(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2017-11673
(P2017-11673A)
(43)公開日　平成29年1月12日(2017.1.12)

(51)Int.Cl.		F I			テーマコード（参考）
H04W 12/06	(2009.01)	H04W	12/06		5K067
H04W 4/04	(2009.01)	H04W	4/04	130	
H04W 92/12	(2009.01)	H04W	92/12		
G06F 21/44	(2013.01)	G06F	21/44		

審査請求 有　請求項の数 33　ＯＬ　外国語出願　（全 20 頁）

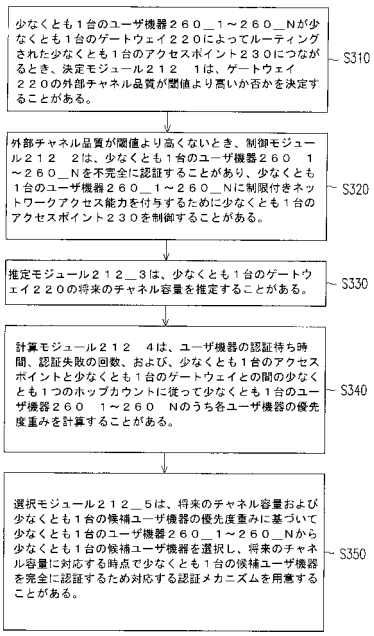
(21)出願番号　特願2015-257718 (P2015-257718)
(22)出願日　平成27年12月30日 (2015.12.30)
(31)優先権主張番号　104120333
(32)優先日　平成27年6月24日 (2015.6.24)
(33)優先権主張国　台湾 (TW)

(71)出願人　390023582
財團法人工業技術研究院
ＩＮＤＵＳＴＲＩＡＬ　ＴＥＣＨＮＯＬＯＧＹ　ＲＥＳＥＡＲＣＨ　ＩＮＳＴＩＴＵＴＥ
台湾新竹縣竹東鎮中興路四段１９５號
Ｎｏ．１９５，Ｓｅｃ．４，ＣｈｕｎｇＨｓｉｎｇＲｄ．，Ｃｈｕｔｕｎｇ，Ｈｓｉｎｃｈｕ，Ｔａｉｗａｎ　３１０４０
(71)出願人　598139748
國立交通大學
台湾新竹市大學路１００１號
(74)代理人　110000729
特許業務法人　ユニアス国際特許事務所

最終頁に続く

(54)【発明の名称】ユーザ機器をＰＯＳＴ認証する方法、コントローラおよびネットワークシステム

(57)【要約】　（修正有）
【課題】ユーザ機器（ＵＥ）をＰＯＳＴ認証する方法、コントローラおよびネットワークシステムを提供する。
【解決手段】ＵＥがゲートウェイによってルーティングされたアクセスポイント（ＡＰ）に接続されているとき、少なくとも１台のゲートウェイの外部チャネル品質が閾値より高いか否かを決定するＳ３１０。外部チャネル品質が閾値より高くないとき、ＵＥを不完全に認証し、ＵＥに付与するネットワーク能力を制限するようにＡＰを制御するＳ３２０。ゲートウェイの将来のチャネル能力を推定するＳ３３０。各ＵＥの優先度重みを計算するＳ３４０。将来のチャネル容量および各ＵＥの優先度重みに従ってＵＥ群から候補ＵＥを選択し、将来のチャネル容量に対応する時点で候補ＵＥを完全に認証するため認証機構を用意するＳ３５０。
【選択図】図３



【特許請求の範囲】
【請求項１】
少なくとも１台のゲートウェイに接続されたコントローラに適合している、少なくとも１台のユーザ機器をＰＯＳＴ認証する方法であって、
前記少なくとも１台のユーザ機器が少なくとも１台のアクセスポイントに接続され、前記少なくとも１台のゲートウェイの外部チャネル品質が閾値より高いか否かを決定することと；、
前記外部チャネル品質が前記閾値より高くない場合、前記少なくとも１台のユーザ機器を不完全に認証し、かつ前記少なくとも１台のユーザ機器に制限付きネットワークアクセス能力を付与するために前記少なくとも１台のアクセスポイントを制御することと；、
前記少なくとも１台のゲートウェイの将来のチャネル容量を推定することと；、
前記ユーザ機器の認証待ち時間、認証失敗の回数、および、前記少なくとも１台のアクセスポイントと前記少なくとも１台のゲートウェイとの間の少なくとも１つのホップカウントに従って前記少なくとも１台のユーザ機器のうち各ユーザ機器の優先度重みを計算することと；、
前記将来のチャネル容量および少なくとも１台の候補ユーザ機器の前記優先度重みに基づいて前記少なくとも１台のユーザ機器から前記少なくとも１台の候補ユーザ機器を選択し、かつ前記将来のチャネル容量に対応する時点で前記少なくとも１台の候補ユーザ機器を完全に認証するため対応する認証メカニズムを用意することと；、
を含む、方法。
【請求項２】
前記コントローラは、ソフトウェア定義型ネットワーキングコントローラであり、
前記コントローラ、前記少なくとも１台のアクセスポイントおよび前記少なくとも１台のゲートウェイは、複数台の車両および予測可能な走行経路を有する列車上に構成されている、請求項１に記載の少なくとも１台のユーザ機器をＰＯＳＴ認証する方法。
【請求項３】
前記少なくとも１台のゲートウェイの前記将来のチャネル容量を推定することは、
前記少なくとも１台のゲートウェイおよび車両個別履歴情報に基づいてチャネル品質推定モデルを確立することと；、
車両の現在の移動情報を取得し、前記現在の移動情報に基づいて前記車両の将来の移動情報を推定することと；、
前記将来の移動情報および前記チャネル品質推定モデルに従って前記少なくとも１台のゲートウェイの将来のチャネル品質を推定することと；、
前記将来のチャネル品質に従って前記少なくとも１台のゲートウェイの前記将来のチャネル容量を推定することと；、
をさらに含む、請求項１に記載の少なくとも１台のユーザ機器をＰＯＳＴ認証する方法。
【請求項４】
時点ｉでの前記将来のチャネル容量は、
Ｂが前記少なくとも１台のゲートウェイの周波数範囲であり、SNR_iが時点ｉでの信号対雑音比であるとして：
$C(i) = B \times \log_2(1 + SNR_i)$
である、請求項１に記載の少なくとも１台のユーザ機器をＰＯＳＴ認証する方法。
【請求項５】
前記少なくとも１台のユーザ機器のうちｎ番目のユーザ機器の前記優先度重みは、
w_1からw_3が重み値であり、ＷＴが前記ｎ番目のユーザ機器の認証待ち時間であり、ｈは、前記ｎ番目のユーザ機器のために働く前記少なくとも１台のアクセスポイントと前記少なくとも１台のゲートウェイとの間の少なくとも１つのホップカウントであり、ＦＴが前記ｎ番目のユーザ機器に対する認証失敗の回数であるとして：
$P(n) = w_1 \times WT + (1 - w_2^{\,h}) + (1 - w_3 \times FT)$

