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

特許第5569670号
(P5569670)

(45)発行日　平成26年8月13日(2014.8.13)　(24)登録日　平成26年7月4日(2014.7.4)

(51)Int.Cl.		F I		
H04W 88/02	(2009.01)	H04W	88/02	140
H04L 9/08	(2006.01)	H04L	9/00	601B
H04W 12/04	(2009.01)	H04W	12/04	
H04W 24/06	(2009.01)	H04W	24/06	
H04B 7/10	(2006.01)	H04B	7/10	A

請求項の数 6　(全 13 頁)

(21)出願番号　特願2009-5563(P2009-5563)
(22)出願日　平成21年1月14日(2009.1.14)
(65)公開番号　特開2010-166210(P2010-166210A)
(43)公開日　平成22年7月29日(2010.7.29)
審査請求日　平成23年12月9日(2011.12.9)

(73)特許権者　304027349
国立大学法人豊橋技術科学大学
愛知県豊橋市天伯町雲雀ヶ丘１－１
(74)代理人　100095577
弁理士　小西　富雅
(74)代理人　100100424
弁理士　中村　知公
(72)発明者　大平　孝
愛知県豊橋市天伯町雲雀ヶ丘１－１　国立大学法人豊橋技術科学大学内
(72)発明者　成田　譲二
愛知県豊橋市天伯町雲雀ヶ丘１－１　国立大学法人豊橋技術科学大学内

最終頁に続く

(54)【発明の名称】秘密鍵共有通信システム及び通信方法

(57)【特許請求の範囲】
【請求項１】
第１の無線装置と第２の無線装置との間の秘密鍵共有通信システムであって、
前記第１の無線装置と前記第２の無線装置の少なくとも一方に備えられる可変指向性アンテナと、
前記第１の無線装置と第２の無線装置との各通信環境において最も高い秘匿条件付相互情報量となる指向性セットを保存する指向性セット保存部と、
前記第１の無線装置と第２の無線装置との通信環境に応じて前記指向性セット保存部に保存された指向性セットを選択し、前記可変指向性アンテナの指向性を制御する指向性制御部と、
を備えてなる秘密鍵共有通信システム。
【請求項２】
前記制御部は、前記第１の無線装置と前記第２の無線装置との間で秘密鍵を生成する前に電波の送受信を行って両者の通信環境を特定し、特定された通信環境に応じて前記指向性セットを選択する、ことを特徴とする請求項１に記載の秘密鍵共有通信システム。
【請求項３】
前記通信環境は送信電力対雑音電力比である、ことを特徴とする請求項１又は２に記載の秘密鍵共有通信システム。
【請求項４】
第１の無線装置と第２の無線装置の少なくとも一方の可変指向性アンテナの指向性を変

更することにより、前記第１の無線装置と前記第２の無線装置との間で秘密鍵共有通信を行う通信方法であって、
前記第１の無線装置と第２の無線装置との各通信環境において最も高い秘匿条件付相互情報量となる指向性セットを指向性セット保存部に保存し、
前記第１の無線装置と第２の無線装置との通信環境に応じて前記指向性セット保存部に保存された指向性セットを選択し、前記可変指向性アンテナの指向性を制御する、ことを特徴とする通信方法。
【請求項５】
前記第１の無線装置と前記第２の無線装置との間で秘密鍵を生成する前に電波の送受信を行って両者の通信環境を特定し、特定された通信環境に応じて前記指向性セットを選択する、ことを特徴とする請求項４に記載の通信方法。
【請求項６】
前記通信環境は送信電力対雑音電力比である、ことを特徴とする請求項４又は５に記載の通信方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は秘密鍵共有通信システム及び通信方法に関する。
【背景技術】
【０００２】
近年、携帯メールや無線LANの普及に伴い、だれもが電波を介してデータ情報交換や電子商取引をする機会が急増してきた。無線は煩雑な配線が不要であり、どこでも使えて便利なので今後益々利用者シーンの広がりが期待できる。
一方で、電波はあらゆる空間へ伝搬するため常に傍受・盗聴の危険にさらされている。一般に、傍受・盗聴の対策技術として暗号化が有効である。
暗号通信を行うためには通信の相手方と「鍵」を共有する必要がある。鍵の方式には大きく分類して「秘密鍵方式」と「公開鍵方式」がある。
現在広く用いられている「公開鍵方式」は「計算量的安全性」に基づいている。「計算量的安全性」とは現存する最速のコンピュータ等を用いても現実時間内では解読不可能なことを意味する。従って、将来的に量子コンピュータ等の実現により現在盗聴されたデータが何年か後に現実時間内で解読される危険性がある。
【０００３】
一方、「秘密鍵方式」は「情報量的安全性」に基づいている。「情報量的安全性」とはコンピュータ等の速度に関係なく安全性が保障される。
秘密鍵方式では、鍵配送問題(鍵情報を盗聴局等の第三者に漏洩することなくどうやって所望の相手方だけと共有するか)が技術的課題である。
最も単純な方法として、鍵情報を紙やカード媒体で相手方に手渡しするという方法もあるが、原始的な方法であるためリアルタイム更新できず発展性に乏しい。最先端の光ファイバ通信分野で最近研究されている量子暗号も一種の秘密鍵であり情報量的安全性を目指す革新的試みであるが、フォトンを粒子として扱うハードウェアが必要であるため現状では非常に高価な装置となる。
鍵配送問題を解決するための手法として、鍵を共有したい２つの無線装置間の伝送路の特性を測定し、その測定した特性に基づいて各無線装置で秘密鍵を生成する方法が提案されている（特許文献1,非特許文献1,非特許文献2）。
この方法は、2つの無線装置間でデータの送受信を繰り返し、RSSI（Received Signal Strength Indicator:受信信号強度、以下同じ）を各無線装置で測定する、これを鍵長回数繰り返してRSSI履歴を各無線装置で作成し、その作成したRSSI履歴に基づいて秘密鍵を生成する。
即ち、伝送路を伝搬する電波は可逆性を示すために、一方の無線装置から他方の無線装

