(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2007-13386
(P2007-13386A)
(43)公開日　平成19年1月18日(2007.1.18)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/28	(2006.01)	H04L	12/28	300M	5K033
		H04L	12/28	307	

審査請求 未請求　請求項の数 11　ＯＬ　（全 31 頁）

(21)出願番号　特願2005-189543 (P2005-189543)
(22)出願日　平成17年6月29日 (2005.6.29)

（特許庁注：以下のものは登録商標）
１．Ｂｌｕｅｔｏｏｔｈ

（出願人による申告）国等の委託研究の成果に係る特許出願（平成１６年度独立行政法人情報処理推進機構「２００４年度次世代ソフトウェア開発事業（セキュアなモバイル＆ＡｄＨｏｃ通信・情報管理機能の開発）」委託研究、産業活力再生特別措置法第３０条の適用を受けるもの）

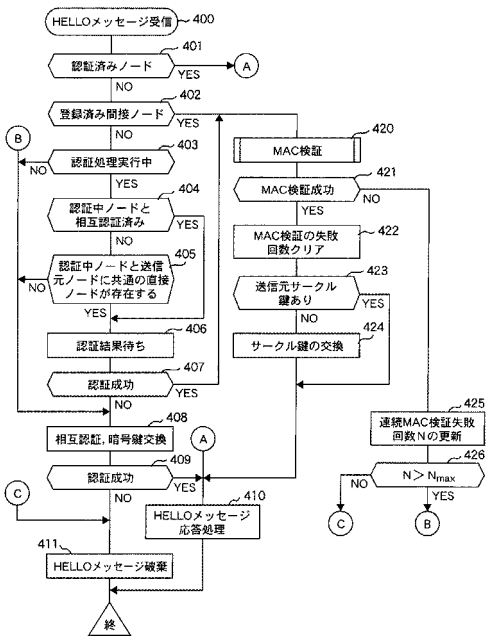
(71)出願人　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　110000350
ポレール特許業務法人
(72)発明者　安藤　英里子
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
(72)発明者　石田　修一
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

最終頁に続く

(54)【発明の名称】アドホックネットワーク用の通信端末および通信制御方法

(57)【要約】
【課題】　各通信端末が最寄りの通信端末と公開鍵を用いて相互認証を行うアドホックネットワークにおいて、相互認証の実行回数を低減できる通信端末と通信制御方法を提供する。
【解決手段】　定期的に生成した制御メッセージに、同一グループに属した各通信端末が共有する暗号鍵でもって検証可能な認証コード（ＭＡＣ）を付加して送信する送信制御メッセージ処理部と、他の通信端末からＭＡＣ情報付き制御メッセージを受信した時、送信元通信端末との間で実行すべき相互認証のための所定の通信手順に代えて、該受信メッセージの付されたＭＡＣの正当性を検証し、検証結果に応じて、上記受信メッセージの破棄、または受信メッセージの内容に応じた処理を実行する受信制御メッセージ処理部とを有するアドホックネットワーク用の通信端末。
【選択図】　図１０

図　１０



【特許請求の範囲】
【請求項１】
無線信号の伝播範囲内に位置した直接通信可能な通信端末を最初の中継ノードとして、同一グループに属した各通信端末が、遠隔位置にある他の通信端末と間接的に通信可能なアドホックネットワーク用の通信端末であって、
定期的に生成した制御メッセージに、上記グループに属した各通信端末が共有する暗号鍵でもって検証可能なメッセージ認証コード（以下、ＭＡＣと言う）を付加し、ＭＡＣ情報付き制御メッセージとして送信する送信制御メッセージ処理部と、
他の通信端末からＭＡＣ情報付き制御メッセージを受信した時、該受信メッセージの送信元通信端末との間で実行すべき相互認証のための所定の通信手順に代えて、該受信メッセージの付されたＭＡＣの正当性を検証し、検証結果に応じて、上記受信メッセージの破棄、または受信メッセージの内容に応じた処理を実行する受信制御メッセージ処理部とを有することを特徴とする通信端末。
【請求項２】
無線信号の伝播範囲内に位置した直接通信可能な通信端末を最初の中継ノードとして、同一グループに属した各通信端末が、遠隔位置にある他の通信端末と間接的に通信可能なアドホックネットワーク用の通信端末であって、
定期的に生成した制御メッセージに、アドホックネットワーク全体で有効となる暗号鍵（以下、アドホック鍵と言う）で該制御メッセージを暗号化して得られたメッセージ認証コード（以下、ＭＡＣと言う）を付加し、ＭＡＣ情報付き制御メッセージとして送信する送信制御メッセージ処理部と、
直接通信可能な相互認証済みの通信端末の識別子を直接ノード識別子として記憶する直接ノード情報テーブルと、
間接通信可能な通信端末の識別子を間接ノード識別子として記憶する間接ノード情報テーブルと、
他の通信端末からＭＡＣ情報付き制御メッセージを受信した時、該受信メッセージが示す送信元識別子が上記直接ノード情報テーブルに登録済みの場合は、該受信メッセージの内容に応じた処理を実行し、上記送信元識別子が上記間接ノード情報テーブルに登録済みの場合は、該受信メッセージの付されたＭＡＣの正当性を検証し、上記送信元識別子が上記直接ノード情報テーブルと間接ノード情報テーブルの何れにも未登録の場合は、上記受信メッセージの送信元との間で相互認証のための所定の通信手順を実行し、上記相互認証またはＭＡＣ検証に失敗した時は上記受信メッセージを破棄し、上記相互認証またはＭＡＣ検証に成功した時は受信メッセージの内容に応じた処理を実行する受信制御メッセージ処理部とを有することを特徴とする通信端末。
【請求項３】
前記制御メッセージが、該制御メッセージの送信元端末と直接的な通信が可能で、既に認証済みの少なくとも１つの通信端末の識別子を示す直接ノードリストを含み、
前記受信制御メッセージ処理部が、前記受信メッセージが示す送信元識別子が、前記直接ノード情報テーブルと間接ノード情報テーブルの何れにも未登録の場合、他の通信端末との間で相互認証手順を実行中でなければ、上記受信メッセージの送信元端末との間で相互認証のための通信手順を開始し、他の通信端末との間で相互認証手順を実行中であれば、該他の通信端末から受信した制御メッセージの直接ノードリストに、今回受信した制御メッセージの送信元端末の識別子が存在するか否かを判定し、存在していなければ、上記受信メッセージの送信元端末との間で相互認証のための通信手順を開始し、存在していれば、実行中の相互認証の結果を待つことを特徴とする請求項２に記載の通信端末。
【請求項４】
前記他の通信端末から受信した制御メッセージの直接ノードリストに、今回受信した制御メッセージの送信元端末の識別子が存在しなかった場合に、前記受信制御メッセージ処理部が、上記他の通信端末から受信した制御メッセージの直接ノードリストと今回受信した制御メッセージの直接ノードリストとに共通する第３の通信端末識別子が存在するか否

かを判定し、共通する第３端末識別子が存在しなければ、上記受信メッセージの送信元端末との間で相互認証のための通信手順を開始し、存在していれば、実行中の相互認証の結果を待つことを特徴とする請求項３に記載の通信端末。

【請求項５】

前記受信制御メッセージ処理部が、前記結果待ちとなっていた相互認証に成功した場合は、前記受信メッセージに付されたＭＡＣの正当性を検証し、上記相互認証に失敗した場合は、上記受信メッセージの送信元との間で相互認証のための所定の通信手順を実行することを特徴とする請求項３または請求項４に記載の通信端末。

【請求項６】

前記ＭＡＣ情報付き制御メッセージが、前記ＭＡＣに付随する情報として、該ＭＡＣの生成に適用されたアドホック鍵の識別子を含み、

前記受信制御メッセージ処理部が、受信した制御メッセージに付加されたアドホック鍵識別子と対応したアドホック鍵を適用して受信メッセージを暗号化し、該暗号化の結果と上記ＭＡＣとを照合することによって、該ＭＡＣの正当性を検証することを特徴とする請求項１～請求項５の何れかに記載された通信端末。

【請求項７】

最新のアドホック鍵と該アドホック鍵の識別子とを示す第１テーブルと、

上記最新のアドホック鍵以外で、アドホックネットワークに存在可能な少なくとも１つのアドホック鍵と該アドホック鍵の識別子とを示す第２テーブルとを有し、

前記送信制御メッセージ処理部が、上記第１、第２テーブルが示すアドホック鍵に従って生成した複数のＭＡＣと、各アドホック鍵の識別子とを付加した形で、前記ＭＡＣ情報付き制御メッセージを送信し、

前記受信制御メッセージ処理部が、受信した制御メッセージに付加されたアドホック鍵識別子に従って上記第１、第２テーブルからアドホック鍵を検索し、何れかのアドホック鍵による暗号化結果が受信メッセージに付されたＭＡＣと一致した場合に、上記受信メッセージを正当と判断することを特徴とする請求項６に記載された通信端末。

【請求項８】

無線信号の伝播範囲内に位置した直接通信可能な通信端末を中継ノードとして、同一グループに属した各通信端末が、遠隔位置にある他の通信端末と間接的に通信できるアドホックネットワークにおける通信制御方法であって、

各通信端末が、定期的に生成した制御メッセージから、上記グループに属した各通信端末が共有する暗号鍵でもって検証可能なメッセージ認証コード（以下、ＭＡＣと言う）を生成し、ＭＡＣ情報付き制御メッセージとして送信し、

他の通信端末からのＭＡＣ情報付き制御メッセージを受信した通信端末が、該受信メッセージの送信元通信端末との間で相互認証のための所定の通信手順を実行し、

上記相互認証に成功した通信端末が、相互認証済みの通信端末の識別子を直接ノード識別子、該受信メッセージから判明した間接通信可能な通信端末の識別子を間接ノード識別子として管理テーブルに記憶し、

上記管理テーブルに記憶された何れかの間接ノード識別子に一致する送信元識別子をもつＭＡＣ情報付き制御メッセージを受信した時、各通信端末が、送信元通信端末との間で実行すべき相互認証に代えて、該受信メッセージのＭＡＣの正当性を検証し、検証に失敗した時は、受信メッセージは破棄し、検証に成功した時は、受信メッセージの内容に応じた処理を実行することを特徴とする通信制御方法。

【請求項９】

各通信端末が、前記制御メッセージとして、自分と直接的な通信が可能で、既に認証済みの少なくとも１つの通信端末の識別子を示す直接ノードリストを含むメッセージを生成し、

他の通信端末からＭＡＣ情報付き制御メッセージを受信した通信端末が、該受信メッセージが示す送信元識別子が、前記管理テーブルに記憶された直接ノード識別子と間接ノード識別子の何れにも該当しなかった場合、他の通信端末との間で相互認証手順を実行中で

なければ、上記受信メッセージの送信元端末との間で相互認証のための通信手順を開始し、他の通信端末との間で相互認証手順を実行中であれば、該他の通信端末から受信した制御メッセージの直接ノードリストの内容から、今回受信した制御メッセージの送信元端末との間での相互認証の要否を判定することを特徴とする請求項８に記載の通信制御方法。

【請求項１０】

前記他の通信端末から受信した制御メッセージの直接ノードリストに、前記受信メッセージの送信元識別子が存在していなければ、該受信メッセージの送信元端末との間で相互認証のための通信手順を開始し、存在していれば、実行中の相互認証の結果を待つことを特徴とする請求項９に記載の通信制御方法。

【請求項１１】

前記他の通信端末から受信した制御メッセージの直接ノードリストに、今回受信した制御メッセージの送信元端末の識別子が存在しなかった場合に、上記他の通信端末から受信した制御メッセージの直接ノードリストと今回受信した制御メッセージの直接ノードリストとに共通する第３の通信端末識別子が存在するか否かを判定し、共通する第３端末識別子が存在しなければ、上記受信メッセージの送信元端末との間で相互認証のための通信手順を開始し、存在していれば、実行中の相互認証の結果を待つことを特徴とする請求項９に記載の通信制御方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、アドホックネットワーク用の通信端末および通信制御方法に関し、更に詳しくは、通信端末間の接続関係が流動的なアドホックネットワークにおいて、セキュリティオーバヘッドを軽減可能な通信端末および通信制御方法に関する。

【背景技術】

【０００２】

アドホックネットワーク（または無線マルチホップネットワーク）は、パソコン、ＰＤＡ、携帯電話など、携帯可能な複数の無線通信端末が、基本的には、アクセスポイントとして機能する固定的な通信装置の介在なしに、自律的に相互接続されたネットワークである。アドホックネットワークでは、互いに対等、且つ自律分散的に振舞う複数の無線通信端末が、無線信号の伝播範囲内に位置した他の通信端末（ノード）と制御メッセージを交信することによって、電話網、携帯電話網、あるいはインターネット等の既存の通信インフラストラクチャに依存することなく、通信ネットワークを構築する。但し、携帯電話網の無線基地局をアドホックネットワークの１つのノードとして、無線通信端末が、アドホックネットワークを介して無線基地局に接続され、例えば、インターネットをアクセスするネットワーク構成としてもよい。

【０００３】

アドホックネットワークに参加した各通信端末は、無線により直接通信可能な他の通信端末を中継ノードとして利用することにより、遠隔位置にある通信端末との間で、間接的なメッセージ通信またはデータパケット通信（無線マルチホップ通信）を行うことができる。

【０００４】

アドホックネットワークでは、或る特定のグループに属する通信端末だけを参加メンバーとして、閉域通信網を構成できる。この場合、グループ内での情報セキュリティを確保するためには、ネットワークに参加しようとする通信端末を認証し、特定グループに所属していない他の通信端末のネットワークへの接続を拒否する必要がある。また、アドホックネットワークの参加メンバー端末（通信ノード）の移動に伴って、通信端末間の接続関係に変化が生じた場合、移動した通信端末が、移動先のメンバー端末との間で、安全かつ円滑に通信を継続できるようにする必要がある。

【０００５】

閉域通信網におけるセキュリティの確保に関する従来技術として、例えば、特開２００

３－６９５８１号公報（特許文献１）には、正当な通信端末によるパケット中継機能を利用して、不正通信端末からの送信パケットによるトラヒックの増加を防止する方法が提案されている。