によって特徴付けられる、請求項１に記載の少なくとも１台のユーザ機器をＰＯＳＴ認証する方法。
【請求項６】
前記将来のチャネル容量および前記少なくとも１台の候補ユーザ機器の前記優先度重みに基づいて前記少なくとも１台のユーザ機器から前記少なくとも１台の候補ユーザ機器を選択することは、
前記各ユーザ機器の前記優先度重みに従って前記少なくとも１台のユーザ機器を降順にソートすることと；、
前記将来のチャネル容量および認証情報サイズに基づいて、前記認証情報サイズによって除算された前記将来のチャネル容量である特定の数を計算することと；、
前記少なくとも１台の候補ユーザ機器の前記特定の数として、より高い優先度重みを有する少なくとも１台のユーザ機器の前記特定の数を選択することと；、
をさらに含む、請求項１に記載の少なくとも１台のユーザ機器をＰＯＳＴ認証する方法。
【請求項７】
前記少なくとも１台のアクセスポイントは、不完全に認証された前記少なくとも１台のユーザ機器につながる第１のポートをさらに含み、
前記第１のポートは、前記制限付きネットワークアクセス能力を、不完全に認証された前記少なくとも１台のユーザ機器に付与する、請求項１に記載の少なくとも１台のユーザ機器をＰＯＳＴ認証する方法。
【請求項８】
前記少なくとも１台のアクセスポイントは、認証サーバに接続された第２のポートをさらに含み、
前記将来のチャネル容量に対応する前記時点で前記少なくとも１台の候補ユーザ機器を完全に認証するため前記対応する認証メカニズムを用意することは、
制御プロトコルによって前記時点で前記第１のポートから前記第２のポートへ接続を切り替えることをさらに含み、
前記認証サーバが前記第２のポートを介して前記少なくとも１台の候補ユーザ機器を完全に認証する、請求項７に記載の少なくとも１台のユーザ機器をＰＯＳＴ認証する方法。
【請求項９】
前記少なくとも１台のアクセスポイントは、第１のポートを有する特定のアクセスポイントを含み、
前記第１のポートは、前記制限付きネットワークアクセス能力を、不完全に認証され、かつ前記第１のポートに接続された前記少なくとも１台のユーザ機器に付与する、請求項１に記載の少なくとも１台のユーザ機器をＰＯＳＴ認証する方法。
【請求項１０】
前記特定のアクセスポイントは、認証サーバに接続された第２のポートをさらに含み、
前記将来のチャネル容量に対応する前記時点で前記少なくとも１台の候補ユーザ機器を完全に認証するため前記対応する認証メカニズムを用意することは、
前記時点で前記第１のポートから前記第２のポートへ接続を切り替えることをさらに含み、
前記認証サーバが前記第２のポートを介して前記少なくとも１台の候補ユーザ機器を完全に認証する、請求項９に記載の少なくとも１台のユーザ機器をＰＯＳＴ認証する方法。
【請求項１１】
前記少なくとも１台の候補ユーザ機器を完全に認証するため前記対応する認証メカニズムを用意することは、
前記少なくとも１台の候補ユーザ機器を認証することが終了し、前記少なくとも１台のアクセスポイントが無制限ネットワークアクセス能力を前記少なくとも１台の候補ユーザ機器に付与することをさらに含む、請求項１に記載の少なくとも１台のユーザ機器をＰＯＳＴ認証する方法。

【請求項１２】
複数のモジュールを記憶する記憶ユニットと；、
前記記憶ユニットに接続され、前記複数のモジュールにアクセスし実行する処理ユニットと；、
を備えるコントローラであって、
前記複数のモジュールは、
少なくとも１台のユーザ機器が少なくとも１台のゲートウェイを介して少なくとも１台のアクセスポイントに接続されている前記少なくとも１台のゲートウェイの外部チャネル品質が閾値より高いか否かを決定する決定モジュールと；、
前記外部チャネル品質が前記閾値より高くない場合、前記少なくとも１台のユーザ機器を不完全に認証し、かつ前記少なくとも１台のユーザ機器に制限付きネットワークアクセス能力を付与するために前記少なくとも１台のアクセスポイントを制御する制御モジュールと；、
前記少なくとも１台のゲートウェイの将来のチャネル容量を推定する推定モジュールと；、
前記ユーザ機器の認証待ち時間、認証失敗の回数、および前記少なくとも１台のアクセスポイントと前記少なくとも１台のゲートウェイとの間の少なくとも１つのホップカウントに従って、前記少なくとも１台のユーザ機器のうち各ユーザ機器の優先度重みを計算する計算モジュールと；、
前記将来のチャネル容量および少なくとも１台の候補ユーザ機器の前記優先度重みに基づいて前記少なくとも１台のユーザ機器から前記少なくとも１台の候補ユーザ機器を選択し、かつ前記将来のチャネル容量に対応する時点で前記少なくとも１台の候補ユーザ機器を完全に認証するため対応する認証メカニズムを用意する選択モジュールと；、
を含む、コントローラ。
【請求項１３】
前記コントローラは、ソフトウェア定義型ネットワーキングコントローラであり、
前記コントローラ、前記少なくとも１台のアクセスポイントおよび前記少なくとも１台のゲートウェイは、複数台の車両および予測可能な走行経路を有する列車上に構成されている、請求項１２に記載のコントローラ。
【請求項１４】
前記推定モジュールは、
前記少なくとも１台のゲートウェイおよび車両個別履歴情報に基づいてチャネル品質推定モデルを確立することと；、
車両の現在の移動情報を取得し、前記現在の移動情報に基づいて前記車両の将来の移動情報を推定することと；、
前記将来の移動情報および前記チャネル品質推定モデルに従って前記少なくとも１台のゲートウェイの将来のチャネル品質を推定することと；、
前記将来のチャネル品質に従って前記少なくとも１台のゲートウェイの前記将来のチャネル容量を推定することと；、
をさらに含む、請求項１２に記載のコントローラ。
【請求項１５】
時点ｉでの前記将来のチャネル容量は、
Ｂが前記少なくとも１台のゲートウェイの周波数範囲であり、SNR_iが時点ｉでの信号対雑音比であるとして：
$C(i) = B \times \log_2(1 + SNR_i)$
である、請求項１２に記載のコントローラ。
【請求項１６】
前記少なくとも１台のユーザ機器のうちｎ番目のユーザ機器の優先度重みは、w_1からw_3が重み値であり、ＷＴが前記ｎ番目のユーザ機器の認証待ち時間であり、ｈは、前記ｎ番目のユーザ機器のために働く前記少なくとも１台のアクセスポイントと前記少なくと

も１台のゲートウェイとの間の少なくとも１つのホップカウントであり、ＦＴが前記ｎ番目のユーザ機器に対する認証失敗の回数であるとして：

$$P(n)=w_1\times WT+(1-w_2{}^h)+(1-w_3\times FT)$$

によって特徴付けられる、請求項１２に記載のコントローラ。

【請求項１７】

前記制御モジュールは、

前記各ユーザ機器の前記優先度重みに従って前記少なくとも１台のユーザ機器を降順にソートすることと；、

前記将来のチャネル容量および認証情報サイズに基づいて、前記認証情報サイズによって除算された前記将来のチャネル容量である特定の数を計算することと；、

前記少なくとも１台の候補ユーザ機器の前記特定の数としてより高い優先度重みを有する少なくとも１台のユーザ機器の前記特定の数を選択することと；、

をさらに含む、請求項１２に記載のコントローラ。

【請求項１８】

前記少なくとも１台のアクセスポイントは、不完全に認証された前記少なくとも１台のユーザ機器につながる第１のポートをさらに含み、

前記第１のポートは、前記制限付きネットワークアクセス能力を、不完全に認証された前記少なくとも１台のユーザ機器に付与する、請求項１２に記載のコントローラ。

【請求項１９】

前記少なくとも１台のアクセスポイントは、認証サーバに接続された第２のポートをさらに含み、前記選択モジュールは、

制御プロトコルによって前記時点で前記第１のポートから前記第２のポートへ接続を切り替えるように構成され、

前記認証サーバが前記第２のポートを介して前記少なくとも１台の候補ユーザ機器を完全に認証する、請求項１８に記載のコントローラ。

【請求項２０】

前記少なくとも１台のアクセスポイントは、第１のポートを有する特定のアクセスポイントを含み、

前記第１のポートは、前記制限付きネットワークアクセス能力を、不完全に認証され、かつ前記第１のポートにつながる前記少なくとも１台のユーザ機器に付与する、請求項１２に記載のコントローラ。

【請求項２１】

前記特定のアクセスポイントは、認証サーバに接続された第２のポートをさらに含み、前記選択モジュールは、

前記時点で前記第１のポートから前記第２のポートへ接続を切り替えるように構成され、前記認証サーバが前記第２のポートを介して前記少なくとも１台の候補ユーザ機器を完全に認証する、請求項２０に記載のコントローラ。

【請求項２２】

前記選択モジュールは、

前記少なくとも１台のアクセスポイントによって、無制限ネットワークアクセス能力を前記少なくとも１台の候補ユーザ機器に付与するようにさらに構成され、前記少なくとも１台の候補ユーザ機器を認証することが終了する、請求項１２に記載のコントローラ。

【請求項２３】

少なくとも１台のゲートウェイと；、

ネットワークにアクセスするために前記少なくとも１台のゲートウェイに接続された少なくとも１台のアクセスポイントと；、

前記少なくとも１台のゲートウェイおよび前記少なくとも１台のアクセスポイントに接続され、少なくとも１台のユーザ機器が前記少なくとも１台のゲートウェイを介して前記少なくとも１台のアクセスポイントに接続されているコントローラと；、

