(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5392102号
(P5392102)

(45)発行日　平成26年1月22日(2014.1.22)　(24)登録日　平成25年10月25日(2013.10.25)

(51)Int.Cl.		F I		
H04W 28/06	(2009.01)	H04W	28/06	110
H04W 12/08	(2009.01)	H04W	12/08	
H04L 12/951	(2013.01)	H04L	12/951	
H04L 12/22	(2006.01)	H04L	12/22	

請求項の数 8　(全 20 頁)

(21)出願番号　特願2010-4228(P2010-4228)
(22)出願日　平成22年1月12日(2010.1.12)
(65)公開番号　特開2010-166564(P2010-166564A)
(43)公開日　平成22年7月29日(2010.7.29)
審査請求日　平成24年9月10日(2012.9.10)
(31)優先権主張番号　12/352,887
(32)優先日　平成21年1月13日(2009.1.13)
(33)優先権主張国　米国(US)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100146776
弁理士　山口　昭則
(72)発明者　ウエイ－ポン　チェヌ
アメリカ合衆国，カリフォルニア州　９５０５０－６２５２，サンタ・クララ，サラトガ・アヴェニュ　４４４番，３７シー号
(72)発明者　奥田　將人
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】無線ネットワークにおいてオーバヘッドを低減する装置及び方法

(57)【特許請求の範囲】
【請求項１】
全てが少なくとも１つの共通のセキュリティ情報の断片を有するべき複数のパケットを特定する段階であり、該複数のパケットの各々はそれ自身のヘッダを有する、段階；
前記複数のパケットを単一の巨大パケットへと連結する段階；
前記複数のパケットに対応する複数のヘッダの中から基本ヘッダを選択する段階；
少なくとも１つのハミング距離を決定する段階であり、各ハミング距離が、前記複数のヘッダのうちの前記基本ヘッダ以外のそれぞれ１つのヘッダに関連付けられ、且つ該それぞれ１つのヘッダと前記複数のヘッダのうちの別の１つヘッダとの間のハミング距離に相当する、段階；
少なくとも１つの符号化された値を決定する段階であり、各符号化された値が、前記複数のヘッダのうちの前記基本ヘッダ以外のそれぞれ１つのヘッダに関連付けられ、且つ該それぞれの１つのヘッダと前記複数のヘッダのうちの少なくとも１つのその他のヘッダとの間の差に基づいて決定される、段階；
前記巨大パケットに付加する巨大ヘッダを生成する段階であり、該巨大ヘッダは、前記基本ヘッダと、前記少なくとも１つのハミング距離と、前記少なくとも１つの符号化された値とを有する、段階；及び
前記少なくとも１つの共通のセキュリティ情報の断片に基づく単一組のセキュリティ情報を、前記巨大パケットに付加する段階；
を有するオーバヘッドを低減する方法。

【請求項２】
前記少なくとも１つの共通のセキュリティ情報の断片は、共通のメッセージ認証コードを有する、請求項１に記載の方法。
【請求項３】
前記少なくとも１つの共通のセキュリティ情報の断片は、暗号化、解読及び認証からなる群から選択されたセキュリティ機能を提供するよう動作する鍵を有する、請求項１に記載の方法。
【請求項４】
前記複数のパケットを単一の巨大パケットへと連結する段階は、単一のＰＨＹバーストにて送信される複数のパケットを単一の巨大パケットへと連結することを有し；且つ
当該方法は更に、前記巨大パケットに付加された前記少なくとも１つの共通のセキュリティ情報の断片に基づいて前記複数のパケットを復元するよう動作する受信器に、無線接続を介して、前記巨大パケットを伝送する段階を有する；
請求項１に記載の方法。
【請求項５】
巨大ヘッダと、連結された複数のパケットと、を有する巨大パケットを受信する段階；
前記巨大ヘッダ内で、基本ヘッダと少なくとも１つのハミング距離及び少なくとも１つの符号化された値とを特定する段階であり、前記基本ヘッダは前記複数のパケットのうちの１つのパケットに関連付けられ、前記少なくとも１つのハミング距離の各々及び前記少なくとも１つの符号化された値の各々は、前記複数のパケットのうちの前記基本ヘッダに関連付けられたパケット以外のそれぞれ１つのパケットに関連付けられている、段階；
前記基本ヘッダと少なくとも１つのハミング距離及び少なくとも１つの符号化された値とに基づいて、前記複数のパケットに対応する複数のヘッダを復元する段階；
前記巨大パケットに付加された少なくとも１つのセキュリティ情報の断片を特定する段階であり、特定されたセキュリティ情報の断片を前記連結された複数のパケットは有していない、特定する段階；及び
前記巨大パケットに付加された前記少なくとも１つのセキュリティ情報の断片に基づいて、前記巨大パケット内の前記複数のパケットを復元する段階；
を有するオーバヘッドを低減する方法。
【請求項６】
前記少なくとも１つのセキュリティ情報の断片を特定する段階は、前記巨大パケットのヘッダ内の前記セキュリティ情報を特定することを有する、請求項５に記載の方法。
【請求項７】
全てが少なくとも１つの共通のセキュリティ情報の断片を有するべき複数のパケットを特定し、ただし、該複数のパケットの各々はそれ自身のヘッダを有し；
前記複数のパケットを単一の巨大パケットへと連結し；
前記複数のパケットに対応する複数のヘッダの中から基本ヘッダを選択し；
少なくとも１つのハミング距離を決定し、ただし、各ハミング距離は、前記複数のヘッダのうちの前記基本ヘッダ以外のそれぞれ１つのヘッダに関連付けられ、且つ該それぞれ１つのヘッダと前記複数のヘッダのうちの別の１つヘッダとの間のハミング距離に相当し；
少なくとも１つの符号化された値を決定し、ただし、各符号化された値は、前記複数のヘッダのうちの前記基本ヘッダ以外のそれぞれ１つのヘッダに関連付けられ、且つ該それぞれの１つのヘッダと前記複数のヘッダのうちの少なくとも１つのその他のヘッダとの間の差に基づいて決定され；
前記巨大パケットに付加する巨大ヘッダを生成し、ただし、該巨大ヘッダは、前記基本ヘッダと、前記少なくとも１つのハミング距離と、前記少なくとも１つの符号化された値とを有し；且つ
前記少なくとも１つの共通のセキュリティ情報の断片に基づく単一組のセキュリティ情報を、前記巨大パケットに付加する；

よう動作するプロセッサを有する、オーバヘッドを低減する装置。
【請求項８】
巨大ヘッダと、連結された複数のパケットと、を有する巨大パケットを受信するよう動作するインタフェース；及び
前記インタフェースに結合されたプロセッサであり：
前記巨大ヘッダ内で、基本ヘッダと少なくとも１つのハミング距離及び少なくとも１つの符号化された値とを特定し、ただし、前記基本ヘッダは前記複数のパケットのうちの１つのパケットに関連付けられ、前記少なくとも１つのハミング距離の各々及び前記少なくとも１つの符号化された値の各々は、前記複数のパケットのうちの前記基本ヘッダに関連付けられたパケット以外のそれぞれ１つのパケットに関連付けられており；
前記基本ヘッダと少なくとも１つのハミング距離及び少なくとも１つの符号化された値とに基づいて、前記複数のパケットに対応する複数のヘッダを復元し；
前記巨大パケットに付加された、前記連結された複数のパケットは有していない少なくとも１つのセキュリティ情報の断片を特定し；且つ
前記巨大パケットに付加された前記少なくとも１つのセキュリティ情報の断片に基づいて、前記巨大パケット内の前記複数のパケットを復元する；
よう動作するプロセッサ；
を有するオーバヘッドを低減する装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、概して無線ネットワークに関し、より具体的には無線ネットワークにおいてオーバヘッドを低減する装置及び方法に関する。
【背景技術】
【０００２】
如何なる無線システムにおいても、無線周波数スペクトルは無線オペレータにとって貴重な資源であり且つ十分でない資源である。従って、無線オペレータには常にスペクトルの効率的な使用が望まれる。特に、スペクトル効率を達成する上で、メディア・アクセス・コントロール（ＭＡＣ）オーバヘッド効率が鍵となる。無線システムにおけるＭＡＣオーバヘッドは、パケットヘッダ、制御パケット及び管理パケット、セキュリティ・コンテクスト、メッセージ認証コード等を含む。ＭＡＣオーバヘッドを可能な限り低減することにより、ＭＡＣ効率を有意に向上させ、ひいては、無線資源を節約することができる。
【発明の概要】
【発明が解決しようとする課題】
【０００３】
本発明は、無線ネットワークにおいてオーバヘッドを低減する装置及び方法を提供することを目的とする。
【課題を解決するための手段】
【０００４】
特定の一実施形態に従って、オーバヘッドを低減する方法は、全てが少なくとも１つの共通のセキュリティ情報の断片を有する複数のパケットを特定する段階を含む。当該方法はまた、前記複数のパケットを単一の巨大パケットへと連結する段階を含む。当該方法は更に、巨大パケットに単一組のセキュリティ情報を付加する段階を含む。この単一組のセキュリティ情報は、前記少なくとも１つの共通のセキュリティ情報の断片に基づく。
【発明の効果】
【０００５】
特定の実施形態の利点は、無線ネットワークが一層効率的にパケットを通信することを可能にすることを含み得る。従って、連結された複数のパケットを有する巨大パケットは、相異なるパケットのために同一のセキュリティ情報が用いられる回数を減少させることによって、パケットのオーバヘッドを低減し得る。このサイズの削減は、パケットの安全

