(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2005-64921
(P2005-64921A)
(43)公開日　平成17年3月10日(2005.3.10)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 12/28	H04L 12/28	300Z	5K033
H04Q 7/38	H04B 7/26	109R	5K067

審査請求 未請求　請求項の数 6　OL　（全 12 頁）

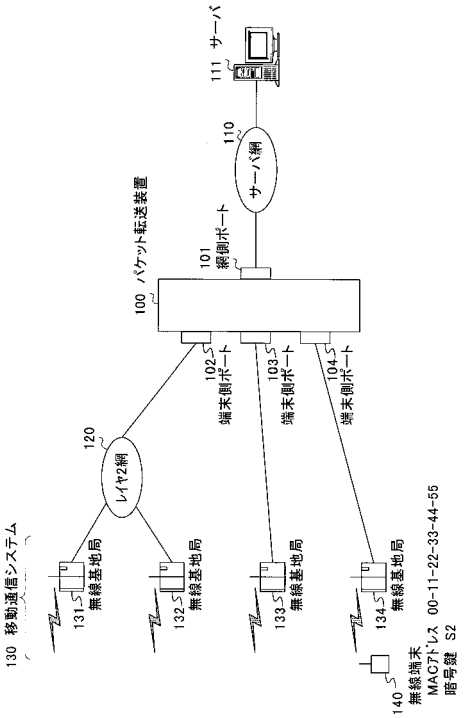
(21)出願番号　特願2003-293189(P2003-293189)
(22)出願日　平成15年8月13日(2003.8.13)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100105050
弁理士　鷲田　公一
(72)発明者　杉浦　幹人
神奈川県横浜市港北区綱島東四丁目３番１号　パナソニックモバイルコミュニケーションズ株式会社内
(72)発明者　飯野　聡
神奈川県横浜市港北区綱島東四丁目３番１号　パナソニックモバイルコミュニケーションズ株式会社内

最終頁に続く

(54)【発明の名称】パケット転送装置及び無線端末収容ネットワークシステム

(57)【要約】
【課題】　局所的な移動に対して安全かつ高速なハンドオーバーが可能で、かつ無線基地局の導入コストが低減できる無線端末収容ネットワークシステムを得ること。
【解決手段】　パケット転送装置１００の網側ポート１０１にはサーバ１１１が接側され、端末側ポート１０２～１０４には移動通信システム１３０が接続される。パケット転送装置１００は、端末側ポート１０２～１０４から受信した暗号化されたパケットを送信元ＭＡＣアドレスに対する暗号鍵を用いて復号化し、認証ができた当該パケットを網側ポートに送信する。また、認証できた前記パケットを受信した端末側ポート１０２～１０４とそのパケットの送信元ＭＡＣアドレスとを関連づけて記憶し、網側ポート１０１からパケットを受信したとき、その送信先ＭＡＣアドレスから対応する端末側ポート１０２～１０４を見つけ出して送信する。無線基地局１３１～１３４は、暗号機能を持たない安価な装置でよい。
【選択図】　図１