置へデータを送信したときのRSSI値は、他方の無線装置から一方の無線装置へデータを伝送したときのRSSI値と比例関係にあるため、RSSI履歴の時間的揺らぎは同じになる。従って、一方の無線装置で測定したRSSI履歴に基づいて生成された秘密鍵は、他方の無線装置で測定したRSSI履歴に基づいて生成された秘密鍵と同じになる。

このように伝送路特性を用いて秘密鍵を生成する方法は２つの無線装置間で、情報を送信せずに電波を相互に送受信するだけで同じ秘密鍵を共有することができる。

【０００４】

また、RSSI履歴を生成する際、どちらかの無線装置が移動局であれば鍵生成毎に前回生成した鍵と独立な鍵を生成可能であるが、無線装置が固定局である屋内環境においては、鍵生成毎に独立な鍵生成が困難である。これを解決するための方法としてエスパアンテナ（非特許文献3）等の可変指向性アンテナを用いる方式が屋内環境においては実用的である。

可変指向性アンテナを用いる方式は一方の無線装置もしくは両方の無線装置が指向性を切り替え可能なアンテナを搭載しており、電波を送受信する際に毎回アンテナの指向性を切り替えることでゆらぎの大きなRSSI履歴を作成することが可能となる。またアンテナの指向性は無数に（例えば3素子エスパアンテナでは2^8^2=65536通り）存在し、鍵生成毎に使用する指向性もしくは使用する指向性の順番が異なるため、前回生成した鍵とは独立な鍵が生成可能である。

【０００５】

RSSI履歴から鍵生成する方法として、各無線装置でRSSI履歴の中央値を計算し、その中央値をしきい値として二値化する方法がある。即ちRSSI値が中央値よりも大きい場合「１」とし、RSSI値が中央値よりも小さい場合「０」として、RSSI履歴を二値化する。そして各無線装置で2値化したビット列は等しくなり、そのビット列が鍵となる。

【０００６】

可変指向性アンテナを用いた秘密鍵共有方式において、要求される耐性として雑音耐性と盗聴耐性がある。雑音耐性は、鍵を共有したい２つの無線装置間の鍵の一致率に関する評価指標であり、鍵の雑音耐性を高めることにより多様な環境下においてリアルタイムで安定した鍵の生成共有が可能となる。盗聴耐性は、鍵を共有したい無線装置の鍵と盗聴局の鍵の一致率に関する評価指標であり、鍵の盗聴耐性を高めることにより盗聴されにくい安全な鍵の生成共有が可能となる。

この雑音耐性と盗聴耐性がトレードオフの関係にある、即ち雑音耐性が高くなる指向性セットでは盗聴耐性が低くなり、盗聴耐性が高くなる指向性セットでは雑音耐性が低くなる傾向にあることが分かっている。

盗聴耐性、雑音耐性を共に高めるためには盗聴耐性の高い指向性セットを選択し、送信電力を増やすことで低減させることも可能であるが、ハードウェアの小型化に伴いバッテリ駆動による機器が増えてきていることを考えると送信電力を増やすことは極力避けたい。

【０００７】

アンテナにつき複数の指向性（リアクタンスセット）を予め定めておいて、アンテナの指向性を当該定められた複数の指向性の間で切り替えることにより雑音特性を高める取り組みが非特許文献４に紹介されている。また、同様にして盗聴耐性を高める取り組みが非特許文献５に紹介されている。

非特許文献６では、リアクタンスセットを決める際に秘匿条件付相互情報量を用いることが示されている。

【０００８】

【特許文献１】特開平２００６－３２４８７０号公報

【非特許文献１】大平　孝，　笹岡秀一，　“盗聴防止アンテナ　-セキュリティ対策への物理層的アプローチ-”，　信学誌,vol88,No.3,pp.190-194Mar.2005

【非特許文献２】岩井誠人，　笹岡秀一，　“電波伝搬特性を活用した秘密情報の伝送・共有技術”，　信学論(B)，vol.J-90B,No.9,pp770-783,2007

