(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2016-520271
(P2016-520271A)
(43)公表日　平成28年7月11日(2016.7.11)

(51)Int.Cl.		F I		テーマコード（参考）
H04W 12/10	(2009.01)	H04W	12/10	5J104
H04W 84/12	(2009.01)	H04W	84/12	5K067
H04W 4/06	(2009.01)	H04W	4/06	150
H04L 9/32	(2006.01)	H04L	9/00	675B
H04L 9/06	(2006.01)	H04L	9/00	601F

審査請求 未請求　予備審査請求 未請求　（全 27 頁）

(21)出願番号　特願2016-515110 (P2016-515110)
(86)(22)出願日　平成26年5月23日 (2014.5.23)
(85)翻訳文提出日　平成27年12月24日 (2015.12.24)
(86)国際出願番号　PCT/US2014/039301
(87)国際公開番号　WO2014/190241
(87)国際公開日　平成26年11月27日 (2014.11.27)
(31)優先権主張番号　61/827,490
(32)優先日　平成25年5月24日 (2013.5.24)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　14/284,785
(32)優先日　平成26年5月22日 (2014.5.22)
(33)優先権主張国　米国 (US)

(71)出願人　595020643
クゥアルコム・インコーポレイテッド
ＱＵＡＬＣＯＭＭ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国、カリフォルニア州　９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ　５７７５
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100109830
弁理士　福原　淑弘
(74)代理人　100158805
弁理士　井関　守三
(74)代理人　100194814
弁理士　奥村　元宏

最終頁に続く

(54)【発明の名称】メッセージ認証をもつブロードキャストＷＬＡＮメッセージのためのシステムおよび方法

(57)【要約】
メッセージ認証をもつマルチキャスト・ワイヤレスローカルエリアネットワーク・メッセージのためのシステム、方法、およびデバイスが本明細書に含まれている。本方法は、複数のワイヤレスデバイスの各々のためのメッセージ完全性検査値を決定することを含む。本方法は、ワイヤレスローカルエリアネットワーク上で複数のデバイスの各々にマルチキャストパケットを送信することをさらに含み、マルチキャストパケットが、複数のデバイスの各々の指示と、複数のデバイスの各々のためのメッセージ完全性検査値とを含む。

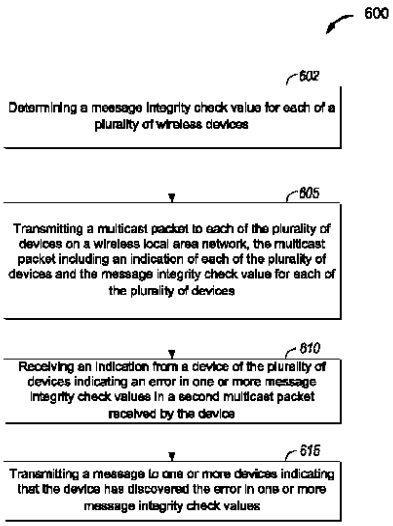

FIG. 6

【特許請求の範囲】
【請求項１】
複数のワイヤレスデバイスの各々のためのメッセージ完全性検査値を決定することと、
ワイヤレスローカルエリアネットワーク上で前記複数のデバイスの各々にマルチキャストパケットを送信することと、前記マルチキャストパケットが、前記複数のデバイスの各々の指示と、前記複数のデバイスの各々のための前記メッセージ完全性検査値とを含む、を備えるワイヤレス通信の方法。
【請求項２】
前記複数のデバイスの各々の前記指示が、前記複数のデバイスの各々のための関連付け識別とメディアアクセス制御アドレスとのうちの少なくとも１つを備える、請求項１に記載の方法。
【請求項３】
前記メッセージ完全性検査値を決定することが、前記マルチキャストパケットのフレームヘッダと、前記マルチキャストパケット中のデータと、前記複数のデバイスのうちの１つの前記指示と、前記マルチキャストパケットのカウンタモード暗号ブロック連鎖メッセージ認証コードプロトコルヘッダ中のペアワイズ過渡鍵および擬似ランダム雑音シーケンス番号と、のうちの１つまたは複数に基づいてメッセージ完全性検査値を決定することを備える、請求項１に記載の方法。
【請求項４】
前記複数のワイヤレスデバイスの各々のための前記メッセージ完全性検査値が、８オクテット未満の短縮されたメッセージ完全性検査値を備える、請求項１に記載の方法。
【請求項５】
前記マルチキャストパケットがフレーム本体を含み、データ長フィールドが前記マルチキャストパケットの前記フレーム本体内に含まれる、請求項１に記載の方法。
【請求項６】
前記マルチキャストパケットが、反転された予約済みビットまたはビットの反転された予約済み組合せをもつカウンタモード暗号ブロック連鎖メッセージ認証コードプロトコルヘッダを含み、前記反転された予約済みビットまたはビットの反転された予約済み組合せは、前記複数のデバイスが、前記マルチキャストパケットを送信側認証をもつマルチキャストパケットとして認識することを可能にするように構成された、請求項１に記載の方法。
【請求項７】
前記複数のデバイスのうちの少なくとも１つから、前記デバイスによって受信された第２のマルチキャストパケット中の１つまたは複数のメッセージ完全性検査値中のエラーを示す指示を受信することと、
１つまたは複数のデバイスに、前記少なくとも１つのデバイスが１つまたは複数のメッセージ完全性検査値中の前記エラーを発見したことを示すメッセージを送信することと
をさらに備える、請求項１に記載の方法。
【請求項８】
前記メッセージが、前記ネットワークにおけるマルチキャストパケットサービスを無効にするようにとの前記１つまたは複数のデバイスへの命令を備える、請求項７に記載の方法。
【請求項９】
前記メッセージが、前記１つまたは複数のデバイスのユニキャスト鍵を変更するようにとの前記１つまたは複数のデバイスへの命令を備える、請求項７に記載の方法。
【請求項１０】
前記メッセージ完全性検査値を決定することが、グループ時間鍵を用いて前記マルチキャストパケット中のデータを暗号化することによって第１のメッセージ完全性検査値を生成することと、次いで、前記第１のメッセージ完全性検査値に基づいて複数のワイヤレスデバイスの各々のためのメッセージ完全性検査値を決定することとを備える、請求項１に

記載の方法。
【請求項１１】
複数のワイヤレスデバイスの各々のためのメッセージ完全性検査値を決定することと、
ワイヤレスローカルエリアネットワーク上で前記複数のデバイスの各々にマルチキャストパケットを送信することと、前記マルチキャストパケットが、前記複数のデバイスの各々の指示と、前記複数のデバイスの各々のための前記メッセージ完全性検査値とを含む、
を行うように構成された送信機
を備えるワイヤレス通信装置。
【請求項１２】
前記複数のデバイスの各々の前記指示が、前記複数のデバイスの各々のための関連付け識別とメディアアクセス制御アドレスとのうちの少なくとも１つを備える、請求項１１に記載の装置。
【請求項１３】
前記メッセージ完全性検査値を決定することが、前記マルチキャストパケットのフレームヘッダと、前記マルチキャストパケット中のデータと、前記複数のデバイスのうちの１つの前記指示と、前記マルチキャストパケットのカウンタモード暗号ブロック連鎖メッセージ認証コードプロトコルヘッダ中のペアワイズ過渡鍵および擬似ランダム雑音シーケンス番号と、のうちの１つまたは複数に基づいてメッセージ完全性検査値を決定することを備える、請求項１１に記載の装置。
【請求項１４】
前記複数のワイヤレスデバイスの各々のための前記メッセージ完全性検査値が、８オクテット未満の短縮されたメッセージ完全性検査値を備える、請求項１１に記載の装置。
【請求項１５】
前記マルチキャストパケットがフレーム本体を含み、データ長フィールドが前記マルチキャストパケットの前記フレーム本体内に含まれる、請求項１１に記載の装置。
【請求項１６】
前記マルチキャストパケットが、反転された予約済みビットまたはビットの反転された予約済み組合せをもつカウンタモード暗号ブロック連鎖メッセージ認証コードプロトコルヘッダを含み、前記反転された予約済みビットまたはビットの反転された予約済み組合せは、前記複数のデバイスが、前記マルチキャストパケットを送信側認証をもつマルチキャストパケットとして認識することを可能にするように構成された、請求項１１に記載の装置。
【請求項１７】
前記複数のデバイスのうちの少なくとも１つから、前記デバイスによって受信された第２のマルチキャストパケット中の１つまたは複数のメッセージ完全性検査値中のエラーを示す指示を受信するように構成された受信機と、
１つまたは複数のデバイスに、前記少なくとも１つのデバイスが１つまたは複数のメッセージ完全性検査値中の前記エラーを発見したことを示すメッセージを送信するようにさらに構成された前記送信機と
をさらに備える、請求項１１に記載の装置。
【請求項１８】
前記メッセージが、前記ネットワークにおけるマルチキャストパケットサービスを無効にするようにとの前記１つまたは複数のデバイスへの命令を備える、請求項１７に記載の装置。
【請求項１９】
前記メッセージが、前記１つまたは複数のデバイスのユニキャスト鍵を変更するようにとの前記１つまたは複数のデバイスへの命令を備える、請求項１７に記載の装置。
【請求項２０】

前記メッセージ完全性検査値を決定することが、グループ時間鍵を用いて前記マルチキャストパケット中のデータを暗号化することによって第１のメッセージ完全性検査値を生成することと、次いで、前記第１のメッセージ完全性検査値に基づいて複数のワイヤレスデバイスの各々のためのメッセージ完全性検査値を決定することとを備える、請求項１１に記載の装置。

【請求項２１】

複数のワイヤレスデバイスの各々のためのメッセージ完全性検査値を決定するための手段と、

ワイヤレスローカルエリアネットワーク上で前記複数のデバイスの各々にマルチキャストパケットを送信するための手段と、前記マルチキャストパケットが、前記複数のデバイスの各々の指示と、前記複数のデバイスの各々のための前記メッセージ完全性検査値とを含む、

を備えるワイヤレス通信装置。

【請求項２２】

前記メッセージ完全性検査値を決定するための前記手段が、前記マルチキャストパケットのフレームヘッダと、前記マルチキャストパケット中のデータと、前記複数のデバイスのうちの１つの前記指示と、前記マルチキャストパケットのカウンタモード暗号ブロック連鎖メッセージ認証コードプロトコルヘッダ中のペアワイズ過渡鍵および擬似ランダム雑音シーケンス番号と、のうちの１つまたは複数に基づいてメッセージ完全性検査値を決定するための手段を備える、請求項２１に記載の装置。

【請求項２３】

前記複数のワイヤレスデバイスの各々のための前記メッセージ完全性検査値が、８オクテット未満の短縮されたメッセージ完全性検査値を備える、請求項２１に記載の装置。

【請求項２４】

前記複数のデバイスのうちの少なくとも１つから、前記デバイスによって受信された第２のマルチキャストパケット中の１つまたは複数のメッセージ完全性検査値中のエラーを示す指示を受信するための手段と、

