

(19) 日本国特許庁(JP)

## 再公表特許(A1)

(11) 国際公開番号

W02007/032499

発行日 平成21年3月19日 (2009.3.19)

(43) 国際公開日 平成19年3月22日 (2007.3.22)

(51) Int.Cl.	F I	テーマコード (参考)
<b>HO4L 9/32 (2006.01)</b>	HO4L 9/00 673B	5J104
<b>HO4W 12/04 (2009.01)</b>	HO4L 9/00 673C	5K067
	HO4Q 7/00 182	

審査請求 有 予備審査請求 未請求 (全 35 頁)

出願番号 特願2007-535571 (P2007-535571)	(71) 出願人 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
(21) 国際出願番号 PCT/JP2006/318433	
(22) 国際出願日 平成18年9月15日 (2006.9.15)	
(31) 優先権主張番号 特願2005-271144 (P2005-271144)	(74) 代理人 100130111 弁理士 新保 斉
(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)	(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) 【要約】

【課題】

識別番号を標的として行われる端末追跡やD o S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を提供すること。

【解決手段】

アクセスポイントの制御通信処理部113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112で次に更新する第3の識別番号を、現在の識別番号及びハッシュ鍵、乱数を用いて発生させると共に、制御通信処理部113が当該無線通信端末にその乱数を含む更新指示信号を送信し、識別番号記憶部121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。無線通信端末が更新指示信号を受信すると、現在の識別番号を第2の識別番号に更新すると共に、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3の識別番号を発生させる無線通信システムを提供する。

【選択図】 図2

**【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

10

20

30

40

50

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を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を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、

10

20

30

40

50

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、M A C (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、

10

20

30

40

50

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

10

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 1 1】

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、

20

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 1 0 に記載の無線通信方法。

【請求項 1 2】

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、

30

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 1 1 のいずれかに記載の無線通信方法。

【請求項 1 3】

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、

40

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 1 2 に記載の無線通信方法。

【請求項 1 4】

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

50

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 1 3 に記載の無線通信方法。

【請求項 1 5】

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 1 6】

前記無線通信端末の識別番号が、M A C (Media Access Control) アドレスである請求項 9 ないし 1 5 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】

【0 0 0 1】

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】

【0 0 0 2】

近年、第 3 世代 ( 3 G ) 移動体通信や、IEEE802.11規格の無線 L A N、IEEE802.16規格の無線 M A N 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。

【0 0 0 3】

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 L A N 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。

【0 0 0 4】

【非特許文献 1】3rd Generation Partnership Project, "3G Security; Security archi

10

20

30

40

50

ecture (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ー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】

10

20

30

40

50

本技術は、識別番号を標的として行われる端末追跡やD o S 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M A C 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M A C 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。

【 0 0 1 3 】

【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.

10

【発明の開示】

【発明が解決しようとする課題】

【 0 0 1 4 】

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D o S 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】

【 0 0 1 5 】

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D o S 攻撃から防御するためにM A C (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。

20

【 0 0 1 6 】

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。

30

【 0 0 1 7 】

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。

【 0 0 1 8 】

40

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。

【 0 0 1 9 】

50



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。

【 0 0 2 0 】

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。

10

【 0 0 2 1 】

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。

【 0 0 2 2 】

20

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。

【 0 0 2 3 】

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。

30

【 0 0 2 4 】

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。

【 0 0 2 5 】

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。

40

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。

【 0 0 2 6 】

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

50

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、M A C (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

10

20

30

40

50

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。

10

【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。

20

【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。

30

【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。

40

【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

50

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、M A C (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D o S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、D o S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。

10

20

30

40

50

## 【 0 0 4 3 】

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。

## 【 0 0 4 4 】

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。

## 【 0 0 4 5 】

【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

## 【 0 0 4 6 】

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。

## 【 0 0 4 7 】

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。

## 【 0 0 4 8 】

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。

## 【 0 0 4 9 】

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。

## 【 0 0 5 0 】

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。

## 【 0 0 5 1 】

10

20

30

40

50

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。

10

【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。

20

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<sub>0</sub>と(第2乱数)Rand<sub>1</sub>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】