性への悪影響を殆ど、あるいは全く伴わずに達成され得る。
【０００６】
その他の技術的利点が、以下の説明、図面及び特許請求の範囲から当業者に容易に明らかになる。また、具体的な利点を列挙したが、様々な実施形態は、列挙した利点のうち、全て又は一部を含むこともあるし、それらの何れをも含まないこともある。
【図面の簡単な説明】
【０００７】
具体的な実施形態及びその利点のより完全な理解のため、添付の図面とともに以下の説明を参照する。
【図１】特定の実施形態に従った、様々な通信ネットワークを有する通信システムを例示する図である。
【図２】エンドポイント及び基地局をより詳細に示す、特定の実施形態に従った無線ネットワークを例示する図である。
【図３】特定の実施形態に従った、元のパケットより少ないオーバヘッドを有する単一の巨大パケットへの、複数のパケットの連結を例示する図である。
【図４】特定の実施形態に従った、無線ネットワークにおいてオーバヘッドを低減する方法を例示する図である。
【発明を実施するための形態】
【０００８】
図１は、特定の実施形態に従った、様々な通信ネットワークを有する通信システムを示している。通信システム１００は複数の相互接続されたネットワーク１１０を有し得る。各ネットワーク１１０は、その他のネットワークから独立して、あるいはそれらと協働して、の何れかで１つ以上の異なるサービスを容易にするように設計された多様な通信ネットワークのうちの何れかとし得る。例えば、ネットワーク１１０は、インターネットアクセス、オンラインゲーム、ファイル共有、ピアツーピア・ファイル共有（Ｐ２Ｐ）、インターネット回線を利用した音声通信（Voice over Internet protocol；ＶｏＩＰ）電話、インターネット回線を利用した映像通信（video over IP）電話、又は一般的にネットワークにより提供されるその他の種類の機能を容易にし得る。ネットワーク１１０は、それらそれぞれのサービスを、有線通信又は無線通信の何れか用の多様なプロトコルの何れかを用いて提供し得る。例えば、ネットワーク１１０ａは、ＷｉＭＡＸとして広く知られた、基地局１２０等の基地局と中継局１３０等の中継局とを含み得るＩＥＥＥ８０２．１６無線ネットワーク（例えば、８０２．１６ｊ又は８０２．１６ｍ）を有していてもよい。ネットワーク１１０ａは、８０２．１６ｊを実装することによって、中継局１３０の使用を提供し得る。中継局を使用するＷｉＭＡＸネットワークは、モバイル・マルチホップ中継（ＭＭＲ）ネットワークと呼ばれることもある。
【０００９】
無線プロトコル（例えば、８０２．１６ｍ）を使用する例えばネットワーク１１０ａ等のネットワーク内では、構成要素間の通信はパケットを用いて行われ得る。これらのパケットは、通信されるべきデータに加えて、ＭＡＣオーバヘッドを含み得る。オーバヘッドは、そのパケットに関する情報（例えば、発信元、宛先、ペイロードのサイズ等）及びセキュリティ情報（例えば、メッセージ認証コード、セキュリティ・コンテクスト等）を含むヘッダを含み得る。この情報は、実際に所望されるデータ又は情報の伝達には直接的に寄与しないにもかかわらず各パケットに含められるので、かなりのオーバヘッドを生じさせ得る。この情報はオーバヘッドを生じさせるが、インテグリティの保護及び潜在的なセキュリティ攻撃及び盗聴からの暗号化をパケットに提供するために必要とされ得る。特定の実施形態において、オーバヘッドは、２つ以上のパケットを単一の巨大パケットへと連結した上で、ヘッダを圧縮し且つ／或いは連結されたパケットに使用されていたセキュリティ情報の量を低減することによって縮減され得る。
【００１０】
パケット（及び巨大パケット）は、無線ネットワーク１１０ａの複数の構成要素間で、

無線リンクを介して通信され得る。より具体的には、エンドポイント、中継局及び／又は基地局の各々間に、例えば無線接続１５０等の無線接続又はリンクが存在し得る。無線接続１５０の各々は、例えば、特定の中心周波数、特定の帯域幅、特定のタイムスロット、及び／又は特定の副チャネルの組み合わせ（例えば、ダウンリンクマップ又はアップリンクマップ内に記述される）等、それ自身の様々な無線資源を有し得る。特定の無線接続１５０の実際の特性は、使用される通信規格（例えば、ＷｉＭＡＸ）に依存し得る。

【００１１】

無線ネットワーク１１０ａにおいて、ＭＡＣオーバヘッドは、パケットヘッダ、制御パケットや管理パケット、セキュリティ情報などを含み得る。単純化のため、セキュリティ情報という用語は、パケットのペイロードを保護（例えば、認証）するために用いられ得る１以上の機構の総括的な用語として用いられる。例えば、８０２．１６システムにおいて、データパケットの暗号文メッセージ認証コード（ＣＭＡＣ）の値、又はＭＡＣ管理メッセージのＣＭＡＣタプル／ＣＭＡＣダイジェストは、セキュリティ情報と見なされ得る。セキュリティ情報の他の一例はＩＰＳｅｃにおける認証ヘッダである。

【００１２】

通信システム１００は、ネットワーク１１０ａ－１１０ｄという４つの異なるネットワークを含んでいるが、用語“ネットワーク”は、ウェブページ、電子メール、文字チャット、ＶｏＩＰ及びインスタントメッセージによって伝送される信号、データ又はメッセージを含めて、信号、データ及び／又はメッセージを伝送可能な何らかのネットワーク又は複数のネットワークの組み合わせを全般的に規定するものと解釈されるべきである。ネットワークの範囲、サイズ及び／又は構成に応じて、ネットワーク１１０ａ－１１０ｄの各々は、ＬＡＮ、ＷＡＮ、ＭＡＮ、ＰＳＴＮ、ＷｉＭＡＸネットワーク、例えばインターネット等の地球規模で分布されたネットワーク、イントラネット、エクストラネット、又はその他の形態の無線若しくは有線のネットワークとして実現され得る。説明及び単純化のため、ネットワーク１１０ａは、少なくとも部分的にＷｉＭＡＸによって実現され得るＭＡＮであり、ネットワーク１１０ｂはＰＳＴＮであり、ネットワーク１１０ｃはＬＡＮであり、ネットワーク１１０ｄはＷＡＮであるとする。

【００１３】

図示した実施形態において、ネットワーク１１０ａ、１１０ｃ及び１１０ｄはＩＰネットワークとし得る。ＩＰネットワークは、データをパケット内に配置し、各パケットを個別に、１つ以上の通信パスに沿って、選択された宛先に送信することによってデータを伝送する。ネットワーク１１０ｂは、例えば、交換局、中央局、移動式電話の交換局、ポケットベルの交換局、遠隔端末、及び世界中に配置されたその他の関連電信設備を含み得るＰＳＴＮである。ネットワーク１１０ｄは、ゲートウェイを介してネットワーク１１０ｂに結合され得る。実施形態に応じて、ゲートウェイはネットワーク１１０ｂ又は１１０ｄの一部であってもよい（例えば、ノード１７０ｅ又は１７０ｃがゲートウェイを有していてもよい）。ゲートウェイは、ＰＳＴＮ１１０ｂが例えばネットワーク１１０ａ、１１０ｃ及び１１０ｄ等の非ＰＳＴＮネットワークと通信することを可能にし得る。

【００１４】

ネットワーク１１０は、相互に、そしてその他のネットワークに、複数の有線リンク１６０、無線接続１５０及びノード１７０を介して接続され得る。有線リンク１６０、無線接続１５０及びノード１７０は、様々なネットワークを接続するだけでなく、エンドポイント１４０を、相互に、そしてネットワーク１１０の何れかに結合されるかその一部であるその他の構成要素に相互接続する。ネットワーク１１０ａ－１１０ｄの相互接続は、エンドポイント１４０がデータを通信したり相互間での信号伝達を制御したりすることを可能にし、且つ、介在する要素又は装置がデータを通信したり信号を制御したりすることを可能にする。従って、エンドポイント１４０のユーザは、ネットワーク１１０ａ－１１０ｄのうちの１つ以上に結合された各ネットワーク要素との間で、データの送受信を行ったり信号を制御したりすることが可能にされ得る。