１つまたは複数のデバイスに、前記少なくとも１つのデバイスが１つまたは複数のメッセージ完全性検査値中の前記エラーを発見したことを示すメッセージを送信するための手段と

をさらに備える、請求項２１に記載の装置。

【請求項２５】

前記メッセージが、前記ネットワークにおけるマルチキャストパケットサービスを無効にするか、または前記１つまたは複数のデバイスのユニキャスト鍵を変更するようにとの前記１つまたは複数のデバイスへの命令を備える、請求項２４に記載の装置。

【請求項２６】

実行されたとき、デバイス中のプロセッサにワイヤレス通信のための方法を実行させる命令を備える非一時的コンピュータ可読媒体であって、前記方法は、

複数のワイヤレスデバイスの各々のためのメッセージ完全性検査値を決定することと、

ワイヤレスローカルエリアネットワーク上で前記複数のデバイスの各々にマルチキャストパケットを送信することと、前記マルチキャストパケットが、前記複数のデバイスの各々の指示と、前記複数のデバイスの各々のための前記メッセージ完全性検査値とを含む、

を備える非一時的コンピュータ可読媒体。

【請求項２７】

前記メッセージ完全性検査値を決定することが、前記マルチキャストパケットのフレームヘッダと、前記マルチキャストパケット中のデータと、前記複数のデバイスのうちの１つの前記指示と、前記マルチキャストパケットのカウンタモード暗号ブロック連鎖メッセージ認証コードプロトコルヘッダ中のペアワイズ過渡鍵および擬似ランダム雑音シーケンス番号と、のうちの１つまたは複数に基づいてメッセージ完全性検査値を決定することを備える、請求項２６に記載のコンピュータ可読媒体。

【請求項２８】
前記複数のワイヤレスデバイスの各々のための前記メッセージ完全性検査値が、８オクテット未満の短縮されたメッセージ完全性検査値を備える、請求項２６に記載のコンピュータ可読媒体。
【請求項２９】
前記複数のデバイスのうちの少なくとも１つから、前記デバイスによって受信された第２のマルチキャストパケット中の１つまたは複数のメッセージ完全性検査値中のエラーを示す指示を受信することと、
１つまたは複数のデバイスに、前記少なくとも１つのデバイスが１つまたは複数のメッセージ完全性検査値中の前記エラーを発見したことを示すメッセージを送信することとをさらに備える、請求項２６に記載のコンピュータ可読媒体。
【請求項３０】
前記メッセージが、前記ネットワークにおけるマルチキャストパケットサービスを無効にするか、または前記１つまたは複数のデバイスのユニキャスト鍵を変更するようにとの前記１つまたは複数のデバイスへの命令を備える、請求項２９に記載のコンピュータ可読媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
[0001]本出願は、一般にワイヤレス通信に関し、より詳細には、メッセージ認証（message authentication）をもつブロードキャスト・ワイヤレスローカルエリアネットワーク（ＷＬＡＮ）メッセージのためのシステム、方法、およびデバイスに関する。
【背景技術】
【０００２】
[0002]多くの電気通信システムでは、通信ネットワークは、いくつかの対話している空間的に分離されたデバイスの間でメッセージを交換するために使用される。ネットワークは、たとえば、メトロポリタンエリア、ローカルエリア、またはパーソナルエリアであり得る、地理的範囲に従って分類され得る。そのようなネットワークはそれぞれ、ワイドエリアネットワーク（ＷＡＮ）、メトロポリタンエリアネットワーク（ＭＡＮ）、ローカルエリアネットワーク（ＬＡＮ）、またはパーソナルエリアネットワーク（ＰＡＮ）に指定されるであろう。ネットワークはまた、様々なネットワークノードとデバイスとを相互接続するために使用されるスイッチング／ルーティング技法（たとえば、回線交換対パケット交換）、送信のために採用される物理媒体のタイプ（たとえば、ワイヤード対ワイヤレス）、および使用される通信プロトコルのセット（たとえば、インターネットプロトコルスイート、ＳＯＮＥＴ（同期光ネットワーキング：Synchronous Optical Networking）、イーサネット（登録商標）など）によって異なる。
【０００３】
[0003]ワイヤレスネットワークは、ネットワーク要素がモバイルであり、したがって動的接続性の必要があるとき、またはネットワークアーキテクチャが固定のトポロジーではなくアドホックなトポロジーで形成されている場合にしばしば選好される。ワイヤレスネットワークは、無線、マイクロ波、赤外線、光などの周波数帯域中の電磁波を使用する非誘導伝搬モード（an unguided propagation mode）では、無形物理媒体（intangible physical media）を採用する。ワイヤレスネットワークは、固定ワイヤードネットワークと比較して、ユーザモビリティと迅速なフィールド展開とを有利に促進する。
【０００４】
[0004]ワイヤレスネットワーク中のデバイスは、互いの間で情報を送信／受信し得る。その情報は、いくつかの態様ではデータユニットと呼ばれることがある、パケットを備え得る。パケットは、ネットワークを介してパケットをルーティングすること、パケット中のデータを識別すること、パケットを処理することなどを行うのに役立つオーバーヘッド情報（たとえば、ヘッダ情報、パケットプロパティなど）、ならびに、パケットのペイロ

ード中で搬送され得るようなデータ、たとえばユーザデータ、マルチメディアコンテンツなどを含み得る。場合によっては、ブロードキャストパケットが送信され得、同じデータがその中でワイヤレスネットワーク中のいくつかのデバイスに同時に送信される。

【発明の概要】

【０００５】

[0005]本発明のシステム、方法、およびデバイスは、それぞれいくつかの態様を有し、それらのうちの単一の態様が単独で本発明の望ましい属性を担当するとは限らない。次に、以下の特許請求の範囲によって表される本発明の範囲を限定することなしに、いくつかの特徴について手短に説明する。この説明を考察すれば、特に「詳細な説明」と題するセクションを読めば、本発明の特徴が、データパケット中でペイロードを送信する際のオーバーヘッドを減少させることを含む利点をどのように提供するかが理解されよう。

【０００６】

[0006]本開示の一態様は、複数のワイヤレスデバイスの各々のためのメッセージ完全性検査値（message integrity check value）を決定することと、ワイヤレスローカルエリアネットワーク上で複数のデバイスの各々にマルチキャストパケットを送信することと、マルチキャストパケットが、複数のデバイスの各々の指示と、複数のデバイスの各々のためのメッセージ完全性検査値とを含む、を備えるワイヤレス通信の方法を提供する。

【０００７】

[0007]複数のデバイスの各々の指示は、複数のデバイスの各々のための関連付け識別（an association identification）とメディアアクセス制御アドレスとのうちの少なくとも１つを含み得る。メッセージ完全性検査値を決定することは、マルチキャストパケットのフレームヘッダと、マルチキャストパケット中のデータと、複数のデバイスのうちの１つの指示と、マルチキャストパケットのカウンタモード暗号ブロック連鎖メッセージ認証コードプロトコルヘッダ（counter mode cipher block chaining message authentication code protocol header）中のペアワイズ過渡鍵（pairwise transient key）および擬似ランダム雑音シーケンス番号と、のうちの１つまたは複数に基づいてメッセージ完全性検査値を決定することを含み得る。複数のワイヤレスデバイスの各々のためのメッセージ完全性検査値は、８オクテット未満の短縮されたメッセージ完全性検査値（a shortened message integrity check value）を含み得る。マルチキャストパケットは、マルチキャストパケットのフレーム本体内にデータ長フィールドを含み得る。マルチキャストパケットは、反転された予約済みビット（a flipped reserved bit）またはビットの反転された予約済み組合せ（flipped reserved combination of bits）をもつカウンタモード暗号ブロック連鎖メッセージ認証コードプロトコルヘッダを含み得、反転された予約済みビットまたはビットの反転された予約済み組合せは、複数のデバイスが、マルチキャストパケットを送信側認証（sender authentication）をもつマルチキャストパケットとして認識することを可能にするように構成される。

【０００８】

[0008]本方法はまた、複数のデバイスのうちの１つのデバイスから、デバイスによって受信された第２のマルチキャストパケット中の１つまたは複数のメッセージ完全性検査値中のエラーを示す指示を受信することと、１つまたは複数のデバイスに、デバイスが１つまたは複数のメッセージ完全性検査値中のエラーを発見したことを示すメッセージを送信することとを含み得る。メッセージは、ネットワークにおけるマルチキャストパケットサービスを無効にする（disable）ようにとの１つまたは複数のデバイスへの命令を含み得るか、または１つまたは複数のデバイスのユニキャスト鍵（unicast key）を変更するようにとの１つまたは複数のデバイスへの命令を含み得る。メッセージ完全性検査値を決定することは、グループ時間鍵（group temporal key）を用いてマルチキャストパケット中のデータを暗号化することによって第１のメッセージ完全性検査値を生成することと、次いで、第１のメッセージ完全性検査値に基づいて複数のワイヤレスデバイスの各々のためのメッセージ完全性検査値を決定することとを含み得る。

【０００９】

[0009]本開示の別の態様は、複数のワイヤレスデバイスの各々のためのメッセージ完全性検査値を決定することと、ワイヤレスローカルエリアネットワーク上で複数のデバイスの各々にマルチキャストパケットを送信することと、マルチキャストパケットが、複数のデバイスの各々の指示と、複数のデバイスの各々のためのメッセージ完全性検査値とを含む、を行うように構成された送信機を備えるワイヤレス通信装置を提供する。

【００１０】

[0010]一態様では、本開示は、複数のワイヤレスデバイスの各々のためのメッセージ完全性検査値を決定するための手段と、ワイヤレスローカルエリアネットワーク上で複数のデバイスの各々にマルチキャストパケットを送信するための手段と、マルチキャストパケットが、複数のデバイスの各々の指示と、複数のデバイスの各々のためのメッセージ完全性検査値とを含む、を備えるワイヤレス通信装置を提供する。

【００１１】

[0011]別の態様では、本開示は、実行されたとき、デバイス中のプロセッサにワイヤレス通信のための方法を実行させる命令を備える非一時的コンピュータ可読媒体であって、上記方法は、複数のワイヤレスデバイスの各々のためのメッセージ完全性検査値を決定することと、ワイヤレスローカルエリアネットワーク上で複数のデバイスの各々にマルチキャストパケットを送信することと、マルチキャストパケットが、複数のデバイスの各々の指示と、複数のデバイスの各々のためのメッセージ完全性検査値とを含む、を備える非一時的コンピュータ可読媒体を提供する。

【図面の簡単な説明】

【００１２】

【図１】[0012]本開示の態様が採用され得るワイヤレス通信システムの一例を示す図。

【図２】[0013]図１のワイヤレス通信システム内で採用され得る例示的なワイヤレスデバイスの機能ブロック図。

【図３】[0014]メッセージ認証をもつマルチキャストフレームフォーマットパケットを示す図。

【図４】[0015]メッセージ認証をもつ別のマルチキャストフレームフォーマットパケットを示す図。

【図５Ａ】[0016]メッセージ認証をもつパケットを送信するための例示的な方法のフローチャート。

【図５Ｂ】[0017]公開鍵（public key）と秘密鍵（private key）とを使用したメッセージ認証をもつパケットを送信するための別の例示的な方法のフローチャート。