30

次にハッシュ関数演算処理部(112)が、現在のMACアドレスTMAC<sub>0</sub>と、発生した乱数Rand<sub>0</sub>、Rand<sub>1</sub>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<sub>1</sub>とTMAC<sub>2</sub>を算出(S2)する。数式に明らかなように、TMAC<sub>2</sub>はTMAC<sub>1</sub>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<sub>tmac</sub>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。

40

【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<sub>0</sub>)と、更新後の現在の鍵(上記の例ではTMAC<sub>1</sub>)、更新後の次の鍵(上記の例ではTMAC<sub>2</sub>)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、

50

再び S 2 , S 3 の処理を行う。これにより、ローカルエリアにおける M A C アドレスの固有性が確保される。

重複確認 ( S 3 ) で問題がなければ、2つの M A C アドレスをメモリ内に一時格納 ( S 4 ) する。

S 1 ? S 4 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。

【 0 0 6 0 】

そして、次に初期化指示ステップとして、制御通信処理部 ( 1 1 3 ) は無線通信端末に対して初期化指示信号を送出する ( S 5 ) 。

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。

【 0 0 6 1 】

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 M A C 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 M A C 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 M A C アドレスである TMA  $C_0$  である。

通常は、初期化指示信号を通信部 ( 2 2 1 ) 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 ( S 6 ) 。

【 0 0 6 2 】

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 ( 1 2 1 ) に当該無線通信端末の現在の M A C アドレスとして TMA  $C_1$  を、次の M A C アドレスとして TMA  $C_2$  を記憶させる ( S 7 ) 。

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 M A C アドレスは TMA  $C_1$  を基本として認識される。もっとも、本願技術では TMA  $C_0$ 、TMA  $C_2$  をいずれも記憶し、かつ通信可能としておくことで、どの M A C 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。

【 0 0 6 3 】

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 ( 2 2 2 ) 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 M A C アドレス TMA  $C_1$  と TMA  $C_2$  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 ( 2 3 1 ) に記憶した現在の M A C アドレスを TMA  $C_1$  に、次の M A C アドレスを TMA  $C_2$  を設定して、以後は TMA  $C_1$  の無線通信端末として振る舞う。

【 0 0 6 4 】

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 M A C 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 M A C アドレス TMA  $C_i$  から更新後の現在の M A C アドレス TMA  $C_{i+1}$  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の更新時間、更新間隔、通し番号 ( 送信回数 ) を記録しておく。

【 0 0 6 5 】

定期更新時、アクセスポイントでは乱数発生処理部 ( 1 1 1 ) 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。

【 0 0 6 6 】

そして、ハッシュ関数演算処理部 ( 1 1 2 ) が第 3 の乱数を用いて次の M A C アドレス

10

20

30

40

50

(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。

10

【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。

20

【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。

30

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。

40

【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】

50



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。

10

【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。

20

【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】

30

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。

40

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。

50

## 【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。

10

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。

20

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】

30

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。

40

## 【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

50

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を経過する。

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

10

20

30

40

50

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。

10

20

30

40

50

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。

10

#### 【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失われる場合とが考えられる。

20

#### 【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を検知する(検知ステップ)。

30

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。

40

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

50

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(REStimer 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。

10

20

30

40

50

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。

10

【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】

20

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。

30

【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。

40

【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

50

。

【図 2 2】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 2 3】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 2 4】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 2 5】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 2 6】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 2 7】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】

【 0 1 2 0 】

- 1 無線通信システム
- 2 M A C アドレス
- 1 0 アクセスポイント
- 1 1 演算手段
- 1 1 1 乱数発生処理部
- 1 1 2 ハッシュ関数演算処理部
- 1 1 3 制御通信処理部
- 1 1 4 検知部
- 1 1 5 識別番号同期制御部
- 1 2 メモリ手段
- 1 2 1 識別番号記憶部
- 1 2 2 鍵記憶部
- 1 3 ネットワークカード
- 2 0 無線通信端末
- 2 1 ネットワークカード
- 2 2 演算手段
- 2 2 1 通信部
- 2 2 2 ハッシュ関数演算処理部
- 2 2 3 攻撃検出処理部
- 2 3 メモリ手段
- 2 3 1 自番号記憶部
- 2 3 2 鍵記憶部