【０００６】

上記特許文献１では、アドホックネットワーク（無線マルチホップネットワーク）を構成する全ての通信端末で共有される第１の秘密情報と、２つの通信端末間で共有される第２の秘密情報とを使って、各無線端末が、送信パケット（通信メッセージ）から第１、第２の検査データを作成し、これらの検査データを付加した形でパケットを送信している。上記パケットを受信した無線端末は、自分が所持する第１の秘密情報を適用して、受信パケットに付された第１の検査データを検証し、検証結果が誤りの場合、受信パケットを破棄し、検証結果が正しい場合は、パケットの宛先をチェックする。無線端末は、受信パケットに宛先が自分宛でなければ、受信パケットを他の無線端末に転送し、宛先が自分宛の場合は、自分が所持する第２の秘密情報を適用して、第２の検査データを検証する。検証結果が誤りの場合、受信パケットを破棄し、検証結果が正しい場合は、受信パケットを受け取る。上記第１の秘密情報としては、認証済みの全ての無線端末が共有するネットワーク鍵が使用され、第２の秘密情報としては、パケットの送信元端末と宛先端末で共有される秘密鍵が使用される。

【０００７】

上記特許文献１では、ネットワーク鍵を未だ持っていない無線端末が、ネットワーク鍵取得のために認証用パケットを送信する場合、上記第１の秘密情報として、公開鍵暗号化方式における秘密鍵を使用し、この秘密鍵で生成された第１の検査データを相手装置が検証する際に必要となる公開鍵を送信パケットに証明書として添付することを提案している。認証用パケットには、第２の検査データは不要である。この場合、認証用パケットを受信した無線端末は、受信パケットに含まれる証明書の正当性を確認した後、証明書から抽出された公開鍵を適用して、上記第１の検査データを検証し、検証結果が誤りの場合、受信パケットを破棄し、検証結果が正しい場合は、宛先を判定して、上述した受信パケットの転送、または受信処理を実行する。

【０００８】

【特許文献１】特開２００３－６９５８１号公報

【発明の開示】

【発明が解決しようとする課題】

【０００９】

上記特許文献１の方法によれば、ネットワーク鍵または公開鍵暗号化方式における正しい秘密鍵と証明書をもっていない不正な無線端末から送信されたパケットは、これを最初に受信した無線端末で破棄されるため、不正パケットによるアドホックネットワーク内でのトラヒックの増加を防止できる。

【００１０】

然るに、上記従来技術では、ネットワークに新たに参加する無線端末へのネットワーク鍵の配布は、ネットワーク内の特定のノード、例えば、無線基地局が行っている。このため、アドホックネットワークに新たに参加しようとする各無線端末は、最初に、ネットワーク鍵の配布元となる特定ノード宛に認証用パケットを送信する必要があるが、新たな無線端末と上記特定ノードとの間に、認証用パケットの中継ノードとなる他の無線端末が存在していない状態では、無線端末がアドホックネットワークに参加できないという問題がある。例えば、複数の無線端末が無線基地局から離れた場所に位置した状態では、これらの無線端末は、無線基地局からネットワーク鍵を受け取れないため、これらの無線端末だけでローカルなアドホックネットワークを構築することができない。

【００１１】

本発明の目的は、ネットワーク鍵を配布する特定サーバ（認証用サーバ）の存在を必要とせずに、高セキュリティのアドホックネットワークを構築できる通信端末および通信制御方法を提供することにある。

本発明の他の目的は、認証処理のためのセキュリティオーバヘッドを軽減できるアドホックネットワーク用の通信端末および通信制御方法を提供することにある。

【課題を解決するための手段】

【００１２】

本発明のアドホックネットワークでは、各通信端末が、直接通信可能な位置にある相互認証済みの通信端末の識別子を直接ノード識別子として記憶しておき、直接ノード識別子として未だ記憶されていない新たな送信元識別子をもつ制御メッセージを受信した時、例えば、公開鍵暗号化方式を適用して、互いに同一のグループに所属した通信端末か否かの相互認証手順を実行し、その後にネットワーク内で必要となる通信メッセージの暗号鍵を相手端末と交換する。

【００１３】

上述した目的を達成するために、本発明によるアドホックネットワーク用の通信端末は、定期的に生成した制御メッセージに、同一グループに属した各通信端末が共有する暗号鍵でもって検証可能なメッセージ認証コード（以下、ＭＡＣと言う）を付加し、ＭＡＣ情報付き制御メッセージとして送信する送信制御メッセージ処理部と、

他の通信端末からＭＡＣ情報付き制御メッセージを受信した時、該受信メッセージの送信元通信端末との間で実行すべき相互認証のための所定の通信手順に代えて、該受信メッセージの付されたＭＡＣの正当性を検証し、検証結果に応じて、上記受信メッセージの破棄、または受信メッセージの内容に応じた処理を実行する受信制御メッセージ処理部とを有することを特徴とする。

【００１４】

更に詳述すると、本発明の通信端末は、無線信号の伝播範囲内に位置した直接通信可能な通信端末を最初の中継ノードとして、同一グループに属した各通信端末が、遠隔位置にある他の通信端末と間接的に通信可能なアドホックネットワーク用の通信端末であって、

定期的に生成した制御メッセージに、アドホックネットワーク全体で有効となる暗号鍵（以下、アドホック鍵と言う）で該制御メッセージを暗号化して得られたメッセージ認証コード（以下、ＭＡＣと言う）を付加し、ＭＡＣ情報付き制御メッセージとして送信する送信制御メッセージ処理部と、

直接通信可能な相互認証済みの通信端末の識別子を直接ノード識別子として記憶する直接ノード情報テーブルと、

間接通信可能な通信端末の識別子を間接ノード識別子として記憶する間接ノード情報テーブルと、

他の通信端末からＭＡＣ情報付き制御メッセージを受信した時、該受信メッセージが示す送信元識別子が上記直接ノード情報テーブルに登録済みの場合は、該受信メッセージの内容に応じた処理を実行し、上記送信元識別子が上記間接ノード情報テーブルに登録済みの場合は、該受信メッセージの付されたＭＡＣの正当性を検証し、上記送信元識別子が上記直接ノード情報テーブルと間接ノード情報テーブルの何れにも未登録の場合は、上記受信メッセージの送信元との間で相互認証のための所定の通信手順を実行し、上記相互認証またはＭＡＣ検証に失敗した時は上記受信メッセージを破棄し、上記相互認証またはＭＡＣ検証に成功した時は受信メッセージの内容に応じた処理を実行する受信制御メッセージ処理部とを有することを特徴とする。

【００１５】

ここで、本発明の通信端末が定期的に送信する制御メッセージは、例えば、ルーティングプロトコルに従って生成されるＨＥＬＬＯメッセージである。また、本発明において、ＭＡＣ生成に適用されるアドホック鍵は、各通信端末で自律的に生成され、暗号鍵配布メッセージによって他の通信端末に報知される。各通信端末は、他の通信端末からの暗号鍵配布メッセージの受信の都度、自分が持っているアドホック鍵と今回他の端末から通知されたアドホック鍵とを比較し、所定のルールで自分が使用すべき最新のアドホック鍵を選択し、受信した暗号鍵配布メッセージを他の通信端末に転送する。

【００１６】

本発明のアドホックネットワークでは、各通信端末が自律的にアドホック鍵を生成するため、或る時点では、アドホックネットワークに複数のアドホック鍵が存在することになる。但し、これらの複数のアドホック鍵は、上述した暗号鍵配布メッセージの受信の都度、実行される鍵選択の繰り返しによって、結果的には、ネットワーク全体で共通する１つの暗号鍵に収斂される。上記自律的なアドホック鍵の生成は、ネットワークにおけるセキュリティを維持するために、比較的長いインターバルで周期的に行われる。

【００１７】

本発明の１つの特徴は、上記ＭＡＣ情報付き制御メッセージ（ＨＥＬＬＯメッセージ）が、例えば、ＭＡＣに付随する情報として、該ＭＡＣの生成に適用されたアドホック鍵の識別子を含み、上記受信制御メッセージ処理部が、受信した制御メッセージに付加されたアドホック鍵識別子と対応したアドホック鍵を適用して受信メッセージを暗号化し、該暗号化の結果と上記ＭＡＣとを照合することによって、該ＭＡＣの正当性を検証するようにしたことにある。

【００１８】

本発明によるアドホックネットワークにおける通信制御方法は、

各通信端末が、定期的に生成した制御メッセージから、同一グループに属した各通信端末が共有する暗号鍵でもって検証可能なメッセージ認証コード（以下、ＭＡＣと言う）を生成し、ＭＡＣ情報付き制御メッセージとして送信し、

他の通信端末からのＭＡＣ情報付き制御メッセージを受信した通信端末が、該受信メッセージの送信元通信端末との間で相互認証のための所定の通信手順を実行し、

上記相互認証に成功した通信端末が、相互認証済みの通信端末の識別子を直接ノード識別子、該受信メッセージから判明した間接通信可能な通信端末の識別子を間接ノード識別子として管理テーブルに記憶し、

上記管理テーブルに記憶された何れかの間接ノード識別子に一致する送信元識別子をもつＭＡＣ情報付き制御メッセージを受信した時、各通信端末が、送信元通信端末との間で実行すべき相互認証に代えて、該受信メッセージのＭＡＣの正当性を検証し、検証に失敗した時は、受信メッセージは破棄し、検証に成功した時は、受信メッセージの内容に応じた処理を実行することを特徴とする。

【発明の効果】

【００１９】

本発明によれば、通信端末の移動に伴ってノード間の接続関係が変化した場合でも、アドホックネットワーク内の何れかの通信端末で既に認証済みの通信端末に関しては、各通信端末が相手端末からの受信メッセージのＭＡＣを検証することによって、時間のかかる相互認証手順を省略できるため、セキュリティオーバヘッドを大幅に低減できる。

【発明を実施するための最良の形態】

【００２０】

以下、本発明の実施の形態について、図面を参照して説明する。

【実施例１】

【００２１】

先ず、図１を参照して、本発明が適用されるアドホックネットワークの概要について説明する。

図１において、１０Ａ－１～１０Ａ－６は、特定のグループに属する通信端末であり、これらの通信端末は、相互の自律分散的な無線通信によって、一時的な閉域通信網であるアドホックネットワークを構成する。１０Ｂは、上記特定グループには属していない他の通信端末を示す。図示した例では、通信端末１０Ａ－２が、通信端末１０Ａ－１、１０Ａ－３、１０Ａ－４と接続関係にあり、１つのサークルＡ２を形成している。また、通信端末１０Ａ－４が、通信端末１０Ａ－２、１０Ａ－５、１０Ａ－６と接続関係にあり、別のサークルＡ４を形成している。後述するように、特定グループに属した２つの通信端末は、それぞれの無線信号到達範囲内に接近した場合に接続関係が発生するものとする。

【００２２】

例えば、通信端末１０Ａ－１と通信端末１０Ａ－３は、直接的な接続関係にはないが、それらに隣接した別の通信端末１０Ａ－２を中継ノードとして利用することによって、互いに通信できる。また、通信端末１０Ａ－１と通信端末１０Ａ－６も、それぞれに隣接する他の通信端末１０Ａ－２、１０Ａ－４を中継ノードとして利用することによって、互いに通信できる。従って、同一のグループに属したこれら複数の通信端末１０Ａ（１０Ａ－１～１０Ａ－６）は、グループ内の他の端末と相互に通信が可能であり、１つのアドホックネットワークを構成できる。

【００２３】

アドホックネットワークでは、各通信端末１０が移動端末（ＭＳ）からなり、通信端末の移動によってネットワークノードの接続関係が動的に変化する。例えば、通信端末１０Ａ－３と通信中の通信端末１０Ａ－１が移動し、新たな通信端末１０Ａ－４と接続関係になると、通信端末１０Ａ－１は、通信端末１０Ａ－４、１０Ａ－２を中継ノードとして、通信端末装置１０Ａ－３との通信を継続できる。ここでは、移動可能な複数の通信端末からなるアドホックネットワークを示しているが、本発明は、ネットワークの１つのノードとして、無線基地局を含み、各通信端末が無線基地局を介して既存の通信網に接続される網構成にも適用できる。

【００２４】

本発明は、上述したアドホックネットワークにおけるグループ内のセキュリティを確保することを目的としており、例えば、グループに属さない他の通信端末１０Ｂが、通信端末１０Ａ－１の無線信号到達範囲に入った場合、通信端末１０Ｂのアドホックネットワークへの接続を拒否する。

【００２５】

上記目的を達成するために、本発明では、各通信端末が、新たな通信端末との接続に際して相互に端末認証を行い、認証された通信端末のみにアドホックネットワークへの参加を許容する。本発明の特徴は、アドホックネットワークにおいて、端末間で通信される制御メッセージにメッセージ認証コード（Message Authentication Code：以下、ＭＡＣと言う）を付与しておき、端末移動に伴ってネットワーク内の端末接続関係に変化が生じた時、移動した通信端末と、該端末と新たな接続関係をもつ同一グループ内の別の通信端末とが、それぞれが受信する制御メッセージに付されたＭＡＣを検証することによって、互いに相手端末が同一アドホックネットワーク内で既に認証済みの端末であることを確認できるようにした点にある。

【００２６】

制御メッセージに付されるＭＡＣは、制御メッセージの内容を暗号鍵で暗号化したものである。ＭＡＣは、制御メッセージ全体を暗号鍵で暗号化する代わりに、制御メッセージの一部、あるいは圧縮された制御メッセージを暗号化したものでもよい。本発明によれば、端末移動に伴って新たな接続関係が生まれた時、ＭＡＣを検証することによって、２つの通信端末間での相互認証手順を省略できるため、セキュリティオーバヘッドを軽減できる。

【００２７】

本発明において、ＭＡＣの生成には、アドホックネットワークを構成する全ての通信端末に共有される暗号鍵が適用される。本明細書では、ＭＡＣの生成に適用される上記暗号鍵を「アドホック鍵」と言う。また、アドホックネットワークに含まれる各サークル内でのみ有効となる暗号鍵を「サークル鍵」と言う。各サークル内では、上記サークル鍵を使って、アドホック鍵の配布が行われる。また、通信端末間で送受信されるデータメッセージは、上記アドホック鍵によって暗号化される。

【００２８】

アドホックネットワークのルーティング方式については、ＩＥＴＦ　ＭＡＮｅｔ（Mobile Ad Hoc Networking）で標準化が検討されている。ここでは、１例として、標準化案の１つとして提案されているＯＬＳＲ（Optimized Link State Routing）を採用したアドホックネットワークについて説明するが、本発明は、他のルーティング方式の適用を妨げる