【００１５】

ノード群１７０は、ネットワーク要素、セッションボーダーコントローラ、ゲートキーパー、基地局、カンファレンス・ブリッジ、ルータ、ハブ、スイッチ、ゲートウェイ、エンドポイント、又は、通信システム１００内でパケット交換を可能にする任意数の通信プロトコルを実装したその他のハードウェア、ソフトウェア若しくは埋込ロジック、の如何なる組み合わせを含んでいてもよい。例えば、ノード１７０ｅはゲートウェイを有していてもよい。ノードウェイ１７０ｅは、ゲートウェイとして、異なる複数のネットワークによって使用される様々なプロトコルの間で通信を翻訳し得る。

【００１６】

エンドポイント１４０及び／又はノード１７０は、ハードウェア、コンピュータ読み取り可能媒体に埋め込まれたソフトウェア、及び／又は、ハードウェアに組み込まれた、あるいはその他の方法で格納された符号化ロジック（例えば、ファームウェア）の何らかの組み合わせによって、ユーザにデータ又はネットワークサービスを提供し得る。例えば、エンドポイント１４０ａ－１４０ｄは、セル方式電話、ＩＰ電話、コンピュータ、ビデオモニタ、カメラ、携帯情報端末、又は、ネットワーク１１０を用いてパケット（又は、フレーム）の通信を支援するその他のハードウェア、埋込ソフトウェア及び／又は符号化ロジックを含み得る。エンドポイント１４０はまた、データ及び／又は信号を送信あるいは受信可能な、無人システム若しくは自動化システム、ゲートウェイ、その他の中間要素、又はその他の装置を含んでいてもよい。

【００１７】

図１は特定の数及び構成のエンドポイント、接続、リンク及びノードを示しているが、通信システム１００は、如何なる数又は構成の、データを通信するための構成要素をも意図するものである。また、通信システム１００の要素は、互いに対して中央に位置する（ローカルな）構成要素や、通信システム１００全体に分散された構成要素を含んでいてもよい。

【００１８】

図２は、特定の一実施形態に従った無線ネットワークを例示しており、エンドポイント及び基地局をより詳細に示している。図示した実施形態は、ＩＰネットワーク２０５、基地局２１０及びエンドポイント２７０を有する簡略化したネットワークである。様々な実施形態において、ネットワーク２００は、如何なる数の、有線又は無線ネットワーク、基地局、エンドポイント、及び／又は、有線又は無線の何れの接続であろうとデータや信号の通信を容易にする、あるいはそれに関与するその他の構成要素（例えば、中継局）、を有していてもよい。

【００１９】

図示した実施形態において、基地局２１０は、プロセッサ２１２、メモリ２１４、インタフェース２１６、無線機２１７及びアンテナ２１８を有している。同様に、エンドポイント２７０は、プロセッサ２７２、メモリモジュール２７４、無線機２７７及びアンテナ２７８を有している。これらの構成要素は、協働して、例えば伝統的な無線ネットワークより少ないオーバヘッドを用いてパケットを通信する等、無線ネットワーク機能を提供する。

【００２０】

ネットワーク２００の様々な構成要素をより詳細に見るに、ＩＰネットワーク２０５は、図１に関連して上述したネットワーク１１０のうちの１つ以上を有し得る。例えば、ＩＰネットワーク２０５は、インターネット、ＬＡＮ、ＷＡＮ、ＭＡＮ、ＰＳＴＮ、又はこれらの組み合わせを有し得る。

【００２１】

便宜上、基地局２１０及びエンドポイント２７０の同様の構成要素は、必要に応じて、併せて説明する。プロセッサ２１２及び２７２は、マイクロプロセッサ、コントローラ、又はその他の好適な計算装置やリソース、又は、無線ネットワークに関する機能を単独あるいはその他の要素（例えば、メモリ２１４及び／又は２７４）とともに提供するように動作可能なハードウェア、埋込ソフトウェア及び／又は符号化ロジックの組み合わせとし

得る。この機能は、ここで説明するような様々な無線機能を提供することを含む。例えば、プロセッサ２１２及び２７２は、何れのパケットを連結すべきか、及びヘッダをどのように圧縮してセキュリティ情報の量を削減するかを決定することが可能であり得る。少なくとも部分的にプロセッサ２１２、２５２及び２７２によって提供される更なる例及び機能については後述する。

【００２２】

メモリモジュール２１４及び２７４は、以下に限定されないが、磁気媒体、光媒体、ランダムアクセスメモリ（ＲＡＭ）、読み出し専用メモリ（ＲＯＭ）、フラッシュメモリ、取り外し可能媒体、又はその他の好適な局所あるいは遠隔メモリ部品を含む、如何なる形態の揮発性メモリ又は不揮発性メモリであってもよい。メモリモジュール２１４及び２７４は、それぞれ、基地局２１０及びエンドポイント２７０によって使用される好適なデータ又は情報を格納し得る。このような好適なデータ又は情報は、コンピュータ読み取り可能媒体に埋め込まれたソフトウェア、及び／又はハードウェアに組み込まれた、あるいはその他の方法で格納された符号化ロジック（例えば、ファームウェア）を含み得る。例えば、特定の実施形態において、メモリモジュール２１４及び２７４は、基地局２１０とエンドポイント２７０との間で通信されるパケットのセキュリティとして使用される暗号に関する情報を格納し得る。メモリモジュール２１４及び２７４はまた、データを適切な構成要素にどのように経路付けるかを決定することに有用なリスト、データベース又はその他のデータ編成を管理してもよい。

【００２３】

無線機２１７及び２７７は、それぞれ、アンテナ２１８及び２７８に結合され、あるいはその一部とされ得る。無線機２１７及び２７７は、その他の基地局、中継局及び／又はエンドポイントに無線接続を介して送出されるデジタルデータを受信し得る。無線機２１７及び２７７はデジタルデータを、適切な中心周波数及び帯域幅パラメータを有する無線信号へと変換し得る。これらのパラメータは、例えば基地局２１０のプロセッサ２１２とメモリ２１４との組み合わせによって、前もって決定されていてもよい。そして、無線信号はアンテナ２１８及び２７８によって適切な受信者に送信され得る。同様に、無線機２１７及び２７７は、それぞれアンテナ２１８及び２７８によって受信された無線信号を、必要に応じてプロセッサ２１２又は２７２によって処理されるデジタルデータへと変換し得る。無線機２１７及びアンテナ２１８は一緒になって無線インタフェースを形成し、無線機２７７及びアンテナ２７８も一緒になって無線インタフェースを形成する。

【００２４】

基地局２１０はまた、基地局２１０とネットワーク２０５との間での信号及び／又はデータの有線通信に使用され得るインタフェース２１６を有している。例えば、インタフェース２１６は、基地局２１０が有線接続上でネットワーク２０５とデータの送受信を行うことを可能にするために必要とされ得る書式設定又は翻訳を実行し得る。図示していないが、エンドポイント２７０も有線インタフェースを含んでいてもよい。

【００２５】

エンドポイント２７０は、基地局２１０との間でデータ及び／又は信号の送受信を行うことが可能な如何なる種類の無線エンドポイントであってもよい。エンドポイント２７０が取り得る種類は、デスクトップコンピュータ、ＰＤＡ、セル方式電話、ノート型コンピュータ、及び／又はＶｏＩＰ電話を含み得る。

【００２６】

それとなく上述したように、基地局２１０及びエンドポイント２７０の構成要素は、ネットワーク２００内のオーバヘッドの量を低減する働きをする。より具体的には、基地局２１０及びエンドポイント２７０は、２つ以上の連結されたパケット、圧縮されたヘッダ及び／又は削減されたセキュリティ情報を含む巨大パケットを用いて通信し得る。巨大パケットの使用は、オーバヘッドの量を、複数の個別の非連結パケットを用いる場合と比較して低減し得る。