【非特許文献３】大平　孝，　飯草恭一，　“電子走査導波器アレーアンテナ，信学論(C)，vol.J87-C,No.1,pp.12-31，Jan. 2004
【非特許文献４】「３素子エスパアンテナを用いた秘密鍵共有方式において雑音耐性を高めるリアクタンスセット」、２００８年電子情報通信学会総合大会　Ｂ－５－１５４
【非特許文献５】「３素子エスパアンテナを用いた秘密鍵共有方式において盗聴耐性を高めるリアクタンスセット」、２００８年電子情報通信学会総合大会　Ｂ－５－１５５
【非特許文献６】「両端末に３素子エスパアンテナを用いた秘密鍵共有システムにおける秘匿条件付き相互情報量」　信学技報ＲＣＳ２００８－３，ｐｐ．１３－１８，Ｍａｙ２００８

【発明の開示】
【発明が解決しようとする課題】
【０００９】
　この発明は雑音耐性と盗聴耐性を包括的に高め、秘密鍵の不一致の低減及び盗聴を抑制可能とすることを目的としている。
　かかる目的を達成するため、まず、アンテナへ付与する好適な指向性のセットを特定する必要がある。
【００１０】
　計算機もしくは実機を用いて、鍵生成を行いたい第１の無線装置及び第２の無線装置並びに第三者で鍵を盗もうとしている第３の無線装置を用意する。第１の無線装置及び第２の無線装置の少なくとも一方は可変指向性アンテナを搭載している。第３の無線装置３は電波の強度測定を行い盗聴するために全方位性または可変指向性アンテナを搭載している。
【００１１】
　例１　　-指向性セットを特定するプロセス-
（１）第１の無線装置および第２の無線装置で共に使用する指向性セットは、ランダムな数値列を用いて用意したランダムな指向性系列で構成される。
（２）そのランダムな指向性系列で構成される指向性セットを用いて第１の無線装置と第２の無線装置との間で電波の送受信を行いRSSI値を測定する。第３の無線装置もRSSI値を測定する。
（３）各無線装置で測定したRSSI値を基に共通の鍵生成アルゴリズム(中央値で２値化等)で鍵生成を行う。
（４）生成された鍵は’０’と’１’の数値列で構成される。そして生成した鍵をビット毎に第１の無線装置、第２の無線装置２、第３の無線装置でどのような組み合わせになっているかを調べる。これを鍵の先頭ビットから順に最後のビットまで行うことで、表１に示す確率変数p1からp8を求める。この確率変数p1からp8を基に秘匿条件付相互情報量を計算する。明細書及び図面において、この秘匿条件付相互情報量をＩｍａｃ（Information Mutual anti-tapping condition）と略することがある。秘匿条件付相互情報量の意味は
秘匿条件付相互情報量=　鍵の実効長　/　生成した鍵長
であり、確率変数p1からp8を用いて以下の式に示す。
【数１】

$$\text{秘匿条件付き相互情報量} = I(\text{第１の無線装置};\text{第２の無線装置}\,|\,\text{第３の無線装置})$$
$$= (p1+p3+p4+p7)\mathrm{H}\left(\frac{p1+p3}{p1+p3+p4+p7}\right)+(p2+p5+p6+p8)\mathrm{H}\left(\frac{p2+p5}{p2+p5+p6+p8}\right)$$
$$-(p1+p4)\mathrm{H}\left(\frac{p1}{p1+p4}\right)-(p2+p6)\mathrm{H}\left(\frac{p2}{p2+p6}\right)-(p3+p7)\mathrm{H}\left(\frac{p3}{p3+p7}\right)-(p5+p8)\mathrm{H}\left(\frac{p5}{p5+p8}\right)$$

上式のHはエントロピー関数であり、次式で定義される。

【数２】

$$H(p) = -p\log p - (1-p)\log(1-p)$$

【表１】

秘匿条件付相互情報量導出に用いる確率変数の定義

第１の無線装置	0	0	0	1	0	1	1	1
第２の無線装置	0	0	1	0	1	0	1	1
第３の無線装置	0	1	0	0	1	1	0	1
発生確率	p1	p2	P3	p4	p5	p6	p7	p8

（５）第１の無線装置、第２の無線装置、第３の無線装置の位置やアンテナの方向を変え繰り返すことであらゆる環境下での秘匿条件付相互情報量を計算し、その平均値を求める。

（６）指向性セットを変えて（全数探索をするのが理想）（１）から（５）を繰り返し行い、秘匿条件付相互情報量が高くなる指向性セットを鍵生成に用いる指向性セットの候補とする。

【００１２】

上記のようにして指向性セットを特定するには手間がかかる。そこで、簡易に指向性セットを特定する方法について検討した。

例２、例３　-使用するハードウェア-

可変指向性アンテナを計算機上もしくは実機で用意する。

実機を用いる場合には振幅及び位相を測定するためのハードウェア（ネットワークアナライザ等）を用意する。またアンテナを回転させる台があることが望ましい。

-指向性セットを用意するプロセス-

空間相関が低くなる指向性セットを探索することを目的とする。

これは空間相関が低くなる指向性セットは秘匿条件付相互情報量が高くなる傾向があるためである。

【００１３】

（１１）ランダムな数値列を用いてランダムな指向性系列で構成される指向性セットを用意する。

（１２）その指向性セット内の指向性の空間相関を求める。例えば指向性セットが４つの指向性から構成されるとき各指向性をD_A, D_B, D_C, D_Dとすると

２種類の複素指向性を$D_A(\Phi), D_B(\Phi)$の２つの指向性の空間相関を次式で示す。

【数３】

$$\left|\rho_{AB}\right| = \frac{\left|\int_0^{2\pi} D_A(\Phi) D_B^{*}(\Phi) d\Phi\right|}{\sqrt{\int_0^{2\pi} \left|D_A(\Phi)\right|^2 d\Phi \int_0^{2\pi} \left|D_B(\Phi)\right|^2 d\Phi}}$$