ものではない。尚、ＯＬＳＲ方式については、ｈｔｔｐ：／／ｗｗｗ．ｉｅｔｆ．ｏｒｇ／ｒｆｃ／ｒｆｃ３６２６．ｔｘｔに詳述されている。

【００２９】

図２（Ａ）は、ＯＬＳＲ方式の制御メッセージの１つであるＨＥＬＬＯメッセージのフォーマットを示す。ＨＥＬＬＯメッセージ２００は、メッセージ種別２０１と、送信元ノードＩＤ２０２と、直接ノードリスト２０３と、ステータスリスト２０４とからなる。

メッセージ種別２０１には、このメッセージがＨＥＬＬＯメッセージであることを示す識別子が設定される。送信元ノードＩＤ２０２は、メッセージの送信元となる通信端末の識別子を示す。直接ノードリスト２０３には、ＨＥＬＬＯメッセージの送信元ノードが把握している１ホップ範囲内のノード（直接ノード）の識別子が列挙される。

【００３０】

ステータスリスト２０４は、直接ノードリスト２０３が示す各直接ノードと送信元ノードとの間の通信状態を示している。ステータスリスト２０４における状態区分としては、例えば、送信元ノードと直接ノードとが相互にメッセージが届くことを確認済みの状態、送信元ノードが直接ノードからのメッセージが届くことのみを確認している状態、などがある。送信元ノードＩＤ２０２、直接ノードリスト２０３、ステータスリスト２０４における各ノード識別子としては、例えば、通信端末のＩＰアドレスが適用される。

【００３１】

ＯＬＳＲ方式では、各通信端末１０Ａ（１０Ａ－１～１０Ａ－６）は、ＨＥＬＬＯメッセージ２００を所定の周期、例えば、２秒毎に自律的にブロードキャストする。本発明では、各通信端末１０Ａは、破線２０５で示すように、ＭＡＣ情報２０５が付加されたＨＥＬＬＯメッセージ２００を送信する。ＭＡＣ情報２０５には、ＨＥＬＬＯメッセージの内容２０１～２０４をアドホック鍵で暗号化して得られた少なくとも１つのＭＡＣが含まれる。ＭＡＣ情報２０５の利用方法については、後で詳述する。

【００３２】

ＨＥＬＬＯメッセージは、無線電波の伝搬範囲内に存在する他の通信端末によって受信される。各通信端末は、他の通信装置からのＨＥＬＬＯメッセージを受信すると、該ＨＥＬＬＯメッセージの内容から、自ノードとは直接通信できないが、ＨＥＬＬＯメッセージの送信元ノードを中継ノードとして利用することによって、間接的に通信可能な通信端末の存在を認識できる。以下の説明では、間接通信において中継ノードとして利用される直接ノード（ＨＥＬＬＯメッセージの送信元ノード）を「ＭＰＲ（Multi Point Relay）ノード」と言う。ＨＥＬＬＯメッセージ２００のステータスリスト２０４には、各直接ノードが送信元ノードにとってＭＰＲノードであるか否かを示す状態情報も含まれている。

【００３３】

例えば、図１に示した通信端末１０Ａ－１にとって、通信端末１０Ａ－２は、これを中継ノードとして利用することによって、無線電波の伝搬範囲外にある通信端末１０Ａ－３と間接的に通信できる。この場合、通信端末１０Ａ－１が送信するＨＥＬＬＯメッセージのステータスリスト２０４には、直接ノードである通信端末１０Ａ－２の識別子と対応して、それがＭＰＲノードであることを示す状態情報が設定される。以下の説明において、ＨＥＬＬＯメッセージのステータスリスト２０４のうち、ＭＰＲノードとなる直接ノードを示すリスト部分を特に「ＭＰＲノードリスト」と定義する。

【００３４】

各通信端末１０Ａは、他の通信端末から受信したＨＥＬＬＯメッセージのステータスリスト２０４の内容から、自分がＭＰＲノードに指定されていることを認識すると、図２の（Ｂ）に示すＴＣ（Topology Control）メッセージ２１０を所定の周期、例えば、５秒毎に自律的にブロードキャストする。ＴＣメッセージを受信した各通信端末は、受信メッセージの送信元ノード識別子を自分のノード識別子に書き換えて、再送信（ＴＣメッセージ転送）する。上記ＴＣメッセージ転送の繰り返しによって、ＴＣメッセージの内容は、アドホックネットワーク上の全てのノードに伝搬する。

【００３５】

ＴＣメッセージ２１０は、図２（Ｂ）に示すように、メッセージ種別２１１と、送信元ノードＩＤ２１２と、生成元ノードＩＤ２１３と、ＭＰＲＳノードリスト２１４とからなる。ＴＣメッセージ２１０にも、ＨＥＬＬＯメッセージ２００と同様、メッセージ内容２１１～２１４をアドホック鍵で暗号化して得られた少なくとも１つのＭＡＣを含むＭＡＣ情報２１５が付加される。

メッセージ種別２１１は、このメッセージがＴＣメッセージであることを示す識別子が設定される。送信元ＩＤ２１２は、ＴＣメッセージの送信元ノードの識別子、生成元ノードＩＤ２１３は、ＴＣメッセージを生成したノードの識別子を示し、ＭＰＲＳノードリスト２１４には、生成元ノードをＭＰＲノードとして指定している直接ノードの識別子が設定されている。生成元ノードが、隣接する複数の直接ノードからＭＰＲノードとして指定されていた場合、ＭＰＲＳノードリスト２１４には、これら複数の直接ノードの識別子が設定される。

【００３６】

各通信端末１０Ａは、他のノードからＴＣメッセージを受信すると、上述したメッセージ転送の他に、該ＴＣメッセージの内容に応じたルーティングテーブルの更新処理を実行する。これによって、各通信端末は、アドホックネットワークのトポロジーの把握と、ルーティングテーブルに従った通信データの配信制御が可能となる。

【００３７】

図３は、通信端末１０Ａ（１０Ａ－１～１０Ａ－６）のハードウェア構成を示す。

通信端末１０Ａは、プロセッサ１０１と、該プロセッサが利用する各種のプログラムおよびデータが格納されるメモリ１０２と、入出力制御装置１０３と、液晶ディスプレイ等の表示装置１０４と、ポインティングデバイス、ボタンキー等の入力装置１０５と、無線モジュール１０６とからなる。このような無線モジュール１０６を備えた通信端末としては、例えば、携帯型の情報処理装置や携帯電話等の移動端末（ＭＳ）が代表的であるが、本発明に適用可能な通信端末のハードウェア構成は、ここに例示した構成に限定されるものではない。

【００３８】

無線モジュール１０６は、携帯電話網や無線ＬＡＮ等における通信プロトコル、例えば、Ｂｌｕｅｔｏｏｔｈ仕様に対応した無線通信動作を行う。無線ＬＡＮの仕様は、ＩＥＥＥ　８０２．１１：ANSI/IEEE Std 802.11 1999 Edition（http://www.ieee.org）等で標準化が進められており、Ｂｌｕｅｔｏｏｔｈの仕様は、粘pecifications of the Bluetooth System, Version1.0B煤ihttp://www.bluetooth.com）に開示されている。

【００３９】

図４は、通信端末１０Ａのメモリ１０２に用意される本発明に関係するソフトウェアの１例を示す。

メモリ１０２には、通信制御プログラム領域１１０と、ノードＩＤ記憶領域１２０と、アドホックネットワーク管理情報記憶領域１３０と、認証鍵記憶領域１４０と、ポリシー記憶領域１５０が定義される。

【００４０】

通信制御プログラム領域１１０には、例えば、メッセージ送受信制御ルーチン、アドホック接続制御ルーチン、相互認証ルーチン、鍵生成管理ルーチン、暗号処理ルーチン等のプログラムが記憶されている。各通信端末は、上記鍵生成管理ルーチンによって、自分が使用するアドホック鍵とサークル鍵を生成する。

【００４１】

ノードＩＤ記憶領域１２０には、通信端末１０Ａの識別情報、例えば、ＩＰアドレスやＭＡＣアドレス等が記憶される。認証鍵記憶領域１４０には、通信端末間での相互認証に必要となる公開鍵暗号方式の鍵情報、例えば、公開鍵、秘密鍵、認証局公開鍵などが記憶される。ポリシー記憶領域１５０には、通信制御プログラム領域１１０の各ルーチンが参照する各種ポリシー（鍵選択ポリシー、鍵生成ポリシー、認証ポリシー、緩和ポリシー等）が記憶されている。

【００４２】
アドホックネットワーク管理情報記憶領域１３０には、アドホックネットワークの構成に必要な情報テーブルとして、自ノード情報テーブル１３１、直接ノード情報テーブル１３３、間接ノード情報テーブル１３４、最新アドホック鍵情報テーブル１３５、存在可能アドホック鍵情報テーブル１３６、鍵情報メッセージ・シーケンス番号テーブル１３７、認証中ノードＩＤテーブル１３８、ＭＡＣ検証失敗回数テーブル１３９が記憶される。
【００４３】
自ノード情報テーブル１３１には、通信端末１０Ａ自身に関する情報として、図５（Ａ）に示すように、自ノードＩＤ１３１ａと、ＭＰＲフラグ１３１ｂと、サークル鍵１３１ｃと、サークル鍵生成時刻１３１ｄが記憶される。自ノードＩＤ１３１ａは、通信端末１０Ａの識別子であり、例えば、通信端末１０ＡのＩＰアドレスを示す。ＭＰＲフラグ１３１ｂは、自ノード（通信端末１０Ａ）が他の通信端末からＭＰＲノードとして指定されているか否かを示すフラグである。サークル鍵１３１ｃは、自ノードで生成したサークル鍵の値を示し、サークル鍵生成時刻１３１ｄは、該サークル鍵の生成時刻を示す。自ノード情報テーブル１３１には、これらの項目以外に、例えば、自ノードの状態を示すステータス情報等が含まれてもよい。
【００４４】
直接ノード情報テーブル１３３は、自ノードが直接通信可能な通信端末（直接ノード）と対応した複数のエントリからなり、各エントリは、図５（Ｂ）に示すように、直接ノードＩＤ１３３ａと、ＭＰＲ指定フラグ１３３ｂと、相互認証情報１３３ｃと、サークル鍵１３３ｄと、ステータス１３３ｅを示している。
【００４５】
ＭＰＲ指定フラグ１３３ｂは、直接ノードＩＤ１３３ａをもつノードが自ノードをＭＰＲノードとして指定しているか否かを示す。相互認証情報１３３ｃは、直接ノードが自ノードとの相互認証で使用した公開鍵や証明情報を示し、サークル鍵１３３ｄは、上記直接ノードが使用しているサークル鍵、ステータス１３３ｅは、自ノードと直接ノードとの間の通信状態を示す。直接ノード情報テーブル１３３は、これらの項目以外に、例えば、直接ノードとの間の通信に適用すべき鍵情報などが含まれていてもよい。
【００４６】
間接ノード情報テーブル１３４は、自ノードが間接的に通信が可能な通信端末（間接ノード）と対応した複数のエントリからなり、各エントリは、図５（Ｃ）に示すように、間接ノードＩＤ１３４ａと、経由ＭＰＲノード１３４ｂと、ホップ数１３４ｃと、証明情報１３４ｄを示している。経由ＭＰＲノード１３４ｂは、間接ノードＩＤ１３４ａをもつノード宛の送信データを最初に中継するＭＰＲノードの識別子を示し、経由ＭＰＲノードとして、複数のＭＰＲノードが指定されてもよい。ホップ数１３４ｃは、自ノードから宛先間接ノード迄のホップ数を示す。証明情報１３４ｄは、経由ＭＰＲノードとの通信に使用される証明データ、例えば、経由ＭＰＲノードから受信したＴＣメッセージに付加されていたＭＡＣを示す。間接ノード情報テーブル１３４には、これらの項目以外に、例えば、間接ノードの状態を示すステータス情報等が含まれていてもよい。
【００４７】
最新アドホック鍵情報テーブル１３５は、図６（Ａ）に示すように、自ノードで選択した最新のアドホック鍵１３５ａと、該アドホック鍵の識別子１３５ｂと、アドホック鍵の生成時刻１３５ｃを示す。鍵識別子１３５ｂは、例えば、ノードＩＤまたは生成時刻の一部あるいは全部を適用して、アドホックネットワーク全体で共通する所定のルールに従って生成される。
【００４８】
アドホックネットワークでは、通信データのセキュリティを維持するために、時間経過に従って、アドホック鍵が所定のルールで変更される。変更されたアドホック鍵が全ての通信装置に行き渡る迄には時間がかかるため、アドホックネットワークには、使用可能な複数のアドホック鍵が存在することになる。

存在可能アドホック鍵情報テーブル１３６は、アドホックネットワークに存在し得る複数のアドホック鍵を管理するためのデーブルであり、自ノードで過去に選択したアドホック鍵または直接ノードから受信したアドホック鍵と対応した複数のエントリからなる。各エントリは、図６（Ｂ）に示すように、アドホック鍵１３６ａと、鍵識別子１３６ｂと、生成時刻１３６ｃと、登録時刻１３６ｄを示している。

【００４９】

アドホック鍵１３６ａは、最新アドホック鍵情報テーブル１３５から消去された旧いアドホック鍵、または直接ノードから受信したアドホック鍵を示す。鍵識別子１３６ｂは、アドホック鍵１３６ａの識別子、生成時刻１３６ｃは、アドホック鍵１３６ａの生成時刻を示す。登録時刻１３６ｄは、アドホック鍵１３６ａのテーブル１３６への登録時刻を示し、有効期限の切れたアドホック鍵を抹消するために利用される。後述するように、登録時刻１３６ｄは、他の通信端末から受信したアドホック鍵情報メッセージの内容に応じて、現在時刻に変更される場合がある。

【００５０】

鍵情報メッセージ・シーケンス番号テーブル１３７は、図６（Ｃ）に示すように、アドホック鍵情報メッセージの送信元を示すノードＩＤ１３７ａと、アドホック鍵情報メッセージのシーケンス番号１３７ｂとの関係を示している。

認証中ノードＩＤテーブル１３８には、図６（Ｄ）に示すように、自ノードとの間で現在相互認証手順を実行中の相手端末を示すノードＩＤ１３８ａが記憶される。

ＭＡＣ検証失敗回数テーブル１３９は、図６（Ｅ）に示すように、ノードＩＤ１３９ａと対応して、ＭＡＣ検証の失敗回数１３９ｂを示している。相互認証に代わるＭＡＣ検証は、検証失敗回数１３９ｂが閾値回数に達する迄、繰り返して実行される。ＭＡＣ検証に成功すると、失敗回数１３９ｂの値がクリアされるため、失敗回数１３９ｂの値は、ＭＡＣ検証の連続的な失敗回数を示している。