【特許請求の範囲】
【請求項１】
クライアントサーバ型の通信を実現するネットワークに配置され、端末側ポートにて授受されるパケットに対してＴＣＰ／ＩＰ通信が可能なレイヤ２処理を行うパケット転送装置であって、
前記端末側ポートから受信した暗号化されたパケットを送信元ＭＡＣアドレスに対する暗号鍵を用いて復号化し、復号化したパケットの認証ができたとき、当該パケットを網側ポートに送信する上り制御手段と、
認証できた前記パケットを受信した端末側ポートとそのパケットの送信元ＭＡＣアドレスとを関連づけて記憶し、網側ポートからパケットを受信したとき、その送信先ＭＡＣアドレスから対応する端末側ポートを見つけ出して送信する下り制御手段と、を具備することを特徴とするパケット転送装置。
【請求項２】
請求項１に記載のパケット転送装置と、前記パケット転送装置の網側ポートに接続されるサーバと、前記パケット転送装置の端末側ポートに接続される移動通信システムの無線基地局とで構成される無線端末収容ネットワークシステムであって、前記無線基地局に収容される無線端末は、無線送信するパケットを暗号化する機能を具備することを特徴とする無線端末収容ネットワークシステム。
【請求項３】
前記下り制御手段は、さらに網側ポートから受信したパケットを送信先ＭＡＣアドレスに対する暗号鍵を用いて暗号化し対応する端末側ポートに送信する機能、を具備することを特徴とする請求項１記載のパケット転送装置。
【請求項４】
請求項３に記載のパケット転送装置と、前記パケット転送装置の網側ポートに接続されるサーバと、前記パケット転送装置の端末側ポートに接続される移動通信システムの無線基地局とで構成される無線端末収容ネットワークシステムであって、前記無線基地局に収容される無線端末は、無線送信するパケットを暗号化する機能と無線受信するパケットを復号化する機能とを具備することを特徴とする無線端末収容ネットワークシステム。
【請求項５】
前記上り制御手段は、端末側ポートに収容される端末装置各々のＭＡＣアドレスと暗号通信を行うための暗号鍵とを組にして記憶する暗号鍵記憶手段と、端末側ポートから受信したパケットの送信元ＭＡＣアドレスをもとに前記暗号鍵記憶手段から暗号鍵を取得する暗号鍵検索手段と、前記暗号鍵検索手段が取得する暗号鍵を用いて受信したパケットのイーサネット（Ｒ）ペイロードを復号化する復号化手段と、前記復号化手段によって復号化されたパケットをもとにパケットの認証を行う認証手段と、前記認証手段が認証できたパケットを網側ポートに送信する上りパケット転送手段とを具備し、前記下り制御手段は、前記認証手段が認証できたパケットに対して送信元ＭＡＣアドレスとパケットを受信した端末側ポートとを組にして記憶する位置情報記憶手段と、網側ポートから受信したパケットの送信先ＭＡＣアドレスをもとに前記位置情報記憶手段から端末側ポートを取得する位置情報検索手段と、前記位置情報検索手段が取得する端末側ポートにパケットを転送する下りパケット転送手段とを具備することを特徴とする請求項１記載のパケット転送装置。
【請求項６】
前記下り制御手段は、さらに網側ポートから受信したパケットの送信先ＭＡＣアドレスをもとに前記暗号鍵記憶手段から暗号鍵を取得する暗号鍵検索手段と、前記暗号鍵検索手段が取得する暗号鍵を用いて網側ポートから受信したパケットのイーサネット（Ｒ）ペイロードを暗号化する暗号化手段とを具備することを特徴とする請求項５記載のパケット転送装置。
【発明の詳細な説明】
【技術分野】
【０００１】

本発明は、クライアントサーバ型の通信を実現するネットワークに配置され、端末側ポートにて授受されるパケットに対してＴＣＰ／ＩＰ通信が可能なレイヤ２処理を行うパケット転送装置及び前記パケット転送装置の端末側ポートに移動通信システムを収容した無線端末収容ネットワークシステムに関する。

【背景技術】

【０００２】

現在、インターネットでは、固定環境でのサービスのみならず、移動環境での使用をサポートするモバイルインターネットへの要望も高まっており、ＩＥＥＥ８０２．１１ｂに代表される無線ＬＡＮを利用したホットスポットサービスが開始されつつある。

【０００３】

ところで、無線通信を行う場合、一般に、無線区間でのセキュリティを確保する必要がある。無線区間でのセキュリティを保つために端末間で実際に利用する暗号鍵を交換してパケットの暗号化を行う方式として、ＲＦＣ２４１１に体系化されたドキュメント群に記載のＩＰｓｅｃ（インターネット・プロトコル・セキュリティ）や、無線基地局と無線端末との間で暗号通信を行うＩＥＥＥ８０２.１１記載のＷＥＰ（ワイヤード・イクイバレント・プライバシ）等が一般に使用されている。ＷＥＰに関してはセキュリティ面での脆弱性が指摘されている。

【０００４】

セキュリティを確保する通信方法に関しては、様々な方式が提案されており、その一例として、図６を参照して特許文献１に開示された通信方法について説明する。図６は、従来の無線端末収容ネットワークシステムの全体構成を示す図である。

【０００５】

図６に示す無線端末収容ネットワークシステムは、ＬＡＮ６０１と、ＬＡＮ６０１に直接接続されるインターネット６０２と、ＬＡＮ６０１に無線基地局６０３を介して接続される無線ＬＡＮ６０４とで構成されている。ＬＡＮ６０１には、認証サーバ６０５が設けられ、無線ＬＡＮ６０４には、無線基地局６０３と無線送受信を行う多数の無線端末６０６が収容されている。

【０００６】

特許文献１に開示された通信方法では、無線端末６０６は、通信を行うに当たって認証サーバ６０５に問い合わせを行うことにより、セッションキーを取得してパケット認証を行うことが可能になる。認証のフレームワークは、ＩＥＥＥ８０２．１ｘに示されている。

【０００７】

要するに、従来の無線端末収容ネットワークシステムは、ネットワーク内に認証サーバ６０５を設け、無線端末６０６が無線基地局６０３にアクセス許可を要求すると、無線基地局６０３が無線端末６０６にＩＤを要求し、それを認証サーバ６０５に転送する。ＩＤを認証した認証サーバ６０５は、無線基地局６０３に承諾メッセージと共に暗号鍵を送る。無線基地局６０３は、受け取った暗号鍵を無線端末６０６に通知する。これによって、無線端末６０６がネットワークにアクセスできるようになる構成である。