を備えるネットワークシステムであって、

前記コントローラは、
前記少なくとも１台のゲートウェイの外部チャネル品質が閾値より高いか否かを決定することと；、
前記外部チャネル品質が前記閾値より高くない場合、前記少なくとも１台のユーザ機器を不完全に認証し、前記少なくとも１台のユーザ機器に制限付きネットワークアクセス能力を付与するために前記少なくとも１台のアクセスポイントを制御することと；、
前記少なくとも１台のゲートウェイの将来のチャネル容量を推定することと；、
前記ユーザ機器の認証待ち時間、認証失敗の回数、および前記少なくとも１台のアクセスポイントと前記少なくとも１台のゲートウェイとの間の少なくとも１つのホップカウントに従って前記少なくとも１台のユーザ機器のうち各ユーザ機器の優先度重みを計算することと；、
前記将来のチャネル容量および前記少なくとも１台の候補ユーザ機器の前記優先度重みに基づいて前記少なくとも１台のユーザ機器から少なくとも１台の候補ユーザ機器を選択し、前記将来のチャネル容量に対応する時点で前記少なくとも１台の候補ユーザ機器を完全に認証するため対応する認証メカニズムを用意することと；、
をさらに含む、ネットワークシステム。
【請求項２４】
前記コントローラは、ソフトウェア定義型ネットワーキングコントローラであり、
前記コントローラ、前記少なくとも１台のアクセスポイントおよび前記少なくとも１台のゲートウェイは、複数台の車両および予測可能な走行経路を有する列車上に構成されている、請求項２３に記載のネットワークシステム。
【請求項２５】
前記コントローラは、
前記少なくとも１台のゲートウェイおよび車両個別履歴情報に基づいてチャネル品質推定モデルを確立することと；、
車両の現在の移動情報を取得し、前記現在の移動情報に基づいて前記車両の将来の移動情報を推定することと；、
前記将来の移動情報および前記チャネル品質推定モデルに従って前記少なくとも１台のゲートウェイの将来のチャネル品質を推定することと；、
前記将来のチャネル品質に従って前記少なくとも１台のゲートウェイの前記将来のチャネル容量を推定することと；、
を含む、請求項２３に記載のネットワークシステム。
【請求項２６】
時点ｉでの前記将来のチャネル容量は、
Ｂが前記少なくとも１台のゲートウェイの周波数範囲であり、SNR_iが時点ｉでの信号対雑音比であるとして：
$C(i) = B \times \log_2(1 + SNR_i)$
である、請求項２３に記載のネットワークシステム。
【請求項２７】
前記少なくとも１台のユーザ機器のうちｎ番目のユーザ機器の前記優先度重みは、
w_1からw_3が重み値であり、ＷＴが前記ｎ番目のユーザ機器の認証待ち時間であり、ｈは、前記ｎ番目のユーザ機器のために働く前記少なくとも１台のアクセスポイントと前記少なくとも１台のゲートウェイとの間の少なくとも１つのホップカウントであり、ＦＴが前記ｎ番目のユーザ機器に対する認証失敗の回数であるとして：
$P(n) = w_1 \times WT + (1 - w_2{}^h) + (1 - w_3 \times FT)$
によって特徴付けられる、請求項２３に記載のネットワークシステム。
【請求項２８】
前記コントローラは、
前記各ユーザ機器の前記優先度重みに従って前記少なくとも１台のユーザ機器を降順にソートすることと；、

前記将来のチャネル容量および認証情報サイズに基づいて、前記認証情報サイズによって除算された前記将来のチャネル容量である特定の数を計算することと；、
前記少なくとも１台の候補ユーザ機器の前記特定の数として、より高い優先度重みを有する少なくとも１台のユーザ機器の前記特定の数を選択することと；、
をさらに含む、請求項２３に記載のネットワークシステム。
【請求項２９】
前記少なくとも１台のアクセスポイントは、不完全に認証された前記少なくとも１台のユーザ機器につながる第１のポートをさらに含み、
前記第１のポートは、前記制限付きネットワークアクセス能力を、不完全に認証された前記少なくとも１台のユーザ機器に付与する、請求項２３に記載のネットワークシステム。
【請求項３０】
前記少なくとも１台のアクセスポイントは、認証サーバに接続された第２のポートをさらに含み、
前記コントローラは、
制御プロトコルによって前記時点で前記第１のポートから前記第２のポートへ接続を切り替えるように構成され、かつ前記認証サーバが前記第２のポートを介して前記少なくとも１台の候補ユーザ機器を完全に認証する、請求項２９に記載のネットワークシステム。
【請求項３１】
前記少なくとも１台のアクセスポイントは、第１のポートを有する特定のアクセスポイントを含み、
前記第１のポートは、前記制限付きネットワークアクセス能力を、不完全に認証され、かつ前記第１のポートにつながる前記少なくとも１台のユーザ機器に付与する、請求項２３に記載のネットワークシステム。
【請求項３２】
前記特定のアクセスポイントは、認証サーバに接続された第２のポートをさらに含み、
前記コントローラは、
前記時点で前記第１のポートから前記第２のポートへ接続を切り替えるように構成され、前記認証サーバが前記第２のポートを介して前記少なくとも１台の候補ユーザ機器を完全に認証する、請求項３１に記載のネットワークシステム。
【請求項３３】
前記コントローラは、
前記少なくとも１台のアクセスポイントによって、無制限ネットワークアクセス能力を前記少なくとも１台の候補ユーザ機器に付与するようにさらに構成され、前記少なくとも１台の候補ユーザ機器を認証することが終了する、請求項２３に記載のネットワークシステム。
【発明の詳細な説明】
【相互参照】
【０００１】
本出願は、２０１５年６月２４日付けで出願された台湾特許出願第１０４１２０３３３号の優先権の利益を主張する。上記特許出願の全体は、参照によって本明細書に組み込まれる。
【技術分野】
【０００２】
本出願は、少なくとも１台のユーザ機器（ＵＥ）をＰＯＳＴ認証する方法、コントローラおよびネットワークシステムに関する。
【背景技術】
【０００３】
高速鉄道は、フランスにおけるＴＶＧ、ドイツにおけるＩＣＥ（インターシティ・エクスプレス）、日本における新幹線、および台湾高速鉄道のように多くの国々で重要な輸送

手段の１つである。高速鉄道の発達および通信機器の普及と共に、ネットワークの要求が高速移動状況において急速に増加している。概して、高速鉄道の列車の最高速度は、毎時約２８０キロメートルである。このような高い移動速度の下で、短い期間内の信号品質の変動は、かなり大きくなるであろう。その上、ドップラー効果の影響によって、受信側での復号誤り率は、増加するであろう。これは、ネットワーク接続が遮断されたとき、ユーザ機器（ＵＥ）にデータを頻繁に再送信させようとする。概して、ＵＥがインターネットにアクセスする前に、ＵＥは、認証・認可・課金（ＡＡＡ）サーバによって認証されるような認証を受け入れることが必要である。しかしながら、ＵＥを認証するための認証プロセスがネットワーク切断のため失敗した場合、ＵＥは、認証プロセスを完了するために引き続き認証データを再送信しようとするであろう。

【０００４】

図１は、列車１００のネットワークシステムを示すブロック図である。図１における列車１００は、予測可能な運行経路および何台もの車両を含んでいる列車、高速鉄道、またはその他の輸送機関でもよい。列車１００は、５台の車両１００＿１～１００＿５を含むことがある。本実施形態では、アクセスポイント（ＡＰ）１０２＿１～１０２＿５は、列車中の車両１００＿１～１００＿５にそれぞれ配備されることがあり、車両１００＿１～１００＿５内の乗客にネットワークアクセス能力をそれぞれ提供することができる。たとえば、アクセスポイント１０２＿１は、車両１００＿１内の乗客が（携帯電話機、タブレットＰＣ、ノートブックコンピュータ、またはその他の同様の装置のような）携帯装置を使ってネットワークにアクセスできるようにすることができ、アクセスポイント１０２＿２は、車両１００＿２内の乗客にネットワークアクセスを提供することができ、残りのアクセスポイント１０２＿３～１０２＿５も同様である。

