらの組合せに基づいてそれがデータを受信し得ると決定する場合、特定のデバイスは、後続のデータウィンドウ中に起動したままでいることがある。特定のデバイスが、ページングウィンドウ中にビーコン、メッセージ、またはその両方を受信しない場合、特定のデバイスは、後続のデータウィンドウ中に「スリープに移行する」(たとえば、スリープモードまたは省電力モードに入る)。

【0109】

[0121]第1のグループ送信ウィンドウ320の第1のページングウィンドウ332を参照すると、第1のデバイスは、データリンクグループの1つまたは複数のデバイスにデータリンクグループチャネル304を介して告知メッセージ336を送信し得る。告知メッセージ336は、第1のデバイスが、データリンクグループのデバイスに配布されるべき図1の第2のグループ鍵142または図2のグループ鍵214などの候補グループ鍵を有することを示し得る。たとえば、告知メッセージ336は、図1の告知メッセージ160または告知メッセージ170を含むか、またはそれに対応し得る。告知メッセージ336に回答して、第2のデバイスは、候補グループ鍵を要求するために第1のデバイスに要求338を送り得る。要求338は、告知メッセージ336と同じページングウィンドウ中に送られるものとして示されているが、他の実装形態では、要求338は、後のページングウィンドウまたは発見ウィンドウ中に第2のデバイスから送られ得る。

【0110】

[0122]第1のデータウィンドウ334中に、要求338に回答して、第1のデバイスと第2のデバイスとは、第1のデバイスが第2のデバイスに候補グループ鍵を送ることを可能にするためにP2P通信を実行し得る。データリンクグループの他のデバイスは、第1のデータウィンドウ334中に起動していない(たとえば、スリープモードまたは省電力モードにある)ことがある。

【0111】

[0123]第2のページングウィンドウ342中に、第2のデバイスは、データリンクグループの1つまたは複数のデバイスにデータリンクグループチャネル304を介して告知メッセージ346を送信し得る。たとえば、告知メッセージ346は、第1のデバイスによって発行された告知メッセージ336に基づき得るか、または第1のデバイスによって発行された告知メッセージ336の転送バージョンであり得る。告知メッセージ346に回答して、第3のデバイスは、候補グループ鍵を要求するために第2のデバイスに要求348を送り得る。第2のデータウィンドウ344中に、第2のデバイスと第3の第2のデバイスとは、第2のデバイスが第3のデバイスに候補グループ鍵を送ることを可能にするためにP2P通信を実行し得る。データリンクグループの第1のデバイスなどの他のデバイスは、第2のデータウィンドウ344中に起動していない(たとえば、スリープモードまたは省電力モードにある)ことがある。

【0112】

[0124]第3のページングウィンドウ352中に、ビーコンまたはメッセージは、通信されないことがある。したがって、第3のデータウィンドウ354中に、データリンクグループのデバイスのすべてが起動していないことがある。第4のページングウィンドウ362中に、第1のデバイスは、データリンクグループの1つまたは複数のデバイスにマルチキャスト告知メッセージ366を送信し得る。したがって、告知メッセージ366を受信したデータリンクグループのデバイスのすべては、第1のデバイスがデータリンクグループの他のデバイスにメッセージをマルチキャストすることを可能にするために、第4のデータウィンドウ364中に起動していることがある。

10

20

30

40

50

【 0 1 1 3 】

[0125]このようにして、図 3 に、送信されるべきデータトラフィックのデータリンクグループを他のデバイスに通知するためにページングウィンドウまたは発見ウィンドウ中にデバイスがビーコン、メッセージ、またはそれらの組合せをどのように送り得るのかについて示す。送信されるべきデータトラフィックを他のデバイスに通知することによって、データトラフィックを受信することを目的としない 1 つまたは複数のデバイスは、データウィンドウ中に起動しない（たとえば、スリープモードまたは省電力モードに入り）、したがって、電力を節約し得る。

【 0 1 1 4 】

[0126]図 4 を参照すると、第 1 の代表的なデバイス 4 0 2 と第 2 の代表的なデバイス 4 0 4 との間で通信する方法 4 0 0 の例示的な実装形態が示されている。方法 4 0 0 は、ラダー図によって示されている。第 1 のデバイス 4 0 2 と第 2 のデバイス 4 0 4 とは、N A N の同じデータリンクグループなどの同じデータリンクグループ中に含まれ得る。たとえば、第 1 のデバイス 4 0 2 と第 2 のデバイス 4 0 4 とは、図 1 のデバイス 1 0 4 ~ 1 1 0 、図 2 のデバイス 2 0 2 、または図 3 を参照しながら説明されるデバイスを含むか、またはそれに対応し得る。データリンクグループが 2 つのデバイス（たとえば、第 1 のデバイス 4 0 2 と第 2 のデバイス 4 0 4 と）を含むものとして説明されるが、他の実装形態では、データリンクグループは 3 つ以上のデバイスを含み得る。

【 0 1 1 5 】

[0127]第 1 のデバイス 4 0 2 は、4 1 2 において、第 1 のデバイス 4 0 2 の第 1 のアクティブ鍵（たとえば、第 1 のアクティブ鍵セット）として第 1 のグループ鍵と第 1 の配布鍵とを設定し得る。第 1 のグループ鍵および第 1 の配布鍵は、それぞれ、図 1 の第 1 のグループ鍵 1 3 2 と第 1 の配布鍵 1 3 4 とを含むか、またはそれに対応し得る。第 2 のデバイス 4 0 4 は、4 1 4 において、第 2 のデバイス 4 0 4 の第 2 のアクティブ鍵（たとえば、第 2 のアクティブ鍵セット）として第 1 のグループ鍵と第 1 の配布鍵とを設定し得る。第 1 のデバイス 4 0 2 は、第 2 のデバイス 4 0 4 が第 2 のアクティブ鍵を設定する前に、その後に、またはそれと同時に第 1 のアクティブ鍵を設定し得る。

【 0 1 1 6 】

[0128]第 1 のデバイス 4 0 2 は、4 2 2 において、第 1 のランダム値を使用して第 1 のカウントダウンを開始し得、第 2 のデバイス 4 0 4 は、4 2 4 において、第 2 のランダム値を使用して第 2 のカウントダウンを開始し得る。たとえば、第 1 のランダム値、第 2 のランダム値、またはその両方は、図 2 のランダム値 2 2 0 を含むか、またはそれに対応し得る。第 1 のカウントダウンは、第 1 のデバイス 4 0 2 において実行される候補グループ鍵（たとえば、候補鍵セット）生成手順に対応し得、第 2 のカウントダウンは、第 2 のデバイス 4 0 4 において実行される候補グループ鍵生成手順に対応し得る。第 1 のデバイス 4 0 2 は、第 2 のデバイス 4 0 4 が第 2 のカウントダウンを開始する前に、その後に、またはそれと同時に第 1 のカウントダウンを開始し得る。

【 0 1 1 7 】

[0129]第 1 のデバイス 4 0 2 は、4 3 2 において、第 1 のカウントダウンの終了を検出し、第 2 のグループ鍵と第 2 の配布鍵とを生成し得る。たとえば、第 1 のデバイス 4 0 2 は、図 2 のカウンタ 2 0 4 などのカウンタの値に基づいて第 1 のカウントダウンの終了を検出し得る。第 2 のグループ鍵は、図 1 の第 2 のグループ鍵 1 4 2 または図 2 のグループ鍵 2 1 4 を含むか、またはそれに対応し得る。第 2 の配布鍵は、図 1 の第 2 の配布鍵 1 4 4 を含むか、またはそれに対応し得る。第 2 のグループ鍵と第 2 の配布鍵とを生成するために、第 1 のデバイス 4 0 2 は、図 1 の鍵論理 1 1 2 または図 2 の鍵生成器 2 0 6 などの 1 つまたは複数の鍵生成器を含み得る。

【 0 1 1 8 】

[0130]第 1 のデバイス 4 0 2 は、4 3 3 において、第 2 のデバイス 4 0 4 に告知メッセージを送り得る。たとえば、告知メッセージは、図 1 の告知メッセージ 1 6 0 を含むか、またはそれに対応し得る。告知メッセージは、第 1 のデバイス 4 0 2 が配布されるべき第

10

20

30

40

50

2のグループ鍵を有することを第2のデバイス404に示し得る。いくつかの実装形態では、告知メッセージは、マルチキャストトラフィック告知メッセージなどのマルチキャストメッセージを含み得る。告知メッセージは、第2のグループ鍵が生成された後に送られるものとして説明されるが、他の実装形態では、告知メッセージは、第1のカウントダウンの終了が検出された後の、第2のグループ鍵が生成される前に送られ得る。

【0119】

[0131]第2のデバイス434は、434において、第2のカウントダウンを終了し得る。たとえば、第2のデバイス434は、第1のデバイス402から告知メッセージを受信したことに応答して候補グループ鍵生成手順を抑制し得る。

【0120】

[0132]第1のデバイス402は、442において、第1の配布鍵を使用して第2のグループ鍵と第2の配布鍵とを符号化(または暗号化)し得る。第1のデバイス402は、443において、第2のデバイス404に鍵配信メッセージを送り得る。たとえば、鍵配信メッセージは、図1の鍵配信メッセージ180を含むか、またはそれに対応し得る。鍵配信メッセージは、符号化(または暗号化)された第2のグループ鍵と符号化(または暗号化)された第2の配布鍵とを含み得る。いくつかの実装形態では、第1のデバイス402は、第1のデバイス402に関連するかまたは関連しないデータリンクグループのデバイスによって受信され得るマルチキャストメッセージとして第2のデバイス404に鍵配信メッセージを送り得る。符号化(または暗号化)された第2のグループ鍵と符号化(または暗号化)された第2の配布鍵とが、単一の鍵配信メッセージ中に含まれるものとして説明されるが、他の実装形態では、符号化(または暗号化)された第2のグループ鍵と符号化(または暗号化)された第2の配布鍵とは別個のメッセージ中で送られ得る。

【0121】

[0133]第2のデバイス404は、444において、第1の配布鍵を使用して符号化(または暗号化)された第2のグループ鍵と符号化(または暗号化)された第2の配布鍵とを復号(または解読)し得る。第1のデバイス402は、452において、第1のアクティブ鍵として第2のグループ鍵と第2の配布鍵とを設定し得、第2のデバイス404は、454において、第2のアクティブ鍵として第2のグループ鍵と第2の配布鍵とを設定し得る。配布鍵を使用するものとして説明されるが、他の実装形態では、候補グループ鍵を符号化(または暗号化)するために配布鍵が使用されないことがある。たとえば、第1のデバイス402は、第1のグループ鍵に基づいて第2のグループ鍵を符号化(または暗号化)し得る。

【0122】

[0134]第2のグループ鍵を符号化(または暗号化)するために第2の第1の配布鍵を使用することによって、第1のデバイス402は、第2のグループ鍵を符号化(または暗号化)し、マルチキャストメッセージとしてデータリンクグループの1つまたは複数のデバイス(たとえば、第2のデバイス404)に第2のグループ鍵を配布し得る。第1の配布鍵が、データリンクグループの各デバイス(たとえば、第2のデバイス404)に知られるので、マルチキャストメッセージは、1つまたは複数のデバイスが第1のデバイス402に関連するのに関連しないのかにかかわらず、1つまたは複数のデバイスに符号化(または暗号化)された第2のグループ鍵を直接送るために使用され得る。したがって、第2のグループ鍵を配布するために、追加のセキュリティ関連付け手順、P2P通信、またはそれらの組合せがデータリンクグループの他のデバイスと第1のデバイスによって実行されない。したがって、配布鍵がデータリンクグループによって使用されるとき、第2のグループ鍵を配布するデータトラフィックの量は、第2のグループ鍵を配布するために配布鍵が使用されないときと比較して低減され得る。

【0123】

[0135]図5を参照すると、データリンクグループ内の通信を示す特定の例示的なタイミング図500が示されている。図5に、データリンクグループのグループ鍵(アクティブグループ鍵など)の寿命および満了を示す。時間t0(図示せず)に、第1のグループ鍵

(鍵1)の生成が開始され得るか、または第1のグループ鍵(鍵1)が生成され得る。第1のグループ鍵(鍵1)の生成について、少なくとも図2を参照しながら説明される。第1のグループ鍵(鍵1)に対応するタイムスタンプが、生成され、図1の鍵配信メッセージ180などのメッセージ中に含まれ得る。特定の実装形態では、鍵識別子143は、タイムスタンプを含み得る。第1のグループ鍵(鍵1)が、第1のグループ鍵(鍵1)に対応するデータリンクグループのデバイス間で送信されるとき、タイムスタンプは、第1のグループ鍵(鍵1)とともにメッセージ中に含まれ得る。図示のように、鍵1は、時間t1にアクティブ鍵になる。データリンクグループのデバイスは、時間t1にカウントダウンを開始し得る。カウントダウンは、第1のグループ鍵(鍵1)の存続期間、関連付けウィンドウまでの時間期間、または他のタイミング情報を示し得る。単一のカウントダウンについて説明されるが、いくつかの実装形態では、複数のカウントダウンが使用され得る。他の実装形態では、カウントダウンは、デバイスが告知メッセージを受信するのに対応する時間などの前の時間に開始し得る。

【0124】

[0136]時間t2に開始し、時間t3に終了する発見ウィンドウ中に、第2のグループ鍵(鍵2)に対応する告知メッセージ510は、データリンクグループのデバイスによって送信される。告知メッセージ510は、データリンクグループのデバイスが第2のグループ鍵(鍵2)を生成するのに応答して送信され得る。告知メッセージ510は、図1の告知メッセージ160、告知メッセージ170、またはそれらの組合せを含むか、またはそれに対応し得る。発見ウィンドウ中に送信される告知メッセージとして説明されるが、他の実装形態では、第2のグループ鍵(鍵2)は、図1および図3を参照しながら説明されるように、データリンクグループのページングウィンドウ中に送信されるページングメッセージによって告知され得る。

【0125】

[0137]告知メッセージ510が特定のデバイスによって送信された後、特定のデバイスは、図1を参照しながら説明されるように、データリンクグループの他のデバイスに第2のグループ鍵(鍵2)を配布するために、ページングメッセージと鍵配信メッセージとを送信し得る。さらに、第2のグループ鍵(鍵2)を受信するデバイスはまた、第2のグループ鍵(鍵2)がデータリンクグループ全体にわたって伝搬するように、他のデバイスに第2のグループ鍵(鍵2)を伝搬し得る。しかしながら、データリンクグループの1つまたは複数のデバイスは、時間t4に発生する関連付けウィンドウの開始時に第2のグループ鍵(鍵2)を受信していないことがある。たとえば、デバイスは、鍵生成器デバイスから複数ホップ離れていることがあり得、第2のグループ鍵(鍵2)は、デバイスに達していないことがあるか、またはデバイスは、特定のデバイスに関連しないことがあり、特定のデバイスは、関連付けウィンドウの開始時にデバイスに第2のグループ鍵(鍵2)を送信していない。関連付けウィンドウは、図1中の第1のデバイス104など、候補グループ鍵(鍵2)を有するデータリンクグループのデバイスに関連しようと1つまたは複数のデバイスが試みる時間に対応し得る。