【特許文献１】特開２００２－１２４９５２号公報（図１）

【発明の開示】

【発明が解決しようとする課題】

【０００８】

上記のように従来の無線端末収容ネットワークシステムでは、認証サーバを利用し、初めに認証を行うことにより無線区間でのセキュリティを確保するようにしている。しかしながら、この方法では、無線端末が無線基地局間を移動するような場合、移動した後に認証サーバとパケットを交換してから暗号通信を開始すれば移動した後もセキュリティの確保は可能であるが、ハンドオーバーに時間を要する。

【０００９】

また、全ての無線基地局は、無線端末毎の暗号鍵を記憶する手段が必要になるので、導

入コストが高くなる。

【００１０】

さらに、ＩＰｓｅｃを使用すれば、ＩＰのサブネットが変わらない限りパケット認証を継続的に行うことは可能であるが、レイヤ２のＭＡＣアドレスの認証ができないという問題がある。

【００１１】

本発明は、かかる点に鑑みてなされたものであり、クライアントサーバ型の通信を実現するネットワークにおいて、端末側ポートにて授受されるパケットに対してＴＣＰ／ＩＰ通信が可能なレイヤ２処理を行う際にセキュリティを保ちながら端末側ポートの変更に高速に対応できるパケット転送装置、及び前記パケット転送装置を用いて構成した無線端末収容ネットワークシステム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】

【００１２】

本発明に係るパケット転送装置は、クライアントサーバ型の通信を実現するネットワークに配置され、端末側ポートにて授受されるパケットに対してＴＣＰ／ＩＰ通信が可能なレイヤ２処理を行うパケット転送装置であって、前記端末側ポートから受信した暗号化されたパケットを送信元ＭＡＣアドレスに対する暗号鍵を用いて復号化し、復号化したパケットの認証ができたとき、当該パケットを網側ポートに送信する上り制御手段と、認証できた前記パケットを受信した端末側ポートとそのパケットの送信元ＭＡＣアドレスとを関連づけて記憶し、網側ポートからパケットを受信したとき、その送信先ＭＡＣアドレスから対応する端末側ポートを見つけ出して送信する下り制御手段とを具備する構成を採る。

【００１３】

この構成によれば、パケット転送装置は、端末側ポートから受信した暗号化されたパケットを送信元ＭＡＣアドレスに対する暗号鍵を用いて復号化し、パケットの認証ができたとき、当該パケットを網側ポートに送信するので、送信元ＭＡＣアドレス毎、つまり端末装置毎に異なる暗号鍵を用いて復号化し、認証を採ることができ、レイヤ２レベルのセキュリティを保つことができる。また、認証できたパケットを受信した端末側ポートとそのパケットの送信元ＭＡＣアドレスとを関連づけて記憶するので、端末装置が端末側ポート間を移動しても安全確実に端末装置が存在する端末側ポートに送信することができる。

【００１４】

本発明に係る無線端末収容ネットワークシステムは、上記発明によるパケット転送装置と、前記パケット転送装置の網側ポートに接続されるサーバと、前記パケット転送装置の端末側ポートに接続される移動通信システムの無線基地局とで構成される無線端末収容ネットワークシステムであって、前記無線基地局に収容される無線端末は、無線送信するパケットを暗号化する機能を具備する構成を採る。

【００１５】

この構成によれば、パケット転送装置は、複数の無線基地局を介して無線端末と通信を行うので、広いエリアの無線端末と通信ができる。このとき、無線端末は、個別に記憶している暗号鍵を用いて送信するパケットを確実に暗号化でき、複数の無線基地局を収容するパケット転送装置が暗号化されたパケットを復号化するので、広いエリアをカバーするために複数必要となる無線基地局には暗号機能を持たない安価な装置を用いても、上り方向の無線区間のレイヤ２レベルでのセキュリティを保つことができる。また、無線端末が移動した先の無線基地局と速やかにレイヤ２レベルでのセキュリティを保つ通信を開始することができる。さらに、無線端末が無線基地局間を移動した場合にも下り方向の経路切り替えを高速に、かつ安全確実に行うことができる。

【００１６】

本発明に係るパケット転送装置は、上記の発明において、前記下り制御手段は、さらに網側ポートから受信したパケットを送信先ＭＡＣアドレスに対する暗号鍵を用いて暗号化し対応する端末側ポートに送信する機能を具備する構成を採る。

