

(19) 日本国特許庁 (JP)

(12) 公 開 特 許 公 報 (A)

(11) 特許出願公開番号
特開2012-217153
(P2012-217153A)

(43) 公開日 平成24年11月8日 (2012.11.8)

(51) Int.Cl.
H04L 9/08 (2006.01)

F I
H04L 9/00 601A
H04L 9/00 601C

テーマコード (参考)
5J104

審査請求 未請求 請求項の数 10 O L (全 19 頁)

(21) 出願番号	特願2012-55568 (P2012-55568)	(71) 出願人	000005821
(22) 出願日	平成24年3月13日 (2012. 3. 13)		パナソニック株式会社
(31) 優先権主張番号	特願2011-77631 (P2011-77631)		大阪府門真市大字門真1006番地
(32) 優先日	平成23年3月31日 (2011. 3. 31)	(74) 代理人	100109667
(33) 優先権主張国	日本国 (JP)		弁理士 内藤 浩樹
		(74) 代理人	100109151
			弁理士 永野 大介
		(74) 代理人	100120156
			弁理士 藤井 兼太郎
		(72) 発明者	西 竜三
			福岡県福岡市博多区美野島4丁目1番62号
			パナソニックシステムネットワークス株式会社内
		Fターム (参考)	5J104 AA01 AA16 AA32 AA41 EA04 FA00 JA03 NA02 NA37 PA07

(54) 【発明の名称】 通信装置、通信システムおよび通信方法

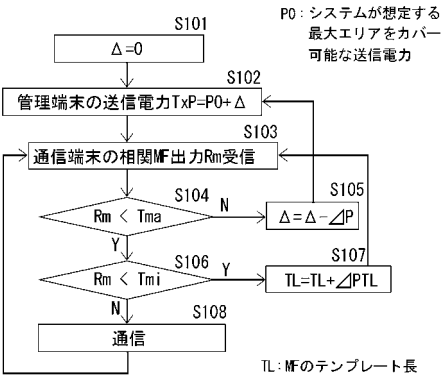
(57) 【要約】

【課題】 第三者による通信内容の傍受可能範囲を制限しつつ、無線通信装置と通信可能な正規の端末装置の範囲制限が緩和され、遠距離においても、無線通信装置と正規の端末装置の通信が可能な通信装置、通信システムおよび通信方法を提供することを目的とする。

【解決手段】 受信した冗長なデータに対して、送信側と同じ符号を作用させた後に積分を行って、送信側の変調方式に対応する復調方式を用いてデータを復調する。積分出力について、上限と下限の閾値を設定して、積分出力が上限の閾値より大きい場合には、通信相手の送信電力を下げ、積分出力が下限の閾値よりも小さい場合には、作用させる符号の長さを長くする。

【選択図】 図7

下り回線（管理端末→通信端末）制御フロー



【特許請求の範囲】

【請求項 1】

他の通信装置と通信を行う通信装置であって、
Nビットの送信データをMビットのビット長に複製する複製手段と（Nは1以上の整数、Mは2以上の整数、 $N < M$ ）、
前記複製手段により複製された送信データに乱数を乗算する乗算手段と、
前記乗算手段により乱数が乗算された送信データを前記他の通信装置に送信する送信手段とを備え、
前記複製手段は、前記他の通信装置からの受信電力に応じて、送信データを複製するビット長をMビットからKビットに変更し（Kは1以上の整数、 $K \neq M$ ）、Nビットの送信データをKビットのビット長に複製することを特徴とする通信装置。

10

【請求項 2】

前記複製手段は、前記受信電力が所定値より小さい場合に、送信データが複製されるビット長をKビット（ $M < K$ ）に変更することを特徴する請求項1記載の通信装置。

【請求項 3】

さらに、送信データの電力を制御する送信電力制御手段を備え、
前記送信電力制御手段は、前記受信電力が所定値より小さい場合に、送信電力を低下させることを特徴とする請求項2記載の通信装置。

【請求項 4】

前記送信電力制御手段は、前記受信電力が第1の閾値より小さい場合に、送信データの電力を低下させ、

20

前記複製手段は、前記受信電力が前記第1の閾値より小さい第2の閾値より小さい場合に、送信データを複製するビット長を変更することを特徴とする請求項3記載の通信装置。

【請求項 5】

前記受信電力は信号成分のみの電力であることを特徴とする請求項1ないし4いずれか1項に記載の通信装置。

【請求項 6】

さらに、前記他の通信装置からMビットの受信データを受信する受信手段を備え、
前記乗算手段は、さらに、前記受信データに乱数を乗算し、
前記複製手段は、さらに、前記乱数が乗算された受信データのビット長をMビットからNビットに短縮し、
前記複製手段は、前記受信データの電力に応じて、前記送信データを複製するビット長とともに、前記受信データに乗算される乱数のビット長をMビットからKビットに変更することを特徴とする請求項1記載の通信装置。

30

【請求項 7】

他の通信装置と通信を行う通信方法であって、
Nビットの送信データをMビットのビット長に複製し（Nは1以上の整数、Mは2以上の整数、 $N < M$ ）、
前記複製された送信データに乱数を乗算し、
前記乱数が乗算された送信データを前記他の通信装置に送信し、
前記送信データを複製する場合において、前記他の通信装置からの受信電力に応じて、送信データを複製するビット長をMビットからKビットに変更し（Kは1以上の整数、 $K \neq M$ ）、Nビットの送信データをKビットのビット長に複製することを特徴とする通信方法。

40

【請求項 8】

送信装置および受信装置を有する通信システムであって、
前記送信装置は、
Nビットの送信データをMビットのビット長に複製する複製手段と（Nは1以上の整数、Mは2以上の整数、 $N < M$ ）、

50

前記複製手段により複製された送信データに乱数を乗算する第 1 の乗算手段と、

前記第 1 の乗算手段により乱数が乗算された送信データを前記受信装置に送信する送信手段とを備え、

前記複製手段は、前記受信電力に応じて、送信データを複製するビット長を M ビットから K ビットに変更し（K は 1 以上の整数、 $K \neq M$ ）、N ビットの送信データを K ビットのビット長に複製し、

前記受信装置は、

前記送信装置から M ビットの受信データを受信する受信手段と、

前記受信データに乱数を乗算する第 2 の乗算手段と、

前記乱数が乗算された受信データのビット長を M ビットから N ビットに短縮する短縮手段とを備え、

前記短縮手段は、前記受信電力に応じて、前記送信データを複製するビット長とともに、前記受信データに乗算される乱数のビット長を M ビットから K ビットに変更し、K ビットの送信データを N ビットのビット長に短縮することを特徴とする通信システム。

【請求項 9】

前記受信装置は、さらに、前記乱数が乗算された受信データを鍵シーケンスとしてマスター鍵を生成するマスター鍵生成手段を備えることを特徴とする請求項 8 記載の通信システム。

【請求項 10】

前記受信データは第 1 の値および第 2 の値の 2 値を含み、

前記マスター鍵生成手段は、さらに、前記受信データにおいて前記第 1 の値のビット数と前記第 2 の値のビット数の差が所定値以下の場合に、前記乱数が乗算された受信データを鍵シーケンスとしてマスター鍵を生成することを特徴とする請求項 9 記載の通信システム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、相手装置と通信する際に、通信する情報の守秘性を確保するための通信装置、通信システムおよび通信方法に関するものである。