【図６】[0018]メッセージ認証をもつパケットを送信するための別の例示的な方法のフローチャート。

【図７】[0019]メッセージ認証をもつパケットを受信するための例示的な方法のフローチャート。

【図８】[0020]メッセージ認証をもつパケットを受信するための別の例示的な方法のフローチャート。

【詳細な説明】

【００１３】

[0021]添付の図面を参照しながら、新規のシステム、装置、および方法の様々な態様について以下でより十分に説明する。ただし、本開示の教示は、多くの異なる形態で実施され得るものであり、本開示全体にわたって提示する任意の特定の構造または機能に限定されるものと解釈すべきではない。むしろ、これらの態様は、本開示が周到で完全になり、本開示の範囲を当業者に十分に伝えるように与えるものである。本明細書の教示に基づいて、本開示の範囲は、本発明の他の態様とは無関係に実装されるにせよ、本発明の他の態様と組み合わされるにせよ、本明細書で開示する新規のシステム、装置、および方法のいかなる態様をもカバーするものであることを、当業者なら諒解されたい。たとえば、本明細書に記載の態様をいくつ使用しても、装置は実装され得、または方法は実施され得る。さらに、本発明の範囲は、本明細書に記載の本発明の様々な態様に加えてまたはそれらの

態様以外に、他の構造、機能、または構造および機能を使用して実施されるそのような装置または方法をカバーするものとする。本明細書で開示する任意の態様が請求項の１つまたは複数の要素によって実施され得ることを理解されたい。

【００１４】

[0022]本明細書では特定の態様について説明するが、これらの態様の多くの変形および置換は本開示の範囲内に入る。好適な態様のいくつかの利益および利点について説明するが、本開示の範囲は特定の利益、使用、または目的に限定されるものではない。むしろ、本開示の態様は、様々なワイヤレス技術、システム構成、ネットワーク、および伝送プロトコルに広く適用可能であるものとし、それらのいくつかを例として、図および好適な態様についての以下の説明において示す。詳細な説明および図面は、本開示を限定するものではなく説明するものにすぎず、本開示の範囲は添付の特許請求の範囲およびそれの均等物によって定義される。

【００１５】

[0023]ワイヤレスネットワーク技術は、様々なタイプのワイヤレスローカルエリアネットワーク（ＷＬＡＮ）を含み得る。ＷＬＡＮは、広く使用されるネットワーキングプロトコルを採用して、近接デバイスを互いに相互接続するために使用され得る。本明細書で説明する様々な態様は、ＷｉＦｉ（登録商標）、またはより一般的には、ワイヤレスプロトコルのＩＥＥＥ８０２．１１ファミリーの任意のメンバーなど、任意の通信規格に適用され得る。

【００１６】

[0024]いくつかの実装形態では、ＷＬＡＮは、ワイヤレスネットワークにアクセスする構成要素である様々なデバイスを含む。たとえば、２つのタイプのデバイス、すなわちアクセスポイント（「ＡＰ」）と（局または「ＳＴＡ」とも呼ばれる）クライアントとがあり得る。概して、ＡＰはＷＬＡＮのためのハブまたは基地局としてサービスを提供し（serve）、ＳＴＡはＷＬＡＮのユーザとしてサービスを提供し。たとえば、ＳＴＡはラップトップコンピュータ、携帯情報端末（ＰＤＡ）、モバイル電話などであり得る。一例では、ＳＴＡは、インターネットへの、または他のワイドエリアネットワークへの一般的な接続性を取得するために、ＷｉＦｉ（たとえば、ＩＥＥＥ８０２．１１プロトコル）準拠ワイヤレスリンクを介してＡＰに接続する。いくつかの実装形態では、ＳＴＡはＡＰとして使用されることもある。

【００１７】

[0025]アクセスポイント（「ＡＰ」）はまた、ノードＢ、無線ネットワークコントローラ（「ＲＮＣ」）、ｅノードＢ、基地局コントローラ（「ＢＳＣ」）、トランシーバ基地局（「ＢＴＳ」）、基地局（「ＢＳ」）、トランシーバ機能（「ＴＦ」）、無線ルータ、無線トランシーバ、または何らかの他の用語を備えるか、それらのいずれかとして実装されるか、あるいはそれらのいずれかとして知られていることがある。

【００１８】

[0026]また、局「ＳＴＡ」は、アクセス端末（「ＡＴ」）、加入者局、加入者ユニット、移動局、リモート局、リモート端末、ユーザ端末、ユーザエージェント、ユーザデバイス、ユーザ機器、または何らかの他の用語を備えるか、それらのいずれかとして実装されるか、あるいはそれらのいずれかとして知られていることがある。いくつかの実装形態では、アクセス端末は、セルラー電話、コードレス電話、セッション開始プロトコル（「ＳＩＰ」）電話、ワイヤレスローカルループ（「ＷＬＬ」）局、携帯情報端末（「ＰＤＡ」）、ワイヤレス接続機能を有するハンドヘルドデバイス、またはワイヤレスモデムに接続された何らかの他の好適な処理デバイスを備え得る。したがって、本明細書で教示する１つまたは複数の態様は、電話（たとえば、セルラーフォンまたはスマートフォン）、コンピュータ（たとえば、ラップトップ）、ポータブル通信デバイス、ヘッドセット、ポータブルコンピューティングデバイス（たとえば、個人情報端末）、エンターテインメントデバイス（たとえば、音楽またはビデオデバイス、あるいは衛星ラジオ）、ゲームデバイスまたはシステム、全地球測位システムデバイス、あるいはワイヤレス媒体を介して通信す

るように構成された他の好適なデバイスに組み込まれ得る。上記で説明したように、本明細書で説明するデバイスのいくつかは、たとえば、ＩＥＥＥ８０２．１１規格を実装し得る。

【００１９】

[0027]図１に、本開示の態様が採用され得るワイヤレス通信システム１００の一例を示す。ワイヤレス通信システム１００は、ワイヤレス規格、たとえば８０２．１１ａｈ規格に従って動作し得る。ワイヤレス通信システム１００は、ＳＴＡ１０６と通信するＡＰ１０４を含み得る。

【００２０】

[0028]様々なプロセスおよび方法は、ＡＰ１０４と複数のＳＴＡ１０６との間の、ワイヤレス通信システム１００における送信のために使用され得る。たとえば、ＯＦＤＭ／ＯＦＤＭＡ（直交周波数分割多元接続）技法に従ってＡＰ１０４とＳＴＡ１０６との間で信号が送信および受信され得る。この場合、ワイヤレス通信システム１００はＯＦＤＭ／ＯＦＤＭＡシステムと呼ばれることがある。代替的に、信号は、ＣＤＭＡ（符号分割多元接続）技法に従ってＡＰ１０４と複数のＳＴＡ１０６との間で送信および受信され得る。この場合、ワイヤレス通信システム１００はＣＤＭＡシステムと呼ばれることがある。

【００２１】

[0029]ＡＰ１０４から複数のＳＴＡ１０６のうちの１つまたは複数への送信を容易にする通信リンクはダウンリンク（ＤＬ）１０８と呼ばれることがあり、複数のＳＴＡ１０６のうちの１つまたは複数からＡＰ１０４への送信を容易にする通信リンクはアップリンク（ＵＬ）１１０と呼ばれることがある。代替的に、ダウンリンク１０８は順方向リンクまたは順方向チャネルと呼ばれることがあり、アップリンク１１０は逆方向リンクまたは逆方向チャネルと呼ばれることがある。

【００２２】

[0030]ＡＰ１０４は、基地局として働き、基本サービスエリア（ＢＳＡ）１０２内のワイヤレス通信カバレージを与え得る。ＡＰ１０４は、ＡＰ１０４に関連し、通信のためにＡＰ１０４を使用する複数のＳＴＡ１０６とともに、基本サービスセット（ＢＳＳ）と呼ばれることがある。ワイヤレス通信システム１００は、中央のＡＰ１０４を有しないことがあり、むしろ、複数のＳＴＡ１０６間のピアツーピアネットワークとして機能し得ることに留意されたい。したがって、本明細書で説明するＡＰ１０４の機能は、複数のＳＴＡ１０６のうちの１つまたは複数によって代替的に実行され得る。

【００２３】

[0031]図２に、ワイヤレス通信システム１００内で採用され得るワイヤレスデバイス２０２において利用され得る様々な構成要素を示す。ワイヤレスデバイス２０２は、本明細書で説明する様々な方法を実装するように構成され得るデバイスの一例である。たとえば、ワイヤレスデバイス２０２は、ＡＰ１０４を備えるかまたは複数のＳＴＡ１０６のうちの１つを備え得る。

【００２４】

[0032]ワイヤレスデバイス２０２は、ワイヤレスデバイス２０２の動作を制御するプロセッサ２０４を含み得る。プロセッサ２０４は中央処理ユニット（ＣＰＵ）と呼ばれることもある。読取り専用メモリ（ＲＯＭ）とランダムアクセスメモリ（ＲＡＭ）の両方を含み得るメモリ２０６は、命令とデータとをプロセッサ２０４に与える。メモリ２０６の一部は不揮発性ランダムアクセスメモリ（ＮＶＲＡＭ）をも含み得る。プロセッサ２０４は、一般に、メモリ２０６内に記憶されたプログラム命令に基づいて論理演算および算術演算を実行する。メモリ２０６中の命令は、本明細書で説明する方法を実装するために実行可能であり得る。

【００２５】

[0033]プロセッサ２０４は、１つまたは複数のプロセッサで実装された処理システムを備えるか、またはそれの構成要素であり得る。１つまたは複数のプロセッサは、汎用マイクロプロセッサ、マイクロコントローラ、デジタル信号プロセッサ（ＤＳＰ）、フィール

ドプログラマブルゲートアレイ（ＦＰＧＡ）、プログラマブル論理デバイス（ＰＬＤ）、コントローラ、状態機械、ゲート論理、個別ハードウェア構成要素、専用ハードウェア有限状態機械、あるいは情報の計算または他の操作を実行することができる任意の他の好適なエンティティ、の任意の組合せを用いて実装され得る。

【００２６】

[0034]処理システムは、ソフトウェアを記憶するための機械可読媒体をも含み得る。ソフトウェアは、ソフトウェア、ファームウェア、ミドルウェア、マイクロコード、ハードウェア記述言語などの名称にかかわらず、任意のタイプの命令を意味すると広く解釈されたい。命令は、（たとえば、ソースコードフォーマット、バイナリコードフォーマット、実行可能コードフォーマット、または任意の他の好適なコードフォーマットの）コードを含み得る。命令は、１つまたは複数のプロセッサによって実行されたとき、本明細書で説明する様々な機能を処理システムに実行させる。