【００１７】

この構成によれば、パケット転送装置では、下り方向パケットに対して、端末が存在する端末側ポートに確実にパケットを送信できる上に、ＭＡＣアドレス毎、つまり端末装置毎に異なる暗号鍵を用いて暗号化することができる。

【００１８】

本発明に係る無線端末収容ネットワークシステムは、上記発明によるパケット転送装置と、前記パケット転送装置の網側ポートに接続されるサーバと、前記パケット転送装置の端末側ポートに接続される移動通信システムの無線基地局とで構成される無線端末収容ネットワークシステムであって、前記無線基地局に収容される無線端末は、無線送信するパケットを暗号化する機能と無線受信するパケットを復号化する機能とを具備する構成を採る。

【００１９】

この構成によれば、無線端末は個別に記憶している暗号鍵を用いて受信する自装置宛のパケットだけを確実に復号化できるので、サーバから送られてくる下り方向のパケットに対してレイヤ２レベルでの通信のセキュリティを保つことができる。また、無線端末が無線基地局間を移動した場合にも下り方向のレイヤ２レベルでの通信のセキュリティを保つことができる。

【００２０】

本発明に係るパケット転送装置は、上記の発明において、前記上り制御手段は、端末側ポートに収容される端末装置各々のＭＡＣアドレスと暗号通信を行うための暗号鍵とを組にして記憶する暗号鍵記憶手段と、端末側ポートから受信したパケットの送信元ＭＡＣアドレスをもとに前記暗号鍵記憶手段から暗号鍵を取得する暗号鍵検索手段と、前記暗号鍵検索手段が取得する暗号鍵を用いて受信したパケットのイーサネット（Ｒ）ペイロードを復号化する復号化手段と、前記復号化手段によって復号化されたパケットをもとにパケットの認証を行う認証手段と、前記認証手段が認証できたパケットを網側ポートに送信する上りパケット転送手段とを具備し、前記下り制御手段は、前記認証手段が認証できたパケットに対して送信元ＭＡＣアドレスとパケットを受信した端末側ポートとを組にして記憶する位置情報記憶手段と、網側ポートから受信したパケットの送信先ＭＡＣアドレスをもとに前記位置情報記憶手段から端末側ポートを取得する位置情報検索手段と、前記位置情報検索手段が取得する端末側ポートにパケットを転送する下りパケット転送手段とを具備する構成を採る。

【００２１】

この構成によれば、パケット転送装置では、暗号鍵記憶手段に、予め収容される端末装置各々のＭＡＣアドレスと暗号鍵とを組にして記憶するので、送信元ＭＡＣアドレス毎つまり端末装置毎に異なる暗号鍵を用いて復号化することができる。また、認証手段がイーサネット（Ｒ）ヘッダの送信元ＭＡＣアドレス、つまり端末装置のＭＡＣアドレスを含めて認証できたパケットをもとに、位置情報記憶手段は端末の位置情報である端末側ポートを記憶するので、下り方向の経路切り替えを速やかに、かつ安全確実に行うことができる。

【００２２】

本発明に係るパケット転送装置は、上記の発明において、前記下り制御手段は、さらに網側ポートから受信したパケットの送信先ＭＡＣアドレスをもとに前記暗号鍵記憶手段から暗号鍵を取得する暗号鍵検索手段と、前記暗号鍵検索手段が取得する暗号鍵を用いて網側ポートから受信したパケットのイーサネット（Ｒ）ペイロードを暗号化する暗号化手段とを具備する構成を採る。

【００２３】

この構成によれば、下り方向のパケットに対して暗号鍵検索手段は、パケットの送信先ＭＡＣアドレス、つまり端末装置のＭＡＣアドレスを用いて当該端末装置の暗号鍵を取得してパケットを暗号化するので、下り方向の通信に関しても端末単位でレイヤ２レベルでのセキュリティを保った通信ができる。

