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

特許第4701434号
(P4701434)

(45)発行日　平成23年6月15日(2011.6.15)　(24)登録日　平成23年3月18日(2011.3.18)

(51)Int.Cl.　　F I
H04L 9/32 (2006.01)　　H04L 9/00 673B
H04W 12/04 (2009.01)　　H04L 9/00 673C
　　H04Q 7/00 182

請求項の数 16　(全 30 頁)

(21)出願番号　特願2007-535571 (P2007-535571)
(86)(22)出願日　平成18年9月15日 (2006.9.15)
(86)国際出願番号　PCT/JP2006/318433
(87)国際公開番号　WO2007/032499
(87)国際公開日　平成19年3月22日 (2007.3.22)
審査請求日　平成20年3月6日 (2008.3.6)
(31)優先権主張番号　特願2005-271144 (P2005-271144)
(32)優先日　平成17年9月16日 (2005.9.16)
(33)優先権主張国　日本国(JP)

(73)特許権者　301022471
独立行政法人情報通信研究機構
東京都小金井市貫井北町４－２－１
(74)代理人　100130111
弁理士　新保　斉
(72)発明者　井上　大介
東京都小金井市貫井北町４－２－１　独立行政法人情報通信研究機構内
(72)発明者　黒田　正博
東京都小金井市貫井北町４－２－１　独立行政法人情報通信研究機構内

最終頁に続く

(54)【発明の名称】無線通信システム及び無線通信方法

(57)【特許請求の範囲】
【請求項１】
単数または複数の無線通信端末と、それに対応する少なくとも１基のアクセスポイントから構成される無線通信システムであって、
該アクセスポイントには少なくとも、
該無線通信端末に固有の現在及び次の識別番号を記憶する識別番号記憶部と、
該無線通信端末との間で共有するハッシュ鍵を記憶する鍵記憶部と、
乱数を発生させる乱数発生処理部と、
鍵付ハッシュ関数による演算処理を行うハッシュ関数演算処理部と、該無線通信端末との通信及び、各処理部への制御処理を行う制御通信処理部と
を備えて、
該制御通信処理部の制御に従っていずれかの無線通信端末について、ハッシュ関数演算処理部で現在の識別番号及びハッシュ鍵、第１の乱数を用いて第２の識別番号を発生させ、さらに該第２の識別番号及びハッシュ鍵、第２の乱数を用いて第３の識別番号を発生させると共に、
該制御通信処理部が当該無線通信端末に該第１及び第２の乱数を含む初期化指示信号を送信し、該識別番号記憶部に記憶した現在の識別番号を第２の識別番号に更新し、さらに次の識別番号を第３の識別番号に設定する一方、
該無線通信端末には少なくとも、
該アクセスポイントとの通信を行う通信部と、

自己に固有の現在及び次の識別番号を記憶する自番号記憶部と、
該アクセスポイントとの間で共有するハッシュ鍵を記憶する鍵記憶部と、
鍵付ハッシュ関数による演算処理を行うハッシュ関数演算処理部と、
を備えて、
通信部が該アクセスポイントから該初期化指示信号を受信すると、ハッシュ関数演算処理部が自番号記憶部に記憶された現在の識別番号及びハッシュ鍵、該第１の乱数を用いて第２の識別番号を発生させ、さらに該第２の識別番号及びハッシュ鍵、第２の乱数を用いて第３の識別番号を発生させると共に、該自番号記憶部に記憶した現在の識別番号を第２の識別番号に更新し、さらに次の識別番号を第３の識別番号に設定する
ことを特徴とする無線通信システム。

【請求項２】
前記アクセスポイントの制御通信処理部が、
少なくとも１回以上、前記初期化指示信号を受信した後に、前記無線通信端末に対して所定の周期で更新指示信号を送信する構成であって、
該制御通信処理部の制御に従っていずれかの無線通信端末について、ハッシュ関数演算処理部で次の識別番号及びハッシュ鍵、第３の乱数を用いて第４の識別番号を発生させると共に、
該制御通信処理部が当該無線通信端末に該第３の乱数を含む更新指示信号を送信し、該識別番号記憶部に記憶した現在の識別番号を次の識別番号に更新し、さらに次の識別番号を該第４の識別番号に更新する一方、
該無線通信端末の通信部が、
該アクセスポイントから該更新指示信号を受信すると、ハッシュ関数演算処理部が自番号記憶部に記憶された次の識別番号及びハッシュ鍵、該第３の乱数を用いて第４の識別番号を発生させると共に、該自番号記憶部に記憶した現在の識別番号を次の識別番号に更新し、さらに次の識別番号を第４の識別番号に更新する
請求項１に記載の無線通信システム。

【請求項３】
前記無線通信端末が、単位時間当たりの通信量を測定してサービス不能攻撃を検出する攻撃検出処理部を備え、攻撃検出時に、該自番号記憶部に記憶した現在の識別番号を次の識別番号に更新すると共に、前記通信部が、アクセスポイントに対して攻撃検出信号を送信し、次いで、アクセスポイントの制御通信処理部が該攻撃検出信号を受信すると、前記識別番号記憶部に記憶した現在の識別番号を次の識別番号に更新すると共に、前記ハッシュ関数演算処理部で更新後の現在の識別番号及びハッシュ鍵、第３の乱数を用いて第４の識別番号を発生させ、該制御通信処理部が当該無線通信端末に該第３の乱数を含む乱数通知信号を送信し、次の識別番号を該第４の識別番号に更新し、
次いで無線通信端末の通信部が該乱数通知信号を受信すると、ハッシュ関数演算処理部が自番号記憶部に記憶された更新後の現在の識別番号及びハッシュ鍵、該第３の乱数を用いて第４の識別番号を発生させると共に、該自番号記憶部に記憶した次の識別番号を第４の識別番号に更新する請求項１又は２に記載の無線通信システム。

【請求項４】
前記無線通信端末の通信部が、
前記アクセスポイントからの初期化指示信号又は更新指示信号を受信すると、該アクセスポイントに向けて確認信号を送信すると共に、
前記アクセスポイントの制御通信処理部が、
該確認信号を受信したことを契機に前記識別番号記憶部に記憶した現在の識別番号及び次の識別番号を更新する
請求項１ないし３のいずれかに記載の無線通信システム。

【請求項５】
前記アクセスポイントにおいて、
前記識別番号記憶部が、前記更新前の現在の識別番号と、更新後の現在の識別番号と、

更新後の次の識別番号とを同時に記憶可能な構成であって、
前記制御通信処理部が、
前記確認信号を受信する前に当該無線通信端末から各識別番号のいずれかからの通信を受信するとそれを検知する検知部と、
検知の結果が更新前の現在の識別番号である場合には再度更新指示信号を送信する一方、検知の結果が更新後の次の識別番号である場合には該識別番号記憶部に記憶した更新前の現在の識別番号を更新後の次の識別番号に更新する識別番号同期制御部と
からなることを特徴とする
請求項４に記載の無線通信システム。
【請求項６】
前記アクセスポイントが、
制御通信処理部における信号の送信時から計時を開始するタイマ部を備えると共に、
前記制御通信処理部に存在確認信号送信部を備える一方、
前記無線通信端末の通信部が、
該存在確認信号を受信すると存在確認応答を送信する存在確認応答部を備える構成において、
更新指示信号の送信から所定の時間が経過したことをタイマ部が検知しても前記確認信号が受信できない場合に、該存在確認信号送信部が前記無線通信端末の次の識別番号に向けて存在確認信号を送信し、
このとき制御通信処理部は、所定の時間が経過したことをタイマ部が検知しても存在確認応答が受信できない場合には再度更新指示信号を送信する一方、存在確認応答を受信した場合には前記識別番号記憶部に記憶した現在の識別番号を次の識別番号に更新する
請求項５に記載の無線通信システム。
【請求項７】
単数または複数の無線通信端末と、それに対応する少なくとも１基のアクセスポイントから構成される無線通信システムであって、
該アクセスポイントには少なくとも、
該無線通信端末に固有の識別番号を記憶する識別番号記憶部と、
該無線通信端末との間で共有するハッシュ鍵を記憶する鍵記憶部と、
乱数を発生させる乱数発生処理部と、
鍵付ハッシュ関数による演算処理を行うハッシュ関数演算処理部と、該無線通信端末との通信及び、各処理部への制御処理を行う制御通信処理部と
を備えて、
該制御通信処理部の制御に従っていずれかの無線通信端末について、ハッシュ関数演算処理部で現在の識別番号及びハッシュ鍵、乱数を用いて第２の識別番号を発生させると共に、該制御通信処理部が当該無線通信端末に乱数を含む更新指示信号を少なくとも所定の周期で送信し、該識別番号記憶部に記憶した現在の識別番号を第２の識別番号に更新する一方、
該無線通信端末には少なくとも、
該アクセスポイントとの通信を行う通信部と、
自己に固有の識別番号を記憶する自番号記憶部と、
該アクセスポイントとの間で共有するハッシュ鍵を記憶する鍵記憶部と、
鍵付ハッシュ関数による演算処理を行うハッシュ関数演算処理部と、
を備えて、
通信部が該アクセスポイントから該更新指示信号を受信すると、ハッシュ関数演算処理部が自番号記憶部に記憶された現在の識別番号及びハッシュ鍵、乱数を用いて第２の識別番号を発生させると共に、該自番号記憶部に記憶した現在の識別番号を第２の識別番号に更新する
ことを特徴とする無線通信システム。
【請求項８】

前記無線通信端末の識別番号が、ＭＡＣ(Media Access Control)アドレスである請求項１ないし７のいずれかに記載の無線通信システム。

【請求項９】

単数または複数の無線通信端末と、それに対応する少なくとも１基のアクセスポイントから構成される無線通信システムにおける通信方法であって、

アクセスポイント及び無線通信端末が予めハッシュ鍵を共有して各々の鍵記憶部に記憶しておき、

アクセスポイントの制御通信処理部の制御に従い、いずれかの無線通信端末について、アクセスポイントのハッシュ関数演算処理部が現在の識別番号及びハッシュ鍵、第１の乱数を用いて第２の識別番号を発生させ、さらに該第２の識別番号及びハッシュ鍵、第２の乱数を用いて第３の識別番号を発生させるアクセスポイント側識別番号発生ステップ、

該制御通信処理部が当該無線通信端末に該第１及び第２の乱数を含む初期化指示信号を送信する初期化指示ステップ、

該アクセスポイント側識別番号発生ステップの後のいずれかの時点において該識別番号記憶部に記憶した現在の識別番号を第２の識別番号に更新し、さらに次の識別番号を第３の識別番号に設定するアクセスポイント側識別番号初期化ステップ、

無線通信端末の通信部が該アクセスポイントから該初期化指示信号を受信すると、ハッシュ関数演算処理部が自番号記憶部に記憶された現在の識別番号及びハッシュ鍵、該第１の乱数を用いて第２の識別番号を発生させ、さらに該第２の識別番号及びハッシュ鍵、第２の乱数を用いて第３の識別番号を発生させる端末側識別番号発生ステップ、

該自番号記憶部に記憶した現在の識別番号を第２の識別番号に更新し、さらに次の識別番号を第３の識別番号に設定する端末側識別番号初期化ステップ

を有することを特徴とする無線通信方法。

【請求項１０】

前記アクセスポイントの制御通信処理部が、

少なくとも１回以上、前記初期化指示信号を受信した後に、前記無線通信端末に対して所定の周期で更新指示信号を送信する構成であって、

該制御通信処理部の制御に従っていずれかの無線通信端末について、ハッシュ関数演算処理部で次の識別番号及びハッシュ鍵、第３の乱数を用いて第４の識別番号を発生させるアクセスポイント側識別番号定期発生ステップ、

該制御通信処理部が当該無線通信端末に該第３の乱数を含む更新指示信号を送信する更新指示ステップ、

該アクセスポイント側識別番号定期発生ステップの後のいずれかの時点において該識別番号記憶部に記憶した現在の識別番号を次の識別番号に更新し、さらに次の識別番号を該第４の識別番号に更新するアクセスポイント側識別番号定期更新ステップ、