【００２７】

[0035]ワイヤレスデバイス２０２はまた、ワイヤレスデバイス２０２と遠隔ロケーションとの間のデータの送信および受信を可能にするために送信機２１０と受信機２１２とを含み得るハウジング２０８を含み得る。送信機２１０と受信機２１２とは組み合わせられてトランシーバ２１４になり得る。アンテナ２１６は、ハウジング２０８に取り付けられ、トランシーバ２１４に電気的に結合され得る。ワイヤレスデバイス２０２はまた、複数の送信機、複数の受信機、複数のトランシーバ、および／または複数のアンテナを含み得る（図示せず）。

【００２８】

[0036]ワイヤレスデバイス２０２はまた、トランシーバ２１４によって受信された信号のレベルを検出し、定量化するために使用され得る信号検出器２１８を含み得る。信号検出器２１８は、総エネルギー、シンボルごとのサブキャリア当たりのエネルギー、電力スペクトル密度および他の信号などの信号を検出し得る。ワイヤレスデバイス２０２はまた、信号を処理する際に使用するデジタル信号プロセッサ（ＤＳＰ）２２０を含み得る。ＤＳＰ２２０は、送信のためのデータユニットを生成するように構成され得る。いくつかの態様では、データユニットは物理レイヤデータユニット（ＰＰＤＵ：physical layer data unit）を備え得る。いくつかの態様では、ＰＰＤＵはパケットと呼ばれる。

【００２９】

[0037]ワイヤレスデバイス２０２は、いくつかの態様では、ユーザインターフェース２２２をさらに備え得る。ユーザインターフェース２２２は、キーパッド、マイクロフォン、スピーカー、および／またはディスプレイを備え得る。ユーザインターフェース２２２は、ワイヤレスデバイス２０２のユーザに情報を伝達し、および／またはそのユーザからの入力を受信する、任意の要素または構成要素を含み得る。

【００３０】

[0038]ワイヤレスデバイス２０２の様々な構成要素はバスシステム２２６によって互いに結合され得る。バスシステム２２６は、たとえば、データバス、ならびに、データバスに加えて、電力バスと、制御信号バスと、ステータス信号バスとを含み得る。ワイヤレスデバイス２０２の構成要素は、何らかの他の機構を使用して、互いに結合されるか、または互いに入力を受け付けるか、または互いに入力を与え得ることを当業者は諒解されよう。

【００３１】

[0039]図２には、いくつかの別個の構成要素が示されているが、その構成要素のうちの１つまたは複数が組み合わされ得るかまたは共通に実装され得ることを当業者は認識されよう。たとえば、プロセッサ２０４は、プロセッサ２０４に関して上記で説明した機能を実装するためだけでなく、信号検出器２１８および／またはＤＳＰ２２０に関して上記で説明した機能を実装するためにも使用され得る。さらに、図２に示す構成要素の各々は、複数の別個の要素を使用して実装され得る。

【００３２】

[0040]いくつかの態様では、ＡＰ１０４から同時にいくつかのＳＴＡ１０６にマルチキャストフレームまたはブロードキャストフレームを送ることが望ましいことがある。たとえば、教室設定（a classroom setting）では、各学生は教師からの同じ指示または資料を必要とし得るので、教師が一度にすべての学生にブロードキャストパケットを送ることが望ましいことがある。また、ブロードキャストパケットまたはマルチキャストパケットがＩＥＥＥ８０２．１１プロトコルネットワークなど、ＷＬＡＮネットワークにおいて望ましいことがある、いくつかの他の設定がある。たとえば、ブロードキャストパケットまたはマルチキャストパケットは、ライブストリーミング、緊急メッセージング、広告、または他の適用例のためにも使用され得る。

【００３３】

[0041]しかしながら、現在のホットスポット（Hotspot）２．０規格は、マルチキャストフレームが十分なセキュリティ機能を含まないことがあるので、これらのマルチキャストフレームを強く阻止する（discourage）。マルチキャストフレームの１つの現在の問題は、マルチキャストパケットのための現在のプロトコルが、ＳＴＡ１０６がＡＰ１０４になりすまし（masquerade as）、マルチキャストフレームを送り得る、「ホール（Hole）１９６攻撃」を受けやすい（vulnerable to）ことがあることである。対称鍵が現在のマルチキャストフレームにおいて使用されるので、そのような脆弱性が存在し得、このことは、ネットワークの一部であるＳＴＡ１０６は、マルチキャストフレームを送る際にＡＰ１０４になりすますことが可能であり得、他のＳＴＡ１０６は、ＡＰ１０４によって送られたマルチキャストフレーム、またはＡＰ１０４になりすましているＳＴＡ１０６によって送られたマルチキャストフレームの間の違いを見分ける（tell）ことが可能でないことを意味する。そのようなりすましＳＴＡ１０６は、たとえば、なりすましＳＴＡ１０６が、他のＳＴＡ１０６からのデータフレームをインターセプトするためにそれ自体のＭＡＣアドレスをＡＰ１０４のＭＡＣアドレスに関連付ける、アドレス解決プロトコル（ＡＲＰ：Address Resolution Protocol）ポイズニング（poisoning）のために使用され得る。したがって、マルチキャストフレームの送信者がＡＰ１０４であることをＳＴＡ１０６が検証することを可能にし、ＷＬＡＮにおいてより多くのセキュアなブロードキャストパケットおよびマルチキャストパケットを使用可能にするために好適なマルチキャストフォーマットを提供することは有益であり得る。

【００３４】

[0042]図３は、高められたセキュリティ機能をもつマルチキャストフレームフォーマットパケット３００を示す。たとえば、このパケット３００は、ＡＰ１０４からＳＴＡ１０６に送られる任意のマルチキャストフレームまたはブロードキャストフレームのために使用され得る。たとえば、このパケット３００は、データフレームのために、および管理フレームのために使用され得る。いくつかの態様では、パケット３００の各部分のためにリストされたオクテットの数は異なり得る。たとえば、パケット３００の各部分のためのオクテットのリストされた数は例にすぎないことがある。

【００３５】

[0043]マルチキャストフレームフォーマットパケット３００は、２オクテットフレーム制御３０５フィールドと、２オクテット持続時間ＩＤ３１０フィールドと、３つの６オクテットアドレスフィールド３１５、３２０、３２５とを含み得る。マルチキャストフレームフォーマットパケット３００は、２オクテットシーケンス制御フィールド３３０と、フレーム本体３３５と、４オクテットフレーム検査シーケンス（ＦＣＳ）３４０とをさらに含み得る。いくつかの態様では、フレーム本体以外の、フレームフォーマット３００のこれらの部分の各々はフレームの前のタイプと同様であり得る。フレーム本体３３５は、ブロック連鎖メッセージ認証コードプロトコル（ＣＣＭＰ）ヘッダ３４５をもつカウンタ暗号モードと、データ長３５０と、暗号化データ（encrypted data）３５５と、グループ時間鍵ベースの（ＧＴＫベースの）ＭＩＣ（メッセージ完全性コード）３６０と、２つまたはそれ以上のＡＩＤまたはＭＡＣ（メディアアクセス制御）アドレス３６５およびＭＩＣ３７０とを含み得る。

【００３６】
[0044]いくつかの態様では、通常のパケットの場合のように、ＣＣＭＰヘッダ３４５および暗号化データ３５５はＧＴＫに基づいて作成され得る。しかしながら、フォーマット３００は、いくつかの点で普通のフレームとは異なり得る。まず、追加のセキュリティを与えるために、フレームが各ＳＴＡ１０６に宛てられるその各ＳＴＡ１０６のために、ＳＴＡ１０６のＡＩＤまたはＭＡＣアドレス３６５が、複数のＳＴＡの各々のためのメッセージ完全性検査（ＭＩＣ）３７０とともに送信され得る。これらの要素は、通常、ＳＴＡ１０６に送られるユニキャストパケット中で送信され得る。いくつかの態様では、各ＳＴＡ１０６のためのＭＩＣ３７０は、フレームヘッダと、データと、ＳＴＡ１０６のＭＡＣアドレスおよび／またはＡＩＤと、ＣＣＭＰヘッダ３４５中のＰＮシーケンス番号およびＳＴＡペアワイズ過渡鍵（ＰＴＫ）とに基づいて生成され得る。しかしながら、いくつかの態様では、代わりにＣＣＭＰヘッダ３４５中のＰＮシーケンス番号、およびＧＴＫのために生成されたＭＩＣに基づいてＭＩＣを生成することが有益であり得る。対称鍵のみを含んだマルチキャストフレームの前のフォーマットとは異なり、そのようなＳＴＡごとのＭＩＣ３７０（a per STA MIC 370）を含むことはホール１９６攻撃（Hole 196 attacks）を防ぎ得る。したがって、マルチキャストパケット３００を受信する各ＳＴＡのためのＡＩＤまたはＭＡＣアドレス３６５およびＭＩＣ３７０を追加することは、マルチキャストまたはブロードキャストパケットにおけるセキュリティの向上を可能にし得る。
【００３７】
[0045]いくつかの態様では、パケット３００のフレーム本体３３５はデータ長フィールド３５０を含み得る。そのようなデータ長フィールド３５０は、パケットのデータ長がユニキャストパケットの持続時間フィールド３１０に基づいて推論され得るので、他のパケットフォーマットでは必要とされないことがある。しかしながら、マルチキャストパケット３００では、データの持続時間は、マルチキャストパケット３００が可変数のＡＩＤまたはＭＡＣアドレス３６５と可変数のＭＩＣ３７０とを有し得るので、持続時間フィールド３１０から推論されないことがある。したがって、マルチキャストパケット中に含まれるデータの長さを示すために追加のデータ長フィールド３５０が使用され得る。
【００３８】
[0046]いくつかの態様では、ＣＣＭＰヘッダ３４５はいくつかの予約済みビットを含み得る。いくつかの態様では、パケットが、ＳＴＡごとのＭＩＣ（per STA MICs）を含んでいるマルチキャストパケットであることをＳＴＡに示すために、予約済みビットのうちの１つが、パケット３００のフォーマットをもつ暗号化ＭＰＤＵ（encrypted MPDU）を示すために使用され得る。たとえば、パケット３００のフォーマットをもつ暗号化ＭＰＤＵを示すために予約済みビットの値が変更され得る。いくつかの態様では、ＣＣＭＰヘッダ３４５中のビットの組合せ（a combination of bits）が予約され（reserved）得、パケットがパケット３００のフォーマットによる暗号化マルチキャストパケットであることをＳＴＡ１０６に示すためにビットの予約済み組合せ（a reserved combination of bits）が選定され得る。たとえば、パケットがパケット３００のフォーマットによる暗号化マルチキャストパケットであることを示すために、ビットの予約済み組合せなど、ビットの組合せの値が変更され得る。予約済みビットまたはビットの予約済み組合せを変更することによって、パケットは、そのパケットが本明細書で説明するセキュリティ機能および／または暗号化を含むことを受信デバイスに示し得る。いくつかの態様では、図３中のＳＴＡごとのＭＩＣ手法の１つの欠点は、マルチキャストパケットがより多数のパケットに伝えられる際、より多くのＳＴＡごとのＡＩＤまたはＭＡＣアドレス３６５が必要とされ、より多くのＳＴＡごとのＭＩＣ３７０が必要とされることであり得る。したがって、パケットが多数のＳＴＡに伝えられる際、増加する量のオーバーヘッド情報が各パケットを用いて送信される必要があり得る。
【００３９】
[0047]いくつかの態様では、各パケット中にＳＴＡごとのＭＩＣ３７０を含めることによって生成されたオーバーヘッドを低減するための１つの可能な方法は、各ＭＩＣのサイ