【発明の効果】

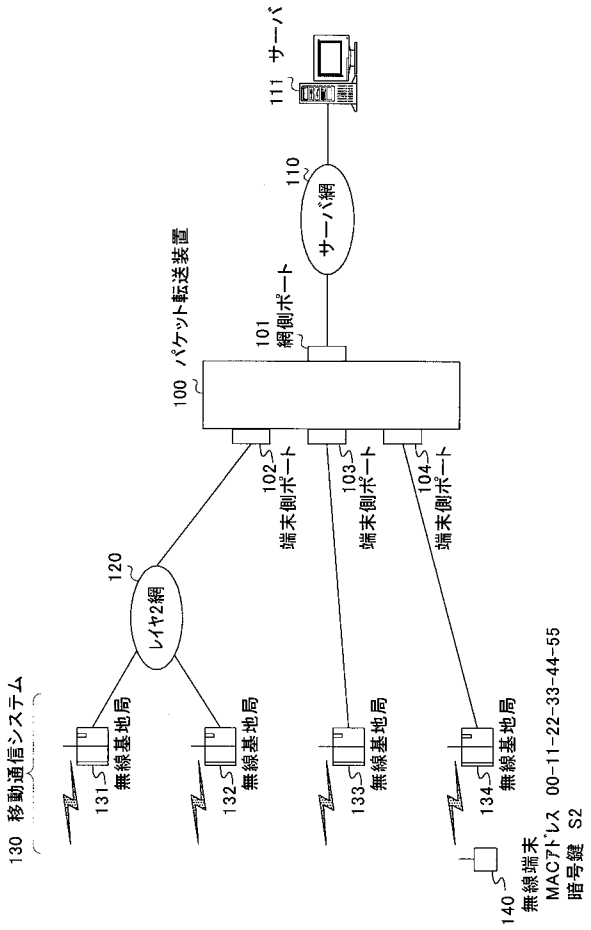
【００２４】
本発明によれば、クライアントサーバ型の通信を実現するネットワークにおいて、端末側ポートにて授受されるパケットに対してＴＣＰ／ＩＰ通信が可能なレイヤ２処理を行う際にセキュリティを保ちながら端末側ポートの変更に高速に対応できるパケット転送装置、及び前記パケット転送装置を用いて構成した無線端末収容ネットワークシステムを提供することができるので、無線基地局の導入コストを低減することができる。
【発明を実施するための最良の形態】
【００２５】
本発明の骨子は、クライアントサーバ型の通信を実現するネットワークに移動通信システムを接続していわゆるモバイルインターネットである無線端末収容ネットワークシステムを構築する場合に、ネットワーク上に端末側ポートにて授受されるパケットに対してＴＣＰ／ＩＰ通信が可能なレイヤ２処理を行うパケット転送装置を無線基地局とネットワークとの間に介在する形で配置し、このパケット転送装置に無線端末の移動に対してレイヤ２レベルでのセキュリティを保ちながら高速なハンドオーバーが行える機能を持たせ、無線基地局の導入コストを低減することである。
【００２６】
以下、本発明の実施の形態について、添付図面を参照して詳細に説明する。
【００２７】
図１は、本発明の一実施の形態に係る無線端末収容ネットワークシステムの全体構成を示す図である。図１に示す無線端末収容ネットワークシステムは、クライアントサーバ型の通信を実現するネットワークに配置されるパケット転送装置１００と、パケット転送装置１００の網側ポート１０１に例えばサーバ網１１０を介して接続されるサーバ１１１と、パケット転送装置１００の端末側ポート１０２～１０４に接続される移動通信システム１３０とで構成されている。
【００２８】
移動通信システム１３０では、無線基地局１３１，１３２が、レイヤ２網１２０を介してパケット転送装置１００の端末側ポート１０２に接続され、無線基地局１３３，１３４が、パケット転送装置１００の端末側ポート１０３，１０４に直接接続されている。そして、無線端末１４０が無線基地局１３４の配下に存在するものとしている。
【００２９】
無線端末１４０は、ＭＡＣアドレス“００－１１－２２－３３－４４－５５”を持ち、さらに暗号通信を行うための暗号鍵Ｓ２を保持している。無線端末１４０は、この暗号鍵Ｓ２を用いて無線送信するパケットを暗号化することができ、さらに無線受信するパケットが暗号化されている場合は復号化することができるようになっている。
【００３０】
無線基地局１３１～１３４は、無線端末１４０とパケット転送装置１００との間のパケット通信を中継するのみであり、暗号通信の手順に介在することはしない。
【００３１】
パケット転送装置１００は、端末側ポート１０２～１０４にて授受されるパケットに対してＴＣＰ／ＩＰ通信が可能なレイヤ２処理を行うが、図２に示す構成によって、無線端末１４０の移動に対してレイヤ２レベルでのセキュリティを保ちながら高速なハンドオーバーが行えるようになっている。
【００３２】
図２は、図１に示すパケット転送装置１００の構成例を示すブロック図である。図２において、パケット転送装置１００は、例えば図１に示したように、サーバ１１１が接続される網側ポート１０１と、移動通信システム１３０が接続される３つの端末側ポート１０２～１０４とを備え、それらの間に暗号通信に関わる要素として、暗号鍵記憶部２００，暗号鍵検索部２０１，復号化部２０２，認証部２０３，上りパケット転送部２０４，位置情報記憶部２０５，位置情報検索部２０６，下りパケット転送部２０７，及び暗号化部２０８を備えている。