【００５１】

上記アドホックネットワーク管理情報記憶領域１３０に用意されるテーブルは、ルーティング方式によって変化する。従って、図５、図６に示したテーブル構成は、本発明の１実施例に過ぎず、本発明を限定するものではない。

【００５２】

次に、図７～図１１参照して、通信端末間におけるＭＡＣ情報付きＨＥＬＬＯメッセージの送受信について説明する。

図７（Ａ）は、ＭＡＣ情報付きＨＥＬＬＯメッセージのフォーマットを示す。

ＭＡＣ情報付きＨＥＬＬＯメッセージ２００Ｍは、図２（Ａ）で説明したＨＥＬＬＯメッセージ２００に、ＭＡＣ情報２０５として、ＭＡＣ個数２０５Ａと、ＭＡＣリスト２０５Ｂと、アドホック鍵の識別子リスト２０５Ｃとを付加した構成となっている。

【００５３】

前述したように、各通信端末は、最新アドホック鍵情報テーブル１３５に記憶された最新アドホック鍵１３５ａの他に、存在可能アドホック鍵情報テーブル１３６にもアドホック鍵１３６ａを記憶している。ＭＡＣ個数２０５Ａは、最新アドホック鍵１３５ａと存在可能アドホック鍵情報テーブル１３６に記憶されたアドホック鍵の合計個数を示し、ＭＡＣリスト２０５Ｂには、これらのアドホック鍵を適用してＨＥＬＬＯメッセージ２００から生成された複数のＭＡＣが設定される。アドホック鍵識別子リスト２０５Ｃは、適用されたアドホック鍵の鍵識別子１３５ｂまたは１３６ｂを示す。

【００５４】

図７（Ｂ）は、ＭＡＣ情報付きＴＣメッセージのフォーマットを示す。

ＭＡＣ情報付きＴＣメッセージ２１０Ｍは、図２（Ｂ）で説明したＴＣメッセージ２１０に、ＭＡＣ情報として、ＭＡＣ個数２１５Ａと、ＭＡＣリスト２１５Ｂと、アドホック鍵の識別子リスト２１５Ｃとを付加した構成となっている。

【００５５】

ＭＡＣ個数２１５Ａは、最新アドホック鍵１３５ａと存在可能アドホック鍵情報テーブ

ル１３６に記憶されたアドホック鍵の合計個数を示し、ＭＡＣリスト２１５Ｂには、これらのアドホック鍵を適用してＴＣメッセージ２１０から生成された複数のＭＡＣが設定される。アドホック鍵識別子リスト２１５Ｃは、適用されたアドホック鍵の鍵識別子１３５ｂまたは１３６ｂを示す。

【００５６】

図８は、ＯＬＳＲ方式の各通信端末１０Ａ（プロセッサ１０１）が、タイマ割り込みによって定期的、例えば、２秒毎に実行するＨＥＬＬＯメッセージの送信ルーチン３００のフローチャートを示す。

ルーチン３００が起動されると、プロセッサ１０１は、ＨＥＬＬＯメッセージ２００を生成（ステップ３０１）した後、図９で詳述するＭＡＣ生成処理（３１０）を実行する。上記ＭＡＣ生成処理３１０によって、ＭＡＣ個数２０５Ａ、ＭＡＣリスト２０５Ｂ、アドホック鍵識別子リスト２０５Ｃを含むＭＡＣ情報２０５が生成される。プロセッサ１０１は、ＨＥＬＬＯメッセージ２００にＭＡＣ情報２０５を付加し（３０２）、ＭＡＣ情報付きのＨＥＬＬＯメッセージ２００Ｍを送信して（３０３）、このルーチン３００を終了する。

【００５７】

図９は、ＭＡＣ生成処理３１０の詳細フローチャートを示す。

ＭＡＣ生成処理３１０では、プロセッサ１０１は、最初に、存在可能アドホック鍵情報テーブル１３６の登録エントリ数（アドホック鍵の個数）をパラメータＩｍａｘに設定し、現在のテーブルエントリを指すためのパラメータｉと、ＭＡＣ個数２０５Ａをカウントするためのパラメータｊをそれぞれ初期値「１」に設定する（ステップ３１１）。次に、プロセッサ１０１は、最新アドホック鍵１３５ａを適用したＨＥＬＬＯメッセージの暗号化によって、最初のＭＡＣを生成し（３１２）、生成されたＭＡＣと使用鍵の識別子１３５ｂをＭＡＣリスト２０５Ｂとアドホック鍵識別子リスト２０５Ｃにそれぞれ追加する（３１３）。

【００５８】

プロセッサ１０１は、パラメータｉとＩｍａｘを比較し（３１４）、ｉ＞Ｉｍａｘでなければ、存在可能アドホック鍵情報テーブル１３６の第ｉエントリが示す登録時刻１３６ｄから、第ｉアドホック鍵の有効性をチェックする（３１５）。登録時刻からの経過時間が所定時間を越えていた場合、プロセッサ１０１は、第ｉアドホック鍵を無効と判断し、パラメータｉの値をインクリメントして（３１９）、ステップ３１４を実行する。

【００５９】

登録時刻からの経過時間が所定時間を越えていなければ、プロセッサ１０１は、第ｉアドホック鍵を有効と判断し、第ｉアドホック鍵を適用してＭＡＣを生成し（３１６）、パラメータｊの値をインクリメントして（３１７）、生成されたＭＡＣと使用鍵の識別子１３６ｂをＭＡＣリスト２０５Ｂとアドホック鍵識別子リスト２０５Ｃにそれぞれ追加する（３１８）。この後、プロセッサ１０１は、パラメータｉの値をインクリメントして（３１９）、ステップ３１４を実行する。ステップ３１４で、ｉ＞Ｉｍａｘとなった時、プロセッサ１０１は、パラメータｊの値をＭＡＣ個数２０５Ａとして設定し（３２０）、この処理３１０を終了する。

【００６０】

図１０は、各端末装置１０Ａ（プロセッサ１０１）が、他の端末からＨＥＬＬＯメッセージを受信した時に実行するＨＥＬＬＯメッセージ受信ルーチン４００のフローチャートを示す。

ＭＡＣ情報付きＨＥＬＬＯメッセージ２００Ｍを受信すると、プロセッサ１０１は、受信メッセージの送信元ノードが既に相互認証済みのノードか否かを判定する（４０１）。受信メッセージの送信元ノードＩＤ２０２が、直接ノード情報テーブル１３３に直接ノードＩＤ１３３ａとして登録済みで、且つ、ステータス１３３ｅが相互認証に成功したことを示していた場合は、プロセッサ１０１は、送信元ノードを相互認証済みノードと判断する。この場合、プロセッサ１０１は、受信ＨＥＬＬＯメッセージに応答した処理（４１０

）を実行して、このルーチンを終了する。但し、送信元ノードを相互認証済みノードと判断された時、受信ＨＥＬＬＯメッセージの正当性判断を更にするために、後述するＭＡＣ検証４２０を実行してから、受信ＨＥＬＬＯメッセージに応答した処理（４１０）を実行するようにしてもよい。

【００６１】

送信元ノードが、相互認証未実施のノードの場合、プロセッサ１０１は、送信元ノードＩＤ２０２が、間接ノード情報テーブル１３４に間接ノードＩＤ１３４ａとして登録されているか否かを判定する（４０２）。送信元ノードＩＤ２０２が、間接ノードＩＤ１３４ａとして登録されていると言うことは、このノードが、アドホックネットワークの他の何れかの通信端末と相互認証に成功したノードであることを意味している。この場合、本発明では、プロセッサ１０１は、送信元ノードとの相互認証を省略し、ＭＡＣ検証（４２０）を実行する。ＭＡＣ検証は、受信メッセージのアドホック鍵識別子リスト２０５Ｃが示す何れかのアドホック鍵を適用して、ＨＥＬＬＯメッセージからＭＡＣを生成し、これとＭＡＣリスト２１５Ｂが示す上記アドホック鍵と対応したＭＡＣとが一致するか否かを判定することことを意味している。ＭＡＣ検証の詳細については、図１１で後述する。

【００６２】

プロセッサ１０１は、ＭＡＣ検証結果を判定し（４２１）、ＭＡＣ検証に成功した場合は、ＭＡＣ検証失敗回数テーブル１３９における上記送信元ノードと対応する検証失敗回数１３９ｂの値をクリア（４２２）した後、上記送信元ノードのサークル鍵を受信済みか否かを判定する（４２３）。この判定は、直接ノード情報テーブル１３３に送信元ノードＩＤ２０２と一致する直接ノードＩＤ１３３ａが登録済みか否かをチェックすることを意味している。サークル鍵が未受信の場合、プロセッサ１０１は、送信元ノードとの間で、図１２で後述するサークル鍵の交換（４２４）を行った後、受信ＨＥＬＬＯメッセージに応答した処理（４１０）を実行する。

【００６３】

ＭＡＣ検証に失敗した場合、プロセッサ１０１は、ＭＡＣ検証失敗回数テーブル１３９における上記送信元ノードと対応する検証失敗回数１３９ｂの値Ｎを更新し（４２５）、Ｎの値を閾値Ｎｍａｘと比較する（４２６）。Ｎ＞Ｎｍａｘでなければ、プロセッサ１０１は、受信ＨＥＬＬＯメッセージを破棄して（４１１）、このルーチンを終了する。これによって、同一ノードが送信する次のＨＥＬＬＯメッセージについて、同様の処理が繰り返される。

【００６４】

Ｎ＞Ｎｍａｘの場合、プロセッサ１０１は、送信元ノードとの間で、図１２で詳述する相互認証と暗号鍵交換手順（４０８）を実行する。プロセッサ１０１は、認証結果を判定し（４０９）、認証に成功した場合は、受信ＨＥＬＬＯメッセージに応答した処理（４１０）を実行し、認証に失敗した場合は、受信ＨＥＬＬＯメッセージを破棄して（４１１）、このルーチンを終了する。

【００６５】

ステップ４０２で、送信元ノードＩＤ２０２が間接ノードＩＤ１３４ａとして未登録と判った場合、プロセッサ１０１は、認証中ノードＩＤテーブル１３８を参照して、現在、他の何れかのノードとの間での認証処理が実行中か否かを判定する（４０３）。認証処理が実行中でなければ、プロセッサ１０１は、送信元ノードとの間で相互認証と暗号鍵交換手順（４０８）を実行する。もし、他のノードとの間での認証処理が実行中の場合は、認証相手となっている他のノードから受信したＨＥＬＬＯメッセージをチェックし、上記送信元ノードＩＤが、該ＨＥＬＬＯメッセージの直接ノードリスト２０３に含まれているか否かを判定する。送信元ノードＩＤが、直接ノードリストに含まれていると言うことは、送信元ノードが認証相手ノードと相互認証済みであることを意味している（４０４）。そこで、プロセッサ１０１は、実行中の認証処理が終了するのを待ち（４０６）、認証に成功した場合は（４０７）、送信元ノードとの相互認証に代えて、ＭＡＣ検証（４２０）を実行し、認証に失敗した場合は、送信元ノードとの間で相互認証と暗号鍵交換手順（４０

８）を実行する。

【００６６】

ステップ４０４で、送信元ノードＩＤが直接ノードリスト２０３に含まれていなかった場合、プロセッサ１０１は、上記認証相手ノードから受信したＨＥＬＬＯメッセージの直接ノードリストと、今回受信したＨＥＬＬＯメッセージの直接ノードリストとを照合し、２つのメッセージに共通するノードＩＤの有無をチェックする（４０５）。もし、共通するノードＩＤが見つかれば、今回受信したＨＥＬＬＯメッセージの送信元ノードと認証相手ノードとが、それぞれ上記共通ノードＩＤをもつ第３のノードと認証済みであることが判る。そこで、プロセッサ１０１は、実行中の認証処理が終了するのを待ち（４０６）、認証に成功した場合は（４０７）、ＭＡＣ検証（４２０）を実行し、認証に失敗した場合は、送信元ノードとの間で相互認証と暗号鍵交換手順（４０８）を実行する。ステップ４０５で共通ノードＩＤが見つからなかった場合は、プロセッサ１０１は、送信元ノードとの間で相互認証と暗号鍵交換手順（４０８）を実行する。

【００６７】

図１１は、ＭＡＣ検証４２０の詳細フローチャートを示す。

ＭＡＣ検証では、プロセッサ１０１は、最初に、受信ＨＥＬＬＯメッセージのＭＡＣ個数２０５Ａをパラメータｉｍａｘに設定し、アドホック鍵を指定するためのパラメータｉの値を初期値「１」に設定する(ステップ４２０１）。次に、プロセッサ１０１は、受信ＨＥＬＬＯメッセージのアドホック鍵識別子リスト２０５Ｃが示す第ｉアドホック鍵識別子と、最新アドホック鍵情報テーブル１３５に記憶された鍵識別子１３５ｂとを比較し（４２０２）、一致した場合は、最新アドホック鍵１３５ａを適用した受信ＨＥＬＬＯメッセージの暗号化によって、ＭＡＣを生成し（４２０４）、該生成ＭＡＣが、受信ＨＥＬＬＯメッセージのＭＡＣリスト２１５Ｂの第ｉＭＡＣと一致するか否かを判定する（４２０５）。一致した場合は、ＭＡＣ検証に成功したと判断して（４２０６）、ＭＡＣ検証４２０を終了する。

【００６８】

生成ＭＡＣとＭＡＣリスト２０５Ｂの第ｉＭＡＣとが一致しなかった場合は、パラメータｉの値をインクリメントし（４２０７）、ｉの値をＩｍａｘと比較する（４２０８）。ｉ＞Ｉｍａｘでなければ、ステップ４２０２に戻り、次の第ｉアドホック鍵識別子を最新アドホック鍵識別子と比較する。第ｉアドホック鍵識別子が最新アドホック鍵識別子に一致しなかった場合、存在可能アドホック鍵情報テーブル１３６から、鍵識別子１３６ｂが第ｉアドホック鍵識別子に一致したアドホック鍵を検索する（４２０３）。第ｉアドホック鍵識別子をもつアドホック鍵が見つかった場合は、このアドホック鍵を適用した受信ＨＥＬＬＯメッセージの暗号化によって、ＭＡＣを生成し（４２０４）、該生成ＭＡＣが、受信ＨＥＬＬＯメッセージのＭＡＣリスト２０５Ｂの第ｉＭＡＣと一致するか否かを判定する（４２０５）。一致した場合は、ＭＡＣ検証に成功したと判断して（４２０６）、ＭＡＣ検証４２０を終了する。