【０００５】

図１に示されるように、列車１００は、車両１００＿３に接続された単一の外部ゲートウェイ１０４（たとえば、クライアント装置（加入者宅内機器、ＣＰＥ）ゲートウェイ）だけを配備している。ゲートウェイ１０４は、ＡＰ１０２＿１～１０２＿５に、車両１０２＿１～１０２＿５の間でネットワーク１０６と通信するために中間アクセスポイントとして、接続されることができる。ネットワーク１０６は、限定されることはないが、ロング・レンジ・エボリューション（ＬＴＥ）、ＷｉＭＡＸ（ワールドワイド・インターオペラビリティ・フォー・マイクロウェーブ・アクセス、ＷｉＭＡＸ）、第３世代移動通信ネットワーク（３Ｇ）、第４世代移動通信ネットワーク（４Ｇ）、またはその他の同様のネットワークでもよい。図１は、ネットワーク１０６の構成を明示していないが、ネットワーク１０６は、実質的に通信規格に基づき、対応するネットワークエンティティを含むように構成され得る。たとえば、通信するためのＬＴＥネットワーク１０６およびゲートウェイ１０４を使用する場合、ネットワーク１０６は、エンハンスト・ノードＢ（ｅＮＢ）と、モビリティ・マネジメント・エンティティ（ＭＭＥ）と、サービング・ゲートウェイ（Ｓ－ＧＷ）と、パケット・データ・ネットワーク・ゲートウェイ（Ｐ－ＧＷ）と、その他のネットワークエンティティとを含むことがあるが、これらに限定されることはない。

【０００６】

列車１００は、単一の外部ゲートウェイ１０４だけを有するので、ゲートウェイ１０４とネットワーク１０６との間のチャネル品質は、列車１００が移動しているとき、急速に変化し、ネットワーク切断の状況が頻繁に起こるであろう。ＵＥの認証プロセスが失敗した場合、外部ゲートウェイの送信キューは、認証データで満たされ、ネットワーク輻輳を引き起こすことがあり得る。

【０００７】

その上、ゲートウェイ１０４のトラフィックを分けるためにゲートウェイ１０４と同様の付加的な冗長ゲートウェイが車両１００＿３内に構築された場合であっても、冗長ゲートウェイのチャネル品質は、ゲートウェイ１０４のチャネル品質と類似しているので、全体的な伝送効率は、依然としてチャネル多様性効果に到達し得ないであろう。

【発明の概要】

【発明が解決しようとする課題】
【０００８】
よく知られた列車によって構築されたネットワークトポロジーでは、外部（アウトバウンド）ゲートウェイの１つの単一構成だけが存在する。前述のとおり、ＵＥの認証プロセスが失敗した場合、外部ゲートウェイの送信キューは、認証データで満たされ、ネットワーク輻輳の現象が起こり得る。
【課題を解決するための手段】
【０００９】
本開示の実施形態は、少なくとも１台のユーザ機器をＰＯＳＴ認証する方法、コントローラ、およびネットワークシステムを提供する。
【００１０】
本開示の実施形態は、少なくとも１台のゲートウェイに接続されたコントローラに適応している、少なくとも１台のユーザ機器をＰＯＳＴ認証する方法に関する。この方法は、少なくとも１台のユーザ機器が少なくとも１台のアクセスポイントに接続され、少なくとも１台のゲートウェイの外部チャネル品質が閾値より高いか否かを決定することと；、外部チャネル品質が閾値より高くない場合、少なくとも１台のユーザ機器を不完全に認証し、少なくとも１台のユーザ機器に制限付きネットワークアクセス能力を付与するために少なくとも１台のアクセスポイントを制御し、少なくとも１台のゲートウェイの将来のチャネル容量を推定することと；、ユーザ機器の認証待ち時間、認証失敗の回数、および、少なくとも１台のアクセスポイントと少なくとも１台のゲートウェイとの間の少なくとも１つのホップカウントに従って少なくとも１台のユーザ機器のうち各ユーザ機器の優先度重みを計算することと；、将来のチャネル容量および少なくとも１台の候補ユーザ機器の優先度重みに基づいて少なくとも１台のユーザ機器から少なくとも１台の候補ユーザ機器を選択し、将来のチャネル容量に対応する時点で少なくとも１台の候補ユーザ機器を完全に認証するため対応する認証メカニズムを用意することと；、を含む。
【００１１】
本開示の別の実施形態は、コントローラに関する。コントローラは、複数のモジュールを記憶する記憶ユニットと、記憶ユニットに接続され、複数のモジュールにアクセスし実行する処理ユニットとを備える。複数のモジュールは、決定モジュールと、制御モジュールと、推定モジュールと、計算モジュールと、選択モジュールとを含む。決定モジュールは、少なくとも１台のゲートウェイの外部チャネル品質が閾値より高いか否かを決定し、少なくとも１台のユーザ機器が少なくとも１台のゲートウェイを介して少なくとも１台のアクセスポイントに接続されている。制御モジュールは、外部チャネル品質が閾値より高くない場合、少なくとも１台のユーザ機器を不完全に認証し、少なくとも１台のユーザ機器に制限付きネットワークアクセス能力を付与するために少なくとも１台のアクセスポイントを制御する。推定モジュールは、少なくとも１台のゲートウェイの将来のチャネル容量を推定する。計算モジュールは、ユーザ機器の認証待ち時間、認証失敗の回数、および少なくとも１台のアクセスポイントと少なくとも１台のゲートウェイとの間の少なくとも１つのホップカウントに従って、少なくとも１台のユーザ機器のうち各ユーザ機器の優先度重みを計算する。選択モジュールは、将来のチャネル容量および少なくとも１台の候補ユーザ機器の優先度重みに基づいて少なくとも１台のユーザ機器から少なくとも１台の候補ユーザ機器を選択し、将来のチャネル容量に対応する時点で少なくとも１台の候補ユーザ機器を完全に認証するため対応する認証メカニズムを用意する。
【００１２】
本開示のさらに別の実施形態は、ネットワークシステムに関する。このネットワークシステムは、少なくとも１台のゲートウェイと、ネットワークにアクセスするために少なくとも１台のゲートウェイに接続された少なくとも１台のアクセスポイントと、少なくとも１台のゲートウェイおよび少なくとも１台のアクセスポイントに接続されたコントローラとを備え、少なくとも１台のユーザ機器が少なくとも１台のゲートウェイを介して少なくとも１台のアクセスポイントに接続されている。コントローラは、さらに、少なくとも１

台のゲートウェイの外部チャネル品質が閾値より高いか否かを決定し、外部チャネル品質が閾値より高くない場合、少なくとも１台のユーザ機器を不完全に認証し、少なくとも１台のユーザ機器に制限付きネットワークアクセス能力を付与するために少なくとも１台のアクセスポイントを制御し、少なくとも１台のゲートウェイの将来のチャネル容量を推定し、ユーザ機器の認証待ち時間、認証失敗の回数、および少なくとも１台のアクセスポイントと少なくとも１台のゲートウェイとの間の少なくとも１つのホップカウントに従って少なくとも１台のユーザ機器のうち各ユーザ機器の優先度重みを計算し、将来のチャネル容量および少なくとも１台の候補ユーザ機器の優先度重みに基づいて少なくとも１台のユーザ機器から少なくとも１台の候補ユーザ機器を選択し、将来のチャネル容量に対応する時点で少なくとも１台の候補ユーザ機器を完全に認証するため対応する認証メカニズムを用意する。

【発明の効果】

【００１３】

以上の事項に基づいて、本開示は、少なくとも１台のユーザ機器をＰＯＳＴ認証する方法、コントローラ、およびこのコントローラのネットワークシステムを提供する。コントローラが、少なくとも１台のゲートウェイの外部チャネル品質は、現在のところ不十分であると決定したとき、コントローラは、少なくとも１台の認証されていない、もしくは、一部分しか認証されていないユーザ機器がネットワークにアクセスするために制限付きネットワークアクセス能力を使用することを一時的に許可する。

【００１４】

前述の事項は、添付図面を適切に参照して後述された詳細な説明の熟読からよりよく理解されるものである。

【図面の簡単な説明】

【００１５】

【図１】列車のネットワークシステムを示すブロック図である。

【００１６】

【図２】本開示の例示的な実施形態によるネットワークシステムである。

【００１７】

【図３】本開示の例示的な実施形態による少なくとも１台のユーザ機器をＰＯＳＴ認証する方法のフローチャートを示す図である。

【００１８】

【図４】本開示の実施形態によるネットワークシステムを示す図である。

【００１９】

【図５】本開示の別の実施形態によるネットワークシステムを示す図である。

【発明を実施するための形態】

【００２０】

以下、当業者によって容易に実現されるように例示的な実施形態を詳細に説明する。発明の概念は、本明細書に記載された例示的な実施形態に限定されることなく、様々な形態で具現化されることがある。