【背景技術】

【0002】

図 15 は、（特許文献 1）に記載された、守秘性を確保したい通信の処理動作を示す図である。

【0003】

以上のような処理フローを有する無線通信装置について、その動作（特許文献 1 に記載された動作）を説明する。

【0004】

新たに通信したい端末装置がいた場合、無線通信装置を登録モードに設定する。登録モードに設定すると、出力電力を減少させることによって、距離の近い通信装置のみが登録可能になり、距離の遠い他の端末装置を排除することが出来る。そして、端末装置からリンク接続要求が受信できれば、リンクは確立するが、リンク接続要求が受信できなければ、再送を繰り返す。これらの処理により、登録作業におけるセキュリティ上の管理が容易になるが、無線通信装置から送信される登録情報を、登録を希望する正規の端末装置が受信可能な範囲が制限される。

【先行技術文献】

【特許文献】

【0005】

【特許文献 1】特開 2003-299146 号公報

【発明の概要】

【発明が解決しようとする課題】

10

20

30

40

50

【0006】

本発明が解決しようとしている課題は、第三者による通信内容の傍受可能範囲を制限しつつ、無線通信装置と通信可能な正規の端末装置の範囲制限が緩和され、遠距離においても、無線通信装置と正規の端末装置の通信が可能な通信装置、通信システムおよび通信方法を提供することである。

【課題を解決するための手段】

【0007】

上記課題を解決するために、本発明は、他の通信装置と通信を行う通信装置であって、Nビットの送信データをMビットのビット長に複製する複製手段と（Nは1以上の整数、Mは2以上の整数、 $N < M$ ）、複製手段により複製された送信データに乱数を乗算する乗算手段と、乗算手段により乱数が乗算された送信データを他の通信装置に送信する送信手段とを備え、複製手段は、他の通信装置からの受信電力に応じて、送信データを複製するビット長をMビットからKビットに変更し（Kは1以上の整数、 $K \neq M$ ）、Nビットの送信データをKビットのビット長に複製する。

【発明の効果】

【0008】

本発明によれば、第1の発明によれば、受信電力が変動した場合であっても、セキュリティを確保しながら第三者へのS/N比を上げることなく、正規の受信者へのS/N比のみを向上させることが出来る。

【図面の簡単な説明】

【0009】

【図1】通信端末を示す外観斜視図

【図2】通信端末のハードウェアの一例を示すブロック図

【図3】管理端末（前面）を示す外観斜視図

【図4】管理端末（背面）を示す外観斜視図

【図5】管理端末のハードウェアの一例を示すブロック図

【図6】通信端末および管理端末の機能ブロック図

【図7】下り回線の制御フローを示す図

【図8】下り回線制御フローの時間軸上での概念図

【図9】モバイル環境での下り回線の制御フローを示す図

【図10】上り回線の制御フローを示す図

【図11】事前処理部の機能ブロック図

【図12】事前処理部の動作を示したタイミングチャートを示す図

【図13】事後処理部の機能ブロック図

【図14】事後処理部の動作を示したタイミングチャートを示す図

【図15】従来の技術における処理手順を示す処理フローを示す図

【図16】実施の形態2における鍵生成共有シーケンスを示す図

【図17】実施の形態2における鍵シーケンス生成を示すブロック図

【図18】マスター鍵生成フローを示す図

【図19】セッション鍵生成を示す説明図

【発明を実施するための形態】

【0010】

上記課題を解決するためになされた第1の発明は、他の通信装置と通信を行う通信装置であって、Nビットの送信データをMビットのビット長に複製する複製手段と（Nは1以上の整数、Mは2以上の整数、 $N < M$ ）、複製手段により複製された送信データに乱数を乗算する乗算手段と、乗算手段により乱数が乗算された送信データを他の通信装置に送信する送信手段とを備え、複製手段は、他の通信装置からの受信電力に応じて、送信データを複製するビット長をMビットからKビットに変更し（Kは1以上の整数、 $K \neq M$ ）、Nビットの送信データをKビットのビット長に複製する通信装置である。

【0011】

第1の発明によれば、受信電力が変動した場合であっても、セキュリティを確保しながら第三者へのS/N比を上げることなく、正規の受信者へのS/N比のみを向上させることが出来る。

【0012】

上記課題を解決するためになされた第2の発明は、第1の発明であって、複製手段は、受信電力が所定値より小さい場合に、送信データが複製されるビット長をKビット ($M < K$) に変更する通信装置である。

【0013】

第2の発明によれば、受信電力が低下した場合に、正規の受信者へのS/N比低下を抑制することが出来る。

【0014】

上記課題を解決するためになされた第3の発明は、第2の発明であって、さらに、送信データの電力を制御する送信電力制御手段を備え、送信電力制御手段は、受信電力が所定値より小さい場合に、送信電力を低下させる通信装置である。

【0015】

第3の発明によれば、ビット長を長く変更することなく、送信電力を低下することで、オーバーヘッドの増大を抑制しながら、通信エリアの不要な拡大を防止することが出来る。

【0016】

上記課題を解決するためになされた第4の発明は、第3の発明であって、送信電力制御手段は、受信電力が第1の閾値より小さい場合に、送信データの電力を低下させ、複製手段は、受信電力が第1の閾値より小さい第2の閾値より小さい場合に、送信データを複製するビット長を変更する通信装置である。

【0017】

第4の発明によれば、受信電力が低下する場合に、送信データの電力を優先した上で、乱数を乗算する送信データの複製範囲を変更するので、通信エリアの不要な拡大を防止した上で、その通信エリア内に存在する正規の受信者へのS/N比低下を抑制することが出来る。

【0018】

上記課題を解決するためになされた第5の発明は、第1ないし4いずれかの発明であって、受信電力は信号成分のみの電力である通信装置である。

【0019】

第5の発明によれば、ノイズなどの外因を除外することが出来るので、正規の受信者へのS/N比が低下する場合に、S/N比を向上させることが出来る。

【0020】

上記課題を解決するためになされた第6の発明は、第1の発明であって、さらに、他の通信装置からMビットの受信データを受信する受信手段を備え、乗算手段は、さらに、前記受信データに乱数を乗算し、複製手段は、さらに、乱数が乗算された受信データのビット長をMビットからNビットに短縮し、複製手段は、受信データの電力に応じて、送信データを複製するビット長とともに、受信データに乗算される乱数のビット長をMビットからKビットに変更する通信装置。

【0021】

第6の発明によれば、ノイズなどの外因を除外することが出来るので、正規の受信者へのS/N比が低下する場合に、S/N比を向上させることが出来る。

【0022】

上記課題を解決するためになされた第7の発明は、他の通信装置と通信を行う通信方法であって、Nビットの送信データをMビットのビット長に複製し (N は1以上の整数、 M は2以上の整数、 $N < M$)、複製された送信データに乱数を乗算し、乱数が乗算された送信データを他の通信装置に送信し、送信データを複製する場合において、他の通信装置からの受信電力に応じて、送信データを複製するビット長をMビットからKビットに変更し

10

20

30

40

50

(K は1以上の整数、 $K \neq M$)、 N ビットの送信データを K ビットのビット長に複製する通信方法。

【0023】

第7の発明によれば、受信電力が変動した場合であっても、セキュリティを確保しながら第三者への S/N 比を上げることなく、正規の受信者への S/N 比のみを向上させることが出来る。