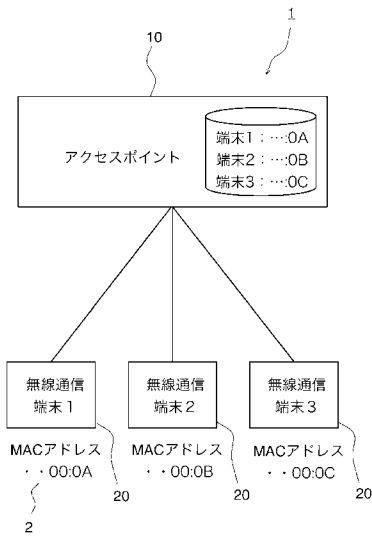
10

20

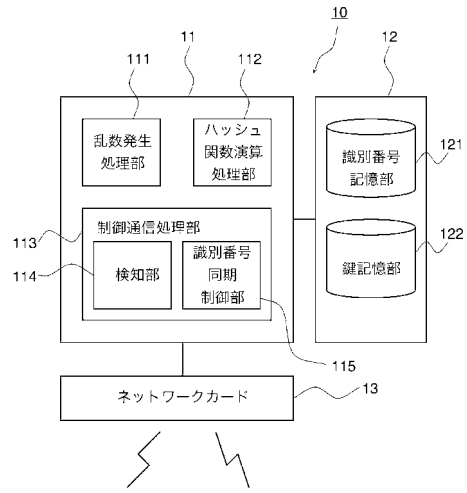
30



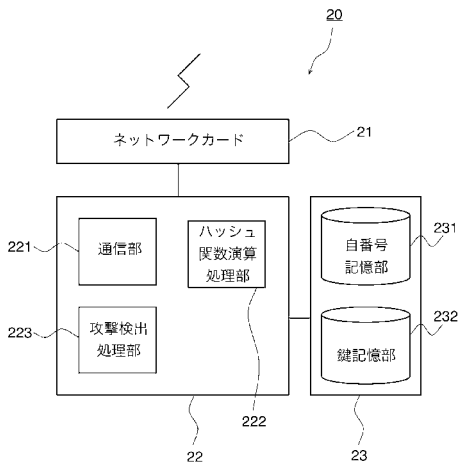
【 図 1 】



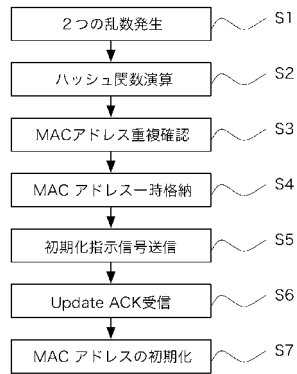
【 図 2 】



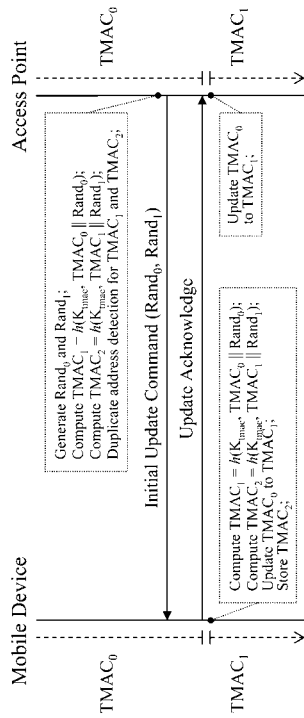
【 図 3 】



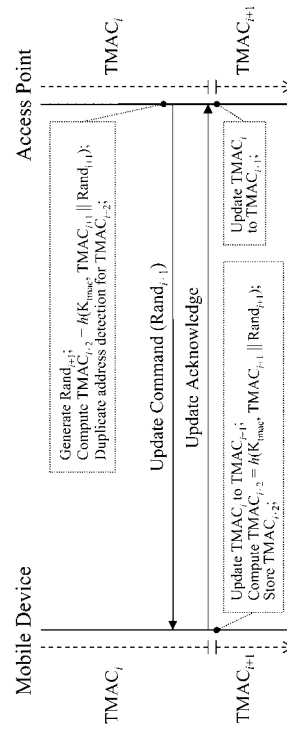
【 図 4 】



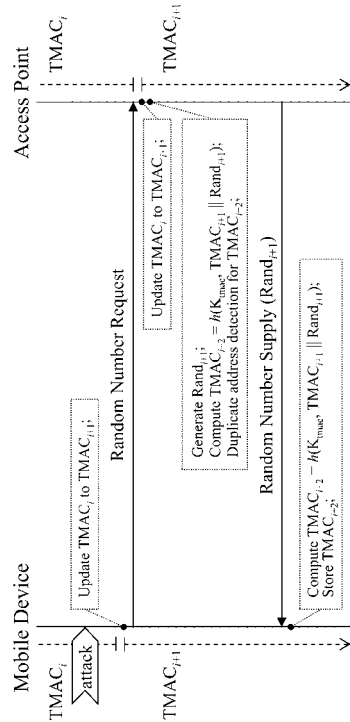
【 図 5 】



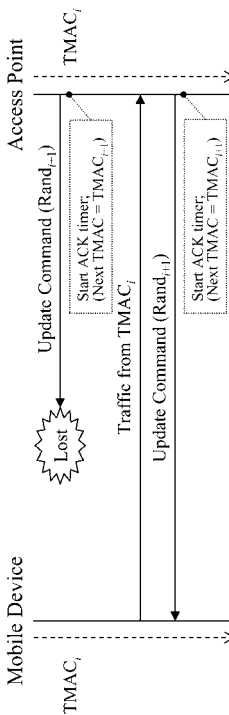
【 図 6 】



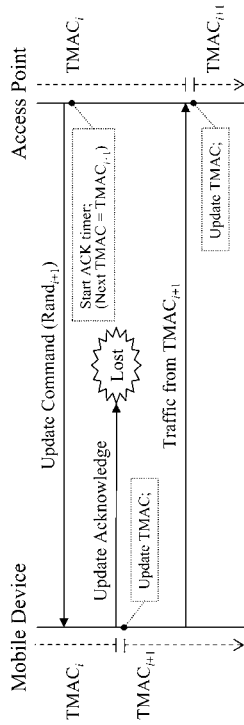
【 図 7 】



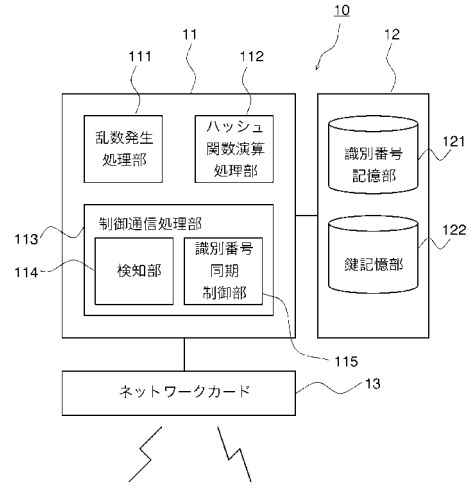
【 図 8 】



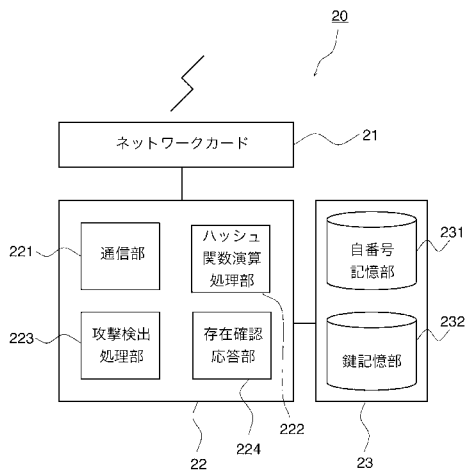
【 図 9 】



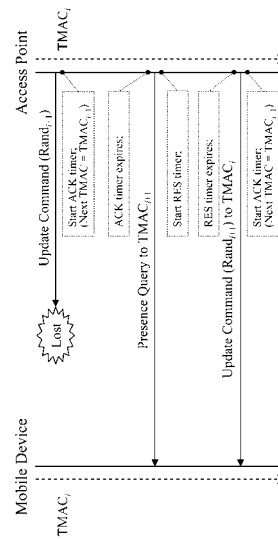
【 図 1 0 】



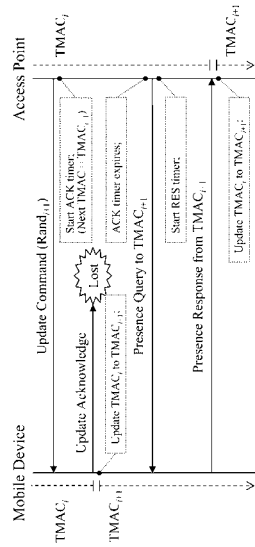
【 図 1 1 】



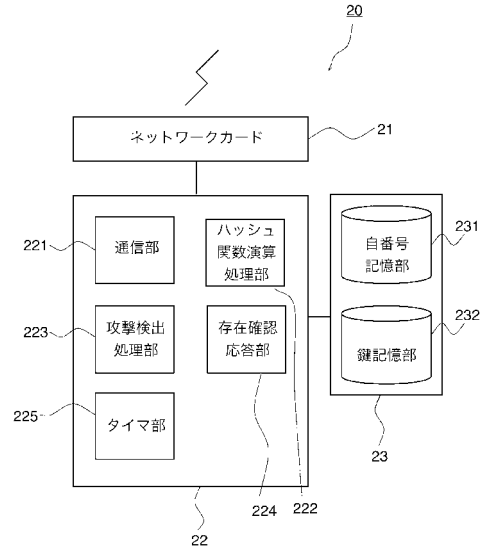
【 図 1 2 】



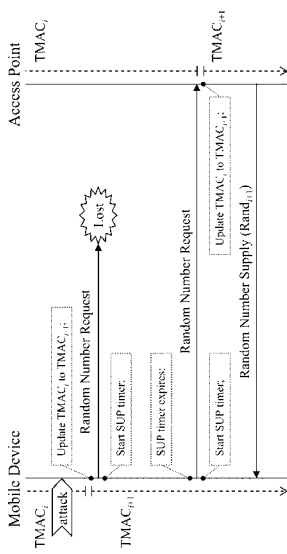
【 図 1 3 】



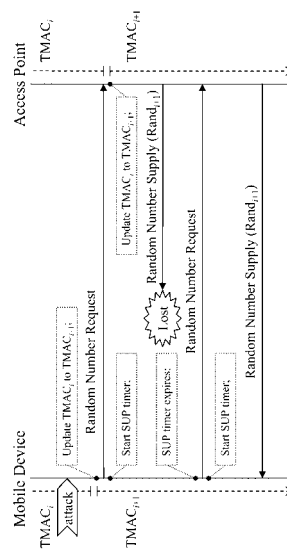
【 図 1 4 】



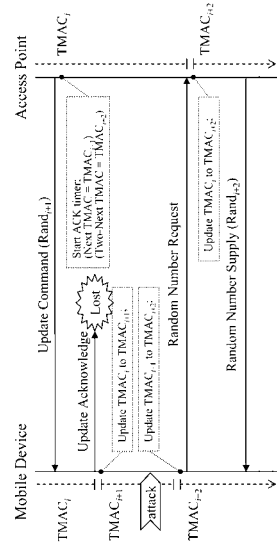
【 図 1 5 】



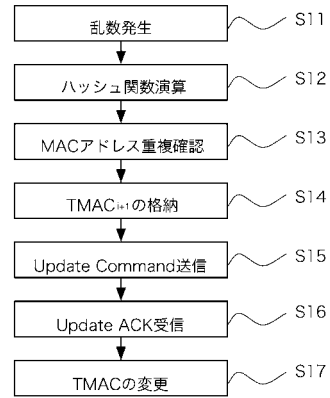
【 図 1 6 】



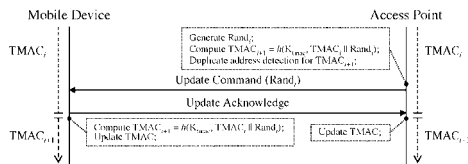
【 図 17 】



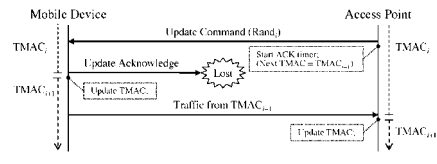
【 図 18 】