【0126】

[0138]関連付けウィンドウは、データリンクグループの各デバイスに知られる所定の時間(関連付けしきい値時間)に開始し得る。関連付けウィンドウは、時間t6に第1のグループ鍵(鍵1)の寿命の満了より前に発生し得、時間t6にまたはその前に第2のグループ鍵(鍵2)がアクティブグループ鍵として設定されるより前に発生し得る。特定の実装形態では、関連付けしきい値時間は、IEEE802.11規格、Wi-Fi Alliance規格、NAN規格、またはそれらの組合せなどのワイヤレス通信規格において定義されている。いくつかの実装形態では、関連付けしきい値時間は、図1の鍵配信メッセージ180などの鍵配信メッセージによって示され得る。たとえば、関連付けしきい値時間は、鍵識別子143によって示され得る。他の実装形態では、関連付けしきい値時間は、データリンクグループのデバイスによってネゴシエートされ得る。

【0127】

[0139] 関連付けウィンドウ中に、1つまたは複数のデバイスが関連付け動作 5 2 0 を実行し得る。例示的な例として、図 1 を参照すると、第 4 のデバイス 1 1 0 は、第 1 のデバイス 1 0 4 に関連付け要求 1 7 5 を送り得、第 1 のデバイス 1 0 4 は、関連付けウィンドウ中に第 4 のデバイス 1 1 0 に関連付け応答 1 7 6 または関連付け拒絶 1 7 8 を送り得る。時間 t 5 に、N A N の第 2 の発見ウィンドウが開始する。1つまたは複数の告知メッセージが第 2 の発見ウィンドウ中に送信され得る。時間 t 6 に、第 2 の発見ウィンドウが終了する。いくつかの実装形態では、関連付けウィンドウは、図 5 に示すように、時間 t 6 に終了し、第 2 の発見ウィンドウを含む。他の実装形態では、関連付けウィンドウは、時間 t 5 に終了し得る。

【 0 1 2 8 】

[0140] t 2 から t 6 までの時間期間は、グループ鍵更新ウィンドウに対応し得る。グループ鍵更新ウィンドウは、データリンクグループの1つまたは複数のデバイスがデータリンクのデバイスに第 2 のグループ鍵 (鍵 2) などの候補グループ鍵を配布する時間期間に対応し得る。第 2 のグループ鍵 (鍵 2) を含む鍵配信メッセージ (図示せず) は、グループ鍵更新ウィンドウ中にデータリンクグループのデバイス間で送信され得る。たとえば、図 1 を参照すると、鍵配信メッセージ 1 8 0 は、データリンクグループのデバイスに送信され得る。第 1 の発見ウィンドウの開始と第 2 の発見ウィンドウの終了との間に起こるものとして示されているが、グループ鍵更新ウィンドウは、複数の発見ウィンドウの間に起こり得る。たとえば、告知メッセージ 5 1 0 は、複数の発見ウィンドウ中に送信 (または、再送信) され得る。複数の発見ウィンドウ中に告知メッセージ 5 1 0 を送信することは、データリンクグループの各デバイスが告知メッセージ 5 1 0 を受信する可能性を増加させ得る。

【 0 1 2 9 】

[0141] 第 3 のグループ鍵 (鍵 3) の生成は、時間 t 7 に開始され得、これは、第 2 のグループ鍵 (鍵 2) の満了の前の特定の所定の量の時間に対応し得る。第 2 のグループ鍵 (鍵 2) は、時間 t 8 に満了し得る。いくつかの実装形態では、時間 t 2 と時間 t 6 との間の持続時間は、時間 t 7 と時間 t 8 との継続時間と同じである。他の実装形態では、時間 t 2 および時間 t 6 との間の持続時間は、時間 t 7 と時間 t 8 との継続時間とは異なる。いくつかの実装形態では、第 1 のグループ鍵 (鍵 1) と、第 2 のグループ鍵 (鍵 2) と、第 3 のグループ鍵 (鍵 3) とは、同じ寿命を有する。他の実装形態では、第 1 のグループ鍵 (鍵 1) と、第 2 のグループ鍵 (鍵 2) と、第 3 のグループ鍵 (鍵 3) とは、異なる寿命を有する。

【 0 1 3 0 】

[0142] このようにして、図 5 に、グループ鍵に関係するタイミングと関係する告知メッセージとについて説明する。発見ウィンドウ中に告知メッセージを送信することは、データリンクグループのデバイスがアクティブ動作モードで動作しており、告知メッセージを受信することが可能である可能性を増加させ得る。さらに、関連付けウィンドウの開始までに候補グループ鍵 (たとえば、潜在的な「次の」アクティブグループ鍵) を受信しなかった1つまたは複数のデバイスは、他のデバイスとの関連付け動作を実行するための指定された時間を有し得る。関連付け動作は、デバイスを、候補グループ鍵を有する別のデバイスに関連付け得、それによって、デバイスが候補グループ鍵を受信することが可能になる。関連付けウィンドウの継続時間は、データリンクグループの各デバイスが候補グループ鍵を有するデバイスに関連する時間を有するターゲット可能性を達成するように設定され得る。

【 0 1 3 1 】

[0143] 図 6 を参照すると、例示的なページ属性 6 0 0 の図。ページ属性 6 0 0 は、ページングメッセージ中に含まれ得る。特定の实装形態では、ページ属性 6 0 0 は、図 1 のページ属性 1 6 9 を含むか、またはそれに対応し得る。ページ属性 6 0 0 が、特定のフィールドを含むものとして図 6 に示されているが、例示は限定するものではない。他の実装形態では、ページ属性 6 0 0 のフィールドは、異なる順序で構成され得、図 6 に示すものよ

10

20

30

40

50

りも少ないフィールドまたは多くのフィールドを含み得る。

【0132】

[0144] ページ属性 600 は、属性 ID フィールド 602 を含み得る。ページ属性 600 は、ページ属性 600 の長さを特定する値を含む長さフィールド 604 を含み得る。ページ属性 600 はまた、データリンクグループを特定する値を含むデータリンクグループ ID フィールド 606 を含み得る。データリンクグループ ID フィールド 606 は、NAN データリンク (NDL) 識別子と呼ばれることもある。

【0133】

[0145] ページ属性 600 は、ページ制御フィールド 608 とトラフィックインジケータまたはグループ鍵生成器 ID フィールド 610 をさらに含む。ページ属性 600 は、随意に、トラフィックタイプインジケータ 612 を含む。ページ制御フィールド 608 は、ページ属性 600 に関する情報を示す。ページ制御フィールド 608 のビットの第 1 のセット 620 は、本明細書でさらに説明するように、ページ属性 600 がトラフィックインジケータを含むのか、またはグループ鍵生成器 ID を含むのかを示し得る。さらに、トラフィックインジケータがページ属性 600 中に含まれる場合、ビットの第 1 のセット 620 は、本明細書でさらに説明するように、トラフィックインジケータのタイプを示し得る。ある特定の実装形態では、ビットの第 1 のセット 620 は 3 ビットを含む。ページ制御フィールド 608 のビットの第 2 のセット 622 は、トラフィックタイプインジケータ 612 がページ属性 600 に含まれるのかどうかを示し得る。ページ制御フィールド 608 のビットの第 3 のセット 624 は予備であり得る。他の実装形態では、ページ制御フィールド 608 中のビットは、別様に分割され得る。

【0134】

[0146] ビットの第 1 のセット 620 によって提供される指示を例示すると、ビットの第 1 のセット 620 が第 1 の特定の値を有する場合、ページ属性 600 を含むページングメッセージを送信するデバイスによる送信をスケジュールされるデータは、マルチキャストデータである。特定の実装形態では、データがマルチキャストデータである場合、トラフィックインジケータまたはグループ鍵生成器 ID フィールド 610 はページ属性 600 中に含まれないことがある。この場合、ページ属性 600 を含むページングメッセージを受信する各デバイスは、ページ制御フィールド 608 のビットの第 1 のセット 620 が第 1 の特定の値を有することを検出することに基づいて、アクティブ動作モードにとどまり得る。ビットの第 1 のセット 620 が、第 2 の特定の値、第 3 の特定の値、または第 4 の特定の値を有する場合、トラフィックインジケータまたはグループ鍵生成器 ID フィールド 610 は、トラフィックインジケータを含む。ビットの第 1 のセット 620 が第 2 の特定の値を有する場合、データは、ユニキャストデータであり得、トラフィックインジケータは、トラフィックインジケータマップ (TIM: traffic indicator map) によって表され得る。ビットの第 1 のセット 620 が第 3 の特定の値を有する場合、データは、ユニキャストデータであり得、トラフィックインジケータは、ブルームフィルタによって表され得る。ビットの第 1 のセット 620 が第 4 の特定の値を有する場合、データは、ユニキャストデータであり得、トラフィックインジケータは、MAC アドレスのリストによって表され得る。ビットの第 1 のセット 620 が第 5 の特定の値を有する場合、トラフィックインジケータまたはグループ鍵生成器 ID フィールド 610 は、グループ鍵生成器 ID を含む。この場合、ビットの第 1 のセット 620 は、候補グループ鍵を生成したデバイスの識別子を示す。この場合、グループ鍵生成器 ID は、候補グループ鍵を生成したデバイスの MAC アドレス (または他の識別子) を含み、トラフィックタイプインジケータ 612 が、ページ属性 600 中に含まれる場合、トラフィックタイプインジケータ 612 は、最も優先度の高いトラフィックタイプを示す。たとえば、トラフィックタイプインジケータ 612 は、トラフィックに対応する最高のサービス品質 (QoS) カテゴリを示し得る。

【0135】

[0147] ページ属性 600 がトラフィックインジケータを含む場合、トラフィックインジケータは、可変サイズを有し、次のデータウィンドウ中に特定のデバイスからトラフィ

ックを受信するようにスケジュールされたデバイスのサブセットを示す。トラフィックインジケータは、TIM、ブルームフィルタ、またはMACアドレスのリストによって表され得る。トラフィックインジケータは、図1の第1のデバイス104からのトラフィックなどのトラフィックを受信するようにスケジュールされた各デバイスを識別し得る。いくつかの実装形態では、ページングメッセージは、複数のページ属性600を含み得る。たとえば、ページングメッセージは、(トラフィックインジケータまたはグループ鍵生成器IDフィールド610とページ制御フィールド608とに基づいて)グループ鍵生成器IDを示す第1のページ属性とデータリンクグループの1つまたは複数のデバイスへの送信のためにスケジュールされた他のデータに対応する第2のページ属性とを含み得る。

【0136】

10

[0148]このようにして、図6に、トラフィックを受信するかまたは鍵生成器デバイスのIDを示すようにスケジュールされたデバイスのリストを示すために、サービス発見フレーム(SDF)、(IEEE802.11に記載されている)パブリックアクションフレーム、管理フレーム、またはNAN管理フレームなどのフレーム中に含まれ得るページ属性600を示す。追加または代替として、ページ属性600は、候補グループ鍵の生成を告知するためにページングメッセージ中に含まれ得る。

【0137】

[0149]図7を参照すると、データリンクグループのデバイスにおける動作の方法700の第1の実装形態が示されている。データリンクグループは、インフラストラクチャ不要のピアツーピアネットワークを含み得る。たとえば、データリンクグループは、NANまたはワイヤレスメッシュネットワークの複数のデバイスを含み得る。複数のデバイスは、それら自体の間の(たとえば、複数のデバイスの間の)データ接続性を形成し得る。方法700は、デバイス104~110のいずれか、図2のデバイス202、図3を参照しながら説明されるデバイスのいずれか、または図4のデバイス402、404のいずれかにおいて実行され得る。

20

【0138】

[0150]方法700は、702において、データリンクグループの第1のデバイスにおいて候補グループ鍵を生成することを含む。たとえば、候補グループ鍵は、図1の第2のグループ鍵142または図2のグループ鍵214を含むか、またはそれに対応し得る。候補グループ鍵は、データリンクグループに対応するグループアドレス指定されたデータメッセージの暗号化、解読、またはその両方を可能にするためにアクティブグループ鍵として設定され得る。第2のグループ鍵142は、図1を参照しながら説明されるように、第1のデバイス104によって生成され得る。

30

【0139】

[0151]方法700は、704において、データリンクグループの第1のデバイスから第2のデバイスに、候補グループ鍵の利用可能性を示す告知メッセージを送信すること、ここで、告知メッセージは、データリンクグループ用に指定されたページングウィンドウ中に送信される、およびここで、告知メッセージは、マルチキャストメッセージを含む、を含む。たとえば、ページングウィンドウは、グループ送信ウィンドウの一部であり得る。例示のために、ページングウィンドウは、図3のページングウィンドウ332、342、352、362のうちの1つであり得る。告知メッセージは、図1の告知メッセージ160または告知メッセージ170を含むか、またはそれに対応し得る。

40

【0140】

[0152]いくつかの実装形態では、告知メッセージは、候補グループ鍵を生成したことに応答して送信され得る。たとえば、告知メッセージは、第1のデバイスがデータリンクグループの別のデバイスから候補グループ鍵を受信したことに応答して送信され得る。別の例として、告知メッセージは、第1のデバイスが候補グループ鍵の生成を開始したことに応答して、または第1のデバイスが候補グループ鍵を生成したことに応答して送信され得る。マルチキャストメッセージ(たとえば、告知メッセージ)は、告知メッセージがグループ鍵告知メッセージであることを示す1つまたは複数のビットを含み得る。たとえば、

50

1つまたは複数のビットは、図1のフラグ162を含むか、またはそれに対応し得る。1つまたは複数のビットは、告知メッセージの特定のフィールド中に含まれ得る。告知メッセージはまた、データリンクグループのグループ識別子と候補グループ鍵を生成した特定のデバイスのデバイス識別子とを含み得る。いくつかの実装形態では、第1のデバイスと特定のデバイスとは同じデバイスであり、他の実装形態では、第1のデバイスと特定のデバイスとは異なるデバイスである。グループ識別子およびデバイス識別子は、図1の、それぞれ、グループ識別子164およびデバイス識別子166、を含むか、またはそれに対応し得る。デバイス識別子は、特定のデバイスのMACアドレスであり得る。さらに、告知メッセージは、特定のデバイスによる候補グループ鍵の生成に関連するタイムスタンプを含み得る。

10

【0141】

[0153]いくつかの実装形態では、第1のデバイスは、告知メッセージを送った後に、候補グループ鍵を含む第2のマルチキャストメッセージを送り得る。第2のマルチキャストメッセージは、図1の第1の配布鍵134などの配布鍵を使用して保護され得る。データリンクグループの各デバイスは、配布鍵の対応するコピーを含む。配布鍵は、候補グループ鍵を含む第2のマルチキャストメッセージを符号化、復号、またはその両方を行うためだけに使用されるように構成され得る。

【0142】

[0154]いくつかの実装形態では、第1のデバイスが告知メッセージを送信するとき、第1のデバイスは、データリンクグループの第2のデバイスに関連し得る。たとえば、第1のデバイスが図1の第1のデバイス104であるとき、第2のデバイスは、図1の第2のデバイス106であり得る。第1のデバイスは、第1のデバイスから第2のデバイスに候補グループ鍵に送りたいという第2のデバイスからの要求を受信し得る。第1のデバイスは、第1のデバイスが第2のデバイスに関連することに対応するペアワイズ鍵を使用して候補グループ鍵を暗号化した後に、第2のデバイスに候補グループ鍵を送り得る。たとえば、ペアワイズ鍵は、第1のデバイスと第2のデバイスとの間に実行されるセキュリティ関連付け手順中に生成され得る。ペアワイズ鍵は、セキュリティ関連付け手順の後に第1のデバイスと第2のデバイスとの間のセキュアな通信を可能にし得る。ペアワイズ鍵は、図1のペアワイズ鍵146を含むか、またはそれに対応し得る。