【００２７】

基地局２１０とエンドポイント２７０との間での通信はパケットによって伝送されると仮定し得る。当初、各パケットは１つのＭＡＣヘッダを含み得る。さらに、パケットがセキュリティ情報を含む（例えば、パケットがセキュリティアルゴリズムを用いて保護される）ことが望ましいことがある。各パケットを用いてヘッダ及びセキュリティ情報を含めることは、パケットがセキュリティトンネルを通して発信される、あるいは単一のリンク上で発信される場合であっても行われ得る。便宜上、基地局２１０は送信器であり且つエンドポイント２７０は受信器であると仮定する。実際には、如何なるエンドポイント、基地局又は中継局（図示せず）も、場合によって、送信器又は受信器となり得る。従って、巨大パケットの生成、符号化、暗号化、送信、受信、解読及び復号化に関して、後述の機能及び／又は構成要素は、如何なる基地局、中継局又はエンドポイントにも適用され得る。パケットの伝送に伴うオーバヘッドの量は、プロセッサ２１２が、無線機２１７及びアンテナ２１８による一組の連結パケットの送信前に、ヘッダ圧縮を適用し且つ該一組の連結パケットでセキュリティ情報を共有することによって低減され得る。

【００２８】

状況に応じて、巨大パケットは、例えば、単一のリンク上で同一の構成要素に複数のパケットを伝送するために使用され得る。他の一例として、巨大パケットは１つ以上のリンクに跨る安全なトンネルを介して伝送されてもよい。状況に依らず、プロセッサ２１２は２つ以上のパケットを連結し、そして、ヘッダ圧縮を実行し、且つ／或いはセキュリティ情報の量を削減し得る。より具体的には、ヘッダ圧縮に関し、各パケットは自身の完全なヘッダで開始し得る。そして、プロセッサ２１２は、連結された複数のパケットのヘッダ内で冗長性を探索し、それを排除し得る。セキュリティ情報の削減に関し、連結パケットのうちの、同一又は類似のセキュリティ情報を有するが別々に送られたであろう複数のパケットは、巨大パケットからの同一のセキュリティ情報を共有し得る。これらの低減技術の双方については、より詳細に後述する。

【００２９】

巨大パケットの受信者がコンテンツを解読できるようにするためには、連結パケット内で情報がどのように編成されているかを知る必要がある。従って、プロセッサ２１２が何らかのヘッダ圧縮法を適用する、あるいは巨大パケットからの何らかのセキュリティ情報を共有する前に、基地局２１０及びエンドポイント２７０（例えば、送信器及び受信器）は、情報を交換し、圧縮アルゴリズムの設定及び詳細について合意する。これは、様々な種類の圧縮アルゴリズムや除外の規則などの中から選択することを含み得る。８０２．１６の状況において、この情報は動的サービス追加要求／応答（ＤＳＡ－ＲＥＱ／ＲＳＰ）メッセージ交換におけるタイプ－レングス－バリュー（ＴＬＶ）の様式で通信され得る。一部の例においては、圧縮設定を変更するために、動的サービス変更要求／応答（ＤＳＣ－ＲＥＱ／ＲＳＰ）メッセージ交換が用いられてもよい。

【００３０】

ヘッダ圧縮及びセキュリティ情報削減の双方の使用は、図３にて見て取ることができる。より具体的には、パケット３１０は、エンドポイント２７０に送信される複数のパケットを表し得る。パケット３１０は単一のパケット３２０へと連結される。次に、巨大パケット３３０内に示されるように、ヘッダ圧縮が適用されて、複数のパケットのヘッダ内の冗長性が排除され得る。そして、連結される全てのパケット（単独で送信される場合のパケット）に唯一の組のセキュリティ情報（例えば、図３に示すようなＣＭＡＣ値）が適用されるように、何らかの暗号化、認証、又は個々のパケットに適用され得るその他のセキュリティ手段が巨大パケット３４０に適用され得る。

【００３１】

特定の実施形態は、単一パケット３２０内の連結される各パケット用に、元のヘッダの組によって使用されていたビットより少ないビットを用いる新たな組のヘッダを生成してもよい。特定の実施形態において、これは、１つのヘッダを基本ヘッダとして用い、残りのヘッダを基本ヘッダ又は先行ヘッダに対するそれぞれの差によって符号化することによって達成され得る。例えば、第１のヘッダを基本ヘッダとし、第２のヘッダを、第１のヘ

ッダと第２のヘッダとの間の差を有する差分ヘッダ（例えば、δｈｄｒ２）で表し、第３のヘッダを、第３のヘッダと第２のヘッダとの間、又は第３のヘッダと第１のヘッダとの間の差を有するそれ自身の差分ヘッダ（例えば、δｈｄｒ３）で表し得る。

【００３２】

特定の実施形態において、２つのヘッダ間の差は、プロセッサ２１２がそれら２つのヘッダのビット列（ストリング）の各ビットに対して‘排他的論理和’（ＸＯＲ、“○”で囲まれた“＋”）演算を用いることによって決定され得る。この演算を用いて、２つのビットが同一である都度‘０’を有し且つ２つのビットが異なる都度‘１’を有する新たなビット列が作り出され得る。便宜上、ＸＯＲ演算の結果列を差分ヘッダと呼んでもよい。２つの２進列の間の異なるビット（例えば、‘１’を生じさせるビット）の数はハミング距離と呼ばれることがある。

【００３３】

２つの元のヘッダの間の既知のハミング距離をそれぞれのヘッダの長さ（例えば、ヘッダ当たりのビット数）とともに用いて、取り得る差分ヘッダの数を決定することができる。より具体的には、ヘッダ１（Ｈｄｒ１）とヘッダ２（Ｈｄｒ２）との間のハミング距離が‘ｍ’に等しく、且つ２つのヘッダの各々が‘ｎ’ビットを有する場合、Ｈｄｒ２の‘ｎ’ビットのうちの‘ｍ’個がＨｄｒ１のそれと異なることが決定される。さらに、何れの‘ｍ’ビットが異なるかを選択するためのＣ（ｎ；ｍ）の組み合わせが存在することが決定される。そして、Ｈｄｒ１が基本ヘッダとして使用される場合、Ｈｄｒ２にはＣ（ｎ；ｍ）個の可能性あるものが存在する。Ｈｄｒ１とＨｄｒ２との間の差は、ｋ＝ceil（ｌｏｇ２Ｃ（ｎ；ｍ））として、ｋビットを用いて符号化され得る。ただし、‘ceil’は、或る実数をそれより大きい側の次の整数にマッピングする天井関数である。

【００３４】

これは例を見ることによって最もよく理解され得る。２つの元のヘッダＨｄｒ１及びＨｄｒ２が各々４ビットの長さを有し、Ｈｄｒ１＝（１，０，０，０）且つＨｄｒ２＝（１，０，１，１）であると仮定する。δｈｄｒ２と表記されるこれら２つのヘッダ間の差である差分ヘッダ２は、Ｈｄｒ１及びＨｄｒ２の最初の２つのビットが同一であり且つ次の２つのビットが異なるので、δｈｄｒ２＝（０，０，１，１）となる。δｈｄｒ２から、プロセッサ２１２は、２つの異なるビットが存在するので、ハミング距離は２であると決定することができる。Ｈｄｒ２の４ビットのうちの２つがＨｄｒ１と異なるので、δｈｄｒ２のビットには、６個の可能性ある配列（０：（０，０，１，１）、１：（０，１，０，１）、２：（１，０，０，１）、３：（０，１，１，０）、４：（１，０，１，０）、５：（１，１，０，０））が存在する。プロセッサ２１２は、これらの６個の可能性あるものを３つのビットを用いて符号化することができる。故に、この例ではδｈｄｒ２＝（０，０，１，１）であるので、プロセッサ２１２は第１の選択肢（０）を用い、δｈｄｒ２の符号化された値は‘０００’となる。そして、Ｈｄｒ１、ハミング距離２、及び符号化された値‘０００’は、Ｈｄｒ２を再構成するためにプロセッサ２７２によって使用され得る。

【００３５】

先の例はＨｄｒ２を圧縮するために（Ｈｄｒ２の元の４ビットより多い）５ビット（ハミング距離の値のための２ビット及びδｈｄｒ２の符号化のための３ビット）を用いる結果となったが、より長い長さを有するヘッダは圧縮によって、より大きな恩恵を受け得る。例えば、ヘッダのビット列の長さが４０に等しく、且つハミング距離の値が８であるとき、δｈｄｒ２の可能性ある組み合わせを符号化するための２７ビット及びハミング距離の値を表すための６ビットが必要とされるのみである。故に、Ｈｄｒ２は４０ビットから３３（２７＋６）ビットに圧縮され得る。特定の実施形態において、プロセッサ２１２は、ヘッダを圧縮することが、圧縮を実際に実行する前に必要なビット数を実際に減少させるかを決定してもよい。