ズを縮小することを含み得る。たとえば、いくつかの態様では、各ＳＴＡごとのＭＩＣ３７０は８オクテットであり得る。そのようなサイズは2^{8*8}個の異なる値を可能にし得る。これは、なりすましＳＴＡが、ＡＰ１０４のふりをする（pretending to be the AP 104）パケットを送信している間にＳＴＡ　ＭＩＣ３７０の適切な値を正しく推測することを極めて困難にし得る。しかしながら、ＳＴＡごとに８オクテットＭＩＣを含めることは、特にマルチキャストパケット３００が多数のＳＴＡ１０６に送信されるとき、各パケットにかなりの量のオーバーヘッドを追加し得る。したがって、より短いＭＩＣ３７０を与えることが有利であり得る。しかしながら、より短いＭＩＣ３７０は、通常、なりすましデバイスが推測することがより容易であるという欠点を有し得る。マルチキャストパケット３００のこの欠陥を解決するために使用され得る１つの方法は、パケットを受信するＳＴＡ１０６の各々により短いＭＩＣ３７０を与え、ＳＴＡ１０６のＭＩＣ３７０が正しくない場合、ＳＴＡ１０６が機構（a mechanism）により他のＳＴＡ１０６にアラートし得るその機構を可能にすることである。

【００４０】

[0048]たとえば、任意のＳＴＡ１０６は、誤ったＭＩＣ３７０をもつマルチキャストフレームを受信すると、不正なエンティティ（a rogue entity）がマルチキャストフレームを送信していることをＡＰ１０４に通知するためのメッセージをＡＰ１０４に送信し得る。いくつかの態様では、ＳＴＡ１０６が、予想される値とは異なる値をもつＭＩＣ３７０を含んでいるパケットを受信した場合、ＳＴＡ１０６はＡＰ１０４にアラートし得る。ＡＰ１０４は、このエラーがＳＴＡ１０６によってパケットを受信する際のエラーによるものであったかどうか、またはパケット自体が、ＡＰ１０４によって送られておらず、なりすましＳＴＡなどの不正なエンティティによって送られていたかどうか、を決定するように構成され得る。ＡＰ１０４は、次いで、そのような不正なエンティティを学習するといくつかのアクションを起こし得る。たとえば、ＡＰ１０４はＢＳＳにおけるマルチキャストサービスを停止し得る。ＡＰ１０４は、不正なデバイスがマルチキャストフレームを送信していることをすべてのデバイスに通知するメッセージをブロードキャストするように構成され得る。このメッセージは、デバイスが不正なデバイスからのフレームを廃棄することを可能にするために、フレームのいくつかのパラメータを含み得る。ＡＰ１０４はまた、ＢＳＳ中のデバイスのユニキャスト鍵を変更し得る。たとえば、ＡＰ１０４は、メッセージがＡＰ１０４によって送られたかどうかを決定するためにデバイスによって使用されるペアワイズ過渡鍵（ＰＴＫ）など、鍵を変更するようにデバイスに命令し得る。たとえば、デバイスがＡＰ１０４になりすましている（masquerading as the AP 104）場合、そのデバイスはネットワーク中のデバイスのうちのいくつかにＭＩＣ３７０をうまく送信していることがある。したがって、各個々のデバイスのためのＭＩＣ３７０はそのデバイスのユニキャスト鍵に少なくとも部分的に基づき得るので、ユニキャスト鍵の変更後に、なりすましデバイスが正しいＭＩＣ３７０の値をそれらのデバイスに送ることができないように、各デバイスがそれのユニキャスト鍵を変更すれば有益であり得る。

【００４１】

[0049]いくつかの態様では、より短いＭＩＣ３７０を各ＳＴＡ１０６に与えるが、誤ったＭＩＣ３７０が受信された場合にＳＴＡ１０６が機構によってＡＰ１０４にアラートし得るその機構をも与えることによって、ネットワークのセキュリティは改善され得る。これはまた、ＡＰ１０４にアラートするためのリアクティブな機構がなければ（without the reactive mechanism）、より長いＭＩＣ３７０を各ＳＴＡ１０６に与えることと比較してオーバーヘッドを低減し得る。たとえば、５つのＳＴＡ１０６がそれぞれ２オクテットＭＩＣ３７０を受信する場合、５つの２オクテットＭＩＣ値３７０の2^{8*2*5}個の異なる可能な組合せがあり得る。これは、2^{8*8}個である、単一の８オクテットＭＩＣの異なる値の数よりも高い。したがって、８オクテットよりも短いＭＩＣ３７０を与えることが有益であり得、ＭＩＣサイズのそのような低減はより大きいＭＩＣサイズよりも低いセキュリティを生じないことがある。

【００４２】

[0050]図４は、高められたセキュリティ機能をもつ別のマルチキャストフレームフォーマットパケット４００を示す。たとえば、このパケット４００は、ＡＰ１０４からＳＴＡ１０６に送られるすべてのフレームのために使用され得る。たとえば、このパケット４００は、データフレームと管理フレームの両方のために使用され得る。いくつかの態様では、パケット４００の各部分のためにリストされたオクテットの数は、例にすぎないことがあるリストされた数とは異なり（vary from）得る。

【００４３】

[0051]マルチキャストフレームフォーマットパケット４００は、２オクテットフレーム制御４０５フィールドと、２オクテット持続時間ＩＤ４１０フィールドと、３つの６オクテットアドレスフィールド４１５、４２０、４２５とを含み得る。パケット４００は、２オクテットシーケンス制御フィールド４３０と、フレーム本体４３５と、４オクテットフレーム検査シーケンス（ＦＣＳ）４４０とをさらに含み得る。いくつかの態様では、フレーム本体以外の、フレームフォーマット４００のこれらの部分の各々はフレームの前のタイプ（previous types of frames）と同様であり得る。フレーム本体４３５は、ブロック連鎖メッセージ認証コードプロトコル（ＣＣＭＰ）ヘッダ４４５をもつカウンタ暗号モードと、暗号化データ４５５と、デジタル署名４７５とを含み得る。

【００４４】

[0052]パケット３００の場合と同様に、パケット４００は、フレーム本体４３５を除くパケットのすべての部分において前のパケット（previous packets）と同様であり得る。パケット３００の場合と同様に、ＣＣＭＰヘッダ４４５は、パケットがマルチキャストパケット４００であるというＳＴＡ１０６への指示を含むように構成され得る。たとえば、ＣＣＭＰヘッダ４４５は、パケットがマルチキャストパケット４００であることを示すために、それの予備値（its reserve value）から反転された（flipped）予約済みビット（reserved bit）を含み得る。いくつかの態様では、ＣＣＭＰヘッダ４４５は、パケットがマルチキャストパケット４００であることを示すために、ビットの予約済み組合せ（a reserved combination of bits）を含み得る。いくつかの態様では、パケット３００とは異なり、デジタル署名４７５は何らかの固定長として定義され得るので、データ長フィールドはパケット４００では必要とされないことがある。したがって、暗号化ブロードキャストデータ４５５の持続時間をＳＴＡ１０６に示すには持続時間フィールド４１０のみで十分であり得る。

【００４５】

[0053]パケット４００が、なりすましＳＴＡ１０６ではなくＡＰ１０４によって送信されたことを保証するために、パケット４００はデジタル署名４７５を含み得る。いくつかの態様では、デジタル署名４７５は公開鍵／秘密鍵方式に基づき得る。この方式では、パケットベースごとのデジタル署名（a per packet-based digital signature）４７５が使用され得る。これは、ＧＴＫデータで暗号化されたデータをハッシングすることと、次いでデータのハッシュ値に基づいてデジタル署名４７５を計算することとを含み得る。いくつかの態様では、デジタル署名４７５は、データまたはデータのハッシュのいずれかに基づいて計算され得る。いくつかの態様では、デジタル署名４７５はまた、カウンタモード暗号ブロック連鎖メッセージ認証コードプロトコル（ＣＣＭＰ）ヘッダ４４５中のシーケンス（ＰＮ）番号に基づき得る。いくつかの態様では、デジタル署名４７５はまた、ＧＴＫによって生成されたＭＩＣに基づいて生成され得る。これは、計算するのがより複雑であり得る、データ全体のためにデジタル署名４７５を計算することを回避し得るので、これはいくつかの態様では有益であり得る。

【００４６】

[0054]デジタル署名４７５は、次いで、フレームに付加され得る。この手法は他の手法に勝るいくつかの利点を提供し得る。たとえば、この手法は、パケット３００の場合のように、各ＳＴＡ１０６のためのいくつかの個々のＭＩＣを付加することよりも小さいことがある、固定長の単一のデジタル署名４７５のみを必要とし得る。同様に、特にＳＴＡの数が大きいとき、単一のシグネチャを計算することは、個々のＭＩＣを計算することより

も単純であり得る。しかしながら、この手法はいくつかの欠点をも有し得る。たとえば、公開／秘密鍵システムにおいて使用されるものなど、非対称暗号化（asymmetric encryption）はより計算量的に複雑（computationally complex）であり得る。これは、ＳＴＡのためのパケットごとの検証（packet-by-packet verification）をより困難にし得る。さらに、公開／秘密鍵ペアの生成は困難であり得る。この状況では、ＡＰ１０４は、それ自体の認証局として働き得、公開／秘密鍵ペアを動的に生成する必要があり得る。これはＡＰにとって計算量的に複雑であり得る。各鍵ペアは、セキュリティを維持するためにある時間期間の後に満了するように構成され得、これは新しい公開／秘密鍵ペアの生成を必要とし得る。