20

【0143】

[0155]他の実装形態では、告知メッセージを送信した後に、第1のデバイスは、データリンクグループの第3のデバイスに関連することを第1のデバイスに求める要求を受信し得る。たとえば、第3のデバイスは、図1の第4のデバイス110を含むか、またはそれに対応し得る。第1のデバイスは、第3のデバイスとのセキュリティ関連付けを行い得、第1のデバイスと第3のデバイスとに対応するペアワイズ鍵は、セキュリティ関連付け中に生成（たとえば、確立）され得る。セキュリティ関連付けの完了の後に、第1のデバイスは、第3のデバイスに候補グループ鍵を送ることを第1のデバイスに求める第2の要求を受信し得る。代替的に、セキュリティ関連付けの完了の後に、第1のデバイスは、第3のデバイスに候補グループ鍵を自動的に送り得る。

30

【0144】

[0156]いくつかの実装形態では、第1のデバイスは、告知メッセージが送信された後に第4のデバイスからメッセージを受信し得る。メッセージは、ザットザメッセージが第2のグループ鍵告知メッセージであることを示し得る。メッセージは、データリンクグループの特定のデバイスによって生成された第2の候補グループ鍵に対応し得る。特定のデバイスと第2のデバイスとは同じデバイスであり得、または特定のデバイスと第2のデバイスとは異なるデバイスであり得る。特定のデバイスと第2のデバイスとが異なるデバイスであるとき、第2のデバイスは、第1のデバイスから1ホップだけ離れていることがあり、特定のデバイスは、第1のデバイスから複数ホップだけ離れていることがある。いくつかの実装形態では、第2の候補グループ鍵は、第1のデバイスによって生成されたアクティブグループ鍵に取って代わり得る。第2の候補グループ鍵を受信する前に、第1のデバ

40

50

イスは、データリンクグループの１つまたは複数のデバイスにマルチキャスト要求を送り得る。マルチキャスト要求に応答して、第１のデバイスは、データリンクグループの特定のデバイスから第２の候補グループ鍵を受信し得る。

【０１４５】

[0157] 第１のデバイスが候補グループ鍵を有する特定のデバイスに関連しないという決定に応答して、第１のデバイスは、第１のデバイスに関連する、候補グループ鍵を有するデータリンクグループの第５のデバイスを識別し得る。第１のデバイスは、データリンクグループの図１の第１のグループ鍵１３２などのアクティブグループ鍵の満了より前に終了する時間期間中に第５のデバイスを識別し得る。時間期間は、第２の告知メッセージが受信された後に開始し得、アクティブグループ鍵の満了の前の所定の時間に終了し得る。たとえば、第１のデバイスは、特定のメッセージが第５のデバイスから第１のデバイスにおいて受信されたことに応答して候補グループ鍵を有するものとして第５のデバイスを識別し得る。特定のメッセージは、第２の告知メッセージが第１のデバイスにおいて受信された後に、その時間期間の終了より前に受信され得る。第１のデバイスは、第５のデバイスに候補グループ鍵を要求し得、アクティブグループ鍵の満了より前に第５のデバイスから候補グループ鍵を受信し得る。いくつかの実装形態では、第１のデバイスは、第２の告知メッセージが受信されると、第５のデバイスに関連し得、第１のデバイスが第５のデバイスから候補グループ鍵を受信すると、第５のデバイスと関連しないことがある。たとえば、第５のデバイスは、配布鍵を使用してマルチキャストメッセージとして第１のデバイスに候補グループ鍵を送信し得る。

【０１４６】

[0158] 方法７００により、データリンクグループのデバイスへの候補グループ鍵の配布が可能になる。候補グループ鍵は、データリンクグループを含むＮＡＮ内での鍵関連のトラフィックとオーバーヘッドとが低減された状態で配布され得る。たとえば、鍵関連のトラフィックは、データリンクグループのデバイスが起動しているときにページングウィンドウ中にグループ鍵告知メッセージなどの告知メッセージを送ることによって低減され得る。別の例として、候補グループ鍵を符号化するためにアクティブ配布鍵が使用され得、符号化された候補グループ鍵が、データリンクグループの１つまたは複数のデバイスにマルチキャストメッセージとして送られ得る。マルチキャストメッセージとして候補グループ鍵を送ることによって、候補グループ鍵は、データリンクグループの第１のデバイスと別のデバイスとの間でセキュリティ関連付け、Ｐ２Ｐ通信、またはそれらの組合せを実行することなしにデータリンクグループの１つまたは複数のデバイスに配布され得る。

【０１４７】

[0159] 図８を参照すると、データリンクグループのデバイスにおける動作の方法８００の第２の実装形態が示されている。方法８００は、ワイヤレス通信のための方法を含むかまたはそれに対応し、デバイス１０４～１１０のいずれか、図２のデバイス２０２、図３を参照しながら説明されるデバイスのいずれか、または図４のデバイス４０２、４０４のいずれかにおいて実行され得る。

【０１４８】

[0160] 方法８００は、８０２において、データリンクグループの第１のデバイスにおいて、グループ鍵と配布鍵とを生成することを含み得る。たとえば、グループ鍵および配布鍵は、図１の第２のグループ鍵１４２と第２の配布鍵１４４とを含むか、またはそれに対応し得る。

【０１４９】

[0161] 方法８００は、８０４において、第２の配布鍵を使用してグループ鍵と配布鍵とを符号化すること、ここで、第２の配布鍵は、データリンクグループのアクティブグループ鍵に対応する、を含み得る。たとえば、第２の配布鍵は、図１の第１の配布鍵１３４を含むか、またはそれに対応し得る。いくつかの実装形態では、第２の配布鍵は、アクティブグループ鍵に対応し得（たとえば、アクティブ鍵セットなどの鍵のセットの一部であり得）、第２の配布鍵は、グループ鍵がアクティブグループ鍵として設定されるまで、鍵配

信メッセージを符号化および復号するために使用可能であり得る。

【 0 1 5 0 】

[0162]方法 8 0 0 は、8 0 6 において、データリンクグループの 1 つまたは複数のデバイスに符号化されたグループ鍵と符号化された配布鍵とを送信することをさらに含む。いくつかの実装形態では、符号化されたグループ鍵と符号化された配布鍵とは、図 1 のワイヤレスネットワーク 1 0 2 などの N A N 中に含まれる複数のデバイスに符号化されたグループ鍵と符号化された配布鍵とをマルチキャストすることによって送信され得る。データリンクグループの各デバイスは、第 2 の配布鍵を含み得、第 2 の配布鍵を使用して符号化されたグループ鍵と符号化された配布鍵とを復号するように構成され得る。

【 0 1 5 1 】

[0163]いくつかの実装形態では、グループ鍵と配布鍵とを生成するより前に、第 2 のグループ鍵（たとえば、候補グループ鍵）と第 2 の配布鍵とがデータリンクグループの別のデバイスから第 1 のデバイスにおいて受信され得る。たとえば、第 2 のグループ鍵は、図 1 の第 1 のグループ鍵 1 3 2 を含むか、またはそれに対応し得る。第 1 のデバイスは、（たとえば、第 2 の候補グループ鍵がアクティブグループ鍵である間に生成される）グループ鍵を生成するより前に第 2 のグループ鍵をアクティブグループ鍵として設定し得る。第 1 のデバイスは、アクティブグループ鍵としての第 2 のグループ鍵の満了を検出したことに応答してグループ鍵をアクティブグループ鍵として設定し得る。したがって、グループ鍵は、データリンクグループのアクティブグループ鍵として第 2 のグループ鍵を置き換え得る。

【 0 1 5 2 】

[0164]いくつかの実装形態では、グループ鍵と配布鍵とを符号化するより前に、図 1 の告知メッセージ 1 6 0 などの告知メッセージが 1 つまたは複数のデバイスに送信され得る。告知メッセージは、グループ鍵に対応し得る。たとえば、告知メッセージは、グループ鍵が配布のために利用可能であることを示し得る。告知メッセージは、グループ送信ウィンドウのページングウィンドウ中に送信され得る。グループ送信ウィンドウは、図 3 のグループ送信ウィンドウ 3 2 0 ~ 3 2 6 のうちの 1 つを含むか、またはそれに対応し得る。符号化されたグループ鍵と符号化された配布鍵とは、グループ送信ウィンドウのデータウィンドウ中に、またはグループ送信ウィンドウの後に発生する別のグループ送信ウィンドウ中に送信され得る。

【 0 1 5 3 】

[0165]方法 8 0 0 により、アクティブ配布鍵（たとえば、第 1 の配布鍵 1 3 4 ）をグループ鍵を符号化するために使用することが可能になり、符号化されたグループ鍵は、データリンクグループの 1 つまたは複数のデバイスにマルチキャストメッセージとして送られ得る。グループ鍵（たとえば、「次の」アクティブグループ鍵として設定するために利用可能な候補鍵）を含むマルチキャストメッセージを送ることによって、グループ鍵は、データリンクグループの第 1 のデバイスと別のデバイスとの間でセキュリティ関連付け、P 2 P 通信、またはそれらの組合せを行うことなしにデータリンクグループの 1 つまたは複数のデバイスに配布され得る。

【 0 1 5 4 】

[0166]図 9 を参照すると、ワイヤレスネットワークのデバイスにおける動作の方法 9 0 0 の第 3 の実装形態が示されている。方法 9 0 0 は、図 1 のデバイス 1 0 4 ~ 1 1 0 のいずれか、図 2 のデバイス 2 0 2、図 3 を参照しながら説明されるデバイスのいずれか、または図 4 のデバイス 4 0 2、4 0 4 のいずれかにおいて実行され得る。

【 0 1 5 5 】

[0167]方法 9 0 0 は、9 0 2 において、データリンクグループの第 1 のデバイスにおいて候補グループ鍵を取得することを含む。たとえば、図 1 を参照すると、第 1 のデバイス 1 0 4 は、第 2 のグループ鍵 1 4 2 を取得し得る。候補グループ鍵は、データリンクグループに対応するグループアドレス指定されたデータメッセージの暗号化、解読、またはその両方を可能にするために潜在的な「次の」アクティブグループ鍵として設定され得る。

いくつかの実装形態では、第 1 のデバイスにおいて候補グループ鍵を取得することは、データリンクグループの別のデバイスから候補グループ鍵を受信することを含み得る。他の実装形態では、候補グループ鍵を取得することは、第 1 のデバイスにおいて候補グループ鍵を生成することを含み得る。

【0156】

[0168]方法 900 は、904 において、データリンクグループの第 1 のデバイスから第 2 のデバイスに、候補グループ鍵の利用可能性を示す告知メッセージを送信することを含む。告知メッセージは、ページングウィンドウ中に、データリンクグループに対応するワイヤレスチャネルを介して送信され得る。いくつかの実装形態では、告知メッセージは、マルチキャストメッセージを含み得る。

10

【0157】

[0169]いくつかの実装形態では、告知メッセージは、候補グループ鍵を取得したことに応答して送信され得る。たとえば、図 1 を参照すると、告知メッセージ 160 は、第 1 のデバイス 104 がデータリンクグループの別のデバイスから第 2 のグループ鍵 142 を受信したことに応答して送信され得る。別の例として、告知メッセージ 160 は、第 1 のデバイス 104 が第 2 のグループ鍵 142 の生成を開始したことに応答して、または第 1 のデバイス 104 が第 2 のグループ鍵 142 を生成したことに応答して送信され得る。マルチキャストメッセージ（たとえば、告知メッセージ 160）は、告知メッセージがグループ鍵告知メッセージであることを示す 1 つまたは複数のビットを含み得る。1 つまたは複数のビットは、告知メッセージ 160 の特定のフィールド中に含まれ得る。告知メッセージ 160 はまた、データリンクグループのグループ ID 164 と第 2 のグループ鍵 142 を生成した特定のデバイスのデバイス ID 166 とを含み得る。

20

【0158】

[0170]いくつかの実装形態では、第 1 のデバイスは、データリンクグループの第 2 のデバイスからトリガメッセージを受信し得、ここで、第 2 のデバイスは、第 1 のデバイスと関連する状態にある。たとえば、第 1 のデバイス 104 は、第 2 のデバイス 106 からトリガメッセージ 167 を受信し得る。第 1 のデバイスは、トリガメッセージを受信したことに応答して第 2 のデバイスに候補グループ鍵を送信し得る。たとえば、第 1 のデバイス 104 は、第 2 のデバイス 106 に第 2 のグループ鍵 142 を含む鍵配信メッセージ 180 を送信し得る。候補グループ鍵は、ペアワイズ鍵に基づいて暗号化され得る。ペアワイズ鍵は、第 1 のデバイスと第 2 のデバイスとの間の関連付けプロセス中に生成され得る。たとえば、第 2 のグループ鍵 142 は、ペアワイズ鍵 146 に基づいて暗号化され得る。特定の実装形態では、候補グループ鍵は、鍵配信メッセージ中に含まれ、鍵配信メッセージは、候補グループ鍵の有効期限を示す鍵識別子を含む。たとえば、鍵配信メッセージ 180 は、第 2 のグループ鍵 142 と鍵識別子 143 とを含み得る。

30

【0159】

[0171]いくつかの実装形態では、アクティブ鍵セットは、アクティブグループ鍵と、アクティブ配布鍵と、アクティブグループ完全性鍵とを含み得る。たとえば、アクティブ鍵セット 130 は、図 1 の第 1 のグループ鍵 132 と、第 1 の配布鍵 134 と、第 1 のグループ完全性鍵 131 とを含み得る。いくつかの実装形態では、候補鍵セットは、候補グループ鍵と、候補配布鍵と、候補グループ完全性鍵とを含み得る。たとえば、候補鍵セット 140 は、図 1 の第 2 のグループ鍵 142 と、第 2 の配布鍵 134 と、第 2 のグループ完全性鍵 141 とを含み得る。

40

【0160】

[0172]いくつかの実装形態では、候補グループ鍵は、アクティブグループ鍵、（アクティブ鍵セットの）アクティブ配布鍵、またはペアワイズ鍵に基づいて符号化され得る。たとえば、第 2 のグループ鍵 142 は、第 1 のグループ鍵 132、第 1 の配布鍵 134、またはペアワイズ鍵 146 に基づいて暗号化され得る。（暗号化された第 2 のグループ鍵 142 を含む）鍵配信メッセージ 180 は、第 1 のグループ鍵 132、第 1 の配布鍵 134、またはペアワイズ鍵 146 に基づいて暗号化され得る。方法 900 は、符号化された候

50

補グループ鍵を送信することを含み得る。符号化された候補グループ鍵は、アクティブグループ鍵、(アクティブ鍵セットの)アクティブ配布鍵、またはペアワイズ鍵に基づいて復号され得る。たとえば、第2の鍵142は、第1のグループ鍵132、第1の配布鍵134、またはペアワイズ鍵146に基づいて解読され得る。特定の実装形態では、グループアドレス指定されたトラフィックは、アクティブ鍵セット中に含まれるアクティブグループ完全性鍵に基づいて検証され得る。

【0161】

[0173]ある実装形態では、第1のデバイスは、グループ鍵更新ウィンドウが満了した後、データリンクグループの特定のデバイスから関連付け要求を受信し得る。特定の実装形態では、第1のデバイスは、関連付け要求を受信したことに応答して特定のデバイスに関連付け応答を送信し得る。関連付け応答により、特定のデバイスが、第1のデバイスに関連することが可能になり得る。たとえば、第1のデバイス104は、第4のデバイス110から関連付け要求175を受信し得、関連付け要求175を受信したことに応答して第4のデバイス110に関連付け応答176を送信し得る。別の実装形態では、第1のデバイスは、基準が満たされないと決定したことに応答して特定のデバイスに関連付け拒絶を送信し得る。たとえば、基準が満たされない場合、第1のデバイス104は、第4のデバイス110に関連付け拒絶178を送信し得る。