【００６９】

存在可能アドホック鍵情報テーブル１３６から、第ｉアドホック鍵識別子をもつアドホック鍵が見つからなかった場合（４２０３）、パラメータｉの値をインクリメントし（４２０７）、ｉの値をＩｍａｘと比較する（４２０８）。ｉ＞Ｉｍａｘでなければ、ステップ４２０２に戻り、ｉ＞Ｉｍａｘとなった場合は、ＭＡＣ検証に失敗したと判断して（４２０９）、ＭＡＣ検証４２０を終了する。

【００７０】

図１２は、相互認証と暗号鍵交換手順４０８の詳細を示す。ここでは、通信端末１０Ａ－１が、通信端末１０Ａ－２からのＨＥＬＬＯメッセージを受信し、通信端末１０Ａ－２との間で相互認証と暗号鍵交換を行う場合について説明する。

相互認証を開始した通信端末１０Ａ－１は、相手端末装置１０Ａ－２が所有する公開暗号鍵を認証するための乱数を生成し（１２０１）、生成された乱数を含む認証開始要求メッセージＭ１を送信する（１２０２）。上記認証開始要求メッセージＭ１を受信した通信

端末１０Ａ－２は、受信メッセージＭ１が示す乱数を公開鍵暗号化方式の秘密鍵ＳＫ２で暗号化して、認証データを作成する（１２０３）。また、通信端末１０Ａ－２も、通信端末１０Ａ－１が所有する公開暗号鍵を認証するための乱数を生成し（１２０４）し、生成された乱数と、上記認証データと、通信端末１０Ａ－２が所有する公開鍵情報（公開鍵ＰＫ２および公開鍵証明情報）とを含む応答メッセージＭ２を通信端末１０Ａ－１に送信する（１２０５）。

【００７１】

通信端末１０Ａ－１は、上記応答メッセージＭ２を受信すると、受信した公開鍵情報に含まれる相手端末の公開鍵証明情報を検証し（１２０６）、受信した公開鍵ＰＫ２による認証データの復号化結果と元の乱数とを照合することによって、認証データを検証し（１２０７）、通信端末１０Ａ－２の正当性を確認する。通信端末１０Ａ－２の正当性を確認すると、通信端末１０Ａ－１は、ステップ１２０３と同様、受信メッセージＭ２が示す乱数を公開鍵暗号化方式の秘密鍵ＳＫ１で暗号化することによって、認証データに作成する（１２０８）。上記認証データは、通信端末１０Ａ－１が所有する公開鍵情報（公開鍵ＰＫ１および公開鍵証明情報）と共に、メッセージＭ３として通信端末１０Ａ－２に送信される（１２０９）。

【００７２】

通信端末１０Ａ－２は、メッセージＭ３を受信すると、通信端末１０Ａ－１と同様、受信した証明情報を検証し（１２１０）、受信した公開鍵ＰＫ１による認証データの復号化結果と元の乱数とを照合することによって、認証データを検証し（１２１１）、通信端末１０Ａ－１の正当性を確認する。通信端末１０Ａ－２が、通信端末１０Ａ－１の正当性を確認したことによって相互認証が完了する。尚、通信端末１０Ａ－１と１０Ａ－２は、相互認証が完了した通信相手のノードＩＤと対応して、直接ノード情報テーブル１３３に、公開鍵と証明情報を相互認証情報１３３Ｃとして記憶する。

【００７３】

相互認証が完了すると、端末間での暗号鍵情報（サークル鍵とアドホック鍵情報）の交換手順が開始される。

通信端末１０Ａ－２は、自ノード情報テーブル１３１が示すサークル鍵１３１ｃと、最新アドホック鍵情報テーブル１３５が示す最新アドホック鍵情報とを含む鍵データメッセージを生成し、該メッセージ内容を通信端末１０Ａ－１の公開鍵ＰＫ１で暗号化し（１２１２）、暗号化鍵データメッセージＭ４として、通信端末１０Ａ－１に送信する（１２１３）。

【００７４】

通信端末１０Ａ－１は、受信した暗号化鍵データメッセージＭ４を秘密鍵ＳＫ１で復号化することによって、通信端末１０Ａ－２が所有するサークル鍵と、最新アドホック鍵情報を抽出する（１２１４）。抽出されたサークル鍵は、直接ノード情報テーブル１３３に登録され、最新アドホック鍵情報は、最新アドホック鍵情報テーブル１３５または存在可能アドホック鍵情報テーブル１３６に反映される（１２１５）。アドホック鍵情報の更新処理については後で詳述する。

【００７５】

通信端末１０Ａ－１は、アドホック鍵情報の更新が終わると、通信端末１０Ａ－２と同様に、自ノード情報テーブル１３１が示すサークル鍵１３１ｃと、最新アドホック鍵情報テーブル１３５が示す最新アドホック鍵情報とを含む鍵データメッセージを生成し、メッセージ内容を通信端末１０Ａ－２の公開鍵ＰＫ２で暗号化し（１２１６）、暗号化鍵データメッセージＭ５として、通信端末１０Ａ－２に送信する（１２１７）。

【００７６】

通信端末１０Ａ－２は、受信した暗号化鍵データメッセージＭ５を秘密鍵ＳＫ２で復号化し（１２１８）、通信端末１０Ａ－１と同様に、直接ノード情報テーブル１３３、最新アドホック鍵情報テーブル１３５、存在可能アドホック鍵情報テーブル１３６を更新する（１２１９）。

【００７７】
以上の実施例から明らかなように、本発明では、通信端末が最初にアドホックネットワークに接続された時、ＨＥＬＬＯメッセージの送信元となる他の通信端末との間で相互認証手順を実行するが、一旦、アドホック鍵を共有すると、ＭＡＣ検証による相手端末の認証が可能となる。従って、本発明によれば、各通信端末は、ユーザの移動によってネットワークの接続関係が変化した場合でも、新たな接続相手となる通信端末との間での相互認証手順の実行を省略し、ＭＡＣ検証によって相互に正当性を確認することができるため、移動に伴う通信オーバーヘッドを大幅に軽減できる。
【００７８】
次に、図１３～図１８を参照して、ＴＣメッセージとアドホック鍵情報メッセージの送受信処理について説明する。
図１３は、ＯＬＳＲ方式の各通信端末１０Ａ（プロセッサ１０１）が、タイマ割り込みによって定期的、例えば5秒毎に実行するＴＣメッセージ送信ルーチン５００のフローチャートを示す。
【００７９】
ＴＣメッセージ送信ルーチン５００が起動されると、プロセッサ１０１は、自ノード情報テーブル１３１のＭＰＲフラグ１３１ｂをチェックする(ステップ５０１）。ＭＰＲフラグが「０」、すなわち、自ノードが他の通信端末からＭＰＲノードとして指定されていなければ、ＴＣメッセージの送信は不要となるため、このルーチンを終了する。
【００８０】
ＭＰＲフラグが「１」に設定されていた場合、プロセッサ１０１は、図２（Ｂ）で説明したＴＣメッセージ２１０を生成し（５０２）、アドホック鍵を適用して、ＴＣメッセージ２１０からＭＡＣ情報２１５を生成し、これをＴＣメッセージ２１０に付加する（５０３）。ＴＣメッセージ２１０用のＭＡＣ情報２１５の生成は、図９で説明したＨＥＬＬＯメッセージ用のＭＡＣ情報２０５の生成と同様の手順で行われるため、詳細説明は省略する。
【００８１】
プロセッサ１０１は、現時点で自分の知っているアドホック鍵情報をアドホックネットワーク内の他の通信端末に配布するために、ＭＡＣ情報付きのアドホック鍵情報メッセージを生成する（５１０）。ＭＡＣ情報付きのアドホック鍵情報メッセージの生成については、図１５を参照して、後で詳述する。この後、プロセッサ１０１は、ＭＡＣ情報付きのＴＣメッセージと、ＭＡＣ情報付きのアドホック鍵情報メッセージを送信して（５０４、５０５）、このルーチンを終了する。尚、アドホック鍵情報メッセージの送信タイミングは、ＴＣメッセージの送信タイミングに合わせる必要はないが、本実施例では、各通信端末が、ＭＡＣ情報付きＴＣメッセージの送信の都度、ＭＡＣ情報付きのアドホック鍵情報メッセージを送信するものとして説明する。
【００８２】
図１４は、ＭＡＣ情報付きのアドホック鍵情報メッセージ２２０Ｍのフォーマットを示す。
ＭＡＣ情報付きのアドホック鍵情報メッセージ２２０Ｍは、このメッセージがアドホック鍵情報メッセージであることを示すメッセージ種別２２１と、メッセージの送信元を示す送信元ノードＩＤ２２２と、メッセージの生成元を示す生成元ノードＩＤ２２３と、メッセージのシーケンス番号２２４、生成元ノードで使用している最新アドホック鍵を示すアドホック鍵２２５、アドホック鍵の識別子２２６と、アドホック鍵の生成時刻２２７と、アドホック鍵情報リスト２２８とを含むアドホック鍵情報メッセージに、ＭＡＣ情報２２９を付加した形となっている。
【００８３】
アドホック鍵２２５、鍵識別子２２６、生成時刻２２７は、最新アドホック鍵情報テーブル１３５の内容と一致している。アドホック鍵情報リスト２２８は、存在可能アドホック鍵情報テーブル１３６から選択された有効期限内のアドホック鍵情報のリストである。

アドホック鍵２２５～アドホック鍵情報リスト２２８の内容は、不正な通信端末で盗聴されないように、サークル鍵１３１ｃで暗号化した形で送信される。

【００８４】

図１５は、ＭＡＣ情報付きアドホック鍵情報メッセージの生成処理５１０の詳細フローチャートを示す。

プロセッサ１０１は、最初に、図１４に示したメッセージ種別２２１～生成時刻２２７からなるアドホック鍵情報メッセージを生成し（５１１）、次に、存在可能アドホック情報テーブル１３６に登録されたアドホック鍵の個数（登録エントリ数）をパラメータＩｍａｘに設定し、現在のテーブルエントリを指すためのパラメータｉの値を「１」に設定する（ステップ５１２）。

【００８５】

プロセッサ１０１は、パラメータｉとＩｍａｘとを比較し（５１３）、ｉ＞Ｉｍａｘでなければ、存在可能アドホック情報テーブル１３６の第ｉエントリが示す登録時刻１３５ｄから、第ｉアドホック鍵の有効性をチェックする（５１４）。登録時刻からの経過時間が所定時間以内であれば、第ｉアドホック鍵は有効と判断される。この場合、プロセッサ１０１は、アドホック鍵情報メッセージのアドホック鍵情報リスト２２８に、存在可能アドホック情報テーブル１３６の第ｉエントリが示すアドホック鍵１３６ａ、鍵識別子１３６ｂ、生成時刻１３６ｃをアドホック鍵情報として追加し（５１５）、パラメータｉの値をインクリメントして（５１７）、ステップ５１２に戻る。

登録時刻からの経過時間が所定時間を超えていた場合は、プロセッサ１０１は、第ｉアドホック鍵を無効と判断し、存在可能アドホック情報テーブル１３６から第ｉエントリを削除し（５１６）、パラメータｉの値をインクリメントして（５１７）、ステップ５１２に戻る。

【００８６】

パラメータｉの値がＩｍａｘを超えると、プロセッサ１０１は、図９で説明したＭＡＣ生成ルーチンと同様の手順で、上記アドホック鍵情報リスト２２８を含むアドホック鍵情報メッセージから、ＭＡＣ情報２２９を生成する（５１８）。この後、プロセッサ１０１は、機密情報となるアドホック鍵２２５～アドホック鍵情報リスト２２８をサークル鍵１３１ｃで暗号化し（５１９）、部分的に暗号化されたアドホック鍵情報メッセージにＭＡＣ情報２２８を付加して（５２０）、ＭＡＣ情報付きアドホック鍵情報メッセージの生成処理５１０を終了する。

【００８７】

本実施例では、上記ＭＡＣ情報付きアドホック鍵情報メッセージ２２０Ｍの内容から判るように、ＭＰＲノードとなった各通信端末が、他の通信端末に、自ノードで選択している最新のアドホック鍵情報の他に、存在可能アドホック鍵情報テーブル１３６が示す有効期間内の過去のアドホック鍵情報も通知するようにしているため、通信相手端末が、自ノードとは異なるアドホック鍵を最新アドホック鍵として使用している場合であっても、ＭＡＣ検証が可能となる。

【００８８】

図１６は、各通信端末１０Ａ（プロセッサ１０１）がＭＡＣ情報付きＴＣメッセージ２１０Ｍを受信した時に実行するＴＣメッセージ受信処理ルーチン６００のフローチャートを示す。

プロセッサ１０１は、ＭＡＣ情報付きＴＣメッセージ２１０Ｍを受信すると、受信メッセージの送信元ノードからのサークル鍵が既に受信済みか否かを判定する（６０１）。サークル鍵の有無は、直接ノード情報テーブル１３３から、直接ノードＩＤ１３３ａが受信メッセージの送信元ノードＩＤ２１２と一致するエントリを検索することによって判明する。直接ノード情報テーブル１３３に送信元ノードＩＤ２１２と対応したエントリが無かった場合、その後に受信されるアドホック鍵情報メッセージＭ２２０Ｍの復号化とＭＡＣ検証ができないため、受信メッセージ２１０Ｍを破棄して（６１１）、このルーチンを終了する。