【００２１】

周知の部品の説明は、分かり易さのため省略され、類似した符号は、全体を通して類似した要素を指す。

【００２２】

実施形態によれば、本開示は、少なくとも１台のＵＥをＰＯＳＴ認証する方法を提供する。実施形態では、少なくとも１台のゲートウェイのチャネル品質は、不十分であるが、少なくとも１台のアクセスポイントは、（制限付きの帯域幅、フローおよび時間などのような）制限付きネットワークアクセス能力を認証プロセスが未だ終了していないような不完全に認証された少なくとも１台のＵＥに付与することがある。さらに、この方法は、少なくとも１台のＵＥから認証されるべきより高い優先度重みを有する少なくとも１台の候補ＵＥを選択するメカニズムを用意し、次に、少なくとも１台の候補ＵＥが適当な時点で

認証プロセスを完了することを許可する。詳細を以下に記載する。例示的な実施形態では、チャネル品質は、限定されることなく、参照信号受信電力（ＲＳＲＰ）、搬送波対干渉雑音比（ＣＩＮＲ）、搬送波雑音比（搬送波対雑音比、ＣＮＲ）、信号対雑音比（ＳＮＲ）、および／または、信号対干渉雑音比（ＳＩＮＲ）として特徴付けられることがあるが、これらに限定されない。

【００２３】

図２は、本開示の例示的な実施形態によるネットワークシステムである。本実施形態では、ネットワークシステム２００は、コントローラ２１０、少なくとも１台のゲートウェイ２２０および少なくとも１台のアクセスポイント２３０を含む。少なくとも１台のアクセスポイント２３０は、列車の車両に配備され、車両のＵＥのために働くこともある。少なくとも１台のゲートウェイ２２０は、アクセスポイント２３０に電気接続されることがあり、アクセスポイント２３０は、少なくとも１台のユーザ機器２６０＿１～２６０＿Ｎ（Ｎは、正の整数である）から、ネットワーク２４０までデータフローをルーティングすることがある。一実施形態では、ユーザ機器からのデータが認証情報であるとき、少なくとも１台のゲートウェイ２２０は、少なくとも１台のアクセスポイント２３０が認証情報を認証サーバ２５０（たとえば、ＡＡＡサーバ）にルーティングすることを実現し易くすることがある。

【００２４】

図１に示されたような周知技術とは違って、図２におけるシステム２００は、少なくとも１台のゲートウェイ２２０に電気接続または無線接続された少なくとも１台のコントローラと、を含む。実施形態では、コントローラ２１０は、記憶ユニット２１２および処理ユニット２１４を含むことがあるソフトウェア定義型ネットワーキング（ＳＤＮ）コントローラでもよい。記憶ユニット２１２は、限定されることなく、メモリ、ハードディスク、または、データを記憶するために、および／または、複数のコードもしくはモジュールを記録するために使用されることがあるその他の要素を含むことがある。処理ユニット２１４は、記憶ユニット２１２に電気接続されている。処理ユニット２１４は、汎用プロセッサ、専用プロセッサ、従来型プロセッサ、デジタル信号プロセッサ、複数のマイクロプロセッサ、１つ以上のデジタル信号プロセッサを含むマイクロプロセッサ、コントローラ、マイクロコントローラ、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・アレイ回路（ＦＰＧＡ）、その他の集積回路、アドバンストＲＩＳＣセットマシン（ＡＲＭ）プロセッサに基づく状態機械、および、類似した物でもよい。

【００２５】

実施形態では、少なくとも１台のアクセスポイント２３０は、ＳＤＮスイッチ機能を有することがあり、情報を交換するためにＳＤＮベースの通信プロトコル（たとえば、ＯｐｅｎＦｌｏｗ）を用いてコントローラ２１０と通信することがある。他の実施形態では、ＳＤＮスイッチは、アクセスポイント２３０がコントローラ２１０と通信することを実現し易くするために、少なくとも１台のアクセスポイント２３０の外側にある装置上に別個のスイッチとして実装されることもある。ＳＤＮにおいて、データ平面と制御平面とは切り離されている。図２は、データフロー用および制御フロー用の伝送路も別々に描いている。

【００２６】

その上、図２は、本実施形態の概念を例示で説明するために単一のゲートウェイ２２０および単一のアクセスポイント２３０だけを示しているが、このことは、開示された考え得る実施形態を制限すると解釈されない。他の実施形態では、これらの技術的特徴は、複数のゲートウェイおよび複数のアクセスポイントを含む本開示のネットワークシステムに同様に適用可能である。

【００２７】

本実施形態では、処理ユニット２１４は、記憶ユニット２１２にアクセスし、決定モジュール２１２＿１、制御モジュール２１２＿２、推定モジュール２１２＿３、計算モジュール２１２＿４、および選択モジュール２１２＿５を実行して、少なくとも１台のユーザ

機器をＰＯＳＴ認証する方法を実行する。

【００２８】

図３は、本開示の例示的な実施形態による少なくとも１台のユーザ機器をＰＯＳＴ認証する方法のフローチャートを示す。図３における方法は、図２のコントローラ２１０によって実行されることがある。図２に表された要素と組み合わせて、図３の例示的な実施形態の詳細を以下に説明する。

【００２９】

最初に、ステップＳ３１０では、少なくとも１台のユーザ機器２６０＿１～２６０＿Ｎが少なくとも１台のゲートウェイ２２０によってルーティングされた少なくとも１台のアクセスポイント２３０につながるとき、決定モジュール２１２＿１は、ゲートウェイ２２０の外部チャネル品質が閾値より高いか否かを決定することがある。外部チャネル品質は、たとえば、少なくとも１台のゲートウェイ２２０とネットワーク２４０との間の（ＳＮＲのような）チャネル品質でもよく、閾値は、設計者によって選択された任意の値（たとえば、２０ｄＢ）でもよい。閾値は、プリセット、無作為に選択、またはネットワークを介して送信されることがある。実施形態では、少なくとも１台のユーザ機器２６０＿１～２６０＿Ｎが少なくとも１台のアクセスポイント２３０につながるとき、少なくとも１台のアクセスポイント２３０は、ＯｐｅｎＦｌｏｗを用いて、（媒体アクセス制御（ＭＡＣ）アドレスおよび国際移動電話加入者識別番号（ＩＭＳＩ）などのような）ユーザ情報をコントローラ２１０に送信することがあるが、これに限定されるものではない。

【００３０】

実施形態では、設計者は、チャネル容量に対応するチャネル品質に基づいて閾値をさらに決定することがある。たとえば、設計者は、少なくとも１つの認証データを十分に送信するためのチャネル容量を見出すことがあり、閾値としてチャネル容量に対応するチャネル品質を決定することがある。この事例では、外部チャネル品質が閾値より高い場合、この外部チャネル品質は、外部チャネル品質に対応するチャネル容量が少なくとも１つの認証データを送信するために十分であることを表現する。外部チャネル品質に対応するチャネル容量が２つの認証情報を転送するために十分であると仮定すると、コントローラ２１０は、認証サーバ２５０を使って認証するためにユーザ機器２６０＿１～２６０＿Ｎ（この場合、Ｎ≧２）のうち２台を直接用意することがある。これに反して、外部チャネル品質が閾値より高くない場合、この外部チャネル品質は、外部チャネル品質に対応するチャネル容量が何らかの認証情報を送信するために不十分であることを表現することがある。

【００３１】

このようにして、ステップＳ３２０において、外部チャネル品質が閾値より高くないとき、制御モジュール２１２＿２は、少なくとも１台のユーザ機器２６０＿１～２６０＿Ｎを不完全に認証することがあり、少なくとも１台のユーザ機器２６０＿１～２６０＿Ｎに制限付きネットワークアクセス能力を付与するために少なくとも１台のアクセスポイント２３０を制御することがある。換言すれば、制御モジュール２１２＿２は、認証されていない、もしくは、一部分しか認証されていないユーザ機器２６０＿１～２６０＿Ｎが少なくとも１台のアクセスポイント２３０を介するインターネットへの制限付きネットワークアクセス能力の状態でネットワーク２４０につながることを許可することがある。一例としてユーザ機器２６０＿１を挙げると、認証されていない、もしくは、一部分しか認証されていないユーザ機器２６０＿１は、制御モジュール２１２＿２を経由してアクセスポイント２３０を介するインターネットへの（限定されることはないが、制限付き帯域幅、制限付きスループット、もしくは、制限付き時間（たとえば、２０分間）のような）能力が制限された状態でネットワーク２４０につながることがある。このようにして、開示された方法は、インターネットにアクセスするユーザ機器２６０＿１の要求を満たすだけでなく、ユーザ機器２６０＿１が不十分な外部チャネル品質の条件下で認証情報を継続して送信することを試みないようにする。換言すれば、本開示の実施形態は、少なくとも１台のゲートウェイ２２０上でネットワーク輻輳を引き起こす可能性を低下させることがあり、認証されていない、もしくは、一部分しか認証されていないユーザのためのインターネッ