【0162】

[0174]いくつかの実装形態では、第1のデバイスは、データリンクグループの第2のデバイスから第2の告知メッセージを受信し得る。第2の告知メッセージは、候補グループ鍵の生成を示し得る。

【0163】

[0175]いくつかの実装形態では、第1のデバイスは、候補グループ鍵をランダムに生成することによって候補グループ鍵を取得し得る。特定の実装形態では、グループ候補鍵は、ランダムに生成された256ビットを含む。いくつかの実装形態では、候補グループ鍵は、ランダム値からのカウントダウンの満了に応答して生成され得る。

【0164】

[0176]いくつかの実装形態では、告知メッセージは、鍵インジケータ、データリンクグループのデータリンクグループ識別子、候補グループ鍵を生成した特定のデバイスのデバイス識別子、またはそれらの組合せを含み得る。たとえば、告知メッセージ160は、鍵インジケータ168と、グループID164と、デバイスID166とを含み得る。特定の実装形態では、鍵インジケータ168は、タイムスタンプ、ハッシュ値、またはその両方を含み得る。

【0165】

[0177]いくつかの実装形態では、鍵インジケータは、第1のデバイスのMACアドレス、ハッシュ値、候補グループ鍵の生成に対応するタイムスタンプ、またはそれらの組合せを含み得る。ハッシュ値は、MACアドレス、候補グループ鍵、またはその両方に基づいて生成され得る。たとえば、告知メッセージ170の鍵インジケータは、第2のデバイス106のMACアドレスを含み得る。デバイス識別子は、第2のグループ鍵142を生成した第1のデバイス104の第2のMACアドレスを含み得る。

【0166】

[0178]いくつかの実装形態では、第1のデバイスは、データリンクグループの第2のデバイスから第2の告知メッセージを受信し得る。第2の告知メッセージは、第2のグループ鍵と第2のタイムスタンプとを含み得る。第1のデバイスは、告知メッセージ中に含まれる第1のタイムスタンプが第2のタイムスタンプよりも前のものであると決定することに基づいて第2のデバイスに候補グループ鍵を送信し得る。特定の実装形態では、第1のデバイス104は、告知メッセージ160の送信の後にデータリンクグループの特定のデバイスから第2の告知メッセージを受信し得る。

【0167】

[0179]いくつかの実装形態では、第1のデバイスは、データリンクグループの鍵生成器

10

20

30

40

50

デバイスとして動作し、データリンクグループの他のデバイスは、鍵生成器デバイスとして動作しないが、第1のデバイスは、鍵生成器デバイスとして動作するように指定される。第1のデバイスが鍵生成器デバイスとしての動作を中止する前に、方法900は、データリンクグループの第1のデバイスから第2のデバイスにメッセージを送信すること、メッセージは、第2のデバイスが、データリンクグループの鍵生成器デバイスとして動作すべきであることを示す、を含み得る。たとえば、第1のデバイス104は、図1を参照しながら説明されるように、第2のデバイスがデータリンクグループの鍵生成器デバイスとして動作すべきであることを示すメッセージを第2のデバイス106に送信し得る。方法900はまた、第1のデバイスにおいて鍵生成動作を終了することを含み得る。方法900は、第1のデバイスによってデータリンクグループとの関連付けを解除すること、第1のデバイスにおいて低電力動作モードに遷移すること、またはその両方を行うことをさらに含み得る。たとえば、第1のデバイス104は、図1を参照しながら説明されるように、鍵生成動作を終了し、低電力動作モードに遷移し得る。

【0168】

[0180]いくつかの実装形態では、第1のデバイスは、データリンクグループの第1のデバイスから第2のデバイスにメッセージを送信し得る。メッセージは、第2のデバイスがデータリンクグループの鍵生成器デバイスとして動作すべきであることを示し得る。第1のデバイスは、メッセージを送った後にデータリンクグループとの関連付けを解除し得る。メッセージを受信したことに応答して、第2のデバイスは、データリンクグループの鍵生成器デバイスとして動作し得る。

【0169】

[0181]他の実装形態では、第1のデバイスは、第2の発見ウィンドウ中に第2の告知メッセージを受信し得、第2の告知メッセージは、データリンクグループの第2のデバイスが第2のグループ鍵を生成したことを示し得る。

【0170】

[0182]いくつかの実装形態では、第1のデバイスは、カウンタを更新し得る。カウンタは、候補グループ鍵の満了に関係し得る。第1のデバイスは、カウンタが特定の値に達したことに応答して新しいグループ鍵を生成し得る。第1のデバイスは、カウンタが特定の値に達するより前に第2の告知メッセージを受信したことに応答してカウンタを更新するのを停止し得る。

【0171】

[0183]いくつかの実装形態では、第1のデバイスは、しきい値数以下のデバイスに関連するように構成され得る。他の実装形態では、第1のデバイスは、必要に応じて他のデバイスに関連する。

【0172】

[0184]いくつかの実装形態では、第1のデバイスは、データリンクグループの第4のデバイスから関連付け要求を受信したことに応答してデータリンクグループの第3のデバイスと関係をたち得る。特定の実装形態では、第1のデバイスが第2のページングウィンドウの終了より前に第3のデバイスにトランスポートされるべきデータをバッファしていないので、第1のデバイスは、第3のデバイスとの関連付けを解除することを決定し得る。別の特定の実装形態では、第1のデバイスは、第4のデバイスから関連付け要求を受信するより前にデータリンクグループの第2のデバイスと関連する状態にあり得、第2のデバイスは、第3のデバイスと関連する状態にあり得る。第4のデバイスは、データリンクグループのデバイスと関連する状態にないことがある。この特定の実装形態では、第1のデバイスは、第3のデバイスが第2のデバイスと関連する状態にあることに基づいて第3のデバイスとの関連付けを解除することを決定し得る。

【0173】

[0185]図10を参照すると、ワイヤレスネットワークのデバイスにおける動作の方法1000の第4の実装形態が示されている。ワイヤレスネットワークは、複数のデータリンクグループを含み得る。方法1000は、デバイス104~110のいずれか、図2のデ

10

20

30

40

50

バイス 2 0 2、図 3 を参照しながら説明されるデバイスのいずれか、または図 4 のデバイス 4 0 2、4 0 4 のいずれかにおいて実行され得る。

【 0 1 7 4 】

[0186]方法 1 0 0 0 は、1 0 0 2 において、データリンクグループの第 1 のデバイスにおいて候補グループ鍵を取得することを含む。たとえば、候補グループ鍵は、図 1 の第 2 のグループ鍵 1 4 2、図 2 のグループ鍵 2 1 4、または図 3 ~ 図 5 を参照しながら説明される鍵のいずれかを含むか、またはそれに対応し得る。図 1 を参照すると、第 1 のデバイス 1 0 4 は、第 2 のグループ鍵 1 4 2 を取得し得る。いくつかの実装形態では、第 1 のデバイスは、第 1 のデバイスにおいて候補グループ鍵を生成することによって候補グループ鍵を取得する。他の実装形態では、第 1 のデバイスは、データリンクグループの別のデバイスから第 1 のデバイスにおいて候補グループ鍵を受信することによって候補グループ鍵を取得する。候補グループ鍵により、データリンクグループに対応するグループアドレス指定されたデータメッセージの暗号化または解読のうちの少なくとも 1 つが可能になり得る。

10

【 0 1 7 5 】

[0187]方法 1 0 0 0 は、1 0 0 4 において、データリンクグループの第 1 のデバイスからデバイスに、利用可能性候補グループ鍵を示す告知メッセージを送信すること、ここで、告知メッセージは、発見ウィンドウ中に、第 1 の通信チャネルを介して送信される、およびここで、告知メッセージは、マルチキャストメッセージを含む、を含む。たとえば、告知メッセージ 1 6 0 は、図 1 の告知メッセージ 1 6 0、告知メッセージ 1 7 0、または図 5 の告知メッセージ 5 1 0 を含むか、またはそれに対応し得る。いくつかの実装形態では、告知メッセージは、発見ウィンドウ中に、N A N 通信チャネルを介して送信され得、告知メッセージは、マルチキャストメッセージであり得る。

20

【 0 1 7 6 】

[0188]いくつかの実装形態では、第 1 の通信チャネルは、図 3 のネイバーアウェアネットワーク (N A N) 通信チャネル 3 0 2 などの N A N 通信チャネルに対応し、グループ鍵更新ウィンドウは、発見ウィンドウの終了と第 2 の発見ウィンドウの開始との間の継続時間を含む。図 3 の第 1 の発見ウィンドウ 3 1 0 と第 2 の発見ウィンドウ 3 1 2 との間の継続時間などのグループ鍵更新ウィンドウは、複数の送信ウィンドウを含み得る。図 1 および図 3 を参照しながら説明されるように、複数の送信ウィンドウの第 1 の送信ウィンドウは、発見ウィンドウの終了からの第 1 のオフセットを有し得、複数の送信ウィンドウの第 2 の送信ウィンドウは、発見ウィンドウの終了からの第 2 のオフセットを有する。

30

【 0 1 7 7 】

[0189]いくつかの実装形態では、方法 1 0 0 0 は、ページングウィンドウ中に N A N の第 1 のデバイスから第 2 のデバイスに、第 1 のデバイスが第 2 のデバイスに送信すべき第 1 のグループ鍵に対応するデータを有することを示すページングメッセージを送信することを含み得る。ページングウィンドウは、グループ送信ウィンドウの一部であり得る。例示のために、ページングウィンドウは、図 3 のページングウィンドウ 3 3 2、3 4 2、3 5 2、3 6 2 のうちの 1 つであり得る。

【 0 1 7 8 】

[0190]いくつかの実装形態では、方法 1 0 0 0 は、第 2 のデバイスからトリガメッセージを受信することと、トリガメッセージを受信したことに応答して候補グループ鍵を送信することとを含み得る。たとえば、トリガメッセージは、図 1 のトリガメッセージ 1 6 7、図 3 の 3 3 8 の要求、または図 3 の要求 3 4 8 を含むか、またはそれに対応し得る。候補グループ鍵は、ペアワイズ鍵に基づいて暗号化され得、ペアワイズ鍵は、第 1 のデバイスと第 2 のデバイスとの間の関連付けプロセス中に生成され得る。たとえば、ペアワイズ鍵は、図 1 のペアワイズ鍵 1 4 6 を含むか、またはそれに対応し得る。肯定応答メッセージは、第 1 のデバイスによって受信され得る。肯定応答メッセージは、第 2 のデバイスが候補グループ鍵を受信したことを示し得る。

40

【 0 1 7 9 】

50

[0191]いくつかの実装形態では、アクティブ鍵セットは、アクティブグループ鍵と、アクティブ配布鍵と、アクティブグループ完全性鍵とを含み得る。たとえば、アクティブ鍵セット130は、図1の第1のグループ鍵132と、第1の配布鍵134と、第1のグループ完全性鍵131とを含み得る。いくつかの実装形態では、候補鍵セットは、候補グループ鍵と、候補配布鍵と、候補グループ完全性鍵とを含み得る。たとえば、候補鍵セット140は、図1の第2のグループ鍵142と、第2の配布鍵134と、第2のグループ完全性鍵141とを含み得る。

【0180】

[0192]いくつかの実装形態では、候補グループ鍵は、アクティブグループ鍵、(アクティブ鍵セットの)アクティブ配布鍵、またはペアワイズ鍵に基づいて符号化され得る。たとえば、第2のグループ鍵142は、第1のグループ鍵132、第1の配布鍵134、またはペアワイズ鍵146に基づいて暗号化され得る。(暗号化された第2のグループ鍵142を含む)鍵配信メッセージ180は、第1のグループ鍵132、第1の配布鍵134、またはペアワイズ鍵146に基づいて暗号化され得る。方法1000は、符号化された候補グループ鍵を送信することを含み得る。符号化された候補グループ鍵は、アクティブグループ鍵、(アクティブ鍵セットの)アクティブ配布鍵、またはペアワイズ鍵に基づいて復号され得る。たとえば、第2の鍵142は、第1のグループ鍵132、第1の配布鍵134、またはペアワイズ鍵146に基づいて解読され得る。特定の実装形態では、グループアドレス指定されたトラフィックは、図1の第1のグループ完全性鍵131など、アクティブ鍵セット中に含まれるアクティブグループ完全性鍵に基づいて検証され得る。

【0181】

[0193]他の実装形態では、候補グループ鍵は、関連付け要求を受信したことに応答して送信され得る。たとえば、(第2のグループ鍵142を含む)鍵配信メッセージ180は、関連付け要求175を受信したことに応答して第1のデバイス104から第4のデバイス110に送信され得る。方法1000はまた、グループ鍵更新ウィンドウが満了した後にNANの特定のデバイスから関連付け要求を受信することを含み得る。グループ鍵更新ウィンドウは、データリンクグループ中での鍵更新動作の実行に対応する特定の時間間隔を含み得る。たとえば、グループ鍵更新ウィンドウは、データリンクグループ中での告知メッセージ、鍵配信メッセージ、またはその両方の生成、送信、受信、またはそれらの組合せに対応し得る。別の実装形態では、方法1000は、関連付け要求を受信したことに応答して特定のデバイスに関連付け応答を送信することを含み、ここで、関連付け応答により、特定のデバイスが、第1のデバイスに関連することが可能になる。たとえば、図1を参照すると、第1のデバイス104は、告知メッセージ160を送信したことに応答して第4のデバイス110から関連付け要求175を受信し得る。第1のデバイス104は、関連付け要求175を受信したことに応答して第4のデバイス110に関連付け応答176を送信し得る。

【0182】

[0194]いくつかの実装形態では、方法1000は、グループ鍵更新ウィンドウが満了した後にデータリンクグループの特定のデバイスから関連付け要求を受信することを含み得る。たとえば、関連付け要求は、図1の関連付け要求175を含むか、またはそれに対応し得る。図3の第1の発見ウィンドウ310と第2の発見ウィンドウ312との間の継続時間などのグループ鍵更新ウィンドウは、データリンクグループ中でのグループ鍵更新動作の実行に対応する特定の時間間隔を含み得る。方法1000はまた、第1の基準を満たすと決定したことに応答して特定のデバイスに関連付け拒絶を送信することを含み得る。たとえば、関連付け拒絶は、図1の関連付け拒絶178を含むか、またはそれに対応し得る。第1の基準は、第1のデバイスに関連するデバイスの数がしきい値以上であるときに満たされ得る。

【0183】

[0195]いくつかの実装形態では、方法1000は、告知メッセージを送信したことに応答して、データリンクグループの特定のデバイスから関連付け要求を受信することを含み

得る。たとえば、第 1 のデバイス 1 0 4 は、図 1 を参照しながら説明されるように、第 1 のデバイス 1 0 4 が告知メッセージ 1 6 0 を送信したことに応答して第 4 のデバイス 1 1 0 から関連付け要求 1 7 5 を受信し得る。方法 1 0 0 0 はまた、第 2 の基準を満たすと決定したことに応答して特定のデバイスに関連付け応答を送信することを含み得る。たとえば、関連付け応答は、図 1 の関連付け応答 1 7 6 を含むか、またはそれに対応し得る。第 2 の基準は、第 1 のデバイスに関連するデバイスの数がしきい値以下であるときに満たされ得る。たとえば、第 1 のデバイス 1 0 4 は、第 1 のデバイス 1 0 4 がしきい値よりも小さい数のデバイスに関連すると決定したことに応答して、関連付け応答 1 7 6 を送信し得る。