【００３６】

上述のように、圧縮の一部は差分ヘッダ（例えば、δｈｄｒ２）を、複数の可能性ある

組み合わせのうちの１つを用いて符号化することに頼るものである。一部の実施形態において、全ての可能性ある組み合わせがネットワークの各構成要素のメモリ（例えば、メモリ２１４及びメモリ２７４）に格納されてもよい。特定の実施形態において、プロセッサ２１２が差分ヘッダを符号化することと、プロセッサ２７２が差分ヘッダを復号化することとの双方を可能にするために或るアルゴリズムが用いられる。

【００３７】

符号化アルゴリズムは、差分ヘッダと２つの元のヘッダのハミング距離とを用いて符号化を決定し得る。特定の実施形態において、差分ヘッダ内のビットは、０から開始する最下位ビット（ＬＳＢ）から、ｎ－１で終了する最上位ビット（ＭＳＢ）まで番号を付けられ得る。特定の実施形態において、符号化アルゴリズムは２項係数に関する公式：Ｃ（ｎ；ｍ）＝Ｃ（ｎ－１；ｍ－１）＋Ｃ（ｎ－１；ｍ）を用いてもよい。換言すれば、左辺は、‘ｎ’ビットのうちの‘ｍ’ビットが‘１’であるような可能性ある組み合わせの総数を表す。右辺は、第１のビットが‘１’に等しい組み合わせの数を表す第１項と、第１のビットが‘０’に等しい組み合わせの数である第２項との２つの部分的な状況を含んでいる。特定の実施形態において、この符号化は、‘ｍ’個の下位ビット（ＬＳＢ）が‘１’に等しい差分ヘッダを‘０’として符号化することによって開始する。そして、‘１’の最上位ビットが左端に到達するまで左に移動され、左への移動の各々によって１だけ符号値が増大される。その後、ＭＳＢの２つがそれらの元の位置（全て右側にある）から左に移動される。この処理は、‘ｍ’個全てのＭＳＢが‘１’に等しくなる（例えば、全ての‘１’が左側になる）まで繰り返し続けられる。ｎ＝５且つｍ＝３の場合を表１に示す。

【００３８】

【表１】

差分ﾍｯﾀﾞ	ﾋﾞｯﾄ4	ﾋﾞｯﾄ3	ﾋﾞｯﾄ2	ﾋﾞｯﾄ1	ﾋﾞｯﾄ0	符号値
00111	0	0	0	0	0	0
01011	0	0	C(5-3;3-3)	0	0	1
10011	0	C(5-4;3-3)	C(5-3;3-3)	0	0	2
01101	0	0	0	C(5-2;3-2)	0	3
10101	0	C(5-4;3-3)	0	C(5-2;3-2)	0	4
11001	0	0	C(5-3;3-2)	C(5-2;3-2)	0	5
01110	0	0	0	0	C(5-1;3-1)	6
10110	0	C(5-4;3-3)	0	0	C(5-1;3-1)	7
11010	0	0	C(5-3;3-2)	0	C(5-1;3-1)	8
11100	0	0	0	C(5-2;3-1)	C(5-1;3-1)	9

最も左の欄は差分ヘッダであり、最も右の欄は符号値である。

【００３９】

ビット０－４の各欄の値は、符号値全体の部分に寄与する値である。１ビットの寄与後の値を決定するための符号化原理は：

・符号値の計算をＬＳＢ（すなわち、最も右のビット）から開始する。

【００４０】

・‘１’に等しいビットの値に０を割り当てる。

【００４１】

・ｉ番目のＬＳＢビットの値が０に等しいとき、該ビットに値Ｃ（ｎ－ｉ－１；ｍ－

ｃ－１）を割り当てる。ただし、ｃは、最も右のビットからｉ番目のＬＳＢまで数えた、‘１’に等しい値を有する累積ビット数である。

【００４２】

例えば、差分列‘１００１１’の場合、ビット２の値はＣ（５－２－１；３－２－１）であり、これは‘１’に等しい。ビット３の値はＣ（５－３－１；３－２－１）であり、これは‘１’に等しい。故に、符号値はこれら２つの値の和であり、これは２に等しい。

【００４３】

特定の実施形態において、プロセッサ２１２はｗｈｉｌｅループを用いて差分ヘッダを符号化し得る。例えば、以下のｗｈｉｌｅループによって符号値（ｖａｌ）が出力され得る：

```
1.    c＝0，val＝0，i＝0；
2.    while（c＜m）{
3.       if（d［i］＝＝1）  c＋＋；
4.       else  val＋＝C（n－i－1；m－c－1）；
5.       i＋＋；}
6.    return  val；
```

ただし、ｄ［ｉ］は、‘ｎ’ビットを有し且つ‘ｍ’のハミング距離を有する差分列（２つのヘッダのＸＯＲ演算によって決定される）のｉ番目のビットである。

【００４４】

同様に、エンドポイント２７０がビット列の長さ（ｎ）、ハミング距離（ｍ）及び符号値（ｖａｌ）を受信するとき、プロセッサ２７２は以下のループを用いて元の差分列を決定することが可能である：

```
1.    c＝0，i＝0；
2.    while（val＞0）{
3.       if（val≦C（n－i－1；m－c－1））{
4.          d［i］＝1；  c＋＋；}
5.       else  {
6.          d［i］＝0；  val－＝C（n－i－1；m－c－1）；}
7.       i＋＋；}
8.    while（c≦m）{
9.        d［i］＝1；  c＋＋；  i＋＋；}
10.   for（j＝i；j＜n；j＋＋）    d［j］＝0；
11.   return  d；
```

差分ヘッダの符号値を復号化した後、エンドポイント２７０は、基本ヘッダ及び差分ヘッダにＸＯＲ演算を適用することによって、ヘッダを容易に解凍することができる。

【００４５】

２つのヘッダを圧縮するのに用いられたのと同じ技術は、複数のヘッダにも適用され得る。より具体的には、複数のヘッダのうちの１つが基本ヘッダとして選択され、次のヘッダがこの第２のヘッダと基本ヘッダとの間の差に基づいて符号化され得る。そして、後続のヘッダは、最初の基本ヘッダ、又はその他の先行ヘッダのうちの１つの何れかとの差に基づき得る。

【００４６】

ヘッダを圧縮するとき、可能な限り少ないビットを使用して差分ヘッダを符号化することが望ましい。従って、複数の差分ビット列を符号化するための最短のスパニング（spanning）パス（例えば、最短のハミルトン経路）又は最小のスパニングツリーを発見することが望ましい。よって、最短経路又は最小スパニングツリーを提供する多様な異なる技術及び／又は方策のうちの何れかを用いて、複数のヘッダの中から基本ヘッダを選択してもよい。例えば、シングルパス法、スタートポロジー法又はツリートポロジー法などの技術が用いられ得る。

【００４７】

シングルパス法は、各ヘッダ（最初の基本ヘッダの後）をその直前のヘッダに基づいて符号化して、複数のヘッダを圧縮することを含む。この手法を用いるとき、全てのヘッダにわたっての最短のハミルトン経路を見出すことが望ましい。解を近似する１つの用い得る方法は、スパニングパスを見出すものである。最初のヘッダが基本ヘッダと見なされ、Ｈｄｒ１と表記される。受信器が全てのヘッダを解読し得るよう、送信器は符号化シーケンス内に、ｘ、ＨＤ２、ＨＤ３、・・・、ＨＤｘ、Ｈｄｒ１、Ｅｎ２、Ｅｎ３、・・・、Ｅｎｘ（ｘはヘッダの数、ＨＤｘはＨｄｒｘのハミング距離であり、Ｅｎｘは、ＨｄｒｘとＨｄｒｘ－１とのＸＯＲ演算結果をδｈｄｒｘとして、δｈｄｒｘの符号値である）なる情報を含めることができる。エンドポイント２７０は、この符号化シーケンスを受信すると、基本ヘッダ、Ｈｄｒ１から始めて、全てのヘッダを順に解凍し得る。ヘッダは完全な状態に復元され得る。最終的に、エンドポイント２７０は、先ずＨｄｒｘ－１を再構成した後にＥｎｘを復号化し、Ｈｄｒｘ－１とＨｄｒｘとの間の差であるδｈｄｒｘを取得し、最後に、Ｈｄｒｘが得られるようにＨｄｒｘ－１とδｈｄｒｘとのＸＯＲ演算を行うことで、Ｈｄｒｘを解凍することができる。