該無線通信端末の通信部が該アクセスポイントから該更新指示信号を受信すると、ハッシュ関数演算処理部が自番号記憶部に記憶された次の識別番号及びハッシュ鍵、該第３の乱数を用いて第４の識別番号を発生させる端末側識別番号定期発生ステップ、

該自番号記憶部に記憶した現在の識別番号を次の識別番号に更新し、さらに次の識別番号を第４の識別番号に更新する端末側識別番号定期更新ステップ

を有することを特徴とする請求項９に記載の無線通信方法。

【請求項１１】

前記無線通信方法の端末側識別番号初期化ステップの後のいずれかの契機において、

前記無線通信端末の攻撃検出処理部が、単位時間当たりの通信量を測定してサービス不能攻撃を検出するサービス不能攻撃検出ステップ、攻撃検出時に、該自番号記憶部に記憶した現在の識別番号を次の識別番号に更新すると共に、前記通信部が、アクセスポイントに対して攻撃検出信号を送信する端末側識別番号緊急更新ステップ、アクセスポイントの制御通信処理部が該攻撃検出信号を受信すると、前記識別番号記憶部に記憶した現在の識別番号を次の識別番号に更新すると共に、前記ハッシュ関数演算処理部で更新後の現在の識別番号及びハッシュ鍵、第３の乱数を用いて第４の識別番号を発生させ、該制御通信処

理部が当該無線通信端末に該第３の乱数を含む乱数通知信号を送信し、次の識別番号を該第４の識別番号に更新するアクセスポイント側識別番号緊急更新ステップ、
無線通信端末の通信部が該乱数通知信号を受信すると、ハッシュ関数演算処理部が自番号記憶部に記憶された更新後の現在の識別番号及びハッシュ鍵、該第３の乱数を用いて第４の識別番号を発生させると共に、該自番号記憶部に記憶した次の識別番号を第４の識別番号に更新する端末側次識別番号緊急更新ステップ
を有することを特徴とする請求項９又は１０に記載の無線通信方法。
【請求項１２】
前記無線通信方法において、初期化指示ステップ又は更新指示ステップに続き、
前記無線通信端末の通信部がアクセスポイントに向けて確認信号を送信する確認信号送信ステップ、
アクセスポイントの制御通信処理部が、該確認信号を受信する確認信号受信ステップを経て
前記アクセスポイント側識別番号初期化ステップ又は前記アクセスポイント側識別番号定期更新ステップ
を実行する
請求項９ないし１１のいずれかに記載の無線通信方法。
【請求項１３】
前記確認信号送信ステップと確認信号受信ステップとの間において、
アクセスポイントの識別番号記憶部に無線通信端末の前記更新前の現在の識別番号と、更新後の現在の識別番号と、更新後の次の識別番号とを同時に記憶し、制御通信処理部に設けた検知部が当該無線通信端末から各識別番号のいずれかからの通信の有無を検知する検知ステップ、
検知の結果が更新前の現在の識別番号である場合には前記更新指示ステップに戻る一方、
検知の結果が更新後の次の識別番号である場合には前記アクセスポイント側識別番号緊急更新ステップ以降を実行する
請求項１２に記載の無線通信方法。
【請求項１４】
前記更新指示ステップから所定の時間が経過したことをアクセスポイントのタイマ部が検知しても前記確認信号受信ステップに到らない場合に、
アクセスポイントの制御通信処理部に設けた存在確認信号送信部が前記無線通信端末の次の識別番号に向けて存在確認信号を送信する存在確認ステップ、
該存在確認信号に対して無線通信端末からの存在確認応答が所定時間内に受信できない場合には前記更新指示ステップに戻る一方、
存在確認応答を受信した場合には前記アクセスポイント側識別番号定期更新ステップを実行する
請求項１３に記載の無線通信方法。
【請求項１５】
単数または複数の無線通信端末と、それに対応する少なくとも１基のアクセスポイントから構成される無線通信システムにおける通信方法であって、
アクセスポイント及び無線通信端末が予めハッシュ鍵を共有して各々の鍵記憶部に記憶しておき、
アクセスポイントの制御通信処理部の制御に従い、いずれかの無線通信端末について、アクセスポイントのハッシュ関数演算処理部が現在の識別番号及びハッシュ鍵、乱数を用いて第２の識別番号を発生させるアクセスポイント側識別番号発生ステップ、
該制御通信処理部が当該無線通信端末に乱数を含む更新指示信号を少なくとも所定の周期で送信する更新指示ステップ、
無線通信端末の通信部が該アクセスポイントから該更新指示信号を受信すると、ハッシュ関数演算処理部が自番号記憶部に記憶された現在の識別番号及びハッシュ鍵、乱数を用

いて第２の識別番号を発生させる端末側識別番号発生ステップ、
無線通信端末の自番号記憶部に記憶した現在の識別番号を第２の識別番号に更新する端末側識別番号更新ステップ、
該更新指示ステップの後のいずれかの時点においてアクセスポイントの識別番号記憶部に記憶した現在の識別番号を第２の識別番号に更新するアクセスポイント側識別番号更新ステップ
を有することを特徴とする無線通信方法。
【請求項１６】
前記無線通信端末の識別番号が、ＭＡＣ(Media Access Control)アドレスである請求項９ないし１５のいずれかに記載の無線通信方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は無線通信システム及び無線通信方法に関し、特に無線通信システムにおける無線通信端末に対する追跡とサービス不能攻撃の防御方法に係る技術である。
【背景技術】
【０００２】
近年、第３世代（３Ｇ）移動体通信や、IEEE802.11規格の無線ＬＡＮ、IEEE802.16規格の無線ＭＡＮなどが注目されている。これらのサービスによって音声や映像、さらに電子商取引などがモバイル環境で利用できるようになる。
同時に、無線通信ネットワークにおけるセキュリティ問題が深刻化している。こうした脅威からネットワークを保護するために、暗号化技術や認証技術が必要とされ、開発が進められている。
【０００３】
例えば、非特許文献１に開示されるような第３世代移動体通信システムの標準化プロジェクトにおけるセキュリティ機構や、非特許文献２に開示されるようなIEEE802.1X規格におけるセキュリティ機構、非特許文献３に開示されるような無線ＬＡＮに向けた802.11i規格におけるセキュリティ機構が知られている。
【０００４】
【非特許文献１】3rd Generation Partnership Project, "3G Security; Security architecture (Release 6)," 3GPP TS 33.102, V6.3.0, 2004年
【非特許文献２】LAN MAN Standards Committee of the IEEE Computer Society, "IEEE Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control," IEEE Standard 802.1X, 2001年
【非特許文献３】LAN MAN Standards Committee of the IEEE Computer Society, "IEEE 802.11 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Amendment 6: Medium Access Control (MAC) Security Enhancements," IEEE Standard 802.11i, 2004年
【０００５】
しかし、従来の技術では上述したように暗号化及び認証技術については改善が進んできたが、無線通信端末の追跡やサービス不能攻撃（Denial of Service attack、以下ではＤｏＳ攻撃と呼ぶ）に対する防御方法については課題として残されている。
【０００６】
特許文献３は、無線通信システムにおける方法と異なるが、移動体の登録情報を信頼されるクライアントに対してのみ開示可能にするための技術である。本技術はプライバシを保護した登録クライアントの情報管理システムを提供することを目的として、情報管理対象となる登録クライアントの登録情報を、時間の経過とともに変化する秘密識別子として登録する。
秘密識別子は、その生成情報としての識別子と、基準時刻と更新時間間隔に対するハッシュ値として算出され、信頼クライアントにのみ生成情報を通知する。本構成により移動

体等の登録クライアントの登録情報を特定の検索クライアント（信頼クライアント）に対してのみ開示可能な構成を開示する。

【０００７】

【特許文献３】特開2002-268950号公報

【０００８】

該構成において、秘密識別子の生成情報は、少なくとも各装置またはユーザに対応付けられた識別子と、基準時刻と、更新時間とを示す値と乱数とを含むデータであり、秘密識別子は、生成情報に対して一方向性ハッシュ関数を適用して算出される値である。

【０００９】

本技術は地理位置情報管理システムにおけるものであって、登録クライアントの識別子からの検索と、位置情報の指定による逆引き検索が可能な構成においても、両検索を併用した登録クライアントの追跡が困難になり、登録クライアント情報の漏洩が防止される。

このように、従来技術では秘密識別子を時間的に変化させて追跡を困難とするような技術は提供されている。

【００１０】

しかし、本技術では識別子の他に秘密識別子を用いなければならないため、一般的な無線通信システムに適用することはできない。また端末に対する攻撃という観点から創出された技術であるためにサービス不能攻撃に対応することができない。

端末追跡を回避し、サービス不能攻撃に対応した無線通信システムにおける防御方法を提供するためには、無線通信端末の識別番号には秘密識別子を用いることはできず、またサービス不能攻撃に対して能動的な対策を有する方法でなければならない。

【００１１】

このような方法の１つとして、本件発明者らによって非特許文献４に開示されるようにＭＡＣアドレスそのものを攻撃時や定期的に更新する技術が知られている。本技術では、アクセスポイントがいずれかの無線通信端末について、現在のＭＡＣアドレスと共有しているハッシュ鍵、乱数を用いてハッシュ関数演算し、次のＭＡＣアドレスを発生させる。そして、攻撃時には無線通信端末からアクセスポイントに更新の要求を行うことで、アクセスポイントが乱数を通知し、無線通信端末側及びアクセスポイント側でＭＡＣアドレスを同期させる。

【００１２】

本技術は、識別番号を標的として行われる端末追跡やＤｏＳ攻撃に対し、通信システムに大きな変更を加えることなく効果的に回避しうる技術として、従来にはない効果を有するものであった。

しかし、この方法によると、乱数を新しく受信してＭＡＣアドレスを更新するまでの間は攻撃にさらされることになり、強力な攻撃の場合には著しく通信が滞る恐れがある。

従って、より高速にＭＡＣアドレスを更新することができる技術が求められている。

【００１３】

【非特許文献４】D.Inoue, R.Nomura, M.Kuroda "Transient MAC Address Scheme for Untraceability and DoS Attack Resiliency on Wireless Network" Proc. 4th annual Wireless Telecommunications Symposium,2005.