【００３３】
暗号鍵記憶部２００は、端末側ポート１０２～１０４に収容される無線端末１４０それぞれが保持するＭＡＣアドレスと、暗号通信を行うための暗号鍵とを組にして予め記憶している。図３は、図２に示す暗号鍵記憶部２００の構成例を示す図であるが、図３に示すように、ＭＡＣアドレスの記憶欄３０１と暗号鍵の記憶欄３０２とが設けられ、ＭＡＣアドレスと暗号鍵とが１対１対応で格納されている。
【００３４】
暗号鍵検索部２０１は、端末側ポート１０２～１０４から受信したパケットの送信元ＭＡＣアドレスを元に暗号鍵記憶部２００を検索し対応する暗号鍵を取得し、復号化部２０２に与える。また、暗号鍵検索部２０１は、網側ポート１０１から受信したパケットの送信先ＭＡＣアドレスを元に暗号鍵記憶部２００を検索し対応する暗号鍵を取得し、暗号化部２０８に与えるようになっている。
【００３５】
復号化部２０２は、暗号鍵検索部２０１が取得した暗号鍵を用いて端末側ポート１０２～１０４から受信したパケットのイーサネット（Ｒ）ペイロードを復号化し、認証部２０３に与える。また、暗号化部２０８は、暗号鍵検索部２０１が取得した暗号鍵を用いて網側ポート１０１から受信したパケットのイーサネット（Ｒ）ペイロードを暗号化し、位置情報検索部２０６に与えるようになっている。
【００３６】
図５は、イーサネット（Ｒ）フレームのフォーマットと暗号化の対象を示す図である。図５に示すように、イーサネット（Ｒ）フレーム５００は、送信先アドレス部５０１と、送信元アドレス部５０２と、フレームのタイプが挿入されるＴＹＰ部５０３と、データが挿入されるペイロード部５０４と、誤りチェックを行うＦＣＳ（Ｆｒａｍｅ　Ｃｈｅｃｋ　Ｓｅｑｕｅｎｃｅ）部５０５とで構成され、ペイロード部５０４が暗号化の対象となっている。
【００３７】
認証部２０３は、復号化部２０２にて復号化されたパケットを元にパケットの認証を行い、認証できたパケットを上りパケット転送部２０４と位置情報記憶部２０５とに与えるようになっている。
【００３８】
上りパケット転送部２０４は、認証部２０３が認証できたパケットを網側ポート１０１に送信する。一方、位置情報記憶部２０５は、認証部２０３が認証できたパケットに対して送信元ＭＡＣアドレスと、そのパケットを受信した端末側ポート１０２～１０４とを組にして記憶する。
【００３９】
図４は、図２に示す位置情報記憶部２０５の構成例を示す図である。図４に示すように、ＭＡＣアドレスの記憶欄４０１と端末側ポートの記憶欄４０２とが設けられ、ＭＡＣアドレスと端末側ポートとが１対１対応で登録される。すなわち、位置情報記憶部２０５は、認証部２０３にて認証できたパケットが既登録（図４（１））であるときは、何もしないが、未登録であるときは、図４（２）に示すように、新規の登録を行うようになっている。
【００４０】
位置情報検索部２０６は、網側ポート１０１から受信したパケットの送信先ＭＡＣアドレスを元に位置情報記憶部２０５から対応する端末側ポートを取得して下りパケット転送部２０７に与える。下りパケット転送部２０７は、位置情報検索部２０６が取得した端末側ポート１０２～１０４にパケットを転送するようになっている。
【００４１】
次に、図１～図５に参照して、以上のように構成される無線端末収容ネットワーク上での通信手順について説明する。無線端末１４０は、ＭＡＣアドレス“００－１１－２２－３３－４４－５５”を持ち、さらに暗号通信を行うための暗号鍵Ｓ２を保持している。