【００４７】

[0055]パケット４００において使用され得る暗号化の１つのタイプは楕円曲線暗号法（ＥＣＣ：elliptic curve cryptography）である。ＥＣＣは、デジタル署名４７５を生成するために使用され得、他の技法に勝る利点を提供し得る。たとえば、ＥＣＣは少量の計算オーバーヘッドを必要とし得る。ＥＣＣを使用するデジタル署名４７５の生成は、暗号法の他の領域において使用され得る方法を伴い得る。たとえば、デジタル署名４７５を暗号化するために、公開鍵暗号化のためのＩＥＥＥ１３６３規格に記載されている楕円曲線デジタル署名アルゴリズム（ＥＣＤＳＡ：Elliptic Curve Digital Signature Algorithm）が使用され得る。いくつかの態様では、デジタル署名４７５は、その両方が参照により本明細書に組み込まれる、ＮＩＳＴ特別公開８００－５６Ａ（NIST Special Publication 800-56A）、「Recommendation for Pair-Wire Key Establishment Schemes Using Discrete Logarithm Cryptography」と、ＦＩＰＳ公開１８６－３、「Digital Signature Standard (DSS)」とに開示されているものなどの技法に少なくとも部分的に基づいて生成され得る。いくつかの態様では、各公開鍵／秘密鍵ペアは、ＡＰ１０４のタイマー同期機能（ＴＳＦ：timer synchronization function）に関して与えられ得る満了時間を含み得る。

【００４８】

[0056]公開鍵／秘密鍵暗号化方法を使用するために、公開鍵はネットワークにおいてＳＴＡ１０６に与えられなければならない。公開鍵を与える際に、各ＳＴＡ１０６は、それが使用している公開鍵がＡＰ１０４によって送られたことを検証するように構成され得る。たとえば、ＡＰ１０４は、ＳＴＡ１０６のＰＴＫを使用して暗号化された暗号化ユニキャストフレーム中でＳＴＡ１０６に公開鍵を送信し得る。これは、鍵の送信者が実際にＡＰ１０４であったことをＳＴＡ１０６が確信することを可能にし得る。

【００４９】

[0057]図５Ａに、メッセージ認証をもつパケットを送信するための例示的な方法のフローチャートを示す。いくつかの態様では、この方法は、ブロードキャストパケットを送るときにＷＬＡＮネットワーク上のＡＰ１０４によって行われ得る。

【００５０】

[0058]ブロック５０５において、ＡＰ１０４は、ワイヤレスローカルエリアネットワーク上で複数のデバイスに送信されるべきブロードキャストパケットのためのデジタル署名を決定し、このデジタル署名は、ブロードキャストパケットを送信するデバイスの識別（an identity）を複数のデバイスの各々が検証することを可能にするために非対称暗号法を使用して暗号化される。いくつかの態様では、このデジタル署名は、楕円曲線暗号法を使用して暗号化され得る。いくつかの態様では、決定するための手段はプロセッサまたは送信機を備え得る。いくつかの態様では、本方法は、公開鍵／秘密鍵ペアを生成することをさらに備え、ここで、公開鍵は、秘密鍵を使用して暗号化されたメッセージを解読するために使用され得る。いくつかの態様では、これらの公開鍵は個々のワイヤレスデバイスに送信され得る。ＡＰになりすましている他のデバイスによって送信されている偽の鍵など、公開鍵の送信に対するセキュリティ攻撃を防ぐために、ブロードキャストパケット中ではなく個々に各ワイヤレスデバイスに公開鍵を送ることが望ましいことがある。これは、デバイスに第１の公開鍵を送るときに特に有用であり得る。いくつかの態様では、ＡＰは、ある時間間隔で公開鍵／秘密鍵ペアを生成することと、新しい鍵ペアが生成された後

にワイヤレスデバイスに新しい公開鍵を送信することとを行うように構成され得る。本明細書で説明するように、更新された公開鍵のこれらの送信は、前の公開鍵を有するデバイスにブロードキャストパケット中で送信され得る。しかしながら、ネットワークに対する新しいデバイスは、そのようなブロードキャストパケットを認証することが可能でないことがあるので、個々にネットワーク上の新しいデバイスに公開鍵を送ることが有用であり得る。

【００５１】

[0059]いくつかの態様では、公開／秘密鍵の各々は満了時間を有し得る。たとえば、この満了時間は、新しい公開／秘密鍵ペアが生成され、ネットワーク中のデバイスに送信され得る時間と一致し得る。この満了時間はいくつかの方法でデバイスに送信され得る。たとえば、この満了タイは、タイマー同期機能の一部としてネットワーク中のデバイスの各々に送信され得る。

【００５２】

[0060]ブロック５１０において、ＡＰ１０４はネットワーク上でブロードキャストパケットを送信し、ブロードキャストパケットはデジタル署名を含む。いくつかの態様では、デジタル署名はパケットのフレーム本体中で暗号化データの後に含まれ得る。いくつかの態様では、パケットを送信するための手段は送信機を備え得る。

【００５３】

[0061]図５Ｂに、公開鍵と秘密鍵とを使用したメッセージ認証をもつパケットを送信するための別の例示的な方法のフローチャートを示す。いくつかの態様では、この方法は、ブロードキャストパケットを送るときにＷＬＡＮネットワーク上のＡＰ１０４によって行われ得る。

【００５４】

[0062]ブロック５２０において、方法５１５は、公開鍵および秘密鍵を生成することを含む。たとえば、公開鍵および秘密鍵は、楕円曲線暗号法または別の形態の非対称暗号法に基づいて生成され得る。いくつかの態様では、公開鍵および秘密鍵を生成するための手段はプロセッサを含み得る。

【００５５】

[0063]ブロック５２５において、方法５１５は、複数のデバイスのうちの１つのデバイスに公開鍵を送信することを含み、公開鍵は、秘密鍵を使用して暗号化されたメッセージを解読するように構成される。たとえば、公開鍵と秘密鍵は、公開鍵が、秘密鍵を使用して暗号化されたメッセージを解読するために使用され得るような、鍵ペアであり得る。しかしながら、非対称暗号法の性質により、メッセージを暗号化するには秘密鍵が必要であり得るので、公開鍵はメッセージを暗号化することが可能でないことがある。いくつかの態様では、公開鍵を送信するための手段は送信機を含み得る。いくつかの態様では、公開鍵を送信することは、公開鍵がその後に使用されないことがある、公開鍵についての満了時間を送信することをも含み得る。たとえば、満了タイマーはタイマー同期機能中に含まれ得る。

【００５６】

[0064]ブロック５３０において、方法５１５は、ワイヤレスローカルエリアネットワーク上で複数のデバイスに送信されるべきブロードキャストパケットのためのデジタル署名を決定することを含み、デジタル署名は、ブロードキャストパケットを送信するデバイスの識別を複数のデバイスの各々が検証することを可能にするために非対称暗号法を使用して暗号化され、ここにおいて、デジタル署名を決定することは、秘密鍵を使用してデジタル署名を決定することを備える。いくつかの態様では、デジタル署名を決定するための手段はプロセッサを含み得る。

【００５７】

[0065]ブロック５３５において、方法５１５は、ネットワーク上でブロードキャストパケットを送信することを含み、ブロードキャストパケットはデジタル署名を含む。いくつかの態様では、ブロードキャストパケットを送信するための手段は送信機を含み得る。

【００５８】
[0066]図６に、メッセージ認証をもつパケットを送信するための別の例示的な方法のフローチャートを示す。いくつかの態様では、この方法は、１つまたは複数のＳＴＡ１０６と通信しているネットワーク上にあるＡＰ１０４など、ワイヤレスデバイスによって行われ得る。
【００５９】
[0067]ブロック６０２において、ＡＰ１０４は、複数のワイヤレスデバイスの各々のためのメッセージ完全性検査値を決定する。たとえば、ＡＰ１０４は、複数のワイヤレスデバイスの各々にマルチキャストパケットを送信することを望み得る。したがって、それらのデバイスがマルチキャストメッセージの送信者を検証することを可能にするために、ＡＰ１０４はデバイスの各々のためのＭＩＣ値を決定し得る。いくつかの態様では、ＭＩＣ値を決定するための手段はプロセッサを含み得る。
【００６０】
[0068]ブロック６０５において、ＡＰ１０４は、ワイヤレスローカルエリアネットワーク上で複数のデバイスの各々にマルチキャストパケットを送信し、マルチキャストパケットは、複数のデバイスの各々の指示と、複数のデバイスの各々のためのメッセージ完全性検査値とを含む。いくつかの態様では、送信するための手段は送信機を含み得る。いくつかの態様では、指示は、マルチキャストパケットが宛てられた各デバイスを識別する１つまたは複数のＭＡＣアドレスまたはＡＩＤであり得る。いくつかの態様では、メッセージ完全性検査値は８オクテット未満の短縮されたメッセージ完全性検査であり得る。たとえば、そのような短縮された値の使用は、ＭＩＣを含んでいるパケットの部分がより短い時間で送信されることを可能にし、したがって、より大きいサイズをもつＭＩＣ値を使用することよりも少ないオーバーヘッドを有し得る。
【００６１】
[0069]ブロック６１０において、ＡＰ１０４は、複数のデバイスのうちの１つのデバイスから、デバイスによって受信された第２のマルチキャストパケット中の１つまたは複数のメッセージ完全性検査値中のエラーを示す指示を受信する。いくつかの態様では、この指示は、他のデバイスがＡＰ１０４になりすましていることがあるかどうかを決定するためにＡＰ１０４によって使用され得る。たとえば、この指示は、パケット中の所与のメッセージ完全性検査値がそうであるべきである値でないとデバイスが決定したときに受信され得る。これは、ＡＰ１０４以外のデバイスがパケットを送信したことを意味し得る。いくつかの態様では、受信するための手段は受信機を含み得る。
【００６２】
[0070]ブロック６１５において、ＡＰ１０４は、１つまたは複数のデバイスに、デバイスがパケット中の１つまたは複数のメッセージ完全性検査値中のエラーを発見したことを示すメッセージを送信する。たとえば、ＡＰ１０４が、ブロック６１０においてデバイスによって受信されたパケットがＡＰ１０４によって送られなかったと決定した場合、ＡＰ１０４は、なりすましＳＴＡについて他のデバイスに警報を出し、なりすましパケットを無視するように他のデバイスに通知し、ＢＳＳにおけるマルチキャストサービスをオフにし、および／またはネットワーク中の１つまたは複数のデバイスのユニキャスト鍵を変更し得る。いくつかの態様では、送信するための手段は送信機を含み得る。
【００６３】
[0071]図７に、メッセージ認証をもつパケットを受信するための例示的な方法のフローチャートを示す。いくつかの態様では、この方法は、ＡＰ１０４と通信しているネットワーク上にあるＳＴＡ１０６など、ワイヤレスデバイスによって行われ得る。
【００６４】
[0072]ブロック７０５において、ＳＴＡ１０６はワイヤレスローカルエリアネットワークを介してブロードキャストパケットを受信し、ブロードキャストパケットはデジタル署名を含む。いくつかの態様では、受信するための手段は受信機を含み得る。
【００６５】

[0073]ブロック７１０において、ＳＴＡ１０６は、パケットを送信するデバイスの識別を検証するために、公開鍵を使用してデジタル署名を解読する。いくつかの態様では、解読するための手段はプロセッサまたは受信機を含み得る。