【発明の開示】

【発明が解決しようとする課題】

【００１４】

本発明は、上記従来技術の有する問題点に鑑みて創出されたものであり、識別番号を標的として行われる端末追跡やＤｏＳ攻撃に対し、一般的な無線通信システムに大きな変更を加えることなく効果的に回避しうる技術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】

【００１５】

本発明は、上記の課題を解決するために、次のような無線通信システムを提供する。すなわち、端末追跡やＤｏＳ攻撃から防御するためにＭＡＣ（Media Access Control)アド

レス等の無線端末の識別番号を動的に変化させることで、識別番号を標的とした攻撃を回避する。その際、識別番号をアクセスポイントと同期を保ち通信の継続性を維持する。

【００１６】

本発明の請求項１に記載の発明は、単数または複数の無線通信端末と、それに対応する少なくとも１基のアクセスポイントから構成される無線通信システムであり、次のような構成を有する。

アクセスポイントには少なくとも、該無線通信端末に固有の現在及び次の識別番号を記憶する識別番号記憶部と、該無線通信端末との間で共有するハッシュ鍵を記憶する鍵記憶部と、乱数を発生させる乱数発生処理部と、鍵付ハッシュ関数による演算処理を行うハッシュ関数演算処理部と、該無線通信端末との通信及び、各処理部への制御処理を行う制御通信処理部とを備える。

【００１７】

そしてアクセスポイントは、制御通信処理部の制御に従っていずれかの無線通信端末について、ハッシュ関数演算処理部で現在の識別番号及びハッシュ鍵、第１の乱数を用いて第２の識別番号を発生させ、さらに該第２の識別番号及びハッシュ鍵、第２の乱数を用いて第３の識別番号を発生させる。

さらに、制御通信処理部が当該無線通信端末に該第１及び第２の乱数を含む初期化指示信号を送信し、該識別番号記憶部に記憶した現在の識別番号を第２の識別番号に更新し、さらに次の識別番号を第３の識別番号に設定する。

【００１８】

無線通信端末には少なくとも、アクセスポイントとの通信を行う通信部と、自己に固有の現在及び次の識別番号を記憶する自番号記憶部と、アクセスポイントとの間で共有するハッシュ鍵を記憶する鍵記憶部と、鍵付ハッシュ関数による演算処理を行うハッシュ関数演算処理部とを備える。

そして、通信部が該アクセスポイントから該初期化指示信号を受信すると、ハッシュ関数演算処理部が自番号記憶部に記憶された現在の識別番号及びハッシュ鍵、該第１の乱数を用いて第２の識別番号を発生させ、さらに該第２の識別番号及びハッシュ鍵、第２の乱数を用いて第３の識別番号を発生させると共に、該自番号記憶部に記憶した現在の識別番号を第２の識別番号に更新し、さらに次の識別番号を第３の識別番号に設定する。

【００１９】

本発明の請求項２の技術は、定期的に識別番号を更新する技術に係る。上記のアクセスポイントの制御通信処理部が、少なくとも１回以上、前記初期化指示信号を受信した後に、前記無線通信端末に対して所定の周期で更新指示信号を送信する構成を提供する。

制御通信処理部の制御に従っていずれかの無線通信端末について、ハッシュ関数演算処理部で次の識別番号及びハッシュ鍵、第３の乱数を用いて第４の識別番号を発生させると共に、該制御通信処理部が当該無線通信端末に該第３の乱数を含む更新指示信号を送信し、該識別番号記憶部に記憶した現在の識別番号を次の識別番号に更新し、さらに次の識別番号を該第４の識別番号に更新する。

【００２０】

一方、無線通信端末の通信部が、アクセスポイントから該更新指示信号を受信すると、ハッシュ関数演算処理部が自番号記憶部に記憶された次の識別番号及びハッシュ鍵、該第３の乱数を用いて第４の識別番号を発生させると共に、該自番号記憶部に記憶した現在の識別番号を次の識別番号に更新し、さらに次の識別番号を第４の識別番号に更新する。

【００２１】

本発明の請求項３の技術は、攻撃を受けた緊急時に識別番号を更新する技術に係る。

本構成によれば、無線通信端末が、単位時間当たりの通信量を測定してサービス不能攻撃を検出する攻撃検出処理部を備え、攻撃検出時に、該自番号記憶部に記憶した現在の識別番号を次の識別番号に更新すると共に、前記通信部が、アクセスポイントに対して攻撃検出信号を送信する。

【００２２】

次いで、アクセスポイントの制御通信処理部が該攻撃検出信号を受信すると、前記識別番号記憶部に記憶した現在の識別番号を次の識別番号に更新すると共に、前記ハッシュ関数演算処理部で更新後の現在の識別番号及びハッシュ鍵、第３の乱数を用いて第４の識別番号を発生させ、該制御通信処理部が当該無線通信端末に該第３の乱数を含む乱数通知信号を送信し、次の識別番号を該第４の識別番号に更新する。

【００２３】

次いで無線通信端末の通信部が該乱数通知信号を受信すると、ハッシュ関数演算処理部が自番号記憶部に記憶された更新後の現在の識別番号及びハッシュ鍵、該第３の乱数を用いて第４の識別番号を発生させると共に、該自番号記憶部に記憶した次の識別番号を第４の識別番号に更新する。

【００２４】

本発明の請求項４に係る技術は、無線通信端末の通信部が、アクセスポイントからの初期化指示信号又は更新指示信号を受信すると、該アクセスポイントに向けて確認信号を送信する構成である。

そして、前記アクセスポイントの制御通信処理部が、確認信号を受信したことを契機に前記識別番号記憶部に記憶した現在の識別番号及び次の識別番号を更新することを特徴とする。

【００２５】

請求項５の発明は、前記アクセスポイントにおいて、識別番号記憶部が、前記更新前の現在の識別番号と、更新後の現在の識別番号と、更新後の次の識別番号とを同時に記憶可能な構成を用いる。

制御通信処理部が、確認信号を受信する前に当該無線通信端末から各識別番号のいずれかからの通信を受信するとそれを検知する検知部と、検知の結果が更新前の現在の識別番号である場合には再度更新指示信号を送信する一方、検知の結果が更新後の次の識別番号である場合には該識別番号記憶部に記憶した更新前の現在の識別番号を更新後の次の識別番号に更新する識別番号同期制御部とからなることを特徴とする。

【００２６】

請求項６に記載の発明は前記アクセスポイントが、制御通信処理部における信号の送信時から計時を開始するタイマ部を備えると共に、前記制御通信処理部に存在確認信号送信部を備える一方、無線通信端末の通信部が、該存在確認信号を受信すると存在確認応答を送信する存在確認応答部を備える。

本構成において、更新指示信号の送信から所定の時間が経過したことをタイマ部が検知しても前記確認信号が受信できない場合に、該存在確認信号送信部が前記無線通信端末の次の識別番号に向けて存在確認信号を送信する。

このとき制御通信処理部は、所定の時間が経過したことをタイマ部が検知しても存在確認応答が受信できない場合には再度更新指示信号を送信する一方、存在確認応答を受信した場合には前記識別番号記憶部に記憶した現在の識別番号を次の識別番号に更新する。

【００２７】

請求項７に記載の発明は、上記と同様の構成からなる無線通信システムであって、アクセスポイントには少なくとも、無線通信端末に固有の識別番号を記憶する識別番号記憶部と、無線通信端末との間で共有するハッシュ鍵を記憶する鍵記憶部と、乱数を発生させる乱数発生処理部と、鍵付ハッシュ関数による演算処理を行うハッシュ関数演算処理部と、無線通信端末との通信及び、各処理部への制御処理を行う制御通信処理部とを備える。

そして、制御通信処理部の制御に従っていずれかの無線通信端末について、ハッシュ関数演算処理部で現在の識別番号及びハッシュ鍵、乱数を用いて第２の識別番号を発生させると共に、該制御通信処理部が当該無線通信端末に乱数を含む更新指示信号を少なくとも所定の周期で送信し、該識別番号記憶部に記憶した現在の識別番号を第２の識別番号に更新する。

【００２８】

一方、該無線通信端末には少なくとも、アクセスポイントとの通信を行う通信部と、自

己に固有の識別番号を記憶する自番号記憶部と、アクセスポイントとの間で共有するハッシュ鍵を記憶する鍵記憶部と、鍵付ハッシュ関数による演算処理を行うハッシュ関数演算処理部とを備える。

そして、通信部が該アクセスポイントから該更新指示信号を受信すると、ハッシュ関数演算処理部が自番号記憶部に記憶された現在の識別番号及びハッシュ鍵、乱数を用いて第２の識別番号を発生させると共に、該自番号記憶部に記憶した現在の識別番号を第２の識別番号に更新する。

【００２９】

請求項８に記載の発明は、前記無線通信端末の識別番号が、ＭＡＣ(Media Access Control)アドレスであることを特徴とする。

【００３０】

請求項９に記載の発明は、単数または複数の無線通信端末と、それに対応する少なくとも１基のアクセスポイントから構成される無線通信システムにおける通信方法を提供するものである。

該方法において、アクセスポイント及び無線通信端末が予めハッシュ鍵を共有して各々の鍵記憶部に記憶しておき、アクセスポイントの制御通信処理部の制御に従い、いずれかの無線通信端末について、アクセスポイントのハッシュ関数演算処理部が現在の識別番号及びハッシュ鍵、第１の乱数を用いて第２の識別番号を発生させ、さらに該第２の識別番号及びハッシュ鍵、第２の乱数を用いて第３の識別番号を発生させるアクセスポイント側識別番号発生ステップを有する。

【００３１】

アクセスポイント側識別番号初期化ステップの前後又は同時に、該制御通信処理部が当該無線通信端末に該第１及び第２の乱数を含む初期化指示信号を送信する初期化指示ステップを有する。

該アクセスポイント側識別番号発生ステップの後のいずれかの時点において該識別番号記憶部に記憶した現在の識別番号を第２の識別番号に更新し、さらに次の識別番号を第３の識別番号に設定するアクセスポイント側識別番号初期化ステップを有する。

次いで無線通信端末の通信部が該アクセスポイントから該初期化指示信号を受信すると、ハッシュ関数演算処理部が自番号記憶部に記憶された現在の識別番号及びハッシュ鍵、該第１の乱数を用いて第２の識別番号を発生させ、さらに該第２の識別番号及びハッシュ鍵、第２の乱数を用いて第３の識別番号を発生させる端末側識別番号発生ステップ、該自番号記憶部に記憶した現在の識別番号を第２の識別番号に更新し、さらに次の識別番号を第３の識別番号に設定する端末側識別番号初期化ステップを有する。

【００３２】

請求項１０に記載の発明は、アクセスポイントの制御通信処理部が、少なくとも１回以上、前記初期化指示信号を受信した後に、前記無線通信端末に対して所定の周期で更新指示信号を送信する構成であって、該制御通信処理部の制御に従っていずれかの無線通信端末について、ハッシュ関数演算処理部で次の識別番号及びハッシュ鍵、第３の乱数を用いて第４の識別番号を発生させるアクセスポイント側識別番号定期発生ステップ、制御通信処理部が当該無線通信端末に該第３の乱数を含む更新指示信号を送信する更新指示ステップを有する。

【００３３】

また、アクセスポイント側識別番号定期発生ステップの後のいずれかの時点において該識別番号記憶部に記憶した現在の識別番号を次の識別番号に更新し、さらに次の識別番号を該第４の識別番号に更新するアクセスポイント側識別番号定期更新ステップを有する。

さらに、無線通信端末の通信部が該アクセスポイントから該更新指示信号を受信すると、ハッシュ関数演算処理部が自番号記憶部に記憶された次の識別番号及びハッシュ鍵、該第３の乱数を用いて第４の識別番号を発生させる端末側識別番号定期発生ステップ、該自番号記憶部に記憶した現在の識別番号を次の識別番号に更新し、さらに次の識別番号を第４の識別番号に更新する端末側識別番号定期更新ステップを有することを特徴とする。