ただし、*は複素共役を意味する。

これを指向性セット内の全ての指向性の組み合わせ($|\rho_{AB}|, |\rho_{AC}|, |\rho_{AD}|, |\rho_{BC}|, |\rho_{BD}|, |\rho_{CD}|$)で計算し、空間相関の平均もしくは、最大値を導出する。

（１３）指向性セットを変えて(全数探索をするのが理想)（１１）（１２）を繰り返し、空間相関の平均（例２）もしくは、最大値が低くなる（例３）指向性セットを鍵生成に用いる指向性セットの候補とする。

【００１４】

例４

更に簡易に指向性をセットを特定するには次のように行う。

可変指向性アンテナを計算機上もしくは実機で用意する。

実記を用いる場合にはFB(Front/Back)比及びEB(Endfire/Broadside)比を導出するために受信電力を測定するためのアンテナ等を用意する。

-指向性セットを用意するプロセス-

（２１）ランダムな数値列を用いてランダムな指向性列で構成される指向性セットを用意する。

（２２）その指向性セット内の各指向性において、水平方向の(0、π/2、π方向)の指向性強度を測定する。具体的にはまず可変指向性アンテナから一定距離Acmに測定用アンテナを置き電波の強度を測定する。次に可変指向性アンテナを中心に、測定用アンテナをπ/2方向へ移動させ電波の強度を測定する。次にさらにそこから測定用アンテナをπ/2方向へ移動させ電波の強度を測定する。これを各指向性に対して行う。

（２３）0度方向とπ方向の電波の強度の比を求めることでFB比が求まる。0度方向とπ/2方向の電波の強度を測定することでEB比がもとまる。

（２４）縦軸にEB比を横軸にFB比をとった2次元平面を考え、各指向性EB比とFB比の対応点をプロットする。そして対応点間のユークリッド距離を計算する。ユークリッド距離は指向性セット内の指向性の数が4個のときは全組み合わせで6通りとなる。２次元の実空間上においてユークリッド距離dは以下のようにして定義される。

【数４】

$$\mathbf{x} = (x1, x2), \mathbf{y} = (y1, y2)$$

$$d(x, y) = \sqrt{(x1 - y1)^2 + (x2 - y2)^2}$$

（２５）このユークリッド距離の最小値を求める。

（２６）指向性セットを変えて（全数探索をするのが理想）（２１）から（２６）を繰り返し、ユークリッド距離の最小値が大きくなる指向性セットを鍵生成に用いる指向性セットの候補とする。

【００１５】

次のようにして指向性のセットを準備することもできる。

例　５　　-使用するハードウェア-

可変指向性アンテナを計算機上もしくは実機で用意する。

実機を用いる場合には振幅及び位相を測定するためのハードウェア（ネットワークアナライザ等）を用意する。

-指向性セットを用意するプロセス-

（３１）ランダムな数値列を用いてランダムな指向性列で構成される指向性セットを用意する。

（３２）その指向性セット内の各指向性において、特定方向（例えばπ方向）の指向性の振幅及び位相を測定する。

（３３）各指向性の振幅と位相を基に極座標系にプロットする。その各点間のユークリッド距離を計算する。セット内指向性が4個の場合には4点がプロットされる。ユークリッド距離は6個求まる。

（３４）このユークリッド距離の最小値を求める。

（３５）指向性セットを変えて（全数探索するのが理想）（３１）から（３４）を繰り返

し、ユークリッド距離の最小値が大きくなる指向性セットを鍵生成に用いる指向性セットの候補とする。

【００１６】

既述の指向性セットの特定方法について再度説明する。

秘密鍵の性能は、実効鍵長を生成した鍵長で正規化した秘匿条件付相互情報量(値の範囲：0～1)で評価される。秘匿条件付相互情報量とは暗号通信を行いたい第１の無線装置と第２の無線装置で共有できている情報量から第三者にさらされる情報量を差し引いた量である。言い換えると実効鍵長は秘匿条件付相互情報量を用いて以下の式で与えられる。

実効鍵長[bit]=鍵長[bit]秘匿条件付相互情報量

実効鍵長が1bit長くなる度に生成される鍵のパターンは2倍になるため、実効鍵長を長くすることは非常に重要である。

【００１７】

秘匿条件付相互情報量を0.5にするための送信電力対雑音電力比は表2のようになる。従来方式と各指標を用いて用意した指向性セットを用いた場合の平均値の差に的を絞って説明する。