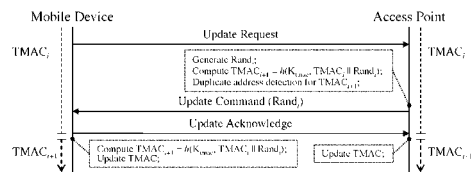
【 図 19 】



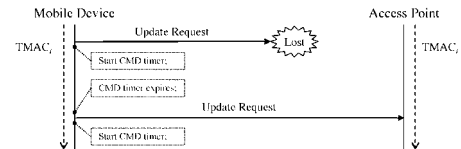
【 図 22 】



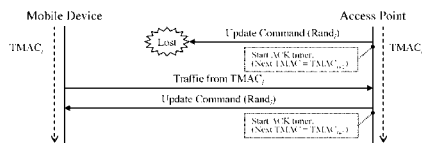
【 図 20 】



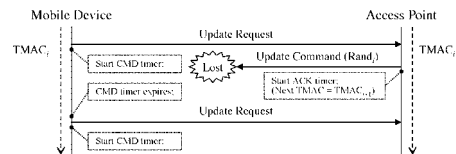
【 図 23 】



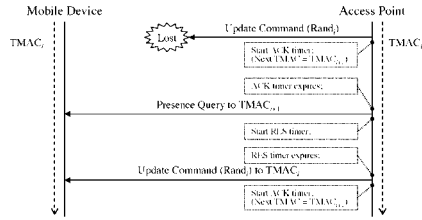
【 図 21 】



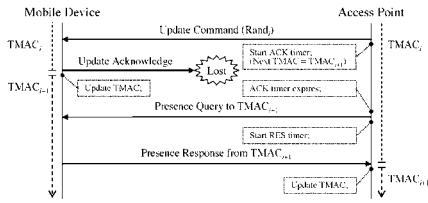
【 図 24 】



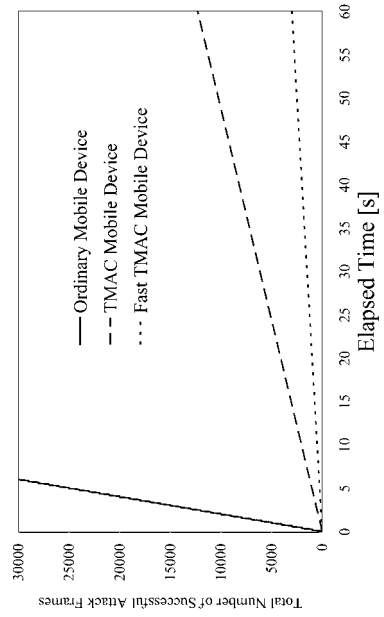
【 図 2 5 】



【 図 2 6 】



【 図 2 7 】



## 【 国際調査報告 】

INTERNATIONAL SEARCH REPORT		International application No. PCT/JP2006/318433
<b>A. CLASSIFICATION OF SUBJECT MATTER</b> H04L9/32(2006.01)i, G09C1/00(2006.01)i, H04Q7/38(2006.01)i  According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b> Minimum documentation searched (classification system followed by classification symbols) H04L9/32, G09C1/00, H04Q7/38  Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2006 Kokai Jitsuyo Shinan Koho 1971-2006 Toroku Jitsuyo Shinan Koho 1994-2006  Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2000-92572 A (Lucent Technologies Inc.), 31 March, 2000 (31.03.00), Full text & EP 982963 A2	1-16