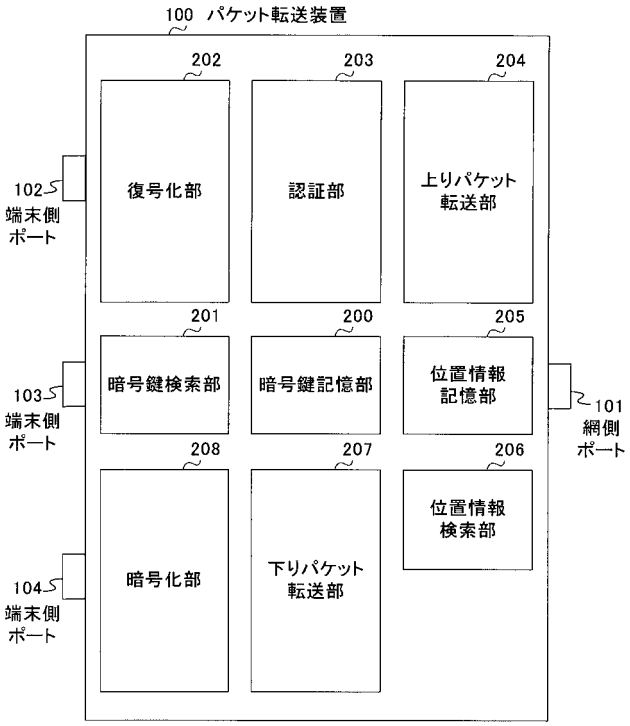
【００４２】
無線端末１４０は、サーバ１１１と通信を行う場合、図５に示すペイロード部５０４のペイロードを暗号化したパケットを無線送信する。このパケットは無線基地局１３４を介してパケット転送装置１００の端末側ポート１０４に受信される。
【００４３】
パケット転送装置１００では、端末側ポート１０４からパケットを受信すると、暗号鍵検索部２０１がそのパケットのイーサネット（Ｒ）ヘッダ（暗号化されていない）の送信元ＭＡＣアドレス００－１１－２２－３３－４４－５５によって無線端末１４０用の暗号鍵Ｓ２を取得する。
【００４４】
復号化部２０２は、暗号鍵検索部２０１が取得した暗号鍵Ｓ２をもとに暗号化されているペイロード部５０４を復号化する。認証部２０３は、復号化されたパケットをもとにパケットの認証を行う。認証が成功した場合、上りパケット転送部２０４は、網側ポート１０１に復号化されたパケットを転送する。一方、位置情報記憶部２０５は、送信元ＭＡＣアドレス００－１１－２２－３３－４４－５５と端末側ポート１０４の組とを新たに記憶する（図４（２））。
【００４５】
また、サーバ１１１が無線端末１４０にパケットを送信する場合、そのパケットは、サーバ網１１０を介してパケット転送装置１００の網側ポート１０１に受信される。
【００４６】
パケット転送装置１００では、網側ポート１０１からパケットを受信すると、暗号鍵検索部２０１が、そのパケットのイーサネット（Ｒ）ヘッダに在る送信先ＭＡＣアドレス００－１１－２２－３３－４４－５５よって無線端末１４０用の暗号鍵Ｓ２を取得する。暗号化部２０８は、ペイロード部５０４を暗号化する。また、位置情報検索部２０６は、そのパケットのイーサネット（Ｒ）ヘッダに在る送信先ＭＡＣアドレス００－１１－２２－３３－４４－５５よって無線端末１４０存在する端末側ポート１０４を取得する。下りパケット転送部２０７は、取得した端末側ポート１０４に暗号化したパケットを送信する。
【００４７】
端末側ポート１０４から送信された暗号化されたパケットは、無線端末１４０が受信し、イーサネット（Ｒ）フレームのペイロード部５０４を保持している暗号鍵Ｓ２を用いて復号化する。
【００４８】
このような手順で通信すると、無線端末単位で暗号鍵を保持しているので、無線端末単位での無線区間のセキュリティを保つことが可能になる。同時に、パケット転送装置は、パケットの認証が成功したときに位置情報記憶部に無線端末の位置を示す端末側ポートを記憶するので、収容する無線基地局間を無線端末が移動した場合でも、下りの経路切り替えをセキュリティを保ったまま瞬時に行うことができる。
【００４９】
また、パケット転送装置では、無線端末のＭＡＣアドレスと暗号鍵を対応付けて記憶しているので、ＭＡＣアドレスの認証が可能になり、レイヤ２レベルでのなりすましが防止できる。また、複数の無線基地局を収容するパケット転送装置が暗号通信を終端するので、広いエリアをカバーするために複数必要となる無線基地局には、暗号機能を持たない安価な装置を用いても無線区間のセキュリティを保つことが可能になる。
【００５０】
ここで、暗号化の方法としては、ＷＥＰを用いてもよいし、ＩＰｓｅｃにて用いられるようなアルゴリズム（ＡＥＳ、トリプルＤＥＳ等）を用いてもよい。また、パケット認証の方法としては、簡単な方法として暗号化されたパケットを復号化して図５に示すイーサネット（Ｒ）フレームのＦＣＳ部５０５を利用してもよい。あるいは、暗号化の際にＩＰｓｅｃ等で用いられるＭＤ（Ｍｅｓｓａｇｅ　Ｄｉｇｅｓｔ）等の認証用の特別なヘッダを付加して確実に行ってもよい。