【００３４】
請求項１１に記載の発明は、緊急時に識別番号を更新する際の無線通信方法である。すなわち、無線通信方法の端末側識別番号初期化ステップの後のいずれかの契機において、前記無線通信端末の攻撃検出処理部が、単位時間当たりの通信量を測定してサービス不能攻撃を検出するサービス不能攻撃検出ステップ、攻撃検出時に、該自番号記憶部に記憶した現在の識別番号を次の識別番号に更新すると共に、前記通信部が、アクセスポイントに対して攻撃検出信号を送信する端末側識別番号緊急更新ステップ、アクセスポイントの制御通信処理部が該攻撃検出信号を受信すると、前記識別番号記憶部に記憶した現在の識別番号を次の識別番号に更新すると共に、前記ハッシュ関数演算処理部で更新後の現在の識別番号及びハッシュ鍵、第３の乱数を用いて第４の識別番号を発生させ、該制御通信処理部が当該無線通信端末に該第３の乱数を含む乱数通知信号を送信し、次の識別番号を該第４の識別番号に更新するアクセスポイント側識別番号緊急更新ステップを有する。
【００３５】
さらに、無線通信端末の通信部が該乱数通知信号を受信すると、ハッシュ関数演算処理部が自番号記憶部に記憶された更新後の現在の識別番号及びハッシュ鍵、該第３の乱数を用いて第４の識別番号を発生させると共に、該自番号記憶部に記憶した次の識別番号を第４の識別番号に更新する端末側次識別番号緊急更新ステップを有することを特徴とする。
【００３６】
請求項１２に記載の発明は、前記の無線通信方法において、初期化指示ステップ又は更新指示ステップに続き、無線通信端末の通信部がアクセスポイントに向けて確認信号を送信する確認信号送信ステップ、アクセスポイントの制御通信処理部が、該確認信号を受信する確認信号受信ステップを経て、前記アクセスポイント側識別番号初期化ステップ又は前記アクセスポイント側識別番号定期更新ステップを実行する構成を提供する。
【００３７】
請求項１３に記載の発明は、確認信号送信ステップと確認信号受信ステップとの間において、アクセスポイントの識別番号記憶部に無線通信端末の前記更新前の現在の識別番号と、更新後の現在の識別番号と、更新後の次の識別番号とを同時に記憶し、制御通信処理部に設けた検知部が当該無線通信端末から各識別番号のいずれかからの通信の有無を検知する検知ステップ、検知の結果が更新前の現在の識別番号である場合には前記更新指示ステップに戻る一方、検知の結果が更新後の次の識別番号である場合には前記アクセスポイント側識別番号緊急更新ステップ以降を実行することを特徴とする無線通信方法である。
【００３８】
請求項１４に記載の発明は、上記の更新指示ステップから所定の時間が経過したことをアクセスポイントのタイマ部が検知しても前記確認信号受信ステップに到らない場合に、アクセスポイントの制御通信処理部に設けた存在確認信号送信部が前記無線通信端末の次の識別番号に向けて存在確認信号を送信する存在確認ステップ、該存在確認信号に対して無線通信端末からの存在確認応答が所定時間内に受信できない場合には前記更新指示ステップに戻る。
一方、存在確認応答を受信した場合には前記アクセスポイント側識別番号定期更新ステップを実行する。
【００３９】
請求項１５に記載の発明は、単数または複数の無線通信端末と、それに対応する少なくとも１基のアクセスポイントから構成される無線通信システムにおける通信方法である。アクセスポイント及び無線通信端末が予めハッシュ鍵を共有して各々の鍵記憶部に記憶しておき、次の各ステップを処理する。
（１）アクセスポイントの制御通信処理部の制御に従い、いずれかの無線通信端末について、アクセスポイントのハッシュ関数演算処理部が現在の識別番号及びハッシュ鍵、乱数を用いて第２の識別番号を発生させるアクセスポイント側識別番号発生ステップ、
（２）該制御通信処理部が当該無線通信端末に乱数を含む更新指示信号を少なくとも所定の周期で送信する更新指示ステップ、

（３）無線通信端末の通信部が該アクセスポイントから該更新指示信号を受信すると、ハッシュ関数演算処理部が自番号記憶部に記憶された現在の識別番号及びハッシュ鍵、乱数を用いて第２の識別番号を発生させる端末側識別番号発生ステップ、

（４）無線通信端末の自番号記憶部に記憶した現在の識別番号を第２の識別番号に更新する端末側識別番号更新ステップ、

（５）該更新指示ステップの後のいずれかの時点においてアクセスポイントの識別番号記憶部に記憶した現在の識別番号を第２の識別番号に更新するアクセスポイント側識別番号更新ステップ。

【００４０】

請求項１６に記載の発明は、無線通信端末の識別番号が、ＭＡＣ(Media Access Control)アドレスである通信方法を提供するものである。

【発明の効果】

【００４１】

本発明は、アクセスポイントと無線通信端末において次に更新する識別番号を保持しているため、無線通信端末において攻撃を検知すると即座に識別番号を変更し、攻撃を逃れることが出来るようになる。

識別番号を定期的に変更することで端末追跡は困難になる。また無線通信端末がＤｏＳ攻撃を検知した際に緊急で識別番号を変更することができるので、ＤｏＳ攻撃の被害が軽減できる。

特に、更新を行う前の識別番号、行った後の識別番号に加え、その次の識別番号をアクセスポイントに保持することで、更新時におけるアクセスポイントと無線通信端末との間の通信に障害が生じても、効率的に再同期を行うことができる。

【発明を実施するための最良の形態】

【００４２】

以下、本発明の実施形態を、図面に示す実施例を基に説明する。なお、実施形態は下記に限定されるものではない。

図１は本発明に係る無線通信システムの全体構成図、図２はアクセスポイントの構成図、図３は無線通信端末の構成図である。

図１に示すように、本無線通信システム（１）は少なくとも１基のアクセスポイント（１０）と、それと通信可能な単数又は複数の無線通信端末（２０）・・から構成される。

【００４３】

通信の過程でアクセスポイント（１０）と無線通信端末（２０）等とは周知のように無線通信端末の識別番号であるＭＡＣアドレス（２）により端末の識別を行っており、アクセスポイント側ではメモリ等の記憶部に各端末のＭＡＣアドレスを記憶する。

ＭＡＣアドレスはＬＡＮなどで使用される伝送制御技術であるＭＡＣ（Media Access Control)で用いられる。ＭＡＣはフレーム(データの送受信単位)の送受信方法やフレームの形式、誤り検出方法などを規定している。

【００４４】

原則としてＭＡＣアドレスはグローバルなネットワークにおいても固有な識別番号として振られており、ネットワークインターフェースカード（ＮＩＣ）に対して４８ビットが定義されている。前半２４ビットがIEEEで管理されたベンダー固有の識別番号で、後半２４ビットが各ＮＩＣの連番である。

しかし、非特許文献５に記述されている通り、これらをソフトウェアからの制御によって自由に変更することは容易である。

【００４５】

【非特許文献５】William A. Arbaugh, Narendar Shankar, Y.C. Justin Wan and Kan Zhang, "Your 802.11 Wireless Network has No Clothes," IEEE Wireless Communications, Volume 9, Issue 6, pp.44-51, 2002年

【００４６】

この方法でＭＡＣアドレスを変更した場合、グローバルな固有性は確保出来ず、仮に同

一のローカルエリアにおいて同一のＭＡＣアドレスが存在した場合にはコンフリクトの原因となる。しかし、あるローカルエリアにおいて同一のＭＡＣアドレスがなければ、必ずしもグローバルなネットワークにおいて固有性が確保できなくとも、コンフリクト等の障害は発生しない。

【００４７】

このようなローカルエリアにおいての識別番号の固有性を確保するためには、各無線通信端末が独自に自己のＭＡＣアドレスを変更することはできない。従って、アクセスポイントが各無線通信端末のＭＡＣアドレスを変更する主導権を握る必要があり、本願はそのためのアクセスポイントにおける処理、無線通信端末における処理、特に両者の識別番号の同期方法を創出した技術である。

【００４８】

本実施例では３つの鍵を用いて通信を行うことを前提とする。すなわち、鍵として、フレーム本体を暗号化するための暗号化鍵と、フレームと共に送信されるメッセージ認証子を算出するための認証鍵と、さらに本願でＭＡＣアドレスの更新時に計算に用いるハッシュ鍵であるＴＭＡＣ鍵である。

これらの鍵を共有する方法は、周知の技術を用いることができる。また同様に通信するフレームの暗号化及び認証についても公知の技術を用いることができ、本願のＭＡＣアドレス変更技術と併用して使うことが望ましい。

【００４９】

本願のアクセスポイントは公知の無線ＬＡＮアクセスポイントなど、無線通信端末と通信を行う諸機構を備えるが、さらに次のような特徴を備える。

すなわち、アクセスポイント（１０）には演算手段（１１）と、メモリ手段（１２）と、実際の通信を司るアンテナを付属したネットワークカード（１３）を備えている。

【００５０】

そして、演算手段（１１）には乱数発生処理部（１１１）、ハッシュ関数演算処理部（１１２）、制御通信処理部（１１３）の諸機能を有している。制御通信処理部（１１３）は本発明によるＭＡＣアドレス変更に係る制御処理や、後述する指示信号の送信・確認信号の受信などの通信処理を司る他、特に検知部（１１４）及び識別番号同期制御部（１１５）を備えている。

【００５１】

さらにメモリ手段（１２）には通信する無線通信端末の識別番号（ＭＡＣアドレス）を記憶している識別番号記憶部（１２１）と、通信で用いる上記の暗号化鍵、認証鍵、ＴＭＡＣ鍵とを記憶する鍵記憶部（１２２）とを有している。言うまでもなく、これらは１個のメモリ上に記憶されていてよい。

【００５２】

次に、図３に示すように無線端末装置（２０）には上記のネットワークカード（１３）と対応して通信を行うアンテナを付属したネットワークカード（２１）と、演算手段（２２）、メモリ手段（２３）を備える。

演算手段にはネットワークカード（２１）を制御し通信を司る通信部（２２１）と、ハッシュ関数演算処理部（２２２）、攻撃検出処理部（２２３）の諸機能を有している。

【００５３】

さらにメモリ手段（２３）には自己の識別番号（ＭＡＣアドレス）を記憶している自番号記憶部（２３１）と、通信で用いる上記の暗号化鍵、認証鍵、ＴＭＡＣ鍵とを記憶する鍵記憶部（２３２）とを有している。上記同様、これらは１個のメモリ上に記憶されていてよい。

【００５４】

以上の構成において、本発明に係るアクセスポイント（１０）及び無線通信端末（２０）とは、最初にＭＡＣアドレスを設定する際の初期化制御、定期的にＭＡＣアドレスを更新する際の定期更新制御、攻撃を受けた時にＭＡＣアドレスを更新する際の緊急更新制御の３種類の制御信号通信を基本とする。

これらの通信はアクセスポイント（１０）における制御通信処理部（１１３）と、無線通信端末（２０）における通信部（２２１）との間で行う。

【００５５】

初期化制御について説述する。初期化制御は、無線通信端末（２０）とアクセスポイント（１０）において１つのＭＡＣアドレスを保持しており、通信が行えている状態であって、これから本願発明による技術を導入するための最初の工程である。

図４は初期化制御の流れ図である。まず乱数発生処理部（１１１）が２種類の乱数（第１乱数）$Rand_0$と（第２乱数）$Rand_1$を発生させる（Ｓ１）。ここで２つの乱数は現在の当該無線端末のＭＡＣアドレス１個に対応して２個発生させる。

【００５６】

次にハッシュ関数演算処理部（１１２）が、現在のＭＡＣアドレス$TMAC_0$と、発生した乱数$Rand_0$,$Rand_1$を用いて次の数１に示されるハッシュ関数を用いて第２及び第３の新しいＭＡＣアドレス$TMAC_1$と$TMAC_2$を算出（Ｓ２）する。数式に明らかなように、$TMAC_2$は$TMAC_1$の算出結果を用いて算出される。一方向ハッシュ関数については公知であり、演算方法も既存の方法を用いることができる。

【００５７】

（数１）

$$TMAC_1 = h(K_{tmac},\ TMAC_0 \ ||\ Rand_0)$$

$$TMAC_2 = h(K_{tmac},\ TMAC_1 \ ||\ Rand_1)$$

上記の式においてｈ（）はハッシュ関数、K_{tmac}はアクセスポイントと無線通信端末で共有しているTMAC鍵である。

【００５８】

算出されたＭＡＣアドレスについて、ハッシュ関数演算処理部においてローカルエリア内に重複したＭＡＣアドレスが存在しないか、重複確認（Ｓ３）を行う。このとき、識別番号記憶部（１２１）には後述するように各無線通信端末について更新前の現在の鍵（上記の例では$TMAC_0$）と、更新後の現在の鍵（上記の例では$TMAC_1$）、更新後の次の鍵（上記の例では$TMAC_2$）の３つの識別番号を記憶しておくことができるのでそのような構成の場合には新旧の識別番号と重複していないかを確認する。

【００５９】

もし重複したＭＡＣアドレスが存在した場合には、乱数発生ステップ（Ｓ１）に戻り、再びＳ２，Ｓ３の処理を行う。これにより、ローカルエリアにおけるＭＡＣアドレスの固有性が確保される。