秘匿条件付相互情報量を指標に用いて用意した指向性セットを用いる場合（例１）、従来方式よりも6.1dB低く、送信電力は従来方式の約25%に抑えられる。

空間相関平均を指標に用いて用意した指向性セットを用いる場合（例２）、従来方式よりも5.5dB低く、送信電力は従来方式の約28%に抑えられる。

空間相関の最大値を指標に用いて用意した指向性セットを用いる場合（例３）、従来方式よりも5.2dB低く、送信電力を従来方式の約30%に抑えられる。

FB比とEB比を指標に用いて用意した指向性セットを用いる場合（例４） 、従来方式よりも3.4dB低く、送信電力を従来方式の約45%に抑えられる。

複素指向性を指標に用いて用意した指向性セットを用いる場合（例５）、従来方式よりも2.1dB低く、送信電力を従来方式の約62%に抑えられる。

【表２】

実施の結果

指標	従来方式	秘匿条件付相互情報量（例１）	空間相関平均（例２）	空間相関の最大値（例３）	FB比とEB比の使用（例４）	複素指向性（例５）
平均[dB]	88.1	82.0	82.6	82.9	84.7	86
従来方式との差[dB]	---	6.1	5.5	5.2	3.4	2.1
標準偏差[dB]	4.8	1.4	1.1	1.3	2.4	3.7
範囲[dB]	83.3-92.9	80.6-83.4	81.5-83.7	81.6-84.2	82.3-87.1	82.3-89.7

上記において、従来方式ではアンテナの指向性をランダムに変化させている。

表２から、例１～例５に示した全ての方式において送信電力の低下を達成できることがわかる。

【００１８】
上記のようにして好適な指向性セットを探索していたところ、指向性セットは通信環境、特に送信電力対雑音電力比（以下、「ＳＮＲ」ということがある）に依存していることに気がついた。即ち、第１のＳＮＲに対しては第１の指向性セットが好適であり、第２のＳＮＲに対して第２の指向性セットが好適な場合がある。
【発明を解決するための手段】
【００１９】
かかる知見に基づきこの発明は完成された。即ち、この発明は次のように規定される。
第１の無線装置と第２の無線装置との間の秘密鍵共有通信システムであって、
前記第１の無線装置と前記第２の無線装置の少なくとも一方に備えられる可変指向性アンテナと、
該アンテナについて予め定められた複数の指向性からなる第１の指向性セット、及び該アンテナについて前記第１の指向性セットとは異なる複数の指向性からなる第２の指向性セットを保存する指向性セット保存部と、
前記第１の無線装置と第２の無線装置との通信環境を参照して前記指向性セット保存部から前記第１又は第２の指向性セットを選択し、前記可変指向性アンテナの指向性を変更する指向性制御部と、
を備えてなる秘密鍵共有通信システム。
【発明を実施するための最良の形態】
【００２０】
図１はこの発明の実施例の秘密鍵共有通信システムの概略構成を示す。
鍵生成を行いたい第１の無線装置１及び、第２の無線装置１００並びに鍵を盗もうとしている第３の無線装置１１０を用意する。
第１の無線装置１は可変指向性アンテナ３と本体部１０を備えている。この第１の無線装置１と同様に第２の無線装置１００も可変指向性アンテナ３と本体部１０を備えてなる。第３の無線装置１１０は盗聴機本体１１５と全方位性アンテナ１１３とを備えている。
【００２１】
可変指向性アンテナ３はその指向性を変更できるものであれば任意の形式のアンテナを用いることができるが、この実施例ではエスパアンテナを採用した。エスパアンテナとはＥＳＰＡＲ（Electronically Steerable Parasitic Array Radiator，電子走査導波器アレー）アンテナであって、１本の給電素子と複数のパラサイト素子とで構成される。各パラサイト素子にはバラクタが付設されており、このバラクタへ印加する電圧を変化させることでアンテナの指向性を変化させることができる。
換言すれば、各バラクタへ印加する電圧を予めセットしておくことにより、所望の指向性をアンテナへ与えることが可能となる。
【００２２】
図１に示すように、本体部１０は指向性制御部２０、指向性セット生成部３０、送信出力制御部５０及び通信制御部６０を大略備えてなる。
指向性制御部２０はエスパアンテナ３の各バラクタへ印加する電圧を制御する。
指向性セット保存部２１は選択された指向性セット保存部２３とＳＮＲ（Signal Noise ratio，送信電力対雑音電力比）保存部２５を備える。選択された指向性セット保存部２３には、秘密鍵共有通信システムに好適な指向性のセットが、ＳＮＲ保存部２５に保存されているＳＮＲに関連付けて保存されている。
【００２３】
指向性セット生成部３０は選択された指向性セット保存部２３に保存する指向性セットを生成するものであり、指向性セットランダム発生部３１と該指向性セットランダム発生部３１で発生された指向性セットの全てを保存する全指向性セット保存部３３を備えている。
指向性ランダム発生部３１が発生した指向性セットに基づき第１の無線装置１と第２の無線装置１００との間で通信を行った際、相手方である第２の無線装置１００から送信さ

れてきた電波の強さに基づきＲＳＳＩ演算部４１がＲＳＳＩ値を演算する。得られたＲＳＳＩ値に基づき、鍵生成部４３は周知の鍵生成アルゴリズム（中央値で２値化する等）に従い秘密鍵を生成する。Ｉｍａｃ演算部４５は生成された鍵に基づき秘匿条件付相互情報量（Ｉｍａｃ）を演算する。Ｉｍａｃ保存部４７は得られた秘匿条件付相互情報量を保存する。無線機の位置やアンテナの向きを変更して演算した秘匿条件付相互情報量の平均値をＩｍａｃ保存部４７へ保存することもできる。