ト時間を改善することもある。

【００３２】

次に、この方法は、ステップＳ３３０～Ｓ３５０によって、少なくとも１台のユーザ機器２６０＿１～２６０＿Ｎから認証されるべきより高い優先度重みを有する少なくとも１台の候補ユーザ機器を選択することがあり、適当な時点で少なくとも１台の候補ユーザ機器を完全に認証することがある。

【００３３】

ステップＳ３３０において、推定モジュール２１２＿３は、少なくとも１台のゲートウェイ２２０の将来のチャネル容量を推定することがある。実施形態では、少なくとも１台のゲートウェイ２２０のチャネル品質推定モデルは、少なくとも１台のゲートウェイ２２０および車両個別履歴情報に基づいて推定モジュール２１２＿３によって構築されることがある。車両個別履歴情報は、たとえば、車両もしくは列車の走行経路と、この走行経路上の様々な区域の走行速度とを含む。少なくとも１台のゲートウェイ２２０の履歴情報は、たとえば、車両もしくは列車の走行経路上で事前に測定された少なくとも１台のゲートウェイ２２０のチャネル品質を含む。

【００３４】

上記から、推定モジュール２１２＿３は、車両もしくは列車の走行経路上の各区域に関して少なくとも１台のゲートウェイ２２０の将来のチャネル品質を推定するため使用されてもよいことが分かることがある。その後に、推定モジュール２１２＿３は、測定された結果に従って、走行経路上の区域に対してチャネル品質のマッピングテーブルを確立することがある（すなわち、少なくとも１台のゲートウェイ２２０のチャネル品質推定モデル）。車両もしくは列車の走行経路および周囲の駅は固定されているので、マッピングテーブルは、非常に信頼性が高い。車両もしくは列車（図示せず）に対するゲートウェイの他の構成のため、推定モジュール２１２＿３は、上記教示に基づいてチャネル品質推定モデルを確立することがある。

【００３５】

少なくとも１台のゲートウェイ２２０のチャネル品質推定モデルが確立された後、推定モジュール２１２＿３は、列車の現在の移動情報を取得することがあり、列車の将来の移動情報を推定するために現在の移動情報を使用することがある。現在の移動情報は、限定されることはないが、衛星測位システム（全地球測位システム、ＧＰＳ）から得られた列車の現在の走行区域および走行速度の情報を含むことがある。列車の将来の移動情報は、限定されることはないが、列車の将来の走行区域および将来の走行速度の情報を含むことがある。列車の走行経路および走行速度は、大まかに予め定められたパラメータであり、その結果、推定モジュール２１２＿３は、現在の移動情報が得られた後に列車の将来の走行経路および列車の将来の走行速度を容易に取得することがある。

【００３６】

次に、推定モジュール２１２＿３は、将来の移動情報およびチャネル品質推定モデルに従って少なくとも１台のゲートウェイ２２０の将来のチャネル品質を推定することがある。たとえば、推定モジュール２１２＿３は、将来の走行区域および将来の走行速度に従ってマッピングテーブルを調べることがあり、走行区域に対するチャネル品質（すなわち、将来のチャネル品質）を取得することがある。その後、推定モジュール２１２＿３は、少なくとも１台のゲートウェイ２２０の将来のチャネル品質に従って将来のチャネル容量を取得することがある。実施形態では、時点ｉでの（ｉは、正の整数である）信号雑音比は、ＳＮＲｉで表されると仮定する。時点ｉに推定モジュール２１２＿３によって推定された将来のチャネル容量は：

$$C(i) = B \times \log_2(1 + SNR_i) \qquad (1)$$

として特徴付けられることがある。式中、Ｂは、少なくとも１台のゲートウェイ２２０の周波数範囲である。

【００３７】

同じ認証メカニズムの下での認証情報サイズの差は、小さい。その結果、時点ｉでの将

来のチャネル容量（すなわち、Ｃ（ｉ））が計算された後、推定モジュール２１１＿３は、少なくとも１台のゲートウェイ２２０が時点ｉで送信することがある認証情報の個数を取得するために、認証情報サイズによるＣ（ｉ）の除算の商（以下では、ｊと称する）を計算することがある。すなわち、ｊは、時点ｉで認証を完了しようとしているユーザ機器の台数であり、この台数が少なくとも１台のゲートウェイ２２０によって許可されている。ｊが４であると仮定すると、このことは、少なくとも１台のゲートウェイ２２０は、ユーザ機器２６０＿１～２６０＿Ｎ（この場合、Ｎ≧４である）のうち４台が時点ｉに各々の認証情報を認証サーバ２５０にそれぞれ送信することを意味する。

【００３８】

ステップＳ３４０において、計算モジュール２１２＿４は、ユーザ機器の認証待ち時間、認証失敗の回数、および、少なくとも１台のアクセスポイントと少なくとも１台のゲートウェイとの間の少なくとも１つのホップカウントに従って、少なくとも１台のユーザ機器２６０＿１～２６０＿Ｎのうち各ユーザ機器の優先度重みを計算することがある。

【００３９】

実施形態では、ｎ番目（１≦ｎ≦Ｎ）のユーザ機器２６０＿ｎの優先度重みは：

$$P(n)=w_1\times WT+(1-w_2{}^{h})+(1-w_3\times FT) \quad (2)$$

として特徴付けられることがある。式中、w_1からw_3は、重み値であり、ＷＴは、ｎ番目のユーザ機器の認証待ち時間であり、ｈは、ｎ番目のユーザ機器のために働く少なくとも１台のアクセスポイントと少なくとも１台のゲートウェイとの間の少なくとも１つのホップカウントであり、ＦＴは、ｎ番目のユーザ機器の認証失敗の回数である。w_1からw_3は、限定されることなく、設計者の要求に基づいて設計者によって選択された（零を含む）いかなる値でもよく、この値は、プリセット、無作為に選択、またはネットワークを介して送信されることがある。ＷＴは、限定されることなく、ｎ番目のユーザ機器が制限付きネットワークアクセス能力を使ってネットワーク２４０にアクセスする時間でもよい。ｈは、限定されることなく、アクセスポイント２３０が少なくとも１台のゲートウェイ２２０にデータを送信する間に合格した装置の台数でもよい。少なくとも１台のアクセスポイント２３０が少なくとも１台のゲートウェイ２２０に直接接続されていると仮定すると、ｈは、１である。少なくとも１台のアクセスポイント２３０が２台の装置（たとえば、２台の他のアクセスポイント）を介して少なくとも１台のゲートウェイ２２０に接続されていると仮定すると、ｈは、３である。ＦＴは、ｎ番目のユーザ機器が認証情報を送信することを試みるが、完全には認証できないような認証失敗の回数である。

【００４０】

他の実施形態では、ｎ番目（ｎは、１からＮまでの整数である）のユーザ機器２６０＿ｎの優先度重みは、限定されることなく、以下の式（３）から（９）のような設計者の要求として特徴付けられることがある。

$$P(n)=w_1\times WT+w_2\times h+(1-w_3\times FT) \quad (3)$$

$$P(n)=w_1\times WT \quad (4)$$

$$P(n)=w_2\times h \quad (5)$$

$$P(n)=(1-w_3\times FT) \quad (6)$$

$$P(n)=w_1\times WT+w_2\times h \quad (7)$$

$$P(n)=w_1\times WT+(1-w_3\times FT) \quad (8)$$

$$P(n)=w_2\times h+(1-w_3\times FT) \quad (9)$$

【００４１】

ステップＳ３５０において、選択モジュール２１２＿５は、将来のチャネル容量および少なくとも１台の候補ユーザ機器の優先度重みに基づいて少なくとも１台のユーザ機器２６０＿１～２６０＿Ｎから少なくとも１つの候補ユーザ機器を選択することがあり、将来のチャネル容量に対応する時点で少なくとも１台のユーザ機器を完全に認証するため対応する認証メカニズムを用意することがある。