【0024】

上記課題を解決するためになされた第8の発明は、送信装置および受信装置を有する通信システムであって、送信装置は、 N ビットの送信データを M ビットのビット長に複製する複製手段と(N は1以上の整数、 M は2以上の整数、 $N < M$)、複製手段により複製された送信データに乱数を乗算する第1の乗算手段と、第1の乗算手段により乱数が乗算された送信データを受信装置に送信する送信手段とを備え、複製手段は、受信電力に応じて、送信データを複製するビット長を M ビットから K ビットに変更し(K は1以上の整数、 $K \neq M$)、 N ビットの送信データを K ビットのビット長に複製し、受信装置は、送信装置から M ビットの受信データを受信する受信手段と、受信データに乱数を乗算する第2の乗算手段と、乱数が乗算された受信データのビット長を M ビットから N ビットに短縮する短縮手段とを備え、短縮手段は、受信電力に応じて、送信データを複製するビット長とともに、受信データに乗算される乱数のビット長を M ビットから K ビットに変更し、 K ビットの送信データを N ビットのビット長に短縮することを特徴とする通信システム。

【0025】

第8の発明によれば、受信電力が変動した場合であっても、セキュリティを確保しながら第三者への S/N 比を上げることなく、正規の受信者への S/N 比のみを向上させることが出来る。

【0026】

上記課題を解決するためになされた第9の発明は、第8の発明であって、受信装置は、さらに、乱数が乗算された受信データを鍵シーケンスとしてマスター鍵を生成するマスター鍵生成手段を備える通信システム。

【0027】

第9の発明によれば、鍵シーケンスとして、伝送誤りの情報を利用することが出来るので、マスター鍵の予測を困難にすることが出来る。

【0028】

上記課題を解決するためになされた第10の発明は、第9の発明であって、記受信データは第1の値および第2の値の2値を含み、マスター鍵生成手段は、さらに、受信データにおいて第1の値のビット数と第2の値のビット数の差が所定値以下の場合に、乱数が乗算された受信データを鍵シーケンスとしてマスター鍵を生成する通信システム。

【0029】

第10の発明によれば、第1の値および第2の値の分布に適度なバランスに設定することが出来るので、鍵シーケンス K を用いた暗号鍵の推測を困難にすることが出来る。

【0030】

(実施の形態1)

以下、本発明の具体的な内容について実施の形態1を用いて説明する。

【0031】

本発明の実施の形態1について図1、2、3、4、5、6、7、8、9、10、11、12、13および14を用いて説明する。

【0032】

図1は、通信端末を示す外観斜視図である。

【0033】

本実施の形態1における通信端末1a、1bは、通信装置の一例であって、図1に示すように、携帯可能な電話器である。通信端末1a、1bは筐体101を有しており、筐体101には、電話番号などを表示するLCD(Liquid Crystal Disp

10

20

30

40

50

lay) 102と、電話番号を指定するためのボタンなどで構成されるキーマトリックス103と、マイク104と、電波を送受信する外部アンテナ105aと、話し相手からの音声を出力するスピーカ106とが設けられている。なお、通信端末の一例として、図1の電話器を示したが、特に電話器に限る必要はなく、通信端末は、アクセスポイントを含む他の通信端末と接続可能な機能を備えた機器（例えばパーソナルコンピュータなどの電子機器）であってもよい。

【0034】

図2は、通信端末のハードウェアの一例を示すブロック図である。

【0035】

通信端末1a、1bは、図2に示すように、破線で示す筐体101内に、回路モジュール110を有している。回路モジュール110には、図1で説明したLCD102やキーマトリックス103の他、ベースバンドIC(Integrated Circuit)111と、無線モジュール124とが実装されている。

【0036】

ベースバンドIC111は、CPU(Central Processing Unit)111aと、音声処理を行うVoIP(Voice over Internet Protocol)ブロック111bと、無線LAN(Local Area Network)のMAC(Medium Access Control)層を制御する無線MACブロック111cと、メインバス111dやローカルバス111eなどのバスとを有している。

【0037】

ベースバンドIC111内のCPU111a、VoIPブロック111b、および無線MACブロック111cは、メインバス111dを介して、SDRAM(Synchronous Dynamic Random Access Memory)112、およびFlash ROM(Flash Read Only Memory)113に接続されている。また、CPU111aは、ローカルバス111eを介して、LCD102、LCDの電源を制御するLCD電源制御IC114、必要なDC(Direct Current)電圧に変換するDC-DC(Direct Current to Direct Current)変換器116、初期化信号を通知するリセットIC118および、電池121に接続され電池121の電圧を測定することにより電池残量が少なくなったことを通知する電池残量検知IC120に接続されている。DC-DC変換器116は、ダイオード119を介して電池121に接続され、リセットIC118、および、LCD102に必要な電圧に昇圧するLCD電源用昇圧回路117は、電池121に接続されている。

【0038】

また、CPU111a、およびVoIPブロック111bは、ローカルバス111eを介して、マイク104からの信号を増幅するアンプ122、および、スピーカ106への信号を増幅するアンプ123に接続されている。アンプ122、123はそれぞれ、マイク104およびスピーカ106に接続されている。さらに、ベースバンドIC111は、キーマトリックス103、ベースバンドICにクロックを供給する発振器115、無線モジュール124、および使用するアンテナをベースバンドIC111から切り替えるアンテナ切り替えSW(Switch)126に接続されている。

【0039】

無線モジュール124は、送受信切り替えSW124aと、受信信号を増幅するLNA(Low Noise Amplifier)124bと、送信信号を増幅するPA(Power Amplifier)124cと、無線信号への変調および無線信号からの復調を行うRF(Radio Frequency)変復調器124dとを有している。また、無線モジュール124は、無線モジュール124にクロックを供給する発振器125、およびアンテナ切り替えSW126に接続されている。アンテナ切り替えSW126は、図1で説明した外部アンテナ105aと、内部アンテナ105bとに接続されている。

【0040】

図3は、管理端末（前面）を示す外観斜視図、図4は、管理端末（背面）を示す外観斜視図である。

【0041】

本実施の形態1における管理端末2は、通信装置の他の一例であって、図3に示すようにルータである。管理端末2は、筐体21を有しており、筐体21の前面には、LED（Light Emitting Diode）などの表示部22が設けられている。筐体21の背面には、図4に示すように、DC電源コネクタ23、RJ45などLAN用モジュージャック24、およびWAN（Wide Area Network）用モジュージャック25が設けられている。DC電源コネクタ23には、図4に示すように、平行ケーブルなどの電力線26が接続される。LAN用モジュージャック24および、WAN用モジュージャック25には、LANケーブル27が接続される。なお、管理端末の一例として、図3および図4のルータを示したが、特にこれに限る必要はなく、管理端末は、アクセスポイントの機能を備えた機器（例えばテレビなどの家電機器）であってもよい。

10

【0042】

図5は、管理端末のハードウェアの一例を示すブロック図である。

【0043】

管理端末2は、図5に示すように、破線で示す筐体21内に、回路モジュール210を有している。回路モジュール210には、メインIC211と、無線LANコントローラ219と、無線モジュール220とが実装されている。

20

【0044】

メインIC211は、CPU211aと、メインバス211fやローカルバス211gなどのバスと、バス上のデータの流れを制御するBCU（Bus Control Unit）211bと、Ethernet（登録商標）のMAC層を制御するMACブロック（EMAC）211c、211dと、PCI（Peripheral Component Interconnect Unit）バスを制御するPCIU211eとを有している。