【 0 1 8 4 】

10

[0196] 方法 1 0 0 0 は、データリンクグループのデバイスにデータを送信することを含み得る。例示のために、第 1 のデバイスは、データリンクグループのデバイスにデータを送信し得、ここで、データは、候補グループ鍵がアクティブグループ鍵として設定された後に候補グループ鍵に基づいて暗号化される。たとえば、図 1 を参照すると、第 1 のデバイス 1 0 4 は、第 2 のデバイス 1 0 6 にデータを送信し得、データは、第 2 のグループ鍵 1 4 2 がアクティブグループ鍵として設定された後に第 2 のグループ鍵 1 4 2 に基づいて暗号化され得る。

【 0 1 8 5 】

[0197] 方法 1 0 0 0 は、アクティブグループ鍵の満了の前に第 2 の候補グループ鍵を生成することを含み得る。たとえば、第 1 のデバイス 1 0 4 は、第 1 のグループ鍵 1 3 2 の満了より前に第 2 のグループ鍵 1 4 2 を生成し得る。

20

【 0 1 8 6 】

[0198] いくつかの実装形態では、方法 1 0 0 0 は、アクティブグループ鍵として候補グループ鍵を設定することを含み得る。たとえば、第 1 のデバイス 1 0 4 は、図 1 を参照しながら説明されるように、第 1 のグループ鍵 1 3 2 のアクティブグループ鍵としての満了の後に、第 2 のグループ鍵 1 4 2 をアクティブグループ鍵として設定し得る。方法 1 0 0 0 はまた、データリンクグループのデバイスにてアクティブグループ鍵に基づいて暗号化されたデータなどのデータを送信することを含み得る。例示のために、第 1 のデバイス 1 0 4 は、図 1 を参照しながら説明されるように、1 つまたは複数のサービスを提供し、ワイヤレスネットワーク 1 0 2 のデバイスにグループアドレス指定されたトラフィックを送信し得る。方法 1 0 0 0 はまた、アクティブグループ鍵の満了の前に第 2 の候補グループ鍵を生成することを含み得る。方法 1 0 0 0 はまた、データリンクグループの複数の発見ウィンドウ中に第 2 の告知メッセージを送信することを含み得る。第 2 の告知メッセージは、第 2 の候補グループ鍵の利用可能性を示し得る。

30

【 0 1 8 7 】

[0199] 方法 1 0 0 0 は、データリンクグループ用に指定されたページングウィンドウ中にデータリンクグループのデバイスに第 2 の候補グループ鍵を配布することを含み得る。方法 1 0 0 0 はまた、第 1 のデバイスに関連する各デバイスから対応する肯定応答メッセージを受信することに基づいて第 1 のデバイスに関連する各デバイスが第 2 の候補グループ鍵を受信したと決定することを含み得る。たとえば、肯定応答メッセージは、図 1 の A C K を含むか、またはそれに対応し得る。方法 1 0 0 0 は、第 1 のデバイスに関連する各デバイスが第 2 の候補グループ鍵を受信したと決定したことに応答して第 2 の告知メッセージの送信を中止することをさらに含み得る。第 1 のデバイス 1 0 4 は、図 1 を参照しながら説明されるように、第 1 のデバイス 1 0 4 が第 1 のデバイス 1 0 4 に関連する各デバイスから M A C A C K を受信したと決定したことに応答して告知メッセージ 1 7 0 を送信することを停止し得る。

40

【 0 1 8 8 】

[0200] いくつかの実装形態では、候補グループ鍵は、図 1 の鍵インジケータ 1 6 8 などの第 1 の鍵インジケータに関係する。たとえば、鍵インジケータ 1 6 8 は、第 2 のグループ鍵 1 4 2 に関係する情報を与え得、鍵インジケータ 1 6 8 は、第 2 のグループ鍵 1 4 2

50

または第2のグループ鍵142の生成に対応するタイムスタンプに基づいて生成されるハッシュ値を含み得る。方法1000は、データリンクグループの第2のデバイスから第2の候補グループ鍵と第2の鍵インジケータとを含む第2の告知メッセージを受信することを含み得る。方法1000は、鍵インジケータと第2の鍵インジケータとの比較に基づいて伝搬のために候補グループ鍵を選択することをさらに含み得る。

【0189】

[0201]いくつかの実装形態では、第1のデバイスは、第1のデバイスがデータリンクグループの発信者であることに基づいて、第1のデバイスがデータリンクグループの他のデバイスの各デバイスよりも多くのデバイスに関連することに基づいて、第1のデバイスが、データリンクグループの他のデバイスの各デバイスよりも長い時間をデータリンクグループ中で過ごしたことに基づいて、第1のデバイスに関連するデバイスの数に基づいて、データリンクグループのトポロジーに基づいて、第1のデバイスがデータリンクグループ中に含まれた持続時間に基づいて、データリンクグループ内の第1のデバイスのランクに基づいて、第1のデバイスのバッテリーレベルに基づいて、またはそれらの組合せで、鍵生成器デバイスとして動作することを決定する。たとえば、第1のデバイス104は、図1を参照しながら説明されるように、1つまたは複数の基準に基づいて鍵生成器デバイスとして動作することを決定し得る。

【0190】

[0202]図11を参照すると、ワイヤレスネットワークのデバイスにおける動作の方法1100の第5の実装形態が示されている。ワイヤレスネットワークは、複数のデータリンクグループを含み得る。方法1100は、デバイス104~110のいずれか、図2のデバイス202、図3を参照しながら説明されるデバイスのいずれか、または図4のデバイス402、404のいずれかにおいて実行され得る。

【0191】

[0203]方法1100は、1102において、データリンクグループの第2のデバイスにおいて、データリンクグループ用に指定されたページングウィンドウ中に第1の通信チャネルを監視することを含む。たとえば、第1の通信チャネルは、図3のNAN通信チャネル302またはデータリンクグループチャネル304を含むか、またはそれに対応し得る。ページングウィンドウは、図3のページングウィンドウ332、342、352、362のうちの1つを含むか、またはそれに対応し得る。

【0192】

[0204]方法1100は、1104において、ページングウィンドウ中にデータリンクグループの第1のデバイスから第2のデバイスにおいて告知メッセージを受信すること、告知メッセージは、候補グループ鍵の利用可能性を示す、ここで、告知メッセージは、マルチキャストメッセージを含む、を含む。たとえば、告知メッセージは、図1の告知メッセージ160または告知メッセージ170を含むか、またはそれに対応し得る。ページングウィンドウは、図3のグループ送信ウィンドウ320、322、324、326などのグループ送信ウィンドウの一部であり得る。

【0193】

[0205]いくつかの実装形態では、第2のデバイスは、候補グループ鍵を取得し得る。第2のデバイスは、ページングウィンドウ中に告知メッセージを受信したことに応答して第1のデバイスにトリガメッセージを送信することによって、およびデータウィンドウ中に第1のデバイスから候補グループ鍵を受信することによって候補グループ鍵を取得し得る。図1を参照すると、トリガメッセージは、図1のトリガメッセージ167を含むか、またはそれに対応し得る。

【0194】

[0206]他の実装形態では、第2のデバイスは、告知メッセージを受信したことに応答して第1のデバイスにトリガメッセージを送信し得る。たとえば、図1を参照すると、第2のデバイス106は、告知メッセージ160を受信したことに応答して第1のデバイス104にトリガメッセージ167を送信し得る。告知メッセージは、図1の鍵インジケータ

168などの鍵インジケータを含み得る。鍵インジケータは、タイムスタンプ、ハッシュ値、またはその両方を含み得る。

【0195】

[0207]いくつかの実装形態では、第2のデバイスは、ページングウィンドウ中にデータリンクグループの第3のデバイスから第2の告知メッセージを受信し得る。第2の告知メッセージは、第2のタイムスタンプを含み得、第2のグループ鍵の生成を示し得る。第2のデバイスは、告知メッセージの第1のタイムスタンプが第2のタイムスタンプよりも前のものであることに基づいて第1のデバイスにトリガメッセージを送信し得る。第2のデバイスは、トリガメッセージを送信したことに応答して、第1のデバイスから候補グループ鍵を受信し得る。

10

【0196】

[0208]他の実装形態では、第2のデバイスは、第1のデバイスがデータリンクグループとの関連付けを解除すると決定したことに応答して第2のグループ鍵を生成し得る。たとえば、図1を参照すると、第2のデバイス106は、第1のデバイス104がデータリンクグループとの関連付けを解除すると決定したことに応答してグループ鍵を生成し得る。

【0197】

[0209]いくつかの実装形態では、方法1100は、カウンタを更新すること、カウンタは、前のグループ鍵の満了に関係する、を含み得る。たとえば、カウンタは、図2のカウンタ204を含むか、またはそれに対応し得る。方法1100はまた、カウンタが、第2のデバイスによる新しいグループ鍵の生成に関係する特定の値に達するより前に告知メッセージを受信したことに応答してカウンタを更新することを停止することを含み得る。

20

【0198】

[0210]いくつかの実装形態では、方法1100は、告知メッセージ中に含まれる第1の鍵インジケータを識別することを含み得る。たとえば、第2のデバイス106は、図1を参照しながら説明されるように、告知メッセージ160中の鍵インジケータ168を識別し得る。方法1100はまた、ページングウィンドウ中にデータリンクグループの第3のデバイスから第2の告知メッセージを受信することを含み得る。第2の告知メッセージは、第2の鍵インジケータを含み得、第2の候補グループ鍵の生成を示し得る。方法1100は、第2の鍵インジケータよりも高い優先度を有する告知メッセージの第1の鍵インジケータに基づいて第1のデバイスにトリガメッセージを送信することを含み得る。たとえば、第2のデバイス106は、告知メッセージ160の鍵インジケータ168に基づいて第1のデバイス104にトリガメッセージ167を送り得る。方法1100は、トリガメッセージを送信したことに応答して第1のデバイスから候補グループ鍵を受信することをさらに含み得る。

30

【0199】

[0211]いくつかの実装形態では、方法1100は、告知メッセージを受信するより前に、第2の候補グループ鍵の生成を開始することを含み得る。たとえば、第2のデバイス106は、図1を参照しながら説明されるように、第1のデバイス104から告知メッセージ160を受信するより前に候補グループ鍵を生成し得る。方法1100はまた、告知メッセージを受信したことに応答して、第2の候補グループ鍵の生成を停止することを含み得る。たとえば、第2のデバイス106は、第1のデバイス104から告知メッセージ160などの告知メッセージを受信したことに応答して、候補グループ鍵の生成を停止するかまたは候補グループ鍵を抑制し得る。

40

【0200】

[0212]いくつかの実装形態では、方法1100は、告知メッセージを受信したことに応答して、データリンクグループのデバイスに告知メッセージを再送信することを含み得る。たとえば、第2のデバイス106は、第1のデバイス104から告知メッセージ160を受信したことに応答して第3のデバイス108と第4のデバイス110とに告知メッセージ170を送信し得る。

【0201】

50

[0213]いくつかの実装形態では、方法 1 1 0 0 は、告知メッセージを受信したことに応答して、第 2 のデバイスが第 1 のデバイスに関連するのかどうかを決定することを含み得る。方法 1 1 0 0 はまた、第 1 のデバイス 1 0 4 が第 2 のデバイス 1 0 6 に関連するという決定に応答して、第 1 のデバイス 1 0 4 に候補グループ鍵を要求することを含み得る。たとえば、第 2 のデバイス 1 0 6 は、図 1 を参照しながら説明されるように、第 2 のデバイス 1 0 6 が第 1 のデバイス 1 0 4 に関連すると決定し得る。

【 0 2 0 2 】

[0214]いくつかの実装形態では、方法 1 1 0 0 は、告知メッセージを受信したことに応答して、第 2 のデバイスが第 1 のデバイスに関連するのかどうかを決定することを含み得る。方法 1 1 0 0 はまた、第 2 のデバイスが第 1 のデバイスに関連しないという決定に応答して、候補グループ鍵を受信し、第 2 のデバイスに関連するデータリンクグループの第 3 のデバイスを識別することを含み得る。たとえば、第 4 のデバイス 1 1 0 は、図 1 を参照しながら説明されるように、第 4 のデバイス 1 1 0 が第 1 のデバイス 1 0 4 に関連しないと決定し得る。第 4 のデバイス 1 1 0 は、第 2 のグループ鍵 1 4 2 がページングメッセージ 1 6 5 または告知メッセージ 1 7 0 をベースされたものとして第 2 のデバイス 1 0 6 を識別し得る。第 3 のデバイスは、データリンクグループのアクティブグループ鍵の満了より前に終了する時間期間中に識別され得る。時間期間は、告知メッセージが受信された後に開始し、アクティブグループ鍵の満了の前の所定の時間に終了し得る。方法 1 1 0 0 は、第 3 のデバイスに候補グループ鍵を要求することを含み得る。方法 1 1 0 0 は、アクティブグループ鍵の満了より前に第 3 のデバイスから候補グループ鍵を受信することをさらに含み得る。たとえば、第 4 のデバイス 1 1 0 は、トリガメッセージ 1 6 7 を送信することによって第 2 のグループ鍵 1 4 2 を要求し得、第 2 のグループ鍵 1 4 2 を含む鍵配信メッセージ 1 8 0 を受信し得る。

【 0 2 0 3 】

[0215]いくつかの実装形態では、方法 1 1 0 0 は、第 2 のデバイスが第 1 のデバイスに関連しないという決定に応答して第 3 のデバイスとのセキュリティ関連付けを実行することを含み得る。特定の実装形態では、セキュリティ関連付けは、図 1 のペアワイズ鍵 1 4 6 などのペアワイズ鍵を確立する。

【 0 2 0 4 】

[0216]方法 1 1 0 0 はまた、第 3 のデバイスから符号化された候補グループ鍵を受信することを含み得る。方法 1 1 0 0 は、第 2 のデバイスにおいて候補グループ鍵を生成するためにペアワイズ鍵に基づいて符号化された候補グループ鍵を復号することを含み得る。たとえば、ペアワイズ鍵は、図 1 のペアワイズ鍵 1 4 6 を含むか、またはそれに対応し得る。方法 1 1 0 0 は、メモリに候補グループ鍵を記憶することをさらに含み得る。たとえば、メモリは、図 2 の鍵記憶装置 2 0 8 を含むか、またはそれに対応し得る。

【 0 2 0 5 】

[0217]いくつかの実装形態では、方法 1 1 0 0 は、第 2 のデバイスが第 1 のデバイスに関連しないという決定に応答して、データリンクグループのアクティブグループ鍵の満了の前の所定の時間を識別することを含み得る。方法 1 1 0 0 はまた、所定の時間の前に、データリンクグループの少なくとも 1 つのデバイスに候補グループ鍵についてのマルチキャスト要求を送ることを含み得る。方法 1 1 0 0 は、マルチキャスト要求に応答してデータリンクグループの第 3 のデバイスから候補グループ鍵を受信することをさらに含み得る。

【 0 2 0 6 】

[0218]図 1 2 を参照すると、ワイヤレスネットワークのデバイスにおける動作の方法 1 2 0 0 の第 6 の実装形態が示されている。ワイヤレスネットワークは、複数のデータリンクグループを含み得る。方法 1 2 0 0 は、図 1 のデバイス 1 0 4 ~ 1 1 0 のいずれか、図 2 のデバイス 2 0 2、図 3 を参照しながら説明されるデバイスのいずれか、または図 4 のデバイス 4 0 2、4 0 4 のいずれかにおいて実行され得る。