重複確認（Ｓ３）で問題がなければ、２つのＭＡＣアドレスをメモリ内に一時格納（Ｓ４）する。

Ｓ１?Ｓ４に係るアクセスポイント側識別番号発生ステップが終了する。

【００６０】

そして、次に初期化指示ステップとして、制御通信処理部（１１３）は無線通信端末に対して初期化指示信号を送出する（Ｓ５）。

該初期化指示信号には、上記で発生させた２つの乱数$Rand_0$と$Rand_1$が含まれている。

【００６１】

図５は初期化制御のシーケンス図である。図５において左端の破線は無線通信端末(Mobile Device)が自己のＭＡＣアドレスをどのように認識しているか、右端の破線はアクセスポイント(Access Point)が当該無線通信端末のＭＡＣアドレスをどのように認識しているかを示している。

該初期化指示信号（Initial Update Command)の宛先は現在のＭＡＣアドレスである$TMAC_0$である。

通常は、初期化指示信号を通信部（２２１）で受信した無線通信端末からは確認信号Update Acknowledgeがアクセスポイントに返され、受信する（Ｓ６）。

【００６２】

そして、アクセスポイント側識別番号初期化ステップでは、制御通信処理部は識別番号

記憶部（１２１）に当該無線通信端末の現在のＭＡＣアドレスとして$TMAC_1$を、次のＭＡＣアドレスとして$TMAC_2$を記憶させる（Ｓ７）。

これにより、アクセスポイントにおいて当該無線通信端末のＭＡＣアドレスは$TMAC_1$を基本として認識される。もっとも、本願技術では$TMAC_0$ $TMAC_2$をいずれも記憶し、かつ通信可能としておくことで、どのＭＡＣアドレスからであっても通信が可能とすることができる。

【００６３】

同時に無線通信端末では、確認信号を送信すると共に、ハッシュ関数演算処理部（２２２）において上記アクセスポイントにおけるのと同様の演算処理を行い、初期化指示信号で受信した乱数を用いて変更するＭＡＣアドレス$TMAC_1$と$TMAC_2$を算出する。これが端末側識別番号発生ステップである。

続いて端末側識別番号初期化ステップとして、自番号記憶部（２３１）に記憶した現在のＭＡＣアドレスを$TMAC_1$に、次のＭＡＣアドレスを$TMAC_2$を設定して、以後は$TMAC_1$の無線通信端末として振る舞う。

【００６４】

以上が初期化制御の処理である。このような初期化の後、本願では定期的にＭＡＣアドレスを更新する定期更新制御を行うことができる。

図６には、定期更新制御のシーケンス図を示す。ここでは更新前の現在のＭＡＣアドレス$TMAC_i$から更新後の現在のＭＡＣアドレス$TMAC_{1+1}$に更新する過程を示している。定期更新の周期は、例えば１０秒間隔にて次の各処理を行うことが望ましい。その場合、アクセスポイントのメモリ手段には、各無線通信端末毎に次回の更新時間、更新間隔、通し番号（送信回数）を記録しておく。

【００６５】

定期更新時、アクセスポイントでは乱数発生処理部（１１１）が第３の乱数として$Rand_{i+1}$を発生させる。ここで、第１?第３の乱数と表記しているが、いずれも乱数を用いる契機に応じて表現を変えて説明をしているにすぎず、それぞれが固定の数値を持つものではない。例えば、第３の乱数という用語は毎回の定期更新時に繰り返し用いられるが、その都度乱数として異なる数値である。

【００６６】

そして、ハッシュ関数演算処理部（１１２）が第３の乱数を用いて次のＭＡＣアドレス（第４のＭＡＣアドレス）を算出する。ここでの第４の意味についても上記同様で、更新前に用いているＭＡＣアドレスを第２、更新後に用いているＭＡＣアドレスを第３とした時に、次のＭＡＣアドレスを意味している。

第４のＭＡＣアドレスについて初期化制御時と同様に重複確認する。以上によりアクセスポイント側識別番号定期発生ステップが終了する。

問題がなければ更新指示ステップとして、該第３の乱数を含む更新指示信号を無線通信端末の通信部（２２１）に向けて送る。

【００６７】

通常は、更新指示信号を通信部（２２１）で受信した無線通信端末からは確認信号Update Acknowledgeがアクセスポイントに返され、受信する。この受信の後、アクセスポイントにおいて前に計算していた第３のＭＡＣアドレスを、現在のＭＡＣアドレスに、第４のＭＡＣアドレスを次のＭＡＣアドレスに、それぞれ更新する。本処理がアクセスポイント側識別番号定期更新ステップである。

【００６８】

一方、無線通信端末では、確認信号を送信すると共に、ハッシュ関数演算処理部（２２２）において上記アクセスポイントにおけるのと同様の演算処理を行い、更新指示信号で受信した乱数を用いて変更するＭＡＣアドレス$TMAC_{i+1}$と$TMAC_{i+2}$を算出する。これが端末側識別番号定期発生ステップである。

続いて端末側識別番号定期更新ステップとして、自番号記憶部（２３１）に記憶した現在のＭＡＣアドレスを$TMAC_{i+1}$に、次のＭＡＣアドレスを$TMAC_{i+2}$を設定して、以後はTMAC

$_{i+1}$の無線通信端末として振る舞う。

【００６９】

本発明の無線通信システムでは、ＤｏＳ攻撃に対して効果的に防御を行うために、緊急のＭＡＣアドレス変更処理が可能である。次に緊急更新処理について説述する。図７は緊急更新処理のシーケンス図である。

まず、無線通信端末には攻撃検出処理部（２２３）が備えられていて、不正なフレームを一定量以上受信した場合に、サービス不能攻撃を受けたと検出するようにしている。これが本無線通信方法における緊急更新制御の処理である。

【００７０】

本実施例では、明らかに不正なフレームやメッセージ認証子を含まないフレームなどが所定の回数以上、例えば１秒間に１０フレーム以上受信した時に、攻撃検出を行う。

攻撃検出処理部（２２３）からの指示により、端末側識別番号緊急更新ステップとして、自番号記憶部（２３１）に記憶した現在のＭＡＣアドレスを$TMAC_i$から次のＭＡＣアドレス$TMAC_{i+1}$に即座に切り替える。そして以後は$TMAC_{i+1}$の無線通信端末として振る舞うため、その時点で攻撃から逃げることができる。このように、瞬時にＤｏＳ攻撃から防御できる点が本願の最大の特徴である。

【００７１】

ＭＡＣアドレスを更新した後に、通信部（２２１）はアクセスポイント（１０）に向けて攻撃検出信号Random Number Requestを送出する。該攻撃検出信号に応じてアクセスポイントの制御通信処理部（１１３）はまず識別番号記憶部から読み出して当該無線通信端末のＭＡＣアドレスを$TMAC_{i+1}$に更新する。このとき、アクセスポイントが、$TMAC_{i+1}$のＭＡＣアドレスである無線通信端末からの攻撃検出信号を受信できるのは、上述したように無線通信端末につき３つのＭＡＣアドレスを記憶し、通信出来る状態にあるからである。

【００７２】

さらに次のＭＡＣアドレスを準備するために、乱数発生処理部（１１１）は新たな第３の乱数を発生し、ハッシュ関数演算処理部（１１２）で第４のＭＡＣアドレス$TMAC_{i+2}$を算出し、重複検査の後、乱数通知信号（Random Number Supply)により該第３の乱数$Rand_{i+1}$を無線通信端末（２０）に通知する。以上が、アクセスポイント側識別番号緊急更新ステップの流れである。

【００７３】

そして、無線通信端末（２０）では、受信した乱数$Rand_{i+1}$を用いて$TMAC_{i+2}$を算出し、自番号記憶部（２３１）に格納する。これにより端末側次識別番号緊急更新ステップも完了する。

【００７４】

以上が、初期化制御、定期更新制御、緊急更新制御におけるアクセスポイント及び無線通信端末の処理の流れである。図５ないし７のように、各信号が相手方に確実に届いた場合には上記処理によって円滑にＭＡＣアドレスの更新が行われる。しかしながら、無線通信におけるフレームはしばしば遅延や欠落が生じることが知られており、通常の方法では正しく通信を継続することができなくなってしまう。

これに対して、本願では仮に各信号が到達しなくとも正常に同期が取れることを特徴としている。

【００７５】

まず、周期的なＭＡＣアドレスの更新処理時における再同期処理につき説述する。事例として、図８のように更新指示信号UpdateCommandが無線通信端末に到達する前に失われる場合と、図９のように無線通信端末には到達したものの確認信号Update Acknowledgeがアクセスポイントに到達せずに失われる場合とが考えられる。

【００７６】

まず図８の場合を検討すると、アクセスポイントは更新指示信号を送出した後も無線通信端末から確認信号を受信するまでは、そのＭＡＣアドレスを$TMAC_i$から更新していない。そのために無線通信端末から何らかの通信(Traffic)があった場合でも、これを正常に

受信することができる。

【００７７】

このとき、制御通信処理部（１１３）には検知部（１１４）を設けてあり、該検知部（１１４）は、受信した信号が新旧いずれのＭＡＣアドレスから受信したものかを検知する（検知ステップ）。

そして、図８の場合には旧アドレスからであることが検知されることで、アクセスポイントの識別番号同期制御部（１１５）は更新指示信号が正常に到達しなかったことを認識でき、その場合には上記送信回数を増やすと共に、乱数については先の更新指示信号と同一の値$Rand_{i+1}$を送信する。

【００７８】

一方、図９の場合を検討すると、更新指示信号が無線通信端末に到達するため、無線通信端末側ではＭＡＣアドレスの変更が行われる。しかし確認信号がアクセスポイントに到達しないので、アクセスポイント側では$TMAC_i$から更新されない。

この場合でも、無線通信端末から何らかの通信があった場合に、制御通信処理部の検知部（１１４）は識別番号記憶部（１２１）に格納していた$TMAC_{i+1}$を参照することにより、本通信が無線通信端末からの通信であることを認識することができる。

【００７９】

さらに、識別番号同期制御部（１１５）はこの通信の到達によって、先の更新指示信号が到達したことと、確認信号が到達しなかったことを認識できる。そこで該識別番号同期制御部（１１５）は上記アクセスポイント側識別番号定期更新ステップと同様の処理により当該無線通信端末のＭＡＣアドレスを変更する処理を実行する。

以上の２通りの場合においても、識別番号記憶部（１２１）に更新前と更新後の両方の現在のＭＡＣアドレスを格納してあることによって、検知部（１１４）と識別番号同期制御部（１１５）が作用して正確なＭＡＣアドレスの再同期を実行することができる。

【００８０】

次に、再同期処理に最適な第２の実施例を図面を用いて説述する。図１０は第２の実施例におけるアクセスポイントの構成図であり、図１１は同無線通信端末の構成図である。

図示の通り、第１の実施例に加えてアクセスポイントの制御通信処理部（１１３）にはタイマ部（１１６）と存在確認信号送信部（１１７）とを、無線通信端末（２０）には存在確認応答部（２２４）を設けている。

【００８１】

本構成において、上述した周期的なＭＡＣアドレスの更新処理時における再同期処理を説述する。ここでも事例として、図１２のように更新指示信号Update Commandが無線通信端末に到達する前に失われる場合と、図１３のように無線通信端末には到達したものの確認信号Update Acknowledgeがアクセスポイントに到達せずに失われる場合とを考える。

【００８２】

まず前者の図１２の事例において、更新指示信号Update Commandを送信すると同時に、タイマ部（１１６）が計時を開始(Start ACK timer)する。正常通信時には所定の時間内に確認信号を受信するが、本事例では更新指示信号が無線通信端末に到達していないため、当然に確認信号は返信されない。

そして、タイマ部（１１６）における計時により所定の確認タイマ時間が経過(ACK timer expires)すると、存在確認信号送信部（１１７）に通知される。存在確認信号送信部（１１７）は、まず識別番号記憶部（１２１）を参照して第２のＭＡＣアドレス$TMAC_{i+1}$に対して存在確認信号Presence Queryを送信する。