【００８９】
直接ノード情報テーブル１３３に、送信元ノードＩＤ２２２と対応するエントリが存在していた場合、プロセッサ１０１は、受信したＴＣメッセージ２１０ＭのＭＡＣ検証を行う（６０２）。図７に示したフォーマットから明らかなように、ＴＣメッセージのＭＡＣは、ＨＥＬＬＯメッセージと同じ構造となっているため、図１１で説明したＨＥＬＬＯメッセージのＭＡＣ検証と同様の手順で検証できる。
【００９０】
ＭＡＣ検証に失敗した場合（６０３）、プロセッサ１０１は、受信メッセージ２１０Ｍを破棄して（６１１）、このルーチンを終了し、ＭＡＣ検証に成功した場合は、受信メッセージが示すＭＰＲＳノードリスト２１４に従ったルーティングテーブルの更新等のＴＣメッセージ処理（６０４）を実行した後、アドホック鍵情報メッセージ２２０Ｍの受信を待つ（６０５）。
【００９１】
アドホック鍵情報メッセージ２２０Ｍを受信すると、プロセッサ１０１は、図１７で詳述するアドホック鍵情報メッセージ受信処理（６２０）を実行する。アドホック鍵情報メッセージ受信処理の実行によって、最新アドホック鍵情報テーブル１３５または存在可能アドホック鍵情報テーブル１３６が更新され、受信メッセージ２２０Ｍが新たなＭＡＣ情報をもつ転送用アドホック鍵情報メッセージに変換される。また、アドホック鍵情報メッセージ２２０Ｍの無用な転送を抑制するために、アドホック鍵情報メッセージ受信処理において、アドホック鍵情報メッセージの転送要否が転送指示フラグによって指定される。
【００９２】
この後、プロセッサ１０１は、ＭＰＲフラグ１３１ｂをチェックし（６０６）、ＭＰＲフラグが「０」であれば、このルーチンを終了する。ＭＰＲフラグが「１」の場合、プロセッサ１０１は、今回受信したＴＣメッセージの送信元ノードＩＤ２１２を自ノードＩＤに書き換え、図９で説明したＭＡＣ生成ルーチン３１０と同様の手順で、新たなＭＡＣ情報２１５を生成し、受信ＴＣメッセージ２２０Ｍを新たなＭＡＣ情報をもつ転送用ＴＣメッセージに変換する（６０７）。プロセッサ１０１は、上記転送用ＴＣメッセージを送信（６０８）した後、転送指示フラグを判定する（６０９）。転送指示フラグが「０」の場合は、このルーチンを終了し、転送指示フラグが「１」の場合は、処理６２０で生成済みの転送用アドホック鍵情報メッセージを送信（６１０）して、このルーチンを終了する。
【００９３】
図１７は、アドホック鍵情報メッセージ受信処理６２０の詳細フローチャートを示す。
アドホック鍵情報メッセージ受信処理６２０では、プロセッサ１０１は、受信メッセージのシーケンス番号２２４をチェックする（６２１）。受信メッセージのシーケンス番号２２４の値が、鍵情報メッセージ・シーケンス番号テーブル１３７が示す該メッセージ送信元ノードＩＤと対応するシーケンス番号１３７ｂの値よりも新しくなければ、プロセッサ１０１は、受信メッセージを破棄し、転送指示フラグを「０」に設定して（６３７）、このルーチンを終了する。
【００９４】
シーケンス番号２２３の値がシーケンス番号１３７ｂの値よりも新しい場合、プロセッサ１０１は、鍵メッセージ・シーケンス番号テーブル１３７のシーケンス番号１３７ｂを上記シーケンス番号２２３が示す最新値に更新し（６２２）、受信メッセージの暗号化部分を復号化する（６２３）。上記復号化に必要なサークル鍵１３３ｄは、直接ノード情報テーブル１３３から、直接ノードＩＤ１３３ａが受信メッセージの送信元ノードＩＤ２２２と一致するエントリを検索することによって得られる。
【００９５】
プロセッサ１０１は、復号化されたアドホック鍵情報メッセージ２２０Ｍを検証対象として、図１１で説明した手順で、ＭＡＣ検証を実行する（６２４）。ＭＡＣ検証の結果（６２５）、検証に失敗した場合は、受信メッセージを破棄し、転送指示フラグを「０」に設定して（６３７）、このルーチンを終了する。

【００９６】
ＭＡＣ検証に成功した場合、プロセッサ１０１は、最新アドホック鍵情報テーブル１３５が示すアドホック鍵１３５ａと、受信メッセージ２２０Ｍが示すアドホック鍵２２５とを比較し、新しい方を最新アドホック鍵として選択する（６２６）。最新アドホック鍵の選択は、ポリシー記憶領域１５０に記憶された鍵選択ポリシーに従って行われ、例えば、アドホック鍵１３５ａの生成時刻１３５ｃと、アドホック鍵２２５の生成時刻２２７とを比較し、生成時刻の遅い方のアドホック鍵が選択される。
【００９７】
上記鍵選択の結果（６２７）、自ノードで使用すべき最新アドホック鍵１３５ａを変更する必要があった場合、プロセッサ１０１は、最新アドホック鍵情報テーブル１３５のアドホック鍵情報（アドホック鍵１３５ａ、鍵識別子１３５ｂ、生成時刻１３５ｃ）を受信メッセージが示すアドホック鍵情報（アドホック鍵２２５、鍵識別子２２６、生成時刻２２７）に置き換え、それまでテーブル１３５に記憶されていた旧いアドホック鍵情報を存在可能アドホック鍵情報テーブル１３６に移動する（６２８）。この後、プロセッサは、図１８で後述するように、受信メッセージのアドホック鍵情報リスト２２８の内容に応じて、存在可能アドホック鍵情報テーブル１３６を更新する（６４０）。
【００９８】
上記鍵選択の結果（６２７）、使用すべき最新アドホック鍵に変更がなければ、プロセッサ１０１は、受信メッセージが示すアドホック鍵情報（アドホック鍵２２５、鍵識別子２２６、生成時刻２２７）が存在可能アドホック鍵情報テーブル１３６に既に登録済みか否かを判定する（６２９）。既に登録済みの場合は、該当エントリの登録時刻１３６ｄを現在時刻に更新（６３０）した後、存在可能アドホック鍵情報テーブルの更新処理６４０を実行する。受信メッセージが示すアドホック鍵情報が存在可能アドホック鍵情報テーブル１３６に未登録の場合は、受信したアドホック鍵情報を存在可能アドホック鍵情報テーブル１３６に登録（６３１）した後、テーブル更新処理６４０を実行する。
【００９９】
存在可能アドホック鍵情報テーブル１３６の更新処理６４０を終えたプロセッサ１０１は、ＭＰＲフラグ１３１ｂをチェックし（６３２）、ＭＰＲフラグが「０」であれば、受信メッセージを破棄し、転送指示フラグを「０」に設定して（６３７）、このルーチンを終了する。
【０１００】
ＭＰＲフラグが「１」の場合、プロセッサ１０１は、送信元ノードＩＤ２２２を自ノードＩＤに書き換えたアドホック鍵情報メッセージ２２０Ｍを対象として、図９で説明した手順に従って、ＭＡＣ情報を生成する（６３３）。プロセッサ１０１は、この後、アドホック鍵情報メッセージ２２０Ｍの機密情報部分をサークル鍵１３１ｃで暗号化し（６３４）、部分的に暗号化されたアドホック鍵情報メッセージにＭＡＣ情報を付加し（６３５）、転送指示フラグを「１」に設定して（６３６）、このルーチンを終了する。
【０１０１】
図１８は、図１７のステップ６４０で実行される存在可能アドホック鍵情報テーブル１３６の更新処理の詳細フローチャートを示す。
プロセッサ１０１は、先ず、受信メッセージ２２０Ｍのアドホック鍵情報リスト２２８に含まれるエントリの個数をパラメータＩｍａｘに設定し、現在のエントリを指すためのパラメータｉの値を初期値「１」に設定する（６４１）。次に、アドホック鍵情報リスト２２８の第ｉエントリが示す鍵識別子が、存在可能アドホック鍵情報テーブル１３６に登録済みか否かを判定する（６４２）。
【０１０２】
既に登録済みの場合は、パラメータｉの値をインクリメントし（６４４）、パラメータｉとＩｍａｘとを比較する（６４５）。ここで、ｉ＞Ｉｍａｘでなければ、ステップ６４２に戻り、ｉ＞Ｉｍａｘの場合は、このテーブル更新処理を終了して、図１７のステップ６３２を実行する。アドホック鍵情報リスト２２８の第ｉエントリの鍵識別子が、存在可

能アドホック鍵情報テーブル１３６に未登録の場合、プロセッサ１０１は、上記第ｉエントリのアドホック鍵情報を含む新たなエントリを存在可能アドホック鍵情報テーブル１３６に追加（６４３）した後、ステップ６４４を実行する。存在可能アドホック鍵情報テーブル１３６に新たなアドホック鍵情報を追加する時、登録時刻１３６ｄとして現在の時刻が設定される。

【０１０３】

以下、図１９～図２４を参照して、本発明のアドホックネットワークにおける通信シーケンスの具体例について説明する。

図１９は、通信端末１０Ａ－２と１０Ａ－３から構成されるアドホックネットワークに、新たな通信端末１０Ａ－１が参加した状態を示し、図２０は、これらの通信端末間の主要な通信シーケンスを示す。

【０１０４】

通信端末１０Ａ－２と１０Ａ－３は、公開鍵による相互認証（２００１）を実行した後、相互に暗号鍵（サークル鍵とアドホック鍵）を交換し（２００２）、アドホック鍵ＡＫを共有した状態となっている。ここで、相互認証（２００１）は、図１２の手順１２０１～１２１１に相当し、暗号鍵交換（２００２）は、図１２の手順１２１２～１２１９に相当している。

【０１０５】

この状態で、新たな通信端末１０Ａ－１が、通信端末１０Ａ－２、１０Ａ－３の無線通信圏内に移動（２００３）し、最初に通信端末１０Ａ－２からのＭＡＣ情報付きＨＥＬＬＯメッセージ２００Ｍ－２を受信し、通信端末１０Ａ－２との間で相互認証手順を実行中に、通信端末１０Ａ－３からのＭＡＣ情報付きＨＥＬＬＯメッセージ２００Ｍ－３を受信した場合を想定する。

【０１０６】

通信端末１０Ａ－１は、ＭＡＣ情報付きＨＥＬＬＯメッセージ２００Ｍ－２を受信すると、送信元の通信端末１０Ａ－２との間で相互認証を開始する（２００４）。この時、通信端末１０Ａ－１は、通信端末１０Ａ－２のノードＩＤを認証中ノードＩＤテーブル１３８に記憶した後、認証開始要求メッセージＭ１を送信し、通信端末１０Ａ－２から、認証データと公開鍵情報とを含む応答メッセージＭ２を受信する。

【０１０７】

本発明では、通信端末１０Ａ－２との相互認証中に、別の通信端末１０Ａ－３からＭＡＣ情報付きＨＥＬＬＯメッセージ２００Ｍ－３を受信すると、通信端末１０Ａ－１は、受信メッセージ２００Ｍ－３の送信元ノードが、ＨＥＬＬＯメッセージ２００Ｍ－２の直接ノードリスト２０３に含まれているか否かを確認する（図１０のステップ４０４）。ここに示した例では、メッセージ２００Ｍ－３の送信元ノードが、ＨＥＬＬＯメッセージ２００Ｍ－２の直接ノードリスト２０３に含まれているため、実行中の認証の結果待ち（２００５）となり、通信端末１０Ａ－３との相互認証を開始することなく、通信端末１０Ａ－２との相互認証を続行し、メッセージＭ２に応答して、認証データと公開鍵情報とを含むメッセージＭ３を通信端末１０Ａ－２に送信する。

通信端末１０Ａ－１と１０Ａ－２は、相互認証が完了すると、相互に暗号鍵を交換する（２００６）。これによって、通信端末１０Ａ－１は、通信端末１０Ａ－２、１０Ａ－３と共通のアドホック鍵を所持した状態（２００７）となる。

【０１０８】

通信端末１０Ａ－１は、通信端末１０Ａ－２との相互認証に成功したため、通信端末１０Ａ－２ですでに認証済みとなっている通信端末１０Ａ－３については、相互認証を省略して、ＨＥＬＬＯメッセージ２００Ｍ－３のＭＡＣ検証を行う（２００８）。ＭＡＣ検証には、通信端末１０Ａ－２から取得した最新のアドホック鍵が適用される。ここに示した例では、通信端末１０Ａ－１は、ＨＥＬＬＯメッセージ２００Ｍ－３のＭＡＣ検証に成功し、通信端末１０Ａ－３とサークル鍵を交換する（２００９）。これによって、通信端末１０Ａ－１は、アドホックネットワークの他の通信端末とデータ通信可能な状態となる。

【０１０９】
図２１は、通信端末１０Ａ－１の移動によって、通信端末間の接続関係が変化した状態を示し、図２２は、図２１に対応する通信端末間の主要な通信シーケンスを示す。
ここに示したアドホックネットワークは、最初、通信端末１０Ａ－１と１０Ａ－２、通信端末１０Ａ－２と１０Ａ－３とが接続関係にある。図２２に示すように、通信端末１０Ａ－２と１０Ａ－３との間の接続は、図２０と同様、公開鍵による相互認証２００１と、暗号鍵（サークル鍵とアドホック鍵）交換２００２の実行によって実現される。また、通信端末１０Ａ－１と１０Ａ－２との接続は、図２０と同様、公開鍵による相互認証２００４と、暗号鍵（サークル鍵とアドホック鍵）交換２００６の実行によって実現される。
【０１１０】
通信端末１０Ａ－１がアドホック鍵ＡＫを取得した状態（２００７）で、通信端末１０Ａ－１の移動に伴って、通信端末１０Ａ－１と通信端末１０Ａ－２との接続関係が断たれ、通信端末１０Ａ－１が通信端末１０Ａ－３の無線通信圏内に入ったと仮定する（２０１０）。この時、通信端末１０Ａ－３からのＭＡＣ情報付きＨＥＬＬＯメッセージ２００Ｍ－３を受信した通信端末１０Ａ－１は、受信メッセージの送信元ノードＩＤが、間接ノード情報テーブル１３４に既に登録済みとなっているため、相互認証を省略して、アドホック鍵ＡＫを適用した受信メッセージのＭＡＣ検証（２００８）を行う。
【０１１１】
この例では、通信端末１０Ａ－１は、ＭＡＣ検証に成功するため、通信端末１０Ａ－３との間でサークル鍵を交換（２００９）し、再びアドホックネットワークでの通信が可能な状態となる。通信端末１０Ａ－３が、通信端末１０Ａ－１からのＭＡＣ情報付きＨＥＬＬＯメッセージを受信した場合でも、同様の結果が得られる。
【０１１２】
図２３は、通信端末１０Ａ－１のグループに所属していない他の通信端末１０Ｂが、アドホックネットワークから離脱した通信端末１０Ａ－１になりすまして、アドホックネットワークへの参加を試みた場合を示し、図２４は、図２３に対応する通信シーケンスを示す。シーケンス２００１～２００７は、図２２と同一である。
【０１１３】
通信端末１０Ａ－１が移動し、アドホックネットワークから離脱（２００８）した後、通信端末１０Ｂが、通信端末１０Ａ－１になりすまして、ＨＥＬＬＯメッセージ２００Ｍ（Ｂ）を送信したと仮定する。この場合、通信端末１０Ｂは、正規のアドホック鍵ＡＫを保有していないため、メッセージ２００Ｍ（Ｂ）は、ＭＡＣ情報を全く持たないか、間違ったＭＡＣが付加されている。従って、メッセージ２００Ｍ（Ｂ）を受信した通信端末１０Ａ－２は、ＭＡＣ検証に失敗し（２０２０）、受信メッセージを破棄する（２０２１）ことになる。
【０１１４】
通信端末１０Ｂが、ＨＥＬＬＯメッセージ２００Ｍ（Ｂ）の送信を繰り返しても、通信端末１０Ａ－２は、ＭＡＣ検証の失敗（２０２２）と、受信メッセージの破棄（２０２３）を繰り返し、ＭＡＣ検証の失敗回数を増やすだけである。ＭＡＣ検証の失敗回数が閾値に達すると、通信端末１０Ａ－２は、通信端末１０Ｂとの間で、公開鍵による相互認証を開始する（２０２４）。この場合、通信端末１０Ａ－２は、通信端末１０Ｂが、アドホックネットワークの正規メンバーが所持すべき公開鍵情報を持っていないため、通信端末１０Ｂを不正端末と判断する。
【０１１５】
相互認証によって一旦、不正と判断された通信端末１０Ｂについては、ノードＩＤを不正端末ＩＤテーブルに登録しておくとよい。不正端末のＩＤを記憶しておくことによって、通信端末１０ＢがＨＥＬＬＯメッセージの送信を繰り返した場合でも、通信端末１０Ａ－２は、受信メッセージの送信元をチェックすることによって、ＭＡＣ検証を行うことなく、受信メッセージを破棄する（２０２５）ことが可能となる。本実施例によれば、セキュリティ確保のための通信オーバーヘッドを軽減して、不正な通信端末１０Ｂのアドホッ