A	JP 2000-115161 A (Lucent Technologies Inc.), 21 April, 2000 (21.04.00), Full text & EP 982958 A2	1-16
A	JP 10-191447 A (NTT Mobile Communications Network Inc.), 21 July, 1998 (21.07.98), Full text (Family: none)	1-16
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 20 November, 2006 (20.11.06)		Date of mailing of the international search report 28 November, 2006 (28.11.06)
Name and mailing address of the ISA/ Japanese Patent Office		Authorized officer
Facsimile No.		Telephone No.

**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/JP2006/318433

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 7-203535 A (International Business Machines Corp.), 04 August, 1995 (04.08.95), Full text & EP 658023 A1	1-16



国際調査報告		国際出願番号 PCT/J P 2 0 0 6 / 3 1 8 4 3 3									
A. 発明の属する分野の分類 (国際特許分類 (IPC)) Int.Cl. H04L9/32(2006.01)i, G09C1/00(2006.01)i, H04Q7/38(2006.01)i											
B. 調査を行った分野 調査を行った最小限資料 (国際特許分類 (IPC)) Int.Cl. H04L9/32, G09C1/00, H04Q7/38											
最小限資料以外の資料で調査を行った分野に含まれるもの <table border="0"> <tr> <td>日本国実用新案公報</td> <td>1922-1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971-2006年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996-2006年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994-2006年</td> </tr> </table>				日本国実用新案公報	1922-1996年	日本国公開実用新案公報	1971-2006年	日本国実用新案登録公報	1996-2006年	日本国登録実用新案公報	1994-2006年
日本国実用新案公報	1922-1996年										
日本国公開実用新案公報	1971-2006年										
日本国実用新案登録公報	1996-2006年										
日本国登録実用新案公報	1994-2006年										
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)											
C. 関連すると認められる文献											
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号									
A	J P 2 0 0 0 - 9 2 5 7 2 A (ルーセント テクノロジーズ インコーポレイテッド) 2000.03.31, 全文 & EP 982963 A2	1-16									
A	J P 2 0 0 0 - 1 1 5 1 6 1 A (ルーセント テクノロジーズ インコーポレイテッド) 2000.04.21, 全文 & EP 982958 A2	1-16									
<input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。		<input type="checkbox"/> パテントファミリーに関する別紙を参照。									