【 0 2 0 7 】

10

20

30

40

50

[0219]方法 1 2 0 0 は、1 2 0 2 において、データリンクグループの第 2 のデバイスにおいて、データリンクグループに対応する発見ウィンドウ中に第 1 の通信チャネルを監視することを含む。たとえば、第 1 の通信チャネルは、図 3 の N A N 通信チャネル 3 0 2 またはデータリンクグループチャネル 3 0 4 を含むか、またはそれに対応し得る。発見ウィンドウは、図 3 の第 1 の発見ウィンドウ 3 1 0 と第 2 の発見ウィンドウ 3 1 2 とを含むか、またはそれに対応し得る。図 1 を参照すると、ワイヤレスネットワーク 1 0 2 (たとえば、N A N) のデータリンクグループの第 2 のデバイス 1 0 6 は、データリンクグループの発見ウィンドウ中にデータリンクグループに対応するワイヤレスチャネルを監視し得る。

【 0 2 0 8 】

10

[0220]方法 1 2 0 0 は、1 2 0 4 において、発見ウィンドウ中にデータリンクグループの第 1 のデバイスから第 2 のデバイスにおいて告知メッセージを受信すること、ここで、告知メッセージは、候補グループ鍵の利用可能性を示す、およびここで、告知メッセージは、マルチキャストメッセージを含む、を含む。たとえば、告知メッセージは、図 1 の告知メッセージ 1 6 0、告知メッセージ 1 7 0、または図 5 の告知メッセージ 5 1 0 を含むか、またはそれに対応し得る。

【 0 2 0 9 】

[0221]特定の実装形態では、第 2 のデバイスは、図 2 のカウンタ 2 0 4 に基づくカウントダウンなどのカウントダウンの満了に応答して第 1 のデバイスに関連付け要求を送信し得る。たとえば、第 4 のデバイス 1 1 0 は、第 1 のデバイス 1 0 4 に関連付け要求 1 7 5

20

【 0 2 1 0 】

[0222]いくつかの実装形態では、第 2 のデバイスは、データリンクグループのページングウィンドウ中に第 1 のデバイスからページングメッセージを受信したことに応答して第 1 のデバイスにトリガメッセージを送信し得る。第 2 のデバイスは、トリガメッセージに応答して第 2 のデバイスにおいて第 1 のデバイスから候補グループ鍵を受信し得る。たとえば、第 2 のデバイス 1 0 6 は、図 1 を参照しながら説明されるように、第 1 のデバイスからページングメッセージ 1 6 5 を受信したことに応答して第 1 のデバイス 1 0 4 にトリガメッセージ 1 6 7 を送信し得る。第 2 のデバイス 1 0 6 は、第 1 のデバイス 1 0 4 から第 2 のグループ鍵 1 4 2 を受信し得る。

30

【 0 2 1 1 】

[0223]他の実装形態では、第 2 のデバイスは、告知メッセージを受信したことに応答して第 1 のデバイスに関連付け要求を送信し得る。たとえば、図 1 を参照すると、第 2 のデバイス 1 0 6 が第 1 のデバイス 1 0 4 に関連しないとき、告知メッセージ 1 6 0 を受信したことに応答して第 1 のデバイス 1 0 4 に関連付け要求 1 7 5 を送信し得る。

【 0 2 1 2 】

[0224]特定の実装形態では、第 2 のデバイスは、第 1 のデバイスから関連付け応答を受信したことに応答して第 1 のデバイスに関連し得る。図 1 の関連付け応答 1 7 6 などの関連付け応答は、第 1 のデバイスが関連するために利用可能であることを示し得る。第 2 のデバイスは、第 2 のデバイスにおいて第 1 のデバイスから候補グループ鍵を受信し得る。第 2 のデバイスは、第 1 のデバイスから図 1 の関連付け拒絶 1 7 8 などの関連付け拒絶を受信したことに応答して第 1 のデバイスに第 2 の関連付け要求を送信し得る。

40

【 0 2 1 3 】

[0225]いくつかの実装形態では、告知メッセージは、第 1 の通信チャネルを介して受信され得る。たとえば、第 1 の通信チャネルは、図 3 の N A N 通信チャネル 3 0 2 を含む得る。方法 1 2 0 0 はまた、第 2 の通信チャネルのページングウィンドウ中に第 1 のデバイスからページングメッセージを受信したことに応答して、第 2 の通信チャネルを介して、第 1 のデバイスにトリガメッセージを送信することを含む得る。たとえば、第 2 の通信チャネルは、図 3 のデータリンクグループチャネル 3 0 4 を含む得る。ページングメッセージは、図 1 のページングメッセージ 1 6 5 またはページングメッセージ 1 9 0 を含むか、

50

またはそれに対応し得る。方法 1 2 0 0 は、第 2 のデバイスにおいて第 1 のデバイスから候補グループ鍵を受信することと、完全性グループ鍵に基づいて候補グループ鍵を検証することとをさらに含み得る。

【 0 2 1 4 】

[0226]いくつかの実装形態では、方法 1 2 0 0 は、告知メッセージを受信した後に、カウントダウンを開始することを含み得る。方法 1 2 0 0 はまた、カウントダウンの満了に応答して、第 2 のデバイスによって、第 2 のデバイスが候補グループ鍵を受信しなかったと決定することを含み得る。方法 1 2 0 0 は、第 2 のデバイスがカウントダウンの満了までに候補グループ鍵を受信しなかったと決定したことに応答して第 1 のデバイスに関連付け要求を送信することをさらに含み得る。たとえば、第 4 のデバイス 1 1 0 は、図 1 を参照しながら説明されるように、それが第 2 のグループ鍵 1 4 2 を受信しなかったと決定し得、第 1 のデバイス 1 0 4 に関連付け要求 1 7 5 を送信し得る。

【 0 2 1 5 】

[0227]いくつかの実装形態では、方法 1 2 0 0 は、第 1 の鍵インジケータを含む告知メッセージを受信するより前に、第 2 のデバイスにおいて第 2 の候補グループ鍵と第 2 の候補グループ鍵の第 2 の鍵インジケータとを生成することを含み得る。たとえば、第 1 のデバイス 1 0 4 は、図 1 を参照しながら説明されるように、ワイヤレスネットワーク 1 0 2 の別のデバイスから告知メッセージを受信するより前に第 2 のグループ鍵 1 4 2 と鍵インジケータ 1 6 8 とを生成し得る。方法 1 2 0 0 はまた、第 2 の鍵インジケータが第 1 の鍵インジケータよりも高い優先度を示すことに基づいて伝搬のために第 2 の候補グループ鍵を選択することを含み得る。たとえば、第 1 のデバイスは、図 1 を参照しながら説明されるように、告知メッセージ 1 6 0 中に含まれる鍵インジケータ 1 6 8 に基づいて伝搬のために第 2 のグループ鍵 1 4 2 を選択し得る。方法 1 2 0 0 は、告知メッセージを受信した後に、第 2 の通信チャネルを介してページングウィンドウ中にデータリンクグループの第 4 のデバイスにページングメッセージを送信すること、第 4 のデバイスは、第 2 のデバイスに関連する、をさらに含み得る。ページングメッセージは、第 2 の候補グループ鍵が第 2 のデバイスから入手可能であることを示し得る。たとえば、第 1 のデバイス 1 0 4 は、図 1 を参照しながら説明されるように、第 4 のデバイス 1 1 0 にページングメッセージ 1 6 5 を送信し得る。

【 0 2 1 6 】

[0228]いくつかの実装形態では、方法 1 2 0 0 は、1 つまたは複数の条件に基づいて第 2 の鍵インジケータが第 1 の鍵インジケータよりも高い優先度を有すると決定することを含み得る。1 つまたは複数の条件は、第 2 の鍵インジケータがより高い優先度の媒体アクセス制御 (M A C) アドレスを示すとき、第 2 の鍵インジケータがより前のタイムスタンプを示すとき、または第 2 の鍵インジケータがより高い優先度のハッシュ値を示すときを含み得る。たとえば、第 2 のデバイス 1 0 6 は、図 1 を参照しながら説明されるように、M A C アドレス、タイムスタンプ、またはハッシュ値に基づいて (第 2 のデバイス 1 0 6 によって生成された候補グループ鍵に対応する) 第 2 の鍵インジケータが告知メッセージ 1 6 0 中に含まれる鍵インジケータ 1 6 8 よりも高い優先度を有すると決定し得る。

【 0 2 1 7 】

[0229]図 7 の方法 7 0 0、図 8 の方法 8 0 0、図 9 の方法 9 0 0、図 1 0 の方法 1 0 0 0、図 1 1 の方法 1 1 0 0、図 1 2 の方法 1 2 0 0、またはそれらの組合せにより、データリンクグループのデバイスへのグループ鍵の配布が可能になる。候補グループ鍵は、データリンクグループを含む N A N またはメッシュネットワーク内での鍵関連のトラフィックとオーバーヘッドとが低減された状態で配布され得る。たとえば、鍵関連のトラフィックは、データリンクグループのデバイスが起動しているときにページングウィンドウまたは発見ウィンドウ中にグループ鍵告知メッセージなどの告知メッセージを送ることによって低減され得る。別の例として、候補グループ鍵 (たとえば、潜在的な「次の」アクティブグループ鍵) を暗号化するためにアクティブ配布鍵が使用され得、暗号化された候補グループ鍵が、データリンクグループの 1 つまたは複数のデバイスにマルチキャストメッセ

ージとして送られ得る。マルチキャストメッセージとして候補グループ鍵を送ることによって、候補グループ鍵は、データリンクグループの2つのデバイス間でセキュリティ関連付け、P2P通信、またはそれらの組合せを実行することなしにデータリンクグループの1つまたは複数のデバイスに配布され得る。

【0218】

[0230] 図7の方法700、図8の方法800、図9の方法900、図10の方法1000、図11の方法1100、図12の方法1200、またはそれらの組合せに示すプロセスは、中央処理ユニット(CPU)、コントローラ、フィールドプログラマブルゲートアレイ(FPGA)デバイス、特定用途向け集積回路(ASIC)、別のハードウェアデバイス、ファームウェアデバイス、またはそれらの任意の組合せなどの処理ユニットによって制御され得る。一例として、図7の方法700、図8の方法800、図9の方法900、図10の方法1000、図11の方法1100、図12の方法1200、またはそれらの組合せは、告知メッセージを送信すること、グループ鍵を配布すること、またはそれらの組合せを行うための命令を実行する1つまたは複数のプロセッサによって実行され得る。さらに、図7~図12の方法のうちの1つの第1の部分は、図7~図12の方法の別の1つの少なくとも第2の部分と組み合わせられ得る。たとえば、図7の方法700の第1の部分は、図8の方法800、図9の方法900、図10の方法1000、図11の方法1100、図12の方法1200、またはそれらの組合せのうちの1つの第2の部分と組み合わせられ得る。

【0219】

[0231] 図13を参照すると、ワイヤレス通信デバイスの特定の例示的な実装形態が示され、全体的に1300と称される。デバイス1300は、メモリ1332に結合されたデジタル信号プロセッサなどのプロセッサ1310を含む。デバイス1300またはその構成要素は、図1のデバイス104~110、図2のデバイス202、図3を参照しながら説明されるデバイス、図4のデバイス402、404またはそれらの構成要素に対応し得る。

【0220】

[0232] 非一時的コンピュータ可読媒体などのメモリ1332は、1つまたは複数の鍵1360と命令1368とを含み得る。命令は、プロセッサ1310によって実行可能であり得る。たとえば、メモリ1332は、図2の鍵記憶装置208を含むか、またはそれに対応し得る。1つまたは複数の鍵1360は、デバイス1300を含むデータリンクグループのグループ鍵1362を含み得る。たとえば、グループ鍵1362は、図1の第1のグループ鍵132、第2のグループ鍵142または図2のグループ鍵214を含むか、またはそれに対応し得る。随意に、1つまたは複数の鍵1360は、データリンクグループの配布鍵1364を含み得る。たとえば、配布鍵1364は、図1の第1の配布鍵134または第2の配布鍵144を含むか、またはそれに対応し得る。いくつかの実装形態では、1つまたは複数の鍵1360は、アクティブグループ鍵および候補グループ鍵などの複数のグループ鍵を含み得る。さらに、1つまたは複数の鍵1360は、アクティブ配布鍵および候補配布鍵などの複数の配布鍵を含み得る。

【0221】

[0233] プロセッサ1310は、鍵論理1312とメッセージ論理1314とを含み得る。鍵論理1312は、図1の鍵論理112、カウンタ204、図2の鍵生成器206、またはそれらの組合せを含むか、またはそれに対応し得る。メッセージ論理1314は、図1のメッセージ論理114を含むか、またはそれに対応し得る。メッセージ論理1314は、図1の告知メッセージ160または告知メッセージ170などの告知メッセージ1316を生成するように構成され得る。告知メッセージ1316は、グループ鍵1362に対応し得る(たとえば、それを含み得る)。

【0222】

[0234] プロセッサ1310は、メモリ1332中に記憶されたソフトウェア(たとえば、1つまたは複数の命令1368のプログラム)を実行するように構成され得る。たとえ

ば、プロセッサ 1310 は、図 7 の方法 700、図 8 の方法 800、図 9 の方法 900、図 10 の方法 1000、図 11 の方法 1100、図 12 の方法 1200、またはそれらの組合せに従って動作するように構成され得る。例示のために、プロセッサ 1310 は、データリンクグループの取得されたグループ鍵 1362 を識別することと、ページングウィンドウ中にデータリンクグループの 1 つまたは複数のデバイスへの告知メッセージ 1316 の送信を開始することとをプロセッサ 1310 に行わせる命令 1368 を実行するように構成され得る。告知メッセージ 1316 は、グループ鍵 1362 に対応し得、告知メッセージ 1316 がグループ鍵告知メッセージであることを示すマルチキャストメッセージとして送信され得る。

【0223】

10

[0235] 別の例として、プロセッサ 1310 は、データリンクグループに対応するグループ鍵 1362 と配布鍵 1364 とを生成することと、アクティブ配布鍵などの第 2 の配布鍵（図示せず）を使用してグループ鍵 1362 と配布鍵 1364 とを符号化することとをプロセッサ 1310 に行わせる命令 1368 を実行するように構成され得る。第 2 の配布鍵は、データリンクグループのアクティブグループ鍵に対応し得る。命令 1368 は、データリンクグループの 1 つまたは複数のデバイスへの暗号化されたグループ鍵と暗号化された配布鍵との送信を開始することをプロセッサにさらに行なわせ得る。

【0224】

[0236] 図 13 に、同じく、プロセッサ 1310 とディスプレイ 1328 とに結合されたディスプレイコントローラ 1326 を示す。コーダ/デコーダ（コーデック）1334 も、プロセッサ 1310 に結合され得る。スピーカー 1336 とマイクロフォン 1338 とが、コーデック 1334 に結合され得る。図 13 はまた、ワイヤレスインターフェース 1340 がプロセッサ 1310 とアンテナ 1342 とに結合され得ることを示す。たとえば、ワイヤレスインターフェース 1340 は、トランシーバ 1341 を介してアンテナ 1342 に結合され得る。トランシーバ 1341 は、送信機、受信機、またはその両方を含み得る。トランシーバ 1341 は、メッセージ論理 1314 によって生成された 1 つまたは複数のメッセージを送信することと、データリンクグループのデバイスなどの他のデバイスによってデバイス 1300 に送信された 1 つまたは複数のメッセージを受信することとを行うように構成され得る。