なお、Ｉｍａｃ演算部４５及びＩｍａｃ保存部４７は、好適な指向性セットを求める方式の例１に該当する。他の例２～例５の方式にしたがって指向性セットも求める場合には、各方式に即した演算部と保存部とを用いることとなる。

【００２４】

指向性セット選択部４９は、Ｉｍａｃ保存部４７に保存されている最も高い値の秘匿条件付相互情報量を値を選択し、それに対応する指向性セットを全指向性セット保存部３３から選択する。そして、選択された指向性セットを選択された指向性セット保存部２３へ保存する。

【００２５】

送信出力制御部５０は第１の無線装置１から送信される電波の出力強度を制御し、ＳＮＲ演算部５１は送信された電波強度に対応してＳＮＲを演算する。

なお、第１のＳＮＲの環境において指向性セット生成部３０を動作させて選択される第１の指向性セットと第２のＳＮＲの環境において同じく指向性セット生成部３０を動作させて得られる第２の指向性セットとは必ずしも一致しない。そこで、ＳＮＲ環境と当該環境における好適な指向性セットとを関連付けで指向性セット保存部２１に保存することが好ましい。

【００２６】

通信制御部６０は、第２の無線装置１００との間で通信を行う際に生成される秘密鍵を用いて、通信対象となるデータをエンコード／デコードする。

第２の無線装置１００は第１の無線装置１と同じ構成である。

第３の無線装置１１０は盗聴の可能性を探るものであり、第１の無線装置１の本体部１０におけるＲＳＳＩ演算部４１、鍵生成部４３及び通信制御部６０と同一若しくは同等の要素を少なくとも備えている。

第１、第２及び第３の無線装置における本体部はコンピュータ装置により実行することができる。

【００２７】

次に、実施例の秘密鍵共有通信システムの動作について説明する。

受信電力対雑音電力比は通信を行う無線装置間距離と送信電力と受信機の雑音指数で決まる。

ここでは無線装置間距離と受信機の雑音指数を固定パラメータとし、送信電力を変えることで受信電力対雑音電力比を変える。

まず送信電力を使用の想定される範囲で最小の値にセットする。

（４１）第１の無線装置１及び第２の第２の無線装置１００で共に使用する指向性セットは、ランダムな数値列を用いて用意したランダムな指向性系列で構成される。

（４２）指向性制御部２０は、指向性セットランダム発生部３１の生成するランダムな指向性セットを用いてアンテナ３の指向性を定め、第１の無線装置１と第２の無線装置１００との間で電波の送受信しRSSI値を測定する（ＲＳＳＩ演算部４１）。第３の無線装置１１０もRSSI値を測定する。指向性セットランダム発生部３１の発生した指向性セットは全て全指向性セット保存部３３に保存される。

（４３）各無線装置で測定したRSSI値を基に共通の鍵生成アルゴリズム(中央値で２値化等)で鍵生成を行う（鍵生成部４３）。

（４４）生成された鍵を基に秘匿条件付相互情報量を計算する（Ｉｍａｃ演算部４５）。

（４５）第１の無線装置１、第２の無線装置１００及び第３の無線装置１１０の位置やアンテナの方向を変え繰り返すことであらゆる環境下での秘匿条件付相互情報量を計算し、

その平均値を求め保存する（Ｉｍａｃ保存部４７）。
（４６）指向性セットを変えて（全数探索をするのが理想）（４１）から（４５）を繰り返し、秘匿条件付相互情報量が高くなる指向性セットを鍵生成に用いる好適な指向性セットとして選択する（指向性セット選択部４９）。これでまず送信電力が低いとき、即ち第１のＳＮＲ環境における最適な指向性セットが求まる。
この指向性セットは具体的にはエスパアンテナのバタクタへ印加する電圧のセットであり、バラクタのリアクタンスのセットと同意である。
なお、指向性セットを構成する指向性は２以上であり、この実施例では３つの異なる指向性を採用し、セットを構成することとしている。
（４７）次に、送信出力制御部５０を動作させて送信電力を少しあげて（３倍程度）（４１）から（４６）を繰り返す。これにより第２のＳＮＲ環境における最適な指向性セットが求められる。送信電力を更にあげることにより、使用が想定される全てのＳＮＲ環境につき最適な指向性セットが求められる。
これらＳＮＲと指向性セットは相互に関係付けられて指向性セット保存部２１に保存される。

【００２８】

かかる通信システムによれば次のようにして通信が実行される（図２参照）。
第２の無線装置１００から全方位性（オムニ）の指向性を用いてパイロット信号が送信される（ステップ１）。第１の無線装置１はこのパイロット信号を受信し、ＲＳＳＩ演算部４１を用いてＲＳＳＩを演算する（ステップ３）。
得られたＲＳＳＩに基づきＳＮＲ演算部５１はＳＮＲを演算する（ステップ５）。ＳＮＲの計算方法を説明する。まず、無線装置１から無線装置２へ電波を送信するタイミングを通知する。つぎに無線装置２では、そのタイミング情報を基に、電波を送信されているときの受信強度と電波を送信されていないときの受信強度をそれぞれ測定する。ＳＮＲは、電波を送信されているときの受信強度と電波を送信されていないときの受信強度の差で求まる。得られたＳＮＲに基づき、指向性制御部２０は、指向性セット保存部２１を参照して、得られたＳＮＲに対応する最適な指向性セットを特定、使用する（ステップ７）。この指向性セットを用いて鍵を生成し（ステップ９）、通信が実行される。
第１の無線装置１からも同様にしてパイロット信号が発信され、第２の無線装置１００において上記と同様な処理が実行される。