【００８３】

このような処理は更新指示信号が正常に無線通信端末に到達したことを前提としているが、実際には到達していないために存在確認信号に対する応答が返ってくることはない。

本実施例ではタイマ部（１１６）が前記存在確認信号の送信と同時に計時を開始(Start RES timer)し、所定の存在確認応答タイマ時間が経過した場合（RES timer expires)には、応答が返ってこないことによって識別番号同期制御部（１１５）は、更新指示信号が

到達していないことを認識できる。
従って、第１の実施例の場合と同様に、送信回数を増やすと共に、乱数については先の更新指示信号と同一の値$Rand_{i+1}$を送信する。
【００８４】
なお、存在確認信号が途中で失われる場合も想定されるが、このときには更新指示信号が到達しなかった場合と同様に確認タイマ時間が時間切れとなり、以降は同様に処理される。
なお、上記確認タイマ時間と存在確認応答タイマ時間は同一時間である必要はなく、適宜設定することができる。
【００８５】
次に図１３の事例、すなわち無線通信端末からの確認信号Update Acknowledgeが途中で失われた場合を説述する。
この場合でも、アクセスポイントの確認タイマ時間は時間切れとなるため、存在確認信号送信部（１１７）が存在確認信号を送信する。この信号はＭＡＣアドレス$TMAC_{i+1}$に対して送られるが、図１３の事例では無線通信端末側ではＭＡＣアドレスが$TMAC_{i+1}$に変更されているため、存在確認信号は正常に到達する。
【００８６】
存在確認信号を受信した無線通信端末は存在確認応答部（２２４）が$TMAC_{i+1}$を発信アドレスとして存在確認応答(Presence Response)を返信する。アクセスポイントでは存在確認応答が存在確認応答タイマ時間内に受信できたことにより無線通信端末においてＭＡＣアドレスが$TMAC_{i+1}$に変更されたことを認識することができる。そこで該識別番号同期制御部（１１５）は上記アクセスポイント側識別番号定期更新ステップと同様の処理により当該無線通信端末のＭＡＣアドレスを変更する処理を実行する。
【００８７】
本発明の第３の実施例として、図１４に示すように無線通信端末（２０）にタイマ部（２２５）を備えた構成を示す。
このタイマ部（２２５）は図１５のように、攻撃検出信号が途中で失われた場合や、図１６のように乱数通知信号が途中で失われた場合に作用する。
まず図１５の場合には、無線通信端末（２０）に対して攻撃（attack)が発生した場合、本願技術により無線通信端末のＭＡＣアドレスは$TMAC_{i+1}$に更新され、上述の通りアクセスポイントに対して攻撃検出信号（Random Number Request）が送出される。該信号の送出と同時にタイマ部（２２５）が計時を開始(Start SUP timer)する。通常は時間内に乱数通知信号が返信されるが、ここでは攻撃検出信号がアクセスポイントに到達していないため、乱数通知信号も到着しない。
【００８８】
そして計時が所定の時間を経過（SUP timer expires)することにより、タイマ部（２２５）は通信部（２２１）から再度攻撃検出信号を送出するように指示する。図中の次の攻撃検出信号はアクセスポイントに到達した様子を示しており、アクセスポイントでＭＡＣアドレスの更新などの処理が進められる。
【００８９】
次に、図１６の事例について説述する。
この場合、最初の攻撃検出信号がアクセスポイントに到達しているため、アクセスポイント側でもＭＡＣアドレスは更新されており、乱数通知信号も送出されている。しかし、この乱数通知信号が途中で失われたことにより、タイマ部（２２５）の計時は図１５の事例と同様に所定時間が経過する。
タイマ部（２２５）は通信部（２２１）から再度攻撃検出信号を送出するように指示し、２度目の攻撃検出信号がアクセスポイントに到達する。
【００９０】
アクセスポイントでは、２度目の攻撃検出信号が到達したことにより、前回の乱数通知信号が到達していないことを知ることができるので、再度前回送出した乱数通知信号を通

知する。
以上のように無線通信端末にタイマ部を設けることで、攻撃検出後にも再同期が効率的に行える。
【００９１】
最後に、図１７は本発明のアクセスポイントの識別番号記憶部（１２１）に更新前の現在のＭＡＣアドレス$TMAC_i$、更新後の現在のＭＡＣアドレス$TMAC_{i+1}$、更新後の次のＭＡＣアドレス$TMAC_{i+2}$を全て記憶しておく構成における再同期処理のシーケンス図である。
本図では、定期更新の更新指示信号（Update Command)に対する確認信号が途中で失われ、アクセスポイントのタイマ部（１１６）における確認信号の計時時間内に、攻撃が生じた場合を示している。
【００９２】
最初の更新指示信号により、無線通信端末側のＭＡＣアドレスは$TMAC_{i+1}$に更新される。さらに、攻撃の検出により$TMAC_{i+2}$に更新される。$TMAC_{i+2}$は更新指示信号で通知された乱数を用いて算出されたものである。
この時点で、アクセスポイント側では確認信号が未達であるため無線通信端末の$TMAC_i$のままである。
【００９３】
本発明では、$TMAC_{i+1}$に更新する指示を行った後も、$TMAC_i$、$TMAC_{i+1}$、$TMAC_{i+2}$の全てのＭＡＣアドレスを保持しているため、無線通信端末（２０）からの攻撃検出信号が$TMAC_{i+2}$のアドレスから送られてきてもそれを受信することができる。そして、識別番号同期制御部（１１５）の作用により、識別番号記憶部（１２１）における現在のＭＡＣアドレスを$TMAC_{i+2}$に更新し、次のＭＡＣアドレスを算出するための乱数を送出することができる。
このように、３つのアドレスを保持することで、更新中に攻撃があった場合などであっても、的確にＭＡＣアドレスの再同期を行うことが可能である。
【００９４】
さらに本発明では第４の実施例として図１０及び図１１に示すアクセスポイント及び無線通信端末を用いて次のような各信号処理を行っても良い。
まず更新指示信号について説述する。本実施例の更新指示信号は、図１８に示すように、まず乱数発生処理部（１１１）が乱数$Rand_i$を発生させる。（Ｓ１１）。ここでiは現在の当該無線端末のＭＡＣアドレス１個に対応して１個発生させる。
【００９５】
次にハッシュ関数演算処理部（１１２）が、発生した乱数$Rand_i$を用いて次の数１に示されるハッシュ関数を用いて第２の新しいＭＡＣアドレス$TMAC_{i+1}$を算出（Ｓ１２）する。算出されたＭＡＣアドレスについて、ハッシュ関数演算処理部においてローカルエリア内に重複したＭＡＣアドレスが存在しないか、重複確認（Ｓ１３）を行う。このとき、識別番号記憶部（１２１）には後述するように各無線通信端末について新旧２つの識別番号を記憶しておくことができるのでそのような構成の場合には新旧の識別番号と重複していないかを確認する。
【００９６】
もし重複したＭＡＣアドレスが存在した場合には、乱数発生ステップ（Ｓ１１）に戻り、再びＳ１２，Ｓ１３の処理を行う。これにより、ローカルエリアにおけるＭＡＣアドレスの固有性が確保される。
重複確認（Ｓ１３）で問題がないときには、制御通信処理部は識別番号記憶部（１２１）に当該無線通信端末の次のＭＡＣアドレスとして$TMAC_{i+1}$を記憶させる。（Ｓ１４）
以上によって、Ｓ１１-Ｓ１４に係るアクセスポイント側識別番号発生ステップが終了する。
【００９７】
そして、次に更新指示ステップとして、制御通信処理部（１１３）は無線通信端末に対して更新指示信号Update Command($Rand_i$)を送出する（Ｓ１５）。

図１９には更新指示に係る信号のシーケンス図を示す。図１９において左端の破線は無線通信端末(Mobile Device)が自己のＭＡＣアドレスをどのように認識しているか、右端の破線はアクセスポイント(Access Point)が当該無線通信端末のＭＡＣアドレスをどのように認識しているかを示している。

該更新指示信号には乱数$Rand_i$を含んでおり、このときの宛先は現在のＭＡＣアドレスである$TMAC_i$である。

通常は、更新指示信号を通信部（２２１）で受信した無線通信端末からは確認信号Update Acknowledgeがアクセスポイントに返され、受信する（Ｓ１６）。

【００９８】

確認信号を受信したアクセスポイントは、無線通信端末においてＭＡＣアドレスが更新されると判定ができるため、制御通信処理部（１１３）の作用により識別番号記憶部（１２１）に記憶された現在のＭＡＣアドレスを上記で算出した第２のＭＡＣアドレスに変更する処理（Ｓ１７）を行い、第２のＭＡＣアドレスは空データとなる。本処理がアクセスポイント側識別番号更新ステップである。

【００９９】

同時に無線通信端末では、確認信号を送信すると共に、ハッシュ関数演算処理部（２２２）において上記アクセスポイントにおけるのと同様の演算処理を行い、更新指示信号で受信した乱数を用いて変更するＭＡＣアドレス$TMAC_{i+1}$を算出する。これが端末側識別番号発生ステップである。

続いて端末側識別番号更新ステップとして、自番号記憶部（２３１）に記憶した現在のＭＡＣアドレスを$TMAC_{i+1}$に更新して、以後は$TMAC_{i+1}$の無線通信端末として振る舞う。

【０１００】

以上のようなＭＡＣアドレスの更新は任意のタイミングで行うことができるが、１つの実施例として周期的、例えば１０秒間隔にてＳ１ないしＳ７の処理を行うことが望ましい。その場合、アクセスポイントのメモリ手段には、各無線通信端末毎に次回の更新時間、更新間隔、通し番号（送信回数）を記録しておく。

【０１０１】

本発明の無線通信システムでは、ＤｏＳ攻撃に対して効果的に防御を行うために、緊急のＭＡＣアドレス変更処理が可能である。次に緊急更新処理について説述する。図２０は緊急更新処理のシーケンス図である。

まず、無線通信端末には攻撃検出処理部（２２３）が備えられていて、不正なフレームを一定量以上受信した場合に、サービス不能攻撃を受けたと検出するようにしている。これが本無線通信方法におけるサービス不能攻撃検出ステップの処理である。

【０１０２】

本実施例では、明らかに不正なフレームやメッセージ認証子を含まないフレームなどが所定の回数以上、例えば１秒間に１０フレーム以上受信した時に、攻撃検出を行う。

攻撃検出処理部（２２３）からの指示により、通信部（２２１）はアクセスポイント（１０）に向けて更新指示要求Update Requestを送出（更新指示要求ステップ）する。該更新指示要求に応じてアクセスポイントの制御通信処理部（１１３）は上記Ｓ１１からの処理を実行するように制御する。

【０１０３】

以上が、更新指示信号と更新指示要求・確認信号の各信号に基づくアクセスポイント及び無線通信端末の処理の流れである。図１９及び２０のように、各信号が相手方に確実に届いた場合には上記処理によって円滑にＭＡＣアドレスの更新が行われる。しかしながら、無線通信におけるフレームはしばしば遅延や欠落が生じることが知られており、通常の方法では正しく通信を継続することができなくなってしまう。

これに対して、本願では仮に各信号が到達しなくとも正常に同期が取れることを特徴としている。

【０１０４】

まず、周期的なＭＡＣアドレスの更新処理時における再同期処理につき説述する。事例

として、図２１のように更新指示信号UpdateCommandが無線通信端末に到達する前に失われる場合と、図２２のように無線通信端末には到達したものの確認信号Update Acknowledgeがアクセスポイントに到達せずに失われる場合とが考えられる。

【０１０５】

まず図２１の場合を検討すると、アクセスポイントは更新指示信号を送出した後も無線通信端末から確認信号を受信するまでは、そのＭＡＣアドレスを$TMAC_i$から更新していない。そのために無線通信端末から何らかの通信(Traffic)があった場合でも、これを正常に受信することができる。

【０１０６】

このとき、制御通信処理部（１１３）には検知部（１１４）を設けてあり、該検知部（１１４）は、受信した信号が新旧いずれのＭＡＣアドレスから受信したものかを検知する（検知ステップ）。