【００６６】

[0074]図８に、メッセージ認証をもつパケットを受信するための例示的な方法のフローチャートを示す。いくつかの態様では、この方法は、ＡＰ１０４と通信しているネットワーク上にあるＳＴＡ１０６など、ワイヤレスデバイスによって行われ得る。

【００６７】

[0075]ブロック８０５において、ＳＴＡ１０６は、ワイヤレスローカルエリアネットワーク上で複数のデバイスに送信されたブロードキャストパケットを受信し、パケットは、複数のデバイスの各々の指示と、複数のデバイスの各々のためのメッセージ完全性検査値とを含む。いくつかの態様では、受信するための手段は受信機を含み得る。

【００６８】

[0076]ブロック８１０において、ＳＴＡ１０６は、複数のデバイスの各々の指示と、複数のデバイスの各々のためのメッセージ完全性検査値とに少なくとも基づいて、パケットを送信したデバイスの識別を検証する。いくつかの態様では、検証するための手段はプロセッサまたは受信機を含み得る。いくつかの態様では、パケットを送信したデバイスの識別が検証されることができなかった場合、ＳＴＡ１０６は、メッセージ完全性検査値中のメッセージ中のエラーを示す指示を送信するように構成され得る。いくつかの態様では、送信するための手段は送信機を含み得る。

【００６９】

[0077]本明細書で使用する「決定すること」という用語は、多種多様なアクションを包含する。たとえば、「決定すること」は、計算すること、算出すること、処理すること、導出すること、調査すること、探索すること（たとえば、テーブル、データベース、または別のデータ構造の中で探索すること）、確認することなどを含み得る。また、「決定すること」は、受信すること（たとえば、情報を受信すること）、アクセスすること（たとえば、メモリ中のデータにアクセスすること）などを含み得る。また、「決定すること」は、解決すること、選択すること、選定すること、確立することなどを含み得る。さらに、本明細書で使用する「チャネル幅」は、いくつかの態様では帯域幅を包含することがあるか、または帯域幅と呼ばれることもある。

【００７０】

[0078]上記で説明した方法の様々な動作は、（１つまたは複数の）様々なハードウェアおよび／またはソフトウェア構成要素、回路、および／または（１つまたは複数の）モジュールなど、それらの動作を実行することが可能な任意の好適な手段によって実行され得る。概して、図に示されたどの動作も、その動作を実施することが可能な対応する機能的手段によって実施され得る。

【００７１】

[0079]本開示に関連して説明した様々な例示的な論理ブロック、モジュール、および回路は、汎用プロセッサ、デジタル信号プロセッサ（ＤＳＰ）、特定用途向け集積回路（ＡＳＩＣ）、フィールドプログラマブルゲートアレイ信号（ＦＰＧＡ）または他のプログラマブル論理デバイス（ＰＬＤ）、個別ゲートまたはトランジスタ論理、個別ハードウェア構成要素、あるいは本明細書で説明した機能を実行するように設計されたそれらの任意の組合せを用いて実装または実行され得る。汎用プロセッサはマイクロプロセッサであり得るが、代替として、プロセッサは、任意の市販のプロセッサ、コントローラ、マイクロコントローラまたは状態機械であり得る。プロセッサはまた、コンピューティングデバイスの組合せ、たとえば、ＤＳＰとマイクロプロセッサとの組合せ、複数のマイクロプロセッサ、ＤＳＰコアと連携する１つまたは複数のマイクロプロセッサ、あるいは任意の他のそのような構成として実装され得る。

【００７２】

[0080]１つまたは複数の態様では、説明した機能は、ハードウェア、ソフトウェア、フ

ァームウェア、またはそれらの任意の組合せで実装され得る。ソフトウェアで実装される場合、機能は、１つまたは複数の命令またはコードとしてコンピュータ可読媒体上に記憶されるか、あるいはコンピュータ可読媒体を介して送信され得る。コンピュータ可読媒体は、ある場所から別の場所へのコンピュータプログラムの転送を可能にする任意の媒体を含む通信媒体と、コンピュータ記憶媒体との両方を含む。記憶媒体は、コンピュータによってアクセスされ得る任意の利用可能な媒体であり得る。限定ではなく例として、そのようなコンピュータ可読媒体は、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ（登録商標）、ＣＤ－ＲＯＭまたは他の光ディスクストレージ、磁気ディスクストレージまたは他の磁気ストレージデバイス、あるいは命令またはデータ構造の形態の所望のプログラムコードを搬送または記憶するために使用され得、コンピュータによってアクセスされ得る、任意の他の媒体を備えることができる。また、いかなる接続もコンピュータ可読媒体と適切に呼ばれる。たとえば、ソフトウェアが、同軸ケーブル、光ファイバーケーブル、ツイストペア、デジタル加入者回線（ＤＳＬ）、または赤外線、無線、およびマイクロ波などのワイヤレス技術を使用して、ウェブサイト、サーバ、または他のリモートソースから送信される場合、同軸ケーブル、光ファイバーケーブル、ツイストペア、ＤＳＬ、または赤外線、無線、およびマイクロ波などのワイヤレス技術は、媒体の定義に含まれる。本明細書で使用するディスク（disk）およびディスク（disc）は、コンパクトディスク（disc）（ＣＤ）、レーザーディスク（登録商標）（disc）、光ディスク（disc）、デジタル多用途ディスク（disc）（ＤＶＤ）、フロッピー（登録商標）ディスク（disk）およびｂｌｕ－ｒａｙ（登録商標）ディスク（disc）を含み、ディスク（disk）は、通常、データを磁気的に再生し、ディスク（disc）は、データをレーザーで光学的に再生する。したがって、いくつかの態様では、コンピュータ可読媒体は非一時的コンピュータ可読媒体（たとえば、有形媒体）を備え得る。さらに、いくつかの態様では、コンピュータ可読媒体は一時的コンピュータ可読媒体（たとえば、信号）を備え得る。上記の組合せもコンピュータ可読媒体の範囲内に含まれるべきである。

【００７３】

[0081]本明細書で開示した方法は、説明した方法を達成するための１つまたは複数のステップまたはアクションを備える。本方法のステップおよび／またはアクションは、特許請求の範囲から逸脱することなく互いに交換され得る。言い換えれば、ステップまたはアクションの特定の順序が指定されない限り、特定のステップおよび／またはアクションの順序および／または使用は特許請求の範囲から逸脱することなく変更され得る。

【００７４】

[0082]説明した機能は、ハードウェア、ソフトウェア、ファームウェア、またはそれらの任意の組合せで実装され得る。ソフトウェアで実装される場合、機能は１つまたは複数の命令としてコンピュータ可読媒体上に記憶され得る。記憶媒体は、コンピュータによってアクセスされ得る任意の利用可能な媒体であり得る。限定ではなく例として、そのようなコンピュータ可読媒体は、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、ＣＤ－ＲＯＭまたは他の光ディスクストレージ、磁気ディスクストレージまたは他の磁気ストレージデバイス、あるいは命令またはデータ構造の形態の所望のプログラムコードを搬送または記憶するために使用され得、コンピュータによってアクセスされ得る、任意の他の媒体を備えることができる。本明細書で使用するディスク（disk）およびディスク（disc）は、コンパクトディスク（disc）（ＣＤ）、レーザーディスク（disc）、光ディスク（disc）、デジタル多用途ディスク（disc）（ＤＶＤ）、フロッピーディスク（disk）およびｂｌｕ－ｒａｙディスク（disc）を含み、ディスク（disk）は、通常、データを磁気的に再生し、ディスク（disc）は、データをレーザーで光学的に再生する。

【００７５】

[0083]したがって、いくつかの態様は、本明細書で提示した動作を実行するためのコンピュータプログラム製品を備え得る。たとえば、そのようなコンピュータプログラム製品は、本明細書で説明した動作を実行するために１つまたは複数のプロセッサによって実行可能である命令を記憶した（および／または符号化した）コンピュータ可読媒体を備え得

る。いくつかの態様では、コンピュータプログラム製品はパッケージング材料を含み得る。

【００７６】

[0084]ソフトウェアまたは命令はまた、伝送媒体を介して送信され得る。たとえば、ソフトウェアが、同軸ケーブル、光ファイバーケーブル、ツイストペア、デジタル加入者回線（ＤＳＬ）、または赤外線、無線、およびマイクロ波などのワイヤレス技術を使用して、ウェブサイト、サーバ、または他のリモートソースから送信される場合、同軸ケーブル、光ファイバーケーブル、ツイストペア、ＤＳＬ、または赤外線、無線、およびマイクロ波などのワイヤレス技術は、伝送媒体の定義に含まれる。

【００７７】

[0085]さらに、本明細書で説明した方法および技法を実行するためのモジュールおよび／または他の適切な手段は、適用可能な場合にユーザ端末および／または基地局によってダウンロードされ、および／または他の方法で取得され得ることを諒解されたい。たとえば、そのようなデバイスは、本明細書で説明した方法を実行するための手段の転送を可能にするためにサーバに結合され得る。代替的に、本明細書で説明した様々な方法は、ユーザ端末および／または基地局が記憶手段をデバイスに結合するかまたは与えると様々な方法を得ることができるように、記憶手段（たとえば、ＲＡＭ、ＲＯＭ、コンパクトディスク（ＣＤ）またはフロッピーディスクなどの物理記憶媒体など）によって提供され得る。さらに、本明細書で説明した方法および技法をデバイスに提供するための任意の他の好適な技法が利用され得る。

【００７８】

[0086]特許請求の範囲は、上記で示した厳密な構成および構成要素に限定されないことを理解されたい。上記で説明した方法および装置の構成、動作および詳細において、特許請求の範囲から逸脱することなく、様々な改変、変更および変形が行われ得る。

【００７９】

[0087]上記は本開示の態様を対象とするが、本開示の他の態様およびさらなる態様は、それの基本的範囲から逸脱することなく考案され得、それの範囲は以下の特許請求の範囲によって決定される。