【００２９】

次に、シミュレーションによる結果を図面を参照にしながら詳細に説明する。
まず、環境により最適な指向性セットが異なることを説明する。ここで環境とはSN(受信信号電力対雑音電力)比のことを指す。しかし、可変指向性アンテナでは指向性によってSN比が異なるため、SN比を用いて議論することができない。そのため、その代価指標として送信電力対雑音電力比を用いる。ここで端末間距離を固定することにより、送信電力対雑音電力比がSN比にダイレクトに効いてくるようにしている。つまり送信電力対雑音電力比によって最適な指向性セットが異なるということは、実際には無線装置間距離や受信機の雑音指数等により最適な指向性セットが異なることを意味する。

【００３０】

図３は秘匿条件付相互情報量を指標として選んだ指向性セットを用いたとき、選んだセット毎に生成した鍵の送信電力対雑音電力比に対する秘匿条件付相互情報量を表したものである。送信電力対雑音電力比が小さい環境(70dBまでは)setDが秘匿条件付相互情報量が最も高く,70-80dBではsetCが秘匿条件付相互情報量が最も高く、80-100dBではsetBが秘匿条件付相互情報量が最も高く、100dB以上ではsetAが秘匿条件付相互情報量が最も高い。このことより環境によって最適な指向性セットが異なることがわかる。

【００３１】

実施例では事前に電波の送受信を行い、環境ごとに最適な指向性セットを選択している。環境毎に最適な指向性セットを用いた場合の結果を図４に示す。比較するために環境によらず単一の指向性セットを用いた場合の平均結果と従来方式による平均結果も示してあ

る。
最適な指向性セットを用いた場合、従来方式よりも送信電力対雑音電力比が低く抑えられているのは明らかである。また環境測定により最適指向性セットを選択する場合の方が単一セットを用いる場合よりも平均して1dB程度高くなっている。また単一セットを用いる場合では送信電力を上げていっても秘匿条件付相互情報量のフロアが0.77程度までしか上がらないのに対し、最適指向性セットを選択する場合にはフロアが0.83程度まで上がる。

【００３２】
上記実施例では、通信環境に応じてより好適な指向性セットを選択するときの指標としてＳＮＲ（送信電力対雑音電力比）を用いたが、他にもＳＩＲ（信号対干渉比）、ＳＩＮＲ（信号対干渉雑音比）または、これらを時系列的に観測して得られるデータ列の統計量（例えば分散やモーメント）を通信環境の指標として利用することができる。
この発明は、上記発明の実施の形態及び実施例の説明に何ら限定されるものではない。特許請求の範囲の記載を逸脱せず、当業者が容易に想到できる範囲で種々の変形態様もこの発明に含まれる。

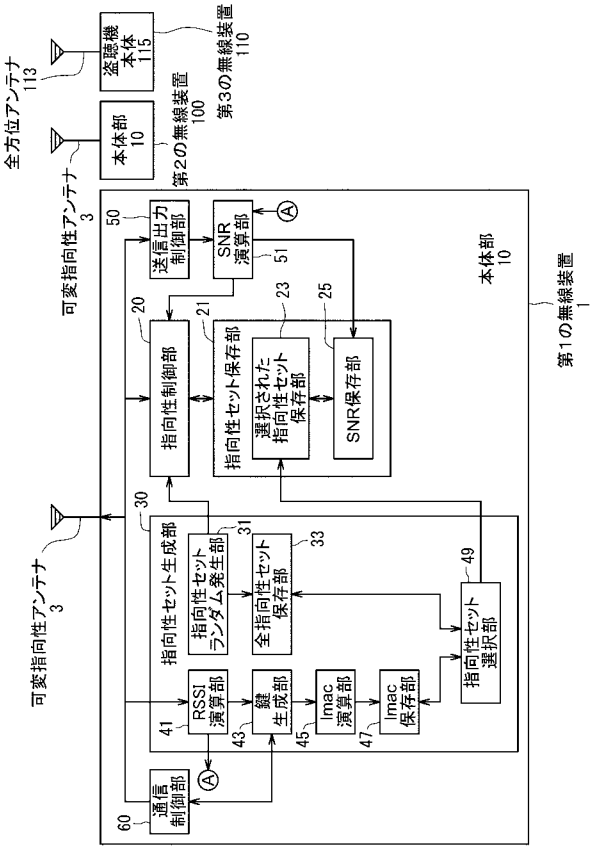
【図面の簡単な説明】

【００３３】
【図１】図１はこの発明の実施例の通信システムで使用する無線装置の構成を示すブロック図である。
【図２】図２は実施例の通信システムの動作を示すフローチャートである。
【図３】図３は指向性セット毎の送信電力対雑音電力比と秘匿条件付相互情報量との関係を示すグラフである。
【図４】図４は送信電力対雑音電力比の環境ごとに最適な指向性セットを選択したときの送信電力対雑音電力比と秘匿条件付相互情報量との関係を示すグラフである。