【0045】

メインIC211内のCPU211aおよびBCU211bは、メインバス211fを介して、SDRAM214と、Flash ROM215とに接続されている。また、CPU211aおよびBCU211bは、ローカルバス211gを介して、メインIC211にクロックを供給する発振器212と、LEDなどの表示部22と、メインIC211に初期化信号を出力するリセットIC213とに接続されている。

30

【0046】

メインIC211内のMACブロック211c、211dはそれぞれ、Ethernet（登録商標）の物理層を制御するPHY（Physical layer）・IC216、217に接続されており、PHY・IC216、217はそれぞれ、WAN用モジュージャック24、LAN用モジュージャック25に接続されている。また、メインIC211は、DC-DC変換器218を介して、DC電源コネクタ23に接続されている。

40

【0047】

DC-DC変換器218は、DC電源コネクタ23から供給されるDC電圧をメインIC211で必要なDC電圧に変換する。

【0048】

無線LANコントローラ219は、MAC層を制御するMACブロック219aと、物理層を制御するPHYブロック219bとを有している。メインIC211内のPCIU211eは、MACブロック219aを介して、PHYブロック219bに接続されている。

【0049】

50

無線モジュール 220 は、メイン IC 211 から送信または受信状態が設定され、送受信切り替え SW 220 a と、受信信号を増幅する LNA 220 b と、送信信号を増幅する PA 220 c と、無線信号への変調および無線信号からの復調を行う RF 変復調器 220 d とを有している。

【0050】

無線モジュール 220 は、無線モジュール 220 にクロックを供給する発振器 221 に接続され、無線モジュール 220 内の RF 変復調器 220 d は、無線 LAN コントローラ 219 内の PHY ブロック 219 b に接続されている。無線モジュール 220 内の送受信切り替え SW 220 a は、メイン IC 211 から使用するアンテナを切り替えるアンテナ切り替え SW 212 を介して、アンテナ 213、214 に接続されている。

10

【0051】

図 6 は、通信端末および管理端末の機能ブロック図である。図 7 は、下り回線の制御フローを示す図である。図 8 は、下り回線制御フローの時間軸上での概念図である。図 9 は、モバイル環境での下り回線の制御フローを示す図である。図 10 は、上り回線の制御フローを示す図である。図 11 は、事前処理部の機能ブロック図である。図 12 は、事前処理部の動作を示したタイミングチャートを示す図である。図 13 は、事後処理部の機能ブロック図である。図 14 は、事後処理部の動作を示したタイミングチャートを示す図である。

【0052】

まず、図 6 を用いて全体の処理の概要について説明する。通信端末 1 a、1 b および管理端末 2 の事前処理部 302、314 で送信すべきメッセージに事前処理を施す。この後、その出力を変調部 303、313 で変調して無線部 304、309、アンテナ 105 a、105 b、308 を介して通信相手に送信する。次に、送信された信号は、アンテナ 105 a、105 b、308、無線部 304、309 を介して復調部 306 および 310 に入力される。復調された信号は、事後処理部 305、312 に入力される。例えば伝送誤りが存在しても、正規の受信者の事後処理部 305、312 では、単位ビット当たりのエネルギーが、伝送誤りが訂正されるレベルまで増幅される。

20

【0053】

図 6 と図 2 を対比すると、図 6 の無線部 304 は、図 2 のベースバンド IC 111 に対応し、図 6 の事前処理部 302、変調部 303、復調部 306、事後処理部 305 は、図 2 の無線モジュール 124 に対応する。

30

【0054】

同様に、図 6 と図 5 を対比すると、図 6 の無線部 309 は、図 5 の無線 LAN コントローラ 219 に対応し、図 6 の事前処理部 314、変調部 313、復調部 310、事後処理部 312 は、図 5 の無線 LAN コントローラ 219 に対応する。

【0055】

次に、図 11 と図 12 を用いて事前処理部 302 および 314 の詳細な処理について説明する。まず、送信データはリサンプリング部 401 に入力される。リサンプリング部 401 に入力された信号は、図 12 に示すように、送信データ 1 ビットの周期がテンプレート 1 周期の長さまで拡張される。

40

【0056】

すなわち、送信データは N ビットとすると、送信データは M ビットのビット長に複製されることになる。N、M の条件は、N は 1 以上の整数、M は 2 以上の整数、 $N < M$ である。図 12 の説明では、 $N = 1$ 、 $M = n$ の場合を示しているが、N、M は、上記条件の範囲で任意である。

【0057】

図 12 において、A、B、C、a1、a2、a3 は各々 1 ビット（2 値信号）を示す。ここでは、これらは +1 または -1 の値をとるものとする。テンプレート 1 周期の長さまで拡張された送信データ 1 ビットに対して乗算器 402 でテンプレートと乗算される。

【0058】

50

次に、図 1 3 と図 1 4 を用いて事後処理部 3 0 5 および 3 1 2 の詳細な処理について説明する。まず、受信したデータは乗算器 5 0 1 に入力される。乗算器 5 0 1 に入力された信号は、送信側と同じテンプレートと乗算される。図 1 4 に示すように、この乗算出力は、テンプレート 1 周期の間、積分器 5 0 2 で積分される。そして判定部 5 0 3 において、積分器 5 0 2 の出力が 0 以上の時には + 1 を、積分器 5 0 2 の出力が負の時には - 1 を出力する。そして、図 1 4 に示すように、判定部 5 0 3 の出力はビットの周期は、デサンプリング部 5 0 4 において元の周期に戻される（つまりビット長を短縮する）。ここで、乗算器 5 0 1 と積分器 5 0 2 の組み合わせの処理を整合フィルタということもある。

【0059】

事後処理を施された後の単位ビット当たりのエネルギーについて考える。本発明では、図 1 4 に示すように、積分出力 $n \cdot A$ の極性（0 以上または負）を判定することで、受信データのビットを復調する。従って、伝送路上のノイズなどに起因して伝送誤りが発生しても、積分出力 $n \cdot A$ の極性が反転しなければ、受信データは正しく復調される。このことは、本発明が、その分だけ伝送誤りに耐性を有していることを示している。この場合、積分する長さ n が大きい程、積分出力 $n \cdot A$ は大きくなり、伝送誤りへの耐性つまり雑音への耐性が改善されることがわかる。

【0060】

次に、図 7 と図 8 を用いて、下り回線の制御処理のフローを説明する。システムが想定する最大通信距離に相当する、管理端末の送信電力を P_0 とし、管理端末の送信電力の制御幅を Δ とする。 Δ の初期値をゼロとする。ここで、図 7 のステップ S 1 0 3 において、通信端末の整合フィルタ（MF）の出力を R_m とする。 R_m は受信電力の一例であって、具体的には、積分器 5 0 2 の出力 $n \cdot A$ である。 R_m は、ノイズなどの外因を含まない受信電力を意味し、換言すれば、信号成分のみの電力を表している。