【図１】

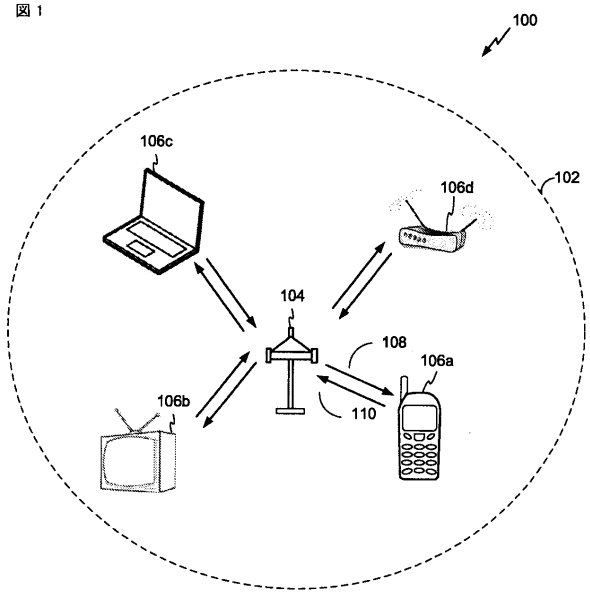

FIG. 1

【図２】

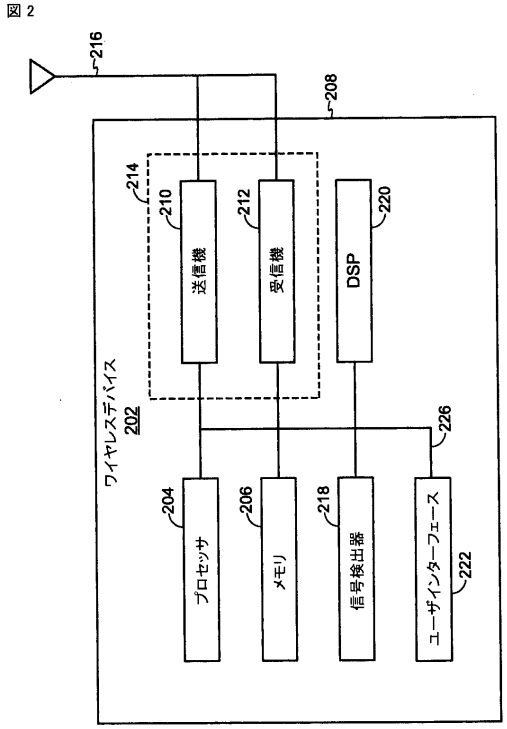

FIG. 2

【図３】

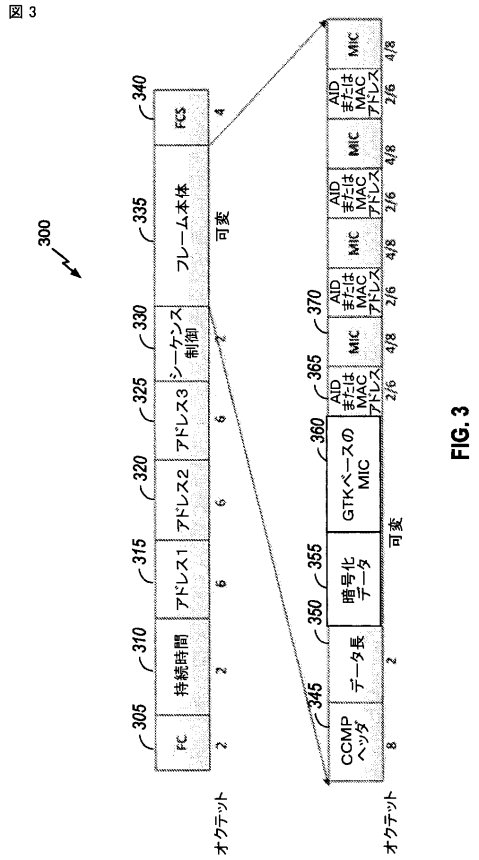

FIG. 3

【図４】

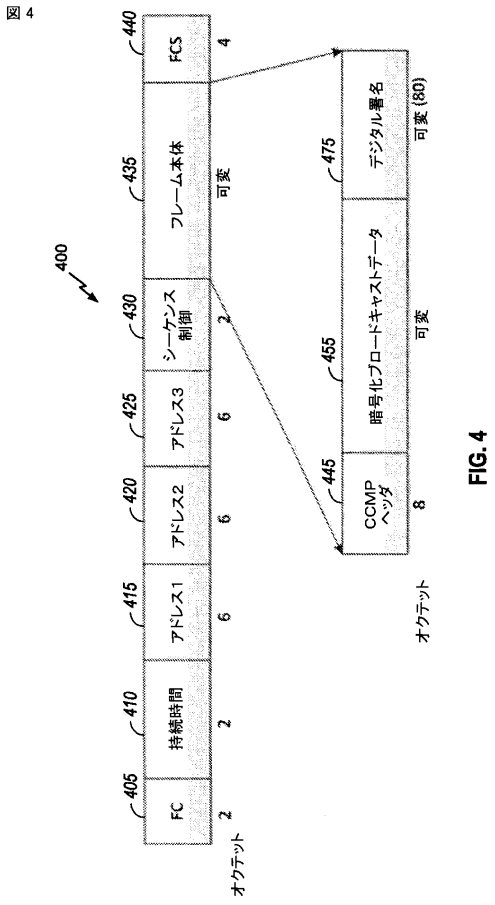

FIG. 4

【図５Ａ】

図 5A

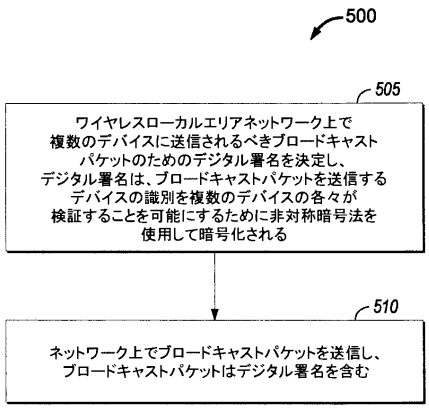

FIG. 5A

【図５Ｂ】

図 5B

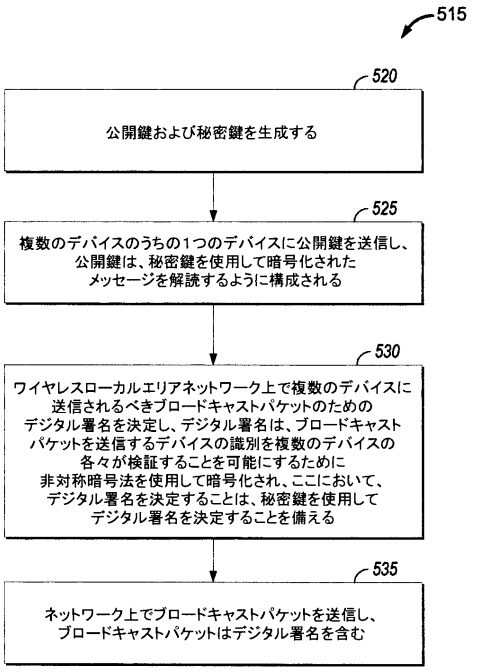

FIG. 5B

【図６】

図 6

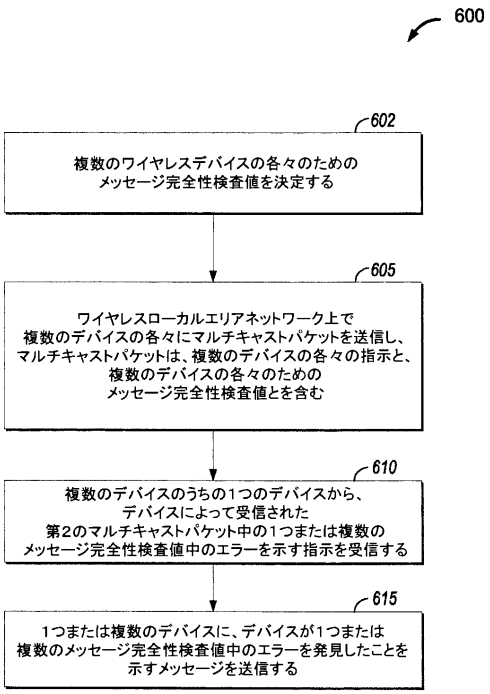

FIG. 6

【図７】

図 7

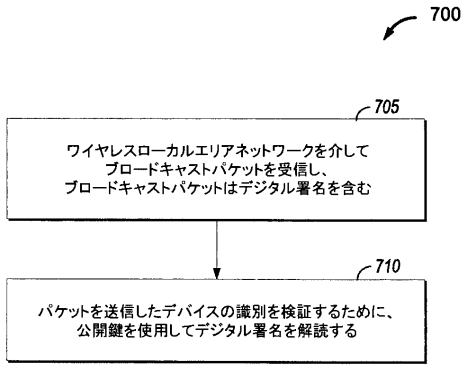

FIG. 7

【図８】

図８

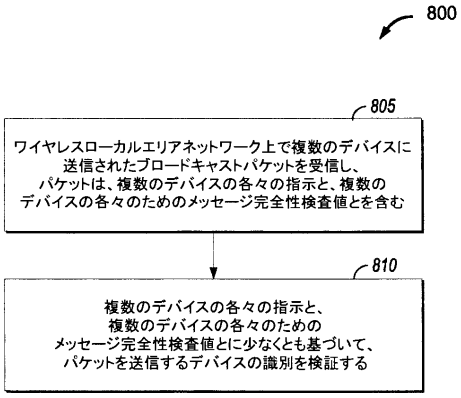
800
805
ワイヤレスローカルエリアネットワーク上で複数のデバイスに
送信されたブロードキャストパケットを受信し、
パケットは、複数のデバイスの各々の指示と、複数の
デバイスの各々のためのメッセージ完全性検査値とを含む
810
複数のデバイスの各々の指示と、
複数のデバイスの各々のための
メッセージ完全性検査値とに少なくとも基づいて、
パケットを送信するデバイスの識別を検証する

FIG. 8

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/039301

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/32
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

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/129236 A1 (SHARMA ATUL [US]) 16 June 2005 (2005-06-16) abstract paragraphs [0013] - [0031] ----- -/--	1-30

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 August 2014	03/09/2014

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

1

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/039301

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CHRISTOPHER SZILAGYI ET AL: "Flexible multicast authentication for time-triggered embedded control network applications", DEPENDABLE SYSTEMS&NETWORKS, 2009. DSN '09. IEEE/IFIP INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 29 June 2009 (2009-06-29), pages 165-174, XP031533174, ISBN: 978-1-4244-4422-9 abstract Section 3, "Multicast authentication with respect to embedded constraints", and section 3.1, "One MAC per receiver"; page 166, right-hand column - page 167, left-hand column	1,11,21, 26

A	PANG L ET AL: "Improved multicast key management of Chinese wireless local area network security standard", IET COMMUNICATIONS, THE INSTITUTION OF ENGINEERING AND TECHNOLOGY, MICHAEL FARADAY HOUSE, SIX HILLS WAY, STEVENAGE, HERTS. SG1 2AY, UK, vol. 6, no. 9, 14 June 2012 (2012-06-14), pages 1126-1130, XP006042786, ISSN: 1751-8628, DOI: 10.1049/IET-COM.2010.0954 the whole document	1-30

1

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2014/039301

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005129236 A1	16-06-2005	US 2005129236 A1	16-06-2005
		WO 2005062522 A1	07-07-2005

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,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,LT,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 アブラハム、サントシュ・ポール
アメリカ合衆国、カリフォルニア州 ９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 チェリアン、ジョージ
アメリカ合衆国、カリフォルニア州 ９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 マリネン、ヨウニ
アメリカ合衆国、カリフォルニア州 ９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ ５７７５

Ｆターム(参考) 5J104 AA08 AA16 AA32 EA04 EA19 GA03 JA21 LA03 NA02 NA37
NA38 PA07
5K067 AA30 EE02 EE10 EE22 HH22 HH24