20

【0225】

30

[0237] いくつかの実装形態では、プロセッサ 1310、ディスプレイコントローラ 1326、メモリ 1332、コーデック 1334、ワイヤレスインターフェース 1340、およびトランシーバ 1341 は、システムインパッケージまたはシステムオンチップデバイス 1322 中に含まれる。特定の実装形態では、入力デバイス 1330 と電源 1344 とが、システムオンチップデバイス 1322 に結合される。さらに、別の特定の実装形態では、図 13 に示すように、ディスプレイ 1328、入力デバイス 1330、スピーカー 1336、マイクロフォン 1338、アンテナ 1342、および電源 1344 は、システムオンチップデバイス 1322 の外部にある。ただし、ディスプレイ 1328、入力デバイス 1330、スピーカー 1336、マイクロフォン 1338、アンテナ 1342、および電源 1344 の各々は、インターフェースまたはコントローラなど、システムオンチップデバイス 1322 の構成要素に結合され得る。

40

【0226】

[0238] 図 1 ~ 図 13 の説明される実装形態のうちの 1 つまたは複数に関連して、第 1 の装置は、データリンクグループの第 1 のデバイスにおいてグループ鍵を取得するための手段を含む。たとえば、グループ鍵を取得するための手段は、図 1 の鍵論理 112、図 2 の鍵生成器 206、受信機 210、図 13 の鍵論理 1312、ワイヤレスインターフェース 1340、トランシーバ 1341、命令 1368 を実行するようにプログラムされたプロセッサ 1310、グループ鍵を取得するための 1 つまたは複数の他の構造、デバイス、回路、モジュール、または命令、あるいはそれらの任意の組合せを含むか、またはそれに対応し得る。グループ鍵は、図 1 の第 1 のグループ鍵 132、図 1 の第 2 のグループ鍵 14

50

2、図2のグループ鍵214、または図3～図5を参照しながら説明されるグループ鍵のいずれかを含むか、またはそれに対応し得る。

【0227】

[0239]第1の装置はまた、ページングウィンドウ中にデータリンクグループの1つまたは複数のデバイスにグループ鍵に対応する告知メッセージを送信するための手段を含む。告知メッセージは、グループ鍵に対応し得、告知メッセージがグループ鍵告知メッセージであることを示すマルチキャストメッセージとして送信され得る。たとえば、告知メッセージを送信するための手段は、図1のメッセージ論理114、図2の送信機212、図13のワイヤレスインターフェース1340、トランシーバ1341、アンテナ1342、命令1368を実行するようにプログラムされたプロセッサ1310、告知メッセージを送信するための1つまたは複数の他の構造、デバイス、回路、モジュール、または命令、あるいはそれらの任意の組合せを含むか、またはそれに対応し得る。

10

【0228】

[0240]1つまたは複数の説明される実装形態に関連して、第2の装置は、データリンクグループに対応するグループ鍵と配布鍵とを生成するための手段を含む。たとえば、生成するための手段は、図1の鍵論理112、図2の鍵生成器206、図13の鍵論理1312、命令1368を実行するようにプログラムされたプロセッサ1310、グループ鍵と配布鍵とを生成するための1つまたは複数の他の構造、デバイス、回路、モジュール、または命令、あるいはそれらの任意の組合せを含むか、またはそれに対応し得る。

【0229】

20

[0241]第2の装置は、第2の配布鍵を使用してグループ鍵と配布鍵とを符号化するための手段を含む。第2の配布鍵は、データリンクグループのアクティブグループ鍵に対応し得る。たとえば、符号化するための手段は、図1のメッセージ論理114、エンコーダ/デコーダ118、図13のメッセージ論理1314、命令1368を実行するようにプログラムされたプロセッサ1310、グループ鍵と配布鍵とを符号化するための1つまたは複数の他の構造、デバイス、回路、モジュール、または命令、あるいはそれらの任意の組合せを含むか、またはそれに対応し得る。

【0230】

[0242]第2の装置はまた、データリンクグループの1つまたは複数のデバイスに符号化されたグループ鍵と符号化された配布鍵とを送信するための手段を含む。たとえば、送信するための手段は、図1のメッセージ論理114、ワイヤレスデバイス1340、図2の送信機212、図13のトランシーバ1341、アンテナ1342、命令1368を実行するようにプログラムされたプロセッサ1310、符号化されたグループ鍵と符号化された配布鍵とを送信するための1つまたは複数の他の構造、デバイス、回路、モジュール、または命令、あるいはそれらの任意の組合せを含むか、またはそれに対応し得る。

30

【0231】

[0243]1つまたは複数の説明する実装形態に関連して、第3の装置は、データリンクグループの第1のデバイスにおいてグループ鍵を取得するための手段を含む。たとえば、取得するための手段は、図1の鍵論理112、図13の鍵論理1312、命令1368を実行するようにプログラムされたプロセッサ1310、グループ鍵を取得するための1つまたは複数の他の構造、デバイス、回路、モジュール、または命令、あるいはそれらの任意の組合せを含むか、またはそれに対応し得る。

40

【0232】

[0244]第3の装置は、データリンクグループの第1のデバイスからデバイスに送信するための手段、告知メッセージはグループ鍵に対応する、を含む。たとえば、符号化するための手段は、図1のメッセージ論理114、第1のデバイス104、図13のメッセージ論理1314、ワイヤレスインターフェース1340、トランシーバ1341、アンテナ1342、命令1368を実行するようにプログラムされたプロセッサ1310、告知メッセージを送信するための1つまたは複数の他の構造、デバイス、回路、モジュール、または命令、あるいはそれらの任意の組合せを含むか、またはそれに対応し得る。告知メッ

50

セージは、マルチキャストメッセージを含み得、NAN通信チャネルなどの通信チャネルを介して、またはデータリンクグループチャネルを介してページングウィンドウ中に送信され得る。

【0233】

[0245] 1つまたは複数の説明する実装形態に関連して、第4の装置は、データリンクグループの第2のデバイスにおいて、発見ウィンドウ中に第1のワイヤレスチャネルを監視するための手段を含む。たとえば、監視するための手段は、図1のメッセージ論理114、第1のデバイス104、図13のメッセージ論理1314、ワイヤレスインターフェース1340、トランシーバ1341、アンテナ1342、命令1368を実行するようにプログラムされたプロセッサ1310、ワイヤレスチャネルを監視するための1つまたは複数の他の構造、デバイス、回路、モジュール、または命令、あるいはそれらの任意の組合せを含むか、またはそれに対応し得る。第1のワイヤレスチャネルは、図3のNAN通信チャネル302またはデータリンクグループチャネル304を含むか、またはそれに対応し得る。

10

【0234】

[0246] 第4の装置は、発見ウィンドウ中にデータリンクグループの第1のデバイスから第2のデバイスにおいて告知メッセージを受信するための手段を含む。たとえば、受信するための手段は、図1のメッセージ論理114、第1のデバイス104、図13のメッセージ論理1314、ワイヤレスインターフェース1340、トランシーバ1341、アンテナ1342、命令1368を実行するようにプログラムされたプロセッサ1310、告知メッセージを受信するための1つまたは複数の他の構造、デバイス、回路、モジュール、または命令、あるいはそれらの任意の組合せを含むか、またはそれに対応し得る。

20

【0235】

[0247] 1つまたは複数の説明される実装形態に関連して、第5の装置は、NANのデータリンクグループの第2のデバイスにおいて、データリンクグループのページングウィンドウ中にデータリンクグループに対応するワイヤレスチャネルを監視するための手段を含む。たとえば、監視するための手段は、図1のメッセージ論理114、図13のメッセージ論理1314、ワイヤレスインターフェース1340、トランシーバ1341、アンテナ1342、命令1368を実行するようにプログラムされたプロセッサ1310、ワイヤレスチャネルを監視するための1つまたは複数の他の構造、デバイス、回路、モジュール、または命令、あるいはそれらの任意の組合せを含むか、またはそれに対応し得る。

30

【0236】

[0248] 第5の装置は、ページングウィンドウ中にデータリンクグループの第1のデバイスから第2のデバイスにおいて告知メッセージを受信するための手段、告知メッセージは、グループ鍵の生成を示す、を含む。たとえば、受信するための手段は、図1のメッセージ論理114、第1のデバイス104、図13のメッセージ論理1314、ワイヤレスインターフェース1340、トランシーバ1341、アンテナ1342、命令1368を実行するようにプログラムされたプロセッサ1310、告知メッセージを受信するための1つまたは複数の他の構造、デバイス、回路、モジュール、または命令、あるいはそれらの任意の組合せを含むか、またはそれに対応し得る。告知メッセージは、マルチキャストメッセージを含み得る。

40

【0237】

[0249] 開示される実装形態のうちの1つまたは複数の、通信デバイス、固定ロケーションデータユニット、モバイルロケーションデータユニット、モバイル電話、セルラー電話、衛星電話、コンピュータ、タブレット、ポータブルコンピュータ、ディスプレイデバイス、メディアプレーヤ、またはデスクトップコンピュータを含み得る、デバイス1300などのシステム、デバイスまたは装置において実装され得る。代替または追加として、デバイス1300は、セットトップボックス、エンターテインメントユニット、ナビゲーションデバイス、携帯情報端末(PDA)、モニタ、コンピュータモニタ、テレビジョン、チューナー、ラジオ、衛星ラジオ、音楽プレーヤ、デジタル音楽プレーヤ、ポータブル音

50

楽プレーヤ、ビデオプレーヤ、デジタルビデオプレーヤ、デジタルビデオディスク（DVD）プレーヤ、ポータブルデジタルビデオプレーヤ、衛星、車両または車両内に組み込まれたデバイス、プロセッサを含むか、または、データもしくはコンピュータ命令を記憶するかもしくは取り出す任意の他のデバイス、あるいはそれらの組合せを含み得る。別の例示的な、非限定的な例として、システム、デバイス、または装置は、ハンドヘルドパーソナル通信システム（PCS）ユニットなどのリモートユニット、全地球測位システム（GPS）対応デバイスなどのポータブルデータユニット、メーター読取り機器、あるいは、プロセッサを含むか、または、データもしくはコンピュータ命令を記憶するかもしくは取り出す任意の他のデバイス、あるいはそれらの任意の組合せを含み得る。

【0238】

10

[0250] 図1～図13の1つまたは複数は、本開示の教示によるシステム、装置、方法、またはこれらの組合せを示し得るが、本開示は、これらの示されたシステム、装置、方法、またはこれらの組合せに限定されない。本明細書で示され、または説明される図1～図13のいずれかの1つまたは複数の機能または構成要素は、図1～図13の別の機能または構成要素の1つまたは複数の他の部分と組み合わせられ得る。したがって、本明細書で説明されるいずれの単一の実装形態も限定的と解釈されるべきではなく、本開示の実装形態は、本開示の教示から逸脱することなく適切に組み合わせられ得る。

【0239】

[0251] さらに、本明細書で開示された実装形態に関連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、プロセッサによって実行される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、およびステップについて、上記では概してそれらの機能に関して説明した。そのような機能がハードウェアとして実装されるか、プロセッサ実行可能命令として実装されるかは、具体的な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、説明した機能を具体的な適用例ごとに様々な方法で実装し得るが、そのような実装決定は、本開示の範囲からの逸脱を生じるものと解釈すべきではない。

20

【0240】

[0252] 本明細書で開示した実装形態に関して説明される方法またはアルゴリズムのステップは、直接ハードウェアに含まれ、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に含まれ、またはその2つの組合せであり得る。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非一時的（non-transient）（たとえば、非一時的（non-transitory））記憶媒体中に存在し得る。例示的な記憶媒体は、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。代替的に、記憶媒体はプロセッサと一体化され得る。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。代替的に、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内の個別の構成要素として存在し得る。

30

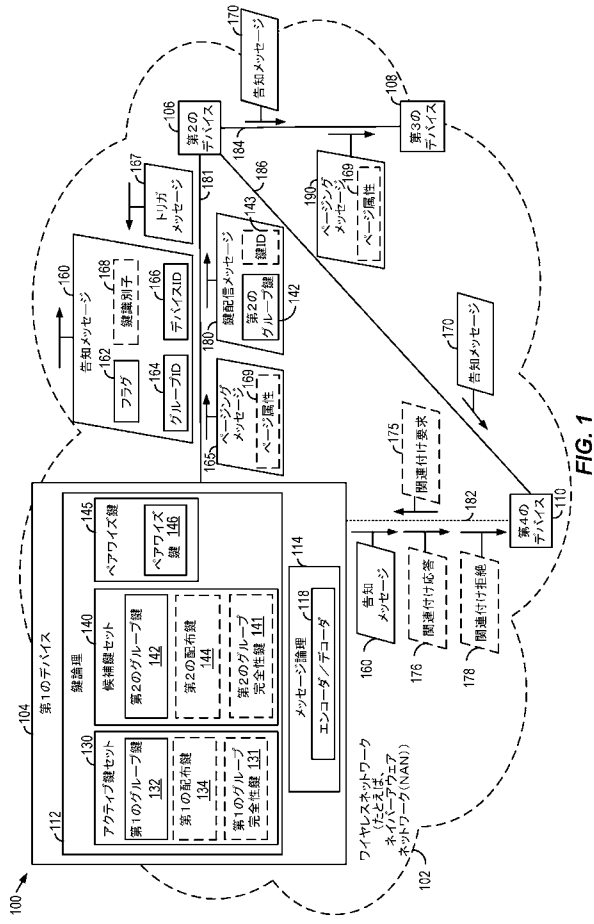
40

【0241】

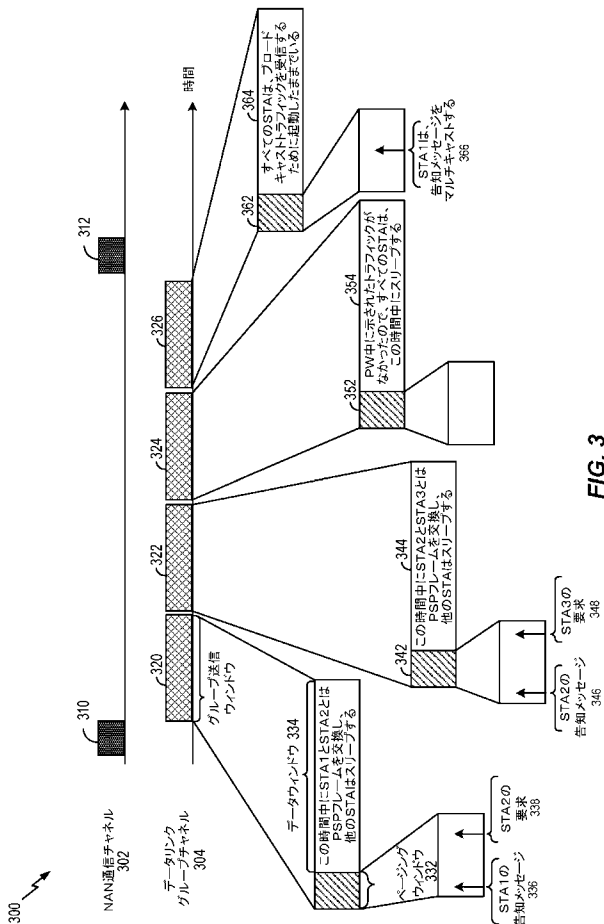
[0253] 開示した実装形態の前の説明は、開示した実装形態を当業者が製作または使用することを可能にするために与えられる。これらの実装形態に対する様々な修正が、当業者には容易に明らかになり、本明細書において定義される原理は、本開示の範囲から逸脱することなく、他の実装形態に適用され得る。したがって、本開示は、本明細書で示した実装形態に限定されるものではなく、以下の特許請求の範囲によって定義される原理および新規の特徴に一致する可能な最も広い範囲を与えられるべきである。