クネットワークへの参加を阻止することが可能となる。

【０１１６】

以上の実施例から明らかなように、本発明によれば、公開鍵による相互認証によって、一旦、アドホックネットワークへの参加を許された通信端末については、移動に伴って通信端末間の接続関係が変化した場合でも、制御メッセージに付加されたＭＡＣを利用して即時に相手装置を検証できるため、相互認証手順の実行による通信オーバーヘッドを回避して、アドホックネットワークのセキュリティを確保することができる。また、本発明は、特に、通信端末の移動に伴ってノード間の接続関係の変化した時、移動した端末と最寄りの通信端末との間のセキュリティオーバヘッドの軽減に有効となる。

【図面の簡単な説明】

【０１１７】

【図１】本発明が適用されるアドホックネットワークの構成を示す図。

【図２】（Ａ）はＯＬＳＲ方式の制御メッセージであるＨＥＬＬＯメッセージのフォーマット、（Ｂ）はＴＣメッセージのフォーマットを示す図。

【図３】通信端末１０Ａのハードウェア構成の一例を示すブロック図。

【図４】本発明の通信端末１０Ａが備えるソフトウェア構成の一例を示す図。

【図５】（Ａ）は自ノード情報テーブル１３１、（Ｂ）は直接ノード情報テーブル１３３、（Ｃ）は間接ノード情報テーブル１３４の一例を示す図。

【図６】（Ａ）は最新アドホック鍵情報テーブル１３５、（Ｂ）は存在可能アドホック情報テーブル１３６、（Ｃ）は鍵情報メッセージ・シーケンス番号テーブル１３７、（Ｅ）は認証中ノードＩＤテーブル１３８、（Ｅ）はＭＡＣ検証失敗回数テーブル１３９の一例を示す図。

【図７】（Ａ）はＭＡＣ情報付きＨＥＬＬＯメッセージのフォーマット、（Ｂ）はＭＡＣ情報付きＴＣメッセージのフォーマットを示す図。

【図８】通信端末が実行するＨＥＬＬＯメッセージ送信ルーチン３００の１例を示すフローチャート。

【図９】図８におけるＭＡＣ生成処理３１０の詳細を示すフローチャート。

【図１０】ＭＡＣ情報付きＨＥＬＬＯメッセージの受信ルーチン４００の１例を示すフローチャート。

【図１１】図１０におけるＭＡＣ検証処理４２０の詳細を示すフローチャート。

【図１２】通信端末１０Ａ－１と１０Ａ－２との間で実行される相互認証と暗号鍵交換のための通信シーケンス図。

【図１３】ＭＡＣ情報付きＴＣメッセージ送信ルーチン５００の１例を示すフローチャート。

【図１４】アドホック鍵情報メッセージのフォーマットを示す図。

【図１５】図１３におけるＭＡＣ情報付きアドホック鍵情報メッセージの生成処理５１０の詳細を示すフローチャート。

【図１６】ＭＡＣ情報付きＴＣメッセージの受信ルーチン６００の１例を示すフローチャート。

【図１７】図１６におけるアドホック鍵情報メッセージの受信処理６２０の詳細を示すフローチャート。

【図１８】図１７における存在可能アドホック鍵情報テーブルの更新処理６４０の詳細を示すフローチャート。

【図１９】アドホックネットワークに新たな通信端末１０Ａ－１が参加した状態を示す図。

【図２０】図１９と対応した本発明のアドホックネットワークにおける通信シーケンス図。

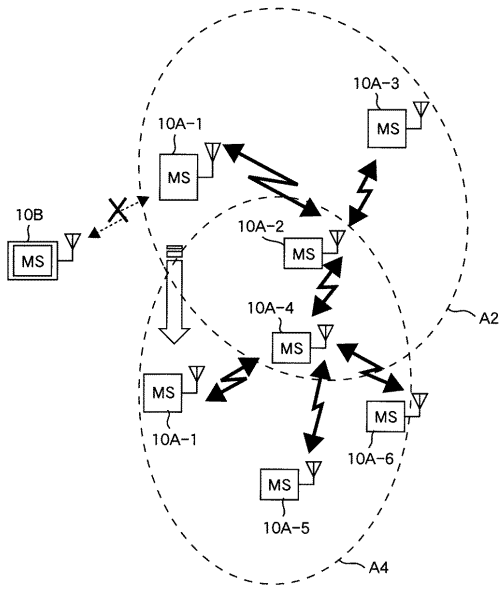
【図２１】アドホックネットワークにおいて通信端末１０Ａ－１が移動した状態を示す図。

【図２２】図２１と対応した本発明のアドホックネットワークにおける通信シーケンス図

。
【図２３】通信端末１０Ａ－１がアドホックネットワークから離脱し、不正な通信端末１０Ｂが参加しようとしている状態を示す図。
【図２４】図２３と対応した本発明のアドホックネットワークにおける通信シーケンス図。
【符号の説明】
【０１１８】
１０：通信端末（移動端末）、１３１：自ノード情報テーブル、１３３：直接ノード情報テーブル、１３４：間接ノード情報テーブル、１３５：最新アドホック鍵情報テーブル、１３６：存在可能アドホック情報テーブル、１３７：鍵情報メッセージ・シーケンス番号テーブル、１３８：認証中ノードＩＤテーブル、１３９：ＭＡＣ検証失敗回数テーブル、２００Ｍ：ＭＡＣ情報付きＨＥＬＬＯメッセージ、２１０Ｍ：ＭＡＣ情報付きＴＣメッセージ、２２０Ｍ：ＭＡＣ情報付きアドホック鍵情報メッセージ、２０５、２１５、２２９：ＭＡＣ情報。