【００４８】

スタートポロジー法においては、プロセッサ２１２は単一の基本ヘッダを見出し、残りのヘッダは共通の基本ヘッダに基づいて符号化される。従って、基本ヘッダからその他全てのヘッダへのハミング距離の合計が最小となるように基本ヘッダを見出すことが望ましい。Ｈｄｒ１と表記されるスタートポロジーに適切な基本ヘッダを見出した後、基地局２１０は、ｘ、ＨＤ２、ＨＤ３、・・・、ＨＤｘ、Ｈｄｒ１、Ｅｎ２、Ｅｎ３、・・・、Ｅｎｘなる情報をエンドポイント２７０に伝達し得る。ヘッダは、受信されると、プロセッサ２７２によって全て共通のヘッダＨｄｒ１から再構成される。例えば、Ｈｄｒｘは、先ず符号値Ｅｎｘからδｈｄｒｘを復号化することによって再構成され得る。そして、Ｈｄｒｘのビット列は、Ｈｄｒ１とδｈｄｒｘとのＸＯＲ演算を行うことによって復元されることが可能である。ツリートポロジー法においては、プロセッサ２１２は最小のスパニングツリーを見出す。そのとき、親ヘッダがその直接の子ヘッダ用の基準として用いられる。最小のスパニングツリーを見出すことの計算時間はプリム（Prim）のアルゴリズムによって決定され得る。ツリーのパターンは、例えば深さ優先探索（depth first search；ＤＦＳ）又は広さ優先探索（breadth first search；ＢＦＳ）等の多様な既知の技術のうちの何れを用いて表されてもよい。ツリーを表すために使用される技術にかかわらず、ツリー構造のシンボル表現を、受信器に容易に伝達され得るように、２進表現に変換することが望ましい。換言すれば、ツリー構造に関する階層変化又はその他の情報を指し示すために使用されるシンボルは、エンドポイント２７０への通信のために２進法で表される必要があり得る。ツリー構造が一旦表されると、基地局２１０は、ｘ、ツリーを表すもの、各ヘッダのその親に対するハミング距離、その他全てのヘッダが由来するルートヘッダ、各子孫ヘッダとその親ヘッダとの間の差の符号値なる情報をエンドポイント２７０に伝達し得る。

【００４９】

実施形態に応じて、ヘッダの圧縮には更なる制約が課されてもよい。例えば、ヘッダ内の特定のビットは圧縮から除外されてもよい。例えば、８０２．１６ｅの状況において、“ｈｅａｄｅｒ　ｃｈｅｃｋｓｕｍ”のフィールドは圧縮から除外され得る。この状況において、８０２．１６ｅの一般的なＭＡＣヘッダ内の最後の８ビットは、符号化された差分表現の中で完全なままに維持され得る。更なる制約の他の一例として、連結パケットのヘッダは、一組の規則に基づいて複数のグループに分割されてもよい。その規則は、異なる種類のヘッダが単一の巨大パケットへと連結されるときの圧縮効率を増大させるように実装される。例えば、８０２．１６ｅの状況において、ＨＴ＝０（ペイロードを伴うヘッダ）の場合とＨＴ＝１（ペイロードを伴わない信号伝達ヘッダ）の場合とで２つのグループに分離されてもよい。更なる他の１つの制約は、圧縮比が一定の閾値より高くなることを手順前に要求することである。

【００５０】

一部の実施形態において、プロセッサ２１２は、ヘッダを圧縮することに加え、連結される複数のパケット間の、暗号及びインテグリティ保護を含むセキュリティ情報を共有してもよい。これは、巨大パケットが圧縮されたヘッダを含むか否かにかかわらずに行われ得る。プロセッサ２１２は、他の方法ではパケットごとに一組のセキュリティ情報を必要とするであろう巨大パケット内の複数のパケットを保護するために一組のセキュリティ情報を用いることによって、セキュリティ情報に関連するオーバヘッドを低減し得る。より具体的には、例えば全てがそれぞれのパケットのコンテンツを暗号化／解読／認証するために共通のセキュリティ鍵を使用する複数のパケットが連結される場合、同一のセキュリティ鍵が巨大パケットに適用され得る。単一の鍵のみを用いることにより、処理要求の有意な増大又はパケット若しくはそのペイロードの安全性の低下を伴うことなく、複数組のセキュリティ情報から単一組のセキュリティ情報へとパケットのオーバヘッドが低減される。

【００５１】

巨大パケットにおいてセキュリティ情報が共有され、あるいは削減され得る少なくとも２つの事例が存在する。第１の事例は、一般的な通信システム内での単一ホップにて生じる。より具体的には、互いの単一ホップ内で２つの局間で通信されるパケットは、全てではないにしても、多くの同一のセキュリティ情報を使用し得る。故に、基地局２１０は、エンドポイント２７０に向けて送信されるパケットを連結し、その巨大パケットに同一の鍵を適用し、唯一の組のセキュリティ情報を用いて巨大パケットの全ての連結パケットを保護し得る。第２の事例は、マルチホップ中継システムにおけるセキュリティトンネルの使用（例えば、セキュリティトンネルは１つ以上の中継局を通り得る）に伴って生じる。セキュリティトンネルの２つの末端局において、該トンネルを通る全てのパケットを暗号化／解読するために同一の鍵が使用され得る。故に、マルチホップシステムにおいてセキュリティトンネルを介して送られる巨大パケットの複数のパケットの間でその鍵を共有し得る。

【００５２】

実施形態又は状況に応じて、パケットのセキュリティ情報は、暗号化されたデータパケット用の認証データであってもよいし、平文で示された制御パケット用の認証データであってもよい。例えば、８０２．１６の状況において、ＡＥＳ－ＣＣＭ（Advanced Encryption Standard－Combined Cipher Machine；ただし、ＣＣＭはＣＢＣ－ＭＡＣを用いたＣＴＲモードを表し、ＣＴＲはカウンターモード暗号化を表し、ＣＢＣは暗号ブロック連鎖を表し、ＭＡＣはメッセージ認証コードを表す）モードにおけるデータパケットのセキュリティ情報は、ＣＭＡＣ値とすることができ、制御パケットのセキュリティ情報はＣＭＡＣダイジェスト又はＣＭＡＣタプルとすることができる。前者のケースにおいて、巨大パケットのペイロード全体を認証するために同一のＣＭＡＣ値が用いられ得る（例えば、８０２．１６ｊにおける中継ＭＡＣ　ＰＤＵ）。後者のケースにおいては、巨大パケット内に連結された全てのＭＡＣ管理メッセージに対して、全てのＭＡＣ管理メッセージを認証するために同一のＣＭＡＣタプルが適用され得る。

【００５３】

巨大パケット内に連結された全てのパケットに単一組のセキュリティ情報を用いることにより、安全性に有意に影響を及ぼすことなく、パケットを通信することに伴う全体的なオーバヘッドが低減される。より具体的には、各巨大パケットは一組のセキュリティ情報を携さえるだけでよい。このセキュリティ情報は巨大パケット、ひいては、その中のパケットを保護し得る。従って、巨大パケット内のパケットの安全性が目に見えて損なわれることなく、オーバヘッドが有意に低減される。

【００５４】

特定の実施形態において、長い連結パケットの例えば無線リンク上での伝送の堅牢性を強化するために、自動再送要求（ＡＲＱ）処理を適用することが望ましいことがある。故に、データの一部のブロックが喪失されたとき、受信器は否定応答（ＮＡＣＫ）を送信者に返送し得るようにされてもよい。送信者は連結パケット内の全てのブロックを再送信す

ることなく、喪失ブロックを送信し得る。同様に、特定の実施形態において、無線リンク上での伝送の物理ＰＨＹレイヤでの堅牢性を強化するために、複合型（ハイブリッド）ＡＲＱ（ＨＡＲＱ）が含められてもよい。

【００５５】

これまで、幾つかの異なる実施形態及び特徴を提示してきた。特定の実施形態は、これらの特徴の１つ以上を、動作上の必要性及び／又は要素の制約に応じて組み合わせ得る。これは、様々な組織及びユーザのニーズに対するネットワーク２００の多大な適応性を可能にし得る。例えば、特定の一実施形態は、大都市圏への無線アクセスを提供するために複数の基地局を使用してもよいし、必要な受信地域を提供するために単一の基地局が複数の中継局とともに用いられてもよい。また、一部の実施形態において、基地局２１０は、より多くの、あるいは、より少ない無線機を有していてもよい。一部の実施形態は更なる、あるいは異なる特徴を含んでいてもよい。

【００５６】

図４は、特定の実施形態に従ったオーバヘッドの低減方法を示している。図４に示す状況を単純化するため、エンドポイントが基地局に複数のパケットを送信すると仮定する（基地局から送信されるパケットにも同じステップ群が適用される）。当該方法はステップ４２０で開始し、全てが少なくとも１つの共通のセキュリティ情報の断片（ピース）を有する複数のパケットが特定される。特定の実施形態において、これは、仮に各パケットが個別に送信されるとした場合に各パケットに添付されるセキュリティの関連性又はセキュリティ情報を検査することを有する。共通のセキュリティ情報は、例えば、暗号化、解読及び／又は認証セキュリティをそれぞれのパケットに提供する鍵を含み得る。