そして、図２１の場合には旧アドレスからであることが検知されることで、アクセスポイントの識別番号同期制御部（１１５）は更新指示信号が正常に到達しなかったことを認識でき、その場合には上記送信回数を増やすと共に、乱数については先の更新指示信号と同一の値を送信する。図１８のＳ１５以降の処理と以下同様である。

【０１０７】

一方、図２２の場合を検討すると、更新指示信号が無線通信端末に到達するため、無線通信端末側ではＭＡＣアドレスの変更が行われる。しかし確認信号がアクセスポイントに到達しないので、アクセスポイント側では$TMAC_i$から更新されない。

この場合でも、無線通信端末から何らかの通信があった場合に、制御通信処理部の検知部（１１４）は識別番号記憶部（１２１）に図１８のＳ１４において格納していた$TMAC_{i+1}$を参照することにより、本通信が無線通信端末からの通信であることを認識することができる。

【０１０８】

さらに、識別番号同期制御部（１１５）はこの通信の到達によって、先の更新指示信号が到達したことと、確認信号が到達しなかったことを認識できる。そこで該識別番号同期制御部（１１５）はＳ１６がなされたものと同様の処理により当該無線通信端末のＭＡＣアドレスを変更する処理（Ｓ１７）を実行する。

以上の２通りの場合においても、識別番号記憶部（１２１）に新旧両方のＭＡＣアドレスを格納してあることによって、検知部（１１４）と識別番号同期制御部（１１５）が作用して正確なＭＡＣアドレスの再同期を実行することができる。

【０１０９】

次に、緊急更新処理時における再同期処理につき説述する。

図２３に示すように、無線通信端末（２０）から更新指示要求Update Requestが送信された場合に、該更新指示要求が途中で失われる事例が想定される。この事例においては、アクセスポイント（１０）は更新指示要求が送信されたことを知ることができないため、無線通信端末側で解決する必要がある。

そこで、無線通信端末（２０）には図示しないタイマ部を備えておき、更新指示要求の送信と同時に計時を開始して所定の時間内にアクセスポイントからの更新指示信号を受信しない場合に、更新指示要求を通信部（２２１）から送信回数を１回増やすと共に再度送信するようにする。

【０１１０】

図２４は、無線通信端末からの更新指示要求は到達したものの、アクセスポイントからの更新指示信号が途中で失われた事例を示している。

この場合に上述の通りアクセスポイント側での再同期処理も行われるが、先に無線通信端末のタイマ部での計時が所定の時間を経過した場合には、更新指示要求を通信部（２２１）から送信回数を１回増やすと共に再度送信すればよい。

【０１１１】

次に、再同期処理について説明する。

図２５のように更新指示信号Update Commandが無線通信端末に到達する前に失われる場合と、図２６のように無線通信端末には到達したものの確認信号Update Acknowledgeがアクセスポイントに到達せずに失われる場合とを考える。

【０１１２】

まず前者の図１５の事例において、更新指示信号Update Commandを送信すると同時に、タイマ部（１１６）が計時を開始する。正常通信時には所定の時間内に確認信号を受信するが、本事例では更新指示信号が無線通信端末に到達していないため、当然に確認信号は返信されない。

そして、タイマ部（１１６）における計時により所定の確認タイマ時間が経過(ACK timer expires)すると、存在確認信号送信部（１１７）に通知される。存在確認信号送信部（１１７）は、まず識別番号記憶部（１２１）を参照して第２のＭＡＣアドレス$TMAC_{i+1}$に対して存在確認信号Presence Queryを送信する。

【０１１３】

このような処理は更新指示信号が正常に無線通信端末に到達したことを前提としているが、実際には到達していないために存在確認信号に対する応答が返ってくることはない。

本実施例ではタイマ部（１１６）が前記存在確認信号の送信と同時に計時を開始し、所定の存在確認応答タイマ時間が経過した場合（RES timer expires)には、応答が返ってこないことによって識別番号同期制御部（１１５）は、更新指示信号が到達していないことを認識できる。

従って、送信回数を増やすと共に、乱数については先の更新指示信号と同一の値を送信する。図１８のＳ１５以降の処理と以下同様である。

【０１１４】

なお、存在確認信号が途中で失われる場合も想定されるが、このときには更新指示信号が到達しなかった場合と同様に確認タイマ時間が時間切れとなり、以降は同様に処理される。

なお、上記確認タイマ時間と存在確認応答タイマ時間は同一時間である必要はなく、適宜設定することができる。

【０１１５】

次に図２６の事例、すなわち無線通信端末からの確認信号が途中で失われた場合を説述する。

この場合でも、アクセスポイントの確認タイマ時間は時間切れとなるため、存在確認信号送信部（１１７）が存在確認信号を送信する。この信号はＭＡＣアドレス$TMAC_{i+1}$に対して送られるが、図２６の事例では無線通信端末側ではＭＡＣアドレスが$TMAC_{i+1}$に変更されているため、存在確認信号は正常に到達する。

【０１１６】

存在確認信号を受信した無線通信端末は存在確認応答部（２２４）が$TMAC_{i+1}$を発信アドレスとして存在確認応答(Presence Response)を返信する。アクセスポイントでは存在確認応答が存在確認応答タイマ時間内に受信できたことにより無線通信端末においてＭＡＣアドレスが$TMAC_{i+1}$に変更されたことを認識することができる。そこで該識別番号同期制御部（１１５）は図１８のＳ１６がなされたものと同様の処理により当該無線通信端末のＭＡＣアドレスを変更する処理（Ｓ７）を実行する。

【０１１７】

本発明の効果を実証するために、無線通信端末から１００ｍｓ毎に１個の無線通信フレームを送信する無線通信システムのシミュレーションを行った。ここでは上記実施例１におけるシステムを用いた。攻撃者が盗聴により収集したＭＡＣアドレスの中から１つの無線通信端末を選んで０．１ｍｓ毎に攻撃フレームを送信する。攻撃時間のあと１００ｍｓは中断する。

この１００ｍｓは攻撃者がＭＡＣアドレスを収集する時間を想定しており、攻撃者がＭＡＣアドレスの収集、攻撃を繰り返している状態をシミュレーションしている。

【０１１８】

図２７は本発明を実装しない通常の無線通信システム（実線）、非特許文献４で開示される攻撃後にアクセスポイントに対して更新要求を行う無線通信システム（長破線）、本発明の無線通信システム（短破線）における攻撃成功のフレーム数を示すグラフである。

このシミュレーション結果から、従来のシステムに対しては顕著に、非特許文献４の技術に対しても１／４程度まで攻撃の成功数を減少させられることが示された。

【図面の簡単な説明】

【０１１９】

【図１】本発明の無線通信システムの全体構成図である。

【図２】本発明のアクセスポイント（第１実施例）の構成図である。

【図３】本発明の無線通信端末（第１実施例）の構成図である。

【図４】アクセスポイントにおける処理の流れ図である。

【図５】初期化制御時のシーケンス図である。

【図６】定期更新制御時のシーケンス図である。

【図７】緊急更新制御時のシーケンス図である。

【図８】更新指示信号が途中で欠落した事例のシーケンス図である。

【図９】確認信号が途中で欠落した事例のシーケンス図である。

【図１０】本発明のアクセスポイント（第２実施例）の構成図である。

【図１１】本発明の無線通信端末（第２実施例）の構成図である。

【図１２】存在確認信号を用いる第２実施例で更新指示信号が途中で欠落した事例のシーケンス図である。

【図１３】存在確認信号を用いる第２実施例で確認信号が途中で欠落した事例のシーケンス図である。

【図１４】本発明の無線通信端末（第３実施例）の構成図である。

【図１５】攻撃検出信号が途中で欠落した事例のシーケンス図である。

【図１６】乱数通知信号が途中で欠落した事例のシーケンス図である。

【図１７】確認信号が途中で欠落し、かつ攻撃を受けた事例のシーケンス図である。

【図１８】第４実施例におけるアクセスポイントにおける処理の流れ図である。

【図１９】第４実施例における更新指示信号のシーケンス図である。

【図２０】第４実施例における更新指示要求のシーケンス図である。

【図２１】第４実施例における更新指示信号が途中で欠落した事例のシーケンス図である。

【図２２】第４実施例における確認信号が途中で欠落した事例のシーケンス図である。

【図２３】第４実施例における更新指示要求が途中で欠落した事例のシーケンス図である。

【図２４】第４実施例における更新指示要求に対する更新指示信号が途中で欠落した事例のシーケンス図である。

【図２５】第４実施例における存在確認信号を用いる場合に、更新指示信号が途中で欠落した事例のシーケンス図である。

【図２６】第４実施例における存在確認信号を用いた場合に、確認信号が途中で欠落した事例のシーケンス図である。

【図２７】本発明と従来技術の無線通信端末におけるサービス不能攻撃のシミュレーション結果を示すグラフである。

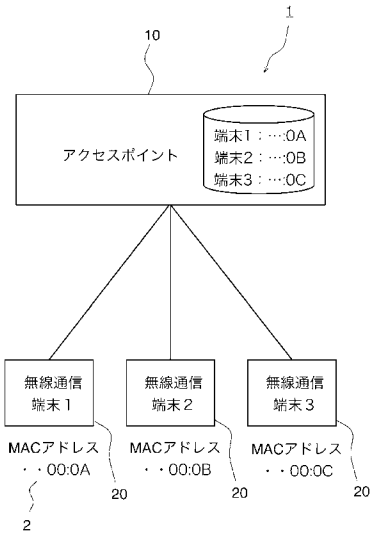
【符号の説明】

【０１２０】

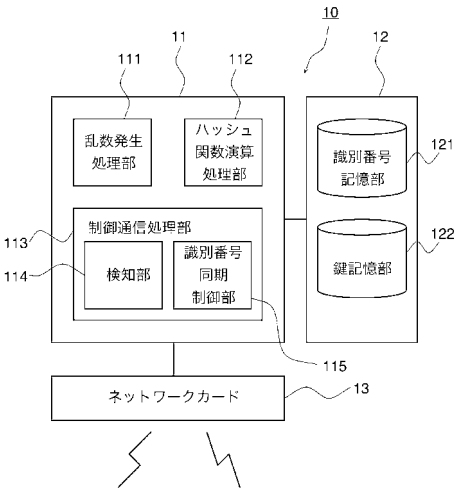
１　無線通信システム
２　ＭＡＣアドレス
１０　アクセスポイント
１１　演算手段
１１１　乱数発生処理部
１１２　ハッシュ関数演算処理部

１１３　制御通信処理部
１１４　検知部
１１５　識別番号同期制御部
１２　メモリ手段
１２１　識別番号記憶部
１２２　鍵記憶部
１３　ネットワークカード
２０　無線通信端末
２１　ネットワークカード
２２　演算手段
２２１　通信部
２２２　ハッシュ関数演算処理部
２２３　攻撃検出処理部
２３　メモリ手段
２３１　自番号記憶部
２３２　鍵記憶部

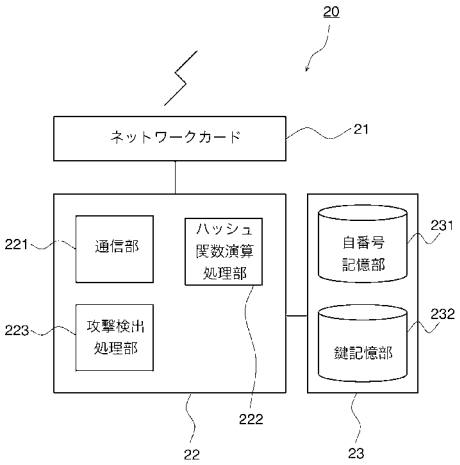
【図１】



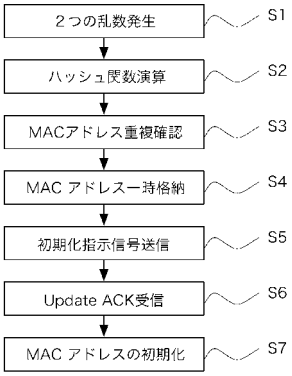
【図２】



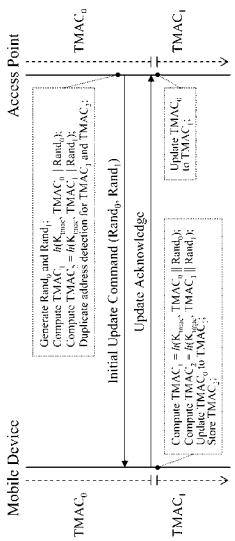
【図３】


20
ネットワークカード
21
通信部
221
ハッシュ
関数演算
処理部
攻撃検出
処理部
223
自番号
記憶部
231
鍵記憶部
232
22
222
23