50

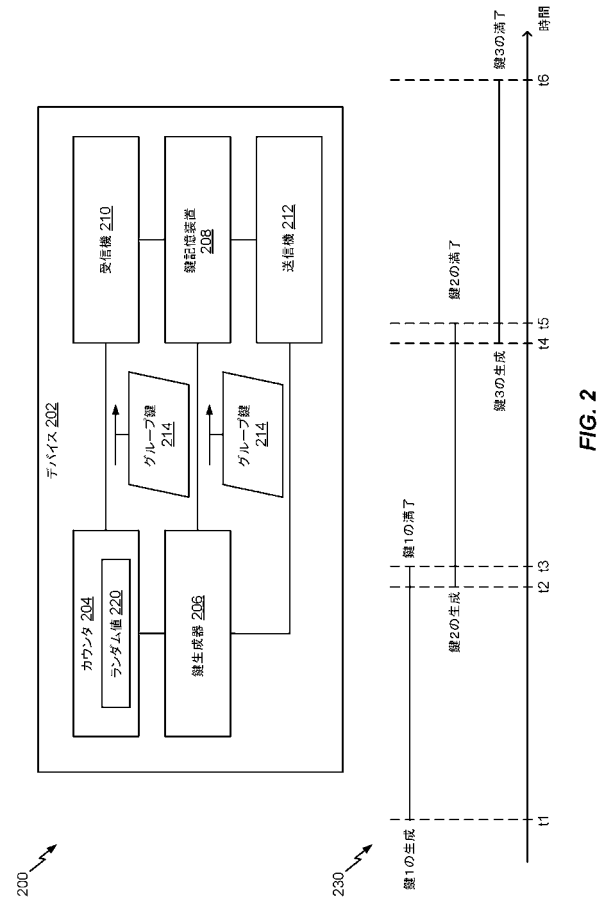
【図 1】



【図 3】



【図 2】



【図 4】

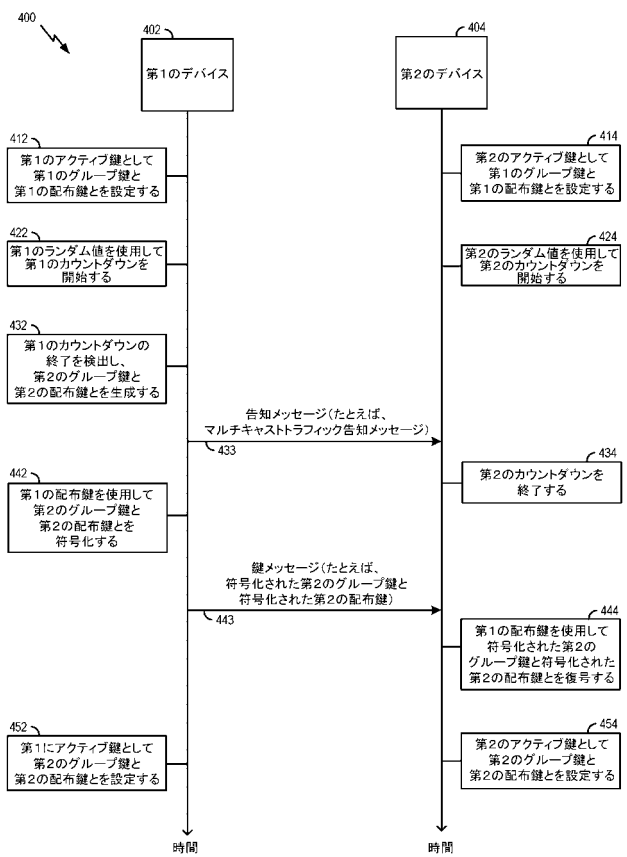


FIG. 4

【 図 5 】

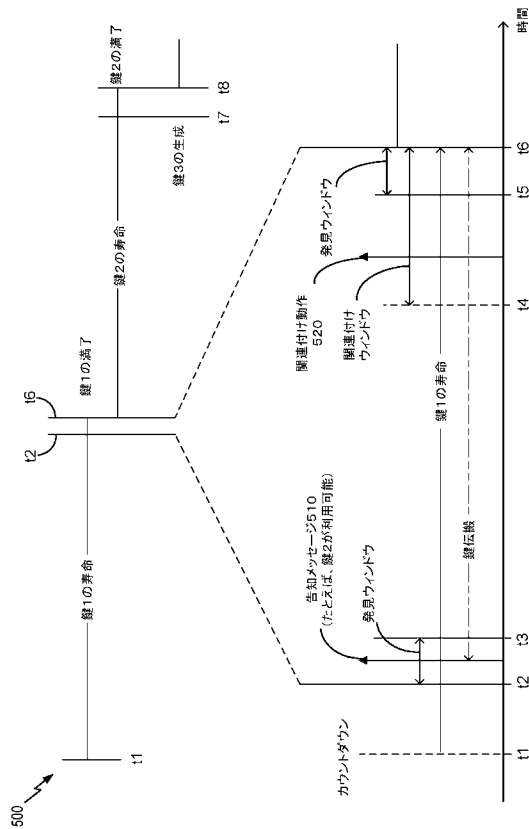


FIG. 5

【 図 6 】

ファイルID	サイズ (オプション)	説明
602	1	属性のタイプを識別する
604	2	属性中の以下のフィールドの長さ
606	6	データリンググループID データリンググループ識別子
608	1	属性中にこのフィールドが存在するのを示す
610	変数	ページングされているデータのリスト (たとえば、データのリスト)
612	1	送信のためにスケジューリングされた トラフィックのタイプ (たとえば、QoSタイプ)

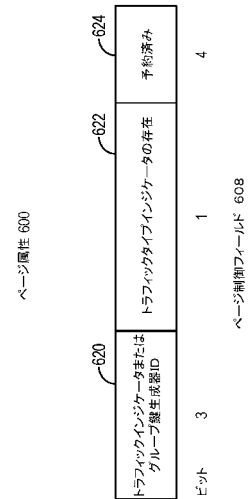


FIG. 6

【 図 7 】

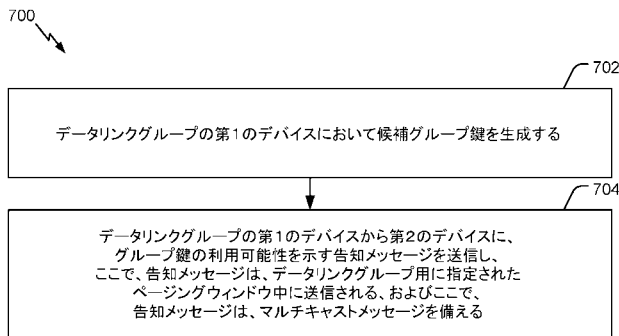


FIG. 7

【 図 8 】

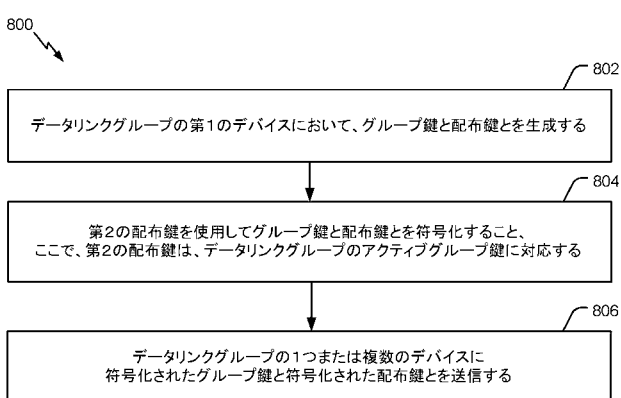


FIG. 8

【 圖 9 】

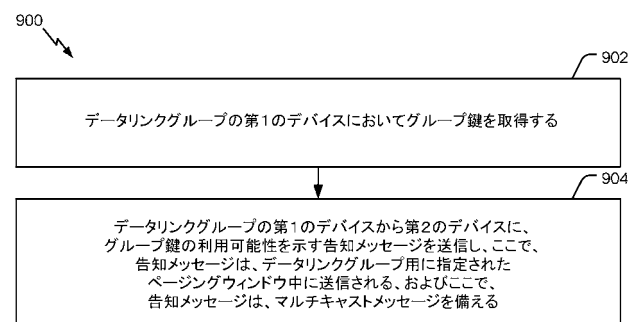


FIG. 9

【 図 1 0 】

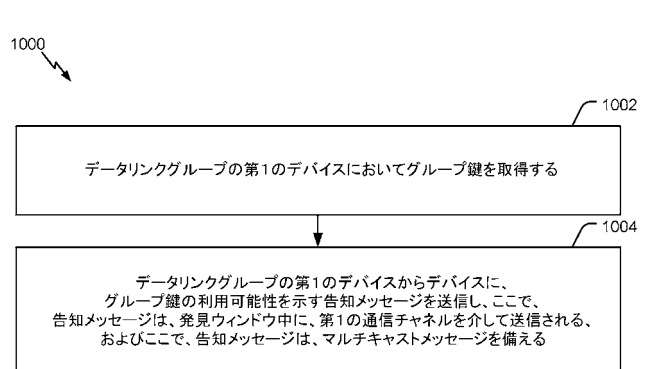


FIG. 10

【図 1 1】

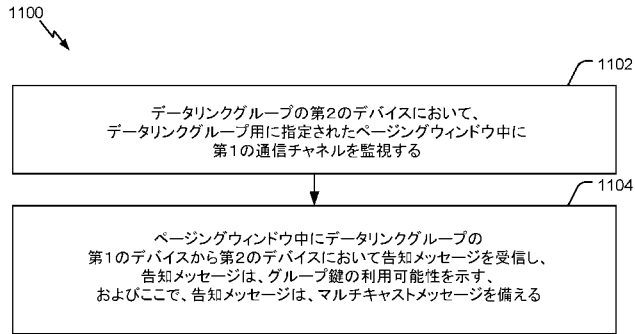


FIG. 11

【図 1 2】

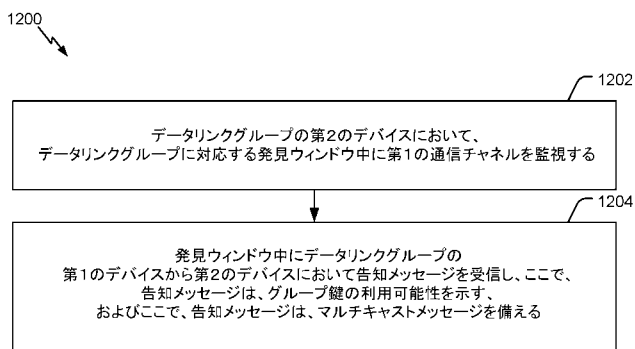


FIG. 12

【図 1 3】

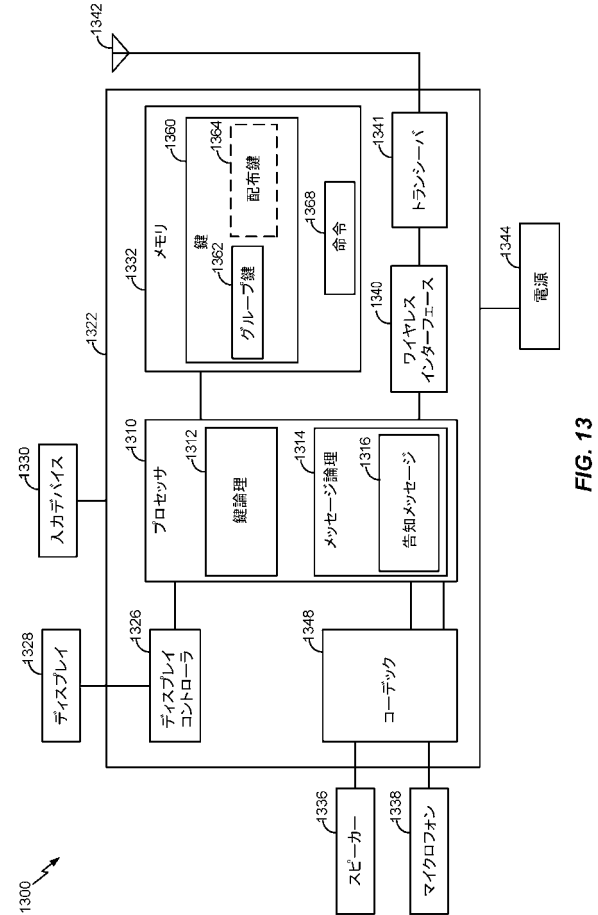


FIG. 13

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2016/015196

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L9/08 H04L29/06 H04W12/04 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)

H04L 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, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6 049 878 A (CARONNI GERMANO [US] ET AL) 11 April 2000 (2000-04-11) column 6, line 51 - column 9, line 24; figures 5,6	1-5, 8-23, 25-30
Y	US 2014/082185 A1 (ABRAHAM SANTOSH PAUL [US] ET AL) 20 March 2014 (2014-03-20) paragraph [0064]; figure 5	1-5, 8-23, 25-30
A	US 2008/175387 A1 (EASTHAM W BRYANT [US]) 24 July 2008 (2008-07-24) paragraphs [0030], [0039], [0064]; figure 7 paragraphs [0053] - [0056]; figures 4,5 paragraphs [0045] - [0050]; figures 2,3 -/--	1-30

☒ 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

22 March 2016

Date of mailing of the international search report

04/04/2016

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Horbach, Christian

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2016/015196

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	W0 2009/118268 A2 (IBM [US]; IBM UK [GB]; SAYRE JOHANNES [US]; BAE MYUNG [US]; KNOP FELIP) 1 October 2009 (2009-10-01) page 17, lines 15-25 -----	1-30

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2016/015196

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 6049878	A	11-04-2000	NONE	

US 2014082185	A1	20-03-2014	CN 104662937 A	27-05-2015
			JP 2015530058 A	08-10-2015
			US 2014082185 A1	20-03-2014
			WO 2014047125 A1	27-03-2014

US 2008175387	A1	24-07-2008	CN 101641903 A	03-02-2010
			EP 2104989 A1	30-09-2009
			JP 5033188 B2	26-09-2012
			JP 2010517330 A	20-05-2010
			KR 20090110334 A	21-10-2009
			RU 2009131314 A	27-02-2011
			TW 200840297 A	01-10-2008
			US 2008175387 A1	24-07-2008
			WO 2008088084 A1	24-07-2008

WO 2009118268	A2	01-10-2009	CN 101981889 A	23-02-2011
			EP 2258093 A2	08-12-2010
			KR 20100133448 A	21-12-2010
			US 2009245518 A1	01-10-2009
			WO 2009118268 A2	01-10-2009

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、アビシエク・プラモド
アメリカ合衆国、カリフォルニア州 9 2 1 2 1 - 1 7 1 4、サン・ディエゴ、モアハウス・ドライブ 5 7 7 5
- (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 9 2 1 2 1 - 1 7 1 4、サン・ディエゴ、モアハウス・ドライブ 5 7 7 5
- (72)発明者 リ、ス・ボム
アメリカ合衆国、カリフォルニア州 9 2 1 2 1 - 1 7 1 4、サン・ディエゴ、モアハウス・ドライブ 5 7 7 5
- (72)発明者 マリネン、ジョウニ・カレビ
アメリカ合衆国、カリフォルニア州 9 2 1 2 1 - 1 7 1 4、サン・ディエゴ、モアハウス・ドライブ 5 7 7 5
- (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 9 2 1 2 1 - 1 7 1 4、サン・ディエゴ、モアハウス・ドライブ 5 7 7 5
- (72)発明者 ライシニア、アリレザ
アメリカ合衆国、カリフォルニア州 9 2 1 2 1 - 1 7 1 4、サン・ディエゴ、モアハウス・ドライブ 5 7 7 5

Fターム(参考) 5J104 AA16 AA34 EA18 NA02 NA37 PA07