【００５７】

ステップ４３０にて、エンドポイントは、共通のセキュリティ情報を有するとして特定された複数のパケットを、巨大パケットへと連結する。この時、共通のセキュリティ情報は、巨大パケット又は連結パケットの何れにも含められない。状況に応じて、これら複数のパケットは、共通の宛先アドレスを共有していてもよいし、単一のＰＨＹバーストにて送信されるように意図されたパケットであってもよい。パケットは、状況に応じて、データパケット、制御パケット、又は制御パケットとデータパケットとの組み合わせを有し得る。

【００５８】

そしてステップ４４０にて、パケットの安全性を維持するため、共通のセキュリティ情報の少なくとも１つのピースに基づく単一組のセキュリティ情報が、巨大パケットに付加される。換言すれば、連結された複数のパケットの全てを保護するために、巨大パケット用の単一のセキュリティ情報が用いられる。

【００５９】

ステップ４５０にて、巨大パケットが受信者の基地局に無線接続を介して伝送される。そしてステップ４６０にて、巨大パケットは基地局によって受信される。特定の実施形態において、巨大パケットは８０２．１６無線接続を介して伝送され得る。一部の実施形態において、巨大パケットは単一バーストとして伝送され得る。

【００６０】

ステップ４７０にて、巨大パケット内でセキュリティ情報が特定される。より具体的には、巨大パケットに付加されたセキュリティ情報が基地局によって特定される。そしてステップ４８０にて、基地局は、巨大パケットから特定したセキュリティ情報に基づいて、上記複数のパケットを復元することができる。より具体的には、基地局は、巨大パケット内に含まれるパケットの解読や正当性の検証等を行い得る。故に、連結された複数のパケットが当初、共通のセキュリティ情報を有していなかったにしても、それらは依然として、巨大パケットに付加されたセキュリティ情報によって同一レベルの安全性で保護される。従って、パケットを伝送することや、それらのセキュリティ情報に関連するオーバヘッドが、パケットの実際の安全性を有意に犠牲にすることなく低減される。

【００６１】

図４に示したステップ群の一部は、必要に応じて、組み合わされ、変更され、あるいは削除されてもよく、また、更なるステップがこのフローチャートに追加されてもよい。例えば、一部の実施形態において、連結されたパケットに付随するヘッダが圧縮されてもよい。さらに、ステップ群は、特定の実施形態の範囲を逸脱することなく、好適な如何なる順序で実行されてもよい。例えば、特定の実施形態において、パケットは、それに既に付加されたセキュリティ情報を有していてもよい。従って、当該方法は、連結されるパケットの各々から共通のセキュリティ情報を除去することと、単一の共通のセキュリティ情報を巨大パケットに付加することとを含んでもよい。

【００６２】

特定の実施形態を詳細に説明してきたが、特定の実施形態の主旨及び範囲を逸脱することなく、それに様々なその他の変形、代用及び改変が為され得ることは理解されるべきである。例えば、動作上の要求又は要望に従って、例えば図２等の特定の図に関して説明した特徴及び機能が、例えば図１等の別の図に関して説明した特徴及び機能とともに用いられてもよい。また、如何なる要素も、必要に応じて通信システム１００に、ネットワーク２００に、あるいは相互に通信を行うために、別個の外部要素、一体化された内部要素、又はそれらの組み合わせとして実現され得る。特定の実施形態はこれらの要素及びそれらの内部要素の構成において多大な柔軟性を意図するものである。

【００６３】

数多のその他の変形、代用、変更、改変及び改良が当業者によって解明され得るが、本発明は、添付の請求項の主旨及び範囲に含まれるそのような全ての変形、代用、変更、改変及び改良を包含するものである。

【００６４】

以上の説明に関し、更に以下の付記を開示する。

【００６５】

（付記１）　全てが少なくとも１つの共通のセキュリティ情報の断片を有する複数のパケットを特定する段階；

前記複数のパケットを単一の巨大パケットへと連結する段階；及び

前記少なくとも１つの共通のセキュリティ情報の断片に基づく単一組のセキュリティ情報を、前記巨大パケットに付加する段階；

を有するオーバヘッドを低減する方法。

【００６６】

（付記２）　前記少なくとも１つの共通のセキュリティ情報の断片は、共通のメッセージ認証コードを有する、付記１に記載の方法。

【００６７】

（付記３）　前記少なくとも１つの共通のセキュリティ情報の断片は、暗号化、解読及び認証からなる群から選択されたセキュリティ機能を提供するよう動作する鍵を有する、付記１に記載の方法。

【００６８】

（付記４）　前記巨大パケットへと連結される前記複数のパケットは、複数のデータパケットを有し；且つ

前記少なくとも１つの共通のセキュリティ情報の断片は、前記データパケットの認証データを有する；

付記１に記載の方法。

【００６９】

（付記５）　前記巨大パケットへと連結される前記複数のパケットは、複数の制御パケットを有し；且つ

前記少なくとも１つの共通のセキュリティ情報の断片は、前記制御パケットの認証データを有する；

付記１に記載の方法。

【００７０】

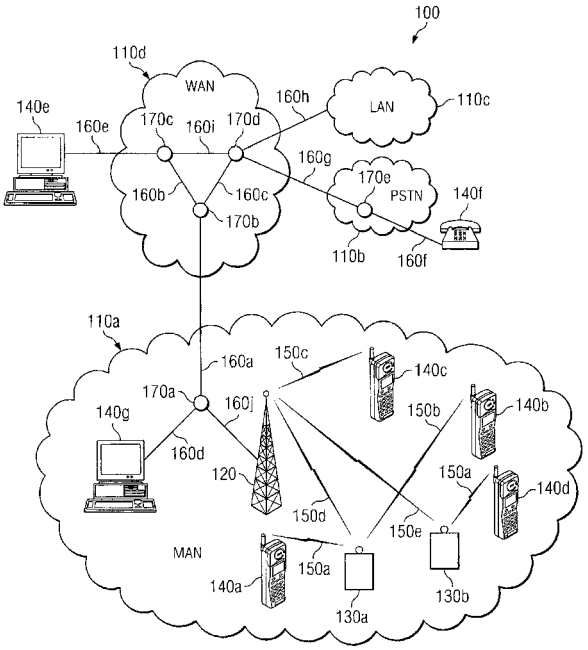
（付記６）　前記複数のパケットを単一の巨大パケットへと連結する段階は、単一のＰＨＹバーストにて送信される複数のパケットを単一の巨大パケットへと連結することを有し；且つ
当該方法は更に、前記巨大パケットに付加された前記少なくとも１つの共通のセキュリティ情報の断片に基づいて前記複数のパケットを復元するよう動作する受信器に、無線接続を介して、前記巨大パケットを伝送する段階を有する；
付記１に記載の方法。
【００７１】
（付記７）　前記複数のパケットの各々はそれ自身のヘッダを有し；且つ
当該方法は更に、前記複数のヘッダのうちの１つ以上を、それぞれのヘッダと前記複数のヘッダのうちの少なくとも１つのその他のヘッダとの間の少なくとも１つの差に基づいて符号化する段階を有する；
付記１に記載の方法。
【００７２】
（付記８）　連結された複数のパケットを有する巨大パケットを受信する段階；
前記巨大パケットに付加された少なくとも１つのセキュリティ情報の断片を特定する段階であり、特定されたセキュリティ情報の断片を前記連結された複数のパケットは有していない、特定する段階；及び
前記巨大パケットに付加された前記少なくとも１つのセキュリティ情報の断片に基づいて、前記巨大パケット内の前記複数のパケットを復元する段階；
を有するオーバヘッドを低減する方法。
【００７３】
（付記９）　前記少なくとも１つのセキュリティ情報の断片を特定する段階は、前記巨大パケットのヘッダ内の前記セキュリティ情報を特定することを有する、付記８に記載の方法。
【００７４】
（付記１０）　前記巨大パケットへと連結された前記複数のパケットは、複数のデータパケットを有し；且つ
前記少なくとも１つのセキュリティ情報の断片は、前記データパケットの認証データを有する；
付記８に記載の方法。
【００７５】
（付記１１）　前記巨大パケットへと連結された前記複数のパケットは、複数の制御パケットを有し；且つ
前記少なくとも１つのセキュリティ情報の断片は、前記制御パケットの認証データを有する；
付記８に記載の方法。
【００７６】
（付記１２）　前記巨大パケットは、基本ヘッダと、２つのヘッダ間の差を表す１つ以上の差分ヘッダとを有し；且つ
当該方法は更に、各々が前記複数のパケットのうちのそれぞれのパケットに関連する複数のヘッダを、前記基本ヘッダと１つ以上の前記差分ヘッダとにより復号化する段階を有する；
付記８に記載の方法。
【００７７】
（付記１３）　全てが少なくとも１つの共通のセキュリティ情報の断片を有する複数のパケットを特定し；
前記複数のパケットを単一の巨大パケットへと連結し；且つ
前記少なくとも１つの共通のセキュリティ情報の断片に基づく単一組のセキュリティ情報を、前記巨大パケットに付加する；