【００４２】

実施形態では、選択モジュール２１２＿５は、各ユーザ機器の優先度重みに従って少な

くとも１台のユーザ機器２６０＿１～２６０＿Ｎを降順にソートすることがあり、将来のチャネル容量（たとえば、Ｃ（ｉ））と認証情報サイズとに基づいて特定の数（以下では、ｊと称する）を計算することがあり、この特定の数は、限定されることなく、認証情報サイズによって除算された将来のチャネル容量Ｃ（ｉ）でもよい。次に、選択モジュール２１２＿５は、少なくとも１台のユーザ機器２６０＿１～２６０＿Ｎから、少なくとも１台の候補ユーザ機器として、ソートされた先行するユーザ機器の特定の数を選択することがある。換言すれば、選択モジュール２１２＿５は、少なくとも１台のユーザ機器２６０＿１～２６０＿Ｎから、少なくとも１台の候補ユーザ機器として、ｊ台のユーザ機器（群）を選択することがある。次に、選択モジュール２１２＿５は、少なくとも１台の候補ユーザ機器をある時点で完全に認証するため認証メカニズムを用意することがある。

【００４３】

少なくとも１台の候補ユーザ機器が認証を完了するとき、選択モジュール２１２＿５は、無制限ネットワーク能力を少なくとも１台の候補ユーザ機器に付与するために少なくとも１台のアクセスポイント２３０を制御することがある。換言すれば、ユーザ機器は、認証を完了した後、無制限帯域幅、無制限スループット、および時間制限なしの状態でネットワーク２４０にアクセスすることがある。

【００４４】

簡潔に言えば、コントローラ２１０が、少なくとも１台のゲートウェイ２２０の外部チャネル品質は、現在のところ不良であると決定したとき、コントローラ２１０は、少なくとも１台のユーザ機器２６０＿１～２６０＿Ｎがネットワークにアクセスするために制限付きネットワークアクセス能力を使用することを一時的に許可することがある。その後、コントローラ２１０が時点ｉでの将来のチャネル品質は、改善されるであろうと推定するとき、コントローラ２１０は、より高い優先度重みを有する少なくとも１台の候補ユーザ機器が適切な時点で認証情報を認証サーバ２５０に送信するために認証機会を用意することがある。

【００４５】

本開示の他の実施形態では、ネットワークシステムは、図４～５に表されるように、ユーザ機器に制限付きもしくは無制限ネットワークアクセス能力を付与するためにアクセスポイントをそれぞれ制御するように構成されることがある。図４における実施形態を参照すると、ネットワークシステム４００は、コントローラ４１０、第１のアクセスポイント４２０＿１、および、認証サーバ４４０に接続された第２のアクセスポイント４２０＿２を含む。たとえば、第１のアクセスポイント４２０＿１は、不完全に認証されたユーザ機器４３０に接続され、制限付きアクセスネットワーク能力をユーザ機器４３０に付与する。前述のとおり、ユーザ機器４３０が第１のアクセスポイント４２０＿１につながるとき、第１のアクセスポイント４２０＿１ｔは、ＯｐｅｎＦｌｏｗを用いてユーザ機器４３０のユーザ情報をコントローラ４１０に転送することがある。その後、本開示の認証メカニズムを用意するときに上記教示に従って、コントローラ４１０は、ユーザ機器４３０が時点ｉに認証されるように試みることを許可することがある。同様に、コントローラ４１０は、時点ｉで第１のアクセスポイント４２０＿１から第２のアクセスポイント４２０＿２へ接続を切り替えるために制御プロトコルを使用することによりユーザ機器４３０に通知することがあり、その結果、認証サーバは、第２のアクセスポイント４２０＿２を介して候補ユーザ機器４３０を完全に認証することがある。制御プロトコルは、限定されることなく、ネットワーク検索および選択メカニズム（アクセスネットワーク発見および選択機能、ＡＮＤＳＦ）でもよい。認証サーバ４４０がユーザ機器４３０を完全に認証した後、コントローラ４１０は、無制限ネットワーク能力をユーザ機器４３０に付与し、ユーザ機器４３０が無制限帯域幅、無制限スループット、および時間制限なしの状態でネットワークにアクセスすることを許可するように、第２のアクセスポイント４２０＿２を制御することがある。

【００４６】

さらに、認証サーバ４４０は、ユーザ機器４３０のタイプに応じてユーザ機器４３０を

認証するために異なったスキームを有することがある。たとえば、ユーザ機器４３０がグローバル・システム・フォー・モバイル（ＧＳＭ）に従って動作する装置であるとき、認証サーバ４４０は、ユーザ機器４３０を認証するために加入者識別モジュール（ＳＩＭ）拡張認証プロトコル（ＥＡＰ）（すなわち、ＥＡＰ－ＳＩＭ）に基づくことがある。別の例では、ユーザ機器４３０が標準的なユニバーサル・モバイル・テレコミュニケーション・システム（ＵＭＴＳ）に従って動作する装置であるとき、認証サーバ４４０は、ユーザ機器４３０を認証するために、ＥＡＰのセキュリティ認証および鍵配布（認証および鍵アグリーメント、ＡＫＡ）（すなわち、ＥＡＰ－ＡＫＡ）に基づくことがある。

【００４７】

本開示の他の実施形態では、ネットワークシステムは、ユーザ機器に制限付きもしくは無制限ネットワーク同時アクセス能力を付与するために特定のアクセスポイントを制御するようにさらに構成されることがある。図５における実施形態を参照すると、ネットワークシステム５００は、コントローラ５１０と、特定のアクセスポイント５２０に接続された認証サーバ５４０とを含む。特定のアクセスポイント５２０は、第１のポートおよび第２のポート（図示せず）をさらに含むことがある。第１のポートは、制限付きネットワーク能力を不完全に認証されたユーザ機器５３０に付与することがあるデフォルトポートでもよい。前述のとおり、ユーザ機器５３０が第１のポートにつながるとき、特定のアクセスポイント５２０は、ＯｐｅｎＦｌｏｗを用いてユーザ機器５３０のユーザ情報をコントローラ５１０に転送することがある。その後、本開示の認証メカニズムを用意するときに上記教示に従って、コントローラ５１０は、ユーザ機器５３０が時点ｉに認証されるように試みることを許可することがある。同様に、コントローラ５１０は、時点ｉで第１のポートから第２のポートに接続を切り替えるためにＯｐｅｎＦｌｏｗを用いてユーザ機器５３０に通知することがあり、その結果、認証サーバ５４０は、第２のポートを介して候補ユーザ機器５３０を完全に認証することがある。認証サーバ５４０がユーザ機器５３０を完全に認証した後、コントローラ５１０は、無制限ネットワーク能力をユーザ機器５３０に付与して、ユーザ機器５３０がこのような無制限帯域幅、無制限スループット、時間制限なしの状態でネットワークにアクセスすることを許可するように特定のアクセスポイント５２０を制御することがある。

【００４８】

実施形態では、第１のポートは、パスワードなしのサービスセット識別子（ＳＳＩＤ）として特徴付けられることがあり、第２のポートは、パスワード付きのサービスセット識別子（ＳＳＩＤ）として特徴付けられることがある。この事例では、認証されていないユーザ機器５３０は、第１のポートに対応するＳＳＩＤに接続するであろう。特定のアクセスポイント５２０が接続を第２のポートに切り替えるようにユーザ機器５３０に通知するとき、特定のアクセスポイント５２０は、ユーザ機器５３０が接続を第２のポートのＳＳＩＤに切り替えることを許可するために、第２のポートのパスワードをユーザ機器５３０にさらに通知することがある。他の実施形態では、第２のポートは、パスワード付きの秘密ＳＳＩＤとして実装されることがある。すなわち、認証されていないユーザ機器５３０は、第１のポートのＳＳＩＤのリストから第２のポートの情報を見つけることができないが、開示された実施形態は、これらに限定されない。