【0061】

次のステップ S 1 0 4 において R_m と閾値 T_{ma} を比較する。閾値 T_{ma} は第 1 の閾値の一例である。 R_m が閾値 T_{ma} より大きい場合には、ステップ S 1 0 5 において、送信電力の制御幅 $\Delta = \Delta - \Delta P$ ($\Delta P > 0$) にして、ステップ S 1 0 2 に戻り送信電力を ΔP だけ小さくする。ステップ S 1 0 4 において R_m が閾値 T_{ma} より小さい場合には、次のステップ S 1 0 6 に進む。ステップ S 1 0 6 において、 R_m が閾値 T_{mi} より小さい場合には、ステップ S 1 0 7 において、整合フィルタのテンプレート長を $\Delta P T L$ だけ長くして、ステップ S 1 0 3 に戻る。閾値 T_{mi} は第 2 の閾値の一例である。第 2 の閾値は第 1 の閾値より小さい値である、関係にある。

【0062】

ステップ S 1 0 7 では、送信データを複製するビット長が M ビットから K ビットに変更される。この場合、 K 、 M の条件は、 K は 1 以上の整数、 $K \neq M$ である。本実施の形態 1 では、 $M = n$ 、 $K > n$ の条件であるが、 K は、上記の範囲で任意である。送信データが存在する場合は、リサンプリング部 4 0 1 は、 $T L + \Delta P T L$ のテンプレート長に対応したビット長まで、送信データを複製する。

【0063】

ステップ S 1 0 6 において、 R_m が閾値 T_{mi} より大きい場合には、通常の通信の処理に進む。図 8 は、以上の処理フローを時間軸上で示したもので、縦軸は整合フィルタの出力 R_m である。

【0064】

以上の処理においては、送信電力は一方的に減少するだけであり、整合フィルタのテンプレートは一方的に長くなるだけである。もし、移動通信時のように、受信信号レベルが大きく変動するような場合には、度々、フェージングなどによって受信信号レベルが大きく落ち込むことがあるが、その度にテンプレート長を長くすると、通信のオーバーヘッドが非常に大きくなり、リアルタイムでの双方向通信が行えなくなる。図 9 は、そのような環境でもリアルタイムでの双方向通信が行えることを目的とした下り回線の制御処理のフローである。

【0065】

図9について説明する。システムが想定する最大通信距離に相当する、管理端末の送信電力を P_0 とし、管理端末の送信電力の制御幅を Δ とする。 Δ の初期値をゼロとする。ここで、図9のステップS203において、通信端末の整合フィルタ(MF)の出力を R_m とする。次のステップS204において R_m と閾値 T_{ma} を比較する。 R_m が閾値 T_{ma} より大きい場合には、ステップS205において、送信電力の制御幅 $\Delta = \Delta - \Delta P$ ($\Delta P > 0$)にして、ステップS202に戻り送信電力を ΔP だけ小さくする。ステップS204において R_m が閾値 T_{ma} より小さい場合には、次のステップS206に進む。ステップS206において、 R_m が閾値 T_{mi} より小さい場合には、ステップS207において、整合フィルタのテンプレート長を ΔPTL だけ長くして、ステップS208に進む。ステップS208において、テンプレート長 TL と閾値 TL_{ma} とを比較する。ステップS208において、テンプレート長 TL が閾値 TL_{ma} より小さい場合には、ステップS203に戻る。ステップS208において、テンプレート長 TL が閾値 TL_{ma} より大きい場合には、次のステップS209において、テンプレート長を $2\Delta PTL$ だけ小さくなるように設定する。さらに次のステップS210において、送信電力を ΔP だけ大きくなるように設定する。そして次のステップS211において、送信電力 $T_x P$ と P_0 を比較して、送信電力 $T_x P$ が P_0 より小さい場合にはステップS202に戻り、送信電力を上げて送信する。ステップS211において、送信電力 $T_x P$ が P_0 より大きい場合には、ステップS212において、送信電力を ΔP だけ小さくなるように設定して、ステップS202に戻り、結局送信電力を変えずに、再送信する。ステップS206において、 R_m が閾値 T_{mi} より大きい場合には、通常の通信の処理に進む。

【0066】

次に、図10を用いて、上り回線の制御処理のフローを説明する。システムが想定する最大通信距離に相当する、通信端末の送信電力を P_0 とし、通信端末の送信電力の制御幅を Δ とする。 Δ の初期値をゼロとする。ここで、図10のステップS303において、管理端末の整合フィルタ(MF)の出力を R_m とする。次のステップS304において R_m と閾値 T_{ma} を比較する。 R_m が閾値 T_{ma} より大きい場合には、ステップS305において、送信電力の制御幅 $\Delta = \Delta - \Delta P$ ($\Delta P > 0$)にして、ステップS302に戻り送信電力を ΔP だけ小さくする。ステップS304において R_m が閾値 T_{ma} より小さい場合には、次のステップS306に進む。ステップS306において、 R_m が閾値 T_{mi} より小さい場合には、ステップS307において、整合フィルタのテンプレート長を ΔPTL だけ長くして、ステップS303に戻る。ステップS306において、 R_m が閾値 T_{mi} より大きい場合には、通常の通信の処理に進む。

【0067】

次に閾値 T_{ma} と T_{mi} について説明する。受信信号のレベル変動の幅に比べて T_{ma} と T_{mi} の差が小さいと整合フィルタ出力 R_m が T_{ma} と T_{mi} の間に入る確率が小さくなり、通常の通信の処理時間が短くなり、リアルタイムでの双方向通信が困難になる。そこで、所定の通信時間を確保する必要がある場合には、整合フィルタ出力 R_m の変動幅をモニターし、所定の通信時間を確保できるように、整合フィルタ出力 R_m が T_{ma} と T_{mi} の間に入るように T_{ma} を設定する。ここで、 T_{mi} は、所定の通信品質の最小値に相当する整合フィルタ出力 R_m になるように設定する。

【0068】

以上のように、本実施の形態1では、受信電力に応じて送信データを複製するビット長を変更するので、受信電力が変動した場合であっても、セキュリティを確保しながら第三者への S/N 比を上げることなく、正規の受信者への S/N 比のみを向上させることができる。

【0069】

また、受信電力が所定値より小さい場合に、送信データが複製されるビット長を K ビット($M < K$)に変更するので、受信電力が低下した場合に、正規の受信者への S/N 比低下を抑制することができる。

【0070】

また、送信データの電力を制御する送信電力制御手段を備え、送信電力制御手段は、受信電力が所定値より小さい場合に、送信電力を低下させるので、ビット長を長く変更することなく、送信電力を低下することで、オーバーヘッドの増大を抑制しながら、通信エリアの不要な拡大を防止することができる。

【0071】

また、受信電力が第1の閾値より小さい場合に、送信データの電力を低下させ、さらに、受信電力が第1の閾値より小さい第2の閾値より小さい場合に、送信データを複製するビット長を変更するので、受信電力が低下する場合に、送信データの電力を優先した上で、乱数を乗算する送信データの複製範囲を変更するので、通信エリアの不要な拡大を防止した上で、その通信エリア内に存在する正規の受信者へのS/N比低下を抑制することができる。

10

【0072】

(実施の形態2)

以下、本発明の具体的な内容について実施の形態2を用いて説明する。なお、通信端末1a、1bおよび管理端末2の構成は、実施の形態1における図1ないし図6、図11および図13と共通である。

【0073】

図16は、実施の形態2における鍵生成共有シーケンスを示す図である。図16を用いて全体の処理の概要について説明する。

20

【0074】

ステップS501において、管理端末2と通信端末1a（または通信端末1b）はともに、送信電力制御を行う。この処理は、実施の形態1における図7および図10に示される処理と同じである。これらの処理により、親機と子機が正常に受信可能な最小の送信電力出力となるように、親機と子機の送信電力が制御される一方で、盗聴者が正常に受信出来る領域の広さを最小限に抑える。