* 引用文献のカテゴリー 「A」特に関連のある文献ではなく、一般的技術水準を示すもの 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」口頭による開示、使用、展示等に言及する文献 「P」国際出願日前で、かつ優先権の主張の基礎となる出願		の日後に公表された文献 「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」同一パテントファミリー文献									
国際調査を完了した日 20.11.2006		国際調査報告の発送日 28.11.2006									
国際調査機関の名称及びあて先 日本国特許庁 (ISA/J P) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号		特許庁審査官 (権限のある職員) 石田 信行	5 S   9 4 6 9								
		電話番号 03-3581-1101 内線 3546									

国際調査報告

国際出願番号 PCT/JP2006/318433

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 10-191447 A (エヌ・ティ・ティ移動通信網株式会社) 1998.07.21, 全文 (ファミリーなし)	1-16
A	JP 7-203535 A (インターナショナル・ビジネス・マシーンズ・コーポレーション) 1995.08.04, 全文 & EP 658023 A1	1-16

## フロントページの続き

(81)指定国 AP(BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), EP(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW

(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

Fターム(参考) 5J104 AA07 AA16 AA41 AA49 EA03 EA04 EA08 EA16 KA02 NA02  
 NA05 NA12 NA36 NA37 PA07  
 5K067 AA30 BB21 CC08 EE02 EE10

(注)この公表は、国際事務局(WIPO)により国際公開された公報を基に作成したものである。なおこの公表に係る日本語特許出願(日本語実用新案登録出願)の国際公開の効果は、特許法第184条の10第1項(実用新案法第48条の13第2項)により生ずるものであり、本掲載とは関係ありません。