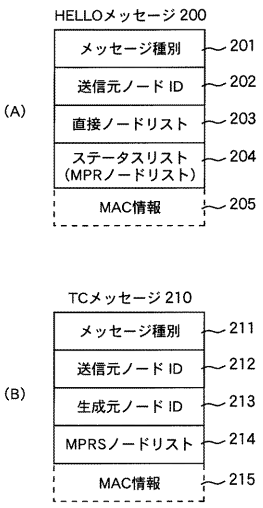
【図１】

図 1



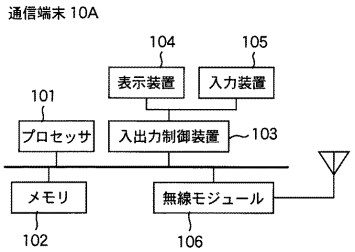
【図２】

図 2



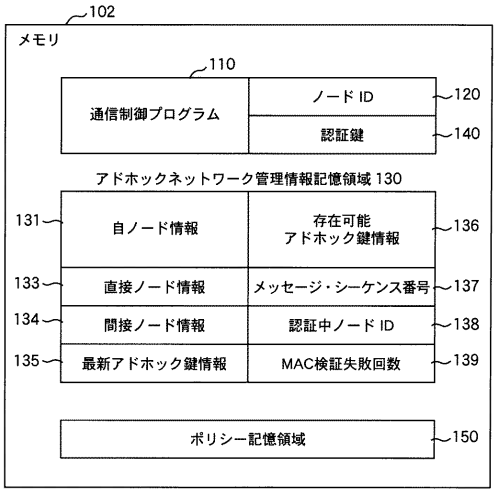
【図３】

図 3



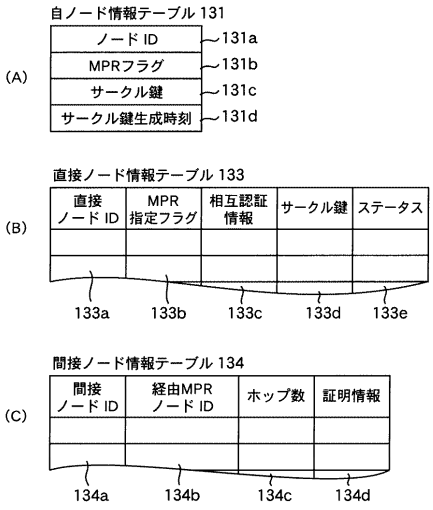
【図４】

図 4



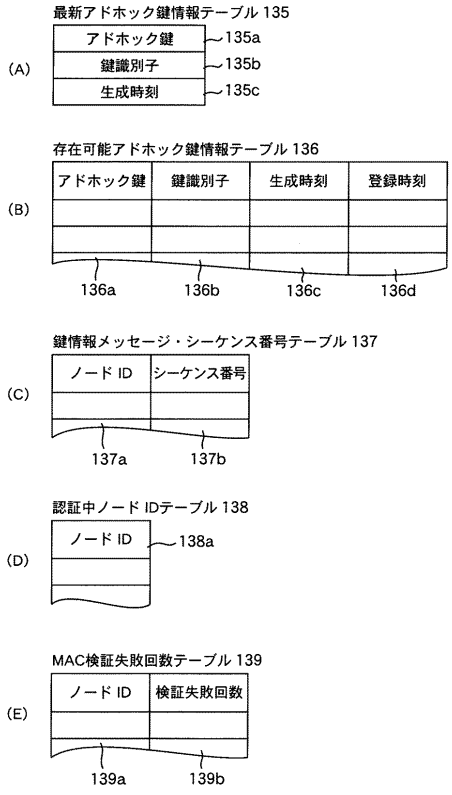
【図５】

図 5



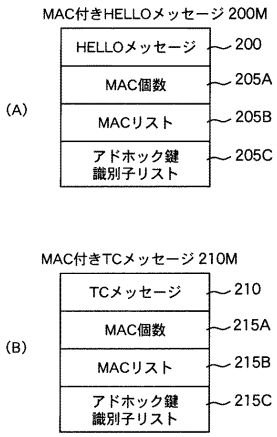
【図６】

図 6



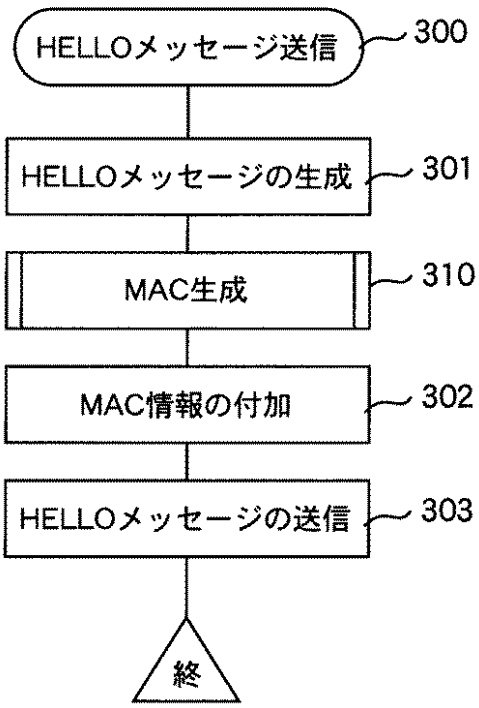
【図７】

図　7



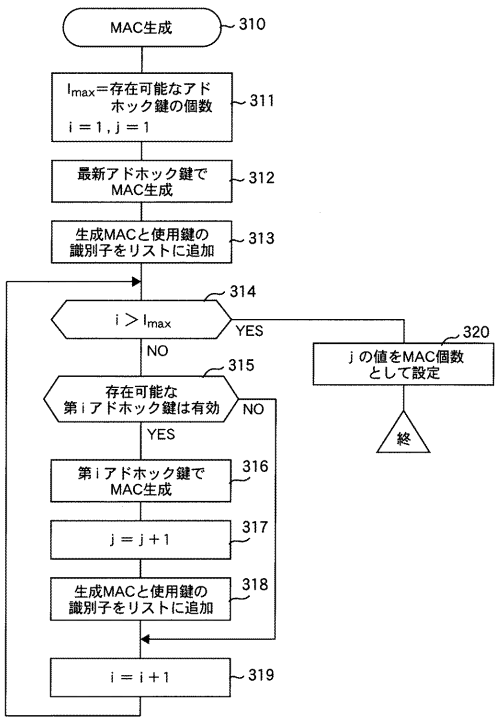
【図８】

図　8



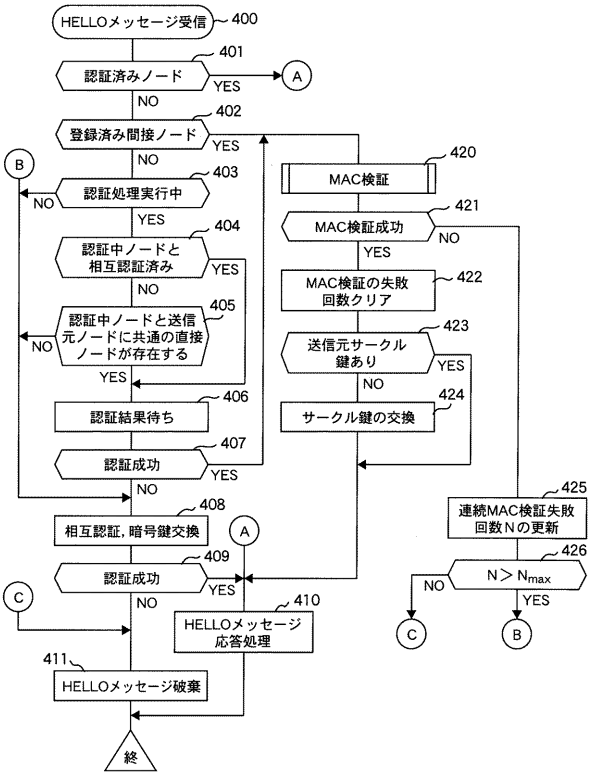
【図９】

図　9



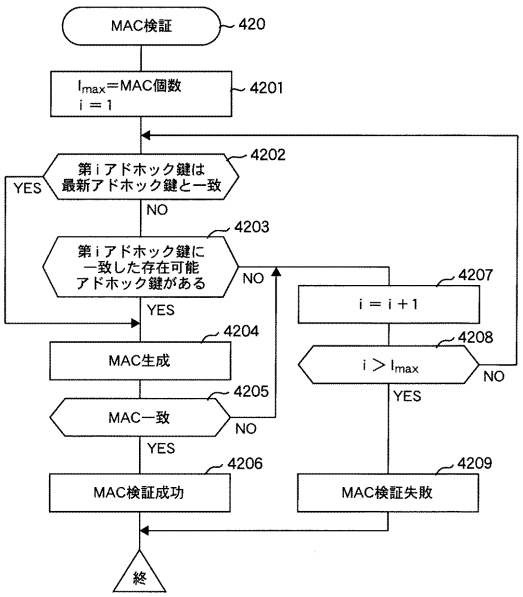
【図１０】

図　10



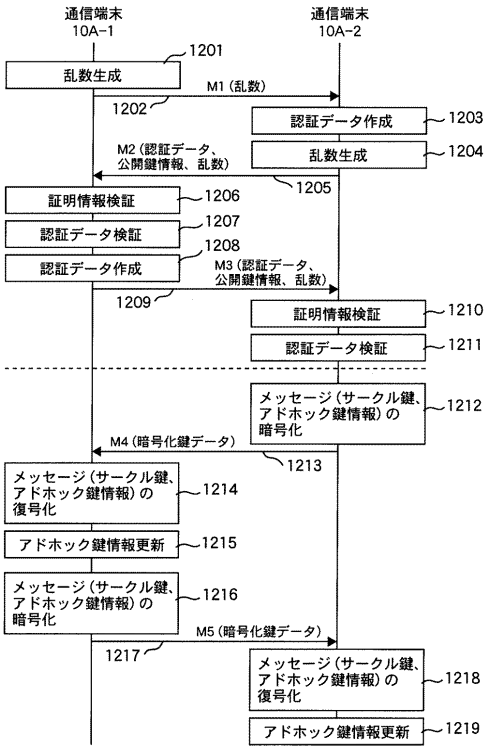
【図１１】

図 １１



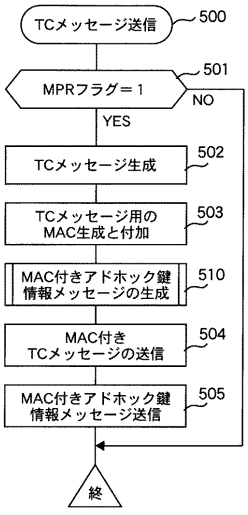
【図１２】

図 １２



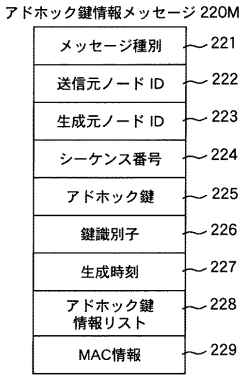
【図１３】

図 １３



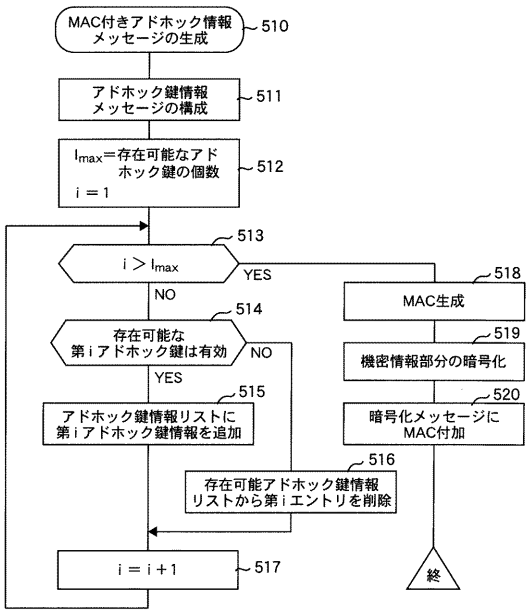
【図１４】

図 １４



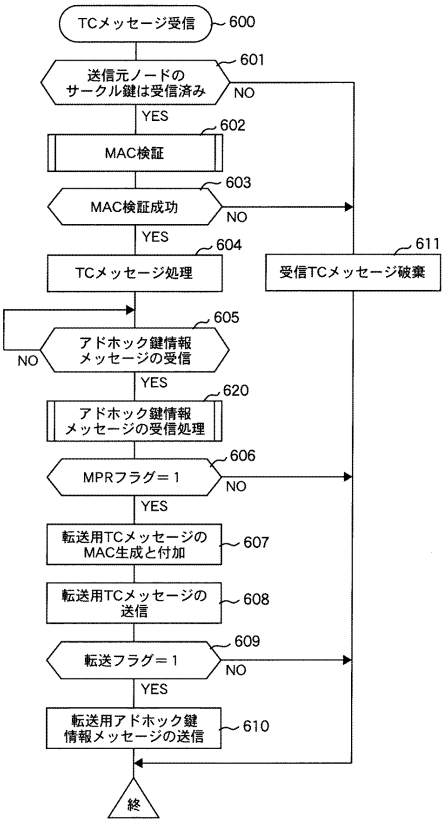
【図１５】

図　１５



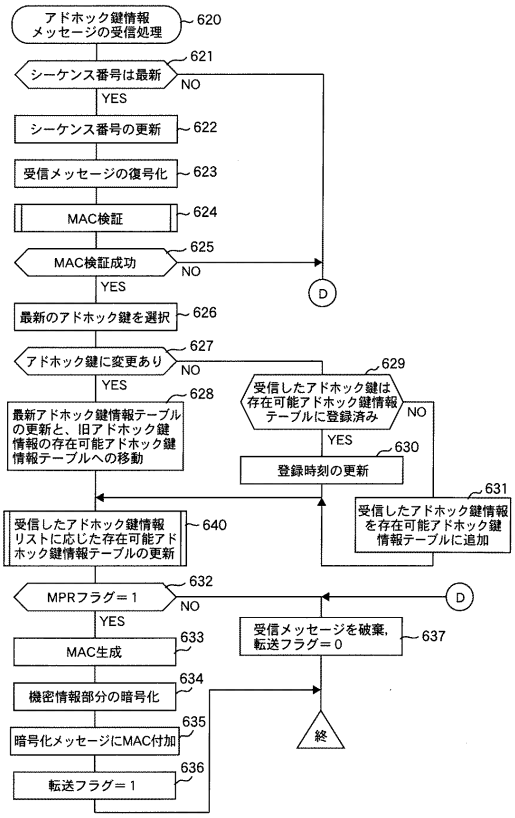
【図１６】

図　１６



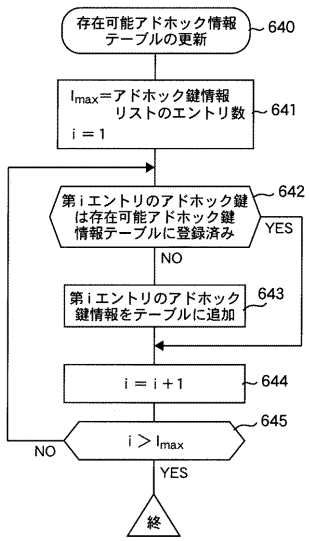
【図１７】

図　１７



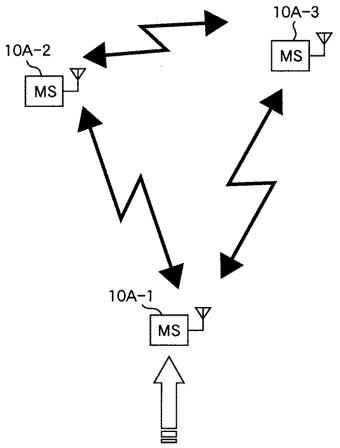
【図１８】

図　１８



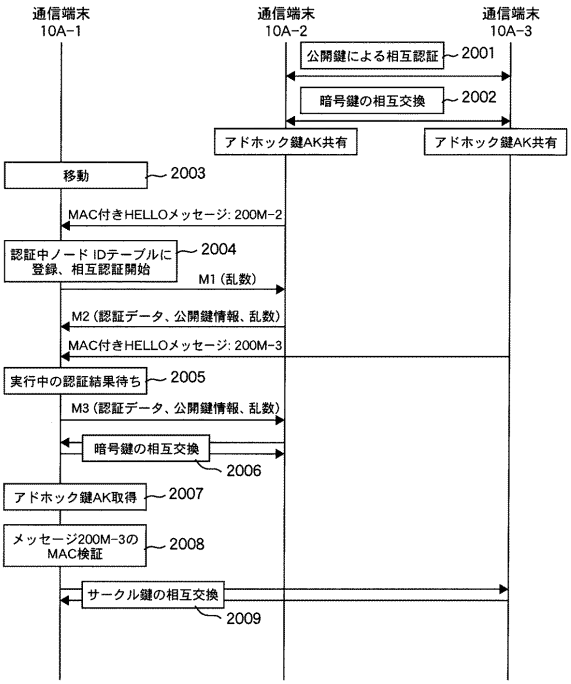
【図１９】

図　１９



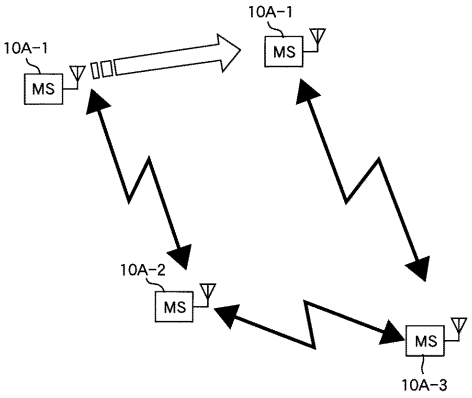
【図２０】

図　２０



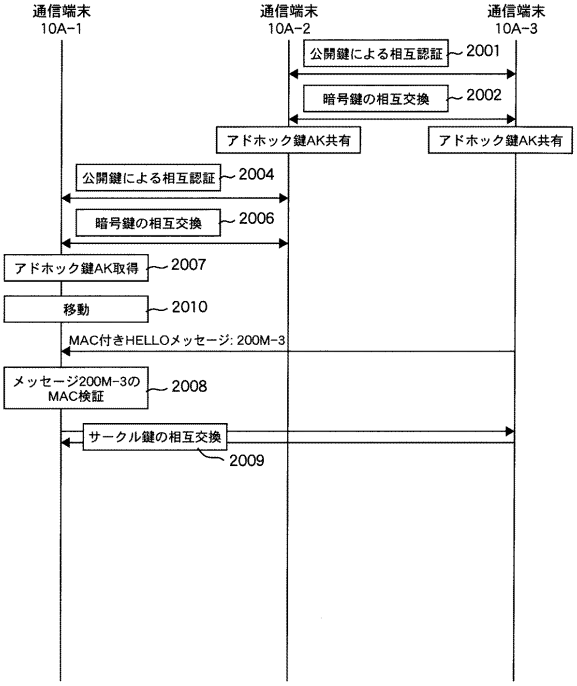
【図２１】

図　２１



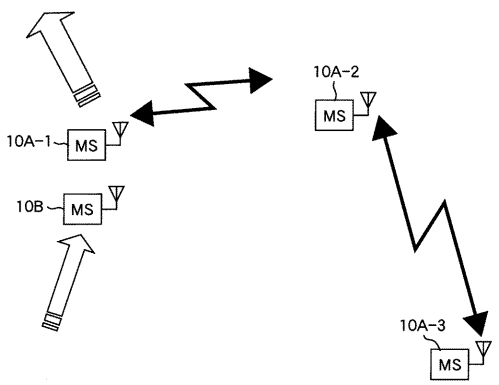
【図２２】

図　２２



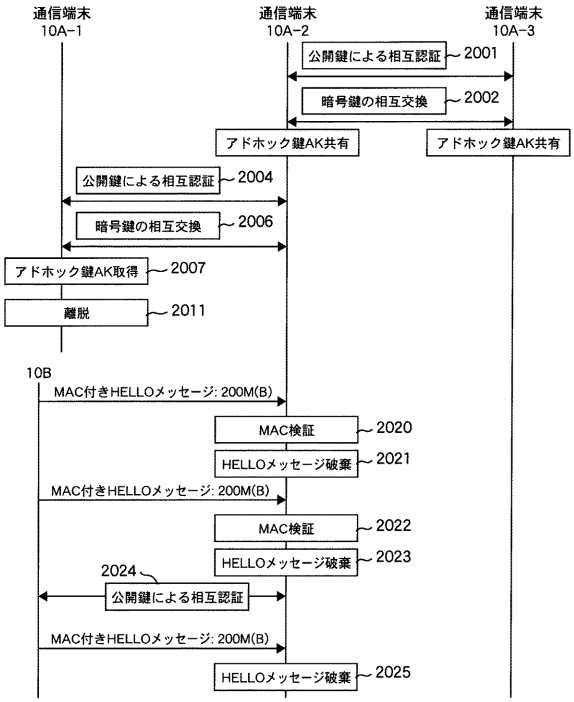
【図２３】

図　２３



【図２４】

図　２４



フロントページの続き

(72)発明者　福澤　寧子
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
(72)発明者　松井　進
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
(72)発明者　河村　英之
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所情報制御システム事業部内

Ｆターム(参考) 5K033 AA03　AA08　CC01　DA19　DB16　DB17　DB18　EA07　EC01　EC03