【0075】

次に、ステップS502において、通信端末1aで符号化データCDを生成する。符号化データCDを生成するための構成は図11と同じである。符号化データCDは、管理端末2、通信端末1a、1b間で既知のデータである。ここでは、複数ビットで構成され、全てが同じ値である。例えば、オール1（1、1、・・・、1）、オール0（0、0、・・・、0）、オール-1（-1、-1、・・・、-1）。

30

【0076】

図6に示す事前処理部302において、リサンプリング部401は、「1」の値からなる送信データ1ビットの周期がテンプレート1周期の長さまで拡張する。ここでは発明の理解を容易にするため、テンプレートの1周期を5ビットとする。従って、リサンプリング部401は、オール1（1、1、1、1、1）で構成される、符号化データCDを出力する。テンプレートが（1、-1、-1、1、1）とすると、乗算器402は、符号化データCDとテンプレートを乗算して、（1、-1、-1、1、1）を出力する。

【0077】

40

通信端末1aの変調部303で所定の変調処理を行い、無線部304は、乗算器402の出力値（1、-1、-1、1、1）に基づく送信データを管理端末2に送信する。送信データが空中の伝送媒体を介して伝送されるが、雑音などの周囲の環境によっては送信データに伝送誤りが生じる。ここでは、伝送誤りによって（1、-1、-1、1、1）の2ビット目と4ビット目が誤り、値が反転したとする。その結果、（1、-1、-1、1、1）が（1、1、-1、-1、1）に変化したことになる。

【0078】

ステップ503において、管理端末2は、送信データを受信すると、鍵シーケンスKを生成する。この処理を、図17を用いて説明する。

【0079】

50

図 17 は、実施の形態 2 における鍵シーケンス生成を示すブロック図である。

【0080】

17 において、管理端末 2 の復調部 310 は、受信された送信データについて復調処理を行い、受信信号（1、1、-1、-1、1）（つまり伝送誤りが生じた乗算器 402 の出力値）を、事後処理部 312 に出力する。事後処理部 312 は、受信信号（1、1、-1、-1、1）を受信信号用シフトレジスタ 601 に入力する。具体的には、受信信号用シフトレジスタ 601 に、図 17 の紙面左から右に掛けて、（1、1、-1、-1、1）が入力される。

【0081】

一方、リファレンスシフトレジスタ 602 には、通信端末 1a と同一のテンプレート（1、-1、-1、1、1）が格納されている。図 17 に示すような対応では、受信信号用シフトレジスタ 601 とリファレンスシフトレジスタ 602 の対応する各ビット同士の排他的論理和が、乗算器 603 で処理される。その結果、各乗算器 603 の出力は鍵シーケンス格納用シフトレジスタ 604 の対応するレジスタに格納される。全ての乗算器 603 の出力が、図 17 紙面上から下に掛けて、レジスタ 604 に（1、-1、1、-1、1）が格納され、それらの値は鍵シーケンス K として出力される。なお、乗算方法は特に排他的論理和に限定されず、他の演算方法でも良い。

【0082】

なお、この場合、仮に、送信データが通信端末 1a から管理端末 2 に伝送される際に、伝送誤りが全く発生していなければ、鍵シーケンス K は、乗算器 402 の出力値（1、-1、-1、1、1）と一致する。

【0083】

ステップ 504 において、鍵シーケンス K（1、-1、1、-1、1）が生成されると、これをもとにして、マスター鍵が生成される。この処理を、図 18 を用いて説明する。

【0084】

図 18 は、マスター鍵生成フローを示す図である。

【0085】

ステップ S601 において、図 16 のステップ S501 で設定された通信端末 1a の送信電力が設定される（つまり、通信端末 1a の送信信号レベル TxP が P0 に設定される）。ステップ S602 において、管理端末 2 は、鍵シーケンス K を生成する。ステップ S603 において、管理端末 2 は、鍵シーケンス K 中の 1 の数と -1 の数の差が所要値以下かどうか判断する。鍵シーケンス K の 1 の数と -1 の数の差が所定値以下でない場合（ステップ S603 の No）、ステップ S604 において、管理端末 2 は、送信信号レベル TxP を P0 から Δ だけ減算するように、通信端末 1a に指示する。通信端末 1a は管理端末 2 からの指示に従って、送信電力が制御し、送信信号レベル TxP を P0 から Δ だけ減算する（ステップ S601）。

【0086】

一方、鍵シーケンス K の 1 の数と -1 の数の差が所定値以下の場合（ステップ S603 の Yes）、ステップ S605 において、管理端末 2 は、鍵シーケンス K をマスター鍵として出力する。このような鍵シーケンス K を、実際に用いる暗号鍵であるセッション鍵のシードとして使用するので、マスター鍵の推測を困難にすることが出来る。

【0087】

本実施の形態で、ステップ S603 の所定値が「2」とすると、鍵シーケンス K は、（1、-1、1、-1、1）で、1 の数と -1 の数の差は「1」であるから、鍵シーケンス K は（1、-1、1、-1、1）として生成が完了する。仮に、鍵シーケンス K がオール 1 となった場合、差は「5」になるので、送信電力を落とすことになる。

【0088】

鍵シーケンス K における「1」と「-1」の分布に適度なバランスがある場合は、それ自体は鍵シーケンス K として次の処理を進めるが、鍵シーケンス K における値の分布がアンバランスな場合は、送信電力を下げるので、鍵シーケンス K がオール 1 または -1 の分

10

20

30

40

50

布に遷移して、鍵シーケンスKの分布が適度なバランスとなる。このように、送信電力を制御することで、鍵シーケンスKにおける「1」と「-1」の分布に適度なバランスに設定することが出来るので、鍵シーケンスKを用いた暗号鍵の推測を困難にすることが出来る。

【0089】

次に、管理端末2はマスター鍵を通信端末1aに送信し、管理端末2と通信端末1aでマスター鍵を共有する。共有方法は、暗号化してから送信してもよく、送信電力を落とした近距離通で暗号化することなく送信することも可能である。さらにユーザが手入力で共有されることも可能である。

【0090】

ステップ505において、管理端末2と通信端末1aは、共有したマスター鍵から、実際の暗号化に用いる、同じセッション鍵を生成する。セッション鍵の生成について、図19を用いて説明する。

【0091】

図19は、セッション鍵生成を示す説明図である。

【0092】

図19において、鍵 $K1_i$ ($i=0, 1, 2, 3, 4$)は鍵 $K1_0$ を i ビット巡回シフトした鍵シーケンスである。 $H(K1_i || K2_j)$ は、 $K1_i$ と $K2_j$ を連結した結果のハッシュ値であり、これをセッション鍵とする。この方法により、長さNの2個のマスター鍵から N^2 個という非常に多くのセッション鍵を生成することが可能となる。つまり、セッション鍵を頻繁に更新して使うことが容易となり、それだけ安全性の高い鍵共有システムとなる。

【0093】

以上のように、実施の形態2では、セッション鍵を生成するのに、予測不可能な物理乱数である、雑音による伝送誤りの情報を利用するので、セッション鍵の予測が困難なものとなり、これを暗号鍵として用いると、安全性の高い暗号システムを構築すること出来る。