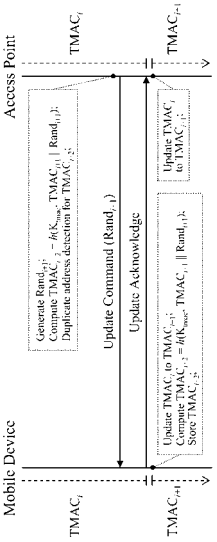
【図４】


２つの乱数発生
S1
ハッシュ関数演算
S2
MACアドレス重複確認
S3
MAC アドレスー時格納
S4
初期化指示信号送信
S5
Update ACK受信
S6
MAC アドレスの初期化
S7

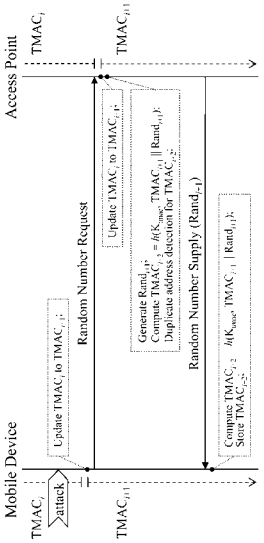
【図５】


Access Point
Mobile Device
Initial Update Command (Rand0, Rand1)
Update Acknowledge

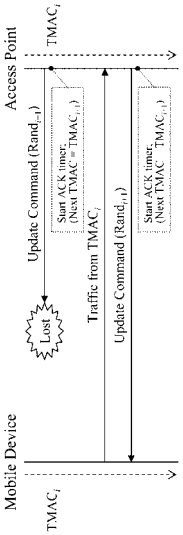
【図６】


Access Point
Mobile Device
Update Command (Rand0, 1)
Update Acknowledge

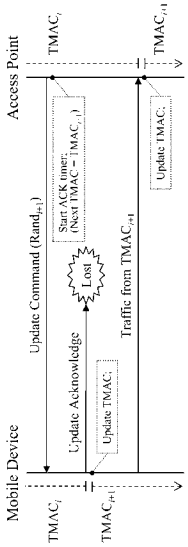
【図７】


Access Point
Mobile Device
Random Number Request
Random Number Supply
attack

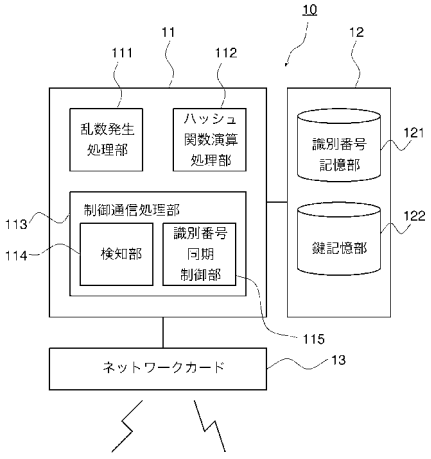
【図８】


Access Point
Mobile Device
Update Command
Lost
Traffic from TMAC
Update Command

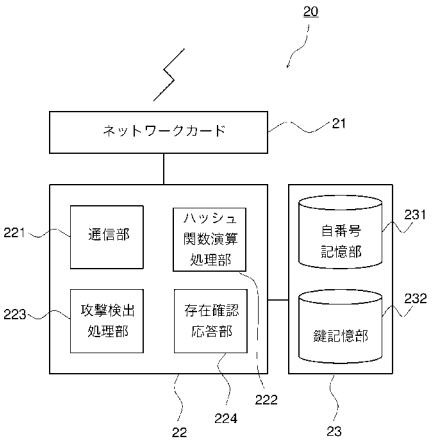
【図９】


Access Point
Mobile Device
Update Command
Update Acknowledge
Lost
Traffic from TMAC
Update TMAC

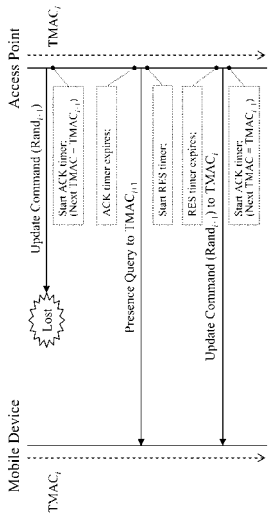
【図１０】


10
11
12
111
112
乱数発生処理部
ハッシュ関数演算処理部
識別番号記憶部
121
制御通信処理部
113
114
検知部
識別番号同期制御部
鍵記憶部
122
115
ネットワークカード
13

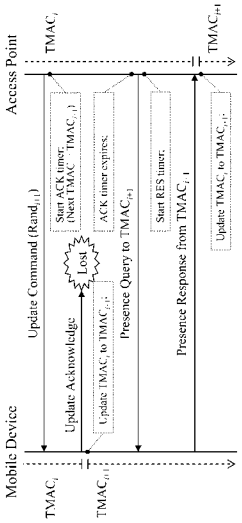
【図１１】



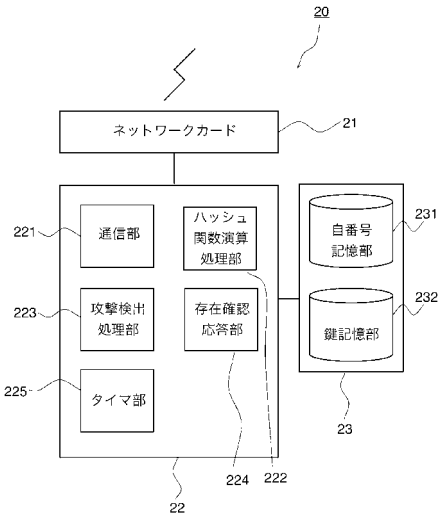
【図１２】



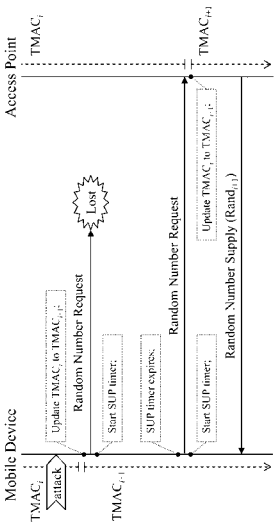
【図１３】



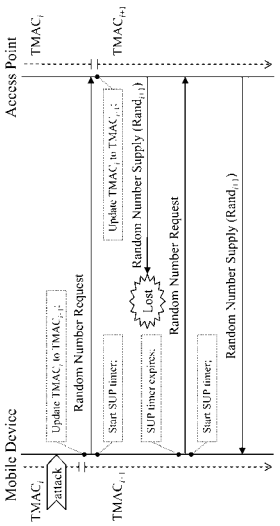
【図１４】



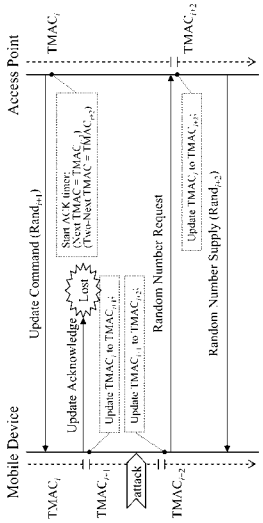
【図１５】



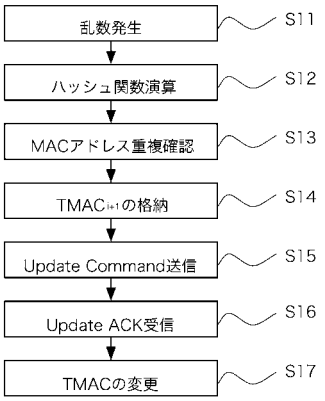
【図１６】



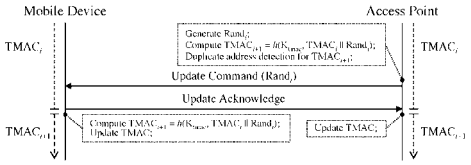
【図１７】



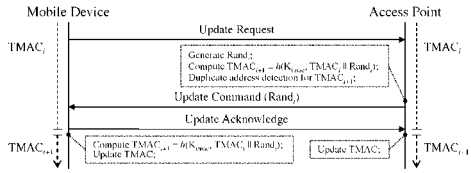
【図１８】



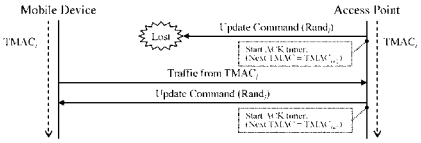
【図１９】



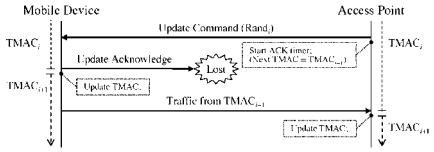
【図２０】



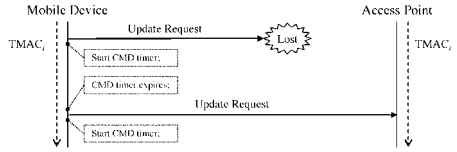
【図２１】



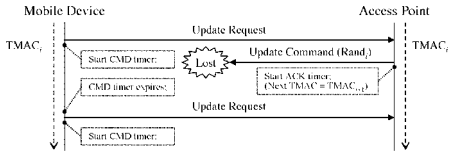
【図２２】



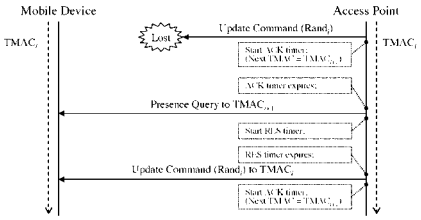
【図２３】



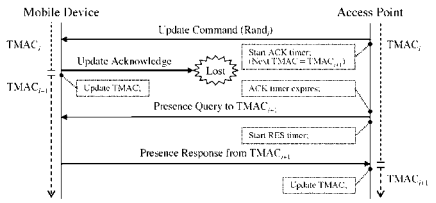
【図２４】



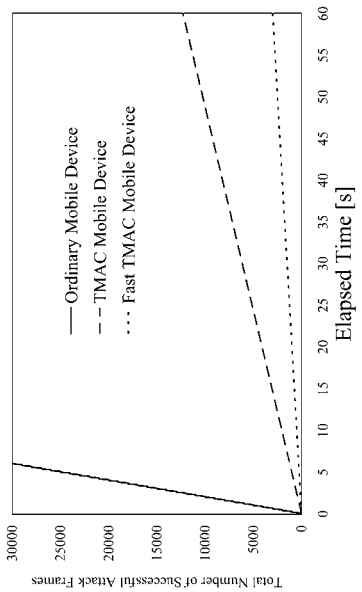
【図２５】



【図２６】



【図２７】



フロントページの続き

(72)発明者　石津　健太郎
東京都小金井市貫井北町４－２－１　独立行政法人情報通信研究機構内

審査官　石田　信行

(56)参考文献　特開２００６－３１１３７３（ＪＰ，Ａ）
特開２００６－２８７２８２（ＪＰ，Ａ）
特開２０００－１１５１６１（ＪＰ，Ａ）
特開２０００－９２５７２（ＪＰ，Ａ）
特開平１０－１９１４４７（ＪＰ，Ａ）
特開平７－２０３５３５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L　9/32
H04W　12/04