【産業上の利用可能性】
【００５１】
本発明は、クライアントサーバ型の通信を実現するネットワークにおいて、端末側ポートにて授受されるパケットに対してＴＣＰ／ＩＰ通信が可能なレイヤ２処理を行う際にセキュリティを保ちながら端末側ポートの変更に高速に対応できるパケット転送装置、及び前記パケット転送装置を用いて構成した無線端末収容ネットワークシステムを可能にすることである。
【図面の簡単な説明】
【００５２】
【図１】本発明の一実施形態に係る無線端末収容ネットワークシステムの全体構成を示す図
【図２】図１に示すパケット転送装置の構成例を示すブロック図
【図３】図２に示す暗号鍵記憶部の構成例を示す図
【図４】図２に示す位置情報記憶部の構成例を示す図
【図５】イーサネット（Ｒ）フレームのフォーマットと暗号化の対象を示す図
【図６】従来の無線端末収容ネットワークシステムの全体構成を示す図
【符号の説明】
【００５３】
１００　パケット転送装置
１０１　網側ポート
１０２～１０４　端末側ポート
１１０　サーバ網
１１１　サーバ
１２０　レイヤ２網
１３０　移動通信システム
１３１～１３４　無線基地局
１４０　無線端末
２００　暗号鍵記憶部
２０１　暗号鍵検索部
２０２　復号化部
２０３　認証部
２０４　上りパケット転送部
２０５　位置情報記憶部
２０６　位置情報検索部
２０７　下りパケット転送部
２０８　暗号化部
５００　イーサネット（Ｒ）フレーム
５０４　ペイロード部

【図１】



【図２】



【図３】

301 MACアドレス	302 暗号鍵
00-11-22-33-44-11	S1
00-11-22-33-44-55	S2
00-11-22-33-44-BB	S3
....	

【図４】

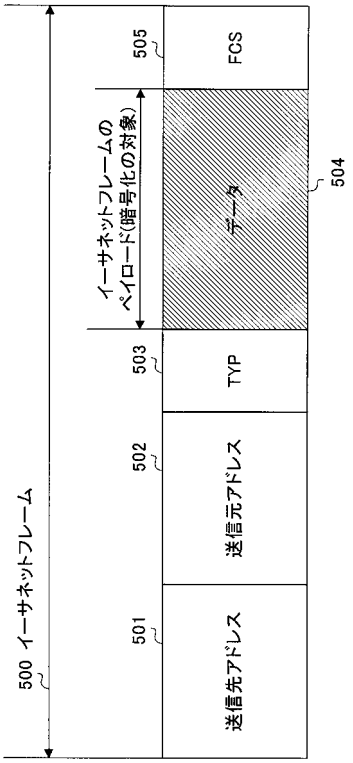
(1)

401 MACアドレス	402 端末側ポート
22-44-66-88-AA-CC	2
11-22-33-44-55-66	1
....	

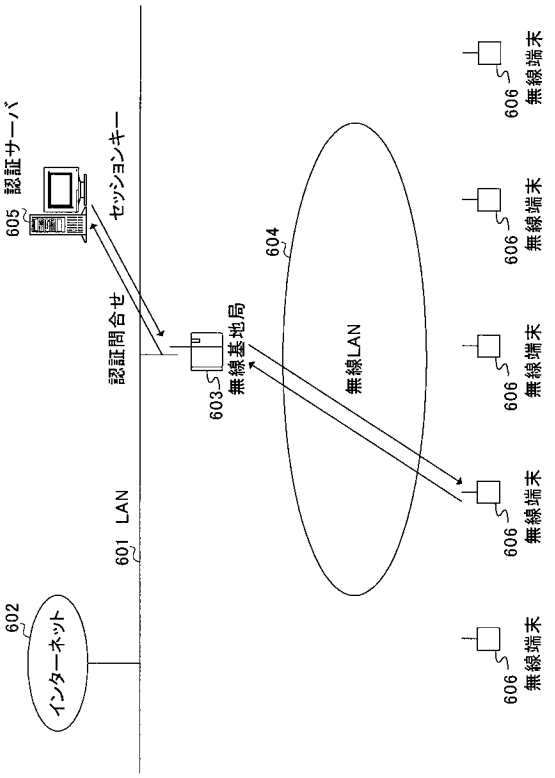
(2)

401 MACアドレス	402 端末側ポート
22-44-66-88-AA-CC	2
11-22-33-44-55-66	1
....	
00-11-22-33-44-55	3

【図５】



【図６】


認証サーバ
605
セッションキー
認証問合せ
LAN
601
インターネット
602
603
無線基地局
604
無線LAN
606
無線端末

フロントページの続き

(72)発明者　石田　寛史
神奈川県横浜市港北区綱島東四丁目３番１号　パナソニックモバイルコミュニケーションズ株式会社内

Ｆターム(参考) 5K033 AA04 AA08 CC01 DA17 DB14 DB16 DB18 DB19 EC03
5K067 AA30 AA35 BB04 BB21 CC08 DD11 DD41 EE02 EE10 EE16
FF02 HH36