【００４９】

要約すれば、本開示は、少なくとも１台のユーザ機器をＰＯＳＴ認証する方法、コントローラ、およびそのネットワークシステムを提供する。コントローラが、少なくとも１台のゲートウェイの外部チャネル品質が現在のところ不良であると決定したとき、コントローラは、少なくとも１台の認証されていない、もしくは、一部分しか認証されていないユーザ機器がネットワークにアクセスするために制限付きネットワークアクセス能力を使用することを一時的に許可する。その後、コントローラが、将来のチャネル品質は、ある時点で改善されるであろうと推定するとき、コントローラは、より高い優先度を有する少なくとも１台の候補ユーザ機器が認証情報をこの時点で認証サーバに送信する認証機会を用意することがある。その結果、本開示の実施形態は、少なくとも１台のゲートウェイ上に

ネットワーク輻輳を引き起こす可能性を低下させると共に、認証されていない、もしくは、一部分しか認証されていないユーザのためのインターネット時間を改善する。

【００５０】

様々な変更および変形が開示された実施形態に対してなされ得ることは、当業者に明白であろう。開示の範囲は、特許請求の範囲およびこれらに記載されたものの均等物によって示されるものであり、明細書および例は、例示的な実施形態に過ぎないと見なされることが意図されている。

【産業上の利用可能性】

【００５１】

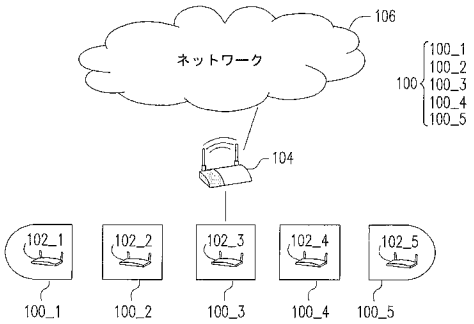
本発明は、車両ネットワーク全体の伝送効率を改善するために使用することができる。

【符号の説明】

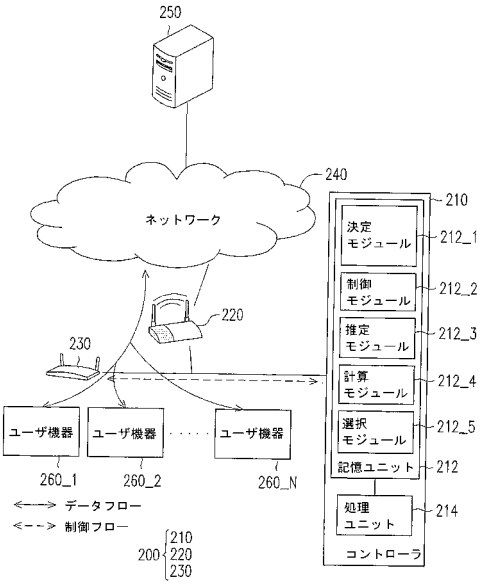
【００５２】

１００　・・・　列車
１００＿１～１００＿５　・・・　車両
１０２＿１～１０２＿５　・・・　アクセスポイント
１０４、２２０　・・・　ゲートウェイ
１０６　・・・　ネットワーク
２００、４００、５００　・・・　ネットワークシステム
２１０、４１０、５１０　・・・　コントローラ
２１２　・・・　記憶ユニット
２１２＿１　・・・　決定モジュール
２１２＿２　・・・　制御モジュール
２１２＿３　・・・　推定モジュール
２１２＿４　・・・　計算モジュール
２１２＿５　・・・　選択モジュール
２３０　・・・　アクセスポイント
２４０　・・・　ネットワーク
２５０、４４０、５４０　・・・　認証サーバ
２６０＿１～２６０＿Ｎ　・・・　ユーザ機器
４２０＿１　・・・　第１のアクセスポイント
４２０＿２　・・・　第２のアクセスポイント
５２０　・・・　特定のアクセスポイント
Ｓ３１０～Ｓ３５０　・・・　ステップ

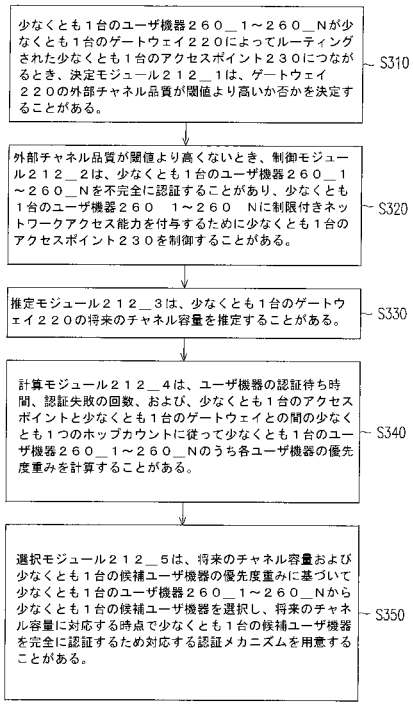
【図１】


106
ネットワーク
100
100_1
100_2
100_3
100_4
100_5
104
102_1
102_2
102_3
102_4
102_5
100_1
100_2
100_3
100_4
100_5

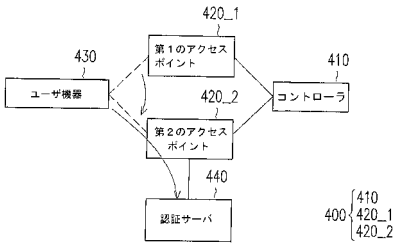
【図２】


250
240
ネットワーク
210
決定モジュール
212_1
制御モジュール
212_2
推定モジュール
212_3
計算モジュール
212_4
選択モジュール
212_5
記憶ユニット
212
処理ユニット
214
コントローラ
220
230
ユーザ機器
ユーザ機器
ユーザ機器
260_1
260_2
260_N
データフロー
制御フロー
200
210
220
230

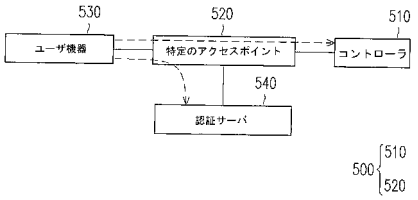
【図３】


少なくとも１台のユーザ機器２６０＿１～２６０＿Ｎが少なくとも１台のゲートウェイ２２０によってルーティングされた少なくとも１台のアクセスポイント２３０につながるとき、決定モジュール２１２＿１は、ゲートウェイ２２０の外部チャネル品質が閾値より高いか否かを決定することがある。
S310
外部チャネル品質が閾値より高くないとき、制御モジュール２１２＿２は、少なくとも１台のユーザ機器２６０＿１～２６０＿Ｎを不完全に認証することがあり、少なくとも１台のユーザ機器２６０　１～２６０　Ｎに制限付きネットワークアクセス能力を付与するために少なくとも１台のアクセスポイント２３０を制御することがある。
S320
推定モジュール２１２＿３は、少なくとも１台のゲートウェイ２２０の将来のチャネル容量を推定することがある。
S330
計算モジュール２１２＿４は、ユーザ機器の認証待ち時間、認証失敗の回数、および、少なくとも１台のアクセスポイントと少なくとも１台のゲートウェイとの間の少なくとも１つのホップカウントに従って少なくとも１台のユーザ機器２６０＿１～２６０＿Ｎのうち各ユーザ機器の優先度重みを計算することがある。
S340
選択モジュール２１２＿５は、将来のチャネル容量および少なくとも１台の候補ユーザ機器の優先度重みに基づいて少なくとも１台のユーザ機器２６０＿１～２６０＿Ｎから少なくとも１台の候補ユーザ機器を選択し、将来のチャネル容量に対応する時点で少なくとも１台の候補ユーザ機器を完全に認証するため対応する認証メカニズムを用意することがある。
S350

【図４】


420_1
第１のアクセスポイント
430
ユーザ機器
410
コントローラ
420_2
第２のアクセスポイント
440
認証サーバ
400
410
420_1
420_2

【図５】


530
520
510
ユーザ機器
特定のアクセスポイント
コントローラ
540
認証サーバ
500
510
520

フロントページの続き

(72)発明者　陳　志成
台灣台中市北屯區平心里５鄰瀋陽路三段１３號
(72)発明者　楊　人順
台灣新竹縣竹北市東海里２鄰東興路二段２８５巷１９弄１３號
(72)発明者　林　逸豪
台灣新竹市東區軍功里２４鄰建功一路１０４巷２０－４４號
(72)発明者　歐　尚▲チュン▼
台灣高雄市前鎮區衛忠路８０號

Ｆターム(参考) 5K067 AA28 BB05 BB21 DD11 DD57 EE02 EE10 EE16 EE44 FF02
FF05 FF16 HH22 HH23 HH36

【外国語明細書】
2017011673000001.pdf