よう動作するプロセッサを有する、オーバヘッドを低減する装置。
【００７８】
（付記１４） 前記少なくとも１つの共通のセキュリティ情報の断片は、共通のメッセージ認証コードを有する、付記１３に記載の装置。
【００７９】
（付記１５） 前記少なくとも１つの共通のセキュリティ情報の断片は、暗号化、解読及び認証からなる群から選択されたセキュリティ機能を提供するよう動作する鍵を有する、付記１３に記載の装置。
【００８０】
（付記１６） 前記巨大パケットへと連結される前記複数のパケットは、複数のデータパケットを有し；且つ
前記少なくとも１つの共通のセキュリティ情報の断片は、前記データパケットの認証データを有する；
付記１３に記載の装置。
【００８１】
（付記１７） 前記巨大パケットへと連結される前記複数のパケットは、複数の制御パケットを有し；且つ
前記少なくとも１つの共通のセキュリティ情報の断片は、前記制御パケットの認証データを有する；
付記１３に記載の装置。
【００８２】
（付記１８） 前記複数のパケットを単一の巨大パケットへと連結するよう動作する前記プロセッサは、単一のＰＨＹバーストにて送信される複数のパケットを単一の巨大パケットへと連結するよう動作するプロセッサを有し；且つ
当該装置は更に、前記プロセッサに結合されたインタフェースを有し、該インタフェースは、前記巨大パケットに付加された前記少なくとも１つの共通のセキュリティ情報の断片に基づいて前記複数のパケットを復元するよう動作する受信器に、無線接続を介して、前記巨大パケットを送信するよう動作する；
付記１３に記載の装置。
【００８３】
（付記１９） 前記複数のパケットの各々はそれ自身のヘッダを有し；且つ
前記プロセッサは更に、前記複数のヘッダのうちの１つ以上を、それぞれのヘッダと前記複数のヘッダのうちの少なくとも１つのその他のヘッダとの間の少なくとも１つの差に基づいて符号化するよう動作する；
付記１３に記載の装置。
【００８４】
（付記２０） 連結された複数のパケットを有する巨大パケットを受信するよう動作するインタフェース；及び
前記インタフェースに結合されたプロセッサであり：
前記巨大パケットに付加された、前記連結された複数のパケットは有していない少なくとも１つのセキュリティ情報の断片を特定し；且つ
前記巨大パケットに付加された前記少なくとも１つのセキュリティ情報の断片に基づいて、前記巨大パケット内の前記複数のパケットを復元する；
よう動作するプロセッサ；
を有するオーバヘッドを低減する装置。
【００８５】
（付記２１） 前記少なくとも１つのセキュリティ情報の断片を特定するよう動作する前記プロセッサは、前記巨大パケットのヘッダ内の前記セキュリティ情報を特定するよう動作するプロセッサを有する、付記２０に記載の装置。
【００８６】

（付記２２）　前記巨大パケットへと連結された前記複数のパケットは、複数のデータパケットを有し；且つ
前記少なくとも１つのセキュリティ情報の断片は、前記データパケットの認証データを有する；
付記２０に記載の装置。
【００８７】
（付記２３）　前記巨大パケットへと連結された前記複数のパケットは、複数の制御パケットを有し；且つ
前記少なくとも１つのセキュリティ情報の断片は、前記制御パケットの認証データを有する；
付記２０に記載の装置。
【００８８】
（付記２４）　前記巨大パケットは、基本ヘッダと、２つのヘッダ間の差を表す１つ以上の差分ヘッダとを有し；且つ
前記プロセッサは更に、各々が前記複数のパケットのうちのそれぞれのパケットに関連する複数のヘッダを、前記基本ヘッダと１つ以上の前記差分ヘッダとにより復号化するよう動作する；
付記２０に記載の装置。
【符号の説明】
【００８９】
１００　通信システム
１１０、２００　ネットワーク
１３０　中継局
１４０、２７０　エンドポイント
１５０、２９０　無線接続
１６０　有線リンク
１７０　ノード
２１２、２７２　プロセッサ
２１４、２７４　メモリ
２１６　インタフェース
２１７、２７７　無線機
２１８、２７８　アンテナ
３１０　パケット
３２０　単一パケット
３３０　巨大パケット

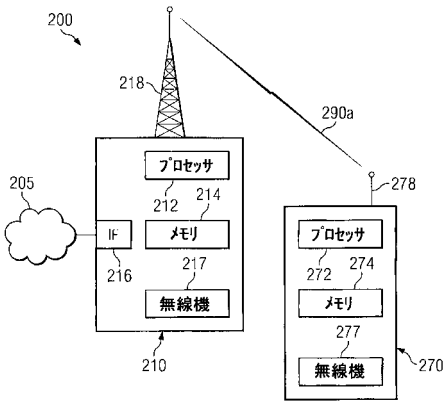
【図１】

特定の実施形態に従った、様々な通信ネットワークを有する通信システムを例示する図



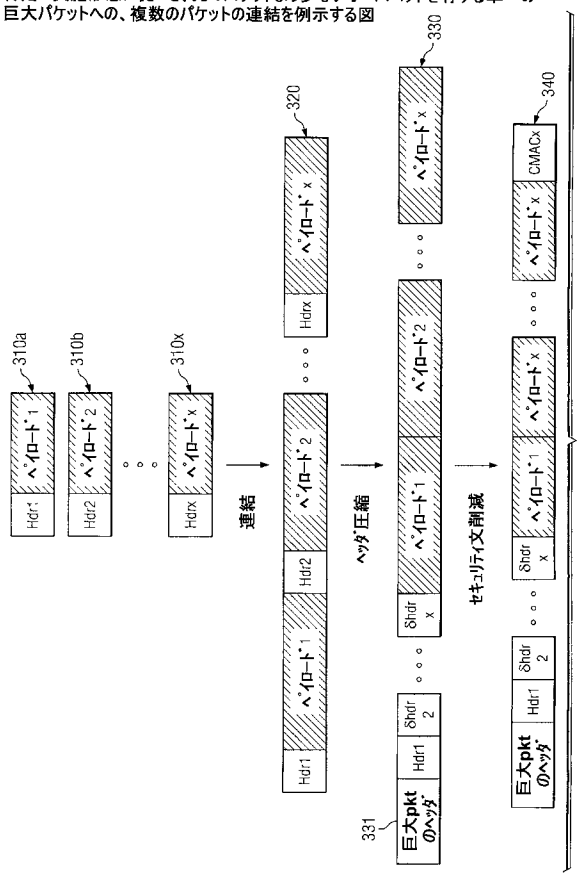
【図２】

エンドポイント及び基地局をより詳細に示す、特定の実施形態に従った無線ネットワークを例示する図



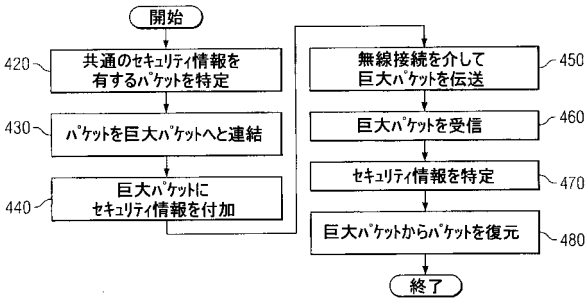
【図３】

特定の実施形態に従った、元のパケットより少ないオーバヘッドを有する単一の巨大パケットへの、複数のパケットの連結を例示する図



【図４】

特定の実施形態に従った、無線ネットワークにおいてオーバヘッドを低減する方法を例示する図



フロントページの続き

(72)発明者　ツェヌシィ　ジュ
アメリカ合衆国，メリーランド州　２０８７８－７３０４，ゲイザースバーグ，グレイスランド・ストリート　６番

審査官　齋藤　浩兵

(56)参考文献　特開２００５－３１１９２０（ＪＰ，Ａ）
国際公開第２００７／０８６９３４（WO，Ａ２）
特表２００４－５０５５０８（ＪＰ，Ａ）
特表２００９－５０４０２３（ＪＰ，Ａ）
特開２００４－３４３５６７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｗ　２８／０６
Ｈ０４Ｌ　１２／２２
Ｈ０４Ｌ　１２／９５１
Ｈ０４Ｗ　１２／０８