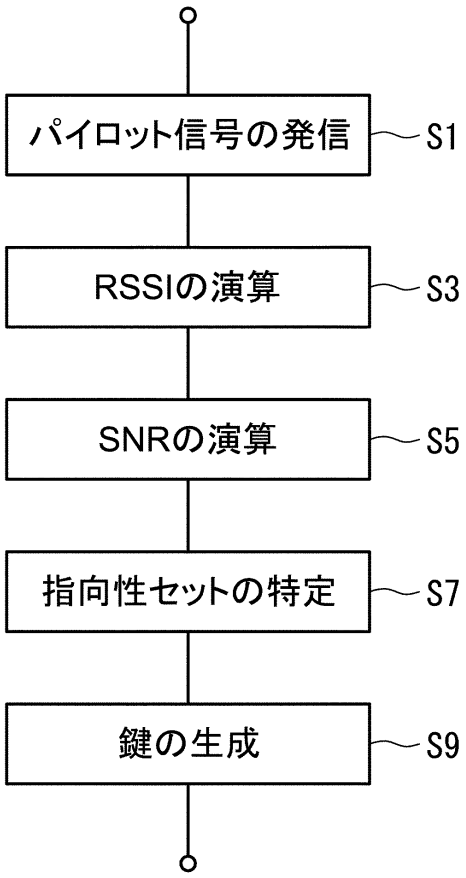
【符号の説明】

【００３４】
１　第１の無線装置
３　可変指向性アンテナ
２０　指向性制御部
２１　指向性セット保存部
３０　指向性セット生成部
５０　送信出力制御部
５１　ＳＮＲ演算部
１００　第２の無線装置
１１０　第３の無線装置

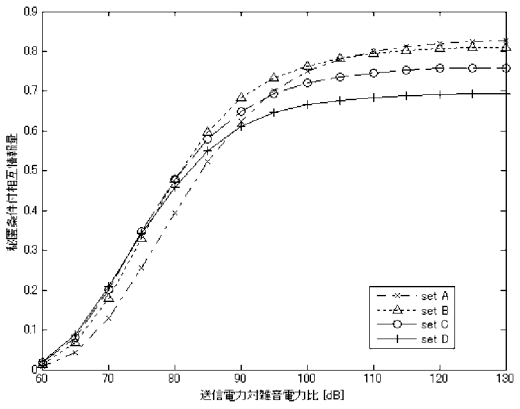
【図１】


全方位アンテナ
113
盗聴機
本体
115
第3の無線装置
110
本体部
10
第2の無線装置
100
可変指向性アンテナ
3
50
送信出力
制御部
SNR
演算部
51
A
本体部
10
第1の無線装置
1
20
指向性制御部
21
指向性セット保存部
23
選択された
指向性セット
保存部
25
SNR保存部
30
指向性セット生成部
31
指向性セット
ランダム発生部
33
全指向性セット
保存部
49
指向性セット
選択部
可変指向性アンテナ
3
41
RSSI
演算部
43
鍵
生成部
45
Imac
演算部
47
Imac
保存部
A
60
通信
制御部

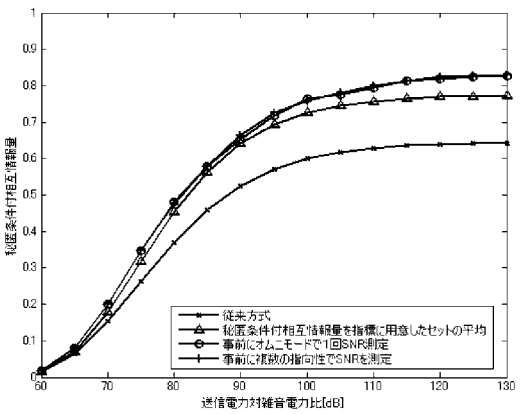
【図２】


パイロット信号の発信
S1
RSSIの演算
S3
SNRの演算
S5
指向性セットの特定
S7
鍵の生成
S9

【図３】


秘匿条件付相互情報量
送信電力対雑音電力比 [dB]
set A
set B
set C
set D

【図４】


秘匿条件付相互情報量
送信電力対雑音電力比[dB]
従来方式
秘匿条件付相互情報量を指標に用意したセットの平均
事前にオムニモードで1回SNR測定
事前に複数の指向性でSNRを測定

フロントページの続き

(72)発明者　長谷川　拓
愛知県豊橋市天伯町雲雀ヶ丘１－１　国立大学法人豊橋技術科学大学内

審査官　石田　昌敏

(56)参考文献　特開２００５－１５０９４９（ＪＰ，Ａ）
特開２００８－２４５０１０（ＪＰ，Ａ）
特開２００７－０７４６００（ＪＰ，Ａ）
特表２００８－５３０９５６（ＪＰ，Ａ）
特開２００８－１６０５３２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｗ　　４／００－９９／００
Ｈ０４Ｂ　　７／０２－　７／１２
Ｈ０４Ｌ　　９／００－　９／０８
Ｈ０４Ｋ　　１／００－　３／００