【0094】

なお、本実施の形態2では、通信相手の送信電力制御を必要としたが、通信相手の送信電力制御の代わりに、自身の受信系において増幅器の利得制御を行うことでも同様の効果を得ることが出来る。

【0095】

また、本実施の形態では、通信相手の符号化データを用いたが、受信信号電力が所要値以上で、ある程度の通信品質が確保されている時に、符号化データ受信以降の処理を行えば、同様の効果を得ることが出来る。

【0096】

以上のような代替の方法を用いれば、通信相手の実装内容に関わらず、自身の実装のみで、前記の非常に高い安全性を有する暗号システムを構築出来る。

【0097】

なお、上記実施の形態1、2は、無線通信について説明したが、有線通信であっても良い。例えば、イーサネット（登録商標）、PLC（電力線通信）、電話線、同軸ケーブルを用いた通信媒体など各種を利用することが出来る。

【産業上の利用可能性】

【0098】

本発明の通信装置、通信システムおよび通信方法は、不正アクセスや盗聴への耐性を有するとともに、高い伝送信頼性を確保するため、伝送路が第3者にも共用されている他、劣悪である無線や電力線を使った通信に適用出来る。

【符号の説明】

【0099】

1a 通信端末

10

20

30

40

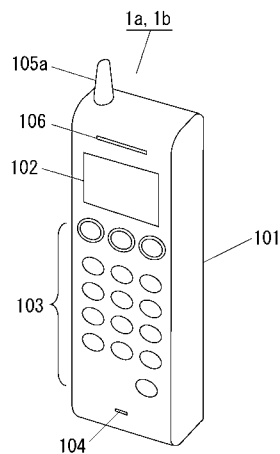
50

- 1 b 通信端末
- 2 管理端末
- 3 0 2 通信端末の事前処理部
- 3 0 3 通信端末の変調部
- 3 0 4 通信端末の無線部
- 3 0 5 通信端末の事後処理部
- 3 0 6 通信端末の復調部
- 3 0 8 管理端末のアンテナ
- 3 0 9 管理端末の無線部
- 3 1 0 管理端末の復調部
- 3 1 2 管理端末の事後処理部
- 3 1 3 管理端末の変調部
- 3 1 4 管理端末の事前処理部
- 4 0 1 事前処理部のリサンプリング部
- 4 0 2 事前処理部の乗算器
- 5 0 1 事後処理部の乗算器
- 5 0 2 事後処理部の積分器
- 5 0 3 事後処理部の判定部
- 5 0 4 事後処理部のデサンプリング部
- 6 0 1 受信信号用シフトレジスタ
- 6 0 2 リファレンスシフトレジスタ
- 6 0 3 乗算器
- 6 0 4 鍵シーケンス格納用シフトレジスタ

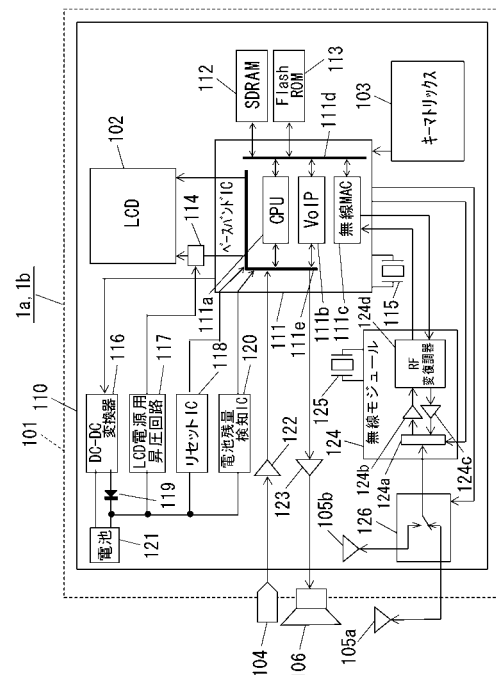
10

20

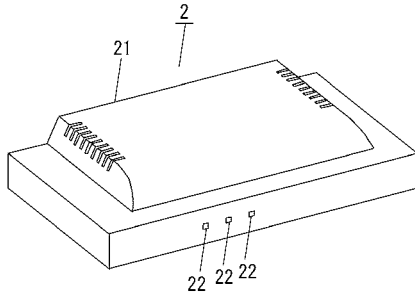
【図 1】



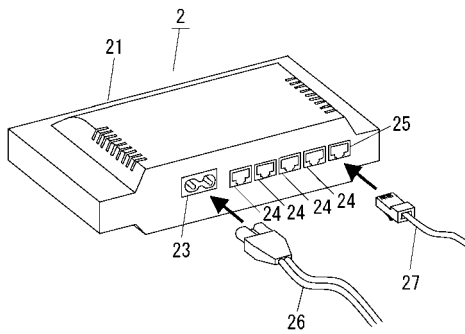
【図 2】



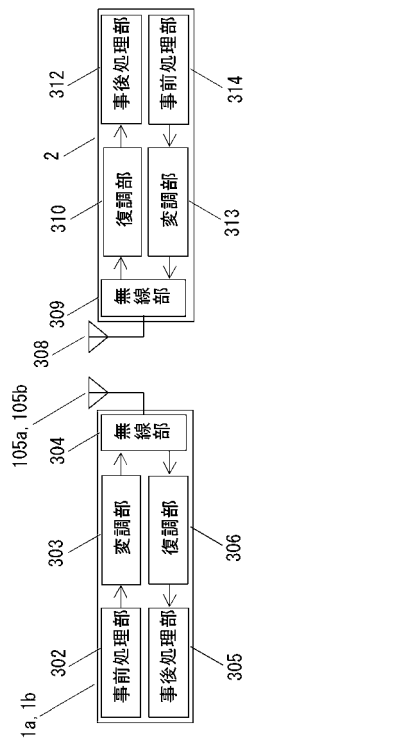
【図 3】



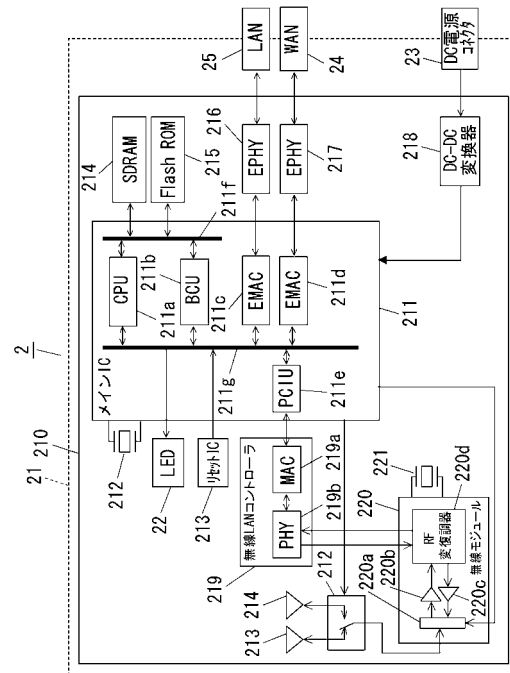
【図 4】



【図 6】

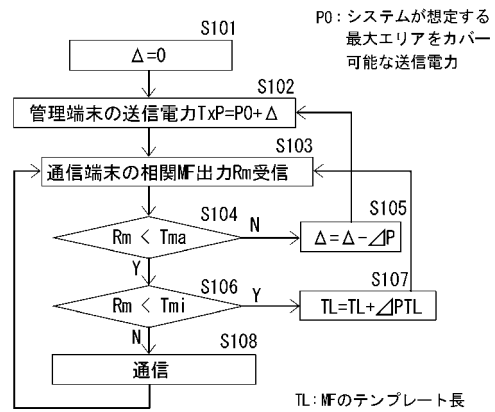


【図 5】

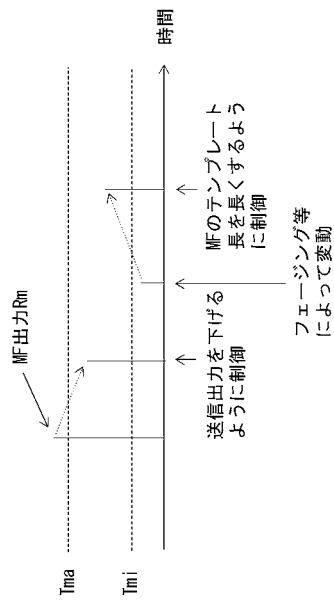


【図 7】

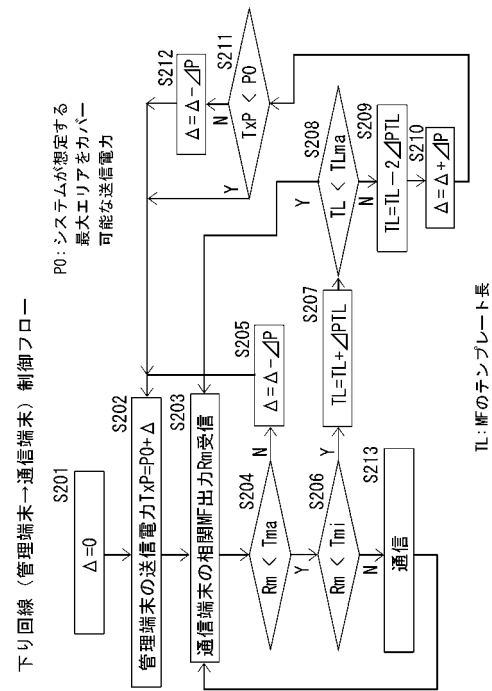
下り回線（管理端末→通信端末）制御フロー



【図 8】

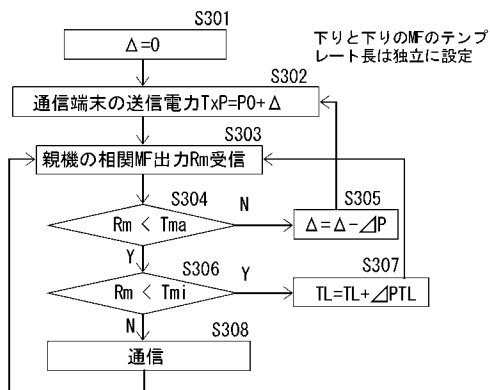


【図 9】

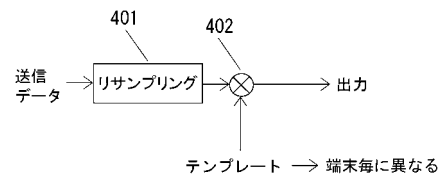


【図 10】

上り回線（通信端末→管理端末）制御フロー

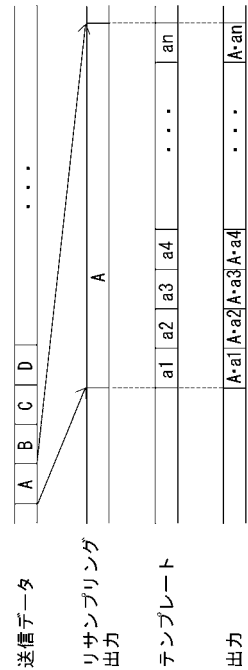


【図 11】

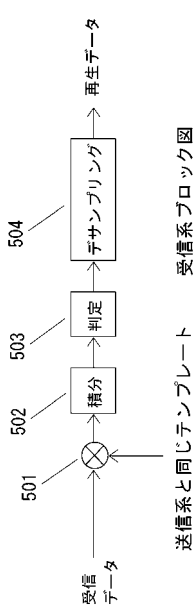


事前処理部の機能ブロック図

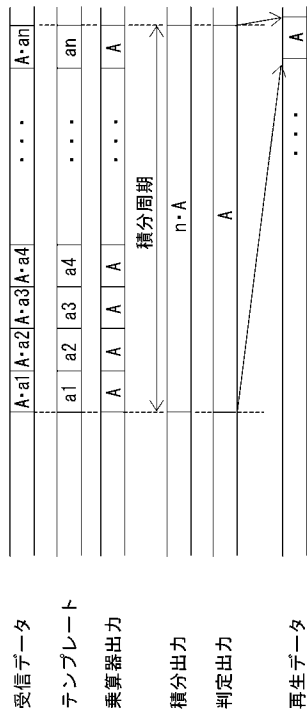
【図 1 2】



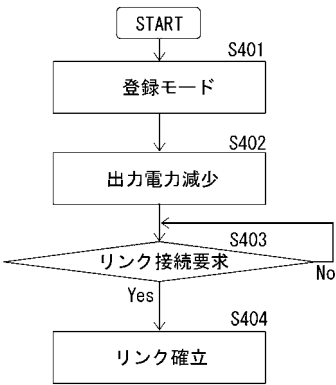
【図 1 3】



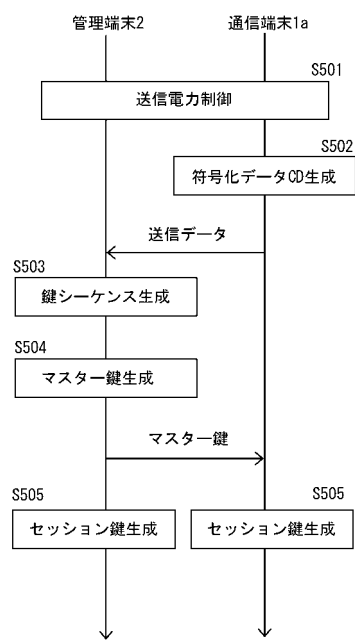
【図 1 4】



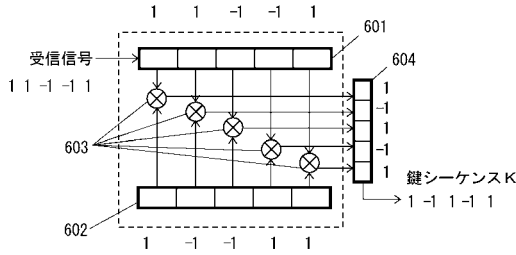
【図 1 5】



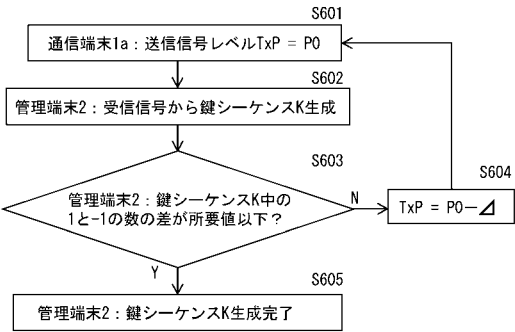
【図 1 6】



【図 1 7】



【図 1 8】